# БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

**Игор Кузевски**

**Експерт за заштита на личните податоци**

# СОДРЖИНА

* Безбедност на лични податоци
* Што да (не) правиме?
* Нарушување на безбедноста на личните податоци
* Проценка на влијанието на заштитата на личните податоци

# Зошто и дали ни е потребна информациска сигурност?

- Преку 90% од целупната e-mail комуникација е таканаречена SPAM
- Лажни веб страници (pharming)
- Лажни e-mail адреси (phishing)
- Злонамерни кодови (интернет вируси)

IF IT SOUNDS TO GOOD TO BELIEVE IT, DON'T BELIEVE IT!!!

# ПОТЕНЦИЈАЛНИ ЗАГУБИ ПРИ БЕЗБЕДНОСНИ НАПАДИ

Финансиски

Недостапни ресурси

Губење на доверба

Кражба на идентитет

Кражба на податоци

Злоупотреба на компјутерските ресурси

# ЗАКАНИ ЗА ИНФОРМАЦИСКАТА СИГУРНОСТ

* Virus
* Worm
* Backdoor
* Trojan
* Key-logger
* Password cracking

# ЕЛЕМЕНТИ НА СИГУРНОСТ

* **ДОВЕРЛИВОСТ (confidentiality)**
* **ИНТЕГРИТЕТ (integrity)**
* **ДОСТАПНОСТ (availability)**
* **АВТЕНТИКАЦИЈА (authenticity)**

# Документација (отчетност)

**Политика за системот за заштита на личните податоци**

најважен и прв документ со кој се документира процесот за управување со системот за заштита на личните податоци кој треба да им одговара на природата, обемот и сложеноста на активностите коишто контролорот ги врши при обработката на личните податоци и ризиците на коишто е изложен.

# Документација (отчетност)

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

Превенирање, реакција и санирање на инциденти

Сигурносни копии и повторно враќање на зачуваните лични податоци

Криптирање на личните податоци

Физичка безбедност

# БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ПРОБИВАЊЕ НА ЛОЗИНКИ

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

# УПРАВУВАЊЕ СО ЛОЗИНКИ

* 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

## УПРАВУВАЊЕ СО 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
* Една лозинка за една цел

# Примери на лоши лозинки

| | |
|---|---|
| 12345678 | Jesus |
| 87654321 | Muhammed |
| Password | username |
| Login | welcome |
| football | Сопственото име и презиме |

# Примери на добри лозинки

| | |
|---|---|
| „Sk0pjeeglavengrad“ | „Скопје е главен град“ |
| B1t0laekonzulskigr@d | „Битола е конзулски град“ |
| E.T.ph0nehome“ | „E.T. phone home“ |
| „Return0ftheJedi“ | „Return of the Jedi“ |
| „Tret0p0luvreme“ | „Трето полувреме“ |
| „Bef0rethera1n“ | „Before the Rain“ |
| „1malidenz@naS“ | „Има ли ден за нас“ |

# ПРЕПОРАКИ

- Заклучете го системот
- Силна лозинка (една лозинка за една сметка)
- Криптирајте
- Сокријте ги важните датотеки

# Што не прави ранливи?

Ниското ниво на свест

Фабричките нагодувања

Зголемената онлајн активност

Ние така работиме од секогаш

# Нарушување на безбедноста

* е секое нарушување на безбедноста, што доведува до случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат.
* Доколку не се реши на соодветен и навремен начин може да резултира со:

- материјална или нематеријална штета
- губење на контрола над личните податоци
- ограничување на правата, дискриминација, кражба на идентитет или измама
- нарушување на угледот
- губење на доверливоста на личните податоци, значителна економска или социјална неповолност за засегнатите физички лица

# Известување на АЗЛП

* Веднаш пд дознавањето дека се случило нарушување на личните податоци, треба да го извести АЗЛП:

- без непотребно одложување
- не подоцна од 72 часа откако ќе се дознае, освен ако се утврди дека нарушувањето на личните податоци веројатно нема да резултира со **ризик** за правата и слободите на физичките лица

