Zabezpečení osobních údajů před kyberútoky

Mgr. Michal Nulíček, LL.M., CIPP/E

CASHLESS FUTURE 2019

23. 10. 2019

ROWAN LEGAL

MEMBER OF MULTILAW

Kyberútok jako hrozba

Úspěšný kybernetický útok = bezpečnostní incident dle GDPR

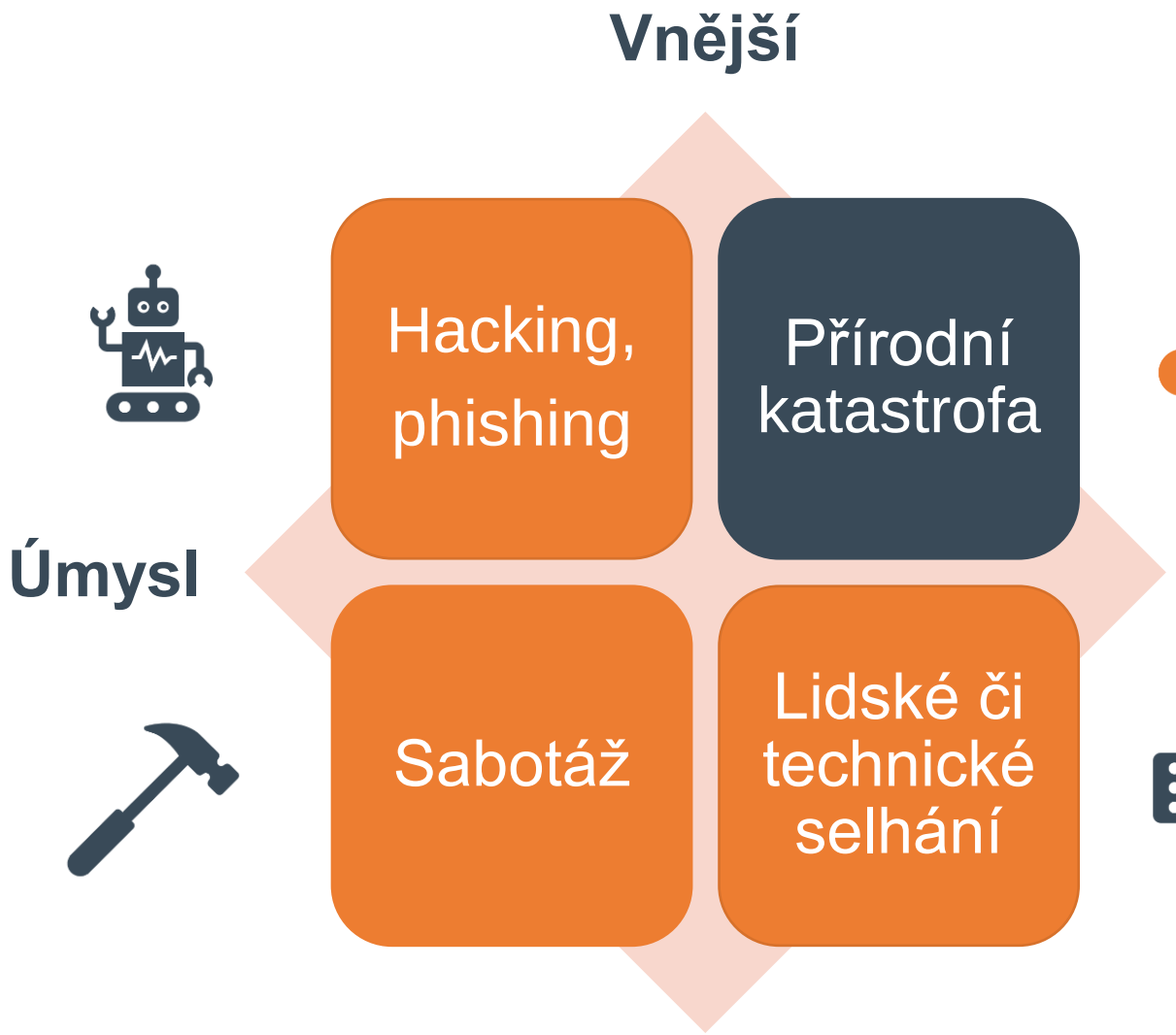
- **Nejzávažnější porušení GDPR – vysoké pokuty**
  - ICO (Velká Británie)
    - **British Airways** – kybernetický útok na web – pokuta ve výši **£ 183M** (cca 1,5 % celosvětového obratu)
    - **Marriott** – zranitelnost v rezervačním systému – pokuta **£ 100M;**
    - **Facebook (Cambridge Analytica)** – pokuta **£ 500k** (před GDPR maximální výše pokuty), pokuta od FTC (USA) ve výši $ 5 mld.
  - NAIH (Maďarsko)
    - útok na IS politické strany prostřednictvím webu – pokuta ve výši **€ 34k.**
- **Roste význam prevence –** vedle pokut mohou být uplatněny náhrady škody, obrovské reputační riziko / ztráta důvěry.


The Guardian
Marriott to be fined nearly £100m over GDPR breach
ICO imposes fine after personal data of 339 million guests stolen by hackers
The international hotel group Marriott is to be fined a
Information Commissi Office after hackers stol
llion guests.
BBC
Sign in
News
Sport
Reel
Worklife
NEWS
Facebook fined £500,000 for Cambridge Analytica scandal
acebook has been fined £500,000 by the UK's data protection watchdog for
role in the Cambridge Analytica data scandal.
BA fined a record £183m af
hackers stole customer deta
British Airways is facing an unprecedented £183 million fine for failing to pro
the "fundamental privacy rights" of half a million of its passengers whose dat
s hacked last year.

