Безбедност на информациите и зошто да се заштитиме?

Информациите претставуваат крвоток на секоја организација

Со поимот **информација** се означува резултатот на обработка, собирање, манипулирање и организирање на податоци на начин што го зголемува знаењето на примателот. Во контекст на безбедноста на информациите, првичната дефиниција е дека информацијата е средство на организацијата, кое како и сите други деловни средства има вредност за организацијата и поради тоа е потребно да биде соодветно заштитена.

Основни типови на информации се:

- Испечатени или напишани на хартија
- Чувани во електронска верзија (компјутер, диск, цеде,..)
- Испратени преку пошта или други електронски врски
- Прикажани на организациските промотивни материјали
- Кажани во разговори (директно или преку телефон).

Безбедноста на информациите е битна за успехот на секоја организација и бара ефективно управување.

Безбедност на информациите претставува обезбедување доверливост, интегритет и достапност на пишаните, изречените и компјутерските информации. Изразите безбедност на информациите и компјутерска сигурност често се користат како синоними, иако вториот поим всушност се однесува на поспецијализиран дел од поширокатa област која се однесува на информациите во било која форма.

Безбедноста на информациите ја заштитува информацијата од низа закани, со цел да обезбеди континуитет на работењето, да минимизира потенцијална деловна штета, да ги максимизира деловните резултати и да ги оправда инвестициите во безбедноста на информациите.

Секоја организација, односно институција, развива *сопствен* систем за безбедност на информациите со сопствено множество барања од аспект на заштитни мерки и контроли како и на нивото на доверливост, интегритет и достапност.

Овие три составни делови на безбедноста на информациите се дефинираат на следниот начин:

- **Доверливост** - Обезбедување дека информациите се достапни само за оние што се овластени да имаат пристап до нив
- **Интегритет** - Осигурување на точноста и комплетноста на информациите и на методите за нивна обработка
- **Достапност** - Обезбедување дека овластените корисници ќе имаат пристап до конкретните информации секогаш кога им е потребно тоа

Најчести закани за безбедноста на информациите се:

- Самите вработени
- Ниската свесност за безбедносните акспекти на информациите
- Експанзија на користење компјутери и компјутерски мрежи
- Интернет и електронската пошта (e-mail)
- Напади од хакери и од вируси
- Елементарни непогоди (пожар, поплава, земјотрес)
- Тероризам

Водич за информатички и комуникациски технологии (ИКТ)

Четвртиот Водич за ИКТ на Метаморфозис е наменет за сите кои сакаат да стекнат основни знаења за безбедноста на информациите.

Водичот е подготвен во рамките на проектот Иницијатива за информациска сигурност, спроведен од Фондацијата Метаморфозис со поддршка од Фондацијата Институт отворено општество Македонија. Проектот има за цел поттикнување на воспоставувањето на сигурноста на информациските системи во сите сегменти на општественото и деловното опкружување, како базична претпоставка за функционирање на информатичкото општество.

Сите изданија на Водичот се достапни во електронска форма на веб-сајтот на Метаморфозис (www.metamorphosis.org.mk). За печатени верзии пишете по е-пошта на info@metamorphosis.org.mk.

СОДРЖИНА

Поим за безбедност на информациите 1
Стандарди и препораки 3
Законска рамка 6
Систем за управување со ИС .12
Кодекс за ИС 12
Измами со банковни картички 14
Што е фишинг и фарминг? . .18
Стратешки насоки 20

Како да се заштитиме од информацискатa НЕбезбедност?

Дилеми :

- **Лично прашање:** Дали може да ни се случи најлошото? Колкава е предизвиканата штета и колку ќе нé чини таа? Колку сме подготвени да вложиме во „осигурување"?
- **Општествено прашање:** Чувствуваме ли обврска за безбедност на информациите со кои располагаме?

Наш одговор е: Воведување Систем за безбедност на информациите според препораките ISO 17799.

Кои се целите на воведувањето безбедност на информациите?

- Зголемена доверба кај клиентите и кај партнерите
- Намалување на ризиците во работењето
- Безбедност на деловни информации преку безбедносни контроли и заштити
- Усогласеност со интернационалните и со локалните регулативи

Денешна вистина: „Поевтино е нешто да се направи отколку да се заштити".

Како до безбедност на информациите?

- **Со воведување** Систем за безбедност на информациите (Information Security Management System – ***ISMS***) во согласност со **ISO 17799** препораки за воведување Систем за безбедност на информациите
- **Со сертифицирање** според Стандардот за управување со безбедност на информациите **ISO27001**

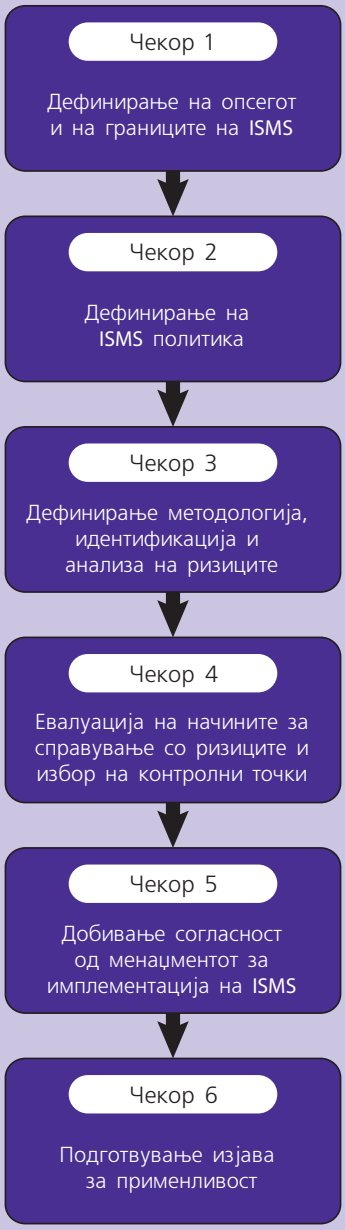
Системот за управување со безбедноста на информациите Ви обезбедува да ги заштитите информациите кои се битен ресурс на вашата организација.

Кои предуслови треба да се обезбедат?

- Свест за потреба од непрекинато работење кое директно зависи од безбедноста на информациите
- Прифаќање на одговорноста за имплементација на ISMS од раководните структури
- Прифаќање на одговорноста за спроведување на ISMS од *сите* вработени
- Организиран пристап
- Посветеност и дисциплина во применувањето
- Подготвеност за перманентно подобрување
- Транспарентност на ISMS (информираност на вработените, клиентите, партнерите)

Како се воведува Систем за безбедност на информациите?

- Преку имплементирање на соодветни заштитни мерки и контроли (политики, практики, процедури)
- Следејќи ги препораките од ISO 17799 - водичи за имплементација на систем за управување со безбедност на информациите базиран на индустриските најдобри практики.
- ISO 17799 има 11 контролни точки кои опфаќаат повеќе безбедносни категории
- Воведување ISMS е комплексен процес презентиран во 6 (шест) чекори опишани во приложената шема.



▶ **Првите 2 чекори** се клучни за успехот на имплементацијата на Системот за управување со безбедноста на информациите - ISMS. Тие опфаќаат дефинирањето на опсегот, границите и политиката на системот. Дефинирањето се базира на основните карактеристики на организацијата, како што се големината, ресурсите, типовите на информации со кои располага, нормативата по која работи итн. За овие два чекора е потребна целосна поддршка и активен ангажман на менаџментот на организацијата.

▶ **Третиот чекор** го опфаќа оценувањето на ризиците за информциите на организацијата. Најпрво се дефинира пристапот и методологијата за оцена, а потоа следи идентификација и анализа. Резултатите се листа на идентификувани ризици и извештај за влијанието на ризиците.

▶ **Четвртиот чекор** ги утврдува начините за справување со идентификуваните и анализираните ризици, определува контролни точки во согласност со стандардот и утврдува контроли што треба да се воведат.

▶ **Петтиот чекор** го опфаќа добивањето согласност од раководството за добиените резултати и имплементацијата на соодветни контроли.

▶ **Последниот чекор (6)** претставува документирање на избраните контролни точки и воведените контроли, како и причините за нивниот избор или правењето исклучоци.

Како ќе знаеме дека нашиот систем е безбеден?

Нашиот одговор е: Сертификација на Системот за управување со безбедноста на информациите според ISO 27001.

Сертификацијата според ISO 27001 се одвива во следните чекори:

▶ **Чекор 1**: Покренување иницијатива за сертификација, анализа на опциите за сертифицирање и потенцијални сертификациски куќи и барање прелиминарни понуди за сертификација.

▶ **Чекор 2**: Избор на сертификациска куќа и достава на формална апликација.

▶ **Чекор 3**: Врз база на добиената апликација, сертификациската куќа определува Ревизорски тим задолжен за сертификацијата и помош при развојот на вашиот ISMS систем

▶ **Чекор 4**: Првичен преглед на главните процеси и соодветната документација од страна на Ревизорскиот тим.

▶ **Чекор 5**: Спроведување на целосна ревизија од страна на Ревизорскиот тим, поднесување на извештај од ревизијата и препораки за подобрување.

▶ **Чекор 6**: Како резултат на успешната ревизија, сертификациската куќа ви доделува сертификат на кој е јасно истакнат опсегот на вашиот Систем за управување со безбедноста на информациите - ISMS.

▶ **Чекор 7:** По успешната сертификација, Ревизорскиот тим има обврска да ја посетува вашата организација редовно секоја година, со цел да го провери вашето работење и да ви помогне во процесот на подобрување

Кои се придобивките од сертифициран систем за управување со безбедноста на информациите?

- Врвниот менаџмент презема одговорност за безбедноста на информациите;
- Независна потврда на Вашиот ISMS Систем и потврда дека се следат соодветните закони и регулативи;
- Зголемена доверба кај Вашите партнери, заинтересирани страни и клиенти (сертификацијата покажува „due diligence");
- Ја подобрува Вашата конкурентност;
- Поголема свесност за безбедноста кај вработените;
- Развиен механизам за мерење на успешноста на ISMS;
- Редовните ревизии придонесуваат за континуирано подобрување во развојот и во напредокот на организацијата;

Стандарди и препораки за информациска сигурност

Како одговор на информациските инциденти и напади првенствено во сферата на информациските системи и комуникациски мрежи се појавуваат упатства - добри практики за обезбедување заштита на информациите и информациско-комуникациските средства. Големата инволвираност на информатичката технологија во сите сфери од животот и дејствувањето само ја надополнува потребата за поголема ефикасност на информациската сигурност, со што на глобално ниво го актуализира процесот на доброволна регулација, т.е. појава на меѓународни стандарди (пример ISO). Дополнително, дури дел од тие препораки и мерки се преточени во конкретни законски акти и решенија, како што е на пример SOX (Sarbanes-Oxley Act of 2002, USA Pub. L. No. 107-204, 116 Stat. 745) регулативата[1].

Во поглед на информативната сигурност, денес може да се идентификуваат повеќе различни иницијативи за изработка и заживување на еден унфициран стандард за имплементација, но и за следење на нивото на заштита на информацијата. Некои од нив се започнати како национални стандарди, кои потоа се објавени дополнително и се прифатени како меѓународни, како, на пример, британскиот стандард - BS 7779, кој е промовиран како меѓународен под името ISO 17799, односно ISO 27001.

Во основа секое регулаторно барање е спецификација на минимум прифатлива имплементација на контроли и мерки за управување на ризиците во рамките на информациските системи (детекција, превенеција и/или корекција). Притоа овие барања може да бидат на ниво на:

- Препорака (discretionary) базирани на принципот на „би требало" (should) или
- Задолжителни (mandatary) базирани на принципот „ќе" (shall), што значи дека станува збор за препораки што мораат да бидат имплементирани, бидејќи се наложени од страна на законски акт или друга повелба од страна на регулаторни тела и субјекти.

Дополнително може да се препознаат два основни главни правци во развојот на стандардите поврзани со сигурноста како што следува:

I Стандарди што ги третираат прашањата на сигурност на едно општо или генерално ниво (ISO 17799/ISO 27001, Common Criteria - ISO 1543, ISO/IEC 13335, ITIL)

II Специјализирани, односно задолжителни барања преточени во стандарди за одредена област, односно деловен процес/индустрија (SOX, HIPAA, Graham Bel).

Во продолжение следи преглед на некои од најважните препораки, односно стандарди што ја третираат областа на информациска сигурност (група I).

[1] Издаден од страна на The American Institute of Certified Public Accountants, www.aicpa.org и прогласен како федерален закон во САД.

