БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Игор Кузевски

Содржина

* ПОИМНИК
* ПРИМЕНА
* СИСТЕМ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ
* МЕРКИ ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

ПОИМНИК

* **Информацискатa сигурност** е состојба на благостојба на информациите и инфраструктурата на која се обработуваат информациите.

Зошто и дали ни е потреба информациска сигурност?

* 90% од целокупната e-mail комуникација е СПАМ
* Креирање на лажни веб-страни, лажни електронски адреси, лажни продавачи на електронски услуги
* Верижни (hoax) комуникации

ПОТЕНЦИЈАЛНИ ЗАГУБИ ПРИ БЕЗБЕДНОСНИ НАПАДИ

* Финансиски
* Недостапни ресурси
* Кражба на идентитет
* Губење на доверба
* Кражба на податоци
* Злоупотреба на компјутерските ресурси

ЗАКАНИ
ЗА ИНФОРМАЦИСКАТА СИГУРНОСТ

* Virus
* Warm
* Backdoor
* Rootkit
* Trojan
* Logic Bomb
* Spyware
* Keylogger
* Password cracking

ПОИМНИК
ЕЛЕМЕНТИ НА СИГУРНОСТ (нов концепт)

* ДОВЕРЛИВОСТ (confidentiality)
* ИНТЕГРИТЕТ (integrity)
* ДОСТАПНОСТ (availability)
* АВТЕНТИКАЦИЈА (authenticity)
* НЕОТПОВИКЛИВОСТ (Non-repudiation)

ФУНДАМЕНТАЛНИ КОНЦЕПТИ

* **ПРЕВЕНЦИЈА**: претходни активности кои се преземаат (анти вирус, заштитен ѕид (firewall), силни лозинки, подигнување на свеста на вработените - careful when downloading files)

* **ОДРЖУВАЊЕ:** активности кои се преземаат како поддршка и надградба на превенцијата (сигурносни копии - backup, управување со злонамерните закани - malware management, слободен простор за надградба и ажурирање (update) за анти вирусот, заштитниот ѕид)

* **РЕАКЦИЈА:** брзина на реакцијата во случај на инцидент

ПОИМНИК

* **Управување со ризик** - идентификација, оценка и негова класификација, која опфаќа координирана примена на ресурси на контролорот за минимизирање, набљудување и контрола на веројатноста и сериозноста која што може да произлезе при обработката на личните податоци, а која може да предизвика материјална или нематеријална штета врз процесите со кои се врши обработка на личните податоци
* **Систем за заштита на личните податоци** - збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци

ПОИМНИК

* Авторизиран пристап
* Администратор на информацискиот систем
* Документ
* Информатичка инфраструктура
* Информациски систем
* Инцидент
* Контрола на пристап
* Овластено лице
* Лозинка
* Колаче (cookie)
* Работна станица
* Медиум
* Сигурносна копија

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Систем за заштита на личните податоци

* псевдонимизација и криптирање на личните податоци;
* способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на информацискиот систем за обработка;
* способност за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент; и
* процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката.

A STATE OF THE ART TECHNOLOGY

ЗА ПСЕВДОНИМИЗАЦИЈАТА

* **„Псевдонимизација“** - обработка на личните податоци на таков начин што личните податоци не можат повеќе да се поврзат со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува

A STATE OF THE ART TECHNOLOGY

УПРАВУВАЊЕ СО РИЗИК

При утврдувањето и проценатa на ризикот се земаат предвид ризиците кои се поврзани со обработката на личните податоци

Управувањето со ризикот ги опфаќа следните фази:

* список (преглед) на сите процеси со кои се врши обработка на лични податоци;
* процена на ризиците за секој процес на обработка на лични податоци;
* спроведување и проверка на планираните мерки; и
* спроведување на периодични безбедносни проверки.

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

НИВОА НА МЕРКИ

Земајќи ги предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, контролорот е должен да примени соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личните податоци.

Техничките и организациските мерки се класифицирани во две нивоа:

- **СТАНДАРДНО**
- **ВИСОКО**.

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

СТАНДАРДНО НИВО

ПОЛИТИКА ЗА СИСТЕМОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Врз основа на Политиката за системот за заштита на личните податоци, контролорот донесува подетални политики и процедури во кои се опишани техничките и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичка инфраструктура

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

СТАНДАРДНО НИВО - ТЕХНИЧКИ МЕРКИ

* Автентикација на овластените лица
* Обезбедување на опремата на која се врши обработка на личните податоци
* Сегрегација на должности и одговорности
* Контрола на пристап до информацискиот систем
* Обезбедување евиденција за секој пристап (logs)
* Обезбедување на преносливите медиуми
* Заштита на внатрешната мрежа
* Обезбедување на серверите
* Обезбедување на веб-страницата на контролорот
* Превенирање, реакција и санирање на инциденти
* Сигурносни копии и повторно враќање на зачуваните лични податоци
* архивирање и чување на податоците
* Управување со преносливи медиуми
* Криптирање на личните податоци
* Физичка безбедност
* Управување со обработувачи

