Kybernetická bezpečnost ve veřejné správě

Jan Dienstbier

Garant platformy KYBEZ

Moto

„Cokoliv je připojeno lze hacknout!“

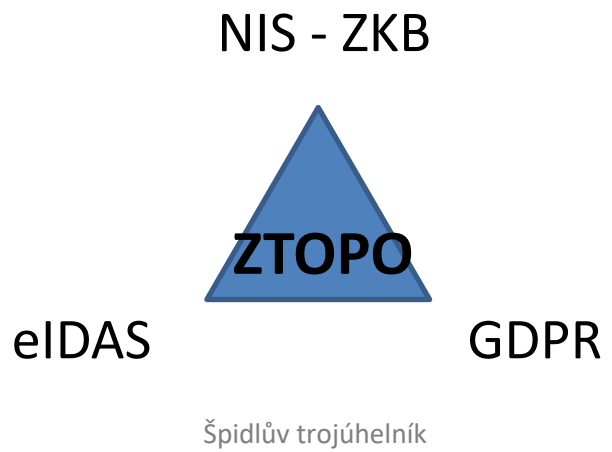
Oddělení kybernetické kriminality

„Rozlišuji pouze dvě kategorie systémů, ty které již hackli a ty, které to ještě nevědí“

John Chambers ex CEO Cisco

Co nás čeká

- **Zákon o KYBERNETICKÉ BEZPEČNOSTI** (181/2014 Sb.) **a jeho novelizace**
  - Rozšíření počtu povinných subjektů
  - Zostřený dohled ze strany NBÚ, vyšší pokuty
- **GDPR** a novela zákona o ochraně osobních údajů
- **eIDAS**
- **Smart cities, internet věcí**
- Výrazný dopad do oblasti bezpečnosti (kybernetické, informací, ochrany osobních údajů…)



Špidlův trojúhelník

Zákon o kybernetické bezpečnosti v novelizované podobě (NIS)

- Rozšíření záběru
  - Poskytovatelé základních služeb (určí NBÚ)
    - ZKB - základní službou je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví:

- energetika
- doprava,
- bankovnictví
- infrastruktura finančních trhů,
- zdravotnictví
- dodávky a rozvody pitné vody
- digitální infrastruktura
- chemický průmysl
- **veřejná správa**

ZKB - informačním systémem základní služby je informační systém, na jehož fungování je závislé poskytování základní služby,

Zákon o kybernetické bezpečnosti v novelizované podobě (NIS)

Dopadová určující kritéria

Dopadové určující kritérium je naplněno v okamžiku, kdy narušení bezpečnosti informací v informačním systému a síti základní služby může způsobit některý z následujících dopadů:

a) omezení základní služby postihující více než 50 000 – 100 000 osob,

b) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,

c) hospodářskou ztrátu vyšší než 250 – 500 milionů Kč,

d) nedostupnost služby poskytované alespoň 50 000 – 100 000 osobám, která není nahraditelná jinou službou,

e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření,

f) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území obce s rozšířenou působností,

g) kompromitaci citlivých údajů o nejméně 200 000 osobách.

Odvětvová určující kritéria

Speciální průřezová kritéria a jejich prahové hodnoty budou nastaveny tam, kde je to relevatní, na základě výsledků jednání pracovní skupiny

- Např. ve zdravotnictví jedno z kriterií - Specializované zdravotnické zařízení, které má v České republice méně než x alternativních zařízení se stejným zaměřením

eIDAS

Nařízení Evropského parlamentu o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním evropském trhu

- Účinnost od 1.7.2016 – přechodné období 2 roky
  - Uznávání prostředků pro elektronickou identifikaci fyzických (el.podpis) a právnických (el.pečeť) osob
    - Vytvoření Národní identitní autority - stát garantuje identitu v kyberprostoru – je to něco až tak nového?
  - Pravidla pro služby vytvářející důvěru
  - Úplné elektronické podání

