ReSPA
Регионална школа
за јавна администрација

Злоупотреба на информатичката технологија (IT) за корупциски цели

Активностите на РеСПА
се финансирани од
Европската унија

РеСПА е заедничка иницијатива на Европската унија и земјите од Западен Балкан, која работи во насока на поттикнување и зајакнување на регионалната соработка помеѓу земјите-членки во областа на јавната администрација. РеСПА се стреми да понуди иновативни и креативни обуки, активности за вмрежување, градење на капацитети и консултантски услуги со цел да се обезбеди дека сите јавни администрации на земјите од регионот ќе се посветат на заедничките вредности на почитување, толеранција, меѓусебна соработка и интеграција.

Превод: Порта Аперта, Подгорица

КОНТАКТ ИНФОРМАЦИИ:
Регионална школа за јавна администрација
Браneловица
П.Фах 31, 81410
Даниловград, Црна Гора

тел.: +382 (0)20 817 200
www.respaweb.eu
e-mail: respa-info@respaweb.eu

CIP – Каталогизација у публикацији
Национална библиотека Црне Горе, Цетиње

ISBN 978-9940-37-003-9
COBISS.CG-ID 29069072

Автори

РеСПА

Горан Пастровиќ, *менаџер за обуки*

Меѓународни автори

Вовед, осврти на поглавјата 1 и 2, под-поглавје 2.9 и Поглавје 3
Тилман Хопе, *експерт за антикорупција*
Вера Девин, *експерт за антикорупција*
Луизе Томасен, *експерт за е-Влада*

Автори од државите

Албанија

Едљира Наси, *експерт за антикорупција*
Енед Керцини, *експерт за е-Влада*

Босна и Херцеговина

Александра Мартиновиќ, *експерт за антикорупција*
Срѓан Ного, *експерт за е-Влада*

Хрватска

Зорислав Петровиќ, *експерт за антикорупција*
Ивана Андријашевиќ, *експерт за е-Влада*

Косово*

Хасан Претени, *експерт за антикорупција*
Дриарт Елшани, *експерт за е-Влада*

Македонија

Марјан Стоилковски, *експерт за антикорупција*
Розалинда Стојова, *експерт за е-Влада*

Црна Гора

Душан Дракиќ, *експерт за антикорупција*
Иван Лазаревиќ, *експерт за е-Влада*

Србија

Немања Ненадиќ, *експерт за антикорупција*
Бојан Цветковиќ, *експерт за е-Влада*

* Со ваквото именување не го прејудицираме статусот на Косово и истото е во согласност со Резолуцијата 1244 на Советот на безбедност и мислењето на Меѓународниот суд на правдата во однос на

Предговор

Суад Мусиќ,
директор на РеСПА

Членот 48, став 3 од Конвенцијата на Обединетите нации против корупцијата (UNCAC) вели дека:

„Државите членки ќе настојуваат да соработуваат, во рамките на своите можности, за да го спречат извршувањето на делата наведени во оваа Конвенција а извршени со употреба на модерна технологија“.

Сè до денес, меѓународните организации не ѝ посветуваа големо внимание на оваа одредба. Всушност, Техничкиот водич за имплементација на UNCAC[1] го содржи следново, и тоа само како насока:

“Ставот 3 (од членот 48) ја признава сè поголемата употреба на компјутерската технологија за извршување на голем број кривични дела кои се опфатени со Конвенцијата и ги повикува Државите членки да настојуваат потесно да соработуваат за да можат соодветно да реагираат на коруптивни кривични дела кои се извршени со употреба на модерна технологија“.

Оваа компаративна студија има цел за прв пат да даде конкретни насоки така што ќе укаже на конкретни случаи на злоупотреба на „модерната технологија“ (IT) за коруптивни кривични дела како и на можните чекори кои можат да се преземат со цел да се обезбеди заштита од таквите злоупотреби.

РеСПА повеќе години е активна на две полиња: интегритет и е-Влада. Со своите регионални мрежи на експерти во овие две полиња РеСПА е во одлична позиција истите да ги обедини во едно, во насока на взаемна корист. Во однос на релевантноста за имплементацијата на UNCAC, ефектот од оваа студија ќе се почувствува во регионот на Западен Балкан а ќе излезе и во меѓународни рамки и тоа многу пошироко од вкупно 172-те Држави членки на UNCAC.

1 U.NODC, 2009, www.unodc.org/unodc/en/treaties/CAC/technical-guide.htmlSS

Садржај

Кратенки

АИ	Административно упатство
АСПА	Школа за јавна администрација на Албанија
БиХ	Босна и Херцеговина
ЦА	Орган за сертификација (Македонија)
CARNet	Хрватска академска и истражувачка мрежа
CCTV	Затворен видео систем
CERT	Компјутерски тим за брзи реакции
CIPS	Систем за заштита на идентификацијата на граѓаните (во Босна и Херцеговина)
COC	Команден оперативен центар (Србија)
CPI	Индекси за перцепција на корупцијата
CSIRT	Тим за реакции во случај на инцидент поврзан со компјутерската безбедност
CAA	Дирекција за цивилна воздушна пловидба (Албанија)
DDoS	Distributed Denial of Service/ Дистрибуирано одбивање на услуга
DECO	Сектор за кривични дела поврзани со економски криминал (Хрватска)
DMS	Систем за управување со документи
DORH	Општинска канцеларија на јавниот обвинител во Дубровник
ENP	Електронска наплата на патарината (Србија)
ERE	Енергетско регулаторно тело на Албанија
e-SEE	Електроника Југоисточна Европа
EU	Европска унија
EUPM	Полициска мисија на Европската унија во Босна и Херцеговина
FTP	File Transfer Protocol/ Протокол за трансфер на датотеки
HAC	Хрватски автопатишта
HDZ	Хрватска демократска заедница
HJCP	Виш судски и обвинителски совет (Босна и Херцеговина)
HJPC	Виш судски и обвинителски совет (Босна и Херцеговина)
HNS	Хрватска народна партија
HRT	Хрватска радиотелевизија
HZMO	Хрватски институт за пензиско осигурување
ICT	Информатичко – комуникациска технологија
IDDEEA	Агенција за документи за идентификација, регистри и размена на податоци (Босна и Херцеговина)
IDS	Систем за откривање на упади
IMPACT	Меѓународно мултилатерално партнерство против компјутерски закани
IPA	Инструмент за претпристапна помош (Босна и Херцеговина)
ISO	Меѓународна организација за стандардизација
ISP	Давател на интернет услуги
IT	Информатичка технологија

JPTC	Центри за обука на правосудството и обвинителството (Босна и Херцеговина)
MIST	Министерство за информатичко општество и телекомуникации
МТСП	Министерство за труд и социјална политика (Македонија)
МО	Министерство за одбрана
МВР	Министерство за внатрешни работи
МП	Министерство за правда
МПЈА	Министерство за правда и јавна администрација (Србија)
MPALSGHR	Министерство за јавна администрација, локална самоуправа и човекови права (Србија)
MUP	Министерство за внатрешни работи на Хрватска
NACS	Национална агенција за компјутерска безбедност (Албанија)
NAIS	Национална агенција за информатичко општество (Албанија)
NDA	Договор за необјавување на информации
NFC	Near-Field communication/ Комуникација на кратко поле
НВО	Невладини организации
OIB	Матичен број (Хрватска)/ Единствен број за идентификација
PARCO	Канцеларија за реформа на јавната администрација (Босна и Херцеговина)
PDA	Персонален дигитален асистент
PKI	Јавна клучна инфраструктура
УЈП	Управа за јавни приходи (Македонија)
SAI BiH	Врховен завод за ревизија на Босна и Херцеговина
SAI RS	Врховен завод за ревизија на Република Српска
ДКСК	Државна комисија за спречување на корупцијата (Македонија)
SDH	Синхрона дигитална хиерархија
SDP	Социјалдемократска партија (Босна и Херцеговина)
SDS	Српска демократска партија (Босна и Херцеговина)
SIPA	Државна агенција за истрага и заштита
SNSD	Партија на независни социјалдемократи (Босна и Херцеговина)
СОА	Агенција за безбедност и разузнавање (Хрватска)
SOP	Стандардни оперативни процедури
SSA	Врховен завод за ревизија (Албанија)
SSL	Secure Sockets Layer/ Сигурносен слој на штекерот
TCMS	Систем за целосно управување со случаи (Босна и Херцеговина)
TIMS	Систем за целосно управување со информации (Албанија и Србија)
UNODC	Канцеларија на Обединетите нации за борба против дрогата и криминалот
USKOK	Биро за сузбивање на корупцијата и организираниот криминал во Хрватска
VM	Министерство за воени ветерани (Хрватска)
VPN	Виртуелна приватна мрежа
VSOA	Воена агенција за безбедност и разузнавање (Хрватска)
WAN	Wide Area Network/ Мрежа на широко подрачје

Вовед

Подготвено од Тилман Хопе

Објавени се голем број публикации кои укажуваат на тоа како корупцијата може да се **спречи** преку доброто користење на информатичките технологии, како што се јавни регистри, транспарентност на имотните листови или електронски набавки. Следниве публикации содржат добри примери за методи кои би можеле да се искористат во информатичките системи за борба против корупцијата:

- Tim Davies/Silvana Fumega, “Mixed incentives: Adopting ICT innovations for transparency, accountability, and anti-corruption”, U4 Issue 2014:4, 38 страници[2]
- UNDP, “Fighting Corruption with e-Government Applications”, APDIP e-Note 8/2006, 4 страници[3]
- Spider, “Increasing Transparency & Fighting Corruption Through ICT - Empowering People & Communities”, ICT4D Series no. 3/2010, 102 страници[4]
- Spider, “ICT for Anti-Corruption, Democracy and Education in East Africa”, Spider ICT4D Series no. 6/2013, 96 страници[5]
- Jamshed J. Mistry/Abu Jalal, “An Empirical Analysis of the Relationship between e-government and Corruption”, The International Journal of Digital Accounting Research, Vol. 12, 2012, стр. 145-176[6]
- Ionescu, Luminita, “The Impact That E-Government Can Have on Reducing Corruption and Enhancing Transparency”, Economics, Management and Financial Markets, Vol. 8, no. 2, 2013, стр.210
- Bertot/Jaeger/Grimes, “Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies”, Government Information Quarterly Vol. 27 Issue 3, 2010, стр. 264
- Richard Heeks, “Information Technology and Public Sector Corruption”, Institute for Development Policy and Management, September 1998, 15 страници[7]
- Transnational Crime and Corruption Centre, “Transnational Crime, Corruption, and Information Technology”, Conference Report 2000, 39 страници[8]

Од друга страна, пак, литературата која се однесува на тоа како информатичката технологија може да се искористи како **алатка** за корупција е мошне ограничена или речиси и да не постои. „Независната комисија против корупција“ (Independent Commission against Corruption) од Хонг Конг го има објавено следново:

2 http://www.u4.no/publications/mixed-incentives-adopting-ict-innovations-for-transparen-cy-accountability-and-anti-corruption/.
3 http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan043296.pdf.
4 http://spidercentre.org/polopoly_fs/1.163640.1390315885!/menu/standard/file/Spi-der%20ICT4D%20series%203%20Increasing%20transparency%20and%20fighting%20cor- ruption%20through%20ICT.pdf.
5 http://spidercentre.org/polopoly_fs/1.163057.1390315079!/menu/standard/file/Spi-der%20ICT4D_no6_2013.pdf.
6 www.uhu.es/ijdar/10.4192/1577-8517-v12_6.pdf.
7 http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN015477.pdf.
8 http://traccc.gmu.edu/pdfs/publications/transnational_crime_publications/variou01.pdf.

- “Ethics at Work - A Guide for Business Managers in the Use of IT”, 2003, 77 страници[9], која става акцент на приватниот бизнис сектор.
- Постојат и одреден број случаи во кои органите задолжени за борба против корупцијата ја идентификувале информатичката технологија како коруптивен ризик во јавниот сектор. Ова се два такви примери:
- Kenya Anti Corruption Commission, “Corruption Prevention Guidelines on ICT Systems in the Public Sector”, март 2008 година[10]
- Independent Commission Against Corruption (ICAC) of New South Wales - NSW (Australia), “Knowing your risks: IT systems”[11]

На интернет страницата на Независната комисија против корупцијата (ICAC) од Нов Јужен Велс (NSW), Австралија, се дадени два кратки примери за корупција во јавниот сектор поврзана со информатичките технологии. Исто така, следниве технички прирачници објавени од меѓународни организации кои се однесуваат на корупцијата едвај и да ја споменуваат информатичката технологија како можен ризик:

- UNODC, Антикорупциски алатки на Обединетите нации (трето издание, 2004 година)[12];
- UNODC, Технички водич за UNCAC, 2009 година[13];
- ОБСЕ, Најдобри пракси во борбата против корупцијата, 2004 година[14];
- Транспаренси Интернешенел, Справување со корупцијата: елементи на национален систем за интегритет, IT Source Book, 2000 година[15];
- Прирачник на USAID за проценка на корупцијата (2006 година)[16].

Ваквото отсуство на доволно насоки е во голема мера во спротивност на Конвенцијата на Обединетите нации против корупцијата (UNCAC) која во членот 48, став 3 ги повикува Државите членки да настојуваат да соработуваат, во рамките на своите можности, за да го спречат извршувањето на делата наведени во оваа Конвенција а извршени со употреба на модерна технологија“. Така, она што навистина веќе подолго време недостасува е една сеопфатна регионална студија на оваа тема.

Читателите на оваа студија ќе се запознаат и со конкретни случаи кои покажуваат како сторителите на коруптивни дела ги искористуваат слабостите на информатичките системи и структури за лична корист. Реалните примери за корупција со користење на информатичките системи како и **добрите примери** на нивно спречување и откривање ќе им дадат инспирација на експертите кои работат на спречување на корупцијата како и на експертите задолжени за безбедност на информатичките системи.

9 http://www.icac.org.hk/new_icac/files/cms/eng/13857pdf.pdf.
10 www.eacc.go.ke/docs/ICT_Guidelines.pdf.
11 http://www.icac.nsw.gov.au/preventing-corruption/knowing-your-risks/it-systems/4911.
12 www.unodc.org/documents/corruption/publications_toolkit_sep04.pdf.
13 www.unodc.org/unodc/en/treaties/CAC/technical-guide.html.
14 www.osce.org/eea/13738.
15 www.transparency.org/publications/sourcebook
16 www.usaid.gov/our_work/democracy_and_governance/technical_areas/anticorruption_handbook/

Оваа студија става акцент само на корупциските ризици кои **конкретно** се однесуваат на информатичките технологии. На пример, корумпираната набавка на информатички технологии или зависност од производителот (vendor lock-in) се корупциски ризици кои може да се случат и со било која друга алатка, како што се набавки на шински возила за јавен превоз или евентуална зависност од производителот (vendor lock-in); така што тие не се корупциски ризици кои конкретно се поврзани само со информатички технологии.

Членките на РеСПА се очекува да имаат различни пристапи и начини на употреба на информатичките технологии, па следствено да научат и нови работи благодарение на **размената** на добри пракси овозможена преку оваа компаративна студија. Со оглед на тоа што во литературата за антикорупција и информатички технологии сè уште не постои типологија на случаи, додадената вредност и ефектите од оваа студија се очекува да излезат и надвор од рамките на регионот на РеСПА.

1. Конкретни примери на злоупотреба на информатичките технологии за корупциски цели

Краток преглед

Подготвено од Тилман Хопе и Луизе Томасен

Конкретните примери кои ги елабориравме тука се избрани по случаен избор и истите не претставуваат репрезентативен избор на случаи од регионот на РеСПА. Важно е да се нагласи дека наведените случаи не значи дека биле предмет на судска постапка, туку за потребите на оваа Студија доволно е дека истите биле пријавени или констатирани од страна на соодветните засегнати страни (како што се медиумите, невладини организации, вработените во администрацијата и сл.). Голем предизвик во идентификувањето на релевантни случаи беше немањето на статистички информации за коруптивни кривични дела поврзани со злоупотреба на информатички технологии како и фактот дека злоупотребата на информатичките технологии за коруптивни цели не е предвидена во агендата на повеќето (да не кажеме на сите) органи задолжени за борба против корупцијата во регионот. Истовремено, се чини дека постои и големо табу против откривањето на слабости во информатичките системи: јавните институции се постојано воздржани во давањето информации кои би укажале на тоа дека нивните информатички системи се многу послаби отколку што јавноста мисли дека се. Така што, иницијаторите на оваа студија сметаа дека сепак е подобро случаите да ѝ бидат предочени на јавноста, без разлика што истите не се докажани, не се целосни ниту репрезентативни, барем не во сите случаи.

Конкретните случаи покажуваат дека злоупотребата на информатичката технологија опфаќа широк спектар на коруптивни кривични дела, и тоа:

- поткуп
- злоупотреба на службената положба
- вршење влијание
- судир на интереси
- кршење на процедурата за набавки
- проневери

Злоупотребата на информатичката технологија за коруптивни цели се случува тогаш кога се работи за финансиски интереси како и во случаи кога злоупотребата на информатичките технологии им служи само на нематеријалните интереси на јавните лица (како што е задоволството од објавување на сензационални приватни податоци). Вакви примери се случуваат во секој можен сектор од власта, вклучувајќи ги јавните претпријатија и компании, како и на сите нивоа на власт (централно и локално). До злоупотреба на информатичката технологија може да дојде и спонтано со цел задоволување на лични потреби (како што е фалсификување на пасош) или истата може да биде дел од шеми на континуиран или организиран криминал (како што се измами во системот на патариниte и сл.).

Големата разновидност на случаи, исто така, покажува дека треба претпазливо да му пристапиме на принципот во кој силно веруваме („е-Владата помага во борбата против корупција“). Информатичката технологија сама по себе не е универзален лек против корупцијата. Во одредени случаи можеме дури и да констатираме дека информатичката технологија им олеснува на сторителите да ги извршат коруптивните кривични дела: транспарентноста на информатичките системи може да делува во нивна корист – трагите кои ги оставаат се помалку видливи кај многу сложените мрежи, а електронската евиденција е исто така со кратко траење. Важноста од постоење на добри мерки за заштита и гаранции (кои подетално ќе бидат елаборирани во Поглавјето 2) е сè поголема имајќи ги предвид студиите на случај опфатени во оваа студија.

Табела 1

Наслов	Коруптивно кривично дело (не мора да било докажано)	Употреба на информатичка технологија	Штета на јавните финансии	Како било откриено коруптивното кривично дело?	Ниво на власт (централно или локално)	Сектор
Случај 1 од Албанија: Корупција во TIMS системот за гранична контрола	Поткуп	Продавање фалсификувани податоци	Да	Внатрешна ревизија	Централно ниво	Органи задолжени за примена на законот
Случај 2 од Албанија: Корупција во електронскиот систем за јавни набавки	Кршење на процедурата за набавки	Неовластен влез/ фалсификување	Да	Надворешна ревизија	Централно ниво	Набавки
Случај 3 од Албанија: корупција на информатичката технологија кај дистрибутер на електрична енергија	Злоупотреба на службена положба Фалсификување	Фалсификување на податоци	Да	Жалби од граѓаните	Централно ниво	Енергетика
Случај 4 од Албаниja: Проневера и фалсификување на книговодствена евиденција	Злоупотреба на службена положба Проневера	Менување на податоци/ измама	Да	Внатрешна ревизија	Централно ниво	Одбрана
Случај 1 од Босна и Херцеговина: Најпознатиот босански хакер меѓу обвинителите	Злоупотреба на службената положба	Компјутерска саботажа	Не	Интерна истрага	Цeнтрално ниво	Правосудство
Случај 2 од Босна и Херцеговина: Уште едно контроверзно вработување во Врховниот завод за ревизија на Република Српска	Злоупотреба на службената положба	Уништување на податоци	Не	Инсајдерски информации	Локално ниво	Набавки
Случај 3 од Босна и Херцеговина: Злоупотреба на електронскиот систем на CIPS проектот	Злоупотреба на службената положба	Фалсификување податоци	Не	Објави во медиумите	Локално ниво	Граѓански регистар
Случај 1 од Хрватска: Јави му се на лекарот за гласови	Незаконско добивање на податоци	Неовластено користење на податоци за пациенти од болницата	Не	Жалба од граѓани	Локално ниво	Здравство
Случај 2 од Хрватска: достапност на доверливата база на Хрватската радиотелевизија на црниот пазар	Незаконско добивање на податоци	Умножување и продавање на податоци од базата на податоци на Хрватската радиотелевизија	Не	Жалба од невладина организација	Централно ниво	Медиуми
Случај 3 од Хрватска: Во потрага по бранителите	Злоупотреба на службена позиција Незаконско добивање на податоци	Продавање или давање податоци од базата на податоци	Не	Објава во медиумите	Централно ниво	Влада
Случај 4 од Хрватска: Со мала помош од јавните службеници, вкупно 68 хрватски пасоши им биле продадени на криминалци	Незаконско добивање на податоци	Проверка на доверливи податоци од информатичките системи на полицијата	Не	Полиција	Централно ниво	Внатрешни работи
Случај 5 од Хрватска: Полицаец фатен на дело додека вметнувал лажни податоци во информатичките системи на полицијата	Манипулирање со постојните податоци и процедури	Електронско создавање на фалсификувана документација со цел да му се помогне на странец да добие хрватско државјанство	Не	Полиција	Централно ниво	Внатрешни работи

Наслов	Коруптивно кривично дело (не мора да било докажано)	Употреба на информатичка технологија	Штета на јавните финансии	Како било откриено коруптивното кривично дело?	Ниво на власт (централно или локално)	Сектор
Случај 6 од Хрватска: Полицајци ги бришат податоци за сообраќајни прекршоци и објавуваат доверливи податоци (како поткуп прифатиле печено јагне и 20 литри вино!)	Незаконско добивање на податоци Манипулирање со податоци и процедури	Незаконско добивање на податоци: објавување доверливи податоци од информатичките системи на полицијата на организираниот криминал. Манипулирање со постојни податоци и процедури: бришење на податоци за сообраќајни прекршоци од информатичките системи на полицијата	Не	Полиција	Локално ниво	Внатрешно ниво
Случај 7 од Хрватска: Случајно фатен при објавување доверливи податоци за возилата и за нивните сопственици	Незаконско добивање на податоци	Објавување доверливи податоци од информатичките системи на полицијата на организираниот криминал	Не	Полиција	Локално ниво	Внатрешни работи
Случај 8 од Хрватска: Секоја година од патарините исчезнуваат 2 милиони евра	Проневера	Бришење на податоци и вметнување на фалсификувани податоци во информатичките системи	Да (околу 2 милиони евра годишно)	Внатрешна ревизија	Централно ниво	Сообраќај
Случај 9 од Хрватска: „Валкани“ полицајци - полицајци им доставиле доверливи податоци на шверцери со оружје	Објавување на доверливи податоци Злоупотреба на службената положба	Објавување на доверливи податоци од информатичките системи на полицијата на организираниот криминал	Не	Полиција	Локално ниво	Полиција
Случај 10 од Хрватска: Полицаец осуден на една година затворска казна затоа што на пријателот му дозволил нелегален риболов	Објавување на доверливи податоци Злоупотреба на службената положба	Објавување на доверливи податоци од информатичките системи на Министерството за внатрешни работи на организираниот криминал	Не	Непознато	Локално ниво	Полицијата
Случај 11 од Хрватска: Виш инспектор злоупотребил службени податоци за да победи на локални избори	Злоупотреба на службената положба Објавување на доверливи информации	Незаконски пристап и објавување на доверливи податоци од информатичките системи на даночната управа	Не	Жалба од граѓанин	Локално ниво	Даноци

Наслов	Коруптивно кривично дело (не мора да било докажано)	Употреба на информатичка технологија	Штета на јавните финансии	Како било откриено коруптивното кривично дело?	Ниво на власт (централно или локално)	Сектор
Случај 12 од Хрватска: Немаш ни еден ден на работа? Не грижи се, секако ќе добиеш пензија!	Измама (фалсификување на работната евиденција) Проневера преку доделување незаслужена пензија	Вметнување фалсификувани податоци во информатичките системи на Хрватскиот институт за пензиско осигурување	Да (околу 20.000 евра)	Интерна жалба	Централно ниво	Социјално осигурување
Случај 1 од Косово: Уништување на докази	Злоупотреба на службената положба Службена измама Фалсификување на официјални документи	Бришење на податоци од сервер	Да	Жалба од граѓанин	Централно ниво	Градежништво
Случај 2 од Косово: Стекнување статус на воен инвалид	Фалсификување на официјални документи. Службена измама	Фалсификување на податоци	Да	Жалба од граѓанин	Централно ниво	Социјални работи
Случај 3 од Косово: Злоупотреба на лозинка	Злоупотреба на службено овластување	Фаворизирање Кражба на лозинка	Да	Интерна жалба	Централно ниво	Здравство
Случај 4 од Косово: Фалсификување на даночна документација	Фалсификување на официјални документи Службена измама	Фалсификување на документи	Да	Интерна жалба од поранешен вработен	Локално ниво	Одржување
Случај 1 од Македонија: Злоупотреба на информатичките системи на патарините	Злоупотреба на службената положба Поткуп Проневера	Неточно евидентирање на бројот и видот на возила во информатичките системи на патарините	Да (околу 2.000 евра)	Внатрешна ревизија	Централно ниво	Транспорт/ сообраќај
Случај 2 од Македонија: Напад врз информатичките системи за јавни набавки	Поткуп Проневера Кршење на процедурата за набавки	Попречување на постапката за набавки Нелегален упад во компјутерски систем	Не/ непознато	Жалба од граѓанин	Централно ниво	Набавки
Случај 3 од Македонија: Злоупотреба на информатичките системи и незаконско објавување на лични податоци	Проневера Злоупотреба на службената положба Евентуален поткуп	Извлекување на лични податоци и креирање официјален документ за друго лице	Непознато	Откривање на фалсификуван документ	Централно ниво	Администрација
Случај 4 од Македонија: Злоупотреба во системот за регистрирање на бројот на работни часови	Проневера Злоупотреба на службената положба	Менување на податоците во системот за работни часови	Да	Внатрешна ревизија	Централно ниво	Администрација

Наслов	Коруптивно кривично дело (не мора да било докажано)	Употреба на информатичка технологија	Штета на јавните финансии	Како било откриено коруптивното кривично дело?	Ниво на власт (централно или локално)	Сектор
Случај 5 од Македонија: Злоупотреба на администраторските права (банкарски гаранции/ увозни квоти)	Проневера Злоупотреба на службената положба Поткуп	Менување и повторно менување на податоци Отворање и користење на лажни сметки	Да (околу 160.000 евра)	Внатрешна-ревизија	Централно ниво	Управата на граничните премини
Случај 1 од Црна Гора: Злоупотреба на службената положба и фалсификување на службени документи	Злоупотреба на службената положба	Фалсификување на податоци	Не	Интерна истрага	Централно ниво	Министерство за внатрешни работи
Случај 2 од Црна Гора: Искористување на информатичката технологија за нанесување политичка штета	Манипулација и злоупотреба на информатички системи Злоупотреба на службената положба	Злоупотреба на информатички системи Фалсификување на податоци	Не	Објави во медиумите (покренати од сторителите)	Централно ниво	Внатрешни работи Телекомуникации
Случај 3 од Црна Гора: Злоупотреба на функција внесување неточни податоци во јавни регистри	Злоупотреба на службената положба Поткуп	Фалсификување на податоци	Да	Интерна истрага	Локално ниво	Катастар Внатрешни работи
Случај 4 од Црна Гора: Незаконско издавање на патни исправи	Злоупотреба на службената положба	Фалсификување на податоци	Не	Интерна истрага	Централно ниво	Внатрешни работи
Случај 1 од Србија: Сексуален акт во Белградска Арена	Злоупотреба на службената положба	Незаконско добивање на податоци Манипулирање на податоци и процедури	Не	Извештаи во медиуми	Централно ниво	Полиција
Случај 2 од Србија: Кога изведувачот за информатички системи „фаќа корен“	Злоупотреба на службената положба Непотизам Кршење на процедурата за набавки	Ризици поврзани со изведувачот на информатички системи Манипулирање со податоци и процедури	Да	Внатрешна ревизија	Централно ниво	Правда
Случај 3 од Србија: Виш јавен службеник ги шпионира вработените	Проневера Злоупотреба на службената положба	Незаконско обезбедување на податоци Манипулирање на податоци и процедури	Не	Дојавувачи (свиркачи)	Централно ниво	Економија
Случај 4 од Србија: „Мафија на патиштата“	Злоупотреба на службената положба Проневера Организиран криминал	Компромитирање на системите на патариште со користење на лажен копроцесорски емулатор. Печатење на двојни билети со исти сериски броеви за камионите. Незаконско подигнување на рампата	Да	Дојавувачи (свиркачи)	Централно ниво	Транспорт/ сообраќај

Албанија

Подготвено од Едљира Наси и Енед Керцини

Случај 1 од Албанија: Корупција во TIMS системот на граничната контрола

Примерот кој го презентираме подолу се однесува на злоупотреба на полициските станици на граничните премини извршена од страна на граничните полициски службеници, преку манипулирање на TIMS информатичките системи (TIMS = Систем за целосно управување со информации) со цел избегнување на давачките кон државата за увоз на возила.

Вовед

Лицето А.И., преку посебно полномошно, му дал право на лицето Е.Х. да користи возило Форд со италијански регистарски таблички. Со овој документ, на лицето Е.Х. му е дадено законско право да делува и да аплицира до релевантните институции за целосна постапка и регистрација на возилото кое било увезено и да помине низ соодветните процедури за да може возилото слободно и легално да се користи во Албанија.

Сепак, лицето Е.Х. имало пријател А.Т. кој бил офицер во воената база Зал-Хер. Се чини дека лицето Е.Х., како сопственик на возилото, му се доверил на офицерот дека возилото веќе извесно време се наоѓа во Албанија но истото немало соодветна документација за негов увоз и влез во државата, а тој (како сопственик) не аплицирал за овие документи заради значителните финансиски обврски поврзани со таквата постапка.

Лицето А.Т. му кажало на лицето Е.Х. дека познава човек кој работи на граничниот премин „Муриќан“ во Скадар и кој може да ги среди работите со документацијата на возилото така што ќе направи да изгледа дека возилото тукушто влегло во Албанија. Се разбира дека за ваквата услуга лицето ќе треба да плати одреден финансиски износ.

Од друга страна, лицето А.Т. се запознало со лицето А.С. кој работел како раководител на Центарот за размена на информации со Црна Гора при Регионалниот директорат за граници и миграција во градот Скадар. Лицето А.Т. му ветило на лицето Е.Х. дека тој би можел да му помогне да обезбеди документ според кој возилото влегло во Албанија пред само неколку дена. Всушност, лицето А.Т. се нафатило да ја заврши оваа работа и, како резултат на тоа, побарало фотокопија од вистинските документи со кои се докажува влез на возилото во Албанија, за да може потоа да изготви нови

документи од граничниот премин во кои ќе прикаже дека возилото влегло во Албанија по 2009 година. Лицето А.Т. е снимено како вели дека вкупната цена претходната година била 15.000 албански леки (околу 105 евра), но оттогаш досега оваа цена се зголемила.

За да може да ги извади документите и да добие помош од лицата А.С. и Е.Х., лицата А.С. и А.Т. се сретнале во едно кафуле на 9 февруари 2013 година за да поразговараат за сите детаљи. Наредниот ден лицата Е.Х. и А.С. повторно се сретнале за да подискутираат за документот за влез на возилото кој требало да се изготви. По неколку дена овие две лица се сретнале уште еднаш, при што А.С. рекол дека ја завршил работата и подготвил извештај од TIMS информатичките системи[17].

Неточна евиденција во информатичкиот систем

Неточниот документ прикажувал дека новиот сопственик на возилото (лицето Е.Х.) влегол во Албанија преку граничниот премин Мурићан на 3 февруари 2013 година, во 05:58 часот, во возилото со регистарски таблички „DK***L“. Овој факт исто така бил документиран во евиденцијата извадена од електронскиот систем на TIMS.

Подоцнежните проверки и ревизии на TIMS системот покажаа дека лицето кое ги направило промените во информатичките системи на TIMS било, всушност, друго лице (Ад.С.). Во дискусиите помеѓу лицата Е.Х. и А.Т., кои подоцна биле раскажани од лицето Е.Х., лицето А.Т. (во својство на контакт лице) му кажал на Е.Х. дека немало потреба ни да се појавува на граничниот премин затоа што сите неопходни активности ќе ги направи лицето А.С. кое, всушност, работело на тој граничен премин.

Ова било направено преку пристап до електронските податоци во TIMS системот и нивно фалсификување. Системот за целосно управување со информации (TIMS) е голема база на податоци која содржи информации за сите државјани на Албанија на кои им е издаден биометриски пасош т.е. станува збор за мнозинството албански државјани од моментот на воведување на биометриските пасоши во Албанија. Системот го евидентира движењето на албанските државјани кои ја поминуваат албанската граница на сите гранични премини. Освен тоа, системот ги зачувува податоците кои се однесуваат на начинот на кој патуваат лицата, местото на поаѓање и/ или крајната нивна дестинација, како и регистарскиот број на возилата. Овие податоци им се достапни и на органите за спроведување на законот и на полицијата. Со оглед на фактот дека од 1 март 2012 година биометриските пасоши се единствена валидна патна исправа за албанските државјани, сите гранични премини користат читачи на биометриски пасоши и опрема за проверка на отисоци од прсти. Евидентирањето на документите во TIMS системот во реално време и нивното очитување во моментот на влез и излез на граничните премини овозможува споредување со постојните податоци и намалување на веројатноста од измами[18].

17 Одлука на Судот бр.1035 од 23 јули 2013 година

18 Размена на информации во врска со Кодексот на однесување на ОБСЕ: Политичко-воени аспекти на безбедноста, Република Албанија, 2013, FSC.EMI/178/14, 22 мај 2014 година

Интервенцијата врз TIMS системот ја направило лицето Ад.С. кое од 1 мај 2010 година работело како системски оператор на граничниот премин Мурићан. На оваа функција тој учествувал во контрола на лицата и возилата и во регистрирањето на влезот и излезот во и од Албанија. Лицето Ад.С. исто така било задолжено (и било свесно) за севкупното управување на TIMS системот за гранична контрола како и за целиот систем на камери. Неговите обврски се дефинирани во соодветните регулативи во кои се содржани насоки и стандарди за работен учинок на оваа функција. Во ова својство тој ги контролирал и работел со подсистемите на TIMS, како што е системот за гранична контрола и системот за податоци од криминална природа, а воедно имал задача и да ја надгледува работата на другиот помошен персонал додека бил на смена за да обезбеди дека се работи точно според процедурите.

Испитување на системот кое беше направено како дел од истражната постапка[19] покажа дека лицето Ад.С. направило измени во TIMS системот со кои лажно прикажало дека лицето Е.Х. наводно влегло во Албанија на 9 февруари 2013 година со цел да избегне плаќање на давачките и даноците кон државата. Оваа негова активност е докажана со TIMS извештајот кој укажува дека корисничкото име (username) на лицето кое ги направило овие измени му припаѓа токму на Ад.С. како и фактот дека, според работниот распоред на граничниот премин, Ад.С. бил оператор на системот во таа смена.

Поради овие активности и поради барањето пари за истите, обвинителството покренало кривична пријава против лицето Ад.С. за правење лажни измени во системот и делување спротивно на јавниот интерес, преку изготвување на лажен извештај кој се однесува на возилото на Е.Х.

А.С. е обвинет за пасивно корумпирање на јавни службеници и осуден е на затворска казна во траење од една година и осум месеци (суспендирана осуда според одредени услови) и истовремено му е забрането една година да врши јавна функција. Лицето Ад.С е исто така обвинето за злоупотреба на службената должност и осудено на затворска казна од шест месеци (суспендирана осуда според одредени услови) и истовремено му е забрането една година да врши јавна функција. Лицето А.Т. е обвинето за извршување незаконско влијание врз службени лица и осудено на затворска казна од шест месеци (суспендирана осуда според одредени услови).

19 Случајот беше разгледуван и по него постапуваше ICS преку свои информатори. Сепак, податоците од информатичките системи подоцна беа разгледувано како доказ од страна на обвинителството

Случај 2 од Албанија: Корупција во електронскиот систем за јавни набавки

Овој случај се однесува на интервенирање во системот за јавни набавки, за корупциски цели, како и на интервенирање во електронското управување со јавните набавки.

Вовед

Во насока на исполнување на својата функција како врховна и независна ревизорска институција во државата, Државниот завод за ревизија спроведе ревизија на Агенцијата за цивилно воздухопловство во 2012 година. Конечниот извештај од ревизијата со наслов „Имплементација на законитоста и регуларност на економско-финансиската активност“ на Агенцијата за цивилно воздухопловство за периодот од 1 јануари 2011 до 31 март 2012 година, и мерките за унапредување на процесот подразбираа, исто така, и преглед на процедурите за набавки[20].

Агенцијата за цивилно воздухопловство е јавен орган со своја финансиска независност – аспект кој ѝ овозможува да ја врши својата активност согласно со меѓународни стандарди и како одговор на потребата на Агенцијата да функционира согласно со високи професионални стандарди.

Управувањето со постапките за набавки во Албанија се одвива согласно со Законот за јавни набавки бр.9643 од 20 ноември 2006 година, Законот за електронски потпис од 25 февруари 2008 година и Одлуката на Советот на министри бр.659 од 3 октомври 2007 година за правилата за спроведување на постапки за јавни набавки со примена на електронски средства, како и според инструкциите и упатствата на Агенцијата за јавни набавки.

Во текот на една постапка за јавна набавка на канцелариска опрема и мебел Државниот завод за ревизија констатира неправилности во постапката за набавка, а одговорите дадени од службените лица кои беа вклучени во истата укажуваа на манипулации со електронските потписи во текот на постапката.

Процес на набавка

Во текот на процесот на набавка, комуникацијата која се одвивала во рамките на нарачателот (Агенцијата за цивилно воздухопловство) укажува на тоа дека навистина имало неправилности во одредени аспекти на електронската набавка. На 20 октомври 2011 година еден од вработените во Агенцијата (лицето Т.) е запознаен со потпишувањето на записникот на одлуката со која се дисквалификува одредена компанија во горенаведениот процес на јавна набавка.

Лицето Т. потоа ги информирало директорите на Агенцијата за цивилно воздухопловство дека комисијата која ги разгледувала понудите никогаш не ја направила наведената евалуација по електронски пат, со оглед на фактот што тој бил во странство. Уште повеќе, тој посочи дека лозинката која ја употребил како корисник на електронскиот систем била сменета без тој да знае за тоа и без негова согласност, со што некој друг ја заокружил постапката на разгледување и евалуација на понудите од фирмите.

Откако биле разгледани сите понуди кои биле доставени електронски (со користење на сменетата лозинка), лицето Т. посочи дека причините за дисквалификување на компанијата која понудила најниска цена немале законски основи. Со оглед на фактот дека таа компанија ги доставила истите технички спецификации кои се барале од страна на Агенцијата за цивилно воздухопловство, нејзиното дисквалификување било нелогично и ќе значи економска штета за државниот буџет и за Агенцијата за цивилно воздухопловство.

Лицето Т. исто така потврди дека никогаш не учествувал во разгледувањето на понудите, ниту пак на состаноците одржани во врска со тоа во текот на 2011 година. Од проверките кои беа направени на порталот на Агенцијата за јавни набавки можеше да се види дека разгледувањето било направено од некое трето лице, откако била сменета лозинката. Како член на комисијата за разгледување на понудите, лицето негира дека го потпишало записникот од состанокот кој се однесува на конкретната постапка на јавна набавка.

Сепак, и покрај овие факти, Државниот завод за ревизија посочува дека директорите на Агенцијата за цивилно воздухопловство не делувале во насока на поправање на ситуацијата со преземање на управни мерки во однос на конкретни лица и како резултат на ова Државниот завод за ревизија го проследи случајот до Јавниот обвинител со укажување дека активностите на Агенцијата за цивилно воздухопловство во однос на набавките биле фиктивни затоа што членовите на групата за разгледување на понудите негирале дека воопшто учествувале во разгледувањето на доставените понуди.

20 Целиот текст на извештајот може да се преземе од интернет страницата на Државниот завод за ревизија: http://www.klsh.org.al/web/pub/autoriteti_avia- cionit_civil_394_1.pdf

Случај 3 од Албанија: Корупција на информатичката технологија кај дистрибутер на електрична енергија

Вовед

Во 2009 година во Албанија се случи приватизација на 76% од акциите на дистрибутерот на електрична енергија – 24% од акциите на дистрибутерот и оператор останаа во сопственост на државата, а 76% од акциите беа продадени на приватната компанија „CEZ Distribution“. Активноста на овој дистрибутер е регулирана од Енергетскиот регулатор на Албанија (ERE).

На 20 јануари 2011 година Канцеларијата за заштита на потрошувачите достави жалба до Јавниот обвинител во Тирана против извршните лица на „CEZ Distribution“ за кривичните дела „измама“ и „компјутерска измама“ согласно со членовите 143 и 143-б од Кривичниот законик. Оваа жалба, заедно со уште една жалба која претходно била доставена од полицијата, укажува на тоа дека компанијата „CEZ Distribution“ им издавала фактури за електрична енергија на потрошувачите со нелогична ставка: „загуби на енергија“ врз основа на која имаме дополнителна наплата на 4.000 киловати за домаќинства и 20.000 киловати за другите потрошувачи. Оваа ставка најмногу се однесува на диви потрошувачи приклучени на енергетската дистрибутивна мрежа кои не се регистрирани и кои не плаќаат никаков износ, или на потрошувачи кои „го штелуваат“ апаратот за мерење електрична енергија. Сепак, во најголем број случаи, потрошувачите се жалеа на тоа дека сметките не ги информираат за големиот износ кој им се наплаќа и кој всушност претставува еден вид казна а не е одраз на реалната потрошувачка на електрична енергија.

Во соопштението издадено на 12 јануари 2011 година Енергетскиот регулатор на Албанија (ERE) ја информира јавноста дека на 15 ноември 2010 година ја има донесено Одлуката бр.90 според која користењето на ставката „загуби на енергија“ е несоодветно и арбитрарно, без никаков законски основ, спротивно на постојната регулаторна рамка и дека „CEZ Distribution” треба да биде казнет за ваквото постапување. Освен тоа, Енергетскиот регулатор на Албанија има добиено околу 14.000 жалби од граѓани[21] во периодот октомври 2010 – јануари 2011 година од кои вкупно 490 казни се платени од граѓаните.

Според медиумите, во тој период (2011 година) дистрибутерот не само што им наплатувал повеќе на потрошувачите туку тоа го правел на арбитрарен начин така што им дозволувал на инспекторите да ги казнуваат граѓаните и фирмите без притоа да се придржуваат до процедурите утврдени од самиот дистрибутер. Уште повеќе, медиумите обвинуваа дека вработените во дистрибутерот биле стимулирани да го прават ова затоа што биле финансиски наградувани ако ги казнуваат своите потрошувачи[22] што довело до тоа голем број на потрошувачи да добијат сметки со прекумерен износ[23]. Сепак, ова не е потврдено во записникот од судот или во неговите одлуки, и покрај фактот што вработените во дистрибутивната компанија не дадоа друго објаснување за горенаведените активности.

Вкупниот износ на финансиски штети кои им биле нанесени на потрошувачите во горенаведениот период се проценува од 4 до 5 милиони евра[24].

Како функционирала шемата на сметки со прекумерен износ

Издавањето фактура на секој клиент го прават теренски оператори кои работат со PDA уред (личен дигитален асистент). PDA уредите го користат вработените во дистрибутивната компанија за очитување на потрошувачката на електрична енергија. Тие веднаш испраќаат преку интернет податоци до серверот за бројот на мерачот, бројот на претплатничкиот договор, позицијата на уредот чија потрошувачка се мери во тој момент (на пример: регистрирање на количеството на потрошени киловат часови) и датумот и времето во кое се врши мерењето. Истовремено се евидентираат и податоци за неправилностите (како што се евентуални технички проблеми, диви приклучоци на енергетската мрежа и сл.).

Податоците од PDA уредите потоа се синхронизираат со системот MYAvis кој е активен на серверот сместен во серверската просторија на податочниот центар (инаку самиот пренос на податоци се одвива преку GPRS платформата) на крајот од секој работен ден. Податоците од соодветниот MYAvis интерфејс поминуваат директно низ системот за наплата, освен оние информации кои се блокирани со филтри (на пример: одредени неправилности или сомнителна наплата кои понатаму подетално се разгледуваат).

Во периодот кога еден од случаите започна да биде разгледуван од страна на судот, исказите укажуваа на тоа дека, всушност, е невозможно вработените електронски да ги менуваат податоците кои се однесуваат на потрошувачите затоа што немаат администраторски права во системот. Ова го наведе обвинителството подетално да ги разгледа податоците од неколку мерења направени од страна на одредени вработени во дистрибутивната компанија против кои имаше доставено жалби. Од листата на измерена потрошувачка на електрична енергија (која исто така го прикажува и местото и времето кога вработените во компанијата го вршеле мерењето) можеше да се види дека имало мерења кои биле правени во невообичаени периоди од ноќта: 22:00 часот, 23:00, 24:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00 итн. и покрај фактот што работното време на вработените е од 08:00 до 16:30 часот.

21 Одлука на судот во Тирана бр. 1633 од 30 јуни 2014 година

22 Skandal/CEZ faturon me shume energji sesa blen, ve gjoba fiktive per te kerkuar rritje cmimi” од 30.11.2011 година, достапно на: http://www.gazetatema.net/web/2011/11/30/skan- dali-cez-faturon-me-shume-energji-sesa-blen-ve-gjoba-fiktive-per-te-kerkuar-rritje-cmimi/

23 “Hetimi, CEZ shperblente punonjesit qe mbifaturonin” http://time.ikub.al/2afad09e2d/44 5564cf92c2c0259d0562e9238b8515/Lajm_Hetimi-CEZ-shperblente-punonjesit-qe-mbifaturo- nin-abonentet.aspx

24 “Prokuroret, hetim 14 mije ankesave per mbifaturim energjie” од 27.11.2011 година, достапно на http://www.shqiptarja.com/lajme/2706/prokuroret-hetim-14-mije-ankesave-per- mbifaturim-energjie-65833.html

Освен тоа, дистрибутивната компанија има воспоставено и посебни процедури за мерење на потрошувачката на електрична енергија кои, меѓу другото, содржат сеопфатни правила и процедури за регулирање на контролниот систем за мерење на потрошувачката како и метод за пресметување на потрошената енергија и на другите казни во случај на диви приклучоци на дистрибутивната мрежа. Оваа регулативно јасно упатува на тоа дека мерењето и казната мора да се вршат во присуство на самиот потрошувач или на негови роднини (слики, видеа и други фактори кои потврдуваат интервенирање во струјомерот). Во отсуство на потрошувачот или на негови родини, или во случај на одбивање да се стави потпис на записникот од мерењето, истиот ќе треба да биде потпишан од лице вработено во друг сектор во компанијата (NTL сектор). Од записникот од мерењето кое било направено може јасно да се види дека ниту потрошувачот ниту вработените во NTL секторот не го потпишале записникот во моментот кога се правеле сметките со прекумерен износ или казни за диви приклучоци на енергетската дистрибутивна мрежа. Индикативно е и тоа што само на 21 октомври 2010 година се евидентирани околу 17 диви повторни приклучоци на енергетската мрежа и тоа скоро сите во меѓусебни интервали од по две минути а некои дури и истовремено[25].

Се претпоставува дека во оваа шема на сметки со прекумерен износ учествувале повеќе од десет луѓе. По откривањето на овој случај беа откриени и други шеми сметки со прекумерен износ и истите добија правна разрешница. Судот осуди неколкумина вработени во компанијата, а во тек се постапки за уште неколку од нив. Во горенаведениот случај сметки со прекумерен износ беа правени со употреба на PDA уреди, но во други случаи обвинувањата укажуваат на тоа дека биле менувани електронските податоци кои биле регистрирани од PDA уредите[26].

Случај 4 од Албанија: Проневера и фалсификување на книговодствена евиденција

Овој случај се однесува на вработено лице задолжено за книговодствената евиденција кое, во период од повеќе години, проневерило пари со кои управувало и ги депонирало на лична банкарска сметка.

Обвинетата М.К. биле шеф на сметководство на полк на командоси во Зал-Хер во Тирана. Во ова својство М.К. вршела дејствија спротивни на законот – префрлала средства кои не биле нејзини на лична банкарска сметка и тоа преку фалсификување на документација и на други податоци.

25 Одлука на судот во Тирана бр. 1633 од 30.06.2014 година
26 “Prokuroria: Skema si CEZ vidhte 15 mije konsumatore” од 15.04.2013 година, достапно на: http://gazeta-shqip.com/lajme/2013/04/15/prokuroria-skema-si-cez-vidhte-15-mije-konsu- matore/

Во 2009 година Секторот за внатрешна ревизија на Министерството за одбрана направил тематска ревизија на примената на важечкото законодавство во однос на платите и надоместоците за вработените во полкот на командоси во Зал-Хер. Ревизијата утврди дека М.К., во својство на шеф на финансии фалсификувала документација (која се однесува на платите на вработените во воената единица бр. 1200)[27].

Сметководственото вештачење дополнително утврди дека М.К. проневерила вкупно 8.668.886 албански леки (61.920 евра) од кои 6.198.326 леки се резултат на зголемување на нето платата а остатокот од 2.470.560 леки се од додатоци на плата, дневници, услуги и сл. Сите овие средства потекнуваат од државниот Буџет и се директно наменети за воената единица бр. 1200 од Зал-Хер, Тирана.

Начинот на кој била организирана работата е таков што специјалистот за финансии ги вршел само оние работи пропишани од шефот на финансии (првенствено поставување на бетон и изготвување на платни списоци). Притоа, специјалистот за финансии не ги надгледувал крајниот платен список и нето платите на вработените затоа што овие работи биле подготвувани од шефот на финансии – во најголем дел од лицето М.К.

Откако ќе бил изготвен платниот список истиот се доставувал по електронски пат на одобрување до началникот на Генералштабот и до командирот на полкот. Обвинетата успеала да го фалсификува платниот список и да добие одобрение од началникот на Генералштабот и од командирот на полкот така што прво добивала писмено одобрение а потоа ги менувала електронските податоци наменети за платите и за банкарски уплати.

Банката не е одговорна за разликата во платите со оглед на фактот што таа не може да ги контролира податоците или да има преглед на платите, дури и ако трансферите на личната сметка на М.К. изгледале поголеми од она што обично би се сметало за исплата на плата. Откако парите ќе легнеле на нејзината сметка таа ќе ги извадела од сметка и ќе ги прикриела на друг начин.

Судот ја прогласи М.К. за виновна и ја осуди на казна затвор од една година[28].

27 Одлука на судот во Тирана бр.41 од 20.01.2012 година
28 Ibid.