Typy hrozeb


Vnější
Úmysl
Náhoda
Vnitřní
Hacking, phishing
Přírodní katastrofa
Sabotáž
Lidské či technické selhání

Typy hrozeb



- osoby s přístupem k údajům ve společnosti
- předávání údajů mimo společnosti
- akvizice/fúze (případ Marriott)

Hacking, phishing

- **Kybernetický útok – prolomení zabezpečení**
  - z pohledu GDPR **jde bezpečnostní incident** (nedostatečné zabezpečení)
    - nutné vyhodnotit riziko, případně ohlásit dozorovému úřadu
  - možná náhrada škody dle GDPR + kompenzace dle bankovní regulace

×

- **Phishingový útok**
  - z pohledu GDPR **nejde o bezpečnostní incident**
  - (!) možná kompenzace dle bankovní regulace

Hrozby v prostředí společnosti

Zaměstnanci a další osoby s přístupem k údajům.

Minimalizace hrozeb – technická a organizační opatření:

- opatření mají odpovídat nejen rizikům ale také stavu techniky, nákladům na provedení, povaze, rozsahu zpracování;

Organizační opatření:

- interní směrnice - o bezpečnosti IT, ochraně osobních údajů, …
- jednoznačné vymezení rolí a odpovědností;
- školení zaměstnanců a dalších osob s přístupem;
- dohoda o mlčenlivosti;
- plán kontrol osob s přístupem údajům apod.
- pravidla výběru zpracovatelů / partnerů.

Technická opatření

- § 13 ZOOÚ (ÚOOÚ dle něho pořád postupuje);
- pseudonymizace a šifrování osobních údajů;
- důvěrnost, integrita, zálohování;
- Data Loss Prevention (DLP) – monitoring zaměstnanců;
  - (!) pracovněprávní aspekty.

Hrozby mimo společnost

- **Hrozba, kdykoliv údaje opouští společnost** – zpracovatelé

Audit zpracovatelů před jejich zapojení a v průběhu spolupráce

- správné nastavení **smlouvy o zpracování**, včetně NDA a technických a organizačních opatření
- správce nemusí být vždy odpovědný za jednání zpracovatele – zpracovatel může být odpovědný sám!

Manuály, checklisty a postupy k řešení incidentu

- např. aby nedošlo k tomu, že zpracovatel ohlásí ÚOOÚ situaci, kterou správce nepovažuje za incident

Certifikace a bezpečnostní záruky

- např. ISO/IEC 27001

Ohlášení bezpečnostního incidentu 1/2

- **Detekce** incidentu – proškolení zaměstnanců (organizační opatření), ale také monitoring neobvyklých aktivit v prostředí společnosti (technické opatření);
- **Mobilizace** odpovědného týmu;
- **Prověření incidentu** – sběr podkladů, včetně případné součinnost třetích stran;
- Přijetí **vhodných opatření** – (!) zvážit i businessové dopady.

Ohlášení bezpečnostního incidentu 2/2

- **Ohlásit dozorovému úřadu do 72 hodin:**
  - běží od **okamžiku, kdy se o něm správce dozví;**
  - (!) **prověřit, zda se se skutečně jedná o incident**, který je třeba ohlašovat – **metodika ENISA** pro určení rizikovosti incidentu;
  - Pokud je naopak **riziko vysoké**, je třeba oznámit narušení i **dotčeným subjektům údajů.**
- **Roste význam prevence;**
- **Odpovědnosti se lze zprostit – veškeré úsilí k tomu, aby k incidentu;**
  - školení zaměstnanců, interní směrnice apod.

Shrnutí

- **Úspěšný kybernetický útok je zpravidla bezpečnostním incidentem;**
- **Nejvyšší pokuty za porušení GDPR uloženy právě za incidenty;**
- **Roste význam prevence**
  - nejen pokuty, ale také uplatnění náhrady škody, reputační riziko / ztráta důvěry;
- **Technická a organizační opatření snižují riziko úspěšnosti útoku;**
  - a současně jsou jimi plněny požadavky GDPR na zabezpečení údajů;
- **72 hodin na ohlášení dozorovému orgánu;**
  - jednat rychle, ale nezapomenout na businessové dopady.

Děkuji za pozornost

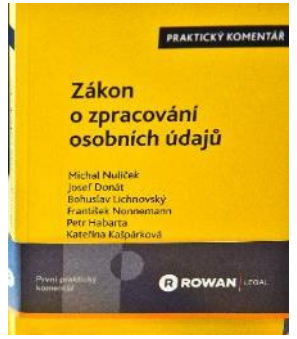
Mgr. Michal Nulíček, LL.M., CIPP/E

nulicek@rowan.legal

ROWAN LEGAL

Praktický komentář: Zákon o zpracování osobních údajů

Michal Nulíček je jedním z autorů praktického komentáře



Více na www.rowan.legal

The LEGAL 500 EMEA TOP TIER 2019

TOP RANKED Chambers EUROPE 2019 Rowan Legal

2018 právnická firma roku

ROWAN LEGAL

+420 224 216 212

www.rowan.legal