Табела: Релевантни стандарди/препораки во делот на информацискатa сигурност

Назив	Издавач/Носител	Домен
ISO/IEC 17799 / BS 7799-1:1999 ***Code of practice for information security management***	Публикуван од страна на меѓународната организација за стандардизација ISO како меѓународен стандард, кој, всушност, произлегува од националниот британски - BS 7799.	Водич, односно работна рамка (анг. framework) со препораки за имплементација и управување со сигурносните ризици и контроли во рамките на информациските системи.
COBIT – Control Objectives for Information and related Technology	IT Governance Institute (www.itgi.org) е основниот издавач и креатор на COBIT - Control Objectives for Information and Related Technology.	Содржи постапки и методологија за процена на адекватноста и целисходноста на преземените контроли и мерки во рамките на информацискиот систем. Акцентот на овој defacto стандард е во воспоставувањето контроли и метрика за усогласување на бизнис- барањата со информацискатa технологија и нејзино успешно менаџирање.
GAISP – Generally Accepted Information Security Principles	Generally Accepted Information Security Principles (GAISP) е објавен од страна на Information Systems Security Association (ISSA).	Универзален стандард што може да се примени на сите нивоа, независно од големината на организацијата.
ISO/IEC 13335 ***Information Technology— Guidelines for the Management of IT Security***	Издавач на овој стандард е меѓународната организација за стандардизација во соработка со комитетот за електротехника позната како ISO/IEC JTC1, поткомисија за сигурност SC27 (IT security techniques).	Прифатлив за сите организации без разлика на нивната големина и профил. Поделен е на повеќе секции кои адресираат различни делови од администрирањето и управувањето со информацискатa сигурност, односно информацискатa технологија воопшто.
ISO/IEC 15408:1999 and *Common Criteria*	Меѓународната организација за стандардизација е издавач на интернационалниот стандард ISO/IEC 15408:1999 *Security Techniques-Evaluation Criteria for IT Security* базиран на *Common Criteria for Information Technology Security Evaluation* (*Common Criteria* или CC).	Common Crtieria односно ISO/IEC 15408:1999 обезбедува разумно ниво осигурување дека процесите, нивната спецификација, евалуација и изведба се во согласност со препораките и контролите за обезбедување на заштитата и интегритетот на информациите.
ITIL – Security Management	Предложен и изработен од страна на United Kingdom's Office of Government Commerce (OGC). (www.itil.co.uk)	ITIL, всушност, преставува кратенка за IT Infrasture Library. Тој содржи препораки и метрика за правилата и насоките при имплементација на системот за управување со процесите во информациските системи, со цел да се обезбеди нивната ефикасност и ефективност.
NIST 800-14 ***Generally Accepted Principles and Practices for Securing Information Technology Systems***	Објавен од страна на The Computer Security Resource Centre при NIST - National Institute of Standards and Technology, USA како дел од NIST's 800 серијата (computer security).	NIST 800-14 ги таргетира менаџерите, професионалците за сигурност, ревизорите и контролните тела, системот развивачи и корисници. Посебно внимание е посветено на контролите во развојот на услугите и сервисите на владините/јавни организации базирани на информатичко- комуникацискатa технологија (e-governance.)

Хронологија	Дополнителни информации
Развојот на препораките почнува во раните 1990-ти од страна на the British Standards Institute . Во 1995 е објавен како BS 7799-1, а потоа и ревидиран во 1999 . Во 2000 е направена негова надополна и тој е објавен како ISO стандард. Во 2002 е објавен вториот дел од стандардот познат како BS7799-2, кој, всушност, преставува надополна со Information Security Management Specification. Во 2005 е објавена новата верзија позната како ISO 27001, која содржи препораки за имплементација на целосен систем за управување со сигурноста на информациските системи - ISMS (information security management system).	ISO 17799 често се користи како генерички термин, кој означува стандард за информативна сигурност иако во суштина тој се состои од две целини: - BS ISO/IEC 17799:2005 (BS 7799 Part 1) *Code of Practice for Information Security*, кој содржи насоки за имплементација на сигурносни контроли по принципот - „you should". - *BS ISO/IEC 27001:2005 (*BS 7799-2) *Information technology, Security techniques Information security management systems -- Requirements* и се користи како мерка/водич при проценатa, односно проверката на ефикасноста на имплементираните контроли, односно претста -вува сертификациски стандард по принципот - „you shell".
Првата верзија на COBIT е објавена во 1996 година, а потоа и негово надополнување во 1998. Во 2000 година е направена нова верзија (3) со воведување нов дел : Management Guideline. Најголемата промена е направена во 2005 година со појавувањето на верзијата 4.0 во кој е вклучен: • COBIT® Security Baseline™ Последната верзија на овој стандард е 4.1 издадена во мај 2007.	Покрај од ITGI, COBIT е поддржан и промовиран од страна на реномираната професионална организација за ревизори на информациски системи : ISACA - Information Systems Audit and Control Association ISACA, (www.isaca.org).
Тековната верзија (вер.3) на овој стандард е од август 2003 и преставува обид за спојување со *Generally Accepted System Security Principles* (GASSP), издаден од International Information Security Foundation (IISF) во 1990s, како и *Commonly Accepted Security Practices and Recommendations* (CASPR).	
Првиот дел од овој стандард е објавен во 1996 додека последниот (дел 5) во 2001. Во 2006 деловите (1) и (2) се изменети и објавени под името „Concepts and Models for ICT Security Management".	ISO/IEC 13335 Information Technology - Guidelines for the Management of IT Security е колекција од 5 дела/документи што покриваат различни аспекти на информациската сигурност.
ISO/IEC 15408:1999 е првпат објавен во 1999. Во 2004 е реализирана нова верзија на *Common Criteria* верзија 2.2. Во 2005 таа е прифатена како ISO/IEC 15408.	Практично преставува обид за обединување на европскиот- ITSEC и северноамериканските критериуми: TSEC, CTCPEC (Canadian Criteria) во една стандардна и усогласена работна рамка и методологија.
ITIL *Security Management* првпат е објавен во 1999. Во 2000 година ITIL е дополнително надграден и прифатен како меѓународен стандард - ISO 20000 (BS 15000).	ITIL, односно ISO 20000 (BS 15000) практично се состои од две целини: - ISO/IEC 20000 Part 1:2005 *"Information technology service management. Specification for Service Management."* - ISO/IEC 20000 Part 2:2005 *"Information technology service management. Code of Practice for Service Management."*
Документот е објавен во декември 1996 година.	NIST 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* е збирка од повеќе документи како што следува: • NIST 800-12 *An Introduction to Computer Security - The NIST Handbook* (октомври 1995) • NIST 800-18 *Guide for Developing Security Plans for Information Technology Systems* (декември 1998)

ЗАКОНСКА РАМКА ЗА ИНФОРМАЦИСКА СИГУРНОСТ

Низа закони во Република Македонија ги регулираат прашањата поврзани со информациите (лични податоци, класифицирани информации) и институциите што поседуваат информации и располагаат со нив, кои треба да се имаат предвид при определувањето на системот за обезбедување сигурност на информациските системи. Она што е карактеристично е дека ниту еден закон не оперира со терминот „безбедност на информациите", иако законите создаваат рамка, а соодветно определени надлежни државни органи обезбедуваат висок степен на заштита на тајноста на податоците.

Законодавството што постои во моментов, во определени мерки ги задоволува ЕУ-стандардите, како и оние на НАТО, кои особено треба да се земаат предвид во контекст на безбедноста на информациите при државните безбедносни системи.

Во ова поглавје прикажани се законските подрачја што се клучни за воведување современ концепт на информациска сигурност, но и областите кои во поширок контекст го допираат прашањето на информациите - нивното собирање, чување, користење, а оттука и нивната безбедност.

Законот за класифицирани информации („Службен весник" на РМ 9/04) ја уредува класификацијата на информациите, условите, критериумите, мерките и активностите што се преземаат за заштита на информациите, правата и обврските на оние што ги создаваат и користат информациите, меѓународната размена и други прашања поврзани со класификацијата на информациите. Неговата цел е да обезбеди законито користење на класифицираните информации и оневозможување секаков вид незаконски пристап до информациите.

Законот дава дефиниции на неколку поими што се од основно значење за безбедноста на информациските системи. Во согласност со законот (член 5):

- „информација" е сознание што може да биде пренесено во која било форма;
- „класифицирана информација" е информација што се заштитува од неовластен пристап или употреба и која се определува со степен на класификација;
- „безбедносен ризик" е можност за нарушување на безбедноста на класифицираната информација;
- „безбедност на класифицираната информација" се активности и мерки со кои се обезбедува заштита на класифицираните информации од неовластен пристап и употреба.

Законот за класифицирани информации дефинира дека со класификацијата на информацијата се определува степенот на заштита на информацијата, која треба да биде соодветна со степенот на штетата што би настанала за Република Македониија од неовластен пристап или неовластена употреба на информацијата.

Информациите што се предмет на класификација се однесуваат особено на: јавната безбеност, одбраната, надворешните работи, безбедносни, разузнавачки и контраразузнавачки активности на органите на државната управа на РМ; системи, уреди, проекти и планови од важност за јавната безбедност, одбраната, надворешните работи; научни истражувања и технолошки, економски и финансиски работи од значење за Република Македонија. Класификацијата на информациите се врши според нивната содржина, при што постојат четири степени на класификација: (1) државна тајна, (2) строго доверливо, (3) доверливо и (4) интерно. Со законот се определува кој вид информации ќе се класифицираат соодветно на определените степени.

Законот определува критериуми, мерки и активности за заштита на класифицираните информации. При утврдувањето на мерките за заштита на класифицираната информација се земаат предвид следниве критериуми:

- степен на класификација
- обем и форма на класифицираната информација
- процена за закана на безбедноста на класифицираната информација

Со законот се определуваат низа мерки и активности за административна, физичка, информатичка и индустриска безбедност, како и безбедност на лицата.

Мерки и активности за безбедност на информациите, во согласност со член 28, се:

- сертификација на комуникациско-информациските системи и процеси;
- процена на можно нарушување на безбедноста на класифицираната информација со упад во информатичкиот ситем и употреба и уништување на класифицираната информација обработувана и чувана во комуникациско-информациските системи;
- утврдување методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицираните информации во електронска форма;
- заштита на информациите при процесирање и чување на класифицирани информации во комуникациско-информациските системи;
- продукција на крипто-клучеви и друг крипто-материјал;
- криптографска заштита на комуникациски, информациски и други електронски системи, преку кои се подготвуваат, пренесуваат, обработуваат и архивираат класифицираните информации;
- определување зони и простории заштитени од компромитирачко електромагнетско зрачење и
- инсталирање уреди за чување на класифицираните информации.

Заштитата на личните податоци како основни слободи и права на граѓаните, а особено правата на приватност во врска со обработката на личните податоци, се остварува во согласност со **Законот за заштита на лични податоци** („Службен весник" на РМ бр. 7/05), кој ја обезбедува правната и институционална рамка за заштита на податоците.

Во согласност со овој закон (член 2, точка 1):

- „личен податок" е секоја информација што се однесува на индентификувано физичко лице или физичко лице, кое може да се идентификува, а лице што може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на единстен матичен број на граѓанинот или врз основа на едно или на повеќе обележја специфични за неговиот физички, ментален, економски, културен или социјален идентитет.
- „обработка на лични податоци" е секоја операција или збир на операции што се изведуваат врз лични податоци, на авоматски или на друг начин, како

што се: собирање, евидентирање, организирање, чување, приспособување или промена, повлекување, консултирање, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, изедначување, комбинирање, блокирање, бришење или уништување.
- „контролор на збирка на лични податоци" е физичко или правно лице, државен орган или друго тело, кое самостојно или со други ги утврдува целите и начинот на обработката на личните податоци.

Обработката на личните податоци, по правило се врши со претходно добиена согласност од субјектот на личните податоци. Забранета е обработка на посебни категории лични податоци, а тоа се податоци што го откриваат расното или етничкото потекло, политичкото, верското или друго уверување, членство во синдикална организација и податоци што се однесуваат на здравствената состојба или на сексуалниот живот. Посебен режим на заштита се предвидува за обработката на единствениот матичен број на граѓанинот.

Законот предвидува тајност и заштита на обработката на личните податоци. Секое лице што има пристап до збирката лични податоци во име на контролорот или обработувачот на збирката лични податоци, вклучувајќи го и самиот обработувач на збирката лични податоци, должен е да обезбеди тајност, заштита на личните податоци и да ги обработува во согласност со овластувањата и инструкциите добиени од контролорот, доколку со друг закон не е утврдено поинаку.