Босна и Херцеговина

Подготвено од Александра Мартиновиќ и Срѓан Ного

Случај 1 од Босна и Херцеговина: хакирање на емаил адресата на генералниот обвинител

Заедничко за сите домашни и меѓународни извештаи за правосудниот систем во Босна и Херцеговина, вклучувајќи ги тука и годишните извештаи за напредокот кои ги објавува Европската комисија, е што укажуваат на тоа дека правосудството е под доминација, контрола и влијание на политичките елити, преку постојани политички обиди да се влијае на назначувањето на судиите и обвинителите во правосудниот систем на Босна и Херцеговина. Сложената и недоволна сигурна природа на правосудниот систем на Босна и Херцеговина и главните негови недостатоци во смисол на независност и непристрасност можат најдобро да се опишат ако го земеме за пример случајот со државниот обвинител (во понатамошниот текст: лицето X.) кој беше обвинет за неовластен влез (хакирање) во емаил адресата на поранешниот генерален обвинител (во понатамошниот текст: лицето Y.) за да го дискредитира веднаш откако лицето Y. било суспендирано од официјалната функција – генерален обвинител.

Еден од можните мотиви зошто лицето X. ја злоупотребило емаил адресата на лицето Y. е во изјавата која ја дало откако лицето Y. било суспендирано – тој јасно вели дека сака да аплицира за функцијата генерален обвинител на Босна и Херцеговина. Исто така, имало и гласини дека лицето X. сакало да заштити некои обвинети лица против кои лицето Y. покренало обвинение.

Лицата X. и Y. наводно биле поврзани со одредени политички партии во Босна и Херцеговина. Лицето Y. имало наводна поврзаност со партијата на Независни социјалдемократи (SNSD) која е главна партија во Република Српска и една од најлијателните партии во Босна и Херцеговина, додека лицето X. тогаш имало наводна поврзаност со Социјалдемократската партија (SDP) на Босна и Херцеговина која, инаку, е најсилната партија во Федерацијата Босна и Херцеговина но и со Унијата за подобра иднина на Босна и Херцеговина.

Истрагата која беше спроведена потврди дека лицето X. се логирало на емаил адресата на лицето Y. и на вработените во обвинителството на Босна и Херцеговина и на неколку медиуми во Федерацијата Босна и Херцеговина им испратило неточни „општи инструкции“. Овие „општи инструкции“ содржеле компромитирачки изјави и биле испратени на 29 јуни 2011 година на меморандум на обвинителството на Босна и Херцеговина со фалсификуван потпис на генералниот обвинител.

Во овие „општи инструкции“ се вели дека најстрого им се забранува на сите вработени во обвинителството на Босна и Херцеговина да даваат какви било коментари на негативните медиумски извештаи кои се однесуваат на генералниот обвинител, особено во однос на извештаите кои се однесуваат на тогаш актуелните афери „прислушување“ и „рекет“ во кои, наводно, бил вмешан и генералниот обвинител.

„Инструкциите“ исто така им забранувале на вработените да ги читаат „Слободна Босна“, „Дани“, „Ослободење“, „Аваз“ и „Сан“ кои се печатат во Федерацијата Босна и Херцеговина, и да не гледаат никакви емисии емитувани од Федералната телевизија (еден од трите јавни сервиси во Босна и Херцеговина), особено не емисијата „60 минути“ која се емитува на тој сервис.

Во нив конкретно е наведено дека „обвинителите кои сметаат дека ќе почнеме со редовни месечни состаноци, согласно со членот 20, став 2 од Правилникот, се будали“.

Кога дознал за овој емаил, генералниот обвинител доставил жалба против непознат сторител до судот во Босна и Херцеговина и до канцеларијата на обвинителот на Босна и Херцеговина по што била издадена наредба на федералната полиција (во рамките на Министерството за внатрешни работи на Федерацијата Босна и Херцеговина) да се започне со истрага.

За време на истрагата инспекторот задолжен за борба против компјутерски криминал во Федералното Министерство за внатрешни работи утврдил дека емаилот на генералниот обвинител бил злоупотребен со користење на мобилен телефон (iPhone 4) регистриран на име на мајката на лицето X. а го користел исклучиво тој самиот. На некаков начин лицето X. успеало да ја дознае лозинката од емаил адресата на генералниот обвинител, влегол во неа од оддалечена локација и ги испратил инструкциите. И покрај фактот што веќе постоеле повеќето од мерките за заштита со кои би се спречила ваквата злоупотреба, се чини дека во овој случај одлучувачки бил човечкиот фактор. По завршувањето на истрагата изготвен е извештај во кој се содржани кривични пријави против обвинителот – лицето X. за злоупотреба на службената положба, фалсификување и измама кој е испратен до надлежниот обвинител (тоа е канцеларијата на обвинителот на Босна и Херцеговина – Сектор за организиран криминал и корупција).

Според некои медиумски извештаи, и покрај големите напори на колегите на лицето X. во канцеларијата на обвинителот да го покријат овој нечуен скандал, сепак за истиот била информирана канцеларијата на Дисциплинскиот совет во рамките на Високиот судски и обвинителски совет (HJCP) на Босна и Херцеговина.

Но ова не беше единственото обвинение против обвинителот X. Тој исто така беше обвинет и за уште две сторени дисциплински дела. Најпрвин, тој наредил уништување на евиденцијата која се однесува на испрашување на сведоци, во присуство на истите сведоци; и тој испратил барање за информации до директорот на администрација на Федералната полиција и тоа со содржина која е несоодветна за

официјална кореспонденција и на функцијата која во тоа време ја извршувало лицето X. Имено, лицето X. побарало од директорот, на еден многу несоодветен начин, да му го открие изворот на информации и уште еднаш да ја разгледа официјалната полициска белешка со која лицето X., високи лица во Владата на Федерацијата Босна и Херцеговина и на Социјалдемократската партија на Босна и Херцеговина се обвинети за организирање заговор против директорот на администрација на Федералната полиција.

По повеќе од една година, на 26 септември 2012 година, канцеларијата на Дисциплинскиот совет во рамките на Високиот судски и обвинителски совет (HJCP) на Босна и Херцеговина постигна заеднички договор со лицето X. во однос на утврдувањето дисциплинска одговорност и преземањето на дисциплински мерки. Со овој договор тој ја призна и ја прифати одговорноста за сторени дисциплински прекршоци а канцеларијата на Дисциплинскиот совет го повлече барањето за утврдување на неговата дисциплинска одговорност за одредени точки од дисциплинската жалба.

Кога ја препорачувала дисциплинската мерка, канцеларијата на Дисциплинскиот совет имала предвид дека „обвинетиот имал успешна кариера како јавен обвинител и дека бил вклучен во комплексни случаи кои бараат високо ниво на стручност и посветеност“. Фактот дека исто така бил и семеен човек и татко на мало дете како и фактот дека бил оптоварен со долгови исто така беа земени предвид како олеснителни околности. Фактот дека против него е во тек повеќе од една истрага по однос на обвинението за поткуп воопшто не беше земен предвид.

Првостепената дисциплинска комисија на обвинители на Високиот судски и обвинителски совет го прифати договорот помеѓу лицето X. и канцеларијата на Дисциплинскиот совет, и одлучи дека лицето X. е одговорно за три дисциплински прекршоци и за кршење на Кодексот на етика во обвинителството. Ова се сметаше за сериозно прекршување на службената положба што ја доведува во врска довербата на јавноста во кредибилитетот на обвинителството и му нанесува штета на општиот углед на обвинителството во Босна и Херцеговина. Лицето X. беше казнето со 10% од плата во период од шест месеци.

Само еден ден откако му била хакирана емаил адресата, лицето Y. (инаку во тоа време ја извршувал функцијата генерален обвинител) бил суспендиран од службената должност поради „несоодветни контакти“ со меѓународни шверцери на оружје. Постојат голем број на официјални докази (фотографии и аудио снимки) за средбите и телефонските разговори кои ги имал со дилери на оружје кои се на црната листа на Обединетите нации а кои укажуваат дека лицето Y. добивало пари и скапи подароци за тоа што ја помагало криминалната мрежа, за на крајот воопшто и да не биде докажано корупциско делување. Лицето Y. изјави дека жали што несоодветните состаноци кои ги имал со тие луѓе му наштетиле на угледот на обвинителството на Босна и Херцеговина, а исто така се договори и со Високиот судски и обвинителски совет да биде преместен на пониско работно место – тој продолжи да работи како обвинител за воени злосторство во Канцеларијата на обвинителството на Босна и Херцеговина, а му беше изречена и дисциплинска казна во вид на намалување на платата во износ од 10% во период од три месеци.

Случај 2 од Босна и Херцеговина: Уште едно контроверзно вработување во Врховниот завод за ревизија на Република Српска

Врховниот завод за ревизија на Република Српска (SAI RS) објави оглас за слободни работни места за „два **помлади** ревизори“. Огласот е објавен во Службен весник на Република Српска од 3 мај 2014 година, на интернет страницата на институцијата (на 29 април 2014 година) и во медиумите. Крајниот рок за конкурирање беше 30 дена од објавувањето.

Во предвидениот период се пријавија вкупно 61 кандидат за овие работни места, а оние лица кои ги исполнуваа бараните општи и посебни критериуми и кои ги доставија сите неопходни докази и релевантна документација беа поканети да полагаат писмен тест.

Тестирањето беше спроведено на 18 јуни 2014 година во кабинетот по информатика на Економскиот факултетот во Бања Лука. Станува збор за електронско тестирање со користење на компјутерите кои се наоѓаа во тие простории.

Согласно претходните искуства во спроведувањето на слични тестови, резултатите од работата на сите кандидати требаше да се испечатат веднаш по завршувањето на тестот, да се ископираат на USB мемориски уред кој му припаѓа на Врховниот завод за ревизија на Република Српска и потоа да се избришат од меморијата на компјутерите на Економскиот факултетот. Исто така, секој кандидат кој го полага тестот вообичаено има право да направи копија од истиот на свој сопствен USB мемориски уред.

Но во конкретниов случај, работите тргнаа наопаку. Иако нема официјална потврда за ова, некои податоци наводно исчезнале поради проблеми во информатичките системи на Економскиот факултет. Во рамките на Врховниот завод за ревизија на Република Српска има неколку претпоставки според кои се шпекулира дека тестовите не биле испечатени во целост или, пак, не сите тестови биле соодветно евидентирани така што недостасуваат некои податоци. Претпоставките одат дотаму што велат дека сè е во ред со технологијата но дека тестовите се чуваат во тајност од страна на раководството на Врховниот завод за ревизија на Република Српска (вклучувајќи ги тука и членовите на комисијата задолжена за постапката за селекција) како изговор во спорниот избор на еден од кандидатите.

Како и да е, факт е дека не постоеле соодветни безбедносни мерки и нивното отсуство овозможило вакво нешто да се случи. На пример, наместо да работат во софтвер кој е безбеден и сигурен, кандидатите ги пишувале тестовите во едноставен ворд документ без каква било заштита па така било кое лице од комисијата задолжена за тестот можело да го менува тестот и одговорите. Уште повеќе, во конкретниов случај на кандидатите не им било дозволено да си направат копија од тестот кој го пополниле на свој USB мемориски уред а исто така не им бил дозволен ниту увид во тестовите.

И покрај тоа што не беа објавени резултатите од тестовите, кандидатите кои влегоа во потесен круг за избор беа повикани на интервјуа закажани за 25 и 27 јуни 2014 година и, според информациите објавени на интернет страницата на Врховниот завод за ревизија на Република Српска, *„Комисијата задолжена за процедурата за избор утврди листа на успешни кандидати и ја достави до генералниот ревизор“.* Врз основа на предложената листа, која не била достапна за јавноста, генералниот ревизор избрал двајца кандидати.

Изборот на првиот кандидат воопшто не беше контроверзен, но и покрај тоа во медиумите се појавија написи за контроверзниот избор на вториот кандидат. Овој случај беше откриен поради сомневањата кај другите кандидати предизвикани од недоволна транспарентност на постапката наведена погоре па затоа некои од кандидатите поднесоа жалби до Врховниот завод за ревизија на Република Српска.

Извори од Врховниот завод за ревизија на Република Српска велат дека до денес не е направено ништо во смисол на воведување безбедносни мерки со кои би се спречиле вакви проблеми во иднина. Освен фактот дека избраниот кандидат имал историјат на загрозување на јавниот ред и мир, неговиот избор на позицијата помлад ревизор е малку несоодветен (кандидатот има 48 години). Барањата за оваа позиција предвидуваат само една година неопходно професионално искуство, а притоа јасно не се кажува дека тоа искуство мора да биде во ревизија. На оваа возраст кандидатот кој бил избран најверојатно е преквалификуван и би можел да биде избран на некоја друга повисока позиција.

Според некои медиумски шпекулации, кандидатот бил избран на таа позиција од одредена политичка партија што потоа го прави подложен на уцени уште од моментот на преземање на функцијата. Ако постојат конкретни докази кои би ги потврдиле ваквите обвинувања, би се очекувало од него да возвраќа со разни услуги кои би значеле заштита на интересот на политичките елити и да ги прикрива информациите и доказите за коруптивни пракси во јавните институции кои се предмет на јавна ревизија од евентуално нивно откривање и кривично гонење.

Во целата оваа приказна на контроверзно назначување лица и вработувања во Врховниот завод за ревизија на Република Српска вреди да се спомене и назначувањето на новиот Генерален ревизор. Имано, прв избор на Комисијата во Собранието на Република Српска задолжена за избор на кандидати беше лице осомничено дека се стекнало со фалсификувана диплома. Поради силниот притисок од медиумите ова лице не беше назначено на функцијата.

Случај 3 од Босна и Херцеговина: злоупотреба на електронскиот систем на CIPS проектот

Проектот за систем на заштита на идентификациските податоци на граѓаните (CIPS) започна во Босна и Херцеговина во месец април 2002 година кога, со цел да биде привремена активност, беше формиран директорат за негова имплементација. Главна задача на проектот беше формирање на посебен дел од системот преку кој ќе се овозможи спроведување на Законот за централни регистри и размена на податоци.

Во 2008 година, согласно со Стратегијата за развој на документи за идентификација овој Директорат стана Агенција за документи за идентификација, регистри и размена на податоци (IDDEEA) на Босна и Херцеговина. Оваа институција ги следи, координира и обезбедува институционално управување со документите за идентификацијата согласно со релевантните стандарди и регулативи на Европската унија и се развива согласно со истите стандарди. Таа е задолжена за персонализација и техничка обработка на следниве документи за идентификација: лични карти, лични карти за странци, возачки дозволи, патни исправи, документација за регистрација на возила и други идентификациски документи во соработка и со согласност од надлежните органи и со посебна одлука на Советот на министри.

Уште од самите почетоци на Проектот за систем на заштита на идентификациските податоци на граѓаните беа евидентирани бројни жалби во врска со злоупотреба на неговиот електронски систем, особено кога се работи за издавање на лични карти и пасоши на ниво на целата држава.

Канцеларијата на обвинителството на Босна и Херцеговина нареди сеопфатна истрага која беше спроведена преку заеднички активности на неколку институции во Босна и Херцеговина и тоа: Државната агенција за истраги и заштита (SIPA), неколку министерства надлежни за внатрешни работи и за полиција, и полициската мисија на Европската унија (EUPM) во Босна и Херцеговина.

Првата голема операција беше спроведена на 28 мај 2008 година кога во неколку градови во Босна и Херцеговина беа уапсени вкупно дваесет лица, по што во 2009 година следеа уште неколку дополнителни апсења. Уапсени беа претежно носители на јавни функции (полициски службеници, вработени во општинската администрација и регистратори, но имаше и лица кои не беа јавни службеници). За некои од овие лица

на јавни функции постоеше сомнение дека се вклучени во организиран криминал преку злоупотреба на нивните финансиски и технички ресурси, овозможувајќи им на тој начин на цели организирани групи незаконски да се стекнат со материјални придобивки.

Први во синџирот беа полициските службеници задолжени за издавање лични документи. Тие имаат пристап до регистарот т.е. до централната евиденција која е дел од системот на Агенцијата во целина во кој се чуваат податоци за сите државјани на Босна и Херцеговина. Полициските службеници ги користеле своите службени компјутери и права за пристап за влез во системот и менување на податоците. Имено, тие ќе пронашле одредено лице во базата на податоци кое имало државјанство на Босна и Херцеговина но на кое никогаш не му била издадена лична карта (на пример, бегалци кои заминале во странство за време на војната и никогаш не се вратиле). Потоа лицето кое сакало да добие фалсификувани документи ќе го испрателе до канцеларијата на регистраторот (инаку уште еден дел од организираната криминална група која оперира под капата на општинската администрација) кој ќе му издадел извод од матичната книга на родени и уверение за државјанство на лажно име, а што се смета за доволно за започнување на постапка за издавање на лична карта. Во одредени случаи се користеле дури и податоци од починати лица: наместо официјално да регистрираат дека одредено лице починало, тие ќе регистрирале дека лицето пријавило загубена важечка лична карта како изгубена и започнувале постапка за издавање на нова лична карта.

Како што се вели во соопштението објавено од Канцеларијата на обвинителството на Босна и Херцеговина, *„осомничените лица беа обвинети за злоупотреба на системот за издавање на лични документи на Босна и Херцеговина и тоа на начин што им овозможувале на граѓани од Босна и Херцеговина и од други земји во регионот издавање на оригинал документи за лична идентификација на Босна и Херцеговина, а кои инаку содржеле лажни информации за идентитетот на тие лица или за нивното државјанство“.*

Истрагата дојде до докази дека овие незаконски добиени лични документи биле до значителен степен користени за криминални активности во разни делови од државата и во регионот. На пример, меѓу нив имаше осомничени лица припадници на Земунскиот клан, инаку осомничени за убиството на поранешниот српски премиер Зоран Ѓинѓиќ и за обид на убиство на српскиот политичар Вук Драшковиќ, како и неколку други припадници на криминалното подземје кои се стекнале со лажни документи за идентификација на Босна и Херцеговина.

Исто така, постоеја и сомненија дека уапсените лица продавале оригинал лични карти и пасоши на Босна и Херцеговина со лажен идентитет по цена од 2.000 евра. Само во Бања Лука биле издадени повеќе од 200 неважечки лични карти и пасоши.

Овој голем случај предизвика огромна штета на угледот на јавните служби во целата држава и, како резултат на тоа, иницирани беа повеќе измени во процедурите за да се спречат вакви слични случаи во иднина. На пример, процедурите во канцеларијата на регистраторот беа значително унапредени па така сега не е можно да се извади уверение за државјанство и извод од матичната книга на родени за трето лице без претходно овластување од тоа лице. Исто така беа воведени и дополнителни електронски проверки во канцелариите на регистраторот, во Министерството за внатрешни работи и кај другите административни органи надлежни за утврдување на идентитетот, престојот и за други податоци на лицата при издавање на лични документи за нив.

Хрватска

Подготвено од Зорислав Петровиќ и Ивана Андријашевиќ

Случај 1 од Хрватска: Јави му се на лекарот за гласови

За време на кампањата за локални избори во месец мај 2013 година граѓаните на Дубровник кои страдаат од дијабетес добија писмо од дијабетолог при Општата болница во Дубровник кој се кандидираше за градоначалник. Всушност, повеќето негови пациенти добија писмо лично од него во кое ги потсетува за неговата кандидатура и истовремено им укажува дека е подготвен да им помогне: *„(...) мојот прв избор е да ви служам вам, драги мои пациенти“.* Тој исто така ги потсетува своите пациенти за огромниот напредок кој бил направен со изградбата на најсовремениот центар за дијабетес и вели *„оваа година славиме 20 години од Здружението на дијабетичари“.* И кога една група на активисти го откриј ова писмо тие веднаш побараа истрага од општинската канцеларија на јавниот обвинител (DORH) во Дубровник.

Веднаш беше покренатa истрага која утврди дека кол центарот на Хрватската народна странка (NHS) (лекарот, инаку, бил нејзин член), повикала точно 3.133 броеви на фиксни телефони во жупанијата Дубровник-Неретва, од кои 3.215 (98%) се броеви на негови пациенти. Сите тие телефонски броеви, заедно со имињата и адресите, се всушност телефонски броеви на негови пациенти и истите се наоѓаат во матичната евиденција на Клиниката за дијабетес и ендокринологија во која работел лекарот. За општинската канцеларија на јавниот обвинител во Дубровник ваквиот висок процент *„дава индикации дека за изборната кампања на дијабетологот бил користен регистарот на пациенти со лични податоци“.* Сепак, тој негирал дека побарал од било кого да му ги достави тие податоци за потребите на изборната кампања.

Во текот на истрагата општинската канцеларија на јавниот обвинител во Дубровник откри дека голем број лица во општата болница во Дубровник имаат пристап до листата на пациенти и до нивните лични податоци. Уште повеќе, обвинителството утврди дека листата која ја користел кол центарот на Хрватската народна странка била изготвена од повеќе лица и дека биле користени повеќе различни извори. Од овие причини, *„не е можно да се утврди од каде и од кого биле добиени овие податоци“* поради што нема основа за понатамошно гонење на кандидатот за градоначалник.

За време на истрагата кандидатот за градоначалник тврдел дека користел јавни податоци за испраќање на писмата и дека можел да обезбеди податоци само за своите пациенти но не и за пациенти кои ги водат други лекари. Сепак, една друга лекарка од истата клиника во која работел дијабетологот кандидат за градоначалник потврди дека секој кој има основно системско познавање може да пристапи до податоците за сите пациенти. Таа тврдеше дека тој самиот ѝ ги прибавил податоците за сите пациенти за една студија која ја правела. Администраторот потврди дека повеќето од сестрите и лекарите имаат овластување да пристапуваат до тие податоци, а тој исто така потврди дека им ги дал податоците на еден друг лекар и на една сестра на нивно претходно барање по повод „некаква годишнина“.

Како резултат на одлуката на општинската канцеларија на јавниот обвинител во Дубровник да не покрене кривична постапка против кандидатот за градоначалник, на 5 март 2014 година клубот на градските советници „Srđ je naš“ ја информираше Хрватската асоцијација за промовирање на правата на пациентите за овој случај на злоупотреба на податоци на пациентите. Целта на оваа комуникација беше да се побара од Асоцијацијата да го искористи своето влијание и да го поддржи барањето на советниците до општинската канцеларија на јавниот обвинител во Дубровник овој случај да се проследи до Канцеларијата на државниот обвинител вон градот Дубровник.

По само неколку дена, на 7 март 2014 година асоцијациите обединети под „Платформата 112“ покренаа обвиненија против општинската канцеларија на државниот обвинител во Дубровник поради сомневање за политичка корупција. Едно од обвиненијата конкретно тврди дека, и покрај фактичките докази, оваа институција неточно ги отфрлила обвинувањата против лекарот дијабетолог. Тие исто така го информираа Народниот правобранител на Хрватска за тоа дека Хрватската агенција за заштита на личните податоци не покренала никаква истрага во однос на ова прашање, а воедно ја критикуваше и Медицинската комора на Хрватска.

Во овој случај имаме најмалку три можни сценарија за злоупотреба на информатичката технологија:

a) Приватните податоци на пациентите биле обезбедени на незаконски начин од некој во Општата болница во Дубровник, се претпоставува близок до кандидатот за градоначалник, со единствена цел создавање поштенска листа за локалните избори;

b) Некој однадвор провалил во базата на податоци – базата била хакирана и никој од болниците не би бил директно одговорен за тоа;

c) Некој од болниците ги обезбедил податоците за друга цел, а потоа до нив дошол и некој близок до кандидатот за градоначалник.

Случај 2 од Хрватска: достапност на доверливата база на Хрватската радиотелевизија на црниот пазар

Според Законот за Хрватска радиотелевизија, секое физичко и правно лице во Хрватска кое поседува телевизиски или радио апарат има обврска да плаќа радиодифузна такса. Хрватската радиотелевизија поседува и управува со регистар на месечни обврзници на оваа радиодифузна такса во Република Хрватска. Овој регистар не е јавно достапен. Со оглед на фактот што истиот содржи лични податоци на корисниците (како што се име и презиме, адреса, матичен број и сл.) управувањето и неговото користење се заштитени со законските одредби кои се однесуваат на безбедноста на личните податоци. Според информациите од Централниот регистар кој е јавно достапен и кој содржи податоци за системите во кои се чуваат лични податоци (во Агенцијата за заштита на личните податоци), регистарот на Хрватската радиотелевизија се наоѓа на сервер до кој физички пристап им се одобрува само на овластени лица. Овие овластени лица т.е. корисници можат да ги користат податоците со внесување на нивното корисничко име и лозинка, или со сертификат. Ова се реализира преку локална мрежа или преку интернет, со користење на заштитени податочни тунели. И конечно, резервните копии се наоѓаат во просторијата во која се наоѓа серверот.

Сепак, во 2004 година на црниот пазар се појави CD со целокупната база на податоци. Ова CD наводно било направено од вработен во Хрватската радиотелевизија кој работи со оваа база на податоци и кој се стекнува со корист од нејзината нелегална продажба.

Во овој конкретен случај се работи за злоупотреба на информатичката технологија со цел намерно умножување и продавање на податоци од страна на лице вработено во Хрватската радиотелевизија кое или имало пристап до регистарот или познавало друго лице кое има таков пристап. Поради ова биле прекршени сите горенаведени технички мерки за заштита, како и одредбите од Генералните правила за работа и однесување на Хрватската радиотелевизија според кои вработените во Хрватската радиотелевизија треба да работат согласно со највисоките професионални и основни етички стандарди и врз основа на неколку вредности, како што се доверливоста и заштитата на податоците, и согласно со важечката законска рамка и општите правила. Но очигледно е дека овие стандарди не биле применети во нашиов случај. Еден член на Управниот одбор на невладината организација „Potrosac“ го пријави овој случај до Секторот за кривични дела поврзани со економски криминал (DECO) при Министерството за внатрешни работи. Поради честите жалби на претплатниците од Далмација кои се чувствуваа „нападнати“ со понуди за услуги од разни компании (а кои ја користеле базата на податоци од Хрватската радиотелевизија), во 2004 година Хрватската радиотелевизија организираше интерна истрага во Секторот за наплата на радиодифузната такса, но оваа истрага не даде никакви резултати и претплатниците сè уште се предмет на „сензационални“ и „сензационалистички“ понуди од разни компании.

Случај 3 од Хрватска: Во потрага по бранителите

Повеќе години по ред едно од најголемите спорни прашања воопшто во Хрватска е утврдувањето на точниот број на воените бранители. Отсекогаш се шпекулирало со тоа колку, всушност, луѓе учествувале во одбраната на земјата за време на Војната за независност и колку од нив биле реално евидентирани како такви. Со оглед на фактот што никогаш не се објавени официјални податоци по ова прашање истото е една од главните теми во политичките пресметки помеѓу владејачката национал-конзервативна партија ХДЗ (Хрватска демократска заедница) и опозицијата. Хрватската демократска заедница отсекогаш била воздржана да го објави регистарот на бранители додека опозицијата ја обвинува ХДЗ за криење на бројките заради тоа што тоа ќе им овозможи на многу луѓе да ги искористат придобивките како да биле бранители иако реално го немаат тоа право. На бранителите им се овозможени бројни бенефиции: високи пензии, бесплатни станови и привилегии при купување возило. Според опозицијата, на овој начин Хрватската демократска заедница купува популарност кај народот. На 6 април 2010 година на интернет страницата www.registarbranitelja.com одеднаш беше објавена нецелосна листа на ветерани[29]. Авторите на оваа интернет страница беа анонимни и, како што тие самите велат на интернет страницата, нивна цел е да се спречи корупцијата и да се натераат хрватските власти конечно да ја објават целата листа на бранители.

Ваквата објава предизвика жестоки реакции низ целата држава. Тогашниот премиер Јадранка Косор ова го нарече „акт на разузнавачкото подземје“ додека Министерството за внатрешни работи веднаш објави дека станува збор за кривично дело кое се казнува со затворска казна во траење до три години. Министерството за одбрана и Министерството за бранители побараа итна истрага од државниот обвинител. Министерството за одбрана исто така објави дека неговиот информациски систем не е загрозен и дека не бил предмет на било какви обиди за компјутерски напад и криминал.

Поранешниот министер за воени бранители тврдеше дека многу лица имаат пристап до тие податоци. Според него, во 2003-тата година, кога тој бил министер, добивал податоци на CD-а. Според господинот Панчиќ, Владата би можела да дознае од каде биле украдени податоци со едноставно споредување на регистарот со информациите кои биле објавени. *„Во времето кога јас бев бранител имавме 403.000 бранители. Денес нивниот број е поголем од 500.000... Можеби некој го украл CD-то уште пред шест години а го објавил дури денес“*, изјави Панчиќ.

По неколку дена полицијата пронајде податоци кај четири лица кои порано биле вработени во подрачната единица за одбрана (регионално одделение на Министерството за одбрана) во Карловац и ги осомничи за кражба на податоците. Истрагата потоа покажа дека овие четири лица навистина ги објавиле податоците на интернет,

29 Ветераните беа вклучени во одбраната преку Министерството за одбрана и Министерството за внатрешни работи – оваа листа ги содржи само лицата вклучени преку Министерството за одбрана.

но и тоа дека вработените во подрачната единица (вкупно 23 на број) имале исто така пристап до истите податоци. Против четирите лица од Карловац не беа покренати обвинениј а. Во медиумите потоа немаше никакви дополнителни вести за тоа дека некој друг, исто така, би бил обвинет за злоупотребата на овие податоци. Владата на Хрватска, инаку, побара од компанијата која ја хостира интернет страницата www.registarbranitelja.com да ги отстрани податоците, но сопственикот одби да го направи тоа. Регистарот на бранители беше на интернет до април 2012 година кога заврши периодот на регистрација на ова домен име. Официјалниот регистар беше објавен на 19 декември 2012 година и содржеше во најголем дел податоци од оние кои беа објавени на горенаведената интернет страница.

Ова е пример за злоупотреба на службената положба. Со оглед на фактот дека податоците беа објавени, можеме да претпоставиме дека некој од една од подрачните единици на Министерството за одбрана ги зел податоците, ги објавил, или ги предал некому (можеби и му ги продал) кој потоа истите ги објавил. Можни се разни мотиви зошто овој регистар бил објавен, почнувајќи од политички спорови па сè до благородни цели (на пример, обид да се подобри транспарентноста). Сепак, останува фактот дека главна причина зошто дојде до ова беше непостоењето на минимум безбедносни протоколи во постапката на ракување со податоците кои им се доставуваат на подрачните единици на Министерството за одбрана во разни градови во Хрватска.

Случај 4 од Хрватска: Со мала помош од јавните службеници, вкупно 68 хрватски пасоши им биле продадени на криминалци

Во заедничка акција на Министерството за внатрешни работи (хрв. Ministarstvo unutarnjih poslova - MUP) и на Бирото за борба против корупција и организиран криминал (*хрв.* Ured za suzbijanje korupcije i organiziranog kriminaliteta – USKOK) под шифрираното име „Граница“ беа идентификувани вкупно седум лица обвинети за фалсификување и продавање на хрватски пасоши на криминалци од Србија, Босна и Херцеговина и Црна Гора. Во периодот од 2006 до крајот на 2010 година оваа група продала вкупно 68 фалсификувани пасоши по цена од 10.000 евра за еден пасош, со што заработила најмалку 680.000 евра.

Една јавна службеничка од Конзулатот на Хрватска во Орашје (Босна и Херцеговина) не беше изведена пред суд затоа што се спогоди со Бирото за борба против корупција и организиран криминал и прифати казна затвор од една година. Една друга службеничка која работеше како виш службеник во Одделението за пасоши во жупаниската полициска управа во Загреб беше обвинета за злоупотреба на службените овластувања и беше осудена на 13 месеци затвор. Пет други припадници на оваа криминална организација сè уште чекаат судење.

Улогата на главниот организатор на целата оваа операција била да обезбедува информации за лица кои се државјани на Хрватска но на кои не им е издаден пасош. Тој потоа организирал фалсификување на пасоши со трети страни (најчесто станувало збор за криминалци), прибирање фотографии и уплата на половина од договорената сума. Улогата на двајцата полицајци и на вишиот службеник во Одделението за пасоши во жупаниската полициска управа во Загреб била да ја проверува точноста на податоците кои претходно ги обезбедил нивниот колега а кои се однесувале на лица кои се хрватски државјани но кои немаат пасош. Овие податоци тие ги проверувале во информатичкиот систем на Министерството за внатрешни работи, поточно во регистарот на патни исправи на хрватските државјани (*хрв.* Evidencija putnih isprava hrvatskih drzavljana) кој всушност е еден од регистрите во информатичкиот систем на Министерството за внатрешни работи.

Тие биле во можност да го прават ова затоа што и двајцата, согласно со работното место кое го имале, поседувале корисничко име и лозинка неопходни за пристап до Регистарот на патни исправи на хрватските државјани. Иако оваа база на податоци требало да се користи само за службени цели, тие ги злоупотребиле своите овластувања и пристапувале до базата за криминални цели.

Откако ќе ги обезбеделе сите неопходни информации за лицата чии фалсификувани пасоши ќе ги користат, го фалсификувале и одобрението за подигнување на пасошите. Со ова овластување пасошот можел да се подигне во дипломатските и конзуларни мисии на Република Хрватска во Босна и Херцеговина и Србија. Овој дел од работата ѝ припаѓал на јавната службеничка која работела во Конзулатот на Хрватска во Орашје (Босна и Херцеговина).

Случај 5 од Хрватска: Полицаец фатен на дело додека вметнувал лажни податоци во информатичкиот систем на полицијата

Во 2005 година еден полициски службеник од Загреб вметнувал лажни податоци во официјалната полициска евиденција со кои се потврдува дека лице на возраст од 64 години од Србија и Црна Гора ја пријавило својата хрватска лична карта за изгубена, и покрај фактот што истото не поседувало ниту хрватско државјанство ниту хрватска лична карта. Уште повеќе, тој испечатил и потврда за загубена лична карта, ја оверил со официјален печат и ја вметнал во информатичкиот систем на Министерството за внатрешни работи, поточно во регистарот на лични карти (*хрв.* Evidencija osobnih iskaznica) кој е еден од регистрите во рамките на информатичкиот систем на Министерството за внатрешни работи. Полицаецот можел да го направи ова затоа што благодарение на своето работно место имал корисничко име и лозинка

за пристап до регистарот на лични карти и, со внесување на лажни податоци во овој регистар ги злоупотребил своите службени овластувања.

При редовен вообичаен мониторинг шефот на полициската станица ја забележал оваа потврда во информатичкиот систем и се посомневал во нејзината автентичност. По направената проверка е утврдено дека потврдата е фалсификувана и дека осомниченият полицаец ги злоупотребил своите службени овластувања. Како резултат на ова полицаецот е отстранет од должност и против него е поднесена кривична пријава.

Според информации од полицијата, осомниченият полицаец не примил поткуп од државјанин на Србија и Црна Гора. Тој ја фалсификувал потврдата за загубена лична карта за да му направи услуга на еден пријател, кој пак имал пријател на 64 годишна возраст кој бил во правна постапка на добивање на хрватско државјанство.

Случај 6 од Хрватска: Полицајци бришат податоци за сообраќајни прекршоци и објавуваат доверливи податоци (како поткуп прифатиле печено јагне и 20 литри вино!)

По подолг период на следење и прислушување, во заедничка организација на Министерството за внатрешни работи и Бирото за борба против корупција и организиран криминал беше спроведена акција под шифрираното име „Камион“ во рамки на која беа уапсени 37 лица од кои 11 полицајци – сите осомничени за објавување доверливи податоци од информатичкиот систем на Министерството за внатрешни работи. Полицајците беа осомничени за злоупотреба на службените овластувања и примање поткуп од сопственици на транспортни фирми, занаетчии и сл. Исто така беа осомничени за објавување информации за локацијата и времето на контроли на транспортните возила од страна на акционерското друштво „Хрватски патишта“ (хрв. Hrvatske autoceste - HAC) и тоа најмалку 80 пати. „Хрватски патишта“ е една од четирите компании кои управуваат со мрежата на автопатишта во Хрватска и вршат надзор врз транспортот на опасни стоки преку добивање на податоци за возилата од информатичкиот систем на Министерството за внатрешни работи. Лицата за горенаведената услуга примиле пари како поткуп, а во еден случај и печено јагне и 20 литри вино. Согласно со нивните овластувања и потреби како сообраќајни полицајци имале корисничко име и лозинка кои им овозможиле пристап до разни бази на податоци во рамките на информатичкиот систем на полицијата, меѓу другото и до податоци за местото и времето на контрола на транспортните возила од страна на акционерското друштво „Хрватски патишта“, надзор врз транспортот на опасни стоки и податоци за возилата. Иако нивна главна задача била да ја осигураат безбедноста на сите учесници во сообраќајот тие сепак ги злоупотребиле своите овластувања и пристапувале до базата на податоци за криминални цели.

Случај 7 од Хрватска: Случајно фатен при објавување доверливи податоци за возилата и за нивните сопственици!

Истовремено со следењето на организатори на меѓународна мрежа на проституција во рамките на заедничката активност на полициите на Хрватска и Шпанија под кодираното име „Каталонија“, детективите сосема случајно откриле и кривично дело од страна на сообраќаен полицаец и на административен службеник во полицијата на Меѓуморската жупанија. Во период од два месеци, полицаецот и административниот службеник објавувале доверливи податоци за возилата и за нивните сопственици на еден од притворените во акцијата „Каталонија“. Тоа притворено лице (инаку поранешен полицаец) не само што регрутирал девојчиња да работат под присила како проститутки во Лорет де Мар во Шпанија туку исто така се занимавал и со препродажба на автомобили. Кога купувал половни возила, сообраќајниот полицаец и административниот службеник му доставувале податоци за автомобилот и за сопственикот преземени од информацискиот систем на Министерството за внатрешни работи, поточно од регистарот на регистрирани моторни возила (хрв. Evidencija registracije cestovnih vozila). Тие можеле да го прават ова затоа што, врз основа на работното место, имале корисничко име и лозинка за пристап до овој регистар со што ги злоупотребиле службените овластувања и ги прекршиле законските одредби за заштита на лични податоци.

Не се знае дали тоа било направено за стекнување парична корист или како услуга на поранешен колега. Против двајцата се поднесени кривични пријави и се суспендирани од полициската служба сè до завршувањето на дисциплинската постапка.

Случај 8 од Хрватска: Секоја година од патариниte исчезнуваат 2 милиони евра

Вкупната должина на мрежата на автопатишта во Хрватска на 31 декември 2013 година е 1.288,5 километри. Кога користат автопатишта возачите имаат обврска да платат патарина. Вкупните приходи од патариниte во 2013 година изнесуваа сдруштво „Хрватски автопатишта“ (хрв. Hrvatske autoceste - HAC, една од четирите компании кои управуваат со мрежата на автопатишта во Хрватска), секоја година исчезнуваат околу 1% од приходите од патарини (помеѓу 1,7 и 2 милиони евра). Главни осомничени за ваквите загуби се вработените во „Хрватски автопатишта“ кои работат на патариниte. „Хрватски автопатишта“ забележа дека некои од нивните вработени изготвуваат и до десет пати повеќе сметки кои потоа се сторнираат и повторно се печатат но со променети податоци. На пример: кога на патаринатa треба да помине камион, вработениот на патаринатa ќе побара од возачот да плати полна цена за камионот (кога секогаш е поголема во споредба со онаа за автомобили), потоа ќе

пристапи во информатичкиот систем, ќе ја сторнира тукушто испечатената сметка, ќе вметне лажни податоци (дека возилото кое поминува не е камион туку автомобил) и ќе испечати нова сметка. Со оглед на тоа дека патаринатa е поскапа за камиони а поевтина за автомобили, вишокот од парите вработениот си ги задржувал за себе.

Во август 2010 година внатрешната ревизиска контрола на акционерското друштво „Аутоцеста Ријека Загреб“, инаку второ по големина друштво кое управува со мрежата на автопатишта во Хрватска, утврди дека вкупно 22 вработени лица краделе пари од патариниte на Демерје и Луцко. Лицата се пријавени во полиција а потоа и отпуштени од работа. Раководејќи се според принципот *in dubio pro reo*, судијата изјави дека судот има сомневања дека овие лица ги злоупотребиле своите службени овластувања и сториле кривично дело, но дека притоа не постојат докази за тоа кривично дело. Читајќи ја ослободителната пресуда, судијата побарал од нив да ја прочитаат поемата „Гавранот“ од Едгар Алан По и да обрнат особено внимание на последната реченица од секој стих: *„Никогаш повторно!“.*

Во овој случај акционерското друштво „Аутоцеста Ријека Загреб“ ги користело интерните информациски системи за ревизија како заштитна мерка против корупција со користење на информатичкиот систем. Како надоврзување на поетската ослободителна пресуда од страна на судијата, со цел да се спречат вакви слични случаи во иднина и како заштитна информатичка мерка, раководството на акционерското друштво „Аутоцеста Ријека Загреб“ одлучи да инсталира камери за следење на работата на вработените на патариниte. Овие камери нема да го снимаат лицето на вработените ниту нивниот глас, туку само работниот простор, рацете и постапката на наплата на патаринатa. Вкупна вредност на оваа инвестиција е 354.000 евра.

Случај 9 од Хрватска: „Валкани“ полицајци - полицајци им доставиле доверливи податоци на шверцери со оружје

Вкупно тројца полицајци од Загреб беа случајно фатени како на шверцери со оружје им доставуваат доверливи податоци од информатичкиот систем на Министерството за внатрешни работи. Додека прислушувале разговор помеѓу шверцери на оружје и полицијата, полициските инспектори слушнале објавување на доверливи податоци од информатичкиот систем на Министерството за внатрешни работи. Освен што објавувале доверливи податоци полицајците исто така бришеле и кривични пријави, фалсификувале документи па дури им давале и совети на некои од уапсените криминалци како да се бранат во текот на истрагата и ги предупредувале во случај полицијата да ги следи.

Првиот осомничен споделувал разни информации и податоци од информатичкиот систем на Министерството за внатрешни работи со свои пријатели, од кои некои биле криминалци. Станува збор за информации за налози за апсење кои биле издадени, приватни информации за келнерката која работела во кафе барот или информации за внукот кој избегал од дома. Другите двајца полицајци му помагале на колегата да ги добие сите овие информации и податоци од информатичкиот систем на Министерството за внатрешни работи.

Тие можеле да ги вршат овие активности затоа што, благодарение на својата работна позиција, имале корисничко име и лозинка за пристап до повеќе регистри, со што ги злоупотребиле своите овластувања и ја прекршиле законската рамка која ја регулира заштитата на личните податоци.

Конкретно, станува збор за следново: *„тајноста, интегритетот, постојаната достапност и контрола на податоците и информациите од користењето на информатичкиот систем на Министерството за внатрешни работи, се имплементираат преку повеќе организациски, системски и програмски мерки и процедури како и преку поделба на овластувањата и надлежностите. Сите корисници на информатичкиот систем на Министерството за внатрешни работи имаат обврска да имплементираат заштита на податоците согласно со упатствата пропишани со Уредбата за заштита на информатичкиот систем на Министерството за внатрешни работи при електронската обработка на податоци, Уредбата за безбедност и заштита на службените податоци на Министерството за внатрешни работи и на други интерни директиви и упатства кои се однесуваат на активностите кои треба да се преземат за заштита на податоците од информатичкиот систем на Министерството за внатрешни работи. Надлежностите на работното место го дефинираат степенот на пристап до податоците“.*

Како резултат од истрагата полицијата поднесе кривични пријави против 23 лица (од кои тројца беа полицајци). Тринаесет од обвинетите се изјасниј за виновни и се договорија со Бирото за борба против корупција и организиран криминал за поблаги казни. Првоосомниченото лице конечно беше осудено на шестмесечна затворска казна која потоа беше заменета со 50 денови општествено корисна работа. Судот, исто така, му забрани да работи како полицаец во наредните три години. Другите двајца полицајци, заедно со уште осуммина лица обвинети за добивање незаконски информации од тројцата полицајци, сè уште чекаат судење.

Случај 10 од Хрватска: Полицаец осуден на една година затворска казна затоа што на пријателот му дозволил нелегален риболов

Во месец мај 2012 година Советот на Жупанискиот суд во Ријека обвини двајца поранешни полицајци и уште едно лица за злоупотреба на доверливи полициски податоци. Првиот поранешен полицаец на свој познаник му објавувал информации од информатичкиот систем на Министерството за внатрешни работи во врска со регистрираните возила и профилите на нивните сопственици. За да го сокрие влегувањето во системот и за да ги обезбеди информациите користел кориснички имиња и лозинки на своите колеги со што ги злоупотребил своите овластувања и ја прекршил законската рамка која ја регулира заштитата на личните податоци.

Конкретно, станува збор за следново: *„тајноста, интегритетот, постојаната достапност и контрола на податоците и информациите од користењето на информатичкиот систем на Министерството за внатрешни работи, се имплементираат преку повеќе организациски, системски и програмски мерки и процедури како и преку поделба на овластувањата и надлежностите. Сите корисници на информатичкиот систем на Министерството за внатрешни работи имаат обврска да имплементираат заштита на податоците согласно со упатствата пропишани со Уредбата за заштита на информатичкиот систем на Министерството за внатрешни работи при електронската обработка на податоци, Уредбата за безбедност и заштита на службените податоци на Министерството за внатрешни работи и на други интерни директиви и упатства кои се однесуваат на активностите кои треба да се преземат за заштита на податоците од информатичкиот систем на Министерството за внатрешни работи. Надлежностите на работното место го дефинираат степенот на пристап до податоците“*

Лицето беше осудено на затворска казна од една година за сторени три кривични дела – злоупотреба на службените овластувања, а исто така и му е забрането да работи во државната администрација во наредните пет години. Уште еден поранешен полицаец беше исто така осуден на пет месеци затвор за поттикнување на други лица да сторат кривични дела, додека нивниот потсетник е осуден на четири месеци затворска казна за истото кривично дело.

Во периодот декември 2007 до јуни 2008 година првиот осуден полицаец исто така објавувал информации од информатичкиот систем на Министерството за внатрешни работи на свој колега во пензија. Овие информации се однесуваат на точните времиња кога патролни чамци на полицијата патролирале во морето околу Пореч со што тој точно знаел кога е безбедно незаконски да се вадат ретките школки со латинско име *Lithophaga lithophaga* кои, инаку, се строго заштитени со Уредбата за означување и строга заштита на ретки видови (Службен весник на Република Хрватска бр. 7/06 и 99/09).

Случај 11 од Хрватска: Постар инспектор злоупотребил службени податоци за да победи на локални избори

Постар инспектор од Даночната управа во рамките на Министерството за финансии во 2010 година пристапувал во информатичкиот систем на даночната управа со цел да утврди колку данок должат неговите конкуренти на изборите за претседател на локалниот огранок на Хрватската демократска партија (HDZ) во делот од Загреб познат како Спанско. Уште повеќе, тој ги искористил податоците од регистарот на даночни обврзници за да покаже колку данок должи неговиот конкурент и тоа го прикажал во летокот наменет за претстојните избори закажани за 1 јуни 2010 година. Во овој леток, освен информациите за даночниот долг, тој исто така напишал: *„Очекувате дека ќе просперираме со вакви лица кои ги избегнуваат даноците кон државата?“*. Тој бил во можност да го направи ова затоа што имал овластување да пристапи до одредени лични податоци на даночните обврзници, вклучувајќи ги тука и податоците за неговиот конкурент. На крајот инспекторот ги добил изборите.

По извесно време неговиот конкурент поднел кривична пријава против него за злоупотреба на службената положба и овластувања до државниот секретар во Даночната управа. Судот за државни службеници го прогласи виновен за *„сериозно прекршување на професионалната должност“* и го казни со намалување од 15% од плата во период од 4 месеци. Инспекторот потоа достави жалба до Вишиот суд за државни службеници кој истата ја отфрли. Врз основа на оваа одлука неговиот конкурент поднесе и жалба против него до Судот на честа на ХДЗ, но партијата беше блага и ги критикуваше за она што го направил.

Според членот 62 од Законот за данок на добивка (Службен весник на Република Хрватска бр.177/04, 73/08, 80/10, 114/11, 22/12, 144/12, Одлука USRH-120/13, 125/13, 148/13) за обезбедување на податоците неопходни за даночно утврдување, даночните обврзници или нивните овластени претставници имаат обврска да достават барање за упис во регистарот на даночни обврзници за данок на добивка до регионалната дирекција на даночната управа надлежна за нив согласно местото на живеење или работење.

Членот 8 од Општиот даночен закон (147/08, 18/11, 78/12, 136/12, 73/13) го воведува концептот даночна тајна. Сите податоци пријавени од даночниот обврзник и сите податоци кои се обезбедуваат при постапката на оданочување се сметаат за даночна тајна. Ова претставува еден вид заштита која спречува неовластено користење или јавно објавување на овие податоци. Обврската за чување даночна тајна се однесува на сите службени лица, експерти и други лица вклучени во процедурите за оданочување. Сепак, членот 8, став 2 од Општиот даночен закон исто така содржи одредби според кои, во одредени околности, некои податоци нема да се сметаат за даночна тајна. Тоа се податоци за датумот на влез и податоци за датумот на излез од системот за данок на додадена вредност, како и податоци за даночни обврзници кои пријавиле

лажни податоци во однос на данокот на додадена вредност. Ставовите 5, 6, 7 и 12 посочуваат во кои случаи нема да се прекрши обврската за чување на даночна тајна. Уште повеќе, според одредбите во членот 9 од Општиот даночен закон страните во еден даночен однос се обврзани да постапуваат со добра волја, што значи совесно и правично. Во конкретниот случај наведен погоре, постариот инспектор од Даночната управа во рамките на Министерството за финансии ги злоупотребил своите овластувања така што манипулирал со податоците од регистарот на даночни обврзници за да го дискредитира својот политички противник и на тој начин ја прекршил даночната тајна. Неговото однесување не било ниту етичко ниту било со добра волја.

Случај 12 од Хрватска: Немаш ни еден ден на работа? Не се грижи, секако ќе ти дадеме пензија!

Иако никогаш не работела, во 2007 година една повозрасна жена започна да добива пензија. Во последните три години добила повеќе од 20.000 евра. Ќерката на оваа жена почнала да работи во Хрватскиот институт за пензиско осигурување (HZMO) од 2007 година како раководител на Секторот за внатрешна ревизија. Нејзините колешки се посомневале дека таа пристапила во пензискиот информациски систем и дека ги сменила податоците за мајка ѝ за таа да може да биде корисник на пензија. Колешките ги пријавиле своите сомневања за можна измама до раководството на Хрватскиот институт за пензиско осигурување. Таа била во можност да го стори ова затоа што имала пристап до два регистри во Хрватскиот институт за пензиско осигурување: матичната евиденција на лица кои користат пензиско осигурување (*хрв.* Matična evidencija o osiguranicima mirovinskog osiguranja) и матичната евиденција за корисниците на правото на пензиско осигурување (*хрв.* Matična evidencija o korisnicima prava iz mirovinskog osiguranja).