Jen tak na okraj – 74% útoků jde přes zneužitou (špatně zabezpečenou) identitu (WannaCry …) a zase ty pokuty - až 2 mil. Kč

GDPR

Nařízení Evropského parlamentu o ochraně a práci s osobními údaji

- V účinnost 25. května 2018
- Nahrazuje předchozí směrnici 95/46 a zákon 101/200 Sb.
- Nejkomplexnější soubor pravidel pro ochranu osobních údajů
- Regulátorem v ČR ÚOOÚ
- Zaváděno kvůli ochraně osob a nejednotné evropské legislativě
- Posílení práv subjektů osobních údajů
- Všude stejně, včetně sankcí – nemalých
- Regulátorem v ČR ÚOOÚ

Závádí institut osobní újmy

GDPR hlavní změny proti stávající situaci

- Hlášení incidentů
- Posuzování vlivu na soukromí (DPIA)
- Jmenování pověřence na ochranu osobních údajů (DPO)
- Security „ by design“ a „ by default“
- Právo na přenositelnost

- Zrušení informační povinnosti
- Gradace povinností dle rizikovosti
- Možnost vyjímek z práv a úpravy domáci legislativou
- One stop shop (vše na jednom místě)

Plynoucí požadavky

- Povinnost přijmout opatření adekvátní rizikům (posouzení dopadu)
  - Procesy
  - Důvod zpracování
  - Jen po dobu nezbytnou
  - Organizační opatření
  - Technická opatření (šifrování, pseudonymizace, anonymizace osobních dat)
- Povinnost uchovat záznam u správců a zpracovatelů
- Spolupráce správce a zpracovatele s dozorovými orgány
- Povinnost hlásit incident do 72 hodin

Pseudonymizace x Anonymizace

- Anonymizace - nevratná změna => nejsou OÚ
- Pseudonimizace - zpracování osobních údajů tak, aby data nemohla být přiřazena ke konkrétní osobě či subjektu – lze opět přiřadit => stále OÚ
- Převážně na databázové vrstvě

Bezvýznamový identifikátor

Bezvýznamový identifikátor, Adresa

Bezvýznamový identifikátor, Jméno, Příjmení, Adresa

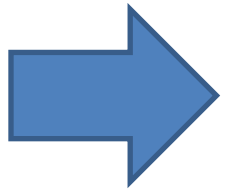
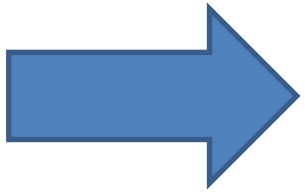
Bezvýznamový identifikátor, Jméno, Příjmení

Správní pokuty

- Odvíjí se od závažnosti a charakteru přestupku
  - Úmysl vs. Nedbalost
  - Počet dotčených subjektů
  - Kroky podniknuté ke zmírnění škody
  - Oblast osobních údajů dotčená porušením nařízení
  - …
- Pokuty ve výši milionů EUR nebo % výše ročního obratu daného subjektu

GDPR revoluce nebo evoluce

Jak pro koho

- Kdo postupoval v souladu se zákonem 101/2000 Sb.  Evoluce
- Kdo ne  REVOLUCE

Závěr

Aby se z toho nestal Bermudský trojúhelníku, musíte:

- Si přestat lhát
- Nepodceňovat reputační riziko
- Postavit se k řešení čelem, nepřehazovat na jiné
- Nevnímat jednotlivé vrcholy izolovaně (ušetří to čas, peníze i nervy)
- Nebát se pořádku
- Zpracovat GAP analýzy
- Navrhnout opatření
- Implementovat opatření
- Nevymlouvat se na blížící se volby
- Nikdy se nezastavit (PDCA cyklus) a stále se zlepšovat

Děkuji za pozornost.

Jan Dienstbier

Garant platformy KYBEZ

info@kybez.cz, www.kybez.cz