За да се обезбеди тајност и заштита на обработката на личните податоци на субјектот, контролорот мора да примени соодветни технички и организациски мерки што одговараат на опремата и на трошоците што се потребни за нивно спроведување, а се однесуваат на:

- оневозможување случајно или незаконско уништување на податоците од збирките лични податоци;
- оневозможување неовластено преправање, откривање или пристап при обработка на личните податоци од збирката лични податоци;
- оневозможување незаконска обработка на личните податоци од збирките лични податоци, особено доколку вклучува пренос на податоците преку мрежа;
- оневозможување пристап на неовластени лица до опремата што се користи за обработка на збирката лични податоци;
- оневозможување неовластено читање, копирање, промена или отстранување медиум, на кој е сместена збирката лични податоци;
- оневозможување неовластено читање, внесување, промена или бришење на податоците од збирката лични податоци;
- оневозможување пристап на корисниците на збирките лични податоци до податоци за кои немаат право да ги обработуваат;
- можноста дополнително да се провери кој пристапил до системот и кои податоци од збирката лични податоци ги читал, внел, променил или избришал, во кое време го направил тоа и од кој уред пристапил;
- оневозможување неовластен пристап до збирката лични податоци од друга локација преку комуникациски уреди;
- оневозможување читање, копирање, промена или бришење податоци при нивен пренос преку комуникациски уреди или при транспорт на медиумот, на кој е сместена збирката лични податоци;
- можност да се провери од кои локации преку комуникациски уреди може да се пристапи до податоците;
- организирање на работата во согласност со посебните барања за заштита на збирката лични податоци и
- оневозможување други форми на незаконска обработка.

Овие мерки треба да обезбедат степен на заштита на личните податоци соодветно на ризикот при обработката и природата на податоците што се обработуваат. Примената на соодветни технички и организациски мерки ја пропишува директорот на Дирекцијата за заштита на личните податоци[1]. Контролорот и обработувачот на збирката лични податоци се должни да водат евиденција на преземените технички и организациски мерки.

Законот во голема мера е усогласен со Директива 95/46/ЕК на Европскиот парламент и Советот на Европа од 24 октомври 1994 за заштита на личните податоци и слободното движење на податоците и Конвенција бр.108/81 за заштита на физичките лица, која се однесува на автоматската обработка на личните податоци, Совет на Европа[2].

Законот за слободен пристап до информации од јавен карактер („Службен весник" на РМ 13/06) ги пропишува условите, начинот и постапката за остварување на правото на слободен пристап до информациите од јавен карактер со кои располагаат имателите на информации[3]. Правото на пристап до информациите го опфаќа правото на лицето овластено да побара информација (сите физички и правни лица) да побара и да добие информација од имателите на информации, како и обврска на имателите на информации да ги направат достапни до јавноста.
Правото на пристап до информациите не ја исклучува потребата за заштита на информациите и грижата за нивната безбедност и не значи дека сите имаат право на пристап до сите информации што ги поседуваат, со кои располагаат или што ги надгледуваат органите на јавната власт (државни или локални).

Имателите на информации ќе одбијат барање за пристап до информацијата, ако побараната информација е:
- класифицирана информација со соодветен степен на тајност;
- личен податок чие откривање би значело повреда на заштитата на личните податоци;
- информација за архивското работење која е утврдена како доверлива;
- информација чие давање би значело повреда на доверливоста на даночната постапка;
- информација стекната или составена за истрага, кривична или прекршочна постапка, за спроведување на управна и граѓанска постапка, а чие давање би имало штетни последици за текот на постапката;
- информација што се однесува на комерцијални и други економски интереси, вклучувајќи ги и интересите на монетарната и фискална политика и чие

[1] Правилникот за техничките и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци е донесен на 19 декември 2005 година http://www.dzlp.gov.mk.
[2] Г-ѓа Маријана Марушиќ, директор на Дирекцијата за заштита на лични податоци, презентација на Втората меѓународна конференција е-Општество.Мк, 15.11.2006.
[3] органите на државната власт и други установи и институции утврдени со закон, органите на општините, на градот Скопје и на општините во градот Скопје, јавните установи и служби, јавните претпријатија, правни и физички лица што вршат јавни овластувања и дејност од јавен интерес, утврдени со закон.

давање ќе има штетни последици во остварувањето на функцијата;
- информација од документ што е во постапка на подготвување и сé уште е предмет на усогласување кај имателот на информации, чие откривање би предизвикало погрешно разбирање на содржината;
- информација за заштита на животната средина, која не е достапна до јавноста заради заштита на здравјето на луѓето и животната средина и
- информација што ги загрозува правата од индустриска или интелектуална сопственост (патент, модел, мостра, стоковен и услужен жиг, ознака на потеклото на производот).

Пристап до овие информации, може да се одобри по исклучок ако со објавувањето на таквата информација последиците врз интересот што се заштитува се помали од јавниот интерес кој би се постигнал со објавувањето на информацијата.

Законот за електронски комуникации („Службен весник" на РМ 13/05) предвидува обврска за операторите на јавни комуникациски мрежи и давателите на јавни комуникациски услуги, поединечно или заеднички, доколку е потребно да донесат соодветни технички и организациски мерки за да обезбедат заштита на нивните мрежи и/или услуги. Мерките мора да обезбедат ниво на безбедност и заштита, соодветна на можни ризици, при чие утврдување е потребно да се имаат предвид техничката оправданост и применливост.

Доверливоста на комуникациите се однесува на а) содржината на комуникациите; б) податоците за сообраќајот и локацијата кои се однесуваат на комуникациите и в) неуспешните обиди за воспоставување конекција. Во согласност со Законот (член 111, став 2) забранети се сите форми на следење, прислушување, прекинување, снимање, чување, пренесување и пренасочување на комуникациите. Операторите на јавните комуникациски мрежи и давателите на јавни комуникациски услуги, нивните застапници, вработените, претставниците и други лица под нивно раководство и контрола се должни да ја штитат доверливоста на комуникациите и по престанувањето на активностите во текот на кои тие биле обврзани да ја штитат доверливоста, Снимањето на комуникациите е под посебен режим во законот. Тоа е дозволено заради обезбедување доказ за пазарните трансакции или за каква било друга деловна комуникација или во рамките на организациите што примаат итни повици заради нивна евиденција, идентификација и постапување.

Прислушувањето на комуникациите, како начин на пристап до информациите, е законски регулирано. **Законот за следење на комуникациите** („Службен весник" на РМ бр.121/06) ги уредува условите и постапката за следење на комуникациите, начинот на постапување, чување и користење на добиените информации и податоци со примената на овој закон и контролата на законитоста на следењето на комуникациите. Следењето на комуникациите се врши со наредба на надлежен суд, освен ако му се наменети или постои согласност на лицето или лицата што се вклучени во комуникацијата. Во согласност со законот за електронски комуникации, операторите, преку кои се врши законското прислушување на комуникациите, се должни да обезбедат трајна евиденција за законското прислушување на комуникациите и да ги заштитат овие податоци како тајна во согласност со законот. Сите податоци, списи и други материјали собрани преку следење на комуникациите се доставуваат до надлежниот суд во рокот определен со наредбата за следење на комуникациите и тие се чуваат под посебен режим од страна на судот.

Кривичното законодавство претрпе измени кои доведуваат до инкриминација на делата насочени кон загрозување на приватноста и информатичката сигур-

СИГУРНОСТ ЗА ДРЖАВНИ ИНСТИТУЦИИ

А. Изработка и донесување потребна законска рамка за подобрена информациска сигурност;
Таа "рамка" треба да содржи, пред сé, а и во согласност со постоечките меѓународни декларации и конвенции/директири:
- Национална политика и стратегија за информациска сигурност
- Измена на закони за битни сфери кои се специјално чувствителни на информациската небезбедност (електронска трговија, е-Влада, финансиски систем, здравствен систем,...)
- Акциски планови за секоја државна институција за спроведување минимални информатичко-безбедносни мерки со придружен национален буџет
- Обезбедување организациска поддршка во државните институции и јавните претпријатија, имателите на информации, на мерките за информациска сигурност (функција/сектор за информациска сигурност, одговорно лице - CISO Chief Information Security Officer)

Б. Активности на национално ниво;
- Покренување акции за зголемување на свеста за постоењето и важноста на информациската небезбедност, ризиците поврзани со тоа и потребата за подготвеност за заштита и брзо закрепнување во случај на реализиран информациски инцидент / напад.

Субјекти за кои би биле наменети предложените акции се :
- Граѓаните и нивните домаќинства;
- Институциите од невладиниот сектор;
- Стопанскиот сектор;
- Државните институции, локалната самоуправа и јавните претпријатија;
- Обезбедување соодветна државна организациска инфраструктура за справување со информациски инциденти (Центри за регистрација на информациски инциденти и поддршка).

В. Активности поврзани со образование и дисеминација на препораките за зголемување на информациската сигурност за сите засегнати странки (граѓани, стопански субјекти);

Г. Активности поврзани со учество во меѓународни соработки, проекти и активности за борба против информациските инциденти;

Д. Обезбедување финансиска поддршка и други олеснувачки мерки за зголемување на информациската сигурност за сите засегнати странки (граѓани, организации од невладиниот сектор и стопанските организации).

ност. Кривичниот закон на РМ („Службен весник" на РМ бр. 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06) во член 147 - Повреда на тајноста на писма или на други пратки, предвидува парична казна или казна затвор до 6 месеци за лицето кое без судска одлука или согласност на лице на кое му се упатени ќе отвори туѓо писмо, телеграма, некое друго затворено писмено известување или пратка или обезбедена електронска пошта или на друг начин ќе ја повреди нивната тајност или ќе задржи, прикрие, уништи или на друг ќе му предаде туѓо писмо, телеграма, затворено писмено известување или пратка или обезбедена електронска пошта. Ако делото е сторено со намера за себе или за друг да се прибави корист или да се нанесе штета, делото ќе се казни со парична казна или казна затвор до 1 година. Ако делото е сторено од службено лице казната е од три месеци до три години, односно од три месеци до пет години. Гонењето се презема по приватна тужба.

Во случаите на злоупотреба на лични податоци (член 149), лицето што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година. Оваа казна му се заканува и на лицето што ќе навлезе во компјутерски информатички систем на лични податоци со намера, користејќи ги за себе или за друг да оствари некаква корист или на друг да му нанесе некаква штета. Ако делото го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години, а доколку го стори правно лице, ќе се казни со парична казна. Казнив е и обидот за извршување на ова дело. Во согласност со КЗ, (член 149-а), тој што неовластено спречува или ограничува друг во пристапот кон јавен информатички систем, ќе се казни со парична казна или со затвор до една година. Ако делото го стори службено лице во вршење на службата или одговорно лице во јавен информатички систем, ќе се казни со парична казна или со затвор од три месеци до три години. Гонењето се презема по приватна тужба. Неовластеното прислушување и тонско снимање е санкционирано на начин што законот со член 151 предвидува парична казна или затвор до 1 година за лицето што со употреба на посебни уреди неовластено прислушува или тонски снима разговор или изјава што не му е наменета. Со оваа казна ќе се казни и тој што ќе му овозможи на неповикано лице да се запознае со разговор или со изјава која е прислушувана или тонски снимана, како и лицето што тонски ќе сними изјава што му е наменета, без знаење на оној што ја дава, со намера да ја злоупотреби или да ја пренесе врз трети лица или тој што таквата изјава непосредно ја пренесува врз трети лица. Ако делото го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години. Гонењето за делото се презема по приватна тужба, освен во случаите кога е сторено од службено лице.

Во кривичните дела против имотот КЗ ги нормира: оштетување и неовластено навлегување во компјутерски систем (член 251), правење и внесување на компјутерски вируси (член 251-а) и компјутерска измама (член 251-б). Оштетувањето и неовластеното навлегување во компјутерски систем подразбира парична казна или казна затвор до три години за лицето што неовластено ќе избрише, измени, оштети, прикрие или на друг начин ќе направи неупотреблив компјутерски податок или програма или уред за одржување на информатичкиот систем или ќе го оневозможи или отежне користењето на компјутерскиот систем, податокот или програмата или компјутерската комуникација. Оваа казна е предвидена и за лицето што неовластено ќе навлезе во туѓ компјутер или систем со намера за искористување на неговите податоци или програми заради прибавување противправна имотна или друга корист за себе или за друг или предизвикување имотна или друга штета или заради пренесување на компјутерските податоци што не му се наменети и до кои неовластено дошол на неповикано лице. Притоа ако со извршување на овие дела е прибавена поголема имотна корист или е предизвикана поголема штетата, казната е затвор од шест месеци до пет години. Ако овие дела се сторени кон компјутерски систем, податоци или програми што се заштитени со посебни мерки на заштита или се користат во работењето на државните органи, јавните претпријатија или јавните установи или во меѓународни комуникации или како член на група создадена за вршење такви дела, казната е затвор од една до пет години, а кога со извршување на делото е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од една до десет години. Лицето што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети или погодни за извршување на овие дела, ќе се казни со парична казна или со затвор до една година. Обидот за делото е, исто така, казнив, а посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото се одземаат.