Во текот на истрагата беше утврдено дека жената ја фалсификувала главната работна книга па против неа е покрената кривична пријава. Сепак, иако истрагата потврди дека мајка ѝ немала право на пензија, полицијата не можеше да докаже дека ќерка ѝ била таа што ѝ помогнала да се стекне со ова право. Конечно, ќерката била преместена од функцијата раководител на Секторот за внатрешна ревизија на функцијата координатор на Секторот за економски работи. Иако мајка ѝ повеќе немала право да добива пензија, таа никогаш не ги вратила парите кои дотогаш нелегално ги добила.

Косово

Подготвено од Хасан Претени и Дриарт Елшани

Напредокот на полето на информатичката технологија значително помогна во осовременувањето на националните институции, со што ефикасноста во нивното работење значително се унапреди. Сепак, не сите работи одат во полза на соодветно и ефикасно работење. Врз основа на работните практики на институциите задолжени за борба против корупцијата, во периодот од 2006 година досега Косово имал многу примери во кои информатичката технологија не била користена за целта за која била наменета.

Секој државен службеник на Косово има своја службена емаил адреса на домејнот @ rks-gov.net. Оваа емаил адреса треба да се користи само за службена комуникација помеѓу службеникот и другите, и само за службени работи. Секој корисник во рамките на овој домејн може лесно да ги дознае емаил адресите на другите лица вработени во државните институции. Овој емаил домејн го користат околу 70.000 лица вработени во косовските институции. Во оваа бројка се опфатени вработените на централно, регионално и локално ниво, понатаму службените лица во сите нивоа на власт (законска, извршна и судска власт); кабинетот на Претседателот и други независни механизми како што се косовската полиција и разни други агенции формирани од Собранието на Косово или преку други механизми.

Службените емаил адреси треба да се користат само за службена комуникација. Сепак, многу често има случаи во кои мрежата се користи за приватни и лични цели, или за комуникација од комерцијална природа или поврзана со политички партии. Лицата кои имаат влијание често знаат да ги злоупотребуваат службените емаил адреси (особено за време на изборни кампањи) така што ги повикуваат државните службеници да гласаат за нив или за нивната политичка партија.

Некои од државните службеници, во соработка со разни бизниси, имаат формирано наводни „професионални здруженија за обука на државните службеници“ во кои се вршат проневери на парите наменети за обука. Уште повеќе, се злоупотребува и компјутерската мрежа на косовските институции така што се испраќаат разни реклами со институциите т.е. државните службеници кои се повикуваа да патуваат во странство на семинари при што трошоците ги покриваат институциите. Ова доведе до тоа службените лица да учествуваат на нестручно организирани обуки, со многу лоша организација кои се покажаа како неефикасни за институцијата, но и како многу профитабилни за компаниите кои ги организираа обуките во соработка со службените лица задолжени за информатичкиот систем.

Во една пригода е забележана и флагрантна злоупотреба на системот, кога директорот на одделение на едно министерство отвори ресторан надвор од главниот град Приштина, го рекламирал отворањето на ресторанот преку емаил адресите на @rks-ks.net и ги користел службените емаил адреси да испраќа покани (дури и до главните раководители на институциите) за присуство на церемонијата на официјалното отворање. Ваквото рекламирање се покажа како штетно за државните службеници затоа што по неколку дена откако медиумите откриј дека државниот службеник користел службена емаил адреса за рекламирање и за испраќање на приватни пораки, неговиот ресторан бил предмет на напад, бил запален и изгорен до темел, по што никогаш повторно не беше отворен. Сепак, можно е ова да се случило и поради гневот на јавноста затоа што отворил ресторан како државен службеник, наместо избраниот начин на комуникација.

Сите косовски институции имаат службени интернет страници но поради недоволната сигурност и безбедност на нивната компјутерска мрежа речиси сите биле најмалку еднаш нападнати од хакери.

Не се ретки случаите во кои државните службеници го користат својот компјутер во работно време да комуницираат со други лица на социјалните мрежи, што се одразува на ефикасноста на нивната работа и на злоупотреба на информатичката технологија во институциите за лични потреби.

Имало и случаи во кои службените лица го користат интернетот, по завршувањето на работното време, да гледаат порнографски материјали или да посетуваат разни други страници кои пропагираат неморал.

Освен горенаведените форми на несакана употреба на информатичката технологија, во текстот кој следи подолу ќе презентираме и неколку конкретни случаи кои им нанеле штета на институциите а притоа профитирале поединци.

Случај 1 од Косово: Уништување на докази

Во периодот по војните во Косово се појавија многу барања за конечно стабилизирање на состојбата и работење во насока на добросостојба на граѓаните, преку создавање нови работни места и овозможување услови за севкупен развој на земјата. Еден од приоритетите на Владата тогаш беше унапредување на патната инфраструктура при што беа доделени значителни финансиски средства за изградба на локални и регионални патишта. Поради пост-воената ситуација на Косово имаше многу малку компании специјализирани за вакви градежни активности. Очекувањата на граѓаните беа големи па поради тоа тие ја поздравуваа секоја ваква преземена активност. Сепак, јавноста наскоро увиде дека градежните работи за изградба и обнова на патиштата не се реализирани според истите стандарди како што тоа било случај пред војната.

Некои од службените лица во Владата ја злоупотребија оваа ситуација. Тие, во соработка со сопствениците на градежните фирми, започнаа да ги злоупотребуваат финансиските средства и да не ги почитуваат важечките закони. Службените лица од државата почнаа да бараат поткуп од секоја фирма која сакаше да добие договор за работа.

Износот кој се барал за секој договор варирал помеѓу 10 и 20% од вкупната вредност на тендерот. Уште од своето формирање Агенцијата за борба против корупцијата добива информации за бројни обвинувања за корупција во ова поле. Најконкретна жалба беше онаа доставена од сопственик на фирма во која тој се жали дека, за да добие договор вреден милиони, државните службеници барале висок износ на поткуп (со седум цифри т.е. 15%) од вкупната вредност на тендерот.

Овој бизнисмен беше мошне загрижен и реши да ја исконтактира Агенцијата за борба против корупцијата, при што беше примен од службените лица на Агенцијата. Согласно мандатот кој го има Агенцијата и потпишаниот Меморандум за соработка со обвинителите на Европската мисија за владеење на правото на Косово (EULEX), Агенцијата одлучи овие информации да ги проследи до EULEX. Вредноста на овој тендер беше многу голема а и лицата кои беа осомничени за барање поткуп исто така се наоѓаа на високи позиции. Се работеше за многу чувствителен случај и истрагата започна веднаш. Во средината на 2007 година истражителите интервенираа во просториите во кои работа овие официјални лица, извршија контрола на истите и обезбедија значително количество на физички материјал, компјутер и друга електронска опрема, при што некои од службените лица беа и уапсени.

По неколку дена, службени лица на Агенцијата запленија и друга електронска опрема која се наоѓаше во Министерството за јавна администрација. Според институционалните правила кои важат за целата јавна администрација на Косово, серверите на кои се чуваат податоците на сите државни институции се наоѓаат токму во ова министерство. Истиот ден истражителите на EULEX исто така уапсија и две лица задолжени за информатичкиот систем. Заклучокот беше дека од серверите на Владата е избришан целокупниот материјал кој истражителите очекуваа дека ќе го пронајдат на тие сервери а кој би ги потврдил сомневањата на Агенцијата за борба против корупцијата за неправилности и кршења на законот. Единствата цел на овие истражители беше да се приберат докази против службените лица инволвирани во корупција па оттука и претпоставката дека се избришани податоците кои служат како доказ дека други фирми доставиле свои понуди со пониски цени. Со бришењето на овие податоци од серверот целта беше тендерот да ѝ се додели на фирмата со највисока цена. Истрагата продолжи уште неколку години и во моментов случајот го добива својата развршница на суд. Листата на обвинети лица ги содржи не само лицата од секторот за патишта туку и две лица задолжени за информатичкиот систем на Министерството за јавна администрација кои ја попречувале истрагата со бришење на податоците од главните сервери. Севкупно станува збор за 8 до 10 службени лица против кои е покрената кривична постапка. Кривичните дела за кои се обвинети се злоупотреба на службената положба, измама на работно место и

фалсификување на официјална документација. Со цел да се спречат слични вакви измами во иднина, серверите би можеле да се стават под одреден вид на независна контрола.

Случај 2 од Косово: Стекнување статус на воен инвалид

Во рамките на Министерството за труд и социјална добросостојба постои посебно одделение за воени инвалиди. Во месец јуни 1999 година, по војната на Косово, многу лица се пријавија за упис на листата на воени ветерани а подоцна, во текот на 2003-2004 година започна и работата врз конкретната листа на воени ветерани. Бројот на барања беше голем затоа што да се биде регистриран во листата значи не само добивање материјални бенефиции туку и посебен медицински третман, купување возила без обврска за плаќање на царинските давачки и некои други привилегии и бенефиции за нив самите и за членовите на нивните семејства. Некои од овие лица веднаш го стекнаа овој статус а некои подоцна – и токму лицата кои подоцна се стекнаа со овој статус, всушност, потоа беа проблемот.

Одредено лице ја извести Агенцијата за борба против корупцијата дека едно друго лице со иницијали Ф.М. ужива воена инвалидска пензија во износ од 200 евра месечно и дека неговиот степен на инвалидитет е оценет на 30%. Лицето кое ја извести Агенцијата потекнува од истото село во кое живее и лицето Ф.М. и тој дефинитивно е сигурен дека Ф.М. нема попреченост од толкав степен. Во Косово, инаку, постојат три воени здруженија: 1) Здружение на ветерани, 2) Здружение на инвалиди и 3) Здружение на национални маченици. Агенцијата за борба против корупција отвори случај и на почетокот побара материјали од овие три здруженија. Лицето Ф.М. било регистрирано како ветеран – учесник во војната но не и како лице со инвалидитет. Поради тоа, Агенцијата го искористи своето законско право и побара податоци и придружна документација од Министерството за труд и социјална добросостојба за лицето Ф.М. По добивањето на бараната документација можеше да се види дека постојат суштински разлики. Основниот документ за добивање на пензија не беше оригинален туку беше фалсификуван. Одговорен за тоа беше службеното лице задолжено за информатичкиот систем – тој го фалсификувал електронското досие на лицето Ф.М. така што во системот внел фалсификувана скенирана документација за добивање на инвалидска пензија. Заклучок на Агенцијата за борба против корупцијата беше дека постојат добри основи за сомневање дека службените лица во оваа канцеларија ги фалсификувале електронските податоци за да се овозможи материјална добивка - инвалидска пензија. Агенцијата го проследи овој случај до државното обвинителство кое, во рок од три месеци, ја ангажираше полицијата во постапка за прибирање докази. За време на криминалната истрага беа утврдени уште многу други неправилности. Правото на инвалидска пензија го уживале повеќе од 1.500 лица така што, со фалсификувани документи, биле пријавени како жртви на војната со инвалидитет а реално тоа не биле. Како последица на ова, личното богатство на лицето кое било раководител на ова одделение исто така значително се зголемило. Во моментов овој случај е во очекување на кривични пријави за дела кои се санкционираат со Кривичниот законик: службена измама и фалсификување на службена документација; додека трите службени лица во Одделението за инвалидски пензии во ова Министерство се суспендирани и без плата. Злоупотребата се правела со скенирање т.е. фалсификување на медицинскиот извештај. Лицето Ф.М. доставило документ со кој покажува дека има медицински проблем кој потекнува од војната во Косово, но овој документ, всушност, не потекнува од периодот на војната туку е изготвен пет години подоцна. Документот содржел датуми како да бил изготвен за време на војната. Овој случај покажува дека не е доволно да се направи само проверка на информатичкиот систем туку треба да се проверат и документите на хартија кои потоа се внесуваат во системот. Уште повеќе, евентуалните слабости на информатичкиот систем можеби ќе значат и потешкотии да се покаже дека документот навистина бил скениран и подоцна пополнуван со податоци, со што би се покрила целата шема на ова дело.

Случај 3 од Косово: Злоупотреба на лозинка

Огласот за вработување на директори на клиники при Универзитетскиот клинички центар на Косово беше неколку пати неуспешен. Кај медицинскиот кадар постои особен интерес за раководните позиции на одделенијата. Во одредени случаи Министерството за здравство (а во други случаи Независна надзорна комисија, како тело кое ги набљудува државните службеници т.е. нивното вработување или отпуштање од работа) ги откажа овие слободни работни места. Во период од повеќе години со најголем број од клиниките управуваа в.д. директори а во месец јуни 2014 година конкурсот за вработување на горенаведените позиции беше затворен. Беше формирана комисија за евалуација, изготвени беа прашањата за интервјуа како и сите подготовки неопходни за процесот на избор и вработување. Во некои клиники беа назначени директори но тоа не беше случај во вкупно осум други клиники. Еден од кандидатите за раководител на една од клиниките доби информации дека некои од другите кандидати однапред ги добиле прашањата што не би смеело да се случи – прашањата треба да останат тајни сè до денот на тестирање. Еден од членовите на Комисијата за надзор ги информираше медиумите[30] а тие ја објавија емаил адресата од која биле испратени прашањата. Притиснат од сите овие факти и од скандалот, член на Комисијата за избор на директори свика прес конференција на која призна дека на некои од кандидатите им биле испратени податоците од неговиот компјутер но дека тој не бил одговорен за тоа. Членот на комисијата се обиде вината да ја префрли на лице кое тој го обвини дека му ја украл и злоупотребил лозинката и кој

30 Дневен весник Tribuna, издание од среда, 13 август 2014 година бр. 1538, 2014 година, стр. 10-11 http://www.gazetatribuna.com/?FaqeID=1

неовластено имал пристап до неговиот компјутер а исто така кажа и дека на тоа лице му ја дал и личната лозинка кога заминал на одмор. Сепак, исходот од овој скандал беше оставка на членот на комисијата, повторно огласување на горенаведените работни места а во врска со преземање на други, дополнителни мерки, Агенцијата за борба против корупцијата сè уште нема информации за тоа.

Минатата година Агенцијата за борба против корупцијата неофицијално беше известена дека помошникот директор на одделение на еден од независните механизми неовластено ја користел емаил адресата на директорот. Има неколку случаи во кои вишите раководители ги овластуваат своите асистенти да пристапуваат до нивната емаил адреса и да комуницираат во нивно име, но конкретниов случај претставува неетичко однесување на асистентката која ја искористила емаил адресата на раководителот на институцијата од дома затоа што во тој период била на породилно боледување.

Случај 4 од Косово: Фалсификување на даночна документација

Ова е случај на фирма за чистење која конкурирала и која го добила договорот за чистење на објектот на едно министерство. Целата постапка почнала да се применува согласно со важечката законска рамка: работата ја добила понудата со најниска цена, склучен е договорот и имплементацијата започнала. Но по неколку месеци започнале да се влошуваат меѓучовечките односи на работниците во таа фирма. Сопственикот на фирмата отпуштил едно лице кое работело во министерството долги години и кое било задолжено за финансии и набавки. Истото лице, сега невработено и разочарано од ситуацијата, одлучува да му се одмазди на поранешниот работодавач и одлучува да ја обвини фирмата. Така што еден ден Агенцијата за борба против корупцијата добила информации од анонимно лице преку емаил: фирмата за чистење која ја поседува лице со сомнително претходно минато добива голем број на тендери за одржување на јавни институции на Косово. Информаторот исто така ѝ укажува на Агенцијата на кој начин оваа фирма ги добила сите тендери – во основа, фирмата не плаќа даноци и затоа може да понуди најниска цена. Доказ за редовно платени даноци е еден од основните документи кои понудувачот мора да ги достави во понудата. Сопственикот на фирмата го искористил своето влијание да го заобиколи ова т.е. имал добри односи со службените лица во даночната управа. Тој платил данок само еднаш, и тоа во висок износ, а потоа во сите постапки на јавни набавки ја користел истата потврда на која само го фалсификувал датумот. Сите службени лица во овие јавни институции можеле да го побараат оригиналниот документ на увид но биле воздржани тоа да го направат затоа што сметале дека си имаат работа со сериозен и возрасен човек и се задоволувале со тоа дека им е доволен скенираниот документ и дека со тоа фирмата ги исполнува нивните барања.

Агенцијата побара информации од оваа фирма од даночната управа со што сомневањата се потврдија како точни. Даноците не биле плаќани редовно а документите кои ги користела фирмата за да добие на тендерите биле фалсификувани и како такви не би можеле да бидат прифатени. Агенцијата ги разгледа и другите тендери кои ги добила оваа фирма при што утврди дека станува збор за една меѓународна институција и три локални институции. Интересно е што фирмата исто така доставила и понуда за одржување на објектот на самата Агенција за борба против корупцијата но во последниот момент од разгледувањето на понудите истата беше повлечена без објаснување. Пред неколку месеци до јавниот обвинител беше доставен кривичен извештај против оваа фирма а сите институции беа информирани за резултатите од истрагата и добија барање од Агенцијата за борба против корупцијата да ги раскинат договорите со оваа фирма. Но и покрај тоа, ниту една од институциите не постапи согласно со овие укажувања. Една меѓународна институција го раскина договорот и покрена постапка пред обвинителството на EULEX за надомест на штета. Агенцијата, исто така, побара од Органот задолжен за разгледување на набавките – тнр. тендерски суд - да ја стави оваа фирма на црна листа за во иднина да не може да добие ниту една друга работа во државните институции. За жал, Агенцијата сè уште нема добиено потврда дека локалните институции постапиле на сличен начин.

Македонија

Подготвено од Марјан Стоилковски и Розалинда Стојова

Дефиниција за корупција во Македонија

Гледано од правен аспект во Република Македонија, „корупцијата се однесува на злоупотреба на функцијата, јавното овластување, службената должност и положба за остварување на каква и да било корист за себе или за друг“[31].

Корупцијата може да се случи на сите нивоа на власт, а нејзини жртви можат да бидат поединци па дури и цели заедници. Корупцијата е комплексен криминал кој најчесто вклучува повеќе од две страни со што е тешко истата да се разграничи од другите видови на криминал, па поради тоа истрагата најчесто не ја третира корупцијата (вклучувајќи ја и корупцијата која се однесува на манипулирање или злоупотреба на информациски системи) како факт сама по себе. Наместо тоа, корупцијата најчесто се доведува во врска со други кривични дела.

Рангирање

Резултатите од двата најнови Индекси за перцепција на корупцијата кои ги објавува Транспаренси Интернешенел (CPI) покажуваат дека Македонија во 2012 година била рангирана на 69-тото место а во 2013 на 67-то место, што во регионален контекст ја става Македонија на второ место меѓу државите на РеСПА[32].

Сепак, од културолошки и социјален аспект важно е да се каже дека македонските граѓани ја рангираат корупцијата како најважен проблем со кој се соочува нивната земја, веднаш по невработеноста и сиромаштијата т.е. нискиот животен стандард. (истражување на UNODC, 2011 година)[33]

Година	Рангирање	Држава	CPI бодување
2012	69	Македонија	43
2013	69	Македонија	44

31 Закон за спречување на корупцијата, измени од 2 јули 2004 година, дефиниција за корупција содржана во членот 1-а: http://www.dksk.org.mk/en/images/stories/PDF/law/2004.pdf
32 Во 2013 година Македонија го дели второто место со Црна Гора.
https://www.unodc.org/documents/data-and-analysis/statistics/corruption/Corruptionreport_fYR_Macedonia_FINAL_web.pdf

Случај 1 од Македонија: Злоупотреба на системот за наплата на патарина

Задолжена да го истражи овој случај беше единицата за борба против корупција и финансиски криминал. На почетокот од истрагата единицата побара официјално да ги добие сите информации во врска со систем од компанијата која го развива и одржува управувањето со патариниte. Истрагата утврди дека во конкретниов случај станува збор за комбинација од разни видови на злоупотреба на информатичкиот систем кои ги направиле вработените, и тоа:

- Злоупотреба на информатичкиот систем со користење на разни овластувања за автентикација во системот, и користење на овластувања за автентикација на други вработени,
- Давање одобрувања за тоа дека возилата можат да поминат, или
- Влегување во информатичкиот систем преку менување на износот кој бил платен, или
- Неевидентирање на сите возила кои поминале на патаринатa, или
- Неиздавање фискални сметки и делење на износот со возачот на возилото по принцип 50:50, или
- Внесување на друга категорија на возила во системот наместо онаа која навистина поминала низ патаринатa.

За прибирање на соодветните докази беа користени специјални истражни мерки. Податоците и информациите кои беа прибрани од информатичкиот систем за време на истрагата помогнаа да се идентификуваат и докажат незаконските активности на организирана криминална група. На крајот, и првенствено преку разни анализи на податоци преземени од информатичкиот систем, беше можно да се направи проценка и да се пресметаат штетите кои биле направени.

Истрагата покажа дека станува збор за злоупотреба направена од лица, во нивно официјално својство, кои го користеле информатичкиот систем, со што им овозможиле на вработените да се стекнуваат со незаконска добивка која, во подоцнежната фаза, била „испрана“ преку законски инвестиции во други добра.

На 1 декември 2011 година беа покренати кривични пријави против 92 лица за злоупотреба на службената положба и овластување, за фалсификување, корупција (примање поткуп) и за членство во организирана криминална група. Со вршење на вакви незаконски активности организираната криминална група незаконски се стекнала со повеќе од 120 милиони денари и предизвикала компанијата да плати казни во ист износ.

Судската постапка заврши на 23 мај 2013 година со осуди кои варираа од 3 до 6 години затвор за вкупно 86 лица како и со пресуди кои предвидуваа плаќање на штетата направена на компанијата во износ од околу 107 милиони денари. Вкупно 11 лица беа осудени со конфискација на нивниот имот во вредност од 5 милиони денари.

По завршувањето на овој случај компанијата која ги поседува патариниte во Република Македонија го унапреди информатичкиот систем за управување со постапката за плаќање на патариниte и за следење на начинот на работа кај вработените. Унапредувањата на системот беа направени и развиени со цел надминување на утврдените и очекувани проблеми, преку автоматизација на работните процеси, избегнување да се внесуваат податоци за вработените во систем и интеракција со самиот процес.

Случај 2 од Македонија: Напад врз информатичкиот систем за јавни набавки

Почнувајќи од 1 јануари 2012 година, во Република Македонија, согласно со членот 8 од Законот за јавни набавки, нарачателите се обврзани да користат електронски аукции кај 100% од објавените тендерски постапки, објавени како отворени постапки, ограничени постапка, постапка со преговарање со претходно објавување и поедноставена конкуретна постапка.

Електронскиот систем за јавни набавки е интернет апликација во која објавите, огласите и тендерите се објавуваат целосно електронски и на која понудувачите електронски ги испраќаат нивните првично доставени понуди.

Системот е во сопственост на Бирото за јавни набавки а е хостиран од локален сервис провајдер. Системот има инсталиран фајервол (огнен ѕид/firewall), конфигуриран е со систем за откривање на упади (Intrusion Detection System - IDS) и користи виртуелна приватна мрежа (VPN) за да се овозможи безбеден пристап до системот. Инаку самиот систем користи безбеден https протокол како и SSL сертификати.

На ниво на самата апликација, системот ги регистрира разните видови корисници, нарачатели (договорни органи) и економски оператори (фирми). Системот има свое ниво на апликациски модули и им доделува на корисниците соодветни пристапни привилегии.

Нарачателите имаат свои интерни корисници на ниво на апликација т.е. локален администратор, единица за набавки, комисија за јавни набавки како и одговорно лице. Економските оператори (фирмите) исто така имаат свои интерни корисници и сите тие имаат исти привилегии и тоа: можност да споделуваат електронски постапки, учество на електронски аукции, поставување прашања итн. Една автентицирана сесија за еден корисник на ниво на апликација трае 40 минути. Ако нема никаква активност од корисникот за време на овој период корисникот ќе биде одјавен од системот.

Во август 2012 година на информатичкиот систем за јавни набавки беше објавено барање за набавка на автомобили. Со постапката на наддавање управуваше информатичкиот систем за јавни набавки а понуди доставија неколку понудувачи. За време на постапката на наддавање информатичкиот систем функционирал одлично сè до последните неколку минути по што се случил пад на системот и повеќе не можел да прима понуди и покрај фактот што корисниците се обидувале да достават нови понуди.

Случајот прво беше пријавен како упад во компјутерски систем и компјутерски криминал. Ова е процедурална пракса која имплицира дека, на почетокот, случаите од овој вид се истражуваат како компјутерски криминал додека во следната фаза на истрагата, и ако има докази за сторени други кривични дела, случајот ќе биде истражуван истовремено и за тие други кривични дела. Со оглед на фактот што овој случај се однесува на јавна набавка на опрема со голема вредност, се сметаше и се третираше како случај на компјутерски криминал и истовремено како еден вид на корупција. Иако не постоеја докази и информации на почетокот дека се случила корупција или злоупотреба, истрагата ги опфати и овие две нешта.

Единицата за компјутерски криминал го истражи овој случај и ги презеде сите чекори неопходни за зачувување на доказите и за обезбедување на сите релевантни информации кои ќе ја помогнат истрагата. На почетокот, од хостинг компанијата и од Бирото за јавни набавки беа побарани сите основни информации за информатичкиот систем, детални технички информации, сите релевантни системски, безбедносни и администраторски записи.

Единицата за компјутерски криминал ги доби inetpub записите од серверот во кој беа содржани IP адресите на сите оние кои пристапиле на апликацијата, апликациските записи и записите во текот на самата аукција. По направената детална анализа на информациите со користење на Linux оперативен систем и bash скрипти, се дојде до сознанија дека за време на критичниот период системот паднал поради „Distributed Denial of Service (Дистрибуирано одбивање на услуга/DDoS)“ напади направени од повеќе IP адреси од странски земји. Истрагата исто така утврди дека последната понуда била доставена од компанијата А неколку секунди пред да падне системот, но кога компанијата Б се обидела да ја достави својата понуда системот не бил достапен и затоа таа не била во можност да прифати нови понуди.

Компанијата Б го пријави случајот како потенцијална злоупотреба и ги достави податоците кои докажуваа дека тие доставиле нова понуда во периодот кога не бил достапен системот за јавни набавки а таа понуда не била регистрирана а поради тоа ни прифатена.

Подоцна, истрагата исто така утврди дека интернет страницата на информатичкиот систем за јавни набавки не била целта на DDoS нападот туку дека целта била друга интернет страница (информативната интернет страница). Од причина што и двата системи биле хостирани на истиот сервер, двете интернет страници не биле достапни.

Врз основа на записите кои беа доставени беше утврдено дека во текот на тој критичен период биле испратени многу барања до системот кои биле предмет на нападот а не интернет сервисот кој го опслужува системот на јавни набавки.

DDoS нападите се еден од методите кои се користат за онеспособување на некои интернет сервиси. До системот се испраќаат голем број барања со што тој станува недостапен затоа што не може одеднаш да го прифати и да го обработи големиот број на барања. Кога системот ќе дојде до точка во која нема да може да се справи со сите барања кои ги добил, тој вообичаено се исклучува. Најчесто ваквите напади се користат со користење на botnet компјутери (мрежа од многу компјутери кои ги контролира еден компјутер со намера за реализирање одредени активности).

Ваквите видови напади не предизвикуваат значителна штета на системот кој е предмет на напад (бришење или менување на податоците). Тие само ги прават недостапни услугите, и тоа обично преку исклучување на одредени системски сервиси и услуги или преку исклучување на системот.

На крајот, за овој случај беше докажано дека претставува злоупотреба на службената положба и корупција но тој дава преглед на постапката и на можните методи за злоупотреба на информатичките системи за целите на корупција, преку злоупотреба на службената положба или социјален инженеринг. Имајќи ги предвид технологиите кои се користат за олеснување и подобрување на секојдневната работа и услуги, можеме да идентификуваме голем број на modi operandi за злоупотреба на информатичките системи.

Системскиот администраторот има целосни привилегии во системот подолг временски период и доколку неговите активности не се контролираат и следат на соодветен начин тој би можел да го злоупотреби системот преку уништување или менување на дигиталните докази, со што ќе биде невозможно да се истражи случајот и да се докажат злоупотреби.

Случај 3 од Македонија: Злоупотреба на информатичкиот систем и незаконско објавување на лични податоци

Развојот на технологиите и примената на нови технички решенија како алатки за давање услуги во јавниот сектор ги зголемува ризиците од можна злоупотреба на службената положба од страна на вработените во институциите од јавниот сектор.

Во овој конкретен случај станува збор за злоупотреба на службената положба и на дозволата за пристап до информатичкиот систем во кој се чуваат податоци со одреден степен на тајност или податоци кои можат да се објават само под одредени услови. Според националното законодавство кое ја регулира заштитата на личните податоци, институцијата која ги чува или обработува личните податоци има обврска да следи посебни постапки за објавување на личните податоци.

Во овој случај еден вработен во јавна институција со пристап до податоците содржани во системот за финансиски примања ја злоупотребил својата службена позиција и ги објавил тие информации. Иако процедурите предвидуваат информациите да можат да се објават само на лично барање на граѓанинот или по барање на агенција задолжена за примена на законот врз основа на судски налог, во нашиов случај вработениот не ја почитувал постапката за објавување на лични податоци и објавил официјален документ генериран од информатичкиот систем во кој се содржани лични податоци. Потоа овој официјален документ беше користен како доказ во граѓанска судска постапка.

Овој случај беше истражуван од три аспекти: злоупотреба на лични податоци од вработено лице и институција (истражувано од Дирекцијата за заштита на личните податоци); злоупотреба на службената положба и услуги на работодавачите (можна корупција т.е. примање поткуп со цел стекнување на други бенефиции и предности); и злоупотреба на лични податоци согласно со членот 149 од Кривичниот законик кој се однесува на злоупотреба на личните податоци (истражувано од Министерството за внатрешни работи).

Истрагата која беше спроведена за злоупотреба на лични податоци и за злоупотреба на службената положба дојде до докази кои покажаа дека вработениот незаконски издал документ од информатичкиот систем и дека тој сторил кривично дело. Доказите за ова беа извадени од информатичкиот систем како и од уредот за видеонадзор (CCTV). Иако во овој конкретен случај не беше докажано примање поткуп или стекнување на други бенефиции и предности, фактот дека вработеното лице имало дозвола да го користи системот но немало одобрение од сопственикот на податоците истите да ги објави, беше сметан од истражителите (полицијата и обвинителството) како вид на корупција, согласно со дефиницијата во националното законодавство.

Овој случај е само еден пример за злоупотреба на службената положба, при што има уште многу други случаи слични на овој т.е. злоупотреба на службената положба за објавување на информации. Факт е дека овие случаи најчесто не се пријавуваат како кривични дела туку се само предмет на интерна истрага, во рамките на самата институција.

Случај 4 од Македонија: Злоупотреба во системот за регистрирање на бројот на работни часови

Во последната деценија системите за евидентирање на работните часови се интегрираат сè повеќе во секојдневната работа на голем број институции, јавни претпријатија, болници и училишта. Овие системи го регистрираат времето на пристигнување и заминување од работното место, како и службеното и приватно отсуство, при што зачуваните податоци се користат за да се изброи бројот на работни часови на вработениот во текот на одреден временски период. Бројот на работни часови се користи за пресметување на платите на вработените, за утврдување на времетраењето на континуирано отсуство на вработеното лице, и за други анализи. Според законската рамка, останувањето на работа прекувремено не значи по автоматизам прекувремена работа. Од друга страна, пак, редовното доцнење на работа во краток временски период е причина за покренување на дисциплински постапки. Ова е особено случај кај институциите кои работат само во една смена, знаејќи го фактот дека во Македонија не постои пракса на „флексибилни“ работни часови во администрацијата.

Во една од институциите каде беше инсталиран ваков систем за регистрирање на работните часови, улогата да биде одговорен за управување со целиот систем (администратор) му беше доделена само на едно лице. Администраторските привилегии подразбираа и можност да се истражат и разгледуваат податоците за присуство на работа и да се изготвуваат општи и конкретни извештаи (како што се извештаи за конкретен вработен, за група на вработени лица или извештаи за одреден временски период).

Откако повеќе од две години работел како системски администратор, вработеното лице ја препознало можноста да го искористи системот во лична полза и тоа така што ќе ги сменел датумите на доаѓање и заминување од/ на работа за истите да одговараат на законски дозволеното време а да не бидат реално прикажани. Вработеното лице ова го правело повеќе од година и пол без притоа да биде забележан од колегите или супервизорите. Еден ден се појавила потреба ова вработено лице да ги промени податоците за тоа утро или за последниот работен ден, без притоа да провери како се управува со податоците и како тие се чуваат во системот, особено без да провери на кој начин се евидентираат активностите на администраторот. Иако ретко, можноста за злоупотреба на системот сепак била искористена и тоа не само за „нагодување“ на задоцнетото доаѓање на работа туку и за менување на цели денови.

Речиси две години откако ја презел улогата на администратор, институцијата направила прераспределба на работните задачи помеѓу вработените, со што друго лице било поставено за системски администратор. Новиот администратор сосема случајно ја отворил евиденцијата (записите) од работење и увидел дека некои настани биле означени со што биле поинакви во однос на другите. Заинтересиран да дознае повеќе зошто токму тие се поинакви во споредба со другите, новиот администратор почнал детално да ја разгледува оваа евиденција и релативно брзо му станало јасно што значеле означените настани кои тој потоа ги пријавил на раководителите.

Процесот на истрага започна со назначување на официјално лице – информатичар од страна на институцијата чија главна задача беше да ги разгледа сите извештаи и евидентирани настани (записи). Заклучокот од оваа постапка целосно коинцидираше со претпоставките кои ги имаше новоназначениот администратор.

Поради лично признание од вработениот овој случај не заврши на суд и беше разрешен интерно во самата институција. Постоеше проценка за финансиска штета поради тоа што лицето не доаѓало на работа и не ги извршувало работните задача и во тој износ лицето беше казнето со адекватни дисциплински мерки, но неговиот договор за работен однос не му беше прекинат.

Случај 5 од Македонија: Злоупотреба на администраторските права

Еден од документите неопходни во постапката за издавање дозволи за увоз е и доставување банкарска гаранција во вредност пропорционална на вредноста на добрата или услугите кои се увезуваат. Правилата се многу строги – колку е повисока банкарската гаранција толку е поголема и вредноста на добрата кои можат да се увезат.

Системот за проверка на податоците на граничните премини и за издавање на дозволите користи податоци кои се внесуваат и чуваат во административниот центар на институцијата А. Иако некои од податоците се обезбедуваат и преку системска размена со други институции, вредноста која е ограничена со банкарската гаранција е онаа која ја внесуваат административните службеници, а не онаа внесена во банкарските информациски системи.

Во периодот на преместување од еден административен центар во друг, еден од администраторите открил начин како да се стекне со полза од позицијата која ја има. Откако бил преместен од административниот центар Б во административниот центар В тој забележал дека и понатаму ги има истите привилегии за пристап па така си отворил нова корисничка сметка за себе. Супер администраторот не вршел редовни проверки и ревизии на привилегиите на администраторите кои биле преместени на други позиции па поради тоа овој администратор можел да стори голем број на недозволени дела користејќи ја оваа новогенерирана корисничка сметка.

Во период од две години и со користење на лажна сметка повеќе од сто пати (а неговата сметка уште дузина пати повеќе), вработениот внесувал повисоки износи на банкарски гаранции пред да бидат направени проверки на граничните премини

а откако ќе завршела контролата ги враќал старите износи. Кога граничните службеници ги провериле своите системи, податоците кои ги внел администраторот одговарале на оние предвидени со законот. Тој, исто така, бил и во постојан контакт со раководителите на фирмата за да знае кога точно добрата ќе пристигнат на граница. Речиси истиот момент потоа евиденцијата во институцијата А покажувала повисок износ на банкарска гаранција.

Случајот беше откриен од внатрешната контрола и ревизија, заедно со секторот за информатичка технологија, при вршењето на редовна ревизија и контрола. Беше формиран истражен тим кој требаше да го разгледа овој случај и да утврди дека ова навистина е случај на корупција (ако во меѓувреме немало и други кривични дела) и до кој степен биле направени кривичните дела.

Со анализа на настаните во системската евиденција, истражниот тимот ги идентификуваше IP адресите од кои биле направени промените, што го доведоа до администраторот. Записите на датотеки не можеа да се менуваат така што беше многу лесно да се утврди листата на активности која ја правел администраторот.

Фактот дека се работи за дело со умисла беше потврден и со изборот на корисничкото име и лозинката за таа сметка. Тој се осигурал дека при редовни проверки на сметка и лозинка, неговата ќе биде меѓу последните за проверка и е една од оние кои не паѓаат во очи, со што избегнал секакво евентуално сомневање.

Беше докажано дека ова лица го злоупотребувало системот на институцијата А во соработка со една локална фирма а беше проценето дека финансиски ја оштетиле државата за 10.614.779,00 денари.

Црна Гора

Подготвено од Душан Дракиќ и Иван Лазаревиќ

Случај 1 од Црна Гора: Злоупотреба на службената положба и фалсификување на службени документи

Во овој конкретен случај станува збор за занемарување на задачите на работното место и незаконско однесување на државен орган т.е. злоупотреба на службената положба од лица вработени во тој орган.

Лицето А имало пасош со поминат рок по што извадило нов пасош. Службените лица во надлежниот орган на Министерството за внатрешни работи на Црна Гора одлучиле да го искористат стариот пасош со поминат рок за криминални цели. Користејќи го службениот печат тие ја продолжиле важноста на овој пасош за уште пет години, со името на лицето А но со фотографија на трето лице Б.

По лицето Б имало распишано потерница од полицијата и како последица на ова лицето А било приведено на пасошка контрола на аеродромот во Лисабон пред да се качи на брод и таму да работи во наредниот период. Откако му ги проверила документите за лична идентификација полицијата му ставила лисици и го однела во Центарот за емигранти на аеродромот каде поминал 48 часа по што полицијата го качила на авион од Лисабон за Белград, преку Швајцарија (рацете сè уште му биле во лисици). Сè до слетувањето во Швајцарија лицето А немало можност да си ги види личните документи. Третманот од страна на португалските власти и сликата која била создадена за него како криминалец значело дека лицето А претрпело душевна болка а неговиот углед бил сериозно разнишан не само во семејството и кај пријателите туку и во неговиот роден град.

Непоништувањето на пасош со поминат рок од страна на службено лице и активностите кои тоа ги направило за продолжување на рокот на тој пасош под истото име но со слика на лицето Б, и сето тоа оверено со службен печат, се активности кои претставуваат кривично дело злоупотреба на службената положба и истовремено значат потврда на незаконско однесување од страна на државните органи.

Во овој случај службените лица во надлежниот орган при Министерството за внатрешни работи не го поништиле пасошот кој, по издавањето на нов пасош, бил преземен од лицето А, инаку државјанин на Црна Гора.

Првостепениот суд надлежен за вакви кривични постапки заклучи дека непоништувањето на пасошот со поминат рок од страна на службените лица, и активностите кои ги наведовме во претходниот дел од текстот, се активности кои претставуваат

кривично дело злоупотреба на службената положба согласно со членот 216, став 1 од Кривичниот законик на Црна Гора, како и кривично дело фалсификување на службени документи согласно со членот 207, став 3 поврзано со ставот 1 од Кривичниот законик. Во тоа време ваквите кривични дела се казнуваа со затворска казна со времетраење од три месеци до пет години. Согласно со членот 216 од Кривичниот законик на Црна Гора злоупотреба на службената положба се случила ако службено лице, со користење на неговата функција или овластувања, ги надмине ограничувањата на тие службени овластувања или не постапи согласно со своите службени овластувања, понатаму ако обезбеди каков било бенефит за себе или за друго лице, ако предизвика каква било штета или ако сериозно ги прекрши правата на друго лице.

По доставената жалба на одлуката донесена во првостепена постапка, Врховниот суд на Црна Гора ја потврди пресудата на Основниот суд и во образложението на својата одлука, со број 902/13 од 12 април 2013 јасно укажува дека:

„сите наведени факти јасно го потврдуваат незаконското однесување на обвинетите – надлежните службени лица од Министерството за внатрешни работи на Црна Гора во Цетиње, кое предизвика штета на оштетената страна а за која, согласно со членот 172, став 1 од претходно важечкиот Закон за договори и прекршоци обвинетиот е одговорен, и согласно со одредбите од членот 154 од истиот закон тој има обврска таквата штета да ја надомести. Во презентирањето на своите заклучоци, Судот исто така се повика и на содржината на претходно наведените конкретни активности кои во овој случај исто така претставуваат незаконско однесување од страна на обвинетите, на сите околности поврзани со овој случај како и на фактот дека е потврден идентитетот на трето лице кое го злоупотребило фалсификуваниот документ на тужителот и неговите идентификациски податоци, и дека тоа лице е веќе одговорно за одреден број кривични дела сторени на територија на друга држава (Италија)“.

Во текот на судската постапка жртвата докажа дека, поради незаконското однесување на службените лица, тој исто така претрпел и нематеријална штета: повреда на неговиот углед, чест, прекршување на слободата и правото на интегритет.

Исто така, врз основа на податоците добиени од бродската компанија за вкупниот приход (по сите основи) на тужителот заработен за време на пловидбата (и изземен за спорниот период) и правилата кои ги регулираат штетите согласно со критериумите на датумот на изречената пресуда (член 189, став од Законот за договори и прекршоци), износот на материјалната штета на тужителот точно ја утврди финансиски вештак ангажиран од судот.

Заклучок 1

Горенаведениот пример покажува дека постои недостаток или проблем во ининформатичкиот систем за издавање на пасоши. Системот би требало (и не успева во тоа) да ги елиминира ризиците пасошите да се користат или да се издаваат и по завршувањето на нивната важност. Исто така е очигледно дека важноста на овој документ не може да се продолжи без внесување на неточни податоци во информатичкиот систем за издавање на патни исправи. Интересно е дека не постојат електронски траги за службените лица кои го издале овој документ. Во информатичкиот систем треба да има податоци за датумот, времето и името на службеното лице кое пристапило на системот и го обработило и издало документот. Ова исто така укажува дека системот за издавање и контрола на патните исправи (особено на граничните премини и на аеродромите) мора да има капацитет за анализирање и елиминирање на ваквите фалсификувани документи ако истите се појавуваат во системот. Сериските (идентификациските) броеви на овие документи треба автоматски да бидат препознаени и трајно да бидат избришани од електронската евиденција, додека самиот информациски систем треба да може да ги препознава истите како неважечки (иако овие податоци би биле корисни само во Црна Гора но не и во други држави).

За да се решат овие и слични проблеми неопходно е сите информатички бази на податоци да бидат редовно ажурирани и да бидат меѓусебно поврзани во што е можно поголем степен со цел серискиот (идентификациски) број на таквите документи да може електронски да се елиминира од понатамошна употреба или од можна злоупотреба од човечки фактор. Сепак, и понатаму останува ризикот ако таквиот документ е физички пренесен во трета земја и таму да се користи како валиден документ, што повторно го покренува прашањето за потребата од регионална информатичка соработка со цел елиминирање на потенцијалните ризици.

Случај 2 од Црна Гора: Искористување на информатичката технологија за нанесување политичка штета

Со цел да се испровоцира политичка дестабилизација и да се дискредитираат одредени високи државни лица/ политичари, или со цел стекнување на лична корист, во медиумите беше објавен наводен список на припадници на криминални организации во кој беа содржани телефонски броеви на високи државни лица/ политичари. Намерата беше да се влијае на јавното мислење преку индиректно поврзување на овие лица со конкретна криминална група и да се создаде слика за наводна поврзаност помеѓу државните органи и организираниот криминал.

На крајот од 2011 година овој список бил испратен од две пошти до еден дневен весник како и електронски од IP адреса на безжична мрежа која се наоѓа во објектот во кој живее вишиот државен службеник. Дневниот весник го објави овој наведен список според кој шефот на криминалната група (по кого Интерпол има распишано потерница за апсење поради шверц со дрога) телефонски разговарал со неколку високи државни лица во Црна Гора. Она што е особено интересно е што листата упатува на телефонска комуникација на шефот на криминалната група во 2008 година а која била чувана три години пред да биде објавена. Ова уште повеќе ги продлабочи сомневањата и шпекулациите дека во овој случај бил вклучен некој од оперативната структура на секторот полиција/ внатрешни работи/ безбедност чии мотиви биле лакомост или одмазда, во насока на предизвикување политичка дестабилизација во државата.

Случајот не заврши на суд затоа што истрагата утврди дека немало телефонска комуникација помеѓу високи лица во Владата/ политичари и главниот организатор на криминалната група, дека листата била фалсификувана и дека не е документ од полицијата, како што беше прикажано во медиумите. Уште повеќе, мобилниот оператор јасно стави до знаење дека објавената листа (дневниот весник тврдеше дека мобилниот оператор ја доставил истата до полицијата за целите на истрагата) не е листа која потекнува од овој оператор т.е. нејзиниот формат и содржина не одговараат на форматот вообичаен за ваквите листи со комуникациски сообраќај кои се доставуваат до овластени органи врз основа на нивно барање а согласно со постојната законска рамка во Црна Гора. Беше утврдено дека листата на лица посочени како главни организатори на криминалната група, а наводно изготвена од полицијата за нејзини истражни/ оперативни цели, била фалсификувана т.е. содржела имиња, броеви и адреси на високи лица од Владата.

Сè уште не се знае од каде изворно потекнува оваа листа или онаа која полицијата ја изготвува за свои оперативни потреби, ниту кој е фалсификаторот кој направил оваа листа да изгледа автентично. Исто така останува непознаница како и врз основа на што полицијата ја добила листата од 2008 година и каква истрага тогаш била спроведена против горенаведениот главен организатор на криминалната група, ниту кои биле резултатите од таа истрага и какви докази успеала да обезбеди.

Не се знае ниту кое лице ги испратило материјалите т.е. емаил пораките од горенаведените IP адреси.

Овој случај е класичен пример на кршење на основните човекови права кои се загарантирани со Уставот и меѓународните конвенции, кршење на правата на приватност и можна злоупотреба на службените овластувања, затоа што листата на разговори не може да се добие без одобрение од судот ниту може да биде објавена во медиумите. Исто така е голема веројатноста овој случај да претставува случај на поткуп и злоупотреба на службената положба, фалсификување на податоци и злоупотреба на информатичкиот систем.

Заклучок 2

Горенаведениот случај јасно укажува на ранливост на информатичките систем и можностите за негова злоупотреба. Тука првенствено се мисли на уставниот принцип кој се однесува на неприкосновеното право на доверливост на писмата, телефонските разговори и на другите средства за комуникација. Од друга страна, пак, е проблемот со евентуалната одговорност на одговорните лица во компанијата – мобилен оператор, првенствено во однос на доверливоста и следењето и злоупотребата на електронската пошта. Операторот има обврска да ги овозможи неопходните технички и организациски предуслови кои дозволуваат следење на комуникациите т.е. да им овозможи на надлежните државни органи добивање на зачуваните податоци за сообраќајот и локацијата, но исклучиво врз основа на судска одлука ако тоа е неопходно во кривична постапка или е неопходно од аспект на државната безбедност на Црна Гора. Јавноста не доби одговор дали воопшто имало вакво одбрение, кои истраги ги спровела полицијата тогаш и зошто. Случајот се покажа како извонредно сложен затоа што содржеше не само потенцијални елементи на злоупотреба на службената положба и овластувања туку и елементи на компјутерски криминал кои бараат високо ниво на знаење, обука и технички капацитети, како и квалитетна меѓународна помош.

Случајот не доби судска разрешница ниту даде одговори на серијата прашања наведени погоре. Не беше утврдена објективна или субјективна одговорност. Се разбира дека, освен политичката штета која беше предизвикана од овие настани, она што е уште поважно е фактот дека ако вакво нешто им се случува на лица кои се на високи позиции во Владата, без разлика на мотивите и причините, тогаш што би можело да им се случи на обичните граѓани на Црна Гора доколку тие бие се нашле во иста или слична ситуација.

Тука исто така треба да ја споменеме несоодветната и недоволна реакција од државните органи во однос на утврдувањето на објективната одговорност за работењето на институциите и на способноста да се откријат сторителите, што недвосмислено ѝ создаде немерлива штета на државата и на општиот принцип на владеење на правото, што се манифестираше преку губење на довербата кај граѓаните во работата на институциите. Неопходно е да бидат вложени дополнителни напори и целосно да се анализира постојниот систем за да бидат утврдени јасни процедури за добивање и користење на оперативни податоци, како и дефинирање на јасни и конкретни превентивни мерки со користење на софтверот и информатичките капацитети. Поконкретно, неопходно е да се продолжи да се работи на подобрување на комуникацијата со јавноста и медиумите во вакви случаи, во насока на поголема доверба на јавноста во работењето на институциите.

Случај 3 од Црна Гора: Злоупотреба на функции и внесување неточни податоци во јавни регистри

Овој случај се однесува на електронско изготвување на лажни дозволи или други сертификати со цел користење на таквите дозволи во правни постапки.

Врз основа на пресуда од Основниот суд во Котор од 2010 година, две лица (службено лице и шеф на општинскиот катастар во една општина во Црна Гора) беа прогласени за виновни за сторено кривично дело злоупотреба на службената положба согласно со членот 416, став 3, поврзано со став 1, од Кривичниот законик на Црна Гора. Пресудата вели дека овие лица ја искористиле својата положба и функција за стекнување на противзаконска корист и ги надминале своите службени овластувања поради тоа што изготвиле и објавиле одлуки за кои немале овластувања да ги изготват. Со првата одлука која ја изготвиле овозможиле повраток (реституција) и пренесување на државно земјиште на лице во чија сопственост, наводно, тоа земјиште се наоѓало претходно. Ова лице го регистрирало земјиштето во електронскиот катастар по што веднаш потоа го продало. Истовремено и на ист начин обвинетите лице издале уште една одлука со лажна содржина со која повторно некое земјиште му било вратено на лице кое, наводно, претходно го поседувало тоа земјиште. И во овој случај, веднаш по направената незаконска регистрација, наводниот сопственик веднаш го продал земјиштето, иако тој немал ниту важечки имотен лист, со помош и потпис на обвинетите службени лица. Со вршење и овозможување на вакви активности и преку реституција на земјиштето, обвинетите лица се стекнале со финансиска корист во износ од 571.307,32 евра.

Овие две лица беа осудени на затворска казна од две години.

Во постапката беше докажано дека двете обвинети лица ги надминале своите службени овластувања. Исто така беше докажано и дека на постапката за реституција и пренесување на земјиштето не ѝ претходела одлука од Советот на општината како и тоа дека одлуката била донесена без барање на овластени лица, поранешните сопственици, со што се избегнала постапката предвидена во вакви случаи. Сите овие активности значеле прифаќање на донесените одлуки во системот на катастарот без притоа да биде испочитувана предвидената процедура ниту, пак, да бидат застапени и заштитени интересите на општината.

Кривичниот законик на Црна Гора го дефинира кривичното дело злоупотреба на службената положба и овластувања како надминување на границите на своите овластувања со цел стекнување на противзаконска материјална корист во износ поголем од 30.000 евра.