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

СТАНДАРДНО НИВО - ОРГАНИЗАЦИСКИ МЕРКИ

* Ограничен пристап со идентификација за пристап до личните податоци
* Организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори
* Уништување на документи по истекот на рокот за нивно чување
* Мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци
* Почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци
* Информирање и едуцирање за заштитата на личните податоци

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

ВИСОКО НИВО - ТЕХНИЧКИ МЕРКИ

* Управување со лозинки
* Сертификација за заштита на личните податоци
* Управување со преносливи медиуми
* Сертификациони постапки
* Пренесување на медиуми
* Пренесување на личните податоци преку мрежа за електронски комуникации

ТЕХНИЧКА И ИНТЕГРИРАНА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Data Protection by Default and Design

* **Техничката и интегрирана заштита на личните податоци** е една од новите мерки кои се воведуваат како задолжителни за контролорите и обработувачите на личните податоци. Согласно оваа мерка, земајќи ги предвид најновите технолошки достигнувања, трошоците за спроведување, природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста на правата и слободите на физичките лица кои произлегуваат од обработката, контролорот ги има следните обврски:

- во моментот на дефинирање на средствата за обработка, како и во моментот на самата обработка, да примени, односно применува соодветни технички и организациски мерки со кои ќе се обезбеди ефикасно спроведување на начелата за заштита на личните податоци, како што се на пример псевдонимизацијата и сведувањето на минимален обем на податоците (data minimization);

- да ги примени сите потребни заштитни мерки во процесот на обработката, со цел за да се исполнат условите за законита обработка на личните податоци и воедно да се обезбеди заштита на правата на субјектите на личните податоци.

ПРОЦЕНКА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ
Data Protection Impact Assessment

Согласно оваа контролна мерка, кога при користење на нови технологии за некој вид на обработка на личните податоци, земајќи ги предвид природата, обемот, контекстот и целите на обработката, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица, пред да биде извршена обработката, контролорот има обврска да изврши проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци (Data Protection Impact Assessment - ДПИА).

ПРОЦЕНКА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ
Data Protection Impact Assessment

Се врши најмалку во следните случаи:

- во случај на систематска и сеопфатна оценка на личните аспекти кои се поврзани со физички лица, која се заснова на автоматска обработка, вклучувајќи и профилирање, а врз основа на која се донесуваат одлуки кои произведуваат правно дејство во врска со физичкото лице или значително влијаат на физичкото лице;
- во случај на обемна обработка на посебните категории на лични податоци или на лични податоци поврзани со казнени осуди и казнени дела; или
- во случај на систематско набљудување на јавно достапни простори во големи размери.

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ
ПРОБИВАЊЕ НА ЛОЗИНКИ
(Password Cracking)

* Guessing - погодување
* Brute Forcing - погодување со сила
* Dictionary attack - претпоставен напад
* Shoulder surfing - „Сиркање“ преку рамо
* Social engineering - Социјален инженеринг

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ЛОЗИНКИ И СЕГРЕГАЦИЈА НА ДОЛЖНОСТИ

* Единствено корисничко име - Unique User Name
* Силна лозинка - Strong Password (complexity requirements, password age limitation, enforcement of password history)
* Праг на заклучување - Account lockout threshold

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ НАСОКИ ЗА ЛОЗИНКИ

* Употреба на фрази (песна, стих, цитат, книга, општо познат факт)
* Несподелување на лозинките со никого НИКОГАШ
* Не ги запишувајте лозинките
* Запамтете ги и не ги чувајте во вашиот паричник или чанта

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ
НАСОКИ ЗА ЛОЗИНКИ
добри лозинки

„Skopjeeglavengrad“	„Скопје е главен град“
B1tolaekonzulskigr@d	„Битола е конзулски град“
E.T.phonehome“	„E.T. phone home“
„ReturnoftheJedi“	„Return of the Jedi“
„Tretopoluvreme“	„Трето полувреме“
„Beforethera1n“	„Before the Rain“
„1malidenz@naS“	„Има ли ден за нас“

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ
НАСОКИ ЗА ЛОЗИНКИ
лоши лозинки

12345678	Isus
87654321	Muhamed
Password	username
Login	welcome
football	Сопственото име и презиме

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ НАСОКИ

* Заклучете го системот
* Силна лозинка
* Исклучени гостински профили
* Преименувајте го администраторскиот профил
* Исклучете го старт менито
* Применете последна верзија на софтвер
* Користете заштитен ѕид (firewall)
* Криптирајте
* Исклучетите ги непотребните сервизи
* Исклучете ги непотребните процеси
* Ревизија
* Скријте ги важните датотеки

ШТО НЕ ПРАВИ РАНЛИВИ?

* Ниското ниво на свест
* Фабричките нагодувања
* Зголемената онлајн активност
* Не инвестирање во безбедносни системи
* Не следење на безбедносните стандарди