Лицето што ќе направи или ќе преземе компјутерски вирус од друг, со намера за внесување во туѓ компјутер или компјутерска мрежа, ќе се казни со парична казна или со затвор до една година. Тој што со употреба на компјутерски вирус ќе предизвика штета во туѓ компјутер, систем, податок или програма, ќе се казни со затвор од шест месеци до три години, а ако со делото е предизвикана поголема штета или делото е сторено во состав на група создадена за вршење такво дело, сторителот ќе се казни со затвор од една до пет години. Казнив е и обидот. Компјутерска измама е кривично дело од понов датум. Со член 251-б се определува дека лицето што со намера за себе или за друг ќе прибави противправна имотна корист со внесување во компјутер или информатички систем невистинити податоци, со невнесување на вистинити податоци, со фалсификување електронски потпис или на друг начин ќе предизвика невистинит резултат при електронската обработка и преносот на податоците, ќе се казни со парична казна или со затвор до три години. Ако сторителот прибавил поголема имотна корист, ќе се казни со затвор од три месеци до пет години, а ако сторителот прибавил значителна имотна корист, ќе се казни со затвор од една до десет години. Тој што компјутерската измама ја сторил само со намера да оштети друг, ќе се казни со парична казна или со затвор до една година. Ако со делото е предизвикана поголема штета, сторителот ќе се казни со затвор од три месеци до три години.

Сигурноста на информациските системи е од посебна важност при обезбедувањето на електронската трговија. Иако ова прашање во Република Македонија не е сé уште целосно законски уредено, одредбите што се поврзани со тоа се наоѓаат во Законот за облигациски односи и во Законот за податоците во електронски облик и електронски потпис.

Во согласност со **Законот за облигациски односи** („Службен весник" на РМ 18/01 и 4/02), примањето и испраќањето изјави на волјата, со цел склучување договор е можно и преку електронски пат (член 23, 23-а, 23-б и 23-в), како и составувањето исправа како форма на договорот (член 64). Притоа треба да се обезбеди сигурност за идентитетот на испраќачот и содржината на информацијата.

Електронското работење, кое вклучува употреба на информатичка и телекомуникациска технологија и употреба на податоци во електронски облик и електронски потпис и во судски, управни постапки во платниот промет е уредено и регулирано со **Законот за податоци во електронски облик и електронски потпис** („Службен весник" на РМ бр. 34/01). Со овој закон се определува времето и местото на праќање и прием на електронската порака; начинот на зачувување на документите, записите и податоците на електронски начин; електронскиот потпис и неговата доказна форма, начинот на издавање на квалификувани сертификати, нивната форма и содржина, како и правата и обврските на издавачите на сертификати. Законот предвидува казни за несоодветно чување или употреба на податоците и средствата за електронско потпишување.

Специфичните закони што уредуваат прашања на различни евиденции содржат одредби за заштита на податоците со кои располагаат. Еден од нив, на пример, е **Законот за матична евиденција на осигурениците и корисниците на правата од пензиско и инвалидско осигурување** („Службен весник" на Република Македонија бр. 16/04). Со овој закон се уредува матичната евиденција за осигурениците и корисниците на правата од пензиско и инвалидско осигурување, која содржи податоци потребни за остварување на правата од пензиско и инвалидско осигурување. Во матичната евиденција се водат податоци за осигурениците, корисниците на правата од пензиско и инвалидско осигурување и обврзниците за плаќање на придонес за пензиско и инвалидско осигурување. Во прибирањето, обработката, користењето, размената и чувањето на податоците, според овој закон, се применуваат одредбите од законот што ја уредува заштитата на личните податоци, ако со овој закон поинаку не е определено. Матичната евиденција ја воспоставува и ја води Фондот за пензиско и инвалидско осигурување на Македонија. Матичната евиденција ја воспоставува и ја води Фондот за пензиско и инвалидско осигурување на Македонија во електронски облик. Техничките и организациските мерки за обезбедување на податоците од матичната евиденција, Фондот ги определува со општ акт.

Кога станува збор за заштита на информациите и законодавството што го уредува ова прашање, предвид треба да се земе и **Уредбата за канцелариско и архивско работење** („Службен весник" на РМ, бр 58/1996 год). Со овој пропис се уредува начинот на работа и правилата на постапување со документарниот материјал и архивската граѓа во канцелариското и архивското работење на сите иматели во Република Македонија (државни органи, претпријатија и други правни лица).

Првиот дел од уредбата, кој се однесува на „канцелариското работење", ги регулира следниве прашања: прием, прегледување, распоредување и заведување на актите, нивно доставување за работа и административно-техничка обработка, разведување и класифицирање на актите, одлагање на решените акти во писарницата. Вториот дел од уредбата се однесува на „архивското работење" на имателите. Во него се регулираат следниве прашања: одбирање на архивската граѓа од документарниот материјал; евидентирање и категоризација на архивската граѓа; попишување и уништување на документарниот материјал; чување, заштита и обезбедување на материјалот и граѓата; предавање на архивската граѓа во Државниот архив.

Уредбата дефинира обврска за одбраната архивска граѓа да се чува, обезбедува и да се заштитува од секаков вид отуѓување, оштетување и уништување, меѓутоа не предвидува посебни правила за начинот на кој ќе се спроведува оваа обврска.

Меѓународни иницијативи

Директивата 46/95/ ЕЗ позната и како Директива на ЕУ за заштита на податоците (European Union Data Protection Directive (EUDPD)) поставува барање до земјите-членки да усвојат национална регулатива со која ќе се стандардизира заштитата на приватноста на податоците на граѓаните низ цела Европска Унија.

Законите за задржување податоци (EU Data Retention laws) бараат од лицата што обезбедуваат јавни комуникациски услуги (интернет и телефонија) да чуваат податоци за секоја испратена електронска порака и оставен телефонски повик во период од 6 месеци до 2 години.

Со резолуцијата на Советот на ЕУ 2002/С 43/02 од 28/01/2002 се дефинирани специфични активности во рамките на мрежната и информациската сигурност за земјите-членки, во кој спаѓаат:

- Промоција на стандардот ISO 15408 (Common Criteria), со цел да се усогласат различните подрачја и имплементации на сигурносните контроли;
- Примена на интероперабилни сигурносни решенија втемелени на препознатливи и потврдени норми и технологии (на пример: користење дигитални сертификати и потписи) во е-услугите имплементирани во земјите-членки на ЕУ;
- Соработка меѓу институциите во поглед на компјутерскиот криминал, односно воспоставување унифициран тим за реакција и за справување со сигурносните ризици и напади преку формирање на таканаречените инцидент менаџмент тим - (CERT - Computer Emergency Response Team).

Дополнително, преку акциски план за е-Европа (i2010 - A European Information Society for growth and employment) се предлага формирање и функционирање на Cyber security task force (CSTF), преку кој ќе се реализира висок степен на сигурност преку размена на класифицирани информации по строго утврдени правила и норми. Дополнително, во сите свои законски акти и програми за развој на е-услугите може да се препознае јасната и недвосмислена заложба на ЕУ и на нејзните органи за усогласување на законските норми за системско решавање на прашањата и проблемите во сите сфери од дејствувањето во поглед на информативната сигурност. Во таа насока, во согласност со уредбата на Европскиот парламент и Советот на Европа, воспоставена е Европска агенција за мрежна и информатичка сигурност наречена: (European Network and Information Security Agency - ENISA, Regulation (EC) No 460/2004 of the

European Parliament and the Council of 10 March 2004, OJ L 77, 13 March 2004). Оваа агенција, државните институции треба да ги координира, усогласи и да ги решава проблемите на ниво на владините органи и да работи на една поширока основа во граѓанскиот и невладин сектор, со цел да се обезбедат сигурни и квалитетни е-сервиси и услуги. ЕНИСА е замислена како централно место за координација на сите сигурносни активности во рамките на Европската Унија.

Покрај овие европски - повеќе или помалку признаени и потврдени стандарди и иницијативи, треба да се напоменат и неколку законски акти и правилници што се донесени во САД, од кој како поважни може да ги наведеме:

- Законот за компјутерска сигурност од 1987 г. (**Computer Security Act**), издаден од страна на Националниот институт за стандарди и технологија (**National Institute of Standards and Technology - NIST**) и се однесува, пред сé, на стандардите и на препораките што треба да ги исполнат копмјутерските системи во државните органи. Посебно е интересено што во овој текст како задолжителна активност се наведува потребата од постојана едукација и надградба на сите учесници и корисници на информациските системи кои располагаат со чувствителни информации;
- Закон за реформа на владината информациска безбедност од 2000 г. (**GISRA - Government Information Security Reform Act**);
- Законот Патриот акт од 2001 г. (**USA Patriot Act**) со посебен акцент на правилата и методите за следење на електронските комуникации и откривањето и компјутерскиот криминал;
- Закон за менаџмент на информациска безбедност на федерално ниво од 2002 г. (**Federal Information Security Management Act - FISMA**).

Како поставен стандард треба да се имаат предвид и некои компаративни решенија, исто така од САД.

- Законот за преносливост и одговорност за здравствено осигурување (**Health Insurance Portability and Accountability Act - HIPAA**) поставува барање пред организациите што обезбедуваат здравствена заштита, организациите што обезбедуваат здравствено осигурување и работодавачите да обезбедуваат заштита и приватност на податоците за здравствената сотојба на корисниците на услуги, осигурениците, односно вработените.
- Законот Грам-Лич-Блајлеј од 1999 г. (**Gramm-Leach-Bliley Act - GLBA, 1999**), познат и како Закон за модернизација на финансиските услуги, ги штити приватноста и безбедноста на приватните информации кои ги собираат, чуваат и процесираат финансиските институции.
- Законот Сарбанес-Оксли од 2002 г. (**Sarbanes-Oxley Act - SOX, 2002**), оддел 404 бара од компаниите што излегуваат на јавниот пазар на капитал да ја проценат ефективноста на нивната внатрешна контрола на финансиското известување во годишните извештаи што ги поднесуваат на крајот на секоја фискална година. Главните офицери за информации (**Chief Information Officers**) се одговорни за безбедноста, точноста и за веродостојноста на сисемите што управуваат и известуваат за финансиските податоци. Законот, исто така, наложува овие компании да бидат подложни на надворешна ревизија, која мора да провери, односно да потврди и да извести за валидноста на дадените извештаи од страна на компаниите.
- Стандардот за безбедноста на податоците на индустријата на платежни картички (**Payment Card Industry Data Security Standard - PCI DSS**) утврдува низа значајни барања за унапредување на безбедноста на информациите на платните сметки. Беше развиен од страна на водечките компании во индустријата на платежни карички, (**American Express, Discover Financial Services, JCB, MasterCard Worldwide, Visa International**), како поддршка на процесот на усвојување на конзистентни мерки за безбедност, а податоците на глобално ниво. Овој стандард опфаќа постапки за управување со безбедноста, политики, постапки, архитектура на мрежата, дизајн на софтвер и други критични заштитни мерки.

Локална самоуправа

Единиците на локалната самоуправа имаат избрани советници, перманентно вработени, привремено вработени и надворешни даватели на услуги, како на самата единица, така и на граѓаните.

Со самото вработување и можност/потреба за користење на компјутерскиот систем во единицата на локалната самоуправа, секој советник, вработен и надворешен корисник треба да бидат запознати со правилата на безбедно и овластено користење на комјутерските ресурси. Сите надворешни добавувачи на сервиси треба да ги почитуваат тие правила и да одговараат за нивното почитување со т.н. Договори за доверливост. Непрекинатиот надзор на користењето на компјутерскиот систем треба да биде редовна практика.

Информациската безбедност е тука за да остане! Целиот процес започнува со донесување политика за информациска безбедност и потоа се надградува со „добри безбедносни" постапки и процедури, кои постојано се надградуваат. Притоа редовно се следи и се подобрува системот на правата и обврските за информациска безбедност.