Поради тоа, судот пресуди дека обвинетите лица (службеник и раководител на општинскиот катастар) дејствувале без овластување во овие случаи. Тие знаеле дека не биле овластени да овозможат реституција и не можеле да го пренесат земјиштето на наводните претходни сопственици. Тие исто така знаеле дека земјиштето било во надлежност на друг општински орган. Доказите исто така покажале дека одлуките кои ги донеле обвинетите не биле поткрепени со документација со која се докажува сопственоста на наводните претходни сопственици на кои ова земјиште им било „вратено“. Уште повеќе, постапката за реституција била реализирана по усно барање на лицето кое го купило земјиштето од наводните претходни сопственици, и покрај фактот дека тоа земјиште е национализиран имот и не може да се продава. Неоспорен факт за судот беше тоа што двете обвинети лица ги пречекориле своите овластувања, постапката предвидена за вакви случаи не била спроведена и интересите на општината не биле заштитени, со што обвинетите го сториле кривичното дело за кое биле обвинети.

Заклучок 3

Горенаведениот пример јасно укажува дека податоците од јавните регистри кои се чуваат електронски можат да бидат предмет на манипулација од страна на лицата овластени да ги користат и да внесуваат податоци.

На внесувањето на податоци во електронските катастарски регистри им претходеше донесување на незаконска одлука, што значи дека овој случај не е само кривично дело злоупотреба на службената положба предвидено со членот 416, став 3, поврзани со ставот 1, од Кривичниот законик на Црна Гора, туку дека можеби има и елементи на кривични дела поврзани со безбедноста на компјутерските податоци. Од овие причини јасно е дека евентуалните купувачи на земјиштето ќе бидат доведени во заблуда при проверка на податоците во катастарот по што ќе бидат изложени на судски постапки за докажување на правото на сопственост.

Во овој случај јасно се покажува дека, по одлуките донесени од општинскиот катастар кој, инаку, немал овластувања да донесе такви одлуки, биле направени промени во базата на податоци на катастарот. Случајот покажа дека постојниот информациски систем и постапката за водење евиденција (особено начини на пристап до базите на податоци и информатичките системи, како и можност да се прават измени во евиденцијата без постење на валидна законска основа) се карактеризира со неадекватност и нецелосност. Од суштинска важност е потребата да се унапреди информатичкиот систем на начин кој јасно и недвосмислено ќе ја дефинира постапката за пристап како и овластувањата според кои се можни пристап до податоците и измена на евиденцијата.

Случај 4 од Црна Гора: Незаконско издавање на патни исправи

Лице вработено во полицијата во Подгорица, Црна Гора (станува збор за службеник во Одделението за патни документи и оружје) беше обвинето за злоупотреба на нејзината службена положба со цел стекнување на бенефиции за други лица во текот на 2004 и 2005 година. Ова службено лице постапило спротивно на Законот за патни исправи и Одлуката за издавање пасоши, обични пасоши, патни сертификати и визи, откако добило барање за издавање на две патни исправи (пасоши) и ги пополнило документите без претходно да го провери идентитетот на апликантот или на лицето за кое било побарано издавање на патни исправи. Таа не ја направила ниту проверката неопходна согласно со горенаведените регулативи со што сторила кривично дело злоупотреба на службената положба согласно со членот 416, став 1 од Кривичниот законик.

Интересно е што во својата првостепена одлука, судот, земајќи ги предвид обвинението, одбраната и сите докази, утврди дека обвинетата треба да биде изземена од судско гонење согласно со членот 363, став 1, точка 1 од Законот за кривична постапка затоа што делото за кое била обвинета не претставувало кривично дело според законот. Во обвинението акцент се става на фактот дека обвинетата презела активности со цел обезбедување корист за тие лица но фактичкиот опис на кривичното дело пропуштил да го спомене делот кој се однесува на фактот дека пасошите им биле издадени на лица посочени во обвинението и во овој дел го испуштил делот кој се однесува на користа стекната за тие лица.

Особено интересен детаљ од пресудата е тоа што обвинетата изјавила дека, иако имала пристап до конкретните патни документи, немало евиденција од тие патни документи ниту, пак, биле пронајдени евентуални барања (апликации). Сите тие едноставно исчезнале. Кога нејзиниот раководител побарал документите да бидат побарани, било утврдено дека тие исчезнале. Интерната истрага не успеала да идентификува ниту едно лица поврзано со нивното исчезнување ниту да дознае што се случило со документацијата. Факт е дека документите биле чувани во архивата која се наоѓала во подрумска просторија на Центарот пред која постојано имало чувар. Сепак, до архивата пристап имаат сите вработени во ова Одделение па обвинетата можела само да шпекулира врз основа на што нејзиниот поранешен раководител дошол до заклучок дека токму таа го сторила тоа дело а не некој од другите седум колеги.

Во текот на постапката дојде до измена на Кривичниот законик: кривичното дело за кое службеничката била обвинета, со новите измени повеќе не се сметало за кривично дело. Така што, според членот 133, став 3 од Кривичниот законик судот имаше обврска да го примени она право кое е најповолно за обвинетиот па така обвинетата беше прогласена за невина во однос на обвинението и постапката беше вратена на повторно судење.

Во повторената судска постапка обвинети беа не само горенаведената службеничка туку и други две службени лица од полицијата/ Министерството за внатрешни работи. Овие две лица беа обвинети за злоупотреба на службената положба за фалсификување и издавање на голем број лични карти, возачки дозволи и пасоши во периодот 2011 – јануари 2013 година. Тие исто така беа обвинети и за внесување на лицата на кои им издале вакви документи во Регистарот на државјани на Црна Гора. И конечно, беа обвинети и за примање поткуп за секој лажно издаден документ во износ од 50 до 1.300 евра. Севкупно земено, обвинението товареше вкупно 17 лица за корупција т.е. давање поткуп и фалсификување на документи.

Две лица беа обвинети за посредување во примањето поткуп. Тие барале лица на кои им биле потребни вакви документи и за одреден надомест ги поврзувале со обвинетите службеници.

Уште едно лице (инженер по компјутерски науки) беше обвинето за фалсификување на документи. Во договор со горенаведените помагачи тој изготвувал лажни потврди за положен возачки испит.

Обвинети беа вкупно седумнаесет лица за плаќање поткуп и фалсификување документи.

Случајот доби судска разрешница во месец јули 2014 година. Службеничката, како главно обвинето лице, беше осудена за примање поткуп, извршување незаконско влијание и помагање на други во фалсификување документи со казна затвор од четири и пол години.

Севкупно земено, крајната пресуда на Посебниот совет на Вишиот суд во Подгорица ја осуди седумнаесетчлената група на вкупно седумнаесет години и четири месеци затвор за фалсификување документи и давање и примање поткуп.

Заклучок 4

Горенаведените примери исто така покажуваат дека постои, или дека имало, пропусти во системот за управување со документацијата на Министерството за внатрешни работи. Не постои електронска евиденција на скенираните барања за издавање на пасоши во информатичкиот систем кои би го елиминирале ризикот од користење и издавање на фалсификувани документи. Исто така, не постои ниту електронска евиденција за тоа кој ги издал таквите документи.

Како можно решение на овој и на слични случаи, неопходно е да се воведе скенирање на документите или да се воведат електронски бази на податоци на сите документи кои биле доставени и издадени на хартија, со задолжителна опција на обезбедување резервна копија за да се обезбеди безбедноста на податоците во случај на нивно намерно или случајно уништување. Понатаму, неопходно е да се унапреди безбедноста

на електронскиот систем во делот на евидентирање на секој физички пристап во просториите во кои се чуваат фајловите и службените документи.

Резиме

Кога станува збор за системот на кривична правда во Црна Гора, Кривичниот законик го смета корупциското криминал за кривично дело злоупотреба на службената положба во Поглавјата XXXIV и XXII. Како такви, корупциските кривични дела се поголема закана за општеството со оглед на тоа што сторители на овие дела се во најголем дел службени (јавни) лица. Со нивните дејствија тие го прекршуваат законскиот и административниот систем и ја намалуваат ефикасноста на државата. Освен очигледните материјални последици предизвикани од овие дела најштетна последица е заканата врз интегритетот на институциите и намалувањето на јавната доверба во работењето на државните и локалните органи, што доведува до уназадување во функционирањето на државата.

Кривичниот законик на Црна Гора ги пропишува следниве случаи на коруптивен криминал:

- перење пари (член 268);
- прекршување на еднаквоста во извршувањето на економска активност (член 269);
- злоупотреба на монополска позиција (член 270);
- злоупотреба на службената положба во деловно работење (член 272);
- предизвикување стечај (член 273) и предизвикување лажен стечај (член 274);
- злоупотреба на позицијата во економијата (член 276);
- пасивен поткуп во деловното работење (член 276а);
- активен поткуп во деловното работење (член 276b СС), (член 278 СС);
- злоупотреба на проценките (член 279);
- објавување трговски тајни (член 280);
- објавување и користење на берзанска тајна (член 281);
- злоупотреба на службената положба (член 416);
- несовесно работење во службата (член 417);
- измама во службата (член 419);
- незаконско влијание (член 422);
- поттикнување на незаконско влијание (член 422А);
- пасивен поткуп (член 423);
- активен поткуп (член 424)

Во основа, овие кривични дела се казнуваат со затворска казна и со конфискација она што било стекнато кога тоа е можно. Сепак, во пракса, овие кривични дела најчесто се поврзуваат со други кривични дела кои во основа не се коруптивни дела но се тесно поврзани со нив. Тука се мисли на фалсификување службена документација

и дела поврзани со безбедноста на компјутерските податоци. Се чини дека во обичајното право сè уште нема доволно примери за коруптивни дела во кои биле злоупотребени компјутерски податоци, но праксата ќе покаже колку се адекватни постојните заштитни мерки предвидени со законот и дали ќе биде неопходно да се воведат нови кривични дела кои се однесуваат на компјутерски криминал.

Останува фактот дека еден од механизмите за ефикасна борба против корупцијата е успешната судска завршница. Ова подразбира ефикасни методи за откривање и прибирање докази и постоење на ефикасни и адекватни санкции.

Институции надлежни за откривање, кривично гонење и санкционирање во Црна Гора се полицијата, јавниот обвинител и судовите. Овие институции се функционално поврзани една со друга и секоја, во рамките на своите надлежности, применува законски мерки и институти во борбата против корупцијата. Сепак, тие понекогаш се соочуваат со потешкотии во примената на овие мерки што бара организирање на стручни дискусии и законски измени во однос на корупцијата. Како орган задолжен за откривање на криминалот, полицијата има потреба од соработка и вклучување на други институции, првенствено банките и другите финансиски институции, Дирекцијата за антикорупциски иницијативи, Дирекцијата за спречување на перење пари, невладиниот сектор и самите граѓани. Од една страна полицијата е овластена да користи посеопфатни методи за прибирање докази (мерки како што се таен надзор во случај на кривично дело корупција, без разлика на начинот на кој биле сторени кривични дела и изречената казна) а од друга страна ваквите методи многу често го покренуваат прашањето за евентуално прекршување на основните човекови права и приватноста.

Без разлика на овие „потиснувачки“ мерки, спречувањето на корупцијата е од голема важност. Таа во основа бара подигнување на свеста, знаењето и на вештините, како и на одговорноста на вработените, од една страна, и овозможување на адекватни физички, технички и финансиски услови за вработените, од друга страна. Така што, еден од современите превентивни методи за обезбедување и овозможување законско и етичко работење кај државните органи е изготвувањето на планови за интегритет на самите органи. Тие се интерни превентивни антикорупциски документи, со нив се мапираат оние области кои би биле најподложни на корупција во самата институција т.е. анализа на ризикот на работните процеси во секој државен орган, институција или услуга. И на крај, плановите за интегритет треба да се разберат како еден вид на стратешко и квалитетно управување со ризикот што би требало да доведе до поголем квалитет на услугите кои ги дава јавниот сектор, намалување на трошоците и поголема отпорност на институциите на незаконски или несакани ефекти. Ова вклучува и дигитализација и користење на информатичка технологија, како едни од клучните елементи.

Србија

Подготвено од Немања Ненадиќ и Бојан Цветковиќ

Во рамките на студијата за коруптивни дела поврзани со информатичката технологија беа направени контакти со следниве институции:

- Министерство за правда
- Канцеларија на комесарот за информации од јавна важност и заштита на лични податоци
- Дирекција за е-Влада
- Министерство за внатрешни работи
- Министерство за финансии
- Народен правобранител

Одговор добивме само од првите две институции и закажавме разговори со нив. Дирекцијата за е-Влада одговори на нашиот повик но не успеавме да договориме разговор со нив.

Случај 1 од Србија: Сексуален акт кај Белградска Арена

На почетокот од месец март 2011 година на интернет се појави видео снимка на сексуален чин пред белградска Арена. Снимениот материјал датира од 24 април 2010 година (во раните утрински часови). Со оглед на тоа што снимката ја евидентирал системот за видео надзор кој го користи Министерството за внатрешни работи за контрола на сообраќајот во Белград, станува збор за јасен случај на коруптивно кривично дело злоупотреба на службената положба.

Првата реакција на луѓето кои беа главни ликови во снимката објавена на интернет беше релативно блага, но во наредните неколку месеци по инцидентот стана јасно дека снимката значително го засегнала нивниот живот и животот на нивните семејства.

Идентитетот на лицата Елизабета М. (24) и Милован С. (24) беше јавно објавен и тие буквално мораа да се кријат од сите обиди за настап во јавноста. Нивните семејства, според исказите, „поминале низ пекол“.

Комесарот за информации од јавна важност и заштита на лични податоци Родољуб Шариќ (во понатамошниот текст: комесарот) достави жалба до канцеларијата на Вишото обвинителство во Белград против „обичен полициски службеник“ за објавување на снимката од сексуалниот акт помеѓу две возрасни лица на интернет, со користење на снимки од системот за видео надзор кој го користи Министерството за внатрешни работи за контрола на сообраќајот во Белград. Тој посочи оти е јасно дека Министерството за внатрешни работи не ги презело сите технички, човечки и организациски мерки на претпазливост за заштита на податоците од системот на видео надзор од евентуална злоупотреба. Во овој конкретен случај информатичкиот систем бил злоупотребен преку незаконско добивање на податоците а преку манипулирање на постојните податоци и процедури. Во времето кога се случило ова единствената законска рамка која грубо би се однесувала на овој случај е интерниот правилник на сообраќајната полиција при Министерството за внатрешни работи според кој снимките од видео надзорот можат да се користат само интерно во рамките на Министерството за внатрешни работи за истражување на околностите на евентуални сообраќајни несреќи. Важно е да се нагласи дека не постои законска рамка во државата која би го регулирала овој случај. Исто така, била направена и манипулација со многу важната интерна политика на Министерството за внатрешни работи на високо ниво според која: *„ако нешто не е јасно регулирано со националното законодавство или со интерните регулативи и правилници на Министерството за внатрешни работи, вработените во Министерството треба да побараат официјална дозвола од Министерството за внатрешни работи наместо да претпоставуваат дека можат да го направат тоа нешто“*.

„Станува збор за настан кој претставува многу грубо кршење на приватноста и сериозно прекршување на Законот за заштита на личните податоци“, изјави комесарот и додаде дека отсуството на неопходните процедури и постоењето на безбедносни дупки се причината зошто дошло до овој инцидент.

Согласно со неговата надлежност комесарот спроведе инспекција за тоа како Министерството за внатрешни работи го применува Законот за заштита на лични податоци, која заврши со издавање предупредување до Министерството за внатрешни работи во кое беше содржана листа од 14 мерки и активности кои треба да се преземат на техничко, организациско и на ниво на вработените со цел заштита на податоците во насока на избегнување на каква било злоупотреба во иднина. Комесарот исто така побара Министерството за внатрешни работи официјално да го информира, во законски предвидениот рок од 15 дена, за планираните мерки и активности кои Министерството за внатрешни работи ќе ги донесе и спроведе за да ги отстрани неправилностите. Во оваа прилика Комесарот се потсети дека Србија нема закон за видео надзор иако има многу голем број на луѓе вклучени во видео надзор.

Почетната реакција од Министерството за внатрешни работи беше дека ќе биде многу тешко да се утврди кој точно ја ископирал снимката и ја ставил на интернет затоа што сите раководители, оператори и администратори во Командниот центар за операции имале пристап до снимките од системот за видео надзор што, заедно

со отсуството на пристап до податоците и безбедносни процедури, се покажа како јасна слабост во управувањето со системот за видео надзор на Командниот центар за операции при Министерството за внатрешни работи.

Откако Комесарот го издаде предупредувањето, Министерството за внатрешни работи презеде конкретни чекори за казнување на лицата инволвирани во овој инцидент. Интерната истрага утврди дека имало 10 компјутери (работни станици) од кои снимката можела да се симне и да се ископира.

Спроведени беа дисциплински постапки за злоупотреба на службената положба против инволвираните полициски службеници кои биле на смена во Командниот центар за операции при Министерството за внатрешни работи во Белград дента кога била направена снимката. Министерството за внатрешни работи објави детални упатства во официјалната инструкција насловена како „Задолжителни услови за употреба и одржување на видео надзорот на градските патишта и раскрсници во Градот Белград“ со цел премостување на постојните недостатоци во безбедносниот систем (како што е, на пример, фактот дека премногу луѓе имале пристап до системот, немањето евиденција во системот за тоа кој пристапил до кој дел од системот, итн.) и тоа не само во системот за видео надзор во Командниот центар за операции при Министерството за внатрешни работи во Белград туку и во слични такви системи на Министерството за внатрешни работи низ целата држава. Сепак, Министерството за внатрешни работи не објави детаљи за истрагата и за дисциплинските постапки така што немаме увид во евентуалните мотиви на сторителите на ова дело.

Комесарот навремено реагираше на активностите на Министерството за внатрешни работи, поздравувајќи го Министерството за конструктивната и корисна реакција на неговото предупредување, велејќи дека, иако според денешните стандарди за безбедност и заштита на податоците преземените чекори не се ништо посебни и се сметаат за стандардни, тие, во специфичните услови во Србија, се добредојдени затоа што недвосмислено претставуваат добра и корисна работа.

Иако оттогаш досега во Србија немало други вакви инциденти, годината 2014-та го искачи проблемот со снимки од системот за видео надзор во нови височини.

Во периодот од 8 до 10 јуни 2014 година на YouTube се појавија две снимки. Во првата е прикажана сообраќајна несреќа која се случила ноќта помеѓу 7 јуни и 8 јуни (сабота кон недела) 2014 година во Нови Сад т.е. прикажан е моментот на судир кога Ауди управувано од Д.В. (21) се судрило странично со возило Поло при што усмртило две девојчиња М.Л. и В.М., како и младо момче А.М., сите на 21 годишна возраст.

Втората снимка која го привлече вниманието на јавноста е од Ниш и покажува пешак М.З. (17) кој е удрен од Ауди на пешачки премин и кој претрпел тешки повреди како резултат од ударот.

Двете снимки беа емитувани од неколку домашни медиуми, заедно со објавувањето на лични информации на сите инволвирани лица.

Надлежниот комесар веднаш спровел истрага и надзор кај Одделението за сообраќајна полиција при Министерството за внатрешни работи во Нови Сад, во јавното комунално претпријатие „Информатика“ од Нови Сад (чии камери ги направиле снимките од автомобилските несреќи и Одделението за сообраќајна полиција во Ниш. Комесарот посочи дека „се соочуваме со реална опасност многубројните CCTV системи да се претворат во продукција на хорор и скандали“ и ги повика медиумите „да ги преиспитаат етичките стандарди на својата професија“. Според комесарот, објективното информирање на јавноста може да се направи и без непотребното нарушување на приватноста на инволвираните лица и без додавање на дополнителна горчина во веќе постојната болка поради загубата на своите сакани. Тој повторно ги потсети полицијата и другите државни органи на членот 42, став 3 од Уставот со кој јасно се забранува и се казнува употребата на лични податоци за други цели, освен за целите за кои биле обезбедени – во овој случај станува збор за придонес кон безбедноста на патиштата и помош во откривањето и докажувањето на криминал.

Семејствата на жртвите од Нови Сад и семејството на сериозно повреденото младо лице од Ниш изјавија дека објавувањето снимки од несреќата со нивните деца е важно за јавноста т.е. дека луѓето треба да видат како навистина се случиле несреќите но и да се намали можности за евентуално прикривање на доказите.

Иако во моментов додека го пишуваме овој текст резултатите од горенаведената инспекција и надзор сè уште не се познати, поуките од овој случај се Србија треба да изготви и донесе Закон за видеонадзор кој мора да биде усогласен со новата верзија на Законот за заштита на лични податоци[34] и директивите на ЕУ во оваа област.

Случај 2 од Србија: Кога изведувачот за информациски системи „фаќа корен“

Сегашното Министерство за правда на Република Србија го наследи поранешното Министерство за правда и јавна администрација, преку спојување на претходното Министерство за правда и делот на јавна администрација од поранешното Министерство за јавна администрација, локална самоуправа и човекови права.

34 https://docs.google.com/viewer?url=http%3A%2F%2Fwww.poverenik.rs%2Fimages%2Fstories%2Fmodel-zakona%2Fmodelzzpl.docx

Мандатот на претходното Министерство за правда траеше до месец јули 2012 година. Министерството за правда и јавна администрација беше формирано во месец јули 2012 година и постоеше до месец април 2014 година кога беше формирано новото Министерство за правда.

Во вкупно 10 години од постењето на јавно владеење во Србија, функцијата правда се наоѓаше во претходното Министерство за правда, по кое следеа помалку од две години заедничко владеење помеѓу функциите правда и јавна администрација. Сепак, како резултат на последната реорганизација на Владата функцијата правда сега е повторно единствена функција во рамките на ново Министерство за правда.

Секторот правда заедно со своите поврзани но независни целини претставува високосложена средина во која секоја целина има свои јасно дефинирани функции, процеси и одговорности и каде постои висок степен на регулација на интеракциите со субјекти и целини од други сектори. Министерството за правда и јавна администрација, како и новото Министерство за правда се цврсто убедени дека, за да може успешно да се управува и раководи со секторот правда информатичката технологија треба да се користи само како алатка за намалување на сложеноста на овој сектор. Стратегијата на претходното Министерство за правда беше сосема спротивна и насочена кон создавање сложени информациски системи кои ја мапираат комплексноста на секторот и бараат значителни буџетски инвестиции за оперативни и трошоци за одржување. Ваквите активности доведоа до голема разноликост во хардверот, софтверот и кај поврзаните информациски системи во рамките на информатичкиот екосистем на секторот правда, што сè уште создава голем проблем во однос на ризиците поврзани со надворешното ангажирање на изведувачи на овие информациски системи и на поврзаните можности за корупција.

Според Помошникот министер задолжен за информатичка технологија во новото Министерство за правда, во секторот правда постојат три различни главни информациски системи кои користат две различни софтверски платформи; две различни платформи на бази на податоци и една платформа на оперативен систем, иако сите тие му припаѓаат на едно семејство на информатички апликации – управување со документи. Ако ги земеме предвид и многуте помали системи (како на пример оние кои ги користи Уставниот суд) тогаш оваа бројка е уште поголема. На овие системи се потрошени повеќе од 10 милиони евра донаторски пари а имаат и буџетски импликации за Србија за трошоци поврзани со функционирањето и одржувањето – 1,5 милиони евра годишно! Ова би било прифатливо доколку целиот сектор правда е покриен со кој било или со сите три различни главни информациски системи, но во моментов покриеноста на секторот е помала од 25%. Заклучокот е дека, за да се покрие целиот сектор правда со сите негови субјекти и целини (75%) неопходна е нова инвестиција во износ помеѓу 20 и 30 милиони евра. Овие финансиски средства новото Министерство за правда ги нема поради кои годишниот буџет за одржување и функционирање нагло би се зголемил на повеќе од 3 милиони евра. Јасно е од горенаведените факти, како и од фактот дека глобалната финансиска криза исто така влијаеше врз тоа кои ресурси ќе останат достапни после намалувањата на буџетите, дека изнаоѓањето на овие средства е тешка задача. Новото Министерство за правда има значителни проблеми околу ризиците поврзани со изведувачите на информатичките системи, нешто што лесно може да доведе до корупциски кривични дела.

Во текот на јавната набавка на мрежни и комуникациски услуги (интернет и VPN WAN) која спаѓа под капата на корупција преку информациски системи и која конкретно може да се опише како „злоупотреба на службената положба“, „непотизам и фаворизирање“ и „прекршување на набавките“ од страна на вработените во претходното Министерство за правда и во полза на истиот информатички изведувач кој го користело претходното Министерство за правда како овозможувач на единствената национална мрежа и на комуникациски услуги. Имено, лице вработено во претходното Министерство за правда задолжено за компјутерски мрежи манипулирало со процедурите дефинирани во договорот помеѓу претходното Министерство за правда и изведувачот на информатичкиот систем во смисол дека процедурите за заштита и контрола не биле применувани или биле значително поедноставени во корист на добавувачите на информатичките системи и со цел намалување на нивните трошоци. Тој исто така ја злоупотребил службената положба со криење (правење недостапни) на податоците во врска со пристапот кој изведувачот на информатичкиот систем го имал во VPN WAN системот и уништувањето на електронска документација во системот со цел да се избегне контрола, следење и надзор на системот од страна на Министерството за правда и јавна администрација и од новото Министерство за правда.

Истото вработено лице во претходното Министерство за правда покажало непотизам и фаворизирање со прекршување на процедурата за набавки кога ги искористил податоците и информациите за системот кои не им биле достапни на повисоките раководители во Министерството за правда за да изготви тендерска документација за новиот тендер за набавка на мрежни и комуникациски услуги. Сепак, министерот во Министерството за правда и јавна администрација не дозволил објавување на оваа тендерска документација затоа што се плашел од негативните ефекти на тендерот кој потенцијално би можел да биде наместен во полза на еден давател на интернет услуги, инаку изведувач на информатичка технологија кој, во времето на тендерот, веќе осум години претходно давал мрежни и комуникациски услуги на ниво на целата држава (интернет и VPN WAN). Наместо тоа, министерот во Министерството за правда и јавна администрација дал налог да се изготви нова и правична тендерска документација, почитувајќи ги законите и користејќи ја најдобрата пракса.

На новото Министерство за правда и на даночните обврзници во Србија им беше нанесена финансиска штета бидејќи изведувачот на информациски системи на почетокот не сакал повторно да ги преговара цената и квалитетот на услугите, ниту му дозволил на новото Министерство за правда да започне нова тендерска постапка. Овој изведувач успеал да ја спречи новата тендерска постапка со користење на сложена шема составена од долготрајни, многубројни и исцрпувачки жалби овозможена благодарение на дупките во Законот за јавни набавки кој тогаш бил на сила. Вработеното лице од претходното Министерство за правда, кога се соочило

со реалноста, си заминало од Министерството за правда и јавна администрација. Притоа, Министерството за правда и јавна администрација покренало формална истрага и го извело случајот пред суд (во моментов овој случај е во рацете на претставниците на новото Министерство за правда).

Заклучокот кој можеме да го извлечеме од овој случај е дека јавните организации не смеат да ги потценат ризиците поврзани со однадвор ангажираните изведувачи на информатичките системи. Тие мора да имаат јасно пропишани процедури секогаш кога користат надворешни услуги. Како што приватниот сектор во иднина сè повеќе ќе биде тој кој ќе овозможува информатички услуги и имајќи предвид дека интерните буџети наменети за човечки ресурси сè повеќе ќе се намалуваат во иднина, изведувачите на информациски системи ќе добиваат сè поголема важност.

Случај 3 од Србија: Висок јавен службеник ги шпионира вработените

Со цел да дознае кој бил тој кој зборувал за нејзиното слабо работење, генералната директорка на Агенцијата за приватизација (во понатамошниот текст: Агенцијата) во тоа време го сменила од работното место раководителот за информатичка технологија на Агенцијата затоа што овој одбил да ја копира електронската пошта од вработените, по што таа му наредила на друго лице да ја копира поштата и со тоа имала пристап до голем број електронски пораки на вработените. Овој случај на „злоупотреба на службената положба“ доведе до нејзино предвремено пензионирање а со тоа и до крај на нејзиното работење како генерален директор на Агенцијата.

Како поранешен генерален директор на Агенцијата таа барала копии од службените емаил пораки од сите вработени во Агенцијата и тоа без нивно знаење, со што ја прекршила нивната приватност. Србија во моментов нема регулатива која ги регулира сопственоста и пристапот до електронската комуникација на вработените во работното време, поради што секој вид на таква комуникација (електронска пошта, чет разговори, телефонски разговори, социјални медиуми и сл.) се сметаат за лична сопственост на вработените. Од овие причини голем број фирми кои работат во Србија имплементираат свои интерни политики и процедури кои ги регулираат правата, обврските и должностите во однос на електронската комуникација. Така што, иако тука стануваше збор за деловни емаил пораки и фактот дека таа беше генерален директор на Агенцијата, неа сепак не ѝ беше дозволено да ги чита тие емаил пораки затоа што Агенцијата немаше соодветни политики и процедури. Не се знае кој сега има пристап до стотици илјади емаил пораки на 300-те вработени симнати после работното време и за време на викенди. Исто така, не се знае дали таа ги споделила со уште некој и ако да, со кого.

Причината за ова барање беше критичен текст за неа кој беше објавен минатиот ноември во еден неделен весник со наслов „Ограбување на Србија - како се поврзани сите инволвирани“ и поднаслов наменет конкретно за неа: „Кој ја врати кралицата на приватизацијата на сцената на криминалот?“. Текстот цитира една емаил порака напишана од еден од вработените со која одредени институции се известуваат дека раководството на Агенцијата ги забранило сите работни средби и им забранило да комуницираат преку емаил.

Вршителот на должност раководител за информациски системи во Агенцијата во тоа време посочи дека овој текст беше основната причина за намерата на генералната директорка „да докаже протекување на информации од Агенцијата“ а таа, всушност, сакаше да дознае кој им кажал на новинарите за нејзиното лошо деловно управување со Агенцијата. Според усни искази, раководителот за информатичка технологија се консултирал со неговиот адвокат за тоа колку е законско копирањето на емаил пораките без претходна согласност од вработените. Адвокатот му одговорил дека таквата наредба не е во согласност со Законот за заштита на личните податоци и со Кривичниот законик. Всушност, адвокатот го информирал дека казните за неовластена обработка на податоци и прекршување на доверливоста изнесуваат од 50.000 до еден милион динари а можна е и затворска казна во траење до две години.

Раководителот за информациски системи изјавил дека, кога ја прашал генералната директорка зошто ѝ требаат ископираните емаил пораки таа му одговорила дека тоа не е негова грижа. Тој исто така изјави дека на состанокот организиран во врска со ова прашање присуствувале и лица кои не се ниту вработени, ниту ангажирани, ниту имаат какви било формални врски со Агенцијата.

Во својот одговор до медиумите, генералната директорка изјави дека никогаш не побарала копирање на емаил пораките и негираше дека била ископирана некоја емаил порака од вработените. Запрашана дали раководителот на информациски системи е отпуштен поради неговото противење на ова барање таа одговори дека тој е отпуштен затоа што не си ја работел работата како што треба т.е. согласно со работниот договор без притоа да соопшти други детаљи. Поранешната генерална директорка посочи дека не знаела за објавениот текст во списанието кој се однесувал на неа и дека тукушто се пензионирала (неколку дена претходно) од позицијата генерален директор на Агенцијата.

Не се знае какви мерки биле преземени за надминување на проблемите во безбедносниот систем на Агенцијата бидејќи информатичкиот систем на Агенцијата бил злоупотребен преку формалниот хиерархиски синџир. Најдобар заклучок кој може да се извлече од овој случај е дека непостоењето на обуки за етика и за корупција со користење на информатичките системи, како и свеста кај јавните службеници, можат да бидат голем проблем затоа што тие се важни како суштинска долгорочна мерка на заштита против корупцијата преку злоупотреба на информатичките системи.

Случај 4 од Србија: „Мафија на патиштата“

Судењето на „мафијата на патиштата“ во Србија кое започна во месец мај 2007 година опфати вкупно 53 лица, најголем дел од нив вработени во јавното претпријатие „Putevi Srbije”. Овие лица електронски ги пренасочувале патариниte. Истиот беше опишан како најголем грабеж со користење на електронски алатки во историјата на правосудството на Србија[35].

Во месец ноември 2009 година Окружниот суд во Белград осуди 41 лице на вкупно 131 година и 10 месеци затвор. Обвинетите беа прогласени за виновни за задржување на дел од парите кои биле наплаќани на патариниte, со што го оштетиле јавното претпријатие „Автопатишта на Србија“ за околу 6,5 милиони евра. Деветмина од обвинетите беа ослободени додека тројца извршија самоубиство во текот на судската постапка[36]. Милан Јоветиќ, инаку вработен во внатрешната контрола во јавното претпријатија „Автопатишта на Србија“ и кој беше посочен како организатор на групата доби највисока затворска казна во траење од шест години. Второобвинетиот Живорад Ѓорѓевиќ кој исто така се сметаше за еден од водачите на групата беше осуден на затворска казна во траење од три години и два месеци[37].

Во јавниот дискурс на Србија вообичаено е да постои сомнеж дека луѓето осомничени и осудени за коруптивни кривични дела се обични „жртвени јагниња“ бидејќи корупцијата на високо ниво не може да функционира без „премолчено одобрување“ од највисоките политички нивоа. Сепак, уникатно за овој случај е што правосудните органи го констатираат токму тоа во својата пресуда:

„Судот смета дека Јоветиќ и Ѓорѓевиќ не се вистинските организатори на групата и дека вистинските организатори, за жал, останууваат непознати. Имаме докази... дека виновни се некои други луѓе... а останува непознато кој бил организаторот во Белград и кој земал 40% од парите”[38].

Како што се вели во пресудата, еден од осудените работници од „Микрос Електроникс изготвил и развил механизми и технички средства кои овозможиле законско дејствување и наплата на пари“ преку „користење на кабли за поврзување, постојни електронски уреди и посебен незаконски софтвер“. Едниот комплет кабли ги поврзувал горниот и долниот печатач на машината за издавање на билети. Други комплет на кабли, со прекинувач, ја поврзувал (или ја исклучувал) рампата за влез на возила и компјутерот на наплатното место. Овој механизам бил инсталиран на наплатните станици „Бубањ Поток“ и „Наис“ (двата краја на автопатот Ниш – Белград). Тој исто така инсталирал и корумпирана копија од софтверскиот фајл „EMU-87“ во постојниот оперативен систем за наплата на патарината. Ова му овозможило евидентирање на сметките за наплата на патарината без да го менува електронскиот систем. Шефовите на смената ќе ја стартувале нелегалната програма пред лицата задолжени за наплата да почнеле со работната смена.

Инаку вообичаениот софтвер, вклучувајќи го тука и оригиналниот фајл „EMU 87“ служел како математички копроцесор за аритметички операции. Со оглед на тоа што старите компјутери немаат копроцесор фајлот „EMU-87“ првично служел само да го емулира овој копроцесор. Бидејќи фајлот изворно бил дел од оригиналниот систем работникот за одржување само го вметнал новиот (нелегален) фајл на местото на стариот фајл. Разликата помеѓу оригиналниот и лажниот „EMU-87“ може да се забележи кога овој фајл ќе се отвори во текст едитор – оригиналниот фајл има „рачки и дршки“ кои го прават нечитлив додека нелегалниот фајл може лесно да се прочита т.е. да се види сметката во која пишува дека била наплатена патарина. Системот овозможува да се видат и својствата на фајлот, датумот на пристапување, итн. Како што објасни еден од контролорите, проверката и ревизијата не ја открија оваа измама затоа што истата не остави никакви траги во системот.

Комбинацијата од кабли, посебни електронски уреди и нелегален софтвер им овозможиле на лицата кои вршат наплата на патарината (припадници на организираната група) истовремено да печатат по две сметки за платена патарина со исти сериски броеви а во системот се регистрирала само едната од нив. Кога патарината, врз основа на оваа двојна сметка, била платено, софтверот дозволувал печатење на сметка без истата да ја евидентира во електронскиот систем за наплатена патарина. Истовремено, со притискање на копчето на камионите им се овозможувало да го продолжат патувањето по направеното плаќање затоа што тоа копче ја прекинувало врската помеѓу системот за електронска контрола на плаќањата, компјутерот и рампата. Истиот работник на Микрос Електроникс кој го инсталирал нелегалниот фајл исто така го одржувал и нелегалниот систем тогаш кога било потребно (менување на кабли, криење на нелегалниот софтвер по потреба, едуцирање на другите како да го користат системот, итн.).

Причината зошто системот можел да функционира толку долг временски период било немањето на ефикасна контрола и претстава за тоа колку, всушност, била раширена оваа криминална мрежа. Припадниците на криминалната група дури не ги ни отстраниле нелегалните кабли по завршувањето на смената, шефовите на смена не ги предупредиле дека треба тоа да го направат и незаконски стекнатите пари обично се чувале во самите кабини откако ќе биле наплатени. Контролата обично се вршела после 18 часот (кога бандата не оперирала) а имало и шифри за рано предупредување за евентуална контрола, итн.

Интересен е фактот, инаку споменат во судската пресуда но не е детално образложен, дека во периодот опфатен со пресудата помеѓу 2004 и 2006 година вкупниот износ на наплатена патарина ефективно се зголемил а инаку би се очекувало да се случи обратното како последица од кражбата. Сепак, ова е јасен индикатор дека системот

35 http://www.setimes.com/cocoon/setimes/xhtml/en_GB/newsbriefs/setimes/ newsbriefs/2007/05/29/nb-06
36 http://www.balkaninsight.com/en/article/serbia-s-road-mafia-get-131-years резултат од пресудата донесена од второстепениот апелациски суд беше минимално намалување на казните.
37 Ibid.
38 Судијата Владимир Вучиниќ, според дневниот весник „Политика“, http://www.balkaninsight.com/en/ article/serbia-s-road-mafia-get-131-years.

за измама функционирал многу подолг временски период и дека истрагата опфатила само некои негови аспекти и сторители.

Овој случај беше прв од овој вид кој ѝ ги отвори очите на јавноста во однос на еден од најпознатите дојавувачи (whistleblowers)[39] во Србија, човек кој бил привремено вработен во „Автопатишта на Србија“. Кога тој почнал да зборува за овие проблеми со другите колеги, реакцијата била да се дозволи да му заврши договорот на почетокот од 2006 година и образложението ќе биде дека „повеќе не постои потреба од неговите услуги“.

„Потоа јас решив да ги докажам сомнежите за кражбите кои се случуваа на патариниte – тема која никој не сакаше да ја актуелизира затоа што сите се плашеа за своите работни места. Јас направив тајно обележување на некои од сметките кои се издаваат на патариниte Ниш – Белград, како и тајно снимање, но за да можам да го докажам случајот неопходна ми е официјална листа на издадени сметки за да можам да покажам дека се работи за дупликати“, изјави тој.

Овој човек ја обележа/ означи сметката која ја добил возач на камион а исто така ја снимил и комуникацијата со возачите. Следно што му било потребно била официјалната листа, но „Автопатишта на Србија“ го одбила ова барање за слободен пристап до информациите. Комесарот за информации неколку пати имал обраќања во јавноста во врска со овој случај. Кога дојавувачот побарал помош од него за да може да ја добие официјалната листа на издадени сметки, комесарот побарал од „Автопатишта на Србија“ да ги објасни причините за отфрлање на барањето за информации. Комесарот не го прифатил аргументот дека станува збор за комерцијална тајна и донел решение со кое се наложува јавно објавување на оваа листа.

„Одлуката која ја донесов беше задолжителна за „Автопатишта на Србија“ согласно со законот но тие не постапија соодветно. Српската Влада, која инаку мора да овозможи спроведување на одлуката на комесарот ако тоа е неопходно, исто така не постапи во однос на ова”.

Човекот кој го изнесе овој случај пред јавноста исто така сведочеше во судскиот процес кој следеше потоа. Интересно е што неговата снимка, инаку еден од потенцијалните докази за криминално здружување, исчезна од судските досиеја пред почетокот на процесот.

39 Србија сè уште нема закон кој би овозможил ефикасна заштита на дојавувачите.

2. Мерки за заштита од злоупотреба на информатичката технологија

Вовед

Подготвено од Луизе Томасен

Случаите дадени како примери во глава 1 се однесуваат на злоупотреба на информатичко-комуникациската технологија (ICT) и на коруптивни кривични дела. За да можеме да извлечеме поуки од овие случаи во смисол на тоа кои мерки на заштита недостасувале и како државите научиле што треба да прават понатаму, авторите од секоја од државите во ова поглавје ќе ги посочат конкретните и општи мерки за заштита против злоупотребата на информатичко-комуникациската технологија за коруптивни цели, секој за својата држава.

Конкретни мерки на заштита од злоупотреба на информатичко-комуникациската технологија за коруптивни активности се:

- Технички мерки за заштита против неовластен пристап и злоупотреба на информатичко-комуникациските системи
- Организациски и процедурални мерки на заштита, како што е принципот „повеќе очи“
- Следење на сообраќајот на податоците и пристапот на вработените до системите со податоци
- Мерки за обука и подигнување на свеста за јавните службеници во однос на ризиците од злоупотреба на информатичко-комуникациската технологија за коруптивни цели и за мерките за заштита
- Ревизија на информатичко-комуникациските системи (внатрешна или надворешна ревизија; иницирана од државен орган или од извештаи или жалби од граѓани или медиуми)
- Мерки на заштита во законската рамка, како што се постоење на сеопфатно управно, граѓанско и кривично законодавство со цел спречување и санкционирање на злоупотребата на информатичко-комуникациската технологија за коруптивни цели

Со оглед на тоа што горенаведените случаи се однесуваат на коруптивни активности со користење на информатичко-комуникацискатa технологија кои веќе се случиле, ние не опфативме примери кои имале конкретен исход и кои резултирале со дополнителни или планирани заштитни мерки. Случаите од глава 1 се случаи на корупција од вистинскиот живот и како такви тие ќе ги надополнат и збогатат заштитните мерки кои треба да бидат воспоставени со цел борба против коруптивните активности кои ја злоупотребуваат информатичко-комуникацискатa технологија.

Можеби некои од горенаведените примери немаа судска разрешница а кај некои не беше сосема јасно кој што направил, каде и на кој начин, но она што е важно е дека можеме да научиме од сите тие случаи – да научиме дека треба да постојат мерки на заштита, каде информатичките системи се ранливи на злоупотреба и корупција и да научиме каков е напредокот на балканските држави во мрежата на РеСПА во насока на реализирање и имплементирање на заштитните мерки против злоупотребата на информатичко-комуникацискатa технологија и корупцијата во јавниот сектор.

Албанија

Подготвено од Едљира Наси и Енед Керцини

Во денешното време на информатика, со оглед на фактот што сè повеќе стануваме зависни од комплексни информациски системи, изненадувачки е колку малку внимание им е посветено на оние кои се задолжени за функционирањето и управувањето со овие системи. Овие луѓе се на функции кои се од огромна важност и кај кои високиот степен на доверба е императив. Незаконските активности од страна на овие лица можат да имаат огромни последици.

Сите случаи наведени подолу во текстот укажуваат на внатрешната закана за информатичките системи. Ќе укажеме дека проблемите со инсајдерите (лицата одвнатре) веќе постојат во рамките на полицијата, воените служби, приватните компании и во енергетскиот сектор. Исто така ќе покажеме дека постои силна тенденција кај раководителите да ги решаваат овие проблеми брзо и тивко, избегнувајќи притоа несакани влијанија од истите врз другите вработени и публицитет.

Не сме во можност навистина да докажеме колку реално се раширени овие проблеми. Она што го прикажуваме се чини дека е само врвот од ледениот брег.

Парадоксален е фактот што, и покрај очигледните интерни проблеми и забележителната ранливост на јавната инфраструктура, малку е направено за да се унапреди заштитата одвнатре а истовремено сите големи инвестиции постојано се посветуваат на откривање и спречување на удари однадвор. Се разбира дека заштитата од надворешни закани е важна но притоа не смееме да ги занемариме и проблемите со човечкиот фактор кои не можат да се решат со технолошки решенија.

Информатичките системи во јавната инфраструктура уште долго време ќе останат ранливи на злоупотреба од оние кои едноставно го познаваат системот: тоа се инсајдерите.

Главните проблеми кои ги нотираме во случаите наведени подолу се неуспехот да се разберат слабостите кај вработеното лице изложено на ризик и неуспехот да се имаат стандардизирани правила кои ќе ја уредуваат употребата на информатичките системи – и двете имаат експлицитни последици за злоупотреба.

Случај 1 од Албанија: Корупција во TIMS системот за гранична контрола

Овој случај претставува типична злоупотреба на службената положба и поткуп на граничен полициски службеник преку намерно внесување на фалсификувани податоци во информатичкиот систем на TIMS (Систем за целосно управување со информации) со цел да се избегне плаќање на давачките кон државата при увоз на возило.

Главната работа тука е фактот што постои голема разлика помеѓу начинот на кој системот вистински функционира во однос на следење на луѓето при преминување на државната граница и начинот на кој бил замислен да ги следи регистарските броеви на возилата.

Напредокот во последните години во однос на документите за идентификација и постоењето на посебни уреди за читање кои се инсталирани на сите гранични премини значително го унапреди процесот на регистрирање на лицата и го подобри квалитетот на автоматско евидентирање на податоците, преку едноставно и транспарентно читање на информациите од биометриските документи за идентификација кои се чуваат електронски во внатрешноста на RFID безбеден чип.

Сепак, истото не може да се каже за начинот на следење на регистарските броеви на возилата каде сè уште имаме рачно работење при читањето на соодветната документација, проверката на автентичноста на информации и проверување со единствените броеви „закопани длабоко внатре“ во добропознатите места во самото возило.

Токму оваа слабост на системот беше успешно искористена од еден инсајдер кој изготви „оригинален“ документ врз основа на неточни информации внесени во TIMS системот. Мораме да потенцираме дека, всушност, информациите беа точни, но временскиот печат беше фалсификуван. Многу поголем проблем (и тоа не е предмет на нашава студија) е фактот што возилото поминало царински преглед при крајот на 2009 година без да ги помине сите предвидени процедури за регистрација.

Во овој конкретен случај не биле користени софистицирани информатички алатки туку станува збор за намерна злоупотреба на информатичкиот систем. Најпрвин информатичкиот систем бил иницира со нерегистрирање на возилото во TIMS системот кога тоа било внесено во земјата а потоа е направена уште една злоупотреба (по четири години) кога сопственикот конечно сакал да го регистрира возилото.

TIMS информатичкиот систем има многу добри кориснички нивоа на привилегии и администрација. Граничните полициски службеници постапувале согласно со правилата и процедурите така што воделе евиденција и соодветно се потпишувале во хартиената евиденција. TIMS исто така има докажан вграден капацитет за евидентирање и следење на тоа кој што направил па затоа беше многу лесно да се идентификува инсајдерот откако биле добиени индикации и истите биле потврдени со другите обезбедени докази. Како таков TIMS системот ги докажа своите капацитети за поддршка на процесот на ревизија.

Не сме во можност да потврдиме дали овој случај довел до подобрувања на самиот систем, но секако дека треба да ги споменеме многубројните софтверски подобрувања на системот, софтверските поправки и други процедурални промени кои се применуваат периодично. Мониторингот и снимањето со системот за видео надзор беше работа која беше земена предвид и истата беше успешно применета како средство за обесхрабрување од намерите за прекршување на правилата и како средство за помош на државните власти да ги идентификуваат неправилностите во текот на истрагите.

Случај 2 од Албанија: Корупција во електронскиот систем за јавни набавки

Овој случај се однесува на кражба на идентитет на корисникот со цел стекнување привилегии во системот за јавни набавки а со јасна намера – менување на конечната одлука во процесот на набавки.

Албанија повеќе години наназад го користи електронскиот систем за јавни набавки и истиот се смета за успешен проект. Системот имаше позитивно влијание врз вкупните трошоци кои државата ги има при набавка на добра или услуги.

Накусо кажано, системот дозволува објавување на тендерска документација. Понудувачите потоа можат да ја испратат (upload) својата документација до системот, заедно со финансиската понуда. Целиот процес е енкриптиран и останува енкриптиран сè до крајниот рок за доставување понуди по што декриптирањето е можно само ако најмалку три или повеќе службени лица го внесат своето корисничко име и лозинка во однапред дефиниран временски период. На некој начин ова овозможува добар степен на транспарентност во постапката. Системот за набавки исто така е во можност да го сортира и автоматски да ги прибира и информира понудувачите за законската рамка, подзаконските акти и директивите. Важно е да се потенцира дека сè повеќе станува добра пракса, пред Државниот завод за ревизија да направи ревизија на работењето на некој јавен орган, претходно да добие целосен детален извештај од системот за јавни набавки во врска со работењето на тој орган и за временскиот период кој планираат да биде опфатен со ревизијата.

Она што го иницираше овој случај беше фактот што Државниот завод за ревизија утврди несовпаѓање помеѓу информациите содржани во електронскиот систем за јавни набавки и тендерската документација на хартија потпишана од соодветната тендерска комисија.

Како дошло до ова? На почетокот, кога Комисијата за јавни набавки ја започнува тендерската процедура таа пристапува кон електронскиот систем за јавни набавки. Слично како кај индивидуалните софтверски апликации, по првичното сетирање секој член на комисијата може да го внесе своето корисничко име и да избере лозинка.

Системот овозможува и „fail back“ функционалност ако некој има потреба да си ја ресетира лозинката. Оваа функционалност може да биде активирана од раководителот на комисијата задолжена за наддавањето. Притоа на корисникот му се испраќа емаил со линк за ресетирање на лозинката согласно со емаил адресата регистрирана за регистрација во системот. Сето ова е во ред но реално го намалува нивото на безбедност на лозинката на тој корисник затоа што генерално сите корисници се регистрирани со нивните официјални емаил адреси кои некогаш се споделуваат со други лица или меѓусебно си ги знаат лозинките. Иако оваа пракса била имплементирана со добри намери – решавање на проблемите на работното место, таа реално не ја намалува безбедноста на системот.

Исто така, имаме идентификувано уште една интересна работа. Иако постојат процедури и регулативи и истите се применуваат на ниво на информатичкиот систем (како што се прифаќање само на силни лозинки и периодични барања за промена на лозинката), сепак почнува да се појавува уште еден човечки фактор – поголема „едноставност во употребата“. Сме виделе податоци кои го потврдуваат ова. Најголем дел од корисниците стануваат нервозни поради барањето за повремена промена на сложените лозинки па наоѓаат решение воопшто да не ја менуваат изворната лозинка која системскиот администратор им ја доделил кога за првпат се логирале во системот. По три месеци нивната сметка ќе се блокира но многу е полесно да се побара ресетирање на лозинката на истата изворна вредност предвидена од системскиот администратор отколку да се памтат нови лозинки. На крајот, сè се сведува на тоа речиси сите лозинки да бидат исти.

Беше речиси невозможно да се докаже што се случило затоа што не постоеја записи на датотетки со кои подлабински ќе можеше да се следи оваа работа. Според Државниот завод за ревизија, единствената работа која со сигурност може да се потврди е фактот дека член на тендерската комисија не бил во Албанија (кој можел и да го докаже тоа).