* Кога известување не може да се изврши во рок од 72 часа, причините за доцнењето треба да го придружуваат известувањето и информациите може да се доставуваат во фази без непотребно дополнително одложување

# Комуницирање со засегнатите субјекти

* Контролорот треба да го комуницира субјектот на личните податоци за нарушувањето на личните податоци, без непотребно одлагање, кога тоа прекршување на личните податоци веројатно ќе резултира со **висок** ризик за правата и слободите на физичкото лице со цел да му се овозможи да ги преземе потребните мерки
* Комуникацијата треба да ја опише природата на прекршувањето на личните податоци, како и препораки за засегнатото физичко лице да ги ублажи потенцијалните негативни ефекти
* Таквите комуникации треба да се направат што е можно побргу и во тесна соработка со АЗЛП

# Што вели ЕДПБ

* смета дека известувањето има голем број на придобивки
- Известувањето за нарушување треба да се гледа како алатка за подобрување на усогласеноста во однос на заштитата на личните податоци
- Контролорите и обработувачите се охрабруваат однапред да планираат и да воспостават процеси за да можат да откријат и навремено да го намалат нарушувањето, да го проценат ризикот за поединците, а потоа да утврдат дали е неопходно да го известат надлежниот надзорен орган и да го комуницираат нарушувањето со засегнатите поединци кога е потребно. Известувањето до надзорниот орган треба да биде дел од тој план за одговор на инцидентот

# Што сметам јас (лично мислење)

* Законското барање за известување е еден од најголемите предизвици за офицерите
* Нарушување (без) известување до АЗЛП сè уште може да се гледа како алатка за учење и искуство
* Барањето за известување троши енергија што може да се искористи за да се ублажат последиците
* Можеме и треба однапред да планираме и да воспоставиме процеси за да можеме да откриеме и навремено да го спречиме нарушувањето, да го процениме ризикот за поединци, без известување
* Тоа е против човечката природа

# Нарушувања ќе се случат, порано или подоцна, НО

* Нарушувањата на податоците може да бидат и симптом за ранлив, можеби застарен режим на безбедност на податоците
* Тие исто така може да укажуваат на слабости на системот што треба да се решат
* Секогаш е подобро да се спречи нарушувањето на податоците со тоа што однапред се подготвуваме преку:
* Правилна имплементација на ТОМ
* Обука и свесност за прашањата за заштита на податоците на вработените

# ОДГОВОРНОСТ И ВОДЕЊЕ ЕВИДЕНЦИЈА

* Без оглед на тоа дали треба или не за нарушувањето да се извести АЗЛП, мораме да водиме документација за сите нарушувања
* Иако на контролорот е да одреди кој метод и структура ќе го користи при документирање на нарушувањата, во однос на информациите што може да се запишуваат, постојат клучни елементи кои треба да бидат вклучени во сите случаи:

- запишете ги деталите во врска со нарушувањето
- Причините
- што точно се случило
- засегнатите лични податоци
- ефекти и последици од нарушувањето
- преземени мерки за надминување

# Проценка (DPIA)

Кога при користење на нови технологии за некој вид на обработка, според 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 е должен да изврши проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци.