Десет принципи за информациска безбедност

1. Назначете *одговорно* лице за информациска безбедност во единицата на локалната самоуправа.
2. Научете како да осознаете дека имате информациско- безбедносен проблем, закана или напад.
3. Научете и подгответе се да се справувате со појавени информациски инциденти.
4. Физички обезбедете ги информациските ресурси (компјутери, податоци, комуникации).
5. Осигурајте ги основните и битните информациски ресурси (бекап, резервна опрема, резервна локација).
6. Дозволете пристап до компјутерите ИСКЛУЧИВО на овластени лица и обезбедете заштита од неовластени корисници.
7. Обезбедете ги информациите (криптирање).
8. Тренинг, тренинг и постојано тренинг!
9. Дефинирајте ја политиката на информациската безбедност и политика за дозволена употреба на компјутери и информации.
10. Обезбедете средства, ресурси и постапки за „регулирано" уништување на постоечките, а сега непотребни информации и компјутери.

СИСТЕМ ЗА УПРАВУВАЊЕ СО ИНФОРМАЦИСКА СИГУРНОСТ

Постигнувањето информациска сигурност е континуиран процес кој претставува комплексен систем од методологии, активности и мерки. Притоа, функционалниот и сигурен информациски систем во најширока смисла на зборот се темели на исполнување на следниве начела:

- **Доверливост** (анг. Confediality) - информацијата не смее да биде достапна или откриена на неовластени лица;
- **Интегритет** (анг. Integrity) - информацијата не смее неовластено или непредвидено да се менува;
- **Достапност** (анг. Availability) - информацијата е достапна во моментот кога има потреба за тоа;
- **Неодречивост** (анг. Non-Repudiation) - неможност за одрекување на активностите поврзани со користење и пристап на информациите;
- **Докажливост** (анг. Accountability) - активностите поврзани со манипулација и пристап до информацијата може да бидат еднозначно забележани и евидентирани;
- **Автентикација** (анг. Authentication) - идентитетот на субјекот и неговите права на пристап до информацијата може еднозначно да се утврди/идентифицира и контролира.
- **Надежност** (анг. Reailability) - обезбедува очекувано и предвидливо однесување, односно состојба на информацискиот систем.

Нарушувањето на некои од овие начела, всушност, значи нарушување на сигурноста на информацискиот систем. Во основа може да се заклучи дека се можни следниве закани и потенцијални нарушувања на нормалното функционирање, кое може да доведе до:

Губење на интегритетот: Интегритетот, всушност, означува потреба информацијата и соодветните информатичко-комуникациски средства да бидат заштитетни од неовластени и несоодветни промени. Ваквите неконтролирани промени во содржината на информацијата значи нарушување на нејзината точност/коректност, односно компромитирање на нејзината валидност и применливост. Нарушениот интегритет на информацијата доведува до погрешно интерпретирање и донесување погрешни заклучоци.

Губење на достапноста: Ова практично означува нарушување на нормалното - очекувано оперативно функционирање на информацискиот систем. Со други зборови, информацијата не е достапна во моментот кога е навистина потребна.

Губење на доверливоста: Неовластено, неавторизирано откривање и пристап до информациите од страна на субјекти/процеси што немаат дозвола за тоа.

Процесот на информативната сигурност треба да биде дизајниран на начин што ќе овозможи, пред сé, да се идентификуваат, мерат, контролираат и следат ризиците поврзани со доверливоста, интегритетот и расположивоста на информациите на една континуирана основа. Ваквиот пристап промовиран од ISO 17799 и ISO 27001 е познат како PDCA (Plan – Do – Check – Act), модел кој се состои од следниве целини (субпроцеси):

1. Планирање на процесот, кој опфаќа:
- Процена на ризикот - континуиран процес на идентификација на слабостите и заканите кон информативните системи. Процесот треба да ја идентификува можноста и фреквенцијата на појавување на заканите за да се утврди евентуалната штета, која би настанала доколку тие се случат;
- Изработка на политика за сигурност на информацис-

КОДЕКС ЗА ИНФОРМАЦИСКА СИГУРНОСТ

Општи одредби

Сигурноста на информациските системи опфаќа безбедносни прашања поврзани со правилно манипулирање и управување со информациите кои се од крајна важност за непречено и за ефикасно одвивање на општествените и деловни процеси.
Секој учесник во процесот - корисник на информацискиот систем е должен да се придржува кон позитивните прописи и законски регулативи, но и кон највисоките начела и норми на однесување, интегритет и чесност при секоја комуникација и користење на информациите. Само на таков начин ќе може да се даде полн придонес во градењето на сигурноста, доверливоста, интегритетот, ефикасноста и квалитетот на информацискиот систем, односно на услугите и на сервисите што се базирани на информатичко-комуникациската технологија.

Сигурноста на информациските системи се дефинира како обезбедување на:

- **Доверливост** - информацијата е достапна само на авторизирани корисници што имаат право на пристап;
- **Интегритет** - заштита на точноста и комплетноста на информацијата и на методите на обработка;
- **Расположивост** - авторизираните корисници имаат пристап до информацијата и до другите придружни средства потребни за нејзина презентација,чување и за дистрибуција во моментот кога има потреба за тоа.

Основни одредби

- Сигурноста на информациските системи е одговорност за секој корисник во информацискиот систем;
- Секој корисник е должен да работи во согласност со законските и подзаконските акти кои ја регулираат областа на информациската сигурност;
- Секој корисник е должен да работи во согласност со интерната корпоративна политика за сигурност на информациските системи и соодветните процедури и упатства што произлегуваат од неа;
- Секој корисник е должен да овозможува непречена внатрешна контрола и ревизија на неговото работење, како и контрола од страна на овластени релевантни надворешни органи;

Користење информатичка опрема

- Користењето на персоналните, преносните компјутери и преносната меморија (USB, дискети, CD-a) мора да биде во согласност со одредбите од интерната корпоративна политика при што секој корисник треба да биде свесен за опасностите што може да се предизвикаат поради неправилно манипулирање со нив;
- Софтверот што се користи мора да е поддржан од лиценцен договор кој специфично ги опишува правата на користење и ограничувањата на производот. Секој корисник мора да се придржува кон одредбите од договорот и не смее незаконски да се

ките системи - секој сопственик на информацискиот систем е должен да донесе политика за сигурност на информацискиот систем, кој ќе претставува стратегија (план) на менаџментот за управување со идентификуваните ризици (од претходниот чекор). Оваа политика треба да биде во согласност со програмата за информатичка сигурност на Р. Македонија, позитивните законски прописи, како и соодветните светски стандарди од оваа област (како што е ISO 27001/БС7799) и да биде практична потврда на посакуваното ниво на адекватна сигурност на информацискиот систем, во согласност со извршената анализа на ризици и закани;

2. Имплементација на сигурносни контроли - секој сопственик на информацискиот ситем е должен да воспостави административни, физички и технички контроли, со кои ќе се изврши заштита на сигурноста на информациите и системите на повеќе нивоа;

3. Тестирање и проверка на сигурноста - секој сопственик на информацискиот систем е должен да воспостави процес на професионално, независно и објективно тестирање и проверка на ефикасноста и адекватноста на имплементираните контроли содржани во политиката за информативната сигурност;

4. Надградба и корекција - секој сопственик на информацискиот систем е должен да воспостави процес на континуирано прибирање и анализа на информациите од аспект на новите закани и слабости, актуелни напади кон информацискиот систем комбинирани со ефикасноста на постојните сигурносни контроли.

Управувањето со сигурноста е комплексен и континуиран процес што ги опфаќа: луѓето (субјекти), процесите, организациската поставеност и користена технологија и следствено истиот треба да биде базиран на прецизно и јасно планирање кое може да биде:

- Стратегиско, кое опфаќа прашања поврзани со посакуваното ниво на сигурност, целите и потребата за сертификација, односно акредитација;
- Тактичко или среднорочно, кое опфака дизајн и имплементација на планираните сигурносни контроли и мерки;
- Оперативно или краткорочно, кое опфаќа секојдневни активности и мерки за контрола и мониторинг на сигурноста (анг. day-to-day activity).

Сигурноста на информацискиот систем може да се обезбеди преку повеќе нивоа на контроли: физички, технички и административни. Овие три категории може дополнително да бидат поделени на контроли за спречување, за откривање или, пак, контроли што се користат за минимизирање, односно коригирање на евентуалните штети настанати како резултат на нарушувањето на сигурносните начела.

- **Физички контроли** кои служат за обезбедување адекватна физичка сигурност во информативниоит систем. Како примери на физички контроли се: употребата на брави, чуварска служба, бедеови, аларми и слични мерки за контрола на пристапот до ресурсите. Овие мерки имаат за цел да спречат можни закани од типот на шпионажа и саботажа, отуѓување и уништување или оштетување од несреќен случај или природна катастрофа (поплава, земјотрес...).
- **Технички или логички контроли** кои се вградени во информатичката опрема, апликативниот софтвер, комуникациската опрема и придружните уреди (како на пример: антивирусна заштита, енкрипција/шифрирање на преносот, автентикација, пристапни листи, употреба на огнени ѕидови - firewall и слично).
- **Административни контроли** вклучуваат воспоставување политики, стандарди, упатства.

копираат и дистрибуираат програми и/или делови од програмски кодови надвор од одредбите на лиценцниот договор;

- Секој корисник треба да се грижи совесно и професионално за доделената компјутерска и комуникациска опрема (персонален или преносен компјутер, печатач, мобилен телефон и друго), да ја заштити од оштетување и од неовластен пристап;
- Секој корисник е должен да го унапредува своето основно познавање на работа со компјутерската технологија, со цел да се обезбеди сигурност и ефикасност во ракувањето со ресурсите, како и заштита на инсталираниот софтвер и податоците од оштетување, бришење, губење и слично;
- Секоја неправилност или сомнителна активност во функционирањето на компјутерската опрема треба да се пријави во соодветниот тим за справување со сигурносни инциденти - таканаречениот Computer Emergency Response Center, CERT;
- Инсталацијата и конфигурацијата на нови хардверски модули, софтверски изданија, програми за надградување, парцијални и помошни програми треба да се вршат само од страна на овластени и стручни лица во согласност со прирачниците и правилата за користење;
- Креирањето резервни копии (backup) на податоците потребно е да се прави со соодветна динамика во согласност со сензитивноста на процесите и на сервисите;

Пристап до информативните системи

- Корисниците на информацискиот систем мора да се идентификуваат единствено и нивниот пристап во компјутерскиот систем мора да биде авторизиран од страна на релевантно лице - раководител/менаџер;
- Корисникот треба да се грижи за доверливоста на доделената лозинка (не смее да ја соопштува на трети лица или јавно да ја презентира);
- Пристапот до инфорамацискиот систем треба да биде базиран на реалната потреба на корисниците доволен да се заврши доделената задача, односно активност, раководејќи се од основните начела за „least privileges" и „need to know".

Користење интернет

- Користењето Интернет не смее да го наруши нормалното и ефикасно изведување на тековните операции во системот или пак да има негативен ефект на сервисите што тој ги нуди;
- При користењето Интернет се забранува:
  - симнување или публикување на содржини (текст, слика, видео, аудио) со експлицитни и/или екстремни пораки за насилство и омраза како и други дејства што се во спротивност со позитивните законски прописи и морални норми на општеството;
  - лажно преставување и криење на сопствениот идентитет;
  - симнување и дистрибуција на софтвер спротивно од авторските права и лиценцните договори;
  - користење Интернет за невластен пристап до други компјутерски системи, односно за учество во нелегални и криминални активности;
- Приклучувањето на Интернет мора да се врши секогаш преку соодветен сигурносен механизам - „firewall" (огнен ѕид);

- Споделувањето, односно оставањето приватни информации на интернет-мрежата (адреса, место на живеење, број на кредитни картички) треба да се прави крајно внимателно и само на познати и проверени web-страници.

Користење е-пошта

- Електронската пошта се обезбедува за брза и ефикасна комуникација и не смее да се злоупотребува за нелегални и криминални активности;
- Корисниците треба да ја почитуваат приватноста на другите и не смеат да се претставуваат лажно при комуникацијата со е-пошта;
- Не треба да се отвораат приложени датотетки или линкови од непознати примачи со „сомнителна" содржина;
- Електронската пошта не треба на ниеден начин негативно да придонесе за достапноста и за расположивоста на сервисите во информацискиот систем;
- Електронската пошта не смее да се користи за дистрибуција на содржини (текст,слика, видео, аудио) со експлицитни и/или екстремни пораки за насилство и омраза во спротивност со позитивните законски прописи и морални норми.

Антивирусна заштита

- Сите персонални компјутери мора да имаат инсталиран антивирусен софтвер поставен и сетиран за да овозможи автоматска заштита и проверка од таканаречените малициозни програми (вируси, spyware, Trojan horse, logic bomb, worms…..);
- Сите медиуми што се користат за чување/пренос на информации задолжително треба да се проверуваат од вируси пред нивната употреба;
- Антивирусниот софтвер на персоналните компјутери не смее да се онеспособи, на кој било начин да се избегне или да се менува неговата конфигурација, со што би се намалила неговата ефикасност и расположивост.