На крајот, добриот дизајн на системот и процедурите нема да се покажат како успешни, а синџирот е силен онолку колку што е силна неговата најслаба алка. Во овој случај сме силно убедени дека било навистина многу лесно да се делува како друго лице, знаејќи ги слабостите поврзани со лозинките и искористувањето на системската можност за ресетирање на лозинката.

Сметаме дека не постои начин да се обезбедат соодветна заштита и безбедност со користење само на лозинки. Новиот систем мора да содржи и можност за користење на двостепена автентикација која нема да остави простор за злоупотреба на системските сметки на други лица.

Случај 3 од Албанија: ИТ корупција кај операторот за дистрибуција на електрична енергија

Овој случај претставува ’незаконска’ манипулација на информатичките системи од висок степен. Системот бил програмиран на начин да ги прикажува системските измени на вредноста на нивото на потрошувачка во системот за наплата. Ова му овозможувало на манипулаторот да го зголемува износот за наплата на сметките за електрична енергија со намера да остварува финансиска корист за компанијата.

Исто така, прибирањето на информации во овој случај претставувало голема потешкотија заради природата на експертизата што се користела за внатрешно управување со системот во рамките на приватната компанија, заради високите парични средства што биле во оптек, како и заради сè поголемото внимание од страна на незадоволната јавност.

Во овој случај недостасуваат вообичаените податоци преку кои се обезбедуваат доволно информации кои би помогнале да се разбере што всушност се случило со информатичките системи. Сепак, успеавме да направиме доволен број претпоставки врз основа на цврстите факти до кои дојдовме во тој момент.

При мерењето на податоци, утврдено е дека во ПДА уредите постои една јамка која, врз основа на одредени показатели, може да се исфилтрира и да не се доставува директно за наплата со оглед на тоа што би можела да обелодени проблематични клиенти, парични казни и други невообичаени прашања поврзани со наплатата, а кои персоналот би требало дополнително да ги разгледа. Фактот што таквите податоци биле филтрирани се чини разбирлив имајќи ги во предвид претходните проблеми поврзани со наплатата како и сомневањето на оние кои биле задолжени за мерењето дека потрошувачите ја штелуваат својата потрошувачка на електрична енергија. Фактот што постапката за мерење според записникот била спроведена за време на доцните вечерни часови и вон работното време на персоналот задолжен за мерење може да биде клучен показател за тоа дека прекумерната наплата била намерна и предмет на злоупотреба.

Временската ознака на трансакцијата е мошне сомнителна и претставувала еден од клучните аларми за време на истрагата. Теренските ПДА оператори не само што го прекршиле протоколот кој го уредува времето на прибирање на податоци, туку вре-

менските ознаки, исто така, покажуваат и фреквенции на користење на електрична енергија кои од човечки аспект се невозможни. Така, претпоставката била дека се прави или манипулација на податоците или фиктивно прибирање на податоци. Анализата на податоците упати на вториот случај.

Овој случај може да се смета и за софистициран обид да се изврши измама врз речиси 15.000 потрошувачи. Повторно може да се утврди истата шема – намерна злоупотреба на информатичките системи, но овој пат за целите на зголемување на профитот на компанијата. Разликата е во тоа што ваквата оперативa не може да биде дело на едно лице, туку во одреден момент се јавила потреба некому да се даде привилегирано одобрение да изврши таква дејство, а со оглед на тоа што профитот директно завршувал во финансиите на компанијата не останува ништо што би објаснило зошто се случило тоа дело, како на пример грешка во системот за наплата или грешка на персоналот.

Случај 4 од Албанија: Проневера и фалсификување во сметководството

Овој случај, навидум значително безопасен, претставува мошне изразена форма на злоупотреба на системот од страна на вработена задолжена за сметководството која во текот на годината проневерила средства кои била задолжена да ги администрира.

За да може подобро да се разбере зошто овој случај е интересен клучно е да се нагласи дека истиот не ја вклучува информацискатa технологија во вистинска смисла, туку попрво извршена е експлоатација од страна на благајничката во отсуството на увид или внимание од нејзините претпоставени.

Како се случило ова? Прво, финансискиот систем кој е задолжен за прифаќање на платниот список и за неговото испорачување преку банкарскиот систем изгледа не бил во можност да изврши истовремена обработка на поединечните детали на платите за целата јавна администрација и останатите владини сектори, како што е воениот сектор во актуелниов случај. Второ, постоел сериозен проблем во однос на довербата кој ја вклучувал внатрешната повисока управа, како и отсуство на двојна проверка на различните потпишани документи за плати од страна на надлежните финансиски органи.

Можеби првиот показател за овие потенцијални проблеми се појавил ненамерно, како резултат на вообичаена грешка, односно нешто што требало да му укаже на финансискиот службеник на слабоста на системот. Потоа, вработената намерно вметнала уште една грешка во платниот список со цел да се увери дека финансискиот систем нема да може правилно да ја детектира грешката, и така да добие потврда дека главната финансиска проверка е извршена за целокупните трошоци за плати кои не смеат да надминат одредени претходно програмирани буџетски ограничувања утврдени на почетокот на фискалната година.

Единственото нешто што вработената требала дополнително да го разработи со цел таквата шема да може да функционира е да направи совршено усогласување на некои од документите во хартиена форма кои се однесуваат на платите. На крајот на месецот овој платен список требало единствено да ја задржи истата сума. Така, табелите лесно можеле да се манипулираат под претпоставка поединечните детали да се задржат на она ниво кое благајничкиот систем очекува да го види како вкупна сума со цел да не се покрене евентуално сомневање. Истовремено, би имало мали негативни разлики за најголем дел од платите на поединечните вработени што би можеле да се сумираат во една единствена сметка која ја вклучува крајната сума. Постоела отворена можност за оваа злоупотреба со оглед на тоа што банките обично не се заинтересирани колкава е вредноста на платата на поединечно вработено лице. Она што е важно е сумата која е исплатена преку благајната да соодветствува со вкупната сума за плати. Различните компоненти и опсег кои фигурираат на платите во воениот сектор, како што се бенефиции и други додатоци, уште повеќе ја намалуваат можноста благајничкиот персонал и банката да изразат сомневање во однос на било што што излегува од нормалните стапки за плата.

Ова е причината зошто овој случај на проневера се одвивал подолг временски период. Сè додека вкупната сума не ја надминувала сумата одобрена од страна на началникот на службата и командантот, шемата можела да продолжи.

Овој тип на злоупотреба на системот може да се опише како таен напад врз комуникациите. Нападот во овој случај бил извршен од страна на лице кое ја уживало довербата на своите претпоставени, кое ги потврдувало платите без дополнителна проверка и кое го злоупотребило сознанието дека благајната и банката ја разменуваат само вкупната сума на плати.

Всушност, во моментов оваа дупка е затворена, со што благајничкиот софтвер сега е модернизиран, а размената на податоци со банките содржи повеќе деталји од благајничкиот систем.

МЕРКИ ПРОТИВ ИТ КОРУПЦИЈА ВО АЛБАНИЈА

Правни мерки за заштита

Во однос на правните мерки за заштита, Албанија неодамна направи измени на правната рамка и Кривичниот законик со цел да ја отслика појавата на компјутерскиот криминал или кривичните дела поврзани со информатичката технологија. Најважните правни норми кои исто така се однесуваат на полето на злоупотреба на бази на податоци и ИТ ресурси, конкретно Законот бр. 10023 донесен на 27 декември 2008 год. "„за одредени дополненија и измени на Законот бр. 7895 од 27 јануари 1995 год., и изменетиот „Кодекс на Република Албанија" предвидуваат нови кривични дела во Кривичниот законик, вклучувајќи компјутерска измама[40], компјутерско фалсификување[41], неовластен пристап до компјутер[42], незаконско снимање на компјутерски податоци[43], попречување на компјутерските податоци[44], попречување на компјутерските системи[45], како и злоупотреба на опрема[46].

40 Член 143/б – Компјутерска измама "Влегувањето, менувањето, бришењето или изоставувањето на компјутерските податоци или интерференцијата во работата на компјутерскиот систем со цел преку измама да се обезбеди за себе или за својата страна неправична економска придобивка или да ќ се причини на трета страна намалување на нејзините средства е дело за кое е предвидена казна затвор од шест месеци до шест години. Ова дело во случај да е сторено со соучесници или повеќе од еднаш или кога истото причинува сериозни материјални последици се казнува со казна затвор од пет до петнаесет години."

41 Член 186/а – Компјутерско фалсификување - "Влегувањето, менувањето, бришењето или изоставувањето на компјутерските податоци на незаконски начин со цел да се создадат лажни податоци за истите да се поднесат и користат како автентични, без оглед на тоа дали создадените податоци се директно читливи или разбирливи, е казниво со казна затвор од шест месеци до шест години. Во случај кога ова дело е сторено од лице кое е задолжено да ги чува и администрира компјутерските податоци, заедно со соучесници, повеќе од еднаш, или истото причинило сериозни материјални последици по јавниот интерес, се казнува со казна затвор од три до десет години."

42 Член 192/б – Неовластен пристап до компјутер - "Неовластениот пристап или прекумерен пристап надвор од овластувањата до компјутерски систем или дел од него, преку прекршување на безбедносните мерки, се казнува парично или со казна затвор до три години. Кога ова дело е сторено во компјутерскиот систем на војската, националната безбедност, јавниот ред, цивилната заштита, здравство или кој било друг компјутерски систем од јавна важност, се казнува со казна затвор од три до десет години."

43 Член 293/а – Незаконско снимање на компјутерски податоци - "Незаконското снимање преку техничка опрема на нејавни преноси на компјутерските податоци од или во рамките на компјутерскиот систем, вклучувајќи и електромагнетни емитувања од еден компјутерски систем кој содржи компјутерски податоци е казниво со казна затвор од три до седум години. Кога ова дело е сторено од/или во компјутерскиот систем на војската, националната безбедност, јавниот ред, цивилната заштита или од кој било друг компјутерски систем од јавна важност, истото се казнува со казна затвор од седум до петнаесет години."

44 Член 293/б – Попречување на компјутерските податоци - "Неовластеното оштетување, искривување, изменување, бришење или потиснување на компјутерските податоци е казниво со казна затвор од шест месеци до три години. Кога ова дело е сторено врз компјутерските податоци на војската, националната безбедност, јавниот ред, цивилната заштита и здравството или врз кои било други компјутерски податоци од јавен интерес казниво е со казна затвор од три до десет години."

45 Член 293/в – Попречување на компјутерските системи - "Создавањето на сериозни и неовластени попречувања со цел да се наштети на работата на компјутерскиот систем преку влегување, оштетување, искривување, менување, бришење или потиснување на податоците е казниво со казна затвор од три до седум години. Кога ова дело е сторено врз компјутерскиот систем на војската, националната безбедност, јавниот ред, цивилната заштита, здравството или кој било друг компјутерски систем од јавен интерес истото се казнува со казна затвор од пет до петнаесет години."

46 Член 293/н – Злоупотреба на опрема - "Производството, чувањето, давањето на употреба, ширењето или кое било друго дејство наменето да стави на располагање одредена опрема, вклучително компјутерски софтвер, компјутерска лозинка, код за пристап или други слични податоци кои се креирани или прилагодени за пристап до компјутерскиот систем или негов дел, чија цел е да стори кривично дело предвидено со членовите 192/б, 293/а, 293/б and 293/в од овој Законик е казниво со казна затвор од шест месеци до пет години."

Понатаму, неодамна беше усвоено законодавството кое ги покрива електронските бази на податоци, со цел да одговори на потребата за правна основа со која ќе се уреди креирањето на електронските бази на податоци со цел да се подобрат јавните услуги; исто така, овие законски акти имаат импликации врз користењето и управувањето со информациите во базата на податоци и процедурите кои вработените треба да ги следат со цел да ги постигнат предвидените законски стандарди во однос на безбедноста на податоците. Законот за државните бази на податоци бр. 10325 од 23 септември 2010 год. предвидува средства за регистрација и управување со државните бази на податоци, како и формирање на Координативно тело надлежно за регулирање на базите на податоци и нивното користење.

Министерот за иновации и информатичка и комуникациска технологија (сега Државен министер за иновации и јавна администрација) му предложи на Советот на министри конкретни мерки за обезбедување на безбедноста на базите на податоци. Конкретно, според Одлуката на Советот на министри бр. 961 од 24 ноември 2012 год. како надлежно координативно тело се именува Националната агенција за информатичко општество, додека според Одлуката на Советот на министри бр. 945 од 2 ноември 2012 год. се одобрува регулативата за администрирање на базите на податоци. Важен аспект од оваа регулатива за администрирање на базата на податоци е утврдувањето на степенот на безбедност, од висок, среден и низок[47], при што степенот на безбедност се утврдува врз основа на параметрите на интегритет, доверливост и достапност на податоците[48]. Исто така, се преземаат и технички мерки за безбедност врз основа на категоризацијата на базата на податоци. Преземените безбедносни мерки се под надзор на Државната агенција за компјутерска безбедност. Сепак, со оглед на тоа што Државната агенција за компјутерска безбедност е релативно нова институција со значително ограничени човечки ресурси, истата е во процес на зголемување на своите капацитети со цел да може да ги исполни барањата предвидени со закон.

Други важни регулативи во однос на прашањата поврзани со ИТ ги вклучуваат следниве закони и документи преку кои се обезбедува правилно спроведување и користење на ИТ системите:

- Закон за електронски потпис, бр. 9880 од 25 февруари 2008 год.
- Закон за заштита на лични податоци, бр. 9887 од 10 март 2008 год. изменет со законот бр. 48/2012
- Вкрстена стратегија за информатичко општество 2008-2013
- Закон за организирање и функционирање на националната инфраструктура на геопросторни информации на Република Албанија, бр. 72/2012
- Изменет Закон за електронски комуникации на Република Албанија, бр. 9918 од 19 мај 2008 год.
- Закон за право за информирање (изгласан кон крајот на септември 2014 год., бр.119/2014 со кој се замени Законот за право на информирање со официјални документи, бр. 8503 од 30 јуни 1999 год.

47 Член 17, Одлука на Советот на министри бр. 945 од 2.11.2012 (Анекс 1)

48 Ibid, член 18

Технички мерки за заштита од корупција

Најголем дел од стратегиите за безбедност на информатичките системи по својата природа се технички, а помалку се однесуваат на лицата. Две главни владини агенции во Албанија, НАИС (Националната агенција за информатичко општество) и НАЦС (Национална агенција за компјутерска безбедност) со помош на АСПА (Албанската школа за јавна администрација) се вклучени во обука за ИТ персоналот со цел подобро да се заштитат владините системи против евентуална корупциска злоупотреба. Улогата на Националната агенција за компјутерска безбедност е посебно важна имајќи во предвид дека ова е институцијата која обезбедува експертиза за контрола на безбедноста и на останатите мерки од базите на податоци. Особените карактеристики на контролата на базите на податоци обезбедуваат интересна позадина за подобро разбирање на начинот на кој се донесуваат мерките за заштита на ИТ. Според регулативата за администрирање на државните бази на податоци, системите подлежат на редовна контрола, односно секоја втора година за базите на податоци со висок степен на безбедност, секоја трета година за оние со среден степен на безбедност и секоја четврта година за базите на податоци со низок степен на безбедност. Постапката што се спроведува обезбедува постоење на технички мерки за заштита, а регулативата предвидува контролата да вклучува потврда на сообразност со инвентарот на средства на системот, контрола врз соодветноста на безбедносните мерки, како и контрола врз правилното спроведување на техничките и безбедносните мерки[49]. Врз основа на извештаите и записниците од спроведените контроли, институциите преземаат соодветни чекори за корекција на евентуална докажана неусогласеност.

Организациски и процедурални мерки за заштита

Согласно со законот, во моментот се спроведува една постапка (Упатство за стандардизација на изготвување на проектната задача за проекти на информатичко комуникациски технологии во јавната администрација, бр. 2 од 9 февруари 2013 год. донесено од Министерот за информатичко општество) според која секој владин орган кој врши ревизија на постоечкиот или гради нов информатички системи мора да добие одобрение по извршен преглед на предложениот дизајн и не смее да добие никаков приговор во однос на предложената проектна задача од страна на експертите во Националната агенција за информатичко општество. Ова е стратегија на Република Албанија за искористување на најдобрата локална стручност и знаење, од моментот на првичното создавање на јавен ИТ проект до моментот на финализација на тендерската документација.

Новата влада на Република Албанија согласно со агендата за борба против корупција неодамна воведе нова постапка со помош на Националната агенција за информатичко општество која се однесува на прифаќањето на информатичките системи. Се очекува да се има поинаков пристап кога станува збор за прифаќање на информатичките системи, при што ќе се овозможи учество на работната група назначена да го спроведе прифаќањето заедно со надворешни експерти. Со ова се очекува значително да се намалат одредени прашања кои претходно беа утврдени кај проектите за информатички системи за време на периодот на прифаќање (премногу толерирање и премногу незавршени работи), кои најчесто беа поврзани со техничкиот и раководниот персонал.

Да се каже дека безбедноста е нешто што лесно може да се купи би било некоректна изјава. Човечкиот фактор е тој кој може да покаже дека дури и најподатливите очекувања можат да бидат неточни.

Обука и подигнување на свеста

Во Албанија се спроведува уште една тековна иницијатива превземена од Националната агенција за компјутерска безбедност во соработка со Албанската школа за јавна администрација, во рамките на која се организираат обуки за речиси целокупниот персонал за информатички технологии вработен во јавните институции и другите владини органи. Обуките покриваат различни теми, како на пример безбедност на системите, и заштита и оценка на надворешниот и внатрешниот ризик. Ова би можело да се смета за прв чекор на позитивен развој во насока на менување на фокусот од опрема и софтвер врз персоналот кој го администрира и користи.

Заклучок

Како заклучок, сигурни сме дека потребно е да се испитаат и други начини на управување со безбедноста на информатичките системи и спречување на корупција која произлегува од самиот систем, со оглед на тоа што често постои тенденција да се занемарат социјалните фактори на ризик од ’внатрешна закана’ и потешкотиите во прилагодување на информациските процеси со неформалните структури на јавните установи.

49 Член 24 (3), Одлука на Советот на министри бр. 945 од 2 ноември 2012 год

Босна и Херцеговина

Подготвено од Александра Мартиновиќ и Срѓан Ного

Примери на мерки за заштита против ИТ злоупотреба

Во случај кога ИТ алатките му наштетуваат на угледот на поединците и институциите, тогаш таквите алатки и технологии стануваат форма на кривично дело. Во многу случаи, активностите на компјутерски криминал во БиХ тешко може да се докажат, а правните последици и казните за таквите дејства се слаби. За да може да се спречат таквите криминални активности, Босна и Херцеговина веќе презема чекори во борбата против компјутерскиот криминал преку спроведување на следните проекти:

- Централизиран систем за заштита на идентификација на граѓани (ИДДЕЕА),
- ПКИ инфраструктура (Закон за електронски потпис на БиХ),
- Централизиран чадор-систем на проекти на е-влада за размена на информации меѓу сите нивоа на владеење во БиХ,
- Проекти на Канцеларијата за реформи во јавната администрација (ПАРЦО) наменети за подобрување на јавната администрација.

Уште многу други активности и проекти се спроведуваат преку Europe Aid и други билатерални фондови кои значително помагаат во борбата против корупција.

Босна и Херцеговина ја потпиша “е-ЈИЕ Агендата за информатичко општество” во 2002 год. во Белград и стана членка на Електронска југо-источна Европа. Во агендата договорено е земјите членки да развијат и усвојат политика и стратегија за развој на информатичко општество на ЈИЕ, како и “Единствен информациски простор на ЈИЕ – Приоритетна област”, со што се дефинира начинот на формирање на јавната инфраструктура за безбедно работење врз основа на квалификуван електронски потпис.

“Законот за електронски потпис” и “Законот за електронски правен и деловен транспорт” беа донесени во 2006 год. Исто така, беа донесени одлуките со кои се уредува теренското користење на електронскиот потпис и сертификатите со цел да се обезбеди правната рамка за спроведување на дигиталниот потпис.

Примери на случај на заштитни мерки во Босна и Херцеговина

Ова е случај кој се однесува на Јавниот обвинител кој наводно ја хакирал електронската адреса на поранешниот Главен обвинител со цел да го дискредитира пред истиот да биде суспендиран од службената должност на Главен обвинител.

Технички мерки за заштита против недозволен пристап и злоупотреба на ИТ системите

Одговорните лица во правосудството на БиХ научија дека постоечките безбедносни мерки не беа доволни да спречат намерен незаконски пристап до компјутерскиот систем, имено пристап до службената електронска адреса на едно вработено лице. Така, правосудството на БиХ ги подобри безбедносните процедури на сите нивоа и го спроведе стандардот ISO / IEC 27001:2005.

Организациски и процедурални мерки за заштита, како што е ’принципот на повеќе очи’

И покрај тоа што сè беше спроведувано според законот, постоечките процедурални мерки за заштита беа недоволни и несоодветни да ја спречат грешката од човечки фактор како и слабата свест за безбедноста на луѓето кои го користат ИТ инфраструктурниот систем.

Следење на движењето на податоци и на пристапот на вработените до системите на податоци

Законите и процедурите во правосудството на БиХ предвидуваат следење на движењето на податоци и на пристапот на вработените до системите на податоци. Според внатрешните извештаи изготвени од различни судски органи, констатирано беше дека следењето е неопходна мерка на претпазливост и заштита против корупција и компјутерски криминал.

Обука и мерки за зголемување на свеста на државните службеници за ризиците од ИТ корупција и за мерките за заштита

Агенцијата за државни службеници на Босна и Херцеговина и слични агенции на ниво на ентитетите ги обучија своите државни службеници како да го намалат ризикот на конфликт на интерес во случај кога истиот ќе се појави и како да го зацврстат кодексот на однесување во јавната администрација на сите нивоа на владина администрација.

Агенцијата за спречување на корупција и координација на борбата против корупција е државна институција која, меѓу другото, е задолжена за развој и следење на образовната обука за спречување и борба против различните форми на корупција. Како резултат на недостиг на политичка волја за кадровско и целосно екипирање на Агенцијата, истата се соочува со недоволен капацитет за целосно да ги спроведе сите задачи предвидени со релевантните закони.

Контрола на ИТ системите

Агенцијата во моментов спроведува дополнителна контрола на ИТ системите со цел да спречи нивна злоупотреба во иднина.

Законски мерки за заштита

- Закон за електронски потпис
- Закон за електронско деловно работење
- Закон за електронски правен и деловен транспорт
- Закон за заштита на класифицирани информации

Случај 2 од Босна и Херцеговина: Уште едно контроверзно вработување во Државниот завод за ревизија на Република Српска

Случај на писмено тестирање на двајца помлади ревизори во Државниот завод за ревизија на Република Српска, каде податоците од тестот исчезнале и каде постои веројатност еден од кандидатите веќе да бил избран уште пред објавувањето на резултатите од тестот.

Технички мерки за заштита против недозволен пристап и злоупотреба на ИТ системи

Што се однесува до безбедносните мерки (технички мерки за заштита) за спречување на овој вид на проблеми во иднина, според изворите на Државниот завод за ревизија на Република Српска досега ништо не е преземено.

Организациски и процедурални мерки за заштита како што е 'принципот на повеќе очи'

Не само што беа евидентирани области во кои работењето се спроведуваше несоодветно согласно со одредбите од законот, туку некои од постоечките технички мерки за заштита, исто така, беа недоволни и несоодветни. Кандидатите наместо да ги полагаат тестовите користејќи безбеден софтвер тие ги пополнуваа тестовите во едноставен ворд формат без каква било заштита, така што секој член од надлежната комисија имал можност да прави измени на тестот. Понатаму, овој пат на кандидатите не им беше дозволено да направат копија од тестот на своите УСБ мемориски уреди и, исто така, овој пат тестовите не им беа вратени за да може да ги разгледаат.

Следење на движењето на податоци и на пристапот на вработените до системите на податоци

Од овој случај организацијата не научи ништо и не постои свесност дека следењето на движењето на податоци е неопходно како мерка за заштита.

Обука и мерки за зголемување на свеста на државните службеници за ризиците од ИТ корупција и за мерките за заштита

Агенцијата за државни службеници на Република Српска ги обучува своите државни службеници да го намалат ризикот од конфликт на интерес и да го зацврстат кодексот на однесување во јавната администрација на сите нивоа на владина администрација.

Контрола на ИТ системите

Организацијата потребно е да спроведе внатрешна контрола на ИТ системите што според законот претставува нејзина обврска.

Законски мерки за заштита

Нема податоци.

Случај 3 од Босна и Херцеговина: Злоупотреба на електронскиот систем на CIPS проектот

Проектот на Системот за заштита на идентификација на граѓани (CIPS) во Босна и Херцеговина започна да се спроведува во април 2002 год., кога на привремена основа беше формиран Директорат за неговото спроведување. Главната задача на проектот беше да создаде дел во системот преку кој Законот за централен регистар и размена на податоци ќе може да се спроведува. Уште од најраната фаза на проектот CIPS, беа регистрирани голем број на жалби во однос на злоупотреба на електронскиот систем, посебно при издавањето на лични карти и патни исправи ширум земјата.

Технички мерки за заштита против недозволен пристап и злоупотреба на ИТ системи

Во периодот од 2012 до 2015 год, IDDEEA ги спроведе следните стандарди: ISO/27001:2005 и ISO/90001:2008 (со нивните закажани ревизии[50]).

Се воспостави Систем за управување со документи (ДМС) на IDDEEA кој се користи за чување на податоците на институциите на ниво на држава и ентитет, како и на податоците на агенциите чии барања треба да бидат усогласени со мошне високите стандарди за ИТ сигурност и безбедност.

Организациски и процедурални мерки за заштита, како што е 'принципот на повеќе очи'

- Да се продолжи со спроведување на поважните стандарди и редовно да се користи службата за контрола согласно со правилата и законодавството на ЕУ, со посебен осврт на стандардите ISO 9001 за управување на квалитет.

- Проверка на безбедноста на вработените спроведена од страна на надлежните органи (Службата за разузнавање и безбедност на БиХ) која обезбедува избегнување на прекршувања на ИТ безбедноста и која прибира лични податоци за целокупниот ангажиран персонал со цел да се направи социјален профил за идна употреба.

Следење на движењето на податоци и на пристапот на вработените до системите на податоци

Во однос на инфраструктурата, институциите за безбедност при пренос на податоци во БиХ имаат воспоставено високософистицирана комуникациска мрежа преку СДХ технологијата (Синхрона дигитална хиерархија) која овозможува брзо, сигурно и ефикасно споделување на податоци, слики и звук. СДХ мрежата претставува затворен систем кој не е поврзан на интернет и кој работи на конкретен опсег на фреквенции покриени за таа цел. Институцијата која ја одржува техничката СДХ мрежа, Агенцијата за документи за лична идентификација, евиденција и размена на податоци (IDDEEA) е задолжена за документите за лична идентификација, нивно чување, персонализација и транспорт, како и за централно чување на евиденцијата и размената на информации меѓу надлежните органи во Босна и Херцеговина.

IDDEEA[51] го следи, координира и уредува институционалното поле на документите за лична идентификација, и како таква има развиено електронски потпис во затворен систем. Искуството на Агенцијата во однос на примената на електронскиот потпис во затворен систем е важно за спроведување на Законот за електронски потпис на БиХ и општо за отворените системи.

Клучни проблеми се:

- Недостиг на институционална поставеност неопходна за координирање на активностите во областа на услугите на е-влада (кои се спроведуваат на различни нивоа и од различни министерства),
- Нерационално користење (несоодветна дистрибуција) на ИТ персоналот,
- Несоодветна примена на политиката и законската рамка на информатичко комуникациските технологии од страна на владините органи на ниво на држава и ентитет, и
- Неуспешно спроведување на упатствата на IDDEEA.

Обука и мерки за зголемување на свесноста на државните службеници за ризиците од ИТ корупција и за мерките за заштита

Агенцијата за државни службеници на БиХ и слични агенции на ниво на ентитет организираат обука за своите државни службеници за намалување на ризикот од конфликт на интерес и за зацврстување на кодексот на однесување во јавната администрација на сите владини административни нивоа.

IDDEEA има спроведено платформа на е-учење за континуирано образование и подобрување на вештините на нејзиниот персонал кои се неопходни за постигнување на највисоките стандарди на ефективност и професионализам.

Агенцијата за спречување на корупција и координација на борбата против корупција е државна институција која, исто така, е задолжена за развој и следење на образовната обука за спречување и борба против различните форми на корупција. Како резултат на недостиг на политичка волја за кадровско и целосно екипирање на Агенцијата, истата има недоволен капацитет за целосно спроведување на задачите предвидени со правосилните закони.

Контрола на ИТ системите

Формирано е Одделение за внатрешна контрола за ИТ информатичките системи со цел спречување на злоупотреба на ИТ системите.

50 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemi d=214&lang=en
51 http://www.iddeea.gov.ba/images/stories/PDF/law_on_agency_final.pdf

Законски мерки за заштита

- Законот за заштита на лицата кои пријавуваат корупција во институциите на Босна и Херцеговина (“Службен весник на Босна и Херцеговина” бр. 100/13)
- Закон за администрација (“Службен весник на Босна и Херцеговина” бр. 32/02 and 102/09),
- “Упатства” на Агенцијата за документи за лична идентификација, евиденција и размена на податоци на Босна и Херцеговина за поднесување внатрешни извештаи за сомневање или загриженост за корупција на вработени, издадени на 31 март 2014 год.

Мерки против ИТ корупција во рамките на борбата против корупција во Босна и Херцеговина

Сите правосилни домашни и меѓународни извештаи за состојбите на корупција во БиХ укажуваат дека корупцијата е меѓу најголемите проблеми со кои се соочува општеството, како и најголема пречка за различните реформи и за целокупниот економски и социјален напредок. Последниот извештај на ЕУ за постигнатиот напредок на БиХ повторно укажува дека земјата се наоѓа во рана фаза на борбата против корупција[52]. Понатаму, клучните антикорупциски закони изменети се на начин на кој се поткопуваат претходните постигнувања. Корупцијата останува широко распространета, со недоволно досие на истрага и гонење на случаи од висок профил.

Судски систем

Во 2013 год. Високиот судски и обвинителен совет (HJPC) превзема низа мерки и конкретни акции за обезбедување попрофесионално и поквалитетно работење на обвинителите. Случајот 1, опишан во поглавје 1, според наше уверување придонесе кон брза автоматизација и професионализација на овој систем.

Знаењето, вештините и разбирањето на тековните проблеми и на важноста на работата на обвинителството се зголемија преку посебниот ангажман на проектот „Зацврстување на капацитетот на обвинителите во кривичниот судски систем” во сферата на образованието. Овие цели се постигнаа преку развивање на наставни програми, организирање на голем број на образовни стратегии, преку соработка со JPTC (Центарот за обука на судството и обвинителството) со цел да се подобри тековниот модел на образование за обвинители, како и да се управува со мрежите на сите чинители во кривичната истрага во образовниот процес. Во рамките на овој процес повеќе од 150 обвинители го унапредија своето знаење во следниве области:

52 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

- кривична постапка против правни лица,
- имунитет на сведоци,
- учење и вештини на истражување,
- посебни истраги,
- компјутерски криминал,
- перење на пари и финансиски истраги,
- недозволена трговија, и
- комуникациски вештини и методологии.

Во однос на погоре наведеното укажавме на голем број на релевантни факти во однос на законодавството и покажавме дека почитувањето на правната рамка во голема мера може да го спречи овој тип на криминал и корупција.

Во дополнение на редовните ревизии, за време на 2013 год. Државниот завод за ревизија на БиХ (SAI BiH) ја спроведе ревизијата на работата насловена “Телекомуникациски решенија во институциите на Босна и Херцеговина”. Извештајот од спроведената ревизија ги нагласи позитивните примери на Високиот судски и обвинителен совет, кој потрошил значително помала сума за интернет услуги, споредено со други институции од ревизорскиот примерок и покрај тоа што Советот имал значително поголем број на корисници.

Зголемената безбедност на судскиот информатички системи на БиХ продолжува да биде еден од стратешките приоритети на земјата како што е посочено во Стратегијата за реформи на судскиот систем во БиХ 2014-2018 година[53]. Исто така, Високиот судски и обвинителен совет ги даде следниве препораки: капиталните инвестиции во правосудството да вклучат замена на застарените компјутери и да се спроведе набавка на компјутерска опрема која во моментот недостасува; надградба на информатичките системи во правосудниот систем; одржување на постоечката опрема и лиценците за софтвер; и обука на ИТ персоналот и другите вработени во судството.

Во рамките на овој процес беше обезбедена компјутеризација на судството и систем на електронска размена на податоци меѓу полициските служби и обвинителствата, кој официјално започна со работа во јуни 2013 год. Обвинителите во обвинителствата ширум земјата сега имаат можност да ги следат електронските записи под јурисдикција на полициските служби согласно со важечката законска рамка. Понатаму, полициските служби имаат можност да го следат статусот на кривичните пријави кои полицијата ги има доставено до обвинителството, а кои се чуваат во нивниот систем за автоматско управување со случаи (TCMS). Системот беше воспоставен согласно со Спогодбата склучена меѓу Високиот судски и обвинителен совет, Министерството за безбедност на БиХ, Државната агенција за истрага и заштита, Граничната полиција и Министерствата за внатрешни работи на сите нивоа на влада. “Поддршка на правосудството на Босна и Херцеговина” (ИПА 2009) и ИПА проектот

53 http://www.mpr.gov.ba/aktuelnosti/propisi/konsultacije/SRSP%20u%20BiH.pdf

“Поддршка на реформите во полицијата” беа двата главни проекти кои резултираа со воспоставувањето на овој систем.

За да може да одговори на растечките потреби на системот, посебно во однос на новиот автоматски систем за управување на случај во судовите и обвинителствата (CMS/TCMS) и за да обезбеди усогласеност на софтверските решенија со актуелните софтверски стандарди, процесот на надградба на сите хардверски и софтверски компоненти на системот на информатичко комуникациски технологии (оптимизирање и консолидација на системот на ИКТ во правосудството на БиХ) продолжи да се одвива во 2013 год. Овој процес се спроведува со цел:

- Колку што е можно повеќе да го намали времето на застој на системот предизвикано од застареност на ИТ опремата и софтверот;
- Да обезбеди најдобро искористување на постоечките капацитети на серверот и мрежата во центрите на податоци на Високиот судски и обвинителен совет;
- Да овозможи нормално работење за корисниците на судскиот систем и лесен пристап до електронските услуги во правосудството, кои се јавно достапни преку интернет;
- Да ја подобри безбедноста на податоците зачувани во базите на податоци на информатичките системи на правосудството; и
- Да ги обезбеди техничките услови неопходни за непречена размена на податоците со надворешните системи (полиција, даночни и други владини електронски регистри), што е од суштинска важност за борбата против корупција и организиран криминал.

Во рамките на овој проект, персоналот од Секторот за информатичко комуникациски технологии на Високиот судски и обвинителен совет спроведе надградба на системот за управување со дигиталните идентитети, како и на системот за електронска пошта во центрите за податоци за обработка и чување на податоци во Високиот судски и обвинителен совет.

Сите овие мерки се нотирани во последниот извештај на ЕУ за напредокот на БиХ. Извештајот нагласува дека информатичко комуникацискиот систем во правосудството е целосно функционален. Системот за управување со случај/автоматскиот систем за управување со случај вклучува повеќе од 3.4 милиони регистрирани случаи, и произведува автоматски извештаи за работата на правосудството, што придонесува кон одлуките за планирање на политиката и стратегиите. Пристапот до веб порталот на правосудството значително се зголеми, како и пристапот на странките и нивните правни застапници до информациите за случајот кој е во судска постапка. Центарот за документација во правосудството, исто така, има забележано значителен пораст на интернет посетите.

Центарот за обука на судството и обвинителството на двата ентитети обезбедува обука за правосудството. Во напор да го подобри и зголеми својот капацитет, двата центри воведоа учење на далечина[54].

Полиција

Како што потврдува Извештајот на ЕУ од 2013 год. за напредокот на Босна и Херцеговина, агенциите и одборите кои се формираа согласнозаконите за реформите во полицијата сè уште ги консолидираат своите функци[55].

Меѓуагенциски тим за следење го надгледуваше спроведувањето на електронскиот систем за размена на податоци во полицијата, а се формираа и регистри во обвинителствата. Некои од техничките аспекти на системот треба дополнително да се разгледаат, вклучувајќи го и фактот дека директоратот за координација на полициските органи сè уште нема пристап до базите на податоци во системот. Европол спроведе целосна ревизија за заштита на податоците.

Агенцијата за поддршка на полицијата е лоцирана на исто место со Директоратот за координација на полициските органи и истата го донесе Правилникот за стандардизација на опрема во полицијата.

Измените на Законот за полициски службеници се очекува да бидат усвоени на државно ниво. Федерацијата на Босна и Херцеговина, кантоните и дистриктот Брчко започнаа иницијативи за усогласување на соодветното законодавство. Измените се однесуваат на технички и оперативни прашања, како што се употреба на оружје и полициски овластувања и засилена заштита на личните податоци[56].

Законот на БиХ[57] го препознава компјутерскиот криминал како форма на криминално однесување при што компјутерската технологија и информатичките системи се користат како алатка или мета за спроведување кривично-правни дејства со соодветни последици.

Основни карактеристики или обележја на компјутерскиот криминал се:

- Социјално опасно и незаконско поведение за кое законот предвидува кривични санкции;
- Посебен начин и средства за извршување на кривично дело со или преку компјутер;

54 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf
55 Процесот на опсежни реформи во полицијата во БиХ, кој започна после граѓанската војна, вклучуваше формирање на неколку важни институции на државно ниво, како: Државна гранична полиција, Служба за надворешни работи на БиХ во рамките на Министерството за безбедност на БиХ, Државната агенција за истрага и заштита (SIPA), Директорат за координација на полициските органи на БиХ, итн
56 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf
57 Кривичен законик на Федерацијата на Босна и Херцеговина - член 393 до 398

- Посебен предмет на заштита, безбедност на компјутерските податоци или информатичките системи во целост или неговите поединечни сегменти; и
- Намерата на сторителот или на некое друго лице на овој начин да стекне корист од таквата штета[58].

Кривични дела поврзани со компјутер и интернет[59]:

- Компјутерски фалсификат
- Компјутерска измама
- Детска порнографија
- Повреда на интелектуалната сопственост

Недозволен пристап:

- Намерен незаконски пристап до компјутерски систем
- Нанесување штета на компјутерските системи и податоци
- Компромитирање на доверливи податоци

Злоупотреба на уреди:

- Намерно и неовластено производство, продажба, набавка и дистрибуција
- Уреди за пристап (вклучувајќи и компјутерски програми)
- Лозинка на компјутер
- CODE
- Други видови информации за пристап при нарачување дејства на компјутерски криминал.

Неовластено следење на податоци:

- Намерно незаконско следење на податоци преку компјутерски систем.
- Заштита на приватноста на нејавни преноси на компјутерски податоци преку следење и снимање.

Попречување на податоците:

- Намерно неовластено оштетување, бришење, уништување, менување на податоци или на неупотребливи компјутерски податоци
- Вметнување на малициозни кодови кои претставуваат закана за интегритетот и можноста за користење на податоци и програми
- Вируси кои се вмрежуваат во податоците

58 http://www.fup.gov.ba/?p = 1697 – Федерална полициска администрација
59 http://www.rs.cest.gov.ba/

Дефинитивно постојат законски мерки за гонење на вакви и слични случаи поврзани со корупција на информатичката технологија, без оглед дали се работи за кражба на податоци или “слушање” на податоците со цел “слушнатите” информации да се споделат со заинтересираните страни.

ИТ системите и внатрешните процедури кои се однесуваат на Системот за управување со документи, Архива, случаи на обвинителство и други релевантни документи и материјали, вклучувајќи го и персоналот кој работи на овие системи се предмет на редовна инспекција од страна на надлежните органи. Во некои институции ова е дефинирано преку внатрешните процедури зависно од профилот на институции. Во овој случај, клучното нешто е спроведувањето на ISO / IEC 27001:2005, со цел да се обезбеди задоволително ниво на безбедност на податоците.

Што да се направи

Да се продолжи со спроведување на поважните стандарди и со редовна контрола согласно со правилата и законодавството на ЕУ, со посебен осврт на стадардите ISO 9001 за управување со квалитет ISO/27001:2005 и ISO/90001:2008.

Да се продолжи со проверка на безбедноста на вработените од страна на надлежните органи со цел избегнување на повреди на ИТ безбедноста и прибирање на лични податоци за сите тековно и идно ангажирани лица со кои ќе послужат за изработка на социјален профил за идна употреба.

Борба против организираниот криминал и тероризам

Слабоста во системското прибирање, анализа и користење на разузнавачки информации од страна на органите за спроведување на законот го спречува стратешкото целење кон организирани криминални групи и активности. Меѓу органите за спроведување на законот не постои системска размена на разузнавачки податоци за целите на заедничко оперативно планирање.

Подготвени се измени на Државниот закон за кривична постапка со цел да се обезбеди поефективно спроведување на посебните истражни мерки, но сè уште не се усвоени.

Во сферата на судска соработка во кривични предмети, подготовките за склучување спогодба со Eurojust сè уште се во рана фаза, но покажуваат напредок. Оценувањето на заштитата на податоци е завршено. Се очекува да се усвојат измените на Законот за заштита на класифицирани информации преку кои законот ќе се усогласи со правосилните стандарди на ЕУ и ќе се обезбеди спроведување на билатералните договори за безбедност.

Компјутерски криминал

Извештајот на Европската комисија од 2013 год. за напредокот на Босна и Херцеговина го нагласува отсуството на стратегија и институции за борба против компјутерски криминал и закани:

„Босна и Херцеговина нема воспоставено ниту стратегија ниту институции кои ќе се осврнат на прашањето на компјутерски криминал и заканите за компјутерската безбедност.. Советот на Министри се уште не го усвоил акцискиот план за воспоставување на Bosnia and Herzegovina Computer Emergency Response/ Readiness Team (CERT – Тим за одговор на компјутерски инциденти). Преземени се активности за воспоставување на CERT. Извештаите за кривични дела кои се подготвуваат од органите за спроведување на законот на Босна и Херцеговина не се однесуваат на компјутерски криминал. Тие не даваат точни податоци за бројот на случаи, истраги или осомничени. Дигиталната форензика и другите технички средства за борба против компјутерскиот криминал на државно и меѓународно ниво се ограничени и недоволни. Дирекцијата за координација на полициските тела е одредена како постојано достапна точка за контакт 24 часа сите седум дена во согласност со Конвенцијата за компјутерски криминал (Конвенција од Будимпешта), но за тоа недостасуваат потребните капацитети"[60].

ДРУГИ МЕРКИ

Размена на податоци меѓу јавните тела

Со проектот "Поддршка на судството во Босна и Херцеговина" (ИПА 2009) и ИПА Проектот "Поддршка на реформите во полицијата" кој започна во 2013 год., со добро утврден процес на имплементација и согласно со договорот со кој се воспостави систем за електронска размена на податоци меѓу полициските служби и обвинителите, - склучен помеѓу Високиот судски и обвинителен совет, Министерството за безбедност на БиХ, Граничната полиција, Државната агенција за истрага и заштита (SIPA) и Министерството за внатрешни работи, Високиот судски и обвинителен совет започна активности кои се очекува да доведат до нова генерација на размена на податоци во БиХ. Во текот на овој процес, погоре споменатите стандарди треба да се спроведат, а системите на податоци да се "ажурираат" со цел да се избегнат примерите на корупција наведени во оваа студија. За да може да се постигне ова, во рамките на овој систем ќе се спроведат алатки и мерки за заштита кои вклучуваат: огнени ѕидови (firewalls), Системи за упатување, откривање и спречување (Intrusion Detection and Prevention Systems (IDS)), тестирање на пробив и скенирање на ранливост (Penetration Testing and Vulnerability Scanning), процедури за пренос на чувствителни податоци, процедури и правила за екстерни системски поврзувања (External System Connections), антивирусни и про-одбранбени алатки, далечинска контрола на пристап, процедури и контрола за влез и излез во просториите, двојна заштита на податоци на оддалечена локација во комбинација со силна лозинка и физичка безбедност, како и постојана обука на вработените за информатичките технологии.

Агенцијата за документи за идентификација, евиденција и размена на податоци на БиХ, претходно Систем за заштита на идентификација на граѓаните (CIPS)[61], претставува добар пример за спроведување на мерките за заштита и безбедност. Сепак, додека на државно ниво агенцијата е добро организирана, за жал, на ниво на локална власт постојат злоупотреби.

Што беше научено од злоупотребата на електронскиот систем на проектот CIPS

Во периодот од 2012 до 2015 год. се спроведуваат стандардите ISO/27001:2005 и ISO/90001:2008 со закажани ревизии[62]. Нивниот Систем за управување со документи, Регистарот на граѓански податоци, и внатрешната средина Oracle, која се користи за чување на податоци во институции и агенции на сите нивоа, е сигурен и безбеден. Проблемот во овој случај, како што е опишано во поглавје 1, е дека надлежните власти (Федерацијата на БиХ преку кантонските Министерства за внатрешни работи, Министерството за внатрешни работи на Република Српска, и надлежните власти, кои функционално делуваат како државни институции на дистриктот Брчко) со строги процедури на работа со податоци, кои истовремено ги дополнуваат, бришат и ажурираат личните податоци на граѓаните.

Надлежните органи, согласно со законот, се сопственици на нивните податоци, а улогата на IDDEEA во овој процес е да ги чува и обезбедува податоците, како и да ги примени сите познати мерки за заштита и добри пракси на безбедност[63]. Со оглед на тоа што ова претставува фактичка ситуација, потребно е да ја споделиме одговорноста за таквите случаи меѓу полициските администрации на БиХ и надлежните органи задолжени за други слични случаи, доколку такви постојат. Ова значи дека нивните стандарди, процедури и општ начин на справување со такви проблеми не се прифатливи.

IDDEEA има обезбедено целосна безбедност на сите нивоа на заштита на податоци за надлежните полициски агенции и надлежните органи во Босна и Херцеговина. Така, корупцијата и злоупотребата на информатичките технологии треба да се бара на сите нивоа на надлежни органи, при што државата треба да ја обезбеди и подобри безбедноста на информациите.

60 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

61 www.iddeea.gov.ba
62 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemi d=214&lang=en
63 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=105&Itemi d=97&lang=en

IDDEEA спроведе дигитален потпис за сите канали на комуникација во Агенцијата, како и за целите на надворешна комуникација со надлежните органи.

Сепак, она што недостасува е Тимот за одговор на компјутерски инциденти[64] (CERT). И покрај тоа што се очекува да се изготви акциски план за CERT[65], истиот сè уште не е развиен.

Електронски потпис

Техничкиот опис на Јавната клучна инфраструктура (PKI)[66] е да развие ниво на безбедност на размената на податоци во примарната техничка компонента на државно ниво. Тоа може да биде или централна инфраструктура со единствен орган за издавање на сертификати и подредени тела кои издаваат сертификати за електронски потпис или независна инфраструктура на ниво на интероперабилност.

Во Босна и Херцеговина не постои PKI за фирми и поединци на државно ниво. Сепак, постојат голем број на независни корисници на PKI, посебно во рамките на електронското банкарство и делумно на полето на е-влада кои работат во затворени системи. Така, техничкиот проблем не се однесува толку многу на отсуството на PKI на државно ниво колку што се однесува на приближување и спојување на разните постоечки PKI и информатички системи. Поврзувањето на разните PKI би го олеснило процесот на делување и работа во јавната администрација.

Безбедноста би била засилена со тоа што сите учесници на електронската размена на податоци или обичните граѓани имаат свој идентитет во овој систем. Ова ја намалува можноста за злоупотреба и овозможува постојано следење на дејствата на луѓето. Сите системи кои се интегрирани во PKI и кои ефективно создаваат еден голем систем значително ја намалуваат можноста за злоупотреба.

ЗАКОНСКА РАМКА

Директива 1999/93/ЕС за рамката на Заедницата за електронски потпис

Оваа Директива ја воспоставува правната рамка за електронски потпис и сертификација на услуги на европско ниво. Целта е да се олесни користењето на електронскиот потпис и да му се помогне на истиот да стане правно признаен во земјите членки.

64 http://www.msb.gov.ba/docs/Strategija_za_CERT.doc
65 http://www.us-cert.gov/
66 http://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx

Одлука на Комисијата 2003/511/ЕС од 14 јули 2003 год. за објавување на референтни броеви кои се општо прифатени стандарди за производи на електронски потпис согласно со Директивата 1999/93/ЕС

Со оваа одлука на Европската комисија Босна и Херцеговина се потпира врз три широко прифатени стандарди на производи на електронски потпис кои предвидуваат почитување на квалификуваниот електронски потпис.

Одлука на Комисијата 2000/709/ЕС – ноември 2000 год.

Според членот 3 (4) на Директивата 1999/93/ЕС на Европскиот парламент и на Советот на Заедницата за електронски потпис, оваа одлука ги поставува критериумите кои земјата членка мора да ги земе предвид при одредување на состојбата на органот кој ќе го поддржи уредот за оценување на усогласеноста при создавање на безбеден потпис.

Правна рамка на БиХ

На државно ниво (БиХ), во моментот на сила се следниве законски акти:

- Закон за електронски потпис (“Службен весник на БиХ”, бр. 91/06)
- Закон за електронски правни и деловни операции (“Службен весник на БиХ”, бр. 88/07)
- Закон за управна постапка (“Службен весник” бр.: 29/02, 12/04, 88/07, 93/09)
- Одлука за основата за користење електронски потпис и обезбедување потврда (“Службен весник на БиХ”, бр. 21/09)
- Одлука за е-трговија и е-влада (“Службен весник” бр. 07/10)
- Одлука за канцелариско работење на министерствата, одделенијата, институциите и другите тела на Советот на Министри (“Службен весник на БиХ” бр. 21/01, 29/03)
- Упатства за подготовка и одржување на службената веб страница на институциите на БиХ (“Службен весник на Босна и Херцеговина” бр. 21/09)
- Закон за заштита на лица кои пријавуваат корупција во институциите на Босна и Херцеговина (“Службен весник на Босна и Херцеговина” бр. 100/13)
- Закон за агенцијата за спречување на корпуција и координација на борбата против корупција (“Службен весник на Босна и Херцеговина ”, декември 2009 год.).

Понатаму, во моментот во подготовка се следниве законски акти:

- Регулатива за внатрешната организација на Министерството за транспорт и врски (формирање на Канцеларија за надзор и акредитација)

- Високиот судски и обвинителен совет (HJPC) им препорачува на извршните власти на БиХ дека Министерството за транспорт и врски треба да ги спроведе правосилните подзаконски акти и да формира институционален капацитет со цел да овозможи целосно спроведување на Законот за електронски потпис и Законот за електронско деловно работење во судскиот информатички систем што првенствено се одразува во можноста за доставување претставки до судот во електронска форма, како и испорака на судските одлуки по електрински пат (оверено од квалифуван дигитален сертификат)[67].