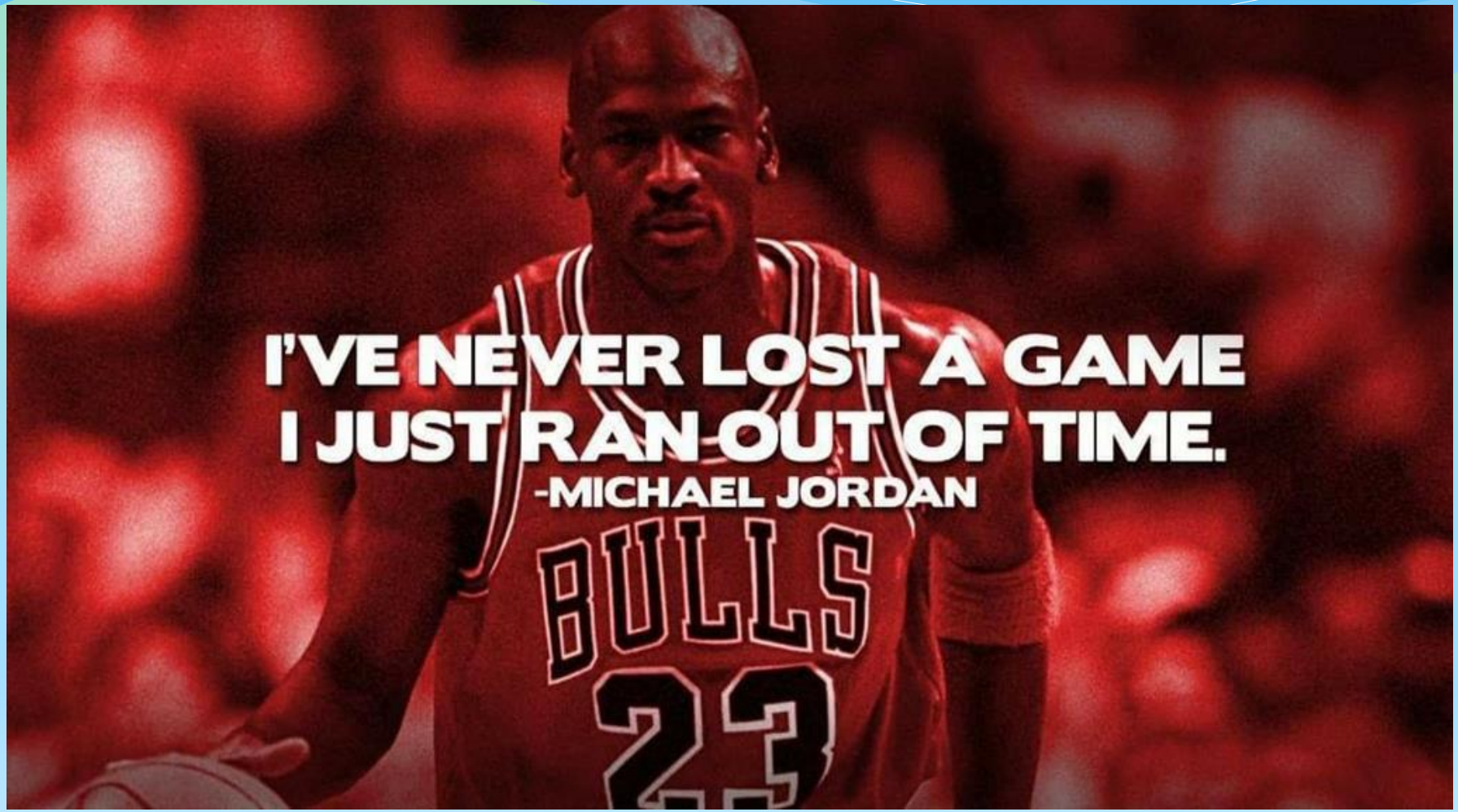
# Проценка (DPIA)

- 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;
- обемна обработка на посебните категории на лични податоци или на лични податоци поврзани со казнени осуди и казнени дела; или
- систематско набљудување на јавно достапни простори во големи размери.

# ЗАВРШНИ МИСЛИ

* НАРУШУВАЊА ЌЕ СЕ СЛУЧУВААТ
* НАЈГОЛЕМА МОЖНОСТ Е ЧОВЕЧКАТА ГРЕШКА
* АВТОМАТИРАЊЕ НА ПРОЦЕСИТЕ
* ИМПЛЕМЕНТАЦИЈА НА СОВРЕМЕНА ТЕХНОЛОГИЈА

# Дали ја губиме „играта“ за заштита на нашата приватност?



# Што би им кажал на луѓето кои сакаат да бидат лидери и претприемачи за да бидат мотивирани?

Ако јас треба нешто да им кажам за да ги мотивирам, во нив нема материјал за лидери и претприемачи

Лидерите за разлика од другите имаат внатрешен локус на контрола и мотивација т.е. се само мотивирани. Тоа ги прави посебни!

На другите им треба некој да ги мотивира за да дејствуваат. Лидерите дејствуваат сами, затоа што имаат внатрешен порив и стремеж работите да ги прават подобри

Elon Musk


Thank you for attention
May the Force be with you
meme-generator.com