ИЗМАМИ СО БАНКОВНИ КАРТИЧКИ

Измамата со банковни картички е во пораст во целиот свет. Најголемата опасност во последните години доаѓа од организирани групи и е интернационална по обем. Блиски врски со дроги, криумчарење на оружје, лихварство и други насилни криминални активности не се невообичаени. Појавата на неколку интернационални криминални групи кои систематски ги напаѓаат финансиските системи преку фалсификување, измама со кредитни картички, измама преку аконтации, компјутерска измама и телекомуникациска измама е најдобар показател за сериозноста на овој проблем во светски рамки.

Дефинирање типови измама

Во индустријата на банкарските картички, измамничката активност е класифицирана и се следи на овие начини:

- Загубени/украдени картички
- Непримени работи
- Преземање сметка
- Измамнички апликации
- Фалсификување/измена на картички
- Фалсификување со копирање податоци (skimming)
- Неовластена употреба/отсуство на картичка
- Генерирање број на сметка
- Измама преку електронска трговија (e-Comerce)

На следните страници дадени се примери и се опишани техниките и технологиите што се користат за измама.

Загубени/украдени картички

Во речиси 50 отсто од сите измами со банковни картички се работи за загубени/украдени картички. Ова ги вклучува и сите неавторизирани трансакции што се појавиле на банковната картичка пријавена како загубена или украдена од страна на сопственикот.
Следните статистички податоци се базирани на примерок од 12.000 случаи на пријавени украдени или злоупотребени картички:

- 18 отсто од картичките биле украдени од паркираните возила на сопствениците, повеќето од просторот за ситни работи под шоферската табла
- 17 отсто од картичките биле украдени на работното место на сопсвениците на картичките, најчесто од палто или од чанта или од незаклучен шкаф.
- 10 отсто од картичките биле украдени од рекреативни објекти
- 10 отсто од картичките биле украдени од џебни крадци, грабнување на чанти итн. Иако овие крадци не се новина, сега тие крадат картички во метроата, аеродромите, туристичките атракции, спортските центри и на други натрупани места, во иста мера колку и готовина.

Непримени работи

Овој вид измама вклучува неавторизирани трансакции на нова или на заменета банковна картичка, која била испратена по пошта на сопственикот, но никогаш не била примена. Поштенските сандачиња во зградите се омилени места за овие крадци. Добивајќи точна информација за испраќањето на картичката, крадецот ќе знае кога новата или заменетата картичка ќе биде испорачана и ќе ги следи патеките на поштарот. Како мерка на претпазливост, издавачите можат да ги известат примачите на картички со претходна најава. Многу издавачи бараат од идните сопственици да го потврдат приемот на картичка. За оваа цел, понекогаш се користи системот на „двојно датирање". Со овој систем, оперативната дата на картичката почнува приближно по 30 дена од официјалната дата на испорака. На овој начин, ако апликантот не ја прими картичката навреме, издавачот има доволно време да преземе мерки. Друг метод за избегнување на овој вид измама е активирањето на картичката. Овде, картичката се испраќа во „блокиран" статус. По примањето на картичката, сопственикот мора да го извести издавачот пред да може да ја употреби картичката.

Преземање сметка

Овој вид измама спаѓа во еден поширок вид на криминал познат како кражба на идентитет - еден од најбрзо растечките проблеми во САД денес.
При ваков вид измама, друга личност незаконски добила легална, постоечка сметка и притоа може да напра-

ви и незаконска промена на адресата.
Во типичен случај на ваква измама, престапникот доаѓа до информации за сметката на сопственикот преку крадење на месечниот извештај од поштенското сандаче или на некој друг незаконски начин. Претставувајќи се како сопственик на картичката, престапникот контактира со издавачот да побара промена на адресата и дополнителна картичка на друго име. Во тоа време или подоцна, престапникот, исто така, може да побара ПИН (личен број за идентификација) за извлекување на готовина од банковни автомати.

Лажни апликации

Друг вообичаен пример на кражба на идентитет е лажна апликација. Терминот „кражба на идентитет" се однесува на случаи во кои една индивидуа добива банковна картичка откако намерно ќе употреби лажни лични информации во апликација, со цел да го измами издавачот. Кога ќе поднесат лажна апликација, престапниците често користат делови од валидна информација. Вообичаен начин на незаконско обезбедување картичка е со давање вистинско име и лажна адреса. Подземјето повеќе ги вреднува картичките обезбедени на овој начин зашто, за разлика од украдените картички, ваквите картички не се потпишани (и нема да се појават во досието за исклучоци).
Во една добро организирана операција, обично од страна на банди, се инсталираат повеќе телефонски линии со различни броеви во еден апартман. Бандата потоа аплицира за картички, употребувајќи еден или повеќе од телефонските броеви како тефонски број на работа на лажниот апликант. Член на бандата е секогаш присутен во апартманот за да потврди дека тоа е работно место на апликантот.

Фалсификувани/изменети картички

Фалсификувана картичка е незаконски произведена и присвоена картичка, понекогаш со кодирана магнетска лента, која и електронски е прифатлива. Фалсификуваните картички порано се правеле со офсет или силкскрин-метод на печатење. Денес, многу фалсификатори користат компјутерско печатење за изработка на фалсификувани картички. Меѓутоа, репродукцијата на холограмски слики на пластика е крајно сложен и скап процес за фалсификаторите. Холограмската безбедност значително го намали фалсификувањето на картичките, кои се голема грижа на издавачите поради многу поголемата парична загуба.

Изменета картичка е оригинална картичка изработена од сертифициран печатач со една или повеќе променети карактеристики, по пат на механички или електронски средства. Изменетата картичка обично е модифицирана со наново изработен врежан број на сметка. Кога пластичната картичка ќе се загрее, врежаниот (изгравираниот) број на сметка може да се израмни и нов број да се вреже на негово место. Бројот, исто така, може да се отстрани со клуч за израмнување на портабл-машина за врежување. Броевите и буквите дури можат да се исечат од една картичка со машинка за перфорирање и да се заменат со броеви и букви од друга картичка.

Фалсификување со копирање податоци од магнетната лента на картичката (skimming)

Со употреба на разни нови техники, криминалците можат да ги ископираат податоците на сопственикот на картичката, кои се содржани на магнетската лента на кредитната, дебитната или АТМ картичка и потоа да ги употребат или за кодирање (шифрирање) на фалсификувана картичка или за рекодирање на загубена/украдена картичка. (Секоја картичка што има магнетска лента може да биде рекодирана со нова информација добиена со копирање, односно **скиминг**. Индустријата за банковни картички овој тип измама сега го нарекува „скимд" фалсификат.
Најчести случаи на скиминг (skimming) се случуваат на:

Во малопродажба - често се нарекуваат повторно лизгање на картичката. Ова сценарио вклучува нечесни работници (или самите сопственици на бизниси), кои употребуваат лесно набавливи направи, наречени „клинови" за снимање на податоците при лизгањето на легитимната картичка. Ваквите „читачи" можат да меморираат и до 200 легитимни броеви на сметки.

При трансфер на податоци од една организација во друга – Во неколку пригоди крадците поставиле телефонски пресретнувачи (taps) за да ги фатат податоците од магнетската лента при нивен трансфер од терминалот на трговецот при авторизирање или при симнување податоци.

Ожичување или насамарување - Можно е да се ожичи или да се стави лента во фискалните апарати и на таков начин да се снимат податоците од магнетската лента додека картичката се лизга на апаратот.

Кога се складирани - Сé повеќе малите бизниси, особено е-бизнисите, воспоставуваат бази на податоци за сметките и за личните податоци на муштериите. Хакерите можат да дојдат до овие бази на податоци, бидејќи информациите за трговците се достапни преку интернет. Хакерите типично пенетрираат една база за податоци и се обидуваат да изнудат податоци од трговецот или едноставно да ги изложат банковните податоци на разни огласни табли за да може секој да ги злоупотреби.

Преку внатрешно загрозување - Бидејќи сé повеќе трговци ги процесираат податоците од магнетната лента, веднаш по продажбата контролата на информациите за сопствениците на картички станува сé покритична. Привремено вработените, договорни изведувачи и продавачи што работат на една продажна локација имаат пристап до податоците за сметките, а со тоа и потенцијал за нивно загрозување. Откако некој криминалец ќе ги ископира податоците за нечија сметка, рекодирањето или фалсификувањето е прилично едноставно. Исто така, опремата потребна да се направи ова е лесно достапна. Лаптоп-компјутерот е многу популарен кај фалсификаторите и кодирачките/рекодирачките софтверски програми се, исто така, достапни. Вистинскиот сопственик на картичката обично не знае дека неговиот број на сметка бил ископиран (украден), сé додека лажна трансакција не се појави на месечниот банковен извештај.

Неовластена употреба/картичката не е присутна

Овој вид измама се случува кога некоја личност ќе употреби туѓ број на сметка за купување преку телефон, пошта или интернет. Картичката и бројот се валидни, но употребата не е. Ова е популарна измама за набавување скапа стока лесна за препродажба, како на (пр. компјутери, електроника, накит итн.) преку пошта или стандардна испорака.

Генерирање број на сметка

Денес е можно да се генерира валиден број на сметка, користејќи различен софтвер достапен на интернет. Овде се мисли на програми, како на пр. CreditMaster, CreditWizard, The Credit and Credit Probe.

Откако еднаш броевите на сметка се генерирани, тие потоа се користат за измами при разни трансакции, како на пр. порачки по пошта/телефон и интернет-трансакции. Броевите на сметките, исто така, може да се користат за правење фалсификувани и изменети картички. Сите броеви на кредитни картички имаат „цифра за проверка". Таа цифра се додава на бројот на сметката за да се провери автентичноста на бројот. Еден едноставен алгоритам, наречен Luhn Modulus 10 Formula (MOD10) се применува на другите цифри од бројот и тој ја дава цифрата за проверка. Со споредба на цифрата за проверка што се добива од алгоритамот со цифрата за проверка кодирана со бројот на сметка, вие можете да потврдите дека имате валиден број на сметка. Овој процес го користат Visa, MasterCard, Discover and American Express.
Иако еден генериран број на сметка може да биде математички валиден, тој може да не постои во портфолиото на издавачот. Софтверските програми не можат да генерираат датуми на престанок на важност, вредност на верификација на картичките (CVV) или имиња на сопственици на картички. Пред да се направат сериозни обиди за измама, броевите на сметката обично се тестирани при трансакции со мали износи. Ако тие се успешни, ќе следи дополнителна измама.

Е-Трговија

Овој вид измама се однесува на која било измамничка активност поврзана со интернет. Досега, ова било ограничено на:
- генерирање на број на сметка,
- телемаркетиншки шеми и
- хакерска пенетрација на трговски бази на податоци.

Телемаркетиншките шеми што се користат за измама се исти со години, како на пр., се нуди заштита на кредитни картички, разни патувачки аранжмани, понуди за плаќање со кредитни картички итн. Хакерите пенетрираат во една база на податоци и се обидуваат да изнудат податоци од трговците или едноставно да ги истакнат банковните информации на различни огласни табли, со цел секој да може да ги злоупотреби.

Надувување на сметката на сопственикот на картичката

„Измама со надувување" се однесува на случаи кога сметката се надувува со лажни плаќања и потоа надуениот баланс се користи или се повлекува. Организирани шеми на надувување на сметки од големи размери се појавиле во доцните 1980-ти години и продолжуваат да бидат сериозен проблем.
Има два вида сценарија за надувување на сметка:

Надувување на сметка на легитимен сопственик на картичка - Во оваа ситуација, оригиналната сметка може и да не била отворена со цел за измама. Подоцна, се променуваат условите на сопственикот и тој ја надувува вредноста на својата сметка со безвредни чекови. Потоа тој ја троши или ја повлекува оваа вредност од сметката, а во некои случаи може да поднесе и извештај за банкрот.

Лажно надувување на сметки – Во ваков случај префинети криминалци отвораат сметки, со цел да измамат финансиска институција, која вклучува шема на надувување.

Загуби причинети од надувување на сметките на легитимни сопственици на картички
Просечната загуба за индустријата за банковни картички по човек била околу 120.000 долари поделена на неколку издавачи.