Јавна набавка

Законот за јавна набавка на Босна и Херцеговина[68] на единствен начин ги вклучува сите договорни страни согласно со Директивата на ЕУ 17/2004 и Директивата 18/2004. Посебните ЕУ правила за јавна набавка се уредуваат преку серија детални директиви со кои се утврдуваат сеопфатните барања за регулирање на постапките за јавни набавки. Во Босна и Херцеговина постојат недоволни конкретни регулативи кои ја дефинираат оваа област согласно со регулативите на ЕУ.

Решението за надминување на недостатоците во системот за јавни набавки би можело да биде на едно тело да му се овозможи да го спроведува процесот на набавки за сите надлежни органи. Ова тело, по претходно спроведен преглед на ИТ и корупција, би поседувало единствен и централизиран софтвер развиен во согласност со Законот за јавни набавки на Босна и Херцеговина и би ги разгледувало потребите на сите нивоа на власт, овозможувајќи ú на власта на тој начин да ги спроведува сите јавни набавки.

Се разбира, предуслов би било да се воведат стандарди и да се обезбеди познавање на пазарот од страна на вработените во однос на ажурирани информации и контакт со добавувачите на опрема. Ова е потребно со цел да се обезбеди купување на само неопходните стоки и услуги, а таквите производи ќе бидат најдобрите меѓу оние кои се на располагање.

67 http://www.hjpc.ba/intro/gizvjestaj/?cid=5889,2,133 http://www.ohr.int/ohr-dept/le- gal/laws-of-bih/police.asp
68 https://www.parlament.ba/sadrzaj/zakonodavstvo/usvojeni/default. aspx?id=46717&langTag=bs-BA&pril=b

Хрватска

Подготвено од Зорислав Петровиќ и Ивана Андријашевиќ

Главната законска рамка за информациска безбедност

Законската рамка за обезбедување на информациска безбедност во информатичките системи на јавната администрација во Република Хрватска се потпира врз следниве најважни закони и подзаконски акти: Закон за информациска безбедност; Закон за тајност на податоците; Закон за заштита на личните податоци; Закон за системот на безбедност и разузнавање; Закон за електронски документи; Закон за електронски потпис; Закон за проверка на безбедноста; Регулатива на мерките за информациска безбедност; Регулатива за содржината, формата, доставувањето и ракувањето со прашалникот за проверка на безбедноста; и Уредба за критериумите за позицијата Советник за информациска безбедност.

Законот за информациска безбедност (Службен весник бр. 79/07) го утврдува концептот на безбедност на информации; мерки и стандарди за безбедност на информациите; области на безбедност на информациите; и надлежни органи за усвојување, спроведување и надзор на мерките и стандардите за безбедност на информациите. Овој Закон се применува на државните органи; на единиците на локална и регионална самоуправа и на правни лица со јавни овластувања кои во опсегот на своето работење користат класифицирани и некласифицирани податоци; како и правни и физички лица кои имаат пристап или раководат со класифицирани и некласифицирани податоци.

Законот за тајност на податоците (Службен весник, бр. 79/07, 86/12) го утврдува концептот на класифицирани и некласифицирани информации; степенот на тајност; постапката за класифиација и декласификација; пристап до класифицирани и некласифицирани информации; заштита на класифицирани и некласифицирани информации; и надзор врз спроведувањето на овој Закон. Законот се применува на државните органи; на единиците на локална и регионална самоуправа; правни лица со јавни овластувања; и правни и физички лица кои согласно со овој Закон имаат пристап или раководат со класифицирани и некласифицирани информации.

Законот за заштита на лични податоци (Службен весник, бр. 103/03, 118/06, 41/08, 130/11, 106/12) ја уредува заштитата на лични податоци во однос на физички лица и надзорот на прибирање, обработка и употреба на личните податоци во Република Хрватска. Неговата цел е да ја заштити приватноста на поединецот, како и човечките права и фундаментални слободи во собирањето, обработката и употребата на личните податоци.

Законот за систем за безбедност и разузнавање на Република Хрватска (Службен весник, бр. 85/08, 86/12) се утврдува за целта на системското прибирање, анализа,

обработка и проценка на информациите важни за државната безбедност, со цел за откривање и спречување на активности на поединци или групи насочени против одржливоста, независноста, интегритетот и суверенитетот на Република Хрватска; кои имаат за цел на насилен начин да ги урнат структурите на државната власт; кои се закануваат да ги повредат човековите права и основни слободи утврдени со Уставот и законите на Република Хрватска; да ги загрозат фундаментите на економскиот систем на Република Хрватска, неопходни за донесување релевантни одлуки за успешно постигнување на националните интереси на полето на државната безбедност, посебно заштитата на двете агенции за безбедност и разузнавање: Агенцијата за безбедност и разузнавање (SOA) и Агенцијата за воена безбедност и разузнавање(VSOA).

Законот за електронски документи (Службен весник, бр. 150/05) го уредува правото на физичките и правни лица за користење на електронски документи во сите деловни дејства и активности, како и во постапките кои се водат пред јавните власти во кои електронската опрема и програми може да се применат во создавањето, преносот, складирањето и чувањето на информации во електронска форма, правосилната важност на електронскиот документ и употребата и движењето на електронски документи.

Законот за електронски потпис (Службен весник бр. 10/02, 80/08, 30/14) го уредува правото на физичките и правните лица за користење на електронски потпис во административните, трговските и останатите оперативи, и правото, обврските и одговорноста на физичките и правните лица поврзано со обезбедување на услуги за потврда на електронскиот потпис.

Законот за проверка на безбедноста (Службен весник, бр. 85/08, 86/12) ги утврдува дефиницијата, видот и степенот на проверка на безбедноста, безбедносните пречки и постапките за спроведување на проверка на безбедноста. Согласно со овој закон, проверката е процедура со која надлежните органи го потврдуваат постоењето на безбедносните пречки за физичките и правни лица.

Регулатива за мерките за информациска безбедност (Службен весник, бр. 46/08) ги утврдува мерките за безбедност на информациите предвидени за ракување со класифицирани и некласифицирани информации. Овој закон се применува на државните органи; единиците за локална и регионална самоуправа; и правните лица со јавни овластувања кои во опсегот на своето работење користат класифицирани и некласифицирани информации; како и физички и правни лица кои имаат пристап или кои ракуваат со класифицирани и некласифицирани информации.

Регулатива за содржината, формата, доставувањето и ракувањето со прашалникот за проверка на безбедноста (Службен весник, бр. 114/08) ја уредува содржината, формата, доставувањето и ракувањето со Прашалникот за проверка на безбедноста за физички и правни лица.

Уредбата за критериумите за позицијата Советник за информациска безбедност (Службен весник, бр. 100/08, 30/11) ги утврдува критериумите за позицијата советник за информациска безбедност. Освен споменатите регулативи, постојат голем број закони и подзаконски акти кои само делумно го разгледуваат прашањето на безбедност на информациите, како што се Законот за електронска трговија; Кривичниот законик; Законот за Архива; Законот за безбедност и заштита итн. Конечно, важно е да се напомене дека како земја членка на НАТО и ЕУ, Хрватска ги хармонизира своите регулативи на полето на информациска безбедност со останатите земји членки на НАТО и ЕУ.

Централни државни органи надлежни за информациска безбедност

Централни државни органи надлежни за информациската безбедност во Хрватска се:

- **Канцеларијата на Советот за државна безбедност**: централниот државен орган кој е одговорен за информациската безбедност го координира и усогласува усвојувањето и спроведувањето на мерките и стандардите за безбедност на информациите во Република Хрватска, и за размена на класифицирани и некласифицирани информации помеѓу Република Хрватска и странски земји и организации (член 14 од Законот за информациска безбедност);
- **Биро за безбедност на информатичките системи**: централен државен орган за техничките области на безбедноста на информатичките системи кај физички и правни лица. Ова се однесува на: стандарди за безбедност на информатичките системи; акредитации за безбедност на информатичките системи; управување со криптирани материјали кои се користат при размена на класифицирани информации; и координација на спречување и одговор на заканите по безбедноста на информатичките системи (член 17 од Законот за информациска безбедност); и
- **Национален CERT**: државен орган одговорен за спречување и заштита од компјутерски закани за јавните информатички системи во Република Хрватска кои работат во рамките на Хрватската академска и истражувачка мрежа (CARNet) – главниот интернет столб за државните сектори во Хрватска. Неговата главна задача е обработка на инцидентите на интернет; односно зачувување на информациската безбедноста во Хрватска. Државниот CERT спроведува проактивни и реактивни мерки во рамките на своите можности со цел да спречи или да ја ублажи евентуалната штета. Корисниците на националниот CERT сите се корисници на интернет во Република Хрватска и обезбедувачи на хостинг услуги и Даватели на интернет услуги (ISP)[69].

69 http://www.carnet.hr/ncd

Општо за безбедноста на информатичките системи

Законот за информациска безбедност дефинира пет области на информациска безбедност за кои се предвидени мерки и стандарди за безбедност на информациите: Проверка на безбедноста; физичка безбедност; безбедност на информациите; безбедност на информатичките системи; и безбедност на деловната соработка.

Областа на безбедност на информациите која е важна за оваа студија е безбедноста на информатичките системи. Според став 1, член 12 од Законот за информациска безбедност, безбедноста на информатичките системи "е област на безбедност на информациите во рамките на која се утврдуваат мерки и стандарди за безбедност на информациите при обработка, чување и пренос на класифицирани и некласифицирани информации во информатичките системи и за заштита и достапност на информатичките системи во процесот на планирање, дизајн, изработка, користење и престанок на работа на информатичките системи''. Понатаму, според истиот член, "акредитација на безбедноста на информатичките системи ќе се спроведе за оној информатички системи во кој се користат податоци класифицирани како ДОВЕРЛИВИ, ТАЈНИ и СТРОГО ДОВЕРЛИВИ. Лицата кои земаат учество во процесот посочен во ставот 1 од овој член мора да имаат сертификат на ниво на СТРОГО ДОВЕРЛИВО или едно ниво повисоко од највисокото ниво на класифицирана информација која се обработува, чува и пренесува во информатичките системи кои се во нивна надлежност. Мерките за физичка заштита на објектите во кои се сместени информатичките системи ќе бидат преземени во согласност со највисокото ниво на класифицирана информација која се обработува, чува или пренесува во наведениот објект". Конечно, "централните државни органи кои се надлежни за безбедност на информациите ќе формираат регистар на сертифицирана опрема и машини кои се користат во информатичките системи на ДОВЕРЛИВО, ТАЈНО и СТРОГО ДОВЕРЛИВО ниво. Регистарот на сертифицирана опрема и машини ќе се формира врз основа на преземање на соодветните регистри на меѓународните организации или преку сопствен процес на издавање сертификат во согласност со меѓународните стандарди''.

Мерките за безбедност на информациите во областа на безбедност на информатичките системи, кои се предвидени со Регулативата за мерки за информациска безбедност, се:

- Мерки за заштита на информатичките системи (заштита на хардверот, софтверот и медиумите за чување на податоци, управувањето со системската конфигурација и пристапот за корисниците, контрола на интерконекција на системите итн.);
- Свесност за безбедност (поставување на правила за безбедност на вработените и обука за безбедност); и
- Планирање на процедури за вонредни ситуации (развој на процедури за следење на случаи на инцидент; управување со континуитет на работа).

Безбедноста на информатичките системи се спроведува ширум целиот животен циклус на информатичките системи (преку безбедносна акредитација) и некласифицирани (прилагодување на стандардите HRN ISO/IEC 27001 и HRN ISO/IEC 17799) системи[70].

Примери на случај на ИТ безбедносните мерки за заштита во Хрватска

Случај 1 од Хрватска: Јави му се на лекарот за гласови

Ова е случај во кој доктор извлекувал податоци од болничкиот систем. Според информациите од јавно достапниот Централен регистар кој содржи записи од системот за чување на личните податоци кој функционира во Агенцијата за заштита на личните податоци, заштитата на личните податоци во рамките на регистарот на лични податоци на пациентите, кој се одржува делумно електронски а делумно во хартиена форма, се обезбедува преку следниве безбедносни мерки: заклучување на документацијата во шкафчиња, систем на видео надзор, пријава и корисничко име, огнен систем за заштита. Во овој конкретен случај, клучниот проблем бил слабата заштита на податоци, вклучувајќи го и фактот што премногу лица имале пристап до базата на податоци. Очигледно, системот на податоци немал функција да снима кој последен ги симнува податоците. Затоа било невозможно да се открие кој ги симнал информациите за писмата на кандидатите за градоначалник.

Случај 2 од Хрватска: достапност на доверливата база на податоци на Хрватската радиотелевизија на црниот пазар

Според Законот за хрватската радиотелевизија, секое физичко и правно лице во Хрватска кое поседува телевизија или радио се обврзува да плаќа радиодифузна такса. ХРТ чува и одржува регистар на месечни радиодифузни обврзници на ХРТ во Република Хрватска. Овој регистар не е достапен за јавноста. Со оглед на тоа што истиот користи лични податоци за корисниците, како име и презиме, адреса, единствен матичен број и сл, управувањето и користењето се заштитени со одредбите од Законот за заштита на лични податоци. Според информациите од јавно достапниот Централен регистар кој содржи копии од системот за чување на личните податоци во Агенцијата за заштита на личните податоци, регистарот на ХРТ се наоѓа во серверот

70 Службена интернет страница на Бирото за безбедност на информатичките системи: https://www.zsis.hr/de- fault.aspx?id=34

до кој физички пристап им е овозможен исклучиво на овластени лица. Овластените корисници ги користат податоците од регистарот преку апликација со внесување на нивното корисничко име и лозинка или сертификат. Апликацијата е достапна преку локалната мрежа и интернет, преку користење на тунели на заштитени податоци. Конечно, безбедносни копии се чуваат во сефот на просторијата во која е сместен серверот.

Во овој случај, ИТ била злоупотребена за намерно копирање и незаконска продажба на податоци од страна на лице вработено во ХРТ кое или имало пристап до регистарот или познавало некого кој има пристап до регистарот. Како резултат, сите гореспоменати технички мерки за заштита биле прекршени, исто како и одредбите на општиот правилник за работа и однесување на ХРТ, според кој вработените во ХРТ треба да работат во согласност со највисоките стандарди за работа и основните етички стандарди, врз основа на одредени вредности, вклучувајќи доверливост и заштита на податоците, согласно со важечкото законодавство и општите правила. Очигледно, овие стандарди не биле применети.

Случај 3 од Хрватска: Во потрага по бранителите

Ова е случај на злоупотреба на службена должност. Очигледно дека некој од Канцеларијата за одбрана ги зел податоците, ги објавил, ги дал, па дури и ги продал на некој друг кој потоа истите ги објавил. Можеби постојат најразлични мотиви за објавување на податоците, од политички спор до мотиви од благородна природа, како што е обид да се зголеми транспарентноста. Сепак, несомнено е дека главната причина зошто тоа се случило е недостигот на минимум безбедносни протоколи вклучени во постапката за справување со податоци кои се дистрибуираат до Канцеларијата за одбрана во различните градови во Хрватска.

Случај 4 од Хрватска: Со мала помош од јавните службеници вкупно 68 хрватски пасоши им биле продадени на криминалци; Случај 5: Полицаец фатен на дело додека вметнувал лажни податоци во информатичките системи на полицијата; Случај 6: Полицаец ги брише податоците за сообраќајни прекршоци и објавува доверливи податоци: како поткуп прифатил печено јагне и 20 литри вино!; и Случај 7: Случајно фатен при објавување доверливи податоци за возилата и нивните сопственици!

“Тајноста, интегритетот, постојаната достапност и контрола на податоците и информациите од информатичките системи за користење на МВР се спроведува преку одреден број на организациски, системски и програмски мерки и процедури, како и преку поделба на одговорноста и овластувањата. Сите корисници на информатичките системи на МВР се обврзани да спроведуваат заштита на податоците, согласно со одредбите од Уредбата за заштита на информатичките системи на МВР заснован на електронска обработка на податоци, Уредбата за безбедност и заштита на службените податоци на МВР и останатите интерни директиви и упатства кои ги регулираат активностите од заштитата на податоците на информатичките системи на МВР. Одговорностите согласно со работната позиција на надлежниот службеник го дефинираат нивото на достапност на податоците.”

Ваквите случаи би можеле да се спречат преку следење на движењето на податоците и на пристапот на вработените до системот на податоци, како и преку обука и мерки за зголемување на свесноста за ризиците на ИТ корупција и за мерките за заштита. Државните службеници треба да ја зголемат својата свесност за важноста на чување на тајноста на нивните лозинки, како и за фактот дека секој пристап до базата на податоци ќе се следи. Најслабата алка во процесот на мерките за заштита е поединецот со неговите доблести и недостатоци.

Случај 8 во Хрватска: Секоја година од патарините исчезнуваат 2 милиони евра

Во овој случај, Аутоцеста Ријека Загреб д.д. ја искористил внатрешната контрола на ИТ системот како мерка за заштита против ИТ корупција. Како надоврзување на поетичната ослободителна пресуда на судијата со цел во иднина да спречи појава на слични случаи и како мерка за заштита на ИТ, управата на НАС одлучила да ин-

сталира камери за видео надзор на работењето на вработените на патариниte. Овие камери нема да ги снимаат лицата на вработените ниту пак нивните гласови, туку само нивните работни простории, раце и процесот на плаќање/земање на патаринатa. Вкупната сума на оваа инвестиција изнесуваше 354.000 евра.

Случај 9 во Хрватска: Валкани полицајци – полицајци им доставиле доверливи податоци на шверцери со оружје; и Случај 10: Полицаец осуден на една година затвор затоа што му дозволил на пријателот нелегален риболов

Овие два случаи покажуваат дека дури и прецизно дефинирани мерки за заштита против корупција на информатичката технологија може да потфрлат. Имено, согласно со правосилното законодавство за безбедност на информациите, Министерството за внатрешни работи (МВР) има предвидено различни мерки за заштита против злоупотреба на информатичките системи кои содржат голем број различни регистри[71]. Според политиката за безбедност и фактот што според одредени документи мерките кои се предвидуваат за заштита на овој систем од злоупотреби се само за службена употреба, невозможно е да се наведат сите мерки за заштита на ИТ. Сепак, некои од нив може да се препознаат преку достапната документација и соопштенијата за јавноста, како што се:

- **Технички мерки за заштита против неовластен пристап и злоупотреба на ИТ системите**. Оваа мерка за заштита ја претставува најчестата закана во мрежниот систем. Првата линија на одбрана против неовластен пристап и злоупотреба на лозинките на ИТ системите. *„Секој полицаец има своја лозинка која му овозможува пристап до различни бази на податоци во иннформацискиот систем на полицијата”*[72], изјави криминалистот Жељко Цвртила. Согласно со нивните овластувања и потреби, на полициските службеници им е овозможен пристап до одредени нивоа на класифицирани информации. Ова им дава “пристап до најголемиот регистар на лични податоци во Република Хрватска”[73]. Според одредбите на горенаведената регулатива за безбедност на информациите, податоците од оваа база на податоци може да се користат само за службена употреба.

- **Следење на движењето на податоците и пристап на вработените до системите на податоци**. Сепак, *“едноставно тешко е ова да се контролира. Колку што мене ми е познато, процесот многу слабо се следи”*, изјави криминалистот Жељко Цвртила. *“Неколку илјади предмети секојдневно се проверуваат. И покрај тоа што е заштитена од хакирање, оваа база, вели тој, не е тешко да се хакира”*, заклучи тој[74]. Како што претходно беше споменато, на секој полицаец му е овозможен одреден пристап до податоците преку неговата лозинка, но никој не проверува потоа зошто полицаецот проверил одредени информации, изјави Цвртила.

- **Обука и мерки за зголемување на свесноста на државните службеници за ризиците од ИТ корупција и за мерките за заштита**. Вработените во Министерството за внатрешни работи земаат учество во различни обуки и проекти за зголемување на свесноста за ризиците од ИТ корупција и за мерките за заштита. Пример на мерки за заштита против ИТ корупција се двата проекти кои имаат цел да го зацврстат административниот капацитет на Министерството на полето на ИТ злоупотреба: Зацврстување на административните капацитети на Министерството за внатрешни работи во борбата против компјутерски криминал (проект во вредност од 700,000 евра) и Проектот за регионална соработка во кривичното судство: Зацврстување на капацитетите во борбата против компјутерски криминал (проектот во вредност од 2.777,778 евра), како и работилници за форензичка мрежа што ги спроведува Министерството за внатрешни работи и Хрватската академска и истражувачка мрежа.

- **Етички кодекс**: Според Етичкиот кодекс *“секое вработено лице е одговорно за етичка употреба на своите доделени овластувања на пристап до личните податоци во базата на податоци на полицијата”*[75]. Вработените во Министерството за внатрешни работи се обврзуваат да дејствуваат во согласност со Етичкиот кодекс. Граѓаните може да пријавуваат случаи на неетичко однесување на државните службеници кај службениците за етика.

- **Ревизија на ИТ системот.** Според Регулативата за внатрешна организација на Министерството за внатрешни работи (Службен весник бр. 70/12, 140/13), постојат две внатрешни организации задолжени за спроведување ревизија на информатичките системи на полицијата. Една е Секторот за безбедност на информациите, кој ја следи работата на организацијата, спроведувањето и ефикасноста на предвидените мерки и стандарди за безбедност на информациите, а другата е Секторот за внатрешна контрола, кој спроведува контрола врз информатичките системи.

- **Законски мерки за заштита**. Членовите 266 до 273 од Кривичниот законик (Службен весник, бр. 125/11, 144/12) ги дефинираат кривичните дела против компјутерските системи, програми и податоци: неовластен и нелегален пристап до компјутерски системи или компјутерски податоци (хакирање на ком-

71 Службена интернет страница на Бирото за безбедност на информатичките системи: https://www.zsis.hr/de- fault.aspx?id=34
72 http://dnevnik.hr/vijesti/hrvatska/svaki-policijski-sluzbenik-ima-lozinku-za-razlicite-baze- podataka.html
73 Potrka, Nikola (2013) Normativna uredenost zastite osobnih podataka u Republici Hrvat- skoj. Policijska sigurnost 22(4): 509-521
74 http://dnevnik.hr/vijesti/hrvatska/svaki-policijski-sluzbenik-ima-lozinku-za-razlicite-baze- podataka.html
75 Potrka, Nikola (2013) Normativna uredenost zastite osobnih podataka u Republici Hrvat- skoj. Policijska sigurnost 22(4): 509-521

пјутер); попречување на работата на компјутерскиот систем; оштетување на компјутерските податоци; неовластено следење на компјутерските податоци; компјутерски фалсификат; компјутерска измама; и злоупотреба на уреди. Според кривичниот законик, за тешки кривични дела против компјутерските системи, програми и податоци се сметаат оние насочени против компјутерски системи и компјутерски податоци кои се во сопственост на државните и локалните власти, како и јавните претпријатија. Конечно, Кодексот вклучува кривични дела поврзани со детска порнографија преку компјутерски системи и компјутерско насилство.

Повторно, важно е да се напомене дека погоре наведените мерки за заштита се само дел од мрежата на мерки за заштита кои се применуваат во Министерството за внатрешни работи. Од безбедносни причини, информациите за другите мерки не ќе се достапни на јавноста.

Случаите опишани погоре покажуваат дека наспроти законската рамка, предвидените процедури, Етичкиот кодекс и различните мерки за заштита, сè уште е можно да се направи злоупотреба на ИТ системите. Најслабата алка на процесот на заштита е поединецот со сите негови доблести и недостатоци. Тешко е дури и да се замисли мерка за заштита која може да обезбеди однесување без корупција.

Случај 11 од Хрватска: Виш инспектор злоупотребил доверливи податоци за да победи на локални избори

Според правосилното законодавство за информациска безбедност, Министерството за финансии усвои различни мерки за заштита од злоупотреба на податоците на даночните обврзници од нивните информатички системи. Заради безбедносната политика и фактот дека документите предвидуваат мерките за заштита на овој систем од евентуални злоупотреби да се користат само за службена употреба, а како што беше презентирано и во претходните случаи, невозможно е сите да се наведат. Сепак, оние кои се откриени презентирани се погоре во случај 10.

Во голем организациски систем, како што е Министерството за финансии кое вработува повеќе од девет илјади лица и кое има свои организациски единици ширум земјата, прашањата на безбедносна политика се предмет на разгледување на неколку организациски единици:

- Секторот за информатички системи во Генералниот секретаријат. Овој Сектор, меѓу другото, има задача да организира, воспостави и одржува единствен информатички системи за Централната канцеларија на Министерството; се грижи за ефикасно и прецизно користење на информатичко комуникациските ресурси; го организира и управува процесот на развој, анализа и повраток на безбедносните копии на податоците; ја следи безбедноста на комуникациите и спроведува мерки за заштита на информатичките системи.
- Секторот за информатички системи во Даночната управа, меѓу другото, спроведува планирање, развој и користење на информатичките системи и ги обучува корисниците на ИТ системот.
- Секторот за информатички системи во Царинската управа, меѓу другото, спроведува планирање, управување, надзор и координација на развој, набавка и работа на бизнис апликации, ИТ услуги и технологии; развива и спроведува политики за заштита и доделува право на пристап до информатичките системи; одредува мерки и квалитет на услуги; обезбедува изработување на безбедносни копии на информатичките системи; планирање на финансиските средства потребни за дозволи, развој и одржување на информатичките системи; и ги обучува корисниците за ИТ системот на Царинската управа.
- Службата за развој и поддршка на оперативно-информатичките системи на Државниот трезор, меѓу другото, обезбедува континуитет и стабилност и неопходно ниво на заштита на работните процедури на Државниот трезор; спроведува задачи на дизајн, оптимизација, анализа, надградба и стандардизација на работните процедури; како и задачи на овластување, безбедност и заштита на податоците.
- Одделение за стратешка анализа и инмформациски систем на Канцеларијата против перење на пари кое, меѓу другото, дизајнира и развива информации и подсистеми на оваа канцеларија; предлага подзаконски акти и внатрешни регулативи во полето на заштита на системски податоци и евиденции во оваа канцеларија; го одржува и спроведува надзорот врз системот за заштита на податоци и евиденции на канцеларијата.

Уште еднаш, важно е да се нагласи дека наведените мерки за заштита се само дел од мрежата на мерки за заштита која се применува во Министерството за внатрешни работи, но кои заради нивната безбедносна природа, не ќе се целосно достапни на јавноста.

Сепак, како и во претходните случаи, и покрај постоењето на законска рамка, процедури, Етички кодекс и различни мерки за заштита, злоупотребата на ИТ системите сè уште е можна појава. Најслабата алка во процесот на мерките за заштита е поединецот со сите негови доблести и недостатоци. Тешко е дури и теоретски да се замисли мерка за заштита која би овозможила однесување без корупција.

Случај 12 на Хрватска: Немаш ни еден ден на работа? Не се грижи, секако ќе ти дадеме пензија!

Мерките за заштита кои се дизајнирани со цел да спречат злоупотреба на главниот регистар на лица кои добиваат пензиско осигурување и на главниот регистар на корисници на право на пензиско осигурување во HZMO се: 1) хронолошко следење на промените во податоците (преку користење на идентификација на корисникот и датум); 2) политика на одобрение за пристап до податоците според работното место и спроведување на мерки за заштита на хардверот и софтверот. Освен овие главни мерки за заштита, исто така, предвидени се: 3) одредби од соодветното законодавство за заштита на лични податоци; и 4) одредби од Етичкиот кодекс и внатрешната ревизија. Сепак, случаи како овој докажуваат дека сè уште постои можност за повреда на сите овие мерки за заштита.

Во изминатите две години, HZMO стана една од првите институции кои земаа учество во проектот за интеграција на системот на посебниот број за лична идентификација (OIB), заедно со Даночната управа на Министерството за финансии, Министерството за јавна администрација и Министерството за внатрешни работи. *"Целта за воведување на посебниот бројот за лична идентификација OIB беше да се создаде единствен личен идентификатор, кој би бил правно прифатен од јавните правни тела на Република Хрватска. Како резултат на создавањето на единствениот личен идентификатор во сите службени евиденции, се создадоа предуслови за размена на компјутерските податоци меѓу правните јавни тела. Само преку размена на компјутерските податоци јавните правни тека може економично и ефикасно да ги разменуваат неопходните податоци од службените евиденции со цел да се обезбеди навремено и конзистентно спроведување на сите предмети во управна, даночна и кривична постапка."*[76]. Имајќи го ова предвид, бројот за лична идентификација се смета за силен инструмент кој, меѓу другото, овозможува систематска борба против корупцијата.

Пред да се интегрира во мрежата за размена на единствениот број на лична идентификација OIB, HZMO функционираше како остров во државната администрација. Имаше сопствена база на податоци со корисници на кои редовно им ги исплаќаше пензиите. Со оглед на тоа што размената на податоци меѓу правните јавни тела не беше можна, после смртта на член на семејството, другите членови на семејството беа обврзани да достават посмртница до регионалната служба на HZMO, односно телото кое би ја исплаќало пензијата на сега починатиот. Оваа процедура отвори можност за измами. Доколку никој не ја однесеше посмртницата до регионалната служба на HZMO, семејството можеше да продолжи да ја добива пензијата.

Сепак, со интеграцијата на HZMO во мрежата на единствениот број за лична идентификација OIB од септември 2013 год оваа дупка се затвори. Со оглед на тоа што предусловот за размена на компјутерски податоци меѓу правните јавни тела е поседување на единствен број за лична идентификација OIB, се откри дека 125,867 од вкупно 1.2 милион пензионери не поседуваат единствен број за лична идентификација. Вториот чекор беше да се отфрли можноста пензиите да се подигнуваат од пошта, и наместо тоа да може да се подигнуваат само преку сметка во банка. Доколку корисниците на HZMO сакаа да продолжат да ја добиваат пензијата, обврзани беа да го достават до HZMO својот единствен број за лична идентификација OIB.

Бројот на пензии без пријавен единствен број за лична идентификација се намали за 49,586 во април 2014 год. и се состои главно од странски корисници. Преку дополнителната размена на податоци со Даночната управа во Министерството за финансии; Министерството за јавна администрација; и Министерството за внатрешни работи, на 8 април 2014 год., исплатата на 9,593 пензии беше стопирана - 9,108 од странство и 485 од Хрватска. HZMO сè уште се обидува да ги открие причините зошто овие пензионери до нив не го доставиле својот единствен број за лична идентификација. *"Дали овие корисници се во Хрватска, дали сè уште се живи, дали некој друг ги користи нивните пензии и незаконски се стекнува со парични средства?"*, изјави Министерот за труд и пензиски систем, г. Мирандо Мршиќ кој додаде: *"Се прават ли евентуални измами, дали се овие лица во Хрватска, каде завршуваат овие пензии, сакаме да ги расчистиме овие работи. Не зборуваме за мали средства, туку за повеќе од 16.6 милиони евра и сакаме овие пари да им ги исплатиме на оние кои имаат право да ги добијат"*[77].

Досега, интеграцијата на HZMO во мрежата на единствениот број за лична идентификација OIB покажа дека 26 семејства продолжиле да примаат пензии на починати членови на семејството. Меѓу нив имало случај на поштар кој редовно исплаќал пензија на семејството на членот кој починал пред 20 години. Само преку овој случај државата имала фактичка загуба од 65,000 евра. Преку вмрежувањето во системот на OIB, исклучена е можноста да се јават случаи како претходните со оглед на тоа што правните јавни тела се тие кои ги прибираат и спроведуваат податоците и автоматски ги известуваат властите за евентуална неконзистентност на податоците.

76 ttp://www.mfin.hr/en/novosti/full-application-of-oib-personal-identification-number

77 http://dnevnik.hr/vijesti/hrvatska/nema-oib-a-nema-mirovine-pod-povecalom-2-400-umirovljenika---309572.html

Косово

Подготвено од Хасан Претени и Дриарт Елсхани

Примери на мерки за заштита против злоупотреба на ИТ

Агенциите од јавниот сектор се потпираат врз системите на информатички технологии (IT) во своето оперативно работење и во овозможувањето на голем дел од своите услуги. Важно е да се обезбеди информациите во овие системи да бидат прецизни и целосни. Исто така, од суштинска важност е овие информации да бидат лесно достапни за легитимни цели, а истовремено и заштитени од злоупотреба. Во Косово постојат само неколку електронски регистри, па така има ниско ниво на случаи на ИТ корупција со оглед на тоа што не постои простор да се прават измени во електронските податоци. Навистина, случаите кои ги избравме укажуваат на отсуство на мерки за заштита кои би се користеле против злоупотреба на податоци, но кои начелно би обезбедиле и заштита на ИТ системите.

Сите случаи презентирани во поглавје 1 од оваа студија ја нагласуваат важноста да се обезбедат подеднакво административни (или законски) и технички мерки за заштита кои ќе се преземат и спроведат од секоја надлежна институција. Понатаму, она што може да го заклучиме од секој од овие случаи е дека гореспоменатите мерки за заштита или не биле преземени или не се почитувале. Дури и во случај кога се донесени мерки за заштита, истите биле нецелосни или им недостасувала јасна дефиниција на процедурите и улогите за намалување на ризиците од злоупотребата на податоците и генералните системи на информатичка технологија. Косово мора да работи понапорно за да ги создаде и спроведе овие мерки за заштита, особено имајќи предвид дека Косово во иднина ќе спроведува многу ИТ системи и ќе мора да ги намали ризиците од злоупотреба на податоците и системите на информатички технологии. Косово сè уште нема преземено никакви конкретни мерки за соодветно разгледување на таквите мерки за заштита. Мерките за заштита кои овде го презентираме би ги намалиле овие ризици и би спречиле злоупотреба на системите на информатички технологии. Во иднина сè ќе биде дигитално, односно употребата на хартија ќе биде ограничена, па така може да се јават нови форми на злоупотреба на кои ќе биде потребно да им се одговори преку различни методи. Таквите методи ќе се потпираат врз мерките за заштита кои овде ги презентираме.

Навистина, во ова студија предлагаме конкретни мерки за заштита на интегритетот на податоците и на ИТ системите од нивна евентуална злоупотреба од човечки фактор. Имаме обезбедено предлози за општи упатства и механизми за електронските системи. Конкретните мерки за заштита и упатствата треба да се применуваат во секоја институција. Овие стандарди и политики се осмислени да ги заштитат ИТ системите и податоците од уништување, менување и фалсификување. Мерките за заштита кои ги предлагаме во поглавје 2 од оваа студија би можеле да се усвојат во форма на политика за целиот спектар на институции со цел истите да може да ги заштитат своите ИТ системи од евентуална злоупотреба.

- Во однос на техничките мерки за заштита, освен централизацијата на некои од ИТ системите, сите останати технички мерки за заштита очигледно недостасуваат. Немаме информации дали се донесени дополнителни технички мерки за заштита. Сепак, информирани сме дека во некои агенции во моментот се прави преглед на процесите на општа примена и одобрување.
- Во однос на организациските и процедуралните мерки за заштита, истите сè уште не се донесени. На пример, ова можеби е резултат на отсуството на јасна дефиниција на улогата и одговорностите или непостоење на принципот на "повеќе очи". Никакви дополнителни мерки за заштита од овој тип не се донесени.
- Во однос на следењето на пристапот на вработените во системите на податоци, организациите имаат научено преку овој случај дека потребно е да се преземат соодветни мерки. Некои од овие мерки, како на пример следење на тоа кој им пристапува на системите на податоци, во моментот се применуваат.
- Во однос на обуката и мерките за зголемување на свесноста, такви мерки сé уште не постојат. Не постои ни план за превземање на такви мерки.
- Во однос на спроведувањето ревизија, во најголем дел од организациите претходно не била направена никаква ревизија кога овој случај бил откриен и немаме информација дали такви мерки во моментот постојат. Некои организации започнаа да спроведуваат целосна ревизија на безбедноста и во моментот се во фаза на спроведување на препораките. Сепак, таквите препораки се однесуваат само на безбедноста, како што е одбрана од компјутерски напад, и не се фокусираат на прашањата кои произлегоа од овој случај.
- Во однос на законските мерки за заштита, во времето кога се појави овој случај такви не постоеја.

Понатаму, она што најмногу може да го научиме од овој случај е дека размената на податоци помеѓу јавните тела може да биде суштинска во борбата против повторна појава на такви случаи. Доколку нивните системи беа интероперабилни, на тој начин, на пример, ќе можеше да се забрза процесот. Постоењето на интероперабилен процес за проверка на даночните документи би го отежнало евентуалното фалсификување на таквите документи.

Мерки против ИТ корупција во Косово

Потребно е да се донесат мерки за заштита со цел да се овозможи соодветно откривање и следење на случаите на корупција. Таквите мерки за заштита потребно е да бидат посеопфатни, разновидни и да вклучуваат: технички мерки за заштита, организациски и процедурални мерки за заштита, следење на движењето на податоци и пристап на вработените до системите на податоци, обука и мерки за зголемување на свесноста, внатрешна или надворешна ревизија, и законски мерки за заштита.

Понатаму, се препорачува да се формира посебно институционално тело во земјата со цел да се заштити интегритетот на податоците и на системите на информатички технологии и да се спречи нивна злоупотреба. Потребно е да се каже дека такво специјализирано тело во моментов не постои во Косово. Во Косово постои посебна Агенција за заштита на приватноста и податоците, но оваа Агенција делува само како чувар на приватноста. Нејзиниот мандат не е доволен и не ги покрива обврските за превземање мерки за заштита во однос на злопотреба на информатичката технологија.

Всушност, не постои никаква институција која се занимава со изготвување и спроведување на мерки за заштита и стандарди во однос на оваа проблематика. Случаите на злоупотреба на информатичката технологија сè уште се широко распространети и честопати остануваат целосно неоткриени. Кога зборуваме за мерки за заштита, вреди да се спомене дека истите би можеле да бидат двострани: технички и административни.

Административните мерки за заштита би можеле да бидат во форма на закони, нормативни акти и административни регулативи со кои би се санкционирале евентуални прекршувања на интегритетот на податоците и генерално на системите на информатичка технологија. Секоја институција би следела јасна инфраструктура на регулативи предвидена со закон.

Техничките мерки за заштита би можеле да бидат во форма на Стандардни работни процедури кои секоја институција би ги следела со цел да обезбеди заштита на податоците и на системите на информатичка технологија од евентуални злоупотреби. Секоја институција би следела листа на проверка за Стандардните работни процедури која би гарантирала максимална заштита и отпор против таквите злоупотреби. Актуелните административни упатства во себе не содржат никакви Стандардни работни процедури.

Во однос на административните мерки за заштита, Косово има усвоено низа закони, стратегии и административни упатства (нормативни акти) кои се однесуваат на употребата на информатички и комуникациски технологии, но законската инфраструктура до сега го нема соодветно адресирано прашањето на интегритет на податоците и злоупотреба на системите на информатичка технологија било конкретно или начелно.

Компјутерски криминал

Во Косово сè уште не е формиран Тим за одговор на компјутерски инциденти (CERT) кој би бил, меѓу другото, задолжен и за заштита на ИТ системите. Предвидено е во блиска иднина таквиот Тим да се формира. Сепак, Тимот за одговор на компјутерски инциденти би бил недоволен со оглед на тоа што тој само реактивно би се справувал со заштита против злоупотреби, наместо да обезбедува и проактивни превентивни мерки.

Други мерки

Постојат и други мерки кои би можеле да се применат во борбата против ИТ корупција. На пример, размена на податоци помеѓу јавните тела и спроведување на општа рамка за интероперабилност која би ја спречила појавата на некои од случаите, како на пример случајот 2. Посебните мерки во јавната набавка на ИТ системите, како на пример е-набавка, исто така би се сметале за релевантни. Косово е во фаза на спроведување на системот на е-набавка. Понатаму, пожелни би биле мерки од типот на податоци кои се однесуваат на отворена власт. Ова би помогнало на размената на податоци помеѓу јавните тела. Косово се наоѓа во почетната фаза од овој процес.

ЗАКОНИ, СТРАТЕГИИ И АДМИНИСТРАТИВНИ УПАТСТВА КОИ СЕ ОДНЕСУВААТ НА ИНФОРМАТИЧКО-КОМУНИКАЦИСКИТЕ ТЕХНОЛОГИИ НА КОСОВО

Закони

Законите во Косово кои се однесуваат на информатичко комуникациските технологии (ИКТ) а кои се применуваат од 2009 год. досега прикажани се во следнава табела:

Табела 2 Спроведени и изменети закони од 2009 до 2014 год.[78]

Бр.	Назив на законот	Дали е внесен во Акцискиот план?	Бр. на законот	Датум на одобрување	Акт и прогласување на законот
1	**Закон за заштита на лични податоци**	ДА	03/L-172	29.04.2010	Указ бр. DL-020-2010, Датум 13.05.2010
2	**Закон за спречување и борба против компјутерски криминал**	ДА	03/L-166	10.06.2010	Указ бр. DL-028-2010, Датум 02.07.2010
3	**Закон за пристап до јавни документи**	ДА	03/L-215	07.10.2010	Указ бр. DL-063-2010, Датум 01.11.2010
4	**Закон за услуги на информатичко општество**	ДА	04/L-094	15.03.2012	Улаз бр. DL-010-2012, Датум 02.04.2012
5	**Закон за спречување на конфликт на интерес во извршување на јавни функции**	ДА	04/L-051	31.08.2011	Указ бр. DL-029-2011, Датум 31.08.2011
6	**Закон на државна архива**	ДА	04/L-088	15.02.2012	Указ бр. DL-007-2012, Датум 01.03.2012
7	**Закон за административни конфликти**	ДА	03/L-202	16.09.2010	Прогласен согласно со член 80.5 од Уставот на Република Косово, Датум 06. 10.2010
8	**Закон за високо образование во Република Косово**	ДА	04/L-037	29.08.2011	Указ бр. DL-036-2011, Датум 31.08.2011

78 Податоци преземени од Собранието на Косово* - Сектор за правни прашања и постапки (AK - DSLP) (2014)

Стратегии

Досега се усвоени следните стратегии:

- Национална стратегија за информатичко општество 2006-2012
- Стратегија за електронско владеење 2009-2015
- Стратегија за е-учење на Косово 2010-2015 со главна цел
- е-учењето да се трансформира во интегрален дел на општиот национален систем на образование
- Стратешки план за образование на Косово 2011-2016 кој содржи осум приоритетни програми вклучувајќи изградба на капацитетот и информатичка и комуникациска технологија
- Стратегија за развој на предуниверзитетското образование 2007-2017

Сепак, ниеден од овие закони и стратегии не се осврнува конкретно на интегритетот на податоците и злоупотребата на системите на информатичка технологија.

Административни упатства

Конечно, во однос на проблематиката на ИТ досега се усвоени следните административни упатства (АУ):

1. А.У. бр. 02/2010 за Управување со информациска безбедност
2. А.У. бр. 01/2010 за Безбедност и пристап до База на податоци
3. А.У. бр. 04/2010 за користење на електронска службена пошта во институциите на Косово
4. А.У. бр. 01/2011 за Управување и користење на интернет во институциите на Косово
5. А.У. бр. 07/2008 за засилување на транспарентноста и стандардизација на интернет веб страници во институциите на Косово
6. А.У. бр. 03/2010 за користење на хардвер и софтвер
7. А.У. бр. 02/2011 за Владиниот портал на Република Косово

Анализата на содржината на овие документи ги откри следниве проблеми:

- АУ за безбедност на информациите формално е издадено во 2010 год., но досега се нема спроведено ниедна програма за социјализација преку која сите страни би можеле да ги разберат своите одговорности и обврски;
- АУ за безбедност на информациите дава опис на техничките политики, но не ја дефинира рамката за управување на системот, вклучувајќи ги улогите, одговорностите и надлежните органи;
- Не постои јасна поврзаност помеѓу Административните упатства или на кој начин истите се дефинирани да ги исполнат одредените барања.

Понатаму, овие административни упатства само делумно се однесуваат на загриженоста, на пример, во однос на правото на пристап до информации во базите на податоци и интернет, и наместо тоа остануваат да бидат во голема мера нејасни. Понатаму, спроведувањето на ова упатство е релативно отежнато со оглед на тоа што ниедна конкретна институција не се занимава со неговата усогласеност. Пред сè, и покрај тоа што општо мислење е дека во Косово постои добра правна инфраструктура, може да се забележи дека голем дел од законите сè уште недостасуваат и/или се нецелосни. Косово мора да работи понапорно со цел да обезбеди законски предвидените мерки за заштита да се добро напишани, усвоени и спроведени.

Технички мерки за заштита

Досега мерките за заштита главно беа ограничени на едноставна заштита на лозинката на поединечните корисници, криптирање на податоците во одредени поединечни случаи, и обид да се заштитат серверите од физичка попреченост. Во моментот, во Косово недостасуваат пософистицирани стратегии и стандарди за технички мерки за заштита во јавниот ИТ сектор.

Македонија

Подготвено од Марјан Стоилковски и Розалинда Стојова

Институционални мерки за заштита

Согласно со одредбите од Законот за спречување на корупција, во 2002 год. Државната комисија за спречување на корупција (ДКСК) беше формирана како независно тело. Со членот 1 од Законот, на ДКСК ú се доделува одговорност да применува мерки и активности со кои се спречува корупцијата во вршењето на власта, јавните овластувања, службената должност и политиките; мерките и активностите за спречување на судирот на интереси; мерките и активностите за спречување на корупција при вршењето работи од јавен интерес на правни лица сврзани со остварувањето на јавните овластувања, како и мерките и активностите за спречување на корупцијата во трговските друштва.

Понатаму, во 2008 год. се формираше Одделение за борба против корупција кое претставува организациска единица во рамките на Секторот за организиран криминал при Министерството за внатрешни работи. Задачите на Единицата за борба против корупција се да ги открие и истражи сите типови на корупција во Република Македонија.

Технички мерки за заштита против недозволен пристап и злоупотреба на ИТ системите и следење на движењето на податоците и на пристапот на вработените до системите на податоци

Како дел од техничката спецификација на информатичките системи, без оглед дали се однадвор ангажирани или развиени внатре во самата организација, постојат неколку постапки кои се применуваат и следат. Некои од постапките се предвидени согласно со соодветното законодавство, но некои од најважните повеќе се резултат на воспоставена пракса наместо законски предвидена обврска. Нивната цел е да спречат користење на ИТ за корупциски цели и се сметаат за најважните барања кои мора да се исполнат на самиот почеток на процесот на тестот за прифаќање. Тие се:

- Водење записник за секој пристап, дополнување, бришење или менување на податоците и, по барање, таквиот записник да се стави на располагање за целите на ревизија и внатрешна контрола. Освен чувањето и архивирањето на записниците никакво друго дејство не е дозволено.
- Обезбедување различни нивоа на идентификација и овластување. Доверливоста на нивото на податоци кои се обработуваат во системот влијае врз степенот на сложеност на процесот на идентификација и овластување. Во сите системи, различните улоги на корисникот се дефинираат во зависност од неговите назначени привилегии, започнувајќи со користење на едноставно корисничко име и лозинка за некои од корисниците, па сè до барање за користење дигитални сертификати или дури само овозможување пристап до податоци од одредена работна станица во строго одредена физичка локација.
- Според Законот за електронско управување, во случај на однадвор обезбеден развој на чување на системи и/или обработка на лични податоци, но не е исклучено и кога системот е развиен внатре во организацијата, едно од барањата е да се формираа околина за развој и тестирање, користење на податоците за тестирање, додека вистинските податоци се чуваат само во околината каде се произведени. Ова овозможува канализиран и контролиран пристап до податоците, но само од вработените лица кои се службено назначени.
- Подготвувањето редовни извештаи за активноста на корисникот преку различните типови на корисници и улоги исто така претставува барање со кое се обезбедува редовен начин на следење на активностите на корисникот. Таквите извештаи се доставуваат до главните администратори и до највисокото раководство.
- Една од најдобрите воспоставени практики за најголем дел од локалните системи е испраќањето електронска порака и/или известување по пат на смс порака до главниот администраторот (администраторите) и до највисокото раководство во случај да се откриени сомнителни активности или активности кои се во процес на извршување.
- Со цел да се обезбеди интернет поврзаност на системот при размена на податоци меѓу системите и со цел да се спречи следење на комуникациите на податоците, сите институции создаваат/воспоставуваат VPN поврзаност која користи криптирани податоци.
- Во рамките на своето работење, надлежните службени лица користат работни станици кои имаат пристап само до оние податоци за кои се задолжени нивните институции и немаат интернет пристап или пристап до другите системи.
- ИТ системите во приватниот и јавниот сектор подлежат на тестирање за нивната ранливост и евентуален пробив на системот. И покрај тоа што тестирањето на евентуален пробив е пошироко распространето во приватниот сектор, честопати јавниот сектор ангажира фирми сертифицирани за вршење тестирање за пенетрација и го користат овој метод за спречување неовластен пристап до ИТ системите.

Организациски и процедурални мерки за заштита како што е 'принципот на повеќе очи'

- Постои тренд на потпишување Договори за доверливост (Non-Disclosure Agreements) со економските оператори и извршители. Таквите договори се изменуваат преку изјава за доверливост на двете договорни страни – договарач и извршител – за лицата кои ќе имаат пристап до системот.

- Физичкиот пристап до системот во кој било момент, без оглед на тоа дали за време на спроведувањето или одржувањето, ќе се овозможи само после добивање потврда за спроведена проверка од Министерството за внатрешни работи за секое инволвирани лице.
- Во институциите има воспоставена пракса на назначување две клучни улоги за два различни типови на вработени: технички администратори и администратори на содржина. Техничките администратори се задолжени за системот на нивото на негова примена, и освен со управувањето на системот и базата на податоци, вработените кои ја имаат оваа улога исто така управуваат со корисниците и нивните дозволи, но не и со податоците кои се чуваат во базите на податоци. Администраторите на содржина се одговорни за управување со податоците кои се чуваат во базите на податоци.

Обука и мерки за зголемување на свесноста на државните службеници за ризиците од ИТ корупција и за мерките за заштита

Жртви на корупција може да бидат граѓани поединци, деловни субјекти или група на лица, но во некои случаи жртва може да биде и самото општество. Борбата против корупција е една од најважните стратешки цели усвоени од министерствата и другите институции, со што се покажува заложбата на Владата на Република Македонија (види Стратегија за реформи во јавната администрација и нејзините Акциски планови[79]). Понатаму, јавниот сектор и граѓаните имаат активна улога во реформирање на општеството, со што ја докажуваат својата желба и подготвеност повеќе да научат за начините на спречување на корупцијата и можностите кои им се на располагање за преземање на правни дејства. Така, институциите и јавниот сектор (НВО) ги имаат превземено следниве дејства: почеста обука за вработените и граѓаните во институциите кои се поранливи на корупција; кампањи за зголемување на јавната свест преку различни канали; печатени летоци; рекламни паноа; кратки ТВ реклами.

Ревизија на ИТ системите (внатрешна или надворешна контрола; иницирана од јавни органи или по добиено известување или приговор од граѓани или од медиуми)

И покрај тоа што вршење ревизија на ИТ системите преку внатрешни и надворешни контроли се прави само за мал број на системи, ова е една од мерките на располагање. Истата се применува во многу ретки случаи, како на пример кога системот управува со доверливи податоци или податоци кои се од важност за државата, како и во случаи кога се обезбедени доволно средства и време.

79 http://mioa.gov.mk/files/pdf/dokumenti/RevidiranAP_SRJA_mioagov.pdf

Законски мерки за заштита

Во 2002 год. се донесе **Законот за спречување на корупција** со што се овозможи спроведување на законската рамка во борбата против корупција. Со последните измени од 2010 година овој закон:

“ги уредува мерките и активностите со кои се спречува корупцијата во вршењето на власта, јавните овластувања, службената должност и политиките; мерките и активностите за спречување на судирот на интереси; мерките и активностите за спречување на корупција при вршењето работи од јавен интерес на правни лица сврзани со остварувањето на јавните овластувања, како и мерките и активностите за спречување на корупцијата во трговските друштва“ (член 1).

Со него се воведува систем на интегритет (пакт за интегритет) и заштита на “дојавувачите”.

- **Законот за електронско управување** ги опишува стандардите кои треба да се исполнат при развој на информатичките системи кои комуницираат и споделуваат податоци и документи со информатички системи од други институции за целите на управна постапка[80]. Подзаконските акти за препознавање на единствената околина и електронската комуникација меѓу институциите за размена на податоци и документи, како и дополнителните упатства за техничките барања, начинот на работа, клиентот на комуникации и препораката за користење на систем на интероперабилност даваат опис на:

  - Техничките барања за хардверската и софтверската инфраструктура на клиентите на комуникации;
  - Единствена околина;
  - Одржување и развој на веб услуги;
  - Протоколи за електронска пошта;
  - Пристап до податоци, предмет на размена;
  - Безбедност и интегритет на податоците, а во дополнителните упатства се воведуваат голем дел од серијата стандарди ISO 27000;
  - Структура на податоците и документите, предмет на размена; и
  - Планирање на основните елементи на архитектурата за комуникации со системот на интероперабилност.

- **Законот за електронски комуникации** обезбедува заштита на правата на корисниците, вклучувајќи и крајните корисници со попреченост во развојот и крајните корисници со посебни социјални потреби и обезбедува доверливост на комуникациите.

80 http://mioa.gov.mk/files/pdf/dokumenti/zakoni/zeu/Zakon_za_elektronsko_upravuvan- je_konsolidiran_tekst.pdf

- **Законот за заштита на личните податоци**, последен пат изменет во 2012 год., е усогласен со соодветните регулативи на ЕУ и се применува на целосната или делумната автоматска обработка на личните податоци. Законот, меѓу другото, дава опис на начините на обработка на личните податоци и утврдените технички барања за заштита на обработката на личните податоци.
- **Законот за користење на податоците од јавниот сектор** усвоен во 2014 год. е одраз на активностите преземени за време на иницијативата за Партнерство на отворена власт. Законот е усогласен со Директивата 2003/98/ЕС на Европскиот парламент и Европскиот совет за повторно користење на податоци од јавниот сектор. "Овој закон ја утврдува обврската на органите и институциите од јавниот сектор за јавно објавување на податоци кои се генерирани при спроведувањето на нивната надлежност во согласност со законот, со цел да се овозможи користењето на таквите податоци од страна на трговски друштва или поединци за создавање на нови информации, содржина, апликации или услуги." Една од целите е да се охрабри "зголемена отчетност и транспарентност на јавниот сектор", што претставува една од алатките за спречување на корупција.
- **Законот за финансиска дисциплина**, усвоен во 2013 год., го уредува навременото исполнување на финансиските обврски кои произлегуваат од спроведувањето на деловните трансакции меѓу економските оператори во приватниот сектор, односно меѓу субјектите од јавниот сектор и економските оператори од приватниот сектор, заради спречување на неисполнување на предвидените парични обврски согласно со одредбите од овој закон. За секоја договорна страна која не ја почитува оваа обврска одредена е парична казна. Спроведувањето на контролираните исплати на паричните обврски цврсто ги поддржува активностите против корупцијата.
- Последните измени на **Законот за јавни набавки** беа донесени во 2014 год. со што се предвидоа неколку поголеми промени. Пред да се направат набавки на стока и услуги кои имаат поголема проценета вредност од она што месечно е дефинирано како мали набавки договорните органи се обврзуваат да спроведат испитување на пазарот. Ова значи обезбедување одреден број. (зависно од проценетата вредност) на пријави за учество од различни добавувачи. Доколку има добавувачи помалку од предвидениот број кои се способни да ги испорачаат побараните стоки или услуги и кои ги исполнуваат условите да се пријават, договорниот орган мора да добие писмена согласност од Советот за јавни набавки, тело формирано согласно со измените на овој Закон.
- Според државното законодавство за класифицирани информации, секој ИТ систем кој поседува или обработува класифицирани информации мора да биде акредитиран од сертифицирани акредитори на државната Дирекција за безбедност на класифицирани информации. При развојот на ИТ системи за обработка на класифицирани информации се усвојуваат посебни упатства за технички карактеристики на хардверот и софтверот што ќе се користи во ИТ системот за класифицирани информации.
- Меѓу останатите правни акти, **Законот за класифицирани информации** на државно ниво се користи како мерка за заштита против неовластен пристап и злоупотреба на ИТ системи.

ДРУГИ МЕРКИ

Мерки за заштита во постапката за набавки и за финансиска дисциплина

Дополнително, воведени се следните барања кои го поддржуваат спречувањето на корупција во постапките за јавни набавки:

- Техничката спецификација не смее да содржи никакви брендови, не смее да биде дури ниту поврзана со наведувачки описи, а деталните барања во спецификацијата треба да бидат исполнети од повеќе од еден добавувач; освен во случаи предвидени со законот каде претходно опишаната постапка ќа се почитува;
- Сите јавни набавки во државните и јавните институции мора да се спроведуваат преку системот за јавни набавки.

Карактеристична софтверска апликација како мерка на заштита

Министерот за труд и социјална политика (МТСП) изјави дека Министерството има спроведено серија активности и анализи на полето на правата за социјална заштита. Понатаму, додаде дека со спроведувањето на новиот софтвер за социјална заштита се откриле случаи на злоупотреба и неточно објавување на информации од страна на корисниците. Подлабоката анализа откри дека таквите злоупотреби не можеле да се направат освен ако не постоела соработка меѓу неколку вработени лица. Како резултат на тоа, започнати се внатрешни контроли и следење на работата на центрите за социјална заштита, при што во неколку случаи откриени се докази за злоупотреба на правото на социјална помош, а против сите сторители поднесени се кривични пријави. Докажано беше дека девет граѓани од еден град А, вработени како референти во јавната установа "Центар за социјални работи" во градот А, ја злоупотребиле својата службена должност и им помогнале на одреден број граѓани незаконски да се стекнат со право за добивање социјална помош.

Во случаи кои претходно се покажале како ранливи на корупција, ИТ системите сега се користат за доделување на СЕМТ дозволи, социјални станови, соби во студентските домови како и за други услуги. Една од најважните услуги е електронското распределување на судски случаи на судиите, утврдена и претставена како мерка 11 во Стратегијата за реформи во јавната администрација и нејзините Акциски планови[81].

Постои електронски образец за анонимно известување за сторена или тековна корупција, достапен на порталот на Управата за јавни приходи (УЈП). Ова е најчесто

81 http://mioa.gov.mk/files/pdf/dokumenti/RevidiranAP_SRJA_mioagov.pdf

користениот образец од овој тип. Анонимноста на испраќачот е загарантирана со тоа што неговата ИП адреса е невидлива за корисниците на УЈП.

Отворената власт како мерка за заштита

Отворањето на јавните податоци и нивното објавување на институционалните портали е еден од форматите со 5 ѕвездички[82], кој накратко ја претставува иницијативата на Партнерството за отворена власт. Станува збор за нов пристап во активностите за борба против корупцијата кој му овозможува на секој субјект да има активна улога во спречувањето и откривањето на корупција. На пример, еден вид на податоци кој во случај да биде доставен се објавува се податоците за финансиска/имотна состојба на високи службеници.

Како дополнителен доказ за заложбата на владата, во 2014 год. се усвои Законот за користење на податоците од јавниот сектор. Со него се утврдува обврската на органите и институциите од јавниот сектор јавно да ги објавуваат податоците кои ги произведуваат во рамките на своите надлежности, со цел да се овозможи користењето на таквите податоци од страна на трговските друштва и поединци за создавање на нови информации, содржина, апликации или услуги. Овој закон, исто така, ги дефинира ограничувањата за склучување ексклузивни договори од страна на институциите.

Согласно со отворање на податоците, законите кои го уредуваат издавањето на службени дозволи кои завршуваат со процес на тестирање, односно извршители, форензичари, проценители, нотари и други, се усогласени со следниве принципи: за секоја професија потребно е да има подготвено најмалку 500 однапред дефинирани прашања кои ќе бидат јавно достапни на релевантните портали. Тестирањето се спроведува по електронски пат исклучиво преку користење на електронски систем за тестирање. Примерокот на прашањата за реалното тестирање се избира по случаен избор според одредени критериуми и обезбедува еднакви можности за сите кандидати. Понатаму, тестирањето треба да се снима со видео уред или да се пренесува преку интернет за да може да се поништи во случај да се забележат или докажат неправилности.

Овој принцип, исто така, треба да се примени и при постапката за вработување на административните службеници како и во спроведувањето на екстерното тестирање на студентите, но во овие случаи без видео надзор и преку користење на различни прашања за секој студент.

82 Планот со пет ѕвездички за Отворени податоци предложен од страна на Tim Berners-Lee, пронаоѓачот на world wide web и иницијаторот на отворените податоци, доделува ѕвезди за изгледот на отворен и поврзан формат на податоци. Една ѕвезда значи податоците се достапни на веб (во каков било формат) во рамките на отворена лиценца, но податоците не мора да бидат структурирани, може да го користат форматот на сопственикот, не мора да користат URI за да упатуваат на работи, и не мора да бидат поврзани со други податоци при обезбедување контекст. Една ѕвезда е најниското ниво на обезбедување отворени податоци.

Црна Гора

Подготвено од Душан Дракиќ и Иван Лазаревиќ

Вовед во примерите на мерки за заштита против злоупотреба на информатичка технологија

За да се намали злоупотребата на податоци потребно е постојано да се следат и развиваат одредени аспекти на информатичко комуникациската технологија. Сепак, во потесна смисла злоупотребата на податоците на државно и понекогаш на локално ниво поверојатно е дека е последица на моралниот статус на општеството и на неволноста на поединецот да се потчини на организираниот ред и усогласеност. ИКТ овозможува квалитетни регистри на бази на податоци дефинирани во согласност со меѓународните стандарди, обезбедува признавање и заштита на домашни и странски физички и правни лица, како и на подвижната и неподвижната сопственост на територијата на државата.

Избраните случаи го насочуваат вниманието кон зголемена потреба од електронски регистри кои ќе ни овозможат да го дефинираме местото на потекло како и електронското чување на централизираните бази на податоци и кои ќе го олеснат нивното користење. Неопходно е да се подобри и стандардизира размената на податоци во рамките на владата преку цврста и податлива ИКТ инфраструктура. Важно е да се модернизира јавната администрација и да се прошират јавните услуги кои се фокусираат врз корисникот, зголемувајќи ја притоа нивната достапност и безбедна испорака преку различни канали.

Случаите, исто така, укажуваат на потребата да се воспостави рамка на интероперабилност која ќе создаде услови за подобрување на квалитетот на управување со податоци и размена на информации меѓу владините агенции, како и да овозможи автоматска размена и користење на податоците кои се чуваат во јавните регистри и во други информатички системи.

МЕРКИ ЗА ЗАШТИТА ВО ПРИМЕРИТЕ НА СЛУЧАЈ ОД ЦРНА ГОРА

Случај 1 од Црна Гора: Злоупотреба на службената положба и фалсификување на службени документи

Случајот на фалсификувана патна исправа со изминатa важност и нејзино користење од трето лице укажува на грешка или пропуст во информатичките системи за издавање патни исправи во Министерството за внатрешни работи, кое треба да ги отстрани сите ризици за користење и повторно издавање на патни исправи со истечен период на важност. Системот не го поврзувал физичкиот документ (патната исправа) со отсликувачка евиденција во база на податоци која би ги содржела истите информации, вклучувајќи и фотографија на сопственикот на патната исправа. Понатаму, не постоеле електронски траги во системот преку кои би можело да се открие службеното лице кое го извршило фалсификатот на патната исправа.

Случајот укажува на недостиг како на технички така и на мерки за заштита со мониторинг/ревизија против злоупотреба.

Патните исправи имаат меѓународна употреба, па овој случај, исто така, укажува и на потребата за електронска размена на податоци и потврда меѓу земјите, како што е случајот меѓу земјите од Шенген зоната.

Случај 2 од Црна Гора: Искористување на информатичката технологија за нанесување политичка штета

Ова е случај каде до медиумите бил испратен погрешен телефонски листинг каде наводно високо службено лице комуницирало со членови на организирана криминална единица.

Горенаведениот пример јасно укажува на прашањето на потенцијална кривична одговорност на одговорни лица во фирмата оператор, посебно во однос на доверливоста и на следењето и злоупотребата на електронската пошта.

Најважната сопственост на фирмата се податоците. Губењето на податоци ја изложува фирмата на судски процес и губење на угледот. Информациите кои се чуваат во базата на податоци се важни. Фирмите рутински чуваат чувствителни, приватни и сопственички информации, како што се бројот на социјално осигурување, кредитни картички, податоци за плати и лични податоци. Фирмите мора да ги чуваат и обезбедат овие информации на доверлив начин, во спротивно се изложуваат на ризикот да го изгубат својот углед и/или приход.

Операторот е обврзан да ги обезбеди потребните технички и организациски услови кои овозможуваат следење на комуникациите, односно да им овозможи на надлежните државни органи да ги добијат задржаните податоци во однос на нивното движење и локацијата, но исклучиво со одлука на судот, доколку тоа се смета неопходно за спроведување на судската постапка (согласно со законот за кривична постапка), или за целта на безбедноста на Црна Гора (посебно според законодавството со кое се уредува работата на разузнавачките служби).

Овој случај немаше судски епилог и не беше утврдена никаква објективна или субјективна одговорност. Така, не може да се утврди со точност кои мерки за заштита во случајот недостасувале.

Случај 3 од Црна Гора: Злоупотреба на функции и внесување на неточни податоци во јавните регистри

Овој случај се однесува на нелегален трансфер на државно земјиште во општинскиот катастар на трето лице преку незаконски измени во катастарот. Случајот вклучува изготвување на погрешен електронски фалсификат кој подоцна би можел да се искористи во судска постапка.

Во Црна Гора постои комбинација на различни електронски и физички регистри на земјиште. Сепак, секоја година бројот на регистри расте. Некои од регистрите се дигитализирани, а податоците во некои случаи може да се споделат по електронски пат. Истите документи може да имаат различно потекло, па понекогаш невозможно да се утврди со точност кој ги подготвил и кој има целосен пристап до нив. Во овој случај, предвидениот услов е документот да се чува електронски, а пристап до регистрите може да имаат само овластени лица.

Како принцип на безбедност, вработените мора да го имаат токму она ниво на привилегираност на пристап кое е неопходно за спроведување на нивната функција или задача. Давањето привилегиран пристап на корисникот кој ја надминува неговата потреба е вообичаена пракса која може да доведе до злоупотреба на прекумерен привилегиран пристап.

Следењето на корисниците помага да се обезбеди:

- Приватноста на податоците, така што само овластени апликации и корисници може да имаат увид во чувствителните податоци.
- Управување со податоците, така што структурата и вредностите на важните бази на податоци нема да се менуваат вон корпоративните процедури за контрола на измени.

Овој случај илустрира што може да се случи кога не е обезбедено доволно следење на пристапот на вработените. Понатаму, во постапката на измени на општинскиот катастар недостасуваат организациски и процедурални мерки за заштита, како што е 'принципот на повеќе очи'. Не била спроведена никаква вкрстена проверка на статусот на земјиштето и сопственоста, ниту техничка ниту од страна на друго вработено лице во општинскиот катастар, ниту пак преку надворешна ревизија.

Случај 4 од Црна Гора: Незаконско издавање на патни исправи

Во Полициската дирекција во Подгорица две барања за издавање нови патни исправи не биле потврдени од страна на службеникот кој работи со такви случаи. Сепак, истражителите не нашле никакви електронски записи во информатичките системи во однос на издавањето на патните исправи, а целокупната документација за скенираните барања за пасоши исчезнала од просторијата за архивирање.

Овој случај покажува дека во информатичките системи не постоеле електронски записи на скенираните барања за издавање патни исправи, нешто што би го елиминирало ризикот за користење и издавање на фалсификувани документи. Исто така, потребно е да се подобри безбедноста на електринскиот систем и евидентирањето на физичкиот пристап до просториите каде што се чуваат датотеките и службените документи.

Компјутерите за управување со базата на податоци и информатичките системи (серверот) треба да бидат опремени со:

- Систем за безбедно логирање и евидентирање на сите пристапи, така што пристапот до серверот може да биде контролиран и ограничен; и
- Механизам за спречување неовластено повлекување и депонирање на подвижни ИТ медиуми, комуникациски портови или конекции за печатење на податоци.

Проверката на автентичност е потврда на идентитетот од страна на системот или базата на податоци врз основа на презентирање единствени акредитиви (веродостојна потврда) во системот. Проверката на автентичност придонесува кон доверливоста на податоците и отчетноста на дејствата во системот преку потврдување на единствениот идентитет на корисникот. Пристапот до телекомуникации, компјутер и апликациски системи за обработка на податоци треба да се дозволи единствено преку внесување на соодветното корисничко име и точната лозинка.

Сè поголем број на апликации и веб услуги на е-Влада бараат и дозволуваат проверка на автентичност и дигитален потпис преку користење на дигитален идентитет. Во овој случај важно е сите релевантни документи да бидат лоцирани на едно место – електронски регистар – а пристапот до регистарот да им биде дозволен само на овластени вработени лица кои поседуваат соодветен дигитален сертификат.

Внатрешниот Орган за сертификација (ОС) во Министерството за информатичко општество и телекомуникации (GOV.ME) беше формиран со цел да овозможи користење на дигитални сертификати кои ќе обезбедат безбедна и сигурна комуникација меѓу државните органи. Од самиот почеток, употребата на дигиталниот сертификат во јавната администрација активно се промовира и спроведува од страна на Министерството за информатичко општество и телекомуникации (МИОТ). Услугите на е-влада, како во МИОТ така и во другите институции имаат за цел да го зголемат користењето на дигиталните сертификати, првенствено заради безбедната размена на податоци и идентификација на корисникот.

Мерки за спречување на ИТ корупција во Црна Гора

Во изминатава деценија, во Црна Гора се зголеми свесноста за корупцијата и оваа тема стана важен приоритет на политичката агенда на земјата. Последователните влади на Црна Гора се заложија за борба против корупцијата и превземени се клучни

произлегуваат од процесот на пристапување кон Европската унија и последователната потреба за прилагодување на државното законодавство кон *acquis communautaire*.

Информатичките и комуникациските технологии се неопходен дел од модерното живеење. Интегрирањето на ИКТ во спроведувањето на секојдневните активности и задачи станува сè поочигледно. Во таа смисла, закани по информатичката и комуникациската структура кои би можеле да ги загрозат достапноста, приватноста и интегритетот, може, исто така, да влијаат врз функционирањето на општеството во целост. Постојат многубројни ИКТ алатки кои може да се користат за време на различните фази на борба против корупцијата, вклучувајќи спречување, откривање, анализа и корективни дејства.

ИКТ не е магично стапче кога станува збор за обезбедување поголема транспарентност и помалку корупција, или зацврстување на демократијата.

- ИКТ може да ги олесни споделувањето на информации и социјалната мобилизација и конечно да обезбеди дигитални платформи каде граѓаните би можеле анонимно да пријавуваат случаи.
- ИКТ може да го олесни работењето на организациите од граѓанското општество кои работат во насока на обезбедување поголема транспаретност и се борат против корупција преку поддржување на комбинирани методи на водење кампањи за транспарентост и одржување обуки за граѓаните во однос на тоа што значи корупцијата и кои се нивните граѓански права.
- ИКТ може да ја подобри транспарентноста во јавниот сектор преку зголемување на координацијата, ширењето на податоци и административниот капацитет на јавните сектори, како и да ја подобри испораката на услуги преку интегрирање на административни системи лесни за користење од страна на корисниците.

ИКТ, исто така, може да има и подиректни интервенции. Преку процеси на автоматска обработка можно е значително да се намали можноста за корупција преку отстранување на човечкиот фактор од местата на собирање на податоците и испораката на услуги – кога лицата се вклучени во е-банкарство не постои службеник за поткуп.

Овде се наведени неколку типови на корупција во борбата против кои ИКТ начелно може да помогне:

- Автоматска обработка: отстранување на човечкиот фактор, а со тоа и на можноста за корупција во оперативното работење
- Транспарентност: отстранување на можноста за дискреција
- Откривање при оперативното работење: деталите и агрегатите од оперативното работење може подеднакво да се следат со цел да откријат аномалии и неочекувани перформанси
- Превентивно откривање: може да се следат интернет-поврзаните социјални мрежи и поединци со цел откривање подготовки за преземање коруптивни дејства
- Зголемување на свесноста: доколку јавноста е свесна за владините правила и процедури се зголемува можноста за давање отпор на арбитрарен третман
- Пријавување: мобилизацијата на корисниците/заедницата за пријавување на случаи ќе го олесни преземањето на корективни дејства кон поединци и реорганизирањето на системите со цел да се избегнуваат “дупки” во работењето
- Одвраќање: објавувањето информации за пријавени случаи на корупција како и соодветните показатели (како што е дисбалансот меѓу приходот и имотот) ќе ги одвратат државните службеници од евентуално вклучување во коруптивни дејства.
- Промовирање на етички пристап: ангажирање на јавноста преку водење дискусии на различни интернет форуми.

Многу е важно да се воспостават процедури за безбедност на податоците со цел да се избегне каков било проблем на полето на злоупотреба на ИТ. Исто така, важно е да се дефинираат одредени мерки за заштита против злоупотреби на информатичката технологија чија цел е извршување на коруптивни дејства.

Законска рамка

Правните документи кои ја формираат основата на функционирањето и понатамошната надградба на модерниот концепт на информатичкото општество во Црна Гора се:

- **Законот за мерки за информациска безбедност** (Службен весник на Република Црна Гора бр. 14/10), го предвидува спроведувањето на мерки и стандарди за информациска безбедност, вклучувајќи ја и состојбата на доверливост, интегритет и достапност на податоците. Овој закон се однесува на државните органи, државната власт, локалната власт, правните субјекти и поединци кои имаат пристап или кои обезбедуваат обработка на податоци. Овој закон не се однесува на информации кои подлежат на информациската безбедност уредена согласно со регулативите за доверливост на податоците;

- **Законот за електронски потпис** (“Службен весник на Република Црна Гора”, бр. 55/03 и “Службен весник на Црна Гора”, бр. 41/10) го уредува користењето на електронскиот потпис во правни, управни, судски и други постапки, како и правата, обврските и одговорностите на правните и физички лица во однос на електронските сертификати, освен ако не е уредено со други регулативи;

- **Законот за електронски документи** го уредува начинот на користење на електронските документи во правна, управна, судска и друга постапка, како и правата и одговорностите на деловните друштва, претприемачите, правните и физички лица, владините тела, државната власт, локалната власт и агенциите и организациите кои вршат јавни овластувања во однос на електронските документи;

- **Закон за класифицирани информации** – правната рамка за процедури за безбедност при размена на класифицирани информации е воспоставена и ги вклучува Законот за класифицирани информации и Кривичниот законик, како и Регулативата за начинот и постапката за назначување на класификација на информациите и Регулативата за евиденција на класифицирани информации;

- Законот за ратификација на **Конвенцијата за компјутерски криминал** – Црна Гора го усвои Законот за ратификација на Конвенцијата за компјутерски криминал на 3 март 2010 год., кој стапи на сила на 1 јули 2010 год. Кривичните дела кои согласно со оваа Конвенција се предвидени како компјутерски криминал вклучуваат широк опсег на ширење вируси, неовластен пристап до компјутерска мрежа преку пиратерија до порнографија и упад во банкарските

системи, злоупотреба на кредитни картички и сите други кривични дела во кои се користат компјутери.

Други важни документи кои треба да се споменат се:

- Студија со дефинирани одговорности на државните органи во борбата против компјутерскиот криминал, вклучувајќи проценка на состојбата во државата и подготвеност во областа на компјутерска безбедност;
- Уредување на деталните услови и начин на спроведување на ИТ мерките за заштита на класифицирани информации;
- Уредување на деталните услови и начин на спроведување на мерките за заштита на класифицираните информации;
- Уредување на деталните услови и начин на спроведување индустриски мерки за заштита на класифицирани информации;
- Уредување на работата и содржината на внатрешната контрола преку спроведување на мерки за заштита на класифицирани информации.

Безбедносни контроли

Потребно е да се обезбедат безбедносни контроли во однос на ИТ корупција. “Контролите на безбедноста на информациите се збир од технички, процесни и политички мерки за заштита кои се изработени да ги заштитат чувствителните податоци преку намалување на утврдените и проценетите ризици во однос на нивната доверливост, интегритет и достапност”[83]. Во рамките на Министерството за информатичко општество и телекомуникации постои Директорат за информатичка инфраструктура во кој функционираат следниве три сектори: Сектор за проектна анализа, планирање и мониторинг; Сектор за инфраструктурни услуги; и Сектор за одговор на компјутерски и безбедносни инциденти на интернет - CIRT. Главните цели на CIRT се:

Спречување, постапување по и отстранување на последиците од компјутерските безбедносни инциденти на интернет и другите ризици по безбедноста на информатичките системи:

- Спречувањето се отсликува во проактивниот начин на дејствување, кој вклучува обезбедување на информации и проценка на информациската безбедност, тестирање на ранливоста, собирање, евидентирање и обработка на податоци за инцидентите, тестирање и спроведување на нови софтверски и хардверски системи за заштита на ИТ ресурси;
- Обработката на податоците и отстранувањето на последиците вклучуваат: утврдување на појавата и степенот на сериозност на инцидентот, причината за инцидентот, посредништво во комуникацијата меѓу сите засегнатите страни во инцидентот; известување за други компјутерски инциденти на интернет / управување со инциденти во компјутерската безбедност CIRT /Тимови за одговор на компјутерски инциденти/ CSIRT тимови, подготовка на извештаи и предупредување за останатите корисници, отстранување на ранливоста на системот, заштита на системот од евентуални инциденти и форензичка анализа.

Обуката на корисниците на полето на информациската безбедност вклучува:

- Објавување публикации, прирачници, софтвер алатки и други корисни информации кои се однесуваат на побезбедно користење на информатичката технологија, кои се достапни на веб порталот (www.cirt.me);
- Организирање курсеви и обука на тема ИТ безбедност и можни начини на заштита и спречување на инциденти кои ја засегаат компјутерската безбедност.

Министерството за информатичко општество и телекомуникации ги има изработено следниве правилници:

- Правилник за мерките и процедурите за заштита на сертификатите и податоците кои се однесуваат на потписниците. Овој правилник ги уредува организациските и техничките мерки за заштита на системот за сертификација во однос на заштита на сертификатите и квалификуваните сертификати, податоците кои се однесуваат на потписниците, како и воспоставувањето и примената на системот за заштита на пристап до сертифицирани записи;
- Правилник за стандарди на информациска безбедност – воспоставување на стандарди на информациска безбедност кои се применуваат во спроведувањето на мерките за информациска безбедност предвидени со регулативите на Владата на Црна Гора;
- Правилник за управување со инциденти во информациската безбедност – Тимот за одговор CIRT ќе развие и одржува план за одговор на инциденти во информациската безбедност кој ќе биде отсликан во дефинирањето на процедурите кои се однесуваат на управувањето со инциденти;
- Правилник за содржината и начинот на чување евиденција и регистар на даватели на услуги на сертификација. Овој документ ја уредува содржината и начинот на чување на евиденцијата за давателите на услуги на сертификација; како и минимум нивото на осигурување против ризик на одговорност за евентуална сторена штета за време на обезбедувањето на услугите на сертификација.;
- Правилник за електронски потпис и напредни мерки за заштита на електронскиот потпис. Со овој Правилник се регулира електронскиот потпис и напредните мерки за заштита на електронскиот потпис, мерките за потврда на идентитетот на потписникот или на давателот на услуга на сертификација во Црна Гора, технички и технолошки процедури за напредно креирање на електронски потпис и услови кои уредите за напредно креирање на електронски потпис мора да ги исполнат;

83 http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Controls-and-Safe- guards.pdf

- Правилник за начинот и условите за административен пристап до веб порталот на Владата на Црна Гора;
- Правилник за користење на ресурси за сметање и комуникации во мрежата на државните органи;

Изјава на пракса за сертифицирање - CPS.

Информацискатa безбедност, исто така, мора да ги исполни условите за доверливост, интегритет и достапност на податоците. Информацискатa безбедност се фокусира на податоците, без оглед на нивната форма: електронски, печатени или податоци во друга форма.

Како резултат на постојаниот пораст на бројот на услуги кои државните органи и субјектите од приватниот сектор им ги обезбедуваат на граѓаните како и на други правни субјекти, неопходно е да се развие клучна информатичка инфраструктура во Црна Гора и да се развијат процедури за заштита.

Клучни активности:

- Дефинирање и заштита на клучната информатичка инфраструктура;
- Зголемување на отпорот на информатичките системи против појава на инциденти;
- Правење анализа на заканите по ИТ инфраструктурата.

Заштита на податоци

Во Министерството за информатичко општество и телекомуникации, формиран е Тим за одговор на компјутерски ургентни состојби /Тим за одговор на инциденти кои ја загрозуваат компјутерската безбедност - CERT/CSIRT (одделение за заштита против компјутерски и безбедносни инциденти на интернет). Потпишана е Административна спогодба помеѓу Министерството за информатичко општество и телекомуникации и Меѓународната телекомуникациска унија со цел да се добие специјализирана техничка помош за потребите на утврдување на Тимот за одговор на компјутерски инциденти - CIRT (Национален тим за обработка и заштита од компјутерски инциденти) кој ќе работи во соработка со мрежата на CIRT формирана од Меѓународното мулти_латерално партнерство против компјутерски закани (IMPACT).

Преку системот на инспекциски надзор, обезбедено е спроведување на Законот за информациска безбедност и на Регулативата за мерките за информациска без_бедност која придонесува кон зголемување на степенот на заштита на податоци.

Примарното членство на CIRT.ME се дефинира како:

- Сите владини институции во Црна Гора;
- Клучната државна инфраструктура во Црна Гора.

Црногорскиот Тим за одговор на компјутерски инциденти CIRT беше формиран согласно со Законот за информациска безбедност на Црна Гора во рамките на Ми_нистерството за информатичко општество и телекомуникации (MIST). Формиран како одвоена организациска единица при Министерството, тимот работи во рамките на Одделението за ИТ инфраструктура и ја покрива областа на државниот CIRT. Тимот е вклучен во справувањето со инциденти во информацискатa безбедност во случај една од страните вклучени во инцидентот да се наоѓа во Црна Гора (доколку припаѓа на доменот ".me" или доколку е во просторот на црногорска IP адреса).

Мисија на CIRT (Тим за одговор на компјутерски инциденти)

- CIRT ќе ги координира и ќе им помогне на владините агенции во спроведувањето на проактивни услуги за намалување на ризиците од појавата на инциденти во компјутерската безбедност, и ќе одговори на такви инциденти во случај на нивно појавување;
- CIRT.ME ќе спроведува кампањи за зголемување на свесноста со цел локалното население да се информира за несаканите ефекти од компјутерските закани и компјутерскиот криминал.

Во рамките на административната поставеност мора да постои утврдена организа_циска хиерархија со цел да се обезбеди најефективното долгорочно, одржливо и соодветно управување со информацискатa безбедност.

И покрај оскудноста на сигурни податоци, постои барем некаков доказ дека ин_фор_матичко комуникацискатa технологија може да биде ефикасна алатка во борбата против корупција. Сепак, потенцијалот на ИКТ ќе може да се оствари само во ком_бинација со реални административни реформи.

Технички мерки за заштита

Овие хардверски и софтверски контроли за заштита на LAN и WAN од неовластен пристап или злоупотреба помагаат во откривање на случаи на злоупотреба или повреда на безбедноста и обезбедуваат безбедност при примена на LAN. Техничките мерки за заштита вклучуваат идентификација и потврда на корисникот, контроли на авторизација и пристап, контроли на интегритет, механизми за следење на процесот на ревизија, контрола на доверливост, и превентивни контроли на одржување на хардвер опремата.

Лозинките се примарниот метод на контрола на пристапот до ресурси и се најчестиот механизам за потврда на идентитетот[84]. Министерството за информатичко опште_ство и телекомуникации (MIST) е одговорно за администрирање на владината мре_жа. MIST обезбедува Мониторинг и администрација на Мрежата: Функцијата на ИТ

84 books.google.de/books?isbn=0080558712

операциите вклучува одговорност за одржување на комуникациската поврзаност и обезбедување за корисниците соодветно ниво на пристап во мрежата. Во однос на лозинките, на ниво на целокупната владина мрежа утврдена е политика секој месец да се креира нова лозинка.

Контролна идентификација

Предизвик за организациите е да утврдат соодветен збир на безбедносни контроли кои, доколку се спроведат и покажат како ефикасни во нивната примена, би биле во сообразност со предвидените безбедносни барања за намалување на влијанието или веројатноста на одредена утврдена закана. За секоја безбедносна категорија потребно е да се спроведуваат различни контроли со цел да се воспостави сеопфатна и цврста рамка за безбедност.

Користењето на криптографија при заштита на податоците на корисниците од изворот до крајната дестинација, познато како криптирање од крај до крај, е силна алатка за обезбедување безбедност на мрежата.

Министерството за информатичко општество и телекомуникации на Владата на Црна Гора (MIST) управува со инфраструктурните јавни клучеви (GOV.ME-PKI) за интерните цели на јавната администрација во Црна Гора. Во Министерството е формирано тело за сертификација во рамките на единствениот Орган за сертификација кое ги сертифицира државните службеници на Министерството за информатичко општество и вработените во Владата на Црна Гора. Овој систем целосно се спроведува согласно со правосилното законодавство, првенствено со Законот за електронски потпис.

Во моментов се планира да се започне со користење дигитални сертификати за логирање во секој личен компјутер PC во владата, но недостигот на средства сè уште претставува проблем и пречка за спроведување на таквата мерка.

Пренос на податоци

Преносот на чувствителни податоци, било преку FTP, систем-до-систем, или пренесување преку веб образец, треба да се спроведе само преку сигурна патека или медиум преку контроли за обезбедување на доверливоста, интегритетот и веродостојноста на содржината. Сите поврзувања од внатрешен систем или база на податоци кон други системи надвор од границите на акредитација треба да се авторизира само врз основа на склучени договори за поврзување на системот, а поврзувањето потребно е постојано да се следи и контролира.

Потребно е да се користат цврсти протоколи за криптографија и безбедност со цел да се осигура преносот на податоци преку отворени, јавни мрежи. Преносот на лични информации од надворешни субјекти кон организацијата, кој вообичаено се прави преку веб страниците, треба да се спроведе преку сигурен сервер со користење на високо ниво на криптирање.

Во моментот, преносот или размената на податоци се прават преку сигурни веб услуги за целите на специјализираните ИТ системи. Поврзувањето се обезбедува преку сигурна мрежа и е криптирано со дигитални сертификати.

Специјализираниот систем за размена на податоци сè уште останува да биде предизвик за Црна Гора. Во моментот сме во фаза на подготовка на проектот со назив “Enterprise service bus” кој ќе им овозможи на владините институции меѓу себе да вршат безбедна размена на податоци. Сепак, недостигот на средства останува да биде проблем во спроведувањето на овој проект.

Далечински пристап

За далечински пристап се смета секој пристап до ресурсот на информации во организацијата кој го има корисникот или системот кој комуницира преку надворешна мрежа или поврзување кое е контролирано надвор од организацијата. Организацијата може да заклучи дека е неопходно да обезбеди далечински пристап до податоците и системите за работниците кои се оддалечени од работната средина или да поддржи операции на далечински локации. Во некои случаи, доставувачите на опрема периодично бараат далечински пристап со цел да прават редовна или ургентна поддршка на системот.

Во Владата на Црна Гора само замениците министри и министрите може да имаат далечински пристап до своите компјутери на ГОВ мрежата.

Во Црна Гора, 88.3% од испитаните трговски друштва изјавија дека во своето работење користеле компјутери во текот на месец јануари 2012 год. Според резултатите од испитувањето, во јануари 2012 год. 53.3% од трговските друштва (кои користеле компјутери во своето работење) им дозволиле на своите вработени далечински пристап до системот на електронска пошта, документите или апликациите на трговското друштво.

Како резултат на зголемените ризици поврзани со пристап надвор од сигурните параметри, организациите потребно е да спроведуваат политики и процеси кои ги уредуваат условите под кои далечинскиот пристап се дозволува или укинува. Далечинскиот пристап треба да се дозволи врз основа на одобрените деловни потреби, да биде ограничен на минимум неопходните привилегии, и да бара одобрување кое периодично ќе се разгледува или оправдува.

Во Црна Гора, само 27.9% од трговските друштва имаат донесено Правилник кој нормативно ги уредува прашањата на информациска безбедност. Исто така, мал процент,

односно само 26.9%. од трговските друштва, спроведуваат проценка на знаењето на вработените во однос на мерките за информациска безбедност.

Координираната поставеност на организациските, институционалните и капацитетите на управување, како и подобрувањето на законите и регулативите се важни прашања за постоењето на информацискатa безбедност во Црна Гора.

Србија

Подготвено од Немања Ненадиќ и Бојан Цветковиќ

Случај 1 од Србија: Сексуален акт во Белградска Арена

Според упатствата на Комесарот за информации од јавна важност и заштита на лични податоци, Министерството за внатрешни работи (МВР) усвои краткорочни, среднорочни и долгорочни мерки за заштита од корупција поврзана со информатички технологии.

Краткорочни мерки за заштита:

- Технички мерки за заштита;
  - Потребно е да се евидентира секој вид на технички пристап до каков било тип на ИТ системи;
  - Се воведоа системи за физичка безбедност како мерка за ограничување и контрола на пристапот до центарот на податоци на МВР во кој централно се чуваат сите податоци;
- Организациски и процедурални мерки за заштита:
  - Пристапот до податоци треба да биде проследен со официјално барање и одобрување (дозвола) од судот (или од канцеларијата на обвинителството) надлежни за разгледување на конкретниот случај (случаи);
  - Бројот на вработени кои имаат директен оперативен пристап до податоците е намален на минимумот потребен за нормално функционирање;
  - Употребата на електронски преносни медиуми во просториите во кои се чуваат податоците целосно се забранува и истиот е придружен со конкретни процедури за пристап до податоци или е забранет во целост (зависно од видот на објектот);
- Мерки за следење;
  - Инсталиран е посебен систем за видео надзор со кој се врши директен мониторинг на пристапот до главниот центар на податоци.

Среднорочните мерки за заштита од ИТ корупција вклучуваат:

- Обука и подигнување на свеста;
  - Обука за вработените во Министерството за правда во однос на ризиците поврзани со ИТ корупција
- Контрола на ИТ системите;
  - Министерството за правда веќе воведе внатрешна контрола на ИТ;
  - Министерството за правда во блиска иднина планира да воведе ISO 27001 и ISO 20000 стандардизација.

Долгорочните мерки за заштита од ИТ корупција вклучија:

- Правни мерки за заштита;
  - Внатрешните административни регулативи беа ажурирани со цел да вклучат забрана за неовластен пристап до податоците во Министерството за правда;
  - Внатрешните административни регулативи беа ажурирани со цел да обезбедат пристапот до податоци да е во согласност со “раздвојувањето на власта” помеѓу министерството, надлежните судови, обвинителствата и затворите;
  - Ажурирани се внатрешните административни регулативи кои се однесуваат на употребата и примената на посебни видови електронски преносни медиуми (оптички дискови, мемориски уреди, смарт телефони, дигитални камери итн.) со цел да се спречи нивната употреба на местото на главниот центар на податоци во Министерството за правда;
  - Членот 42, ставот 3 од Уставот експлицитно го спречува и казнува користењето на лични податоци надвор од целите на нивното прибирање.

Случај 2 од Србија: Кога изведувачот за ИТ “фаќа корен”

Преку овој вистински случај се разоткри зависноста на Министерството за правда од неговиот надворешно ангажиран ИТ персонал и големиот број на различни видови ризици поврзани со ангажирањето надворешни ИТ експерти. Преземените мерки за заштита вклучија краткорочни, среднорочни и долгорочни мерки со кои значително се намалија ризиците поврзани со ангажирање надворешни ИТ експерти.

Краткорочните мерки за заштита од ИТ корупција вклучија:

- Технички мерки за заштита;
  - Потребно е да се евидентира секој вид на технички пристап до каков било тип на ИТ системи;
  - Се воведоа системи за физичка безбедност како мерка за ограничување и контрола на пристапот до центарот на податоци на МВР во кој централно се чуваат сите податоци;
- Организациски и процедурални мерки за заштита

- Пристапот до податоци треба да биде проследен со официјално барање и одобрување (дозвола) од судот (или од канцеларијата на обвинителството) надлежни за разгледување на конкретниот случај (случаи);
- Никој, ниту ни највисокиот ешалон на вработени во МВР, нема пристап до податоците без да добие претходно одобрување (дозвола) од судот (канцеларијата на обвинителството);
- Секој суд (или канцеларија на обвинителството) може да има пристап само до своите податоци – пристапот до податоци кои им припаѓаат на други субјекти е забранет;
- Лицата кои се однадвор ангажирани како ИТ експерти немаат пристап до главниот центар на податоци без обезбедена придружба од минимум двајца вработени од Министерството;
- Бројот на вработени кои имаат директен оперативен пристап до податоците е намален на минимумот потребен за нормално функционирање;
- Секој вид на надградба и ажурирање на ИТ системите треба да се прави во главниот центар на податоци – никому не е дозволено да има далечински пристап;
- Употребата на електронски преносни медиуми во просториите во кои се чуваат податоците целосно се забранува;

• Мерки за следење;
  - Инсталиран е посебен систем за видео надзор со кој се врши директен мониторинг на пристапот до главниот центар на податоци.

Среднорочните мерки за заштита од ИТ корупција вклучуваат:

• Обука и подигнување на свеста;
  - Обука за вработените во Министерството за правда во однос на ризиците поврзани со ИТ корупција
• Контрола на ИТ системите;
  - Министерството за правда веќе воведе внатрешна контрола на ИТ;
  - Министерството за правда во блиска иднина планира да воведе ISO 27001 и ISO 20000 стандардизација.

Долгорочните мерки за заштита од ИТ корупција вклучија:

• Правни мерки за заштита;
  - Внатрешните административни регулативи беа ажурирани со цел да вклучат забрана за неовластен пристап до податоците во Министерството за правда;
  - Внатрешните административни регулативи беа ажурирани со цел да обезбедат пристапот до податоци да е во согласност со "раздвојувањето на власта" помеѓу министерството, надлежните судови, обвинителствата и затворите;
  - Ажурирани се внатрешните административни регулативи кои се однесуваат на употребата и примената на посебни видови електронски преносни медиуми (оптички дискови, мемориски уреди, смарт телефони, дигитални камери итн.) со цел да се спречи нивната употреба на местото на главниот центар на податоци во Министерството за правда;
  - Закон за јавни набавки ("Службен весник на Република Србија", бр. 124/12).

Случај 3 од Србија: Генералниот директор ги шпионира вработените

Не е познато кои мерки биле преземени со цел да се спречи злоупотребата на ИТ во Агенцијата за приватизација откако презентираниот случај јасно посочи на слабости во човечкиот фактор во Агенцијата за приватизација, кој беше клучната и фокална точка за вршење злоупотреба на ИТ.

Случај 4 од Србија: "Мафија на патиштата"

Според наведеното во пресудата за случајот "Мафија на патиштата", мерките за заштита од ИТ корупција со години не функционирале. Членовите на бандата навремено биле информирани за контролите, така што имале доволно време да ги скријат доказите на криминалот. Контролите обично се спроведувале после 18 часот, кога бандата не дејствувала. Понатаму, наспроти фактот што досието EMU-87 било фалсификат и се разликувало од оригиналот, вистината веќе со години останува неразјаснета. Со оглед на тоа што електронскиот систем за наплата и регистрација на возила "нормално" функционирал, таквиот прекин не бил утврден со ниедна контрола. Вработениот од фирмата која го одржувала електронскиот систем на "Србија Пат" имал административни овластувања и се чини дека никој од "Србија Пат" не вршел надзор на нивното работење.

Системот за регистрација на поединечни наплаќачи на патарина кои поседувале единствен документ за лична идентификација во пракса не функционирал. Идентификациските броеви биле видливи за колегите, а раководителите на смена често ги менувале вработените.

Краткорочните мерки за заштита од ИТ корупција вклучија:

• Технички мерки за заштита;
  - Инсталиран е дополнителен но одвоен сензорски ИТ систем со кој ќе се следат типовите и бројот на возила кои поминуваат на патариниte (сега статистичките податоци од оригиналниот систем мора да се совпаднат со оние од новиот сензорски систем)

- Воведени се системи за физичка безбедност како мерка за ограничување и контрола на пристапот до просториите во кои се чуваат податоци за корисниците.

Немаме информации дали биле преземени организациски, процедурални и мониторинг мерки и од каков вид биле тие мерки.

Немаме информации дали и каков вид на краткорочни мерки за заштита од ИТ корупција биле преземени.

Долгорочните мерки за заштита од ИТ корупција вклучуваат воведување нов вид услуга за плаќање на патарина наречен “ENP” (на англиски јазик: “електронско плаќање на патарина”) кој целосно се заснова врз електронското плаќање со NFC картички со цел да се спречи каков било директен пренос на готовина меѓу лицата вклучени во наплатата на патарина.

Проактивно објавување на информации – алатка за спречување на ИТ корупција

Српскиот Закон за слободен пристап до информации (“Службен весник на Република Србија”, бр. 120/04, 54/07, 104/09 и 36/10) предвидува задолжително објавување на “Информативен прирачник” за сите јавни установи (финансирани од Буџетот) а содржината на овој документ е дефинирана со ’Упатството на Комесарот’ (последно издание од 2010 година)[85]. Информативниот прирачник се објавува електронски и истиот се ажурира најмалку еднаш месечно. Оваа публикација има за цел да обезбеди голем број корисни информации во однос на отчетноста на владините тела во врска со податоците за јавни набавки, буџет, донации и државна помош. Останатите информации се однесуваат на структурата на владините тела или услугите што им ги обезбедуваат на граѓаните. Сепак, за целите на оваа анализа, најважните делови од законот се одредбите од членот 37, 38 и 39.

Членот 37 го уредува “чувањето на носителите на информации”. Носители на информации се медиуми во кои се чуваат податоци, како на пример хартија, хард дискови, бази на податоци, видеоленти, итн. Јавниот орган мора да ги утврди различните видови на такви медиуми кои се користат за чување на информации, според типот, количината (точна или проценета), како и според типот на податоци кои ги чуваат. Понатаму, органите мора да утврдат каде се чуваат таквите “носители на информации” (организациски единици или посебни места во органот, како што се архиви, библиотеки или електронски бази на податоци) како и местата за чување во овие простории (на пример, метални шкафчиња, полици со датотеки, заеднички сервер или посебна компјутерска опрема). Од јавните органи се бара да дадат краток опис на кој начин носителите на информации се чуваат и одржуваат во пракса (дали се обезбедува безбедно снимање на податоците на некој друг носител, дали компјутерите се заштитени од вируси, дали некое друго лице освен вработените има пристап до носителот на информации, дали се врши периодичен преглед на усогласеност со барањата за чување на носители на информации итн.) и да посочат дали условите за чување соодветствуваат со регулативите или потребата или да упатат на потребата за нивно чување во случај да не постојат такви регулативи.

Според членот 38 и 39 јавните органи треба задолжително да објавуваат информации за типот на информации со кои располагаат како и за типот на податоци за кои се обезбедува пристап. Типот на информации би можел, на пример, да биде следниот (според наведеното во Упатствата):

- збир на регулативи
- издадени мислења
- записници од состаноци
- одлуки
- жалби
- склучени договори
- звучни и видео записи од настани организирани од државните органи
- писма од граѓани
- разни видови комуникација со јавноста
- документи за плати, вработени, јавни набавки
- нацрт документи во подготовка
- службени записи
- барања и молби на клиенти и сл.

Информациите за достапноста на податоците треба да се обезбедат на начин кој ќе овозможи споредба со листата на поседуваните типови на информации. Доколку информациите се точни и сеопфатни, јавноста може да ги смета органите за отчетни и, меѓу другото, да спречи ситуации во кои државни службеници би тврделе дека одредени информации не се во надлежност на тој орган или дека се изгубени итн. Во реалноста, најголем дел од органите не се придржуваат кон оваа норма и не обезбедуваат детални информации за носителите на податоци ниту информации за типот на податоци. Оваа состојба се очекува наскоро да се надмине со очекуваните измени на Законот за слободен пристап до информации со што процедурите за надзор и санкции ќе станат поефикасни.

85 http://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/uputstvo-informator/uputstvoen.doc

Кривичните прекршоци се предвидени со законот, спроведувањето е непознато

Кривичниот законик на Република Србија (Службен весник на РС, бр. 85/2005, 88/2005, 107/2005) со дополнетите измени од 31 август и 29 декември 2009 година, и 24 декември 2012 година, во глава XXVII предвидуваат санкции за сторени кривични прекршоци против безбедноста на компјутерските податоци.

Првиот кривичен прекршок во оваа група е "*Оштетување на компјутерските податоци и програми"* (член 298). Лицето може да се казни парично или со казна затвор во времетраење од една година доколку тој/таа *"без овластување ги избрише, измени, оштети, прикрие или на друг начин ги направи неподобни за употреба компјутерските податоци или програми"*. Во случаи во кои причинетите штети се поголеми, тоа може да значи казна затвор до пет години. Опремата и уредите кои се користеле во извршувањето на кривичното дело ќе бидат одземени.

"Компјутерската саботажа" (член 299) предвидува казна до пет години затвор за:

"лицето кое влегува, уништува, брише, оштетува, прикрива или на друг начин ги прави неподобни за употреба компјутерот или програмата или кое ги оштетува и уништува компјутерот или другата опрема за електронска обработка и пренос на податоци со намера да спречи или значително да ја наруши електронската обработка и пренос на податоци кои се од важност за владините органи, претпријатија и други субјекти".

