Aktéri Cyber Security
Kto, prečo, ako ...

Rastislav Janota
Predseda
Výbor pre kybernetickú bezpečnosť
Bezpečnostná rada SR
NBÚ

KOHO SA TÝKA KB?

Koho sa týka kybernetická a informačná bezpečnosť?

NÁS VŠETKÝCH!!!

Veď každý je zodpovedný za svoje vlastné dáta.

PREČO EURÓPSKA REGULÁCIA?

- Jednotný digitálny trh Európskej únie
- Cezhraničná podstata kybernetických incidentov
- Viac a viac údajov dostupných prostredníctvom komunikačných sietí
- Viac a viac služieb dostupných prostredníctvom komunikačných sietí

- Snaha EU o zvýšenie schopností kybernetickej bezpečnosti na úrovni členských štátov (ČS)
- Snaha o zlepšenie kooperácie medzi ČS v oblasti kybernetickej bezpečnosti
- Snaha o vytvorenie silného hráča z EU v oblasti kybernetickej bezpečnosti

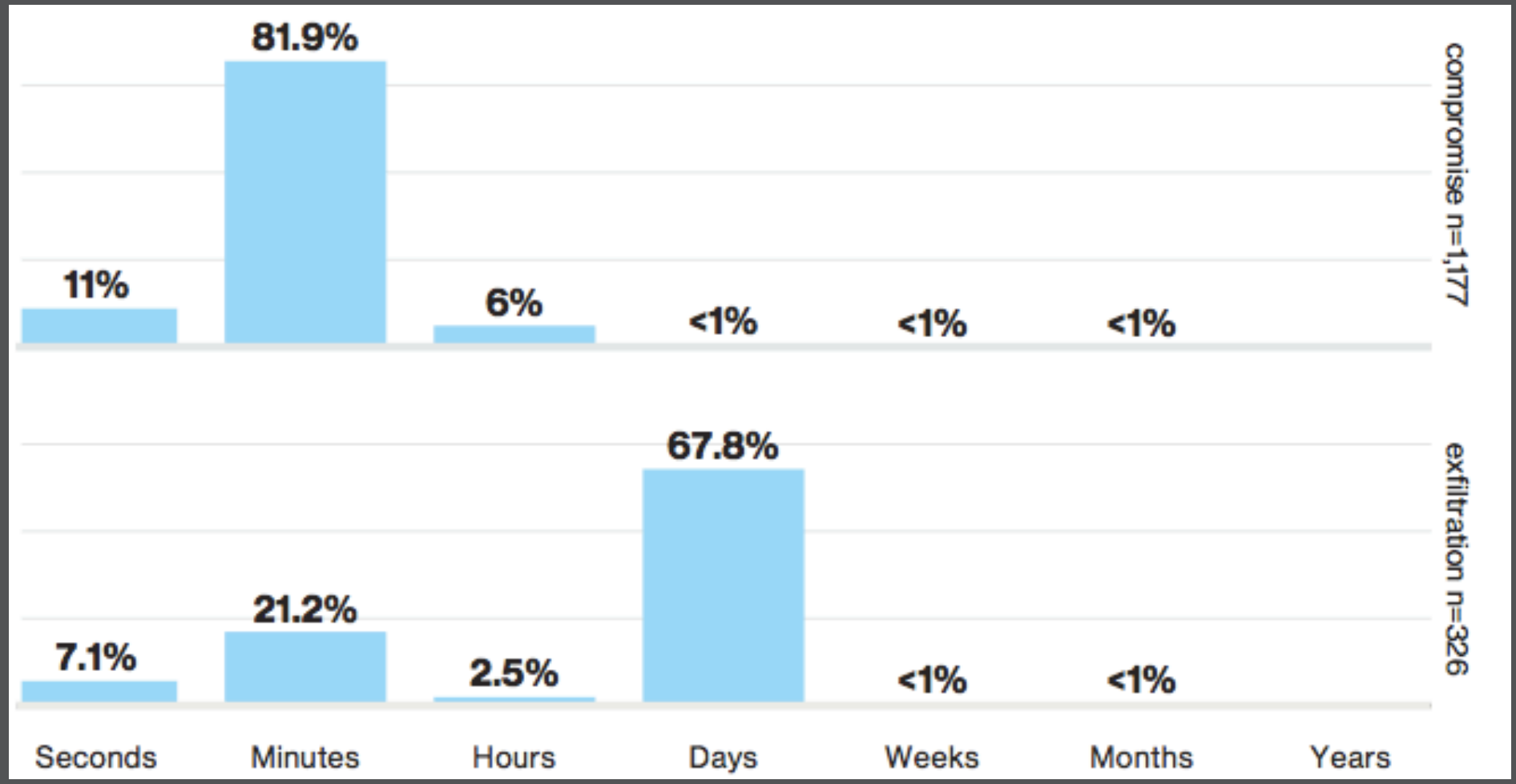
- Vytvorenie úvodu do problematiky na úrovni EU pre zachytenie trendov v oblasti kybernetickej bezpečnosti vzhľadom na rýchly rozvoj technológii ako IoT, connected cars a pod.

AKÉ REGULÁCIE EXISTUJÚ A KOHO SA TÝKAJÚ?

- **General Data Protection Regulation (GDPR) – 2016/679**
  - Regulácia sa týka subjektov spracovávajúcich akékoľvek osobné údaje
  - Regulátor – Úrad na ochranu osobných údajov
- **Payment Services Directive (PSD2) – 2015/2366**
  - Regulácia sa týka subjektov s bankovou licenciou SR
  - Regulátor – Národná banka Slovenska
- **Regulatory framework for electronic communications (2009)**
  - Podľa zoznamu firiem zapísaných v zozname podnikov (oblasť elektronických komunikácii)
  - Regulátor - Úrad pre reguláciu elektronických komunikácií a poštových služieb