Лажно надувување сметки

Отворањето на сметки заради измами од страна на организирани криминални групи е ризична област која е во пораст. Во некои случаи, овие групи биле во можност да ги прикријат лажните идентитети со тоа што имале оригинални матични броеви. Ваквиот вид организиран криминал во САД започнал околу 1989 год.
Едно типично сценарио за измамничка сметка би изгледало вака:
Осомниченият отвора кредитни сметки, кои често почнуваат со мали инстантКредит-сметки, а потоа апликираат за кредитни картички. Сметката созрева за 18 до 36 месеци, додека други сметки се отвораат. Во текот на овој период, сметката има некоја употреба и е навремено платена. Исто така, има барања за зголемување на кредитот и промена на адресата. Други имиња често се додадени или отстранети од сметката. Ако осомниченият смета дека ги добил сите можни кредитни покачувања, тој почнува процес на надувување. Тој прави големи плаќања, често преку кредитниот лимит со безвредни платежни средства, големи готовински аванси, квази-готовина и купува скапа стока. Плаќањето продолжува сé додека банката не ја блокира сметката. Осомниченият престанува да го користи лажниот идентитет и се префрлува на друг. Загубите од овој тип измама за индустријата на банковните картички се многу повеќе од 100.000 долари по ентитет.

Истражувачки согледувања на лажни надувувања на сметки

Во многу случаи, еден осомничен има многу идентитети и секое од тие имиња има многу сметки. За вакви случаи следните чекори се корисни:
Да се бараат поврзани сметки што го користат истото име, адреса и матичен број (број за социјално осигурување).
Да се откријат побарувачки депозитни сметки, кои се користат за лажни плаќања.
Да се откријат други сметки кои биле платени преку осомничената депозитна сметка, што, всушност, е клучен фактор во поврзувањето на наизглед неповрзани случаи.
Да се бараат слични/исти локации за готовински аванси и купувања од сите осомничени сметки. Ова може да доведе до тајно вклучен трговец, банкарски службеник и сл.

Трговски измамнички шеми

Овде се дадени некои типични видови измами на трговски локации.

Трговски заговор

Трговскиот заговор се случува кога нечесни трговци се во дослух еден со друг, со некој муштерија или крадец на картички, со цел да измамат финансиска институција. Со оваа шема тешко може да се бори, а може да предизвика големи загуби. Еве некои примери:

Двајца трговци соработуваат при размена на загубени или украдени картички за да направат фиктивни трансакции. Трговецот снима трансакција со муштерија (или друг трговец како наводен муштерија), го задржува производот, но бара наплата од финансиската институција за тоа. Трговецот потоа ја дели наплатената сума со тој што е во дослух, односно со наводниот муштерија.
Трговецот наизглед рутински бара овластување за купување скапи работи, користејќи украден, фалсификуван или компјутерски генериран број на сметка.

Повикот до овластувачкиот центар на издавачот ќе потврди дека бројот постои и може да се употреби за измама. Ако картичката не е пријавена како украдена, нечесниот трговец може да процесира високо вредна трансакција (да купи нешто скапо) преку неговиот бизнис. Ако, пак, картичката е пријавена како укредена, трговецот може да ја распредели сумата од трансакцијата (купувањето) на неколку фактури, со тоа што сумите ќе бидат под неговиот продажен лимит. Оваа измама често ги вклучува и вработените на трговецот.

Перење пари

Овој тип измама се случува кога некој легитимно потпишан трговец депонира сметкопотврди за продажни трансакции во името на операторот, кој нема склучено трговски договор со финансиска институција. Обично, таквите оператори не можат да добијат трговски договор и затоа им приоѓаат на легитимно потпишаните трговци за да ги исперат сметкопотврдите за продажни трансакции за нив. Понекогаш, тие вработуваат брокер за да им пристапат на легитимните трговци. Во замена за депонирање на сметкопотврдите, на легитимниот трговец му се дава процент (во опсег од 1-20 отсто)од тоталната вредност на сметкопотврдите. Во многу случаи, лажниот оператор ги пере парите со легитимен трговец неколку недели пред да отиде кај друг трговец, обично пред повратните сметки (chargebacks) да почнат да се натрупуваат.

Измама со бела пластика

Бела пластика е генерички термин, кој се однесува на парче пластика во која било боја со големина на банковна картичка, која е кодирана со број на сметка, дата на престанок на важност и име на сопственикот. Оваа картичка е слична со банковната картичка само со големината и со кодираните податоци. Овие картички се прифатени кога има заговор меѓу трговецот и измамникот. Пластичната картичка се користи за да се отпечатат (врежат) потврдите за продажни трансакции, кои се депонирани на сметката на трговецот. Овој тип измама, исто така, може да вклучува и лажни јавни операции. Измамниците, претставувајќи се како трговци, набавуваат Visa/MasterCard привилегии за нивните фиктивни бизниси и финансиската институција ги снабдува со кодер и бланко- сметкопотврди. Дузини сметкопотврди се отпечатени (врежани) со лажни картички. Измамниците подоцна ги депонираат сметкопотврдите за големи суми, ги собираат парите и се губат. Картичките употребени за ваков вид измама не се вистински фалсификат на оригиналните картички, туку бела пластика со врежани (изгравирани) податоци добиени од оригинални картички.

Кој е жртва на измама со кредитни картички?

Надвор од банкарските кругови често има забуна за тоа кој е жртва (жалител) во случај на злоупотреба на кредитна картичка.

Одговорност на издавачот

Во повеке од 70 отсто на случаи на измама со банкарски картички, жртва е банката- издавач. Со други зборови, обично издавачот на крај ја носи финансиската одговорност за износи, кои сопственикот на картичката тврди дека не ги потрошил.

Нулта одговорност на сопственикот на картичката

Политиката на Visa нулта одговорност им овозможува на сопствениците на Visa-картичките максимална заштита од измама. Со оваа политика, од издавачите се бара да ја ограничат одговорноста на сопствениците на картичките на 0 долари за сите неовластени трансакции. Издавачот може да го зголеми лимитот на одговорност на сопственикот само ако институцијата одреди (врз основа на значителен доказ) дека сопственикот на картичката бил крајно невнимателен при ракувањето со својата сметка или картичка.

Одговорност на трговците

Трговците главно не се одговорни за измамничка трансакција ако за време на трансакцијата тие:
- примат овластување;
- генерираат сметкопотврда за трансакцијата со ознака (импринт) на картичката (рачна или електронска) и обезбедат потпис на сопственикот или перосонален број за идентификација (ПИН).

Ако трговецот не ги изведе овие барани чекори, неговата фирма подлежи на наплата (chargeback). Ова е формален процес што му овозможува на издавачот да ја наплати сумата од продажбата од крајниот корисник на средствата, затоа што трговецот не постапил во согласност со барањата. Ако крајниот корисник на средствата одлучи дека побарувањето е валидно, тогаш крајниот корисник ќе ги одземе овие средства од сметката на трговецот.

Прашања за трговците кога картичката не е пред нив

За трговците што процесираат не лице-в-лице трансакции, како што се порачки по пошта или телефон и интернет-трансакции, постои поголема шанса за измама и финансиска одговорност зашто во таков случај нема импринт (отпечаток) од картичката, ниту потпис на сопственикот на картичката. Кога нарачките се примаат по ваков пат тие се поподложни на измама и затоа трговците треба да останат претпазливи при вакви ризични практики и да употребуваат средства за детекција на измама.

Заклучок

Преку горенаведените примери на можни начини на измами поврзани со банковни картички, целта е сите субјекти што се поврзани со работењето со овие картички да се запознаат со можните потенцијални опасности и последици кои се базираат на досегашните искуства.
Криминалните дејствија на несовесни поединци или групи, кои преку овие злоупотреби сакаат да стекнат противправна материјална корист, секако ќе продолжат и во иднина и должност на сите субјекти во овој процес е да преземат сé за да се минимизираат штетните последици од овие криминални активности.

ШТО Е ФИШИНГ (PHISHING) И ФАРМИНГ (PHARMING)?

Фишинг е термин што се користи кога се работи за присвојување на идентитетот на легитимната организација или веб-сајт, употребувајќи фалсификувана е-пошта, односно имејл (e-mail) и/или веб-страници (web pages) и со цел да се убедат корисниците да ги споделат своите кориснички имиња (user names), лозинки (passwords) и личните податоци (име, броеви на кредитни картички, матични броеви или броеви за социјално осигурување), со цел тие да бидат злоупотребени. Ова, исто така, се вика и кражба на идентитет. Фишинг е релативно нов термин, употребен во некои извештаи уште во 1996 година, а во медиумите е спомнат во 1997 година.

При фишинг-нападите се користи **социјален инженеринг** и **технички трикови** за да се украдат личните и финансиските податоците на корисникот. При тоа најчесто се користи е-пошта за да се наведат мушториите да посетат лажни веб-сајтови кои го имитираат изгледот на легитимни брендови, како банки и компании за е-малопродажба или кредитни картички. Сличен е резултатот и кога се вршат измами преку системи за директен разговор (chat).

Шемите на техничките трикови значат вметнување криминален програм (crimeware) во компјутерот на жртвата за да се украдат податоците директно, често користејќи шпијунски програми, т.н. тројански коњи, со кои се следи она што корисникот го пишува на тастатура (spyware, trojan horse, keylogger). Фарминг криминалните програми погрешно ги наведуваат интернет-корисниците на лажни сајтови или прокси-сервери, типично преку т.н. киднапирање на ДНС.

Меѓу сајтовите што биле погодени од вакви измами или скемови (scams) се и Yahoo, Microsoft, AOL, eBay, Paypal, Hotmail, Earthlink, Barclays iBank, Citibank, Halifax, Nat West Bank – Nationwide, MSN, FDIC (Federal Deposit Insurance Corporation), Lloyds TSB, АТѝТ, Fleet Homelink и US Bank.

Некои од овие веб-сајтови ги нарекуваат овие фалсификати измамнички или спуф-имејл (spoof e-mail), кој е попрактичен "кориснички" термин. Измамниците овие спуф-имејлови ги дистрибуираат како спам (spam), преку праќање пораки до масовни листи, без разлика на тоа дали примателите се корисници на одреден сајт легитимен сајт чиј идентитет се злоупотребува или не.

Поголемиот дел од фишинг-скемовите се состои од фалсификуван имејл, кој е поврзан со фалсификувана веб-страница или сајт. Текстот на имејлот ве наведува да пополните основна процедура со користење линк, кој отвора лажна веб-страница. Таа основна процедура, покрај другите работи, вклучува потврдување на бројот на вашата сметка, информации за невалидни кредитни/дебитни картички, обид за киднапирање на вашата сметка, награди, суспендирање на вашата сметка итн. Во многу случаи имејлот го вклучувал и вирусот црв, како на пр. Mimail worm.

Измамниците често користат и дупки кај програмите за пристап на интернет, како "бубачката" во разгледувачот Интернет експлорер која додека Мајкрософт не ја запре во февруари 2003 година овозможи огромен број измами преку прикажување лажна адреса на тековната страница.

Фалсификуваните, односно лажните веб-страници обично содржат формулар што треба да им ги обезбеди потребните информации на скемерите, за тие да направат измама. Ова обично значи злоупотреба на кредитните/дебитните картички на жртвите за отворање онлајн-сметки и киднапирање онлајн-сметки, со цел да украдат пари. На пр., на корисниците на eBay им беа украдени сметките на овој начин додека скемерите ги користат сметките за понуда на скапи работи, добиваат и наплатуваат порачки од купувачи, но стоката никогаш не ја испорачуваат. На други жртви им бил уништен кредитниот и финансискиот статус (credit score) кога нивниот идентитет бил употребен за собирање финансии, а некои жртви, пак, виделе дека некој ги искористил нивните кредитни или дебитни картички за онлајн-купување стоки.

Заштитете се од станување жртва на фишинг скем со следење на овие едноставни правила:

- На секој имејл гледајте со сомневање - Она што го гледате во текстот на имејлот може да биде фалсификат, адресата на испраќачот или повратната адреса може да бидат лажни и насловот на имејлот може да биде изманипулиран за да го прикрие својот вистински идентитет.
- Никогаш не кликнувајте на линк во имејл за да посетите веб-страница. Ако веќе морате да одите таму, внесете ја адресата во адресната лента на разгледувачот (прелистувачот).
- Никогаш не праќајте ваши лични или финансиски информации по е-пошта.
- Секогаш кога ги користите вашите сметки на интернет, проверувајте ги вашите сметки за пократко од еден месец.
- Внимателно прегледајте ги вашите месечни банковни извештаи и проверете дали сите трансакции се легитимни. Ако некоја трансакција е сомнителна или вие не сте ја направиле, контактирајте веднаш со вашата банка или со издавачот на картичката.
- Осигурете се дека вашиот софтвер е надграден (up-to-date) - на пр. ако користите оперативен систем Мајкрософт виндоуз, вклучувајте го Windows update секој ден кога за првпат ќе се приклучите на интернет. Ако користите други оперативни системи или пребарувачи, тогаш секојдневно проверувајте дали има надградби (updates).
- Ако веќе морате да ги искористите вашите финансиски информации преку интернет, уверете се дека имате осигурување од измама.