"Создавање и вметнување на компјутерски вируси" (член 300) предвидува казна до шест месеци затвор за *"оној кој создава компјутерски вирус со намера истиот да го вметне во друг компјутер или компјутерска мрежа".* Доколку сторителот "*вметне компјутерски вирус во друг компјутер или компјутерска мрежа и притоа причини штета"* казната ќе биде до две години затвор. Опремата и уредите кои се користеле за извршување на кривичното дело ќе бидат одземени.

"Компјутерската измама" (член 301) се дефинира на следниот начин:

"Секој оној кој внесува неточни податоци, кој нема да внесе точни податоци или кој на друг начин ги прикрива и лажно прикажува податоците и на тој начин влијае врз резултатите на електронската обработка и пренос на податоци со намера да си обезбеди за себе или за некој друг незаконска материјална добивка и на тој начин да причини материјална штета на другото лице, ќе биде казнет со парична казна или казна затвор до три години."

За кривични дела или причинета штета на поголема вредност, казната затвор може да биде до десет години.

"Неовластен пристап до компјутер" и до *"Компјутерска мрежа на обработка на електронски податоци"* (член 302) предвидува казна до три години затвор, зависно од штетата.

Спречувањето или ограничувањето на пристапот до јавна компјутерска мрежа (член 303) се казнува со казна затвор до три години.

"Неовластеното користење на компјутер или компјутерска мрежа" (член 304) утврдува дека:

"Секој оној кој користи компјутерски услуги или компјутерска мрежа со намера да се стекне со незаконска материјална добивка за себе или за некој друг, ќе биде казнет со парична казна или казна затвор до три месеци. Гонењето за ова кривично дело се презема по приватна тужба."

Последната измена од оваа група е *"Изработка, набавка, и давање на други средства за извршување кривични дела против безбедноста на компјутерските податоци"* (член 304а):

"Оној кој неовластено користи, произведува, набавува, продава или им дава на други за нивно користење компјутери, компјутерски системи, компјутерски податоци или софтвер наменети за извршување на едно од кривичните дела предвидени во членот 298 до 303 ќе биде казнет со казна затвор од шест месеци до три години. Предметите од ставот 1 од овој член ќе бидат одземени."

Србија, исто така, има предвидено широк опсег на кривични прекршоци кои би можеле да се користат за казнување на корупцијата (злоупотреба на моќ, земање поткуп, давање поткуп, вршење на незаконско влијание и сл.), кривични прекршоци кои се речиси целосно усогласени со релевантните меѓународни стандарди. Некој би можел погрешно да заклучи дека системот на кривичното законодавство за борба против ИТ корупција е ефикасен. Сепак, тоа не е ни блиску до вистината. Целокупниот број на случаи во кои корупцијата (ИТ или друг вид корупција) целосно се истражува и финализира е сè уште мал, а посебно случаите кои вклучуваат јавни службеници на високи позиции или големи суми на пари сè уште се крајно ретки. Ситуацијата не е ништо подобра ни кога станува збор за истрагата и начелно за криминалот поврзан со ИТ. Србија веќе неколку години има посебно одделение во обвинителството за борба против компјутерски криминал. Веб страницата на ова одделение, кое работи од 2006 година, сè уште е во "фаза на изработка"; а најновите статистички податоци се од пред три години[86].

86 http://www.beograd.vtk.jt.rs/

Стекнати поуки – Преземање мерки за заштита од корупција поврзана со ИТК во јавниот сектор на земјите од Западен Балкан

Подготвено од Луизе Томасен

Поединечните мерки за заштита кои беа наведени во воведниот дел и кои се опишани во оваа глава нагласуваат дека ниедна мерка за заштита не може да постои одвоено. Заштитата од корупција поврзана со ИТК предвидува да се донесат сите предвидени мерки за заштита бидејќи истите меѓусебно се поддржуваат и надополнуваат. Е-владата никогаш не е чисто техничко прашање. Е-владата не се однесува само на технологијата, туку исто така и на јавната администрација, на кој начин работиме, како соработуваме во рамките на владата, јавната администрација, заедницата, стопанството и општеството во целост. Е-владата никогаш не смее да се гледа засебно и независно од останатиот дел од општеството.

Борбата против корупција станува приоритет за земјите од Западен Балкан во мрежата на ReСПА. Неколку национални автори забележуваат како примерите на случај ја нагласуваат потребата за зголемена свест за конкретни прашања кои се однесуваат на корупција и е-влада, но како фокусот и мерките се разликуваат. Во Албанија, новата Влада на Албанија ја ажурираше својата агенда за борба против корупцијата и неодамна воведе нова постапка за прифаќање на информациските системи. Во Босна и Херцеговина, државните и домашните извештаи наведуваат дека корупцијата е еден од најголемите проблеми во општеството, а Извештајот на Европската комисија за напредокот на земјата во 2013 година наведува недостиг од стратегија и институции за борба против компјутерскиот криминал и закани. Во Косово, државните власти забележуваат дека не постојат никакви институции кои се занимаваат со изработка и спроведување на мерки и стандарди за заштита од корупција поврзана со ИТК, и дека многу случаи на злоупотреба на ИТК поминуваат целосно неоткриени, додека српските државни власти забележуваат дека целокупниот број на случаи во кои корупцијата (без или со вклученост на ИТК) целосно се истражува е начелно мал, а посебно случаите кои вклучуваат службеници на високи позиции или големи суми на пари. И покрај тоа што Србија има формирано посебно одделение во обвинителството за борба против компјутерски криминал уште во 2006 година, не многу информации се достапни преку тоа одделение.

Авторите од Црна Гора забележуваат дека свеста за корупција се зголемила и станала важен приоритет на политичката агенда на земјата, и тоа не само на актуелната влада. Во црногорското Министерство за информатичко општество и телекомуникации сега постои Директорат за информатичка инфраструктура со три сектори: Одделение за проектна анализа, планирање и мониторинг; Одделение за инфраструктурни услуги и заштита; и CIRT (Тим за одговор на компјутерски инциденти). Црногорските автори, исто така, укажуваат на постоењето на неколку студии и регулативи за борба против компјутерскиот криминал и заштита на информациите. Во Црна Гора, борбата против корупција е една од најважните стратешки цели на владата. Понатаму, Црногорците исто така организираат кампањи за подигнување на свеста, обука за вработените и граѓаните за начините на спречување на корупцијата, информирање за можностите за преземање правни дејства, а исто така ја демонстрираат и заложбата на владата за спроведување на Стратегијата за реформи во јавната администрација и Акцискиот план. Во Хрватска постои законодавно тело за информациска безбедност, како и посебни централни државни органи задолжени за заштита на "интегритетот и достапноста на информациските системи во процесот на планирање, дизајнирање, изработка, користење и престанок на работа на информацискиот систем".

Не би можеле да направиме директна споредба меѓу земјите со цел да утврдиме колку напреднале во борбата против корупција поврзана со ИТК со оглед на тоа што немаме статистички податоци што би го поткрепиле тоа. Сепак, преку придонесот кој го обезбедија државните органи може цврсто да заклучиме дека се прават напори на ниво на држава и изгледа дека Хрватска, Македонија и Црна Гора се поистрајни во обезбедувањето заштита на ИТК во јавниот сектор од злоупотреби и корупција од останатите земји кои се предмет на оваа студија.

Технички мерки за заштита – пристап до податоци

ИКТ во јавниот сектор може да овозможи зголемена транспарентност во однос на лицата кои имаат пристап и кои ги користат податоците од јавниот сектор. Но, од друга страна, пак, може да овозможи и поголема злоупотреба отколку што тоа би било можно без постоењето на ИТК, како што е фалсификување на податоци, незаконско добивање на податоци и уништување на податоци.

Повторно да нагласиме дека нашите примери на случај не претставуваат репрезентативен примерок, туку она што е очигледно од Табелата 3 е дека гледаме повеќе примери на фалсификувани податоци отколку примери на незаконско добивање на податоци, а најмалку случаи на фактичко уништување на податоци.

Табела 3: Примери на случај на злоупотреба овозможена преку пристап до податоци

Фалсификување податоци	Нелегално обезбедување на податоци	Уништување на податоци
Случај 3 од Босна и Херцеговина: Злоупотреба на електронскиот систем на CIPS проектот	Случај 1 од Хрватска: Јави му се на лекарот за гласови	Случај 2 од Босна и Херцеговина: Уште едно контроверзно вработување во Врховниот завод за ревизија на Република Српска
Случај 8 од Хрватска: Секоја година од патарините исчезнуваат два милиони евра	Случај 11 од Хрватска: Постар инспектор злоупотребил службени податоци за да победи на локални избори	Случај 6 од Хрватска: Полицајци ги бришат податоците за сообраќајни прекршоци и објавуваат доверливи податоци и како поткуп прифатиле печено јагне и 20 литри вино
Случај 12 од Хрватска: Немаш ни еден ден на работа? Не грижи се, секако ќе ти дадеме пензија	Случај 2 од Хрватска: Достапност на доверливата база на хрватската радиотелевизија на црниот пазар	Случај 8 од Хрватска: Секоја година од патарините исчезнуваат два милиони евра
Случај 1 од Косово: Уништување на докази	Случај 3 од Хрватска: Во потрага по бранителите	Случај 1 од Косово: Уништување на докази
Случај 2 од Косово: Стекнување статус на воен инвалид	Случај 4 од Хрватска: Со мала помош од јавните службеници, вкупно 68 хрватски пасоши им биле продадени на криминалци криминалци	
Случај 4 од Косово: Фалсификување на даночна документација	Случај 6 од Хрватска: Полицајци ги бришат податоците за сообраќајни прекршоци и објавуваат доверливи податоци и како поткуп прифатиле печено јагне и 20 литри вино	
Случај 1 од Македонија: Злоупотреба на ИТ системот на патарините	Случај 7 од Хрватска: Случајно фатен при објавување доверливи податоци за возилата и за нивните сопственици	
Случај 3 од Македонија: Злоупотреба на информацискиот систем и незаконско објавување на лижоклични податоци	Случај 2 од Црна Гора: Користење на ИТ за нанесување политичка штета	
Случај 4 од Македонија: Злоупотреба на системот за регистрирање на работни часови	Случај 3 од Македонија: Злоупотреба на ИТ системот и незаконско објавување на лични податоци	
Случај 1 од Црна Гора: Злоупотреба на службената положба и фалсификување на службени документи	Случај 1 од Србија: Сексуален акт во Белградска Арена	
Случај 2 од Црна Гора: Користење на ИТ за нанесување политичка штета		
Случај 3 од Црна Гора: Злоупотреба на функција и внесување на неточни податоци во јавните регистри		
Случај 4 од Црна Гора: Незаконско издавање на патни исправи		
Случај 4 од Србија: Мафија на патиштата		

Така, заштитата на пристапот до податоци е од клучна важност и вклучува не само контрола врз пристапот, туку и обезбедување на соодветно ниво на автентикација.

Контрола на пристап – управување со лозинката и идентитетот на корисникот

Контролата и ограничувањето на пристапот до системот се прават преку доделување на корисничко име и лозинка на персоналот. Најголем дел од системите кои споделуваат податоци или опслужуваат повеќе од еден корисник имаат обезбедено одредена контрола на пристап, како и шема на корисничко име и лозинка. Во одвоените системи, податоците и компјутерските програми треба да се обезбедат преку контрола на пристап до самиот компјутер. Можеби се подразбира самото по себе дека пристапот треба да биде ограничен само на овластени корисници, но ова не секогаш е случај.

Во примерот на случај 4 од Србија (Мафија на патиштата), системот на регистрирање на индивидуалните наплаќачи на патарина со нивен единствен идентификациски број не функционирал во пракса. Идентификациските броеви биле видливи за колегите, но раководителите на смена често ги менувале вработените. Во примерот на случај 5 од Македонија (Злоупотреба на администраторските права – банкарски гаранции/увозни квоти), вработениот кој имал администраторски права открил дека ги задржал привилегиите на пристап после неговото преместување од еден во друг административен центар. Потоа изработил лажна корисничка сметка и времено ја користел за менување на податоците на банкарски гаранции, и во сојузништво со една локална компанија извршил компјутерска измама на границата. Главниот администратор не вршел редовни проверки и ревизија на привилегиите на администраторите префрлени од едно на друго место, па така администраторот имал можност да изврши кривично дело преку користење на новонаправената корисничка сметка. Во други случаи, злоупотребата или крадењето на лозинки, како во примерот на случај од Косово (Злоупотреба на лозинка), примерот на случај 1 од Босна и Херцеговина (Најпознатиот босански хакер меѓу обвинителите) и примерот на случај 2 од Албанија (Корупција во електронскиот систем за јавни набавки) отвораат можност за корупција. И покрај тоа што системот за е-набавки кој се користи во Албанија изгледа дека ги почитува сите потребни мерки за претпазливост, системот на електронска пошта кој се користи за поддршка на системот за е-набавки ги поткопал сите добри намери бидејќи овој случај бил откриен откако проценката на набавки била направена од трето лице после промена на лозинката. Всушност, сите корисници меѓусебно си ги знаеле своите лозинки. И покрај тоа што таквата пракса се спроведувала во знак на добра намера за решавање на евентуални работни прашања, истата ја намалила целокупната безбедност на системот.

Лозинките и името на корисникот треба секогаш да бидат лични и доверливи. Она што на почетокот би се сметало за подобен начин на управување во секојдневниот работен живот, како на пример позајмување на лозинка на колегите или на подредените во

синџирот на хиерархија со цел разрешување на некоја итна задача, или ресетирање на лозинката на дефолт вредност која ќе им биде позната на останатите и која повеќе нема да се чува во тајност, може да биде предмет на злоупотреба како што наведовме во примерите погоре. Доколку е неопходно на некој колега да му се обезбеди пристап до системот и податоците, тоа треба да се направи така што: 1) вработениот ќе ја користи својата лична идентификација при логирање во системот; 2) записите од секој пристап до системот и податоците се чуваат; и 3) се доделува само ограничен и наменски пристап со одреден временски рок.

Соодветно ниво на пристап до податоците и системите

Неколку случаи експлицитно нагласуваат што би можело да се случи кога нивото на пристап до податоците е несоодветно, односно кога се доделува поголема автентикација до системот и податоците од она што е стриктно неопходно за извршување на непосредните задачи на вработените.

Во случајот 5 од Македонија (Злоупотреба на правата на администраторот (банкарски гаранции/ увозни квоти) и случајот 3 од Црна Гора (Злоупотреба на функции и внесување неточни податоци во јавните регистри), вработените имале многу поголем пристап за менување или внесување на податоци од она што им било стриктно неопходно да си ја завршат работата. Во двата случаи тие ги злоупотребиле своите функции и успеале да направат податоците/документите кои ги презентирале пред надворешни страни да изгледаат законски.

Физички пристап до податоци и документи

Физичкиот пристап до просторите во кои се чуваат податоци или физички копии од податоците за потврда, озаконување итн. треба да бидат ограничени само на овластен персонал, чиј што пристап ќе биде како логован така и мониториран.

Во случајот 2 од Хрватска (Достапност на доверливата база на хрватската радиотелевизија на црниот пазар) копија од лиценцираната база на податоци на хрватската радиотелевизија (Регистар на ХРТ) била продадена на црниот пазар. Физичкиот пристап до просторијата на серверот во која се чува Регистарот на ХРТ бил доделен исклучиво на овластени лица, но пристапот до базата на податоци исто така се овозможува и преку локалната мрежа и интернет преку користење на заштитени тунели за проток на податоци. Без оглед на тоа дали базата на податоци била ископирана директно од серверот во просторијата во која е сместен серверот или далечински, хрватските автори забележуваат дека стандардите за ограничување на физички пристап не се применувале.

Во случајот 4 од Црна Гора (Незаконско издавање на патни исправи) авторите забележуваат дека е неопходно да се воведе пракса на скенирање на документите или да се утврди електронска база на податоци за сите документи кои се доставуваат и издаваат на хартија со можност за задолжителна двојна заштита, со цел да се осигура безбедноста на податоците во случај на нивно намерно или ненамерно уништување. Исто така, потребно е да се подобри безбедноста на електронскиот систем со кој се снима физичкиот пристап до просториите каде што се чуваат фајловите и официјалните документи. Случајот 3 од Црна Гора (Злоупотреба на функциите и внесување неточни податоци во јавните регистри), во кој има комбинација на различни електронски и физички регистри на земјиште е дури уште посложен. Истите документи може да имаат различно потекло, па понекогаш невозможно е да се утврди со точност кој ги изработил документите и кој има целосен пристап до истите. Во овој случај, барањето е документацијата да се чува електронски, а пристапот до физичките и електронските регистри им е дозволен само на овластени лица.

Во случајот 1 од Србија (Сексуален акт во Белградска Арена) воведени биле клучни картици за ограничување на пристапот до просториите во кои се чуваат податоците. Употребата на електронски преносни медиуми во просториите во кои се чуваат податоци сега е строго ограничена и е проследена со посебни процедури за пристап до податоци или пак е целосно забранета (зависно од типот на просториите).

Во Црна Гора, физичкиот пристап до системите, било за време на нивното спроведување или одржување, сега бара претходно добивање дозвола од Министерството за внатрешни работи за секое инволвирано лице.

Процедури и стандарди за безбедност

Авторите од Босна и Херцеговина, Македонија, Црна Гора и Србија упатуваат на спроведувањето на стандардот ISO 27001 за Управување со информациска безбедност и стандардот ISO 9001 за Управување на квалитет како конкретни мерки за заштита кои се спроведуваат во форма на безбедносни процедури со цел да се осигура безбедноста и интегритет на податоците. Во Босна и Херцеговина правосудството ги има подобрено безбедносните процедури на сите нивоа, како оние предвидени со стандардот ISO 27001 и спроведениот стандард ISO / IEC 27001:2005. Во Србија, Министерството за внатрешни работи и Министерството за правда планираат во блиска иднина да го воведат стандардот ISO 27001. Во Црна Гора, Правилникот на стандарди за информациска безбедност ги утврдува стандардите за информациска безбедност кои се применуваат во спроведувањето на мерките за информациска безбедност предвидени со регулативата на Владата на Црна Гора. Во Македонија, Законот за електронско управување ги опишува стандардите кои мора да се исполнат при развивањето на ИКТ системи кои комуницираат, споделуваат податоци и документи во јавната администрација. Во подзаконските акти, воведени се дополнителни упатства за спроведување на голем дел од контролите предвидени со серијата стандарди на ISO 27000.

Резервни копии и записи на датотеки (лог фајлови)

Записите на датотеки овозможуваат подоцна да може да се изврши контрола на системот со цел да се утврди кој и што точно направил и кога. Истото важи и за резервните копии бидејќи резервните копии претставуваат евиденција на тоа како изгледале податоците во даден момент.

Во случајот 1 од Косово (Уништување на докази) целокупниот материјал што истражителите очекувале да го најдат на серверот на Министерството за јавна администрација и што би ги потврдил сомневањата на Агенцијата за спречување на корупција во однос на неправилности и прекршувања на законот, бил избришан од серверите на владата. Она што е уште посериозно во овој случај е дека за целокупната јавна администрација во Косово серверите за чување на податоци за сите владини институции се лоцирани во Министерството. Таквите податоци биле избришани од она што се смета за најзаштитена средина на податоци во Косово.

Во случајот 4 од Македонија (Злоупотреба во системот за регистрирање на бројот на работни часови), истрагата во записите на датотеки била суштинска во откривањето на злоупотребата. Македонските автори забележуваат дека некои од тековните пракси се утврдени според соодветното законодавство, но други пак се утврдени без постоење на формална основа во законите или подзаконските акти. Таквите пракси вклучуваат правење записи за секој пристап, дополнување, бришење или менување на податоците, и овозможување пристап до записите на датотеки по барање за целите на ревизија и внатрешна контрола. Освен чувањето и архивирањето на записите, никакво друго дејство не е дозволено.

Конечно, се забележува и случајот на IDDEEA (Агенција за идентификациски документи, регистри и размена на податоци) во Босна и Херцеговина, агенција која е одговорна за утврдувањето на електронската размена на податоци меѓу полициските власти и обвинителите и која започна со активност која доведува до нова генерација на размена на податоци во БиХ. Барањата се чување на резервна копија на оддалечена локација која е добро заштитена со лозинка, во комбинација со физичка безбедност.

Интероперативност меѓу ИКТ системите во јавните институции и формирање на базни регистри

Интероперативност е термин кој се користи да се опише способноста на разните системи и организации да работат заедно (интероперативно работење). За да може да бидат интероперативни системите треба да имаат капацитет да разменуваат податоци. Пречките за размена на податоци по правило вклучуваат технички, семантички, организациски и правни пречки, но дополнително може да се додаде уште една компонента– довербата. За да може податоците од една организација да бидат изложени пред друга организација потребно е одреден степен на доверба меѓу страните во размената; во спротивно, искуството ни вели дека соработката

многу брзо ќе престане да функционира. Гаранцијата на интегритетот и заштитата на податоци од злоупотреба се од клучна важност за интероперативноста и се суштински за реализирање на е-владиниот потенцијал за намалување на административниот товар преку интеграција на е-владините алатки: паметно користење на информациите кои граѓаните и деловните субјекти им ги обезбедуваат на јавните власти за заокружување на административните процедури; промовирање на електронските процедури во доминантен канал за обезбедување на е-владините услуги; и принципот на 'единствено еднаш' регистрирање на релевантните податоци. Последново предвидува граѓаните и деловните субјекти да ги доставуваат одредените стандардни информации само еднаш бидејќи канцелариите на јавната администрација преземаат дејство за интерно споделување на таквите податоци, така што никаков дополнителен товар не паѓа врз граѓаните или деловните субјекти.

Од посебна важност е заштитата на интегритетот на базните регистри на земјата. Базните регистри се основни градежни блокови на е-владата во земјата и сè повеќе во комуникацијата меѓу земјите. Тие се состојат од главните бази на податоци во кои се содржани ажурираните категории на сето она што е потребно за владата и јавниот сектор да бидат ефикасна администрација која нуди добри услуги (како електронски, така и неелектронски) на граѓаните и деловните субјекти, како и за развивање и спроведување на ефективни политики. Базните регистри се отелотворение на принципот 'само еднаш'. Најтипичните регистри од овој тип содржат детални податоци за граѓаните (раѓање, брачна состојба, смрт, адреси, единствен матичен број, патна исправа/лична карта итн.) и за сите претпријатија (големина, година на основање, број на вработени, сектор на активност, даночна обврска и плаќање, често поврзани и со регистри во кои се прикажува годишниот обрт, профит итн.). Постоењето на земјишни и градежни регистри, исто така, е вообичаена пракса, како и регистрите на возила, транспортни мрежи, водни патишта итн. Базните регистри може да го елиминираат удвојувањето на напорите на јавните власти и да ја намалат веројатноста за појава на грешка. На тој начин, изработката на базните регистри и интероперативниот систем потребен за истите да може да бидат споделувани меѓу надлежните министерства и агенции е основен фундамент на е-владата.

Сепак, доколку јавните ИКТ системи се компромитирани или се ранливи на злоупотреба, последиците може да бидат далекосежни и да имаат економски, социјални и правни импликации за сите, односно за јавната администрација, граѓаните, деловните субјекти итн.

Во случајот 12 од Хрватска (Немаш ни еден ден поминато на работа? Не грижи се, секако ќе ти дадеме целосна пензија!), преку интеграцијата на податоци и консолидацијата на основните регистри меѓу властите со користење на национален единствен личен број за идентификација (мрежа за размена на "ЕИБ", единствен идентификациски број) се постигнала заштита преку 'принципот на повеќе очи', и на тој начин се решиле проблемите опишани во случајот така што Хрватскиот институт за пензиско осигурување (HZMO) бил интегриран во мрежата за размена на ЕИБ и била спроведена ревизија на податоците за пензионерите.

Случаите во глава 1 опфаќаат примери на она од што се составени базните регистри, како случајот 3 од Босна и Херцеговина (Злоупотреба на електронскиот систем на проектот CIPS) и случајот 3 од Црна Гора (Злоупотреба на функции и внесување неточни податоци во јавните регистри).

Во босанскиот случај се забележува дека од почетокот на проектот на Системот за заштита на идентификацијата на граѓаните (CIPS) во 2002 година имало голем број на поплаки – посебно при издавањето на лични карти и патни исправи ширум земјата. Фактот што централниот регистар бил компромитиран е од суштинска важност, а босанските автори забележуваат дека и покрај тоа што Агенцијата за идентификациски документи, регистри и размена на податоци (IDDEEA), која сега е одговорна за CIPS, спровела широк опсег на мерки за заштита и е усогласена со стандардите на високо ниво за безбедност и сигурност на ИКТ, сè уште постојат проблеми во однос на размената на податоци со другите органи, недостиг на институционални аранжмани за координација на е-владините активности и неспроведување на упатствата на IDDEEA ширум јавната администрација. Ова може да го компромитира не само системот на CIPS, туку исто така и желбата на јавните органи да ги направат своите системи интероперативни.

Случајот 3 од Црна Гора се однесува на општинскиот катастар каде незаконски измени во катастарот овозможиле нелегален пренос на државно земјиште од општинскиот катастар на трето лице. Овој случај вклучил изработка на фалсификувана електронска потврда која подоцна може да се искористи во правна постапка. Не се упатува на никакви стекнати поуки и дополнителни мерки за заштита спроведени во овој случај. Но овој случај илустрира што би можело да се случи доколку пристапот до мониторинг на вработените е недоволен и како истиот може да го компромитира целокупниот регистар.

Случајот 5 од Македонија (Злоупотреба на администраторските права – банкарски гаранции/увозни квоти) илустрира што се случува кога еден јавен орган – гранични службеници – е зависен од информациите и податоците од друг орган како гаранција на информации за трета страна (банкарска гаранција), и каде вредноста ограничена со фактичката банкарска гаранција ја внесуваат административни службеници наместо истата директно да се добие од информацискиот систем на банките. Авторите не споменуваат никакви последици по соработката меѓу јавните органи кои биле инволвирани во случајот, но може да се очекува предупредување и барање за интегритет на податоците.

Мониторинг и ревизија

Резервните копии и записите на датотеки се 'технички' овозможувачи на заштитните мерки за мониторинг и ревизија, но постојат и некои други релевантни прашања при разгледување на потребата за мониторинг и ревизија на ИКТ системите.

Најслабата алка меѓу системите и процесите

Неколку случаи од глава 1 упатуваат на неопходноста организацијата да ги заштити сите свои процеси и да преземе посебни чекори за заштита од електронска и физичка злоупотреба. Дури и 'совршените' ИКТ системи се онолку безбедни (а податоците податливи) колку и нивниот влезен материјал. Доколку погрешни податоци бидат внесени во ИКТ системите, интегритетот на целиот систем ќе биде компромитиран. Мониторингот и ревизијата мора да ги опфатат сите деловни процеси и системи без оглед дали се физички или електронски.

Во случајот 4 од Албанија (Проневера и фалсификување на книговодствената евиденција) вработениот одговорен за книговодствената евиденција ги проневерил парите со фалсификување на платниот список преку добивање на писмени одобренија (физички копии), а потоа ги менувал електронските податоци за плати како и податоците кои се испраќале до банката. Со оглед на тоа што не била извршена ревизија на усогласеност меѓу физичката копија и електронските записи, слабата алка се наоѓала меѓу овие две "процедури". Албанските власти, исто така, посочуваат на недостигот од проверки во финансискиот систем кој не бил во можност да врши истовремена обработка на поединечните детаљи од платниот список наспроти вкупната сума. Понатаму, недостасувала и вкрстена проверка меѓу разните потпишани документи за платниот список од страна на финансиските органи.

Во случајот 2 од Косово (Стекнување на статус на воен инвалид) злоупотребата била извршена за време на скенирањето, при што медицинскиот извештај бил фалсификуван. Сторителот Ф. М доставил документ со кој прикажал дека за време на војната во Косово имал медицински проблеми. Документот не датира од воениот период, туку бил изготвен 5 години подоцна. Истиот содржел датуми кои би сугерирале на тоа дека бил изготвен за време на војната.

Примерот на фалсификуваната патна исправа со изминат рок која била користена од трето лице во случајот 1 од Црна Гора (Злоупотреба на службена положба и фалсификување на службени документи) упатува на формална грешка или пропуст во информацискиот систем за издавање на патни исправи во Министерството за внатрешни работи (МВР), кој по правило треба да го елиминира ризикот за користење и повторно издавање на патни исправи во случај на изминат рок на важност. Системот не го поврзал физичкиот документ (патната исправа) со отсликаниот запис од базата на податоци во кои се содржани точно истите информации, вклучително и фотографијата на носителот на патната исправа. Понатаму, немало никакви електронски траги во

системот со кои би се утврдиле службениците кои ја издале фалсификуваната патна исправа. Ранливоста на системот во овој случај се согледува во некохерентноста меѓу фактичките и обработените физички патни исправи во системот на МВР.

Конечно, случајот 4 од Косово (Фалсификување на даночната документација) укажува што би можело да се случи кога никој не врши проверка на потенцијалната слаба точка или алка. Во овој случај, сопственикот на претпријатието кое склучило договор со јавна установа за обезбедување хигиеничарски услуги ја искористило "моќта" врз основа на добро поставените односи со даночните службеници. После една првична исплата на данок во висока вредност, во сите други идни понуди тој ја користел истата фактура, но со фалсификувани датуми. Сите службеници во институциите имале право да го побараат оригиналниот документ, но не го правеле тоа зашто сметале дека работат со постара личност и под изговор дека скенираниот документ е доволен да ги задоволи нивните барања. Сепак, никој не извршил никаква проверка и тоа самото по себе претставува ранливост. Овде се справуваме со случај во кој службениците можеле да ја заштитат постапката на набавка преку барање на увид во даночната документација, но никој тоа не го сторил.

Мониторингот и ревизијата, како и правните и процедурални мерки за заштита треба да ги опфаќаат и да се однесуваат на сите системи и процеси (електронски и физички) кои ги користат јавните установи.

Ранливост во ангажирањето надворешни услуги и ризици поврзани со ангажирање надворешен експерт за ИТ

Случајот 2 од Македонија (Напад врз ИТ системот за јавна набавка) претставува интересен случај во кој системот за е-набавка ги запазил сите можни технички мерки за заштита, но станал ранлив на напад од дистрибуирано одбивање на услуга (DDoS) бидејќи бил хостиран во споделена средина со ISP. И покрај тоа што македонските власти не докажале злоупотреба на службена позиција и корупција, овој случај дава преглед на процедурата и потенцијалните методи на злоупотреба на ИКТ системите за целите на корупција преку злоупотреба на службената позиција или социјален инженеринг. Системскиот администратор има целосни привилегии во системот подолг временски период и доколку неговите активности не се соодветно контролирани и мониторирани тој може да го злоупотреби системот преку уништување или менување на дигиталните докази и на тој начин да оневозможи истрага на случајот и докажување на злоупотреба.

Случајот 2 од Србија (Кога ИТ изведувачот "фаќа корен") претставува случај во кој надворешно ангажираниот ИТ експерт остварува внатрешни контакти со кои може да ги манипулира податоците и процедурите во своја корист за да го продолжи поволниот договор за обезбедување надворешни услуги. Во меѓувреме, законите и регулативите за набавка во Србија биле изменети, но непристојниот вработен го искористил своето познавање на системот и барањата посебно во корист на актуелниот ангажиран ИТ

изведувач со цел да ги намали трошоците за изнајмување надворешни услуги. Тој ги скрил или ја оневозможил расположивоста на податоците во однос на пристапот на ИТ изведувачот до VPN WAN системот и ја уништил електронската документација во системот така што јавната установа (Министерство за правда и јавни работи, а подоцна Министерство за правда) не можело да врши контрола, мониторинг и надзор врз системот.

Во случајот 3 од Албанија (ИТ корупција кај дистрибутер на електрична енергија), фирмата оператор за дистрибуција на електрична енергија била во најголем дел приватизирана. Преку шема на издавање на сметки со прекумерен износ, погрешно читање на струјомерите преку PDA уредот (личен дигитален асистент), постоеле наводи дека електронските податоци се менуваат во ИТ системот на фирмата откако истите се регистрираат од PDA уредот и на тој начин сметките за електрична енергија на корисниците се впишуваат со прекумерен износ. PDA уредите и постапките за читање на струјомерите првично биле наменети да обезбедат точно пресметување на износот за наплата. Но неовластениот пристап и фалсификувањето на податоци, можеби (но сè уште недокажано) и со помош на управата, ја уништува довербата која јавноста ја имала во процесот на читање на струјомерите.

Конечно, нашата збирка случаи на корупција поврзана со ИКТ содржи три примери на измама и проневера во фирмите задолжени за патариниte (Случајот 8 од Хрватска, Случајот 1 од Македонија и случајот 4 од Србија)[87]. Во случајот на Хрватска и Македонија, наплатата на патариниte им била доделена како надворешна услуга на приватни фирми, додека во Србија фирмата била целосно во државна сопственост. Преку шеми кои се протегаат од проневера од страна на вработени во случаите од Македонија и Хрватска, па сè до елаборираната и пософистицирана шема во српскиот пример, ризикот од измама и проневера постои тогаш кога има директна наплата на патарината и кога не постои соодветен мониторинг на вработените. Во случаите од Хрватска и Македонија злоупотребата била откриена преку внатрешна контрола. Во случајот од Србија интерен дојавувач информирал за злоупотребата. Во сите три случаи подоцна се спровеле засилени технички мерки за заштита и мониторинг на вработените.

Во случај кога ИКТ системите му се доделуваат на надворешен изведувач, јавните тела во контактот со своите ИТ изведувачи мора да обезбедат можност да го мониторираат и да вршат контрола на системот не само на истиот оној начин кој го применуваат во однос на интерниот систем, туку и повеќе од тоа, со оглед на тоа што ангажирањето надворешни услуги начелно претпоставува помала контрола врз системот.

87 Случајот 8 од Хрватска (Секоја година од патариниte исчезнуваат 2 милиони евра), Случајот 1 од Македонија (Злоупотреба на информацискиот систем на патариниte), и случајот 4 од Хрватска ("Мафија на патиштата")

Организациски и процедурални мерки за заштита

Во Албанија секоја владина институција која го ревидира постојниот информатички систем или која гради нов, во моментот прво мора да добие нацрт преглед и да нема никакви приговори во однос на описот на проектот од страна на експертите во Државната агенција за информатичко општество. Понатаму, предавањето на системот од ангажираниот развоен програмер до корисникот од јавниот сектор преку процедура на 'прифаќање на информатичкиот систем' тежнее кон обезбедување на подобар интегритет и квалитет на информатичките системи во јавниот сектор. Во Босна и Херцеговина, ИТ системите во полицијата и нивниот оперативен персонал сега се предмет на редовна проверка од страна на надлежните органи. Во Хрватска, согласно со Регулативата на мерки за информациска безбедност, сега се предвидени процедури за итно планирање (изработка на процедури кои треба да се следат во случај на инцидент поврзан со безбедноста и процедури за управување со континуитетот на деловното работење). Авторите од Македонија забележуваат тенденција на потпишување на договори за доверливост меѓу економските оператори и изведувачите при што двете страни се согласни да не објавуваат информации за лицата кои имаат пристап до системот. Понатаму, во македонските институции сега постои усвоена пракса на раздвојување на улогите на техничките администратори и администраторите на содржина (податоци). Техничките администратори се одговорни за системот на ниво на примена и на ниво на управување со корисници и давање дозволи за пристап. Администраторите за содржина се одговорни за управување со податоците кои се чуваат во базите на податоци, но не и за управувањето со самите системи. Во Црна Гора, Министерството за информатичко општество и телекомуникации има изработено неколку правилници за работа со цел да ги обезбеди стандардите, заштитата на податоци, управувањето со инцидент, содржината и начинот на чување на записите од автентикација на давателите на услуги, пристапот до е-владиниот портал и користењето на интерната мрежа на државните органи. Конечно, во Србија и Министерството за внатрешни работи и Министерството за правда сега спроведуваат процедури со кои се регулира пристапот до податоци со цел да се обезбеди заштита од злоупотреба. Понатаму, во Министерството за правда никој, па дури ни вработените на високи позиции, немаат пристап до податоците без претходно одобрение од судот или од обвинителството.

Заштита преку принципот на 'повеќе очи'

Некои примери од глава 1 демонстрираат 'едноставна' примена на принципот на 'повеќе очи'. На пример, случајот 5 од Хрватска (Полицаец фатен на дело при внесување фалсификувани податоци во информацискиот систем на полицијата) каде раководителот на полициската станица ја забележал писмената потврда во информацискиот систем на Министерството за внатрешни работи или случајот 4 од Македонија (Злоупотреба во системот на регистрирање на бројот на работни часови) каде прераспределбата на работни задачи значи дека новиот администратор имал увид во записите од системот на работни часови, па така извршил ревизија преку примена на принципот на 'повеќе очи' и го открил несовпаѓањето.

Во случајот 12 од Хрватска (Немаш ни еден ден поминато на работа? Не грижи се, секако ќе добиеш целосна пензија!), консолидацијата на податоци во регистарот на ЕИБ (ЕИБ = Единствен идентификациски број) ја постигнува примената на принципот на 'повеќе очи'. Принципот на 'повеќе очи' ќе можел да се примени во случајот 4 од Косово (Фалсификување на даночна документација) доколку јавните службеници во разните владини институции кои изнајмувале надворешни услуги инсистирале на проверка на точноста на даночните документи, и во тој случај злоупотребата ќе можела да се открие многу порано, а процесот на набавки ќе бил заштитен. Истиот недостиг од двојна проверка важи и за случајот 3 од Црна Гора (Злоупотреба на функција и внесување неточни податоци во јавните регистри) каде во записите на општинскиот катастар недостасувале организациски и процедурални мерки за заштита, како што е принципот на 'повеќе очи'. Не била направена никаква двојна проверка на статусот и сопственоста на земјиштето, ниту техничка, ниту пак од кој било од вработените во општинскиот регистар, ниту пак преку надворешна ревизија.

Етички кодекс

Можеби како резултат на случаите 9 и 10 од Хрватска кои се однесуваат на злоупотреба на информатичката технологија од страна на полициски службеници, и случајот 11 од Хрватска (Постар инспектор злоупотребил доверливи податоци за да победи на локални избори!) 'Кодексот на етика' се применува од страна на јавните службеници, а вработените во Министерството за внатрешни работи и Министерството за финансии се обврзани да делуваат согласно со истиот. Она што е подеднакво важно е што граѓаните имаат можност да ги известат службениците за етика за евентуално неетичко однесување од страна на државните службеници.

Податоци на отворена влада; да ú се дозволи на јавноста да помогне во заштитата на интегритетот и точноста на податоците

Авторите од Македонија ги споменуваат отворената влада и отворените податоци како пример на активности за спречување на корупција кои им овозможуваат на граѓаните да имаат активна улога во спречувањето и утврдувањето на корупција. Како таков, примената на принципот на 'повеќе очи' преку учество на граѓаните во разгледување на податоците, како на пример оние кои се однесуваат на конечниот или имотниот статус на високи службеници, може да се овозможи преку отворање на владините податоци. Од претходна студија на ReSPA која беше спроведена во 2012 година[88], знаеме дека во тој период Хрватска, Србија и Црна Гора беа на почетокот на спроведувањето на одредени иницијативи во однос на отворените податоци.

88 Регионална споредбена е-владина студија на ReSPA (2012), достапна на: http://respaweb. eu/download/doc/Regional+comparative+eGov+study+-+web.pdf/dfab3d5a78e0d10e9- a6a80827e36a277.pdf

Обука, етика и свесност за интегритет

Во Албанија, Државната агенција за компјутерска безбедност во соработка со Албанската школа за јавна администрација презема тековна иницијатива за организирање обуки за речиси сите ИТ вработени во јавните институции. Обуката вклучува безбедност и заштита на системот и проценка на ризик. Во Босна и Херцеговина постои нов модул за обука на обвинители во областа, на пример, на компјутерски криминал и комуникациски вештини.

Во Хрватска, Регулативата на мерките за информациска безбедност предвидува подигнување на свеста за безбедноста како во утврдувањето на правилата за безбедност така и во образованието на вработените. Вработените во Министерството за внатрешни работи учествуваат во разни обуки и проекти за подигнување на свеста за ризиците од ИКТ корупција и мерките за заштита. Примери за ова се два проекти кои имаат цел да ги зацврстат административните капацитети на Министерството за внатрешни работи во борба против компјутерскиот криминал и проектот за регионална соработка во кривичното судство: зацврстување на капацитетите во борбата против компјутерскиот криминал. Проектот, исто така, вклучува работилници за мрежите на форензичари кои ги спроведува Министерството за внатрешни работи и Хрватската академска и истражувачка мрежа.

Во Србија, Министерствата за правда и внатрешни работи сега ги обучуваат своите вработени за ризиците од ИКТ корупција.

Во Македонија, Стратегијата за реформи во јавната администрација и Акцискиот план предвидуваат обука и подигнување на свеста за корупција како на државните службеници така и на граѓаните. Црна Гора нуди образование на корисниците во областа на информациска безбедност и спречување на компјутерски инциденти.

Само Косово има известено дека не постојат ниту мерки ниту план за понуда на обука и подигнување на свеста на државните службеници за ризиците и мерките за заштита од ИКТ корупција.

Дојавувачи

Некои корупциски дела може да се откријат само преку внатрешни извори кои дојавуваат за вистинската состојба. Ова посебно важи доколку управата е таа која е инволвирана во корупција. Случајот 4 од Косово (фалсификување на даночната документација) и случајот 4 од Србија (мафија на патиштата) илустрираат како управата и/или целокупната организација може да ги занемарат случаите на злоупотреба на функција, службена измама, проневера и организиран криминал, создавајќи култура во која сите се 'вклучени' во злоупотребата, не се осмелуваат да сторат ништо во врска со тоа и ја прифаќаат ситуацијата било заради тоа што се плашат од реперкусии доколку ја откријат злоупотребата или заради тоа што имаат корист од истата.

Човечки фактор

Доколку и сите мерки за заштита од ИКТ корупција се почитуваат, сепак, не постои гаранција дека системите нема да бидат злоупотребени. Незаконската наредба од раководителот за извлекување на електронска пошта како во случајот 3 од Србија (Виш јавен службеник ги шпионира вработените) или случајот 2 од Албанија (Корупција во електронскиот систем за јавни набавки) каде мнозинството корисници станува вознемирено, посебно со периодичните измени на сложените лозинки, па прибегнува кон краткиот пат да ги остави лозинките неизменети со дефолт вредноста која системскиот администратор првично им ја дал кога се логирале првпат, ќе продолжат и понатаму.

Свеста меѓу вработените за сериозноста на компромитирање на системите ќе биде клучна за обезбедување и заштита на системите. Ова вклучува свест не само за безбедносните импликации, туку и за димензиите на етика и интегритет во работењето на државните службеници. Државните службеници мора да бидат свесни за своите права и обврски, а земјите поединечно мора да утврдат модалитети за поддршка на етичкото однесување.

Законски мерки за заштита

Авторите од засегнатите држави наведуваат низа законски акти и државни стратегии кои покриваат разни области, како што се: административни процедури; електронски документи; класифицирани информации; електронски потпис; заштита на лични податоци; јавни набавки; корупција и кривичен законик. Целта на оваа студија не е да прави споредбена анализа на законските мерки за заштита во секоја од засегнатите држави со оглед на тоа што истите се веќе дадени како придонес кон илустрирање на правните мерки за заштита релевантни за поединечните случаи.

Интересна поука од оваа студија е фактот што постојат случаи каде преземените правни мерки за заштита не биле соодветни за обезбедувањето заштита од ИКТ корупција.

Авторите од Косово известуваат дека: *"во однос на административните мерки за заштита, Косово има усвоено низа закони, стратегии и административни упатства (нормативни акти) кои се однесуваат на употребата на информатичките и комуникациските технологии, но законската инфраструктура досега го нема соодветно уредено, посебно или начелно, прашањето на интеграција на податоците и злоупотреба на системите на информатичка технологија."*

Постојат само неколку случаи (како на пример оваа студија) во кои се дава опис на несоодветните законски мерки за заштита од злоупотреба, и како такви истите се сметаат за поуки кои треба да се разгледаат. Во случајот 2 од Македонија (Напад врз ИТ системот за јавна набавка) правилата за набавка изгледа не ја земаат предвид ситуацијата во која процесот на електронска понуда е нарушен од "технички" причини. Во друг случај на набавки – Случајот 2 од Србија (Кога ИТ изведувачот "фаќа корен") – се известува дека ИТ изведувачот ја запрел новата тендерска постапка преку користење на сложена и исцрпна шема на жалби достапна преку дупките во Законот за јавни набавки. Оттогаш законот бил изменет ("Службен весник на Република Србија", бр. 124/12).

Во случајот 1 од Србија (Сексуален акт во Белградска Арена) интерните административни регулативи се ажурирани со цел да го обезбедат следното: 1) неовластениот пристап до податоците на Министерството за внатрешни работи сега се дефинира не само како дисциплински, туку како кривично дело; и 2) користењето на податоците за која било друга цел освен за првично предвидената за која податоците биле прибрани сега се дефинира како кривично дело (не само како дисциплински прекршок).

Примерите на случај во оваа студија се само примери. Не постојат репрезентативни информации од кои би можело да се извлече заклучок во однос на општите празнини во законски предвидените мерки за заштита.

3. Препораки на ниво на политика за ублажување на ризиците од корупција во ИКТ

Подготвено од Тилман Хопе и Луизе Томасен

Дел 1 – Препораки наменети за експертите за борба против корупција

Секој чинител кој работи на спречување на корупција треба да ја прифати ИКТ не само како алатка за борба против корупцијата, туку и како ризик за извршување корупција. Така, следниве мерки се сметаат за неопходни за експертите за **борба против корупција**:

1. Експертите за борба против корупција треба да остваруваат **блиска соработка** за целите на утврдување и спречување на ризиците од корупција преку злоупотреба на ИКТ.

2. Телата за спречување на корупција во рамките на својот каталог на стандардни ризици за корупција треба да ја вклучуваат и можноста за злоупотреба на ИКТ за коруптивни цели. Проценката на ризикот во јавната администрација треба да вклучува безбедност на ИКТ од ризици од корупција. **Проценката на ризик** треба да вклучува преглед на секој од подолу наведените ИТ обележја (Дел 2 од Препораките).

3. Раководителите на јавните институции како и јавните службеници треба да бидат **свесни** за ризиците кои ги наложува ИКТ во однос на корупцијата. Телата за спречување на корупција треба активно да нудат совети за затворање на безбедносните дупки во ИТ на јавната администрација.

4. Телата за спречување на корупција и центрите за стручно образование треба да нудат **обука** за ризиците од корупција поврзани со ИКТ; таквата обука треба да вклучува експерти за ИКТ.

5. Државните **стратегии** и акциските планови за борба против корупцијата треба да вклучуваат дел за спречување на корупцијата поврзана со злоупотреба

на ИКТ. Доколку други стратегии (како онаа за е-влада или за реформите во јавната администрација) веќе се занимаваат сеопфатно со засилувањето на ИТ против злоупотреби, политиката за борба против корупцијата треба да содржи барем одредница која ќе упатува на други стратегии и која ќе обезбеди координација меѓу експертите за борба против корупција и експертите за ИТ во однос на реформските мерки.

6. Органите за спроведување на законот и телата за спречување на корупција треба да прибираат **статистички** податоци за корупцијата поврзана со ИКТ, да ги анализираат шемите и соодветно да усвојуваат реформски мерки

Дел 2 – препораки наменети за експертите за е-влада

1. Пристапот до сите нејавни податоци и системи потребно е да се заштити преку обезбедување **контрола на пристап** со користење на посебна идентификација со име и лозинка на корисникот.

2. Во секое јавно тело управата има одговорност да обезбеди соодветно **ниво на пристап** до податоците. Пристапот до нејавните податоци се доделува само доколку истиот се побара за целите на извршување на непосредни задачи.

3. **Физичкиот пристап** до просториите во кои се чуваат податоци или физички копии од податоците треба да биде ограничен само на овластен персонал чиј пристап ќе биде подеднакво регистриран и мониториран.

4. Јавните установи мора да ги спроведуваат **стандардите за информациска безбедност**, како што е ISO 27001, со цел да обезбедат безбедност и интегритет на податоците.

5. За секоја јавна установа треба да се изработат **планови за опоравување од незгода и продолжување со работа** во случај на безбедносни инциденти. Плановите мора да ги опишат процедурите кои треба да се следат во случај на инцидент, како што е обезбедување континуитет во работењето и да ги утврдат и да се согласни околу одговорностите за преземање итни дејства.

6. Сите јавни установи треба да спроведат **процедури за резервна поддршка** со периодична целосна поддршка на сите системи и податоци. Ова ги вклучува десктоп и лаптоп компјутерите. Резервните копии треба физички да се чуваат на друго место.

7. **Записите на датотеки** (лог фајловите) се дел од структурата за мониторинг и надзор во организацијата. Тие, исто така, претставуваат важна алатка за внатрешна контрола. Копиите од записите на датотеки треба, исто така, да се чуваат на друго место и/или одвоени од самата апликација. Администраторите

(технички) на записите на датотеки не треба да бидат од редовите на персоналот кој е одговорен за менување на содржината (податоците).

8. Јавните тела мора да ја спречат ранливоста на сите процеси, без оглед дали се физички или електронски, од коруптивна злоупотреба. **Компромитиран процес или чекор во процесот ќе влијае врз сите останати процеси со кои истиот влегува во интеракција**. ИКТ системите кои зависат од влезните податоци од други системи или процеси се безбедни од корупција онолку колку што се безбедни системите и процесите со кои влегуваат во интеракција.

9. **Базните регистри** бараат посебни и засилени безбедносни мерки бидејќи тие се суштински основни елементи за кохерентна интероперативна еВлада.

10. **Ангажирањето надворешни услуги** за развој, одржување и распределба на ИТ бара засилена претпазливост на јавните установи кои ја ангажираат таквата услуга. Одговорноста е елемент кој никогаш не може да биде ангажиран.. При ангажирање на надворешни услуги, обезбедете пристапот до податоците да биде овозможен само за овластен назначен персонал кој ќе подлежи на мониторинг и внатрешна контрола.

11. Потребно е **раздвојување на улогите** на персоналот одговорен за податоците (содржината) и персоналот одговорен за системите (технологијата).

12. **Контролата** на системот и патеките на контрола никогаш не смее да бидат мониторирани и администрирани од ист ИТ администратор.

13. Надзорот и примената на принципот на **'повеќе очи'** треба да претставува интегрален дел не само во дизајнот и развојот на системот, туку и во секојдневното работење.

14. Податоците на отворена влада и учеството на граѓаните преку целосен увид во податоците од јавниот сектор може да обезбедат 'проверка на реалноста' и да го подобрат квалитетот на податоците, како и да откријат неправилности и злоупотреба. Исто така, важно во овој котекст е да се обезбедат за јавноста канали на доставување повратни информации до владата и јавниот сектор. Во случај на корупција/ неправилности, канцеларите за етика каде граѓаните може да известуваат за неетичко однесување на државните службеници може да претставуваат форма на таков канал.

15. Во обуката за подигнување на свеста за етика и интегритет потребно е да се обезбеди вклученост и на персоналот одговорен за ИКТ.