Кражба на идентитетот преку интернет

Кражбата почнува со подметнат, фалсификуван имејл (hoax email), кој упатува подметната веб-страница. Ваквите пораки лажно го покажуваат испраќачот како легитимна адреса за е-пошта (како на пр. service@paypal.com во еден од примерите подолу). Во имејлот или ќе бидете прашани за вашите информации таму и тогаш или, пак, имејлот ќе ве упати на преправен, "пресоблечен" линк што изгледа дека води на легитимна адреса, а всушност насочува кон фалсификувана веб-страница или сајт каде што тие ќе се обидат да го украдат вашиот идентитет.

Ќе ја погледнеме скеминг-техниката, позната под името „фишинг" (phishing), кој станува растечки проблем на интернет. Само во 2004 година имало покачување од 40 отсто во бројот на забележани напади и ситуацијата е со тенденција на влошување. Терминот „фишинг" доаѓа од англискиот збор што значи риболов, зашто означува сличен пристап. Измамниците или скемерите (риболовците) испраќаат големи количества имејлови („јадици") на повеќе случајни адреси на интернет. Овие имејлови се чини дека доаѓаат од најразлични банки, финансиски институции и сајтови, како eBay, AOL и PayPal, кои од жртвите бараат да ги внесат нивните информации за сметки и кредитни картички, поради најразлични причини, од наводни „проблеми" со компјутерските системи, кои ги губат деталите за сметките од причини, како што е проверка дали последната „трансакција" била неавторизирана итн.

Иако само мал дел од луѓето (околу 5 отсто) одговараат на вакви пораки, тоа за скемерите е сé уште голем процент на одговор со минимален ризик. Во моментот не е незаконски да се праќаат фишинг е-меилс; криминал се случува само кога скемрите ќе дој-

дат до потребните информации.
Нема 100 отсто одбрана од фишинг-шемите, освен да се биде свесен за опасностите и буден во случај да станете нечија цел.
Фишинг имејловите се појавуваат во најразлични облици и големини. Некои изгледаат екстремно професионални и реални, додека други, пак, се непреработени и лошо составени. Некогаш тоа се прави смислено за да се остави погрешен впечаток на потенцијалната жртва дека има работа со некој недоволно образован за ваква измама, а другпат тоа е одраз на лошото познавање на англискиот јазик на креаторите на скемот. Најчеста техника е да и се каже на жртвата дека имало некаков проблем со нејзината сметка и дека таа мора да биде потврдена за да не се затвори или суспендира. Примачот (жртвата) потоа се наведува или да ги внесе своите податоци во формулар во имејлот или да кликне на некој линк до „официјалната страна" на наводниот испраќач на имејлот. Тој линк, всушност, води до измамничка, спуф-страница (**spoof page**) креирана да изгледа исто како оригиналната страна што ја имитира, па на прв поглед не можете да ја забележите разликата. Некои од пософистицираните спуфови дури го фалсификуваат и УРЛ во полето за адреса, па на тој начин и адресата на сајтот изгледа автентична. Еве еден пример на понов, типичен спуф-имејл:

Изгледа доволно реалистичен, но не е. Независно од тоа кој пристап бил употребен, откако вие ќе ги вметнете и поднесете своите податоци, тие се препратени директно на скемерот, кој може да ја злоупотреби вашата сметка.

За да избегнете да станете жртва на фишинг, следете ги следниве основни правила:

• Никогаш не верувајте му на испраќачот на имејл
Дали знаете дека е можно да се фалсификува повратната адреса во имејлот? За оние што се помалку компјутерски образовани, тоа е оној дел од имејлот што ви кажува од кого е имејлот. Испраќачот може да избере име и адреса какви што сака, затоа не верувајте му на имејлот само затоа што изгледа дека е од легитимна адреса. Добро е познат фактот дека преку 95 отсто од фишинг-нападите користат фалсификувани, спуф имејл-адреси за да изгледаат поавтентични.

• Секогаш проверувајте ја содржината
Додека повеќето професионални спуфови можат да бидат речиси исти со оригиналните, останатите лесно се забележуваат. Вообичаената техника што ја користат скемерите е целиот текст во имејлот да го направат како слика, која кога ќе се кликне, преку линк, води до спуф веб-страница. Ова тактика се употребува за да се избегнат скенерите на имејловите, кои можат да го скенираат текстот, но не и сликите. Ако не можете да кликнете и да го селектирате текстот како што правите нормално со глушецот, едноставно тоа е скем (**scam**). Автентичните имејлови никогаш не се составени на овој начин. Лошиот правопис и граматика се најточни откривачи на скемови, зашто покажуваат грешки во самото име на испраќачот, на пр. '**Alert from Citibank**'. Банките и сличните институции не испраќаат имејлови со такви лоши грешки.

• Не отворајте ги прикачените писма (**attachments**)
Понекогаш еден спуф-имејл доаѓа со **attachment** привезок, односно прикачено писмо. Не отворајте го! Може да е безопасно, но нема потреба да ризикувате. Ова е највообичаениот начин за ширење на вирусите и освен што може да се работи за скем-имејл може да се обиде и да успее да го инфицира вашиот компјутер со програми што крадат информации од вас без ваше знаење.

• Направете ажурирање на сигурноста на вашиот компјутер
Еден незаштитен компјутер на интернет е како куќа без брави - екстремно чувствителен. За да го направите посигурен и обезбеден може да ги преземете овие 3 чекори:

Набавете антивирус-програма (и постојано правете update). Антивирусните програми треба да бидат постојано во вашиот компјутер и да го скенираат секој фајл во случај да е инфициран и потоа тие можат да го отстранат од вашиот систем. Основно е да правите постојано ажурирање на антивирусната програма, оти нови вируси се појавуваат секојдневно. Повеќето антивирусни програми работат автоматски.

Набавете програма за отстранување шпијунски програми и ажурирајте ја постојано. Овие програми се основен придружник на антивирус-програмите, затоа што можат да најдат програми кои антивирусот не може да ги најде. Некои програми познати како '**spyware**' не се класифицирани како вируси, но сé уште се потенцијално штетни, зашто можат да останат на вашиот компјутер и да собираат информации без ваше знаење или согласност. Некои дури можат да го снимат секој знак што ќе го внесете преку тастатура и на тој начин да дојдат до информации за вашата кредитна картичка и лозинка.

Ажурирајте го вашиот оперативен систем. За разлика од корисниците на Линукс, корисниците на Виндоуз се соочуваат со далеку почести закани поради безбедносни дупки кои напаѓачите можат да ги искористат да неовластен влез и крадење информации. Мајкрософт постојано ги поправа сите дефекти што ќе ги најде, поставувајќо ги најновите ажурирања на сајтот **http://windowsupdate.microsoft.com.**

• Никогаш не откривајте ги вашите лични податоци
Ова е наједноставното правило од сите. Банките, финансиските институции и сл. никогаш нема да ви пратат имејл, во кој ќе ви бараат директно да ја потврдите вашата сметка, ниту да направите ажурирање на вашите податоци преку имејл. Тоа едноставно не се случува. Во такви ретки случаи кога се појавуваат проблеми тие директно ќе ви се јават по телефон, писмо или на друг начин. Дури и ако имејлот изгледа автентичен, повеќе од веројатно е дека не е. На пр. дали знаевте дека еден линк може да покаже една адреса, но всушност да оди на сосема друга. Вие може да кликнете на линкот со име **www.paypal.com**, но, всушност, да стигнете на **www.steallyourmoney.com**. Посетувајте ги веб- сајтовите директно.

СТРАТЕШКИ НАСОКИ

Пред сé, потребно е јасно и недвосмислено да се потврди заложбата на сите чинители во процесот: државни органи, компании, банки, финансиски институции, граѓански и невладини организации, за имплементација на сигурен информациски систем реализиран преку воспоставување стандарди, правила, препораки, но и конкретни законски решенија што ќе ја регулираат оваа област. Оваа заложба потоа треба да се реализира преку конкретни активности и проекти, на неколку нивоа:

- Унапредување на законската рамка со која се уредуваат постапките, мерките и контролата при воспоставување сигурен информациски систем на сите нивоа;
- Хармонизација на практиките на национално ниво со најдобрите практики на ЕУ и на НАТО во поглед на безбедноста на информациите;
- Прифаќање на ISO 17799, односно ISO 27001 како национален стандард за сигурност на информациските системи;
- Изработка на национални и локални политики и стратегии за информациска сигурност;
- Спроведување на сигурносни контроли преку конкретни решенија произлезени од законските норми, односно националната програма;
- Формирање и промоција на национален CERT – Computer Emergency Response Team;
- Континуирана едукација и подигање на свеста и знаењето на корисниците на сите нивоа во поглед на информативната сигурност.

Стратегискиот пристап потоа ќе обезбеди да произлезат низа нови закони или дополнување на веќе постоечките акти и правилници, сé во интерес на имплементацијата на сигурни информативни системи како основен предуслов за развој на е-услугите и сервисите, односно фаќање приклучок кон современиот свет, односно европската интеграција.
Националната стратегија за развој на информатичкото општество во Република Македонија, во состав на својот акциски план ги содржи следниве проекти:

- ПР3.27 ISO 17799
- ПР3.38 Национална политика за ИКТ-безбедност
- П3.39 Безбедносна сертификација
- П3.40 Национално тело за ИКТ-безбедност
- ПГ6.02 е-Сигурност

Воедно, националната стратегија за електронски комуникации, која моментно се наоѓа во собраниска процедура, има посебно поглавје за безбедност на информациите.

Безбедноста на информациите е комплексно мултидисциплинарно подрачје, кое не може системски да биде уредено со еден закон. Во Република Македонија, на овој план претстои системска разработка на законодавството, која ќе започне со идентификација на сите закони што уредуваат прашања на прибавување, користење и чување информации, нивна внатрешна хармонизација и хармонизација со законодавството на ЕУ и стандардите на НАТО, како и развој на реални планови и мерки за соодветна имплементација на законодавството. Ова законодавство треба да биде само еден дел од целокупната национална стратегија за информациска сигурност, која со учество на сите заинтересирани страни треба да биде донесена во Република Македонија.

Развојот на стандардите и мерките за информациска сигурност го условува и користењето на информатичката технологија и развојот на информациската инфраструктура во државата. Со овие стандарди и мерки треба да се изедначи начинот на постапување со информациите, со оглед на нивната специфика, кај различните органи и лица што прибавуваат, користат или управуваат со информации.

Зајакнувањето на сигурноста во овој момент на развој и барање директни странски инвестиции е особено важна во бизнис-секторот, па оттука контролатата на прибавување, чување и управувањето со информациите се јавува како иманентна потреба.
Детална анализа на законодавството и неговата хоризонтална и вертикална хармонизација е еден од чекорите што треба да бидат преземени за обезбедување безбедност на информациите.

Корисни веб-сајтови

www.enisa.europa.eu
ЕНИСА - Европска агенција за мрежна и информатичка сигурност

security.practitioner.com
Референтна точка за безбедност на информациите, од аспект на ISO 27001

www.pravo.org.mk
База на закони од Република Македонија достапна преку интернет

windowsupdate.microsoft.com
Ажурирања на оперативниот систем Мајкрософт Виндоуз

www.linuxsecurity.com
Портал за безбедносни прашања во врска со оперативниот систем Линукс

www.edri.org
ЕДРИ - европска асоцијација на НВО за дигитални права.

www.oecd.org/sti/security-privacy
Оддел за информациска безбедност и приватност при ОЕЦД

Автори на текстот: Сашо Мицков, Љубомир Трајковски, Неда Здравева, Марјан Ристески, Јован Петров и Јорданка Петрушевска.

Лектура: Маја Катарова

Графичка обработка: Бојана Димитрова

Текстовите во овој водич се генерирани во рамките на проектот Иницијатива за информациска сигурност, со поддршка од Фондацијата Институт отворено општество - Македонија (www.soros.org.mk) и на мрежната програма за информации на Институтот отворено општество (www.soros.org).

МЕТАМОРФОЗИС

Метаморфозис е независна, непартиска и непрофитна фондација со седиште во Скопје, Република Македонија. Нејзини главни цели се развој на демократија и просперитет преку промоција на економија базирана на знаење и информатичко општество.

Адреса за контакт: Фондација Метаморфозис
ул. „Наум Наумовски - Борче" 88-а
1000 Скопје, Македонија
телефон: +389 2 3109 325
факс: +389 2 3225 206
е-пошта: info@metamorphosis.org.mk
веб-сајт: www.metamorphosis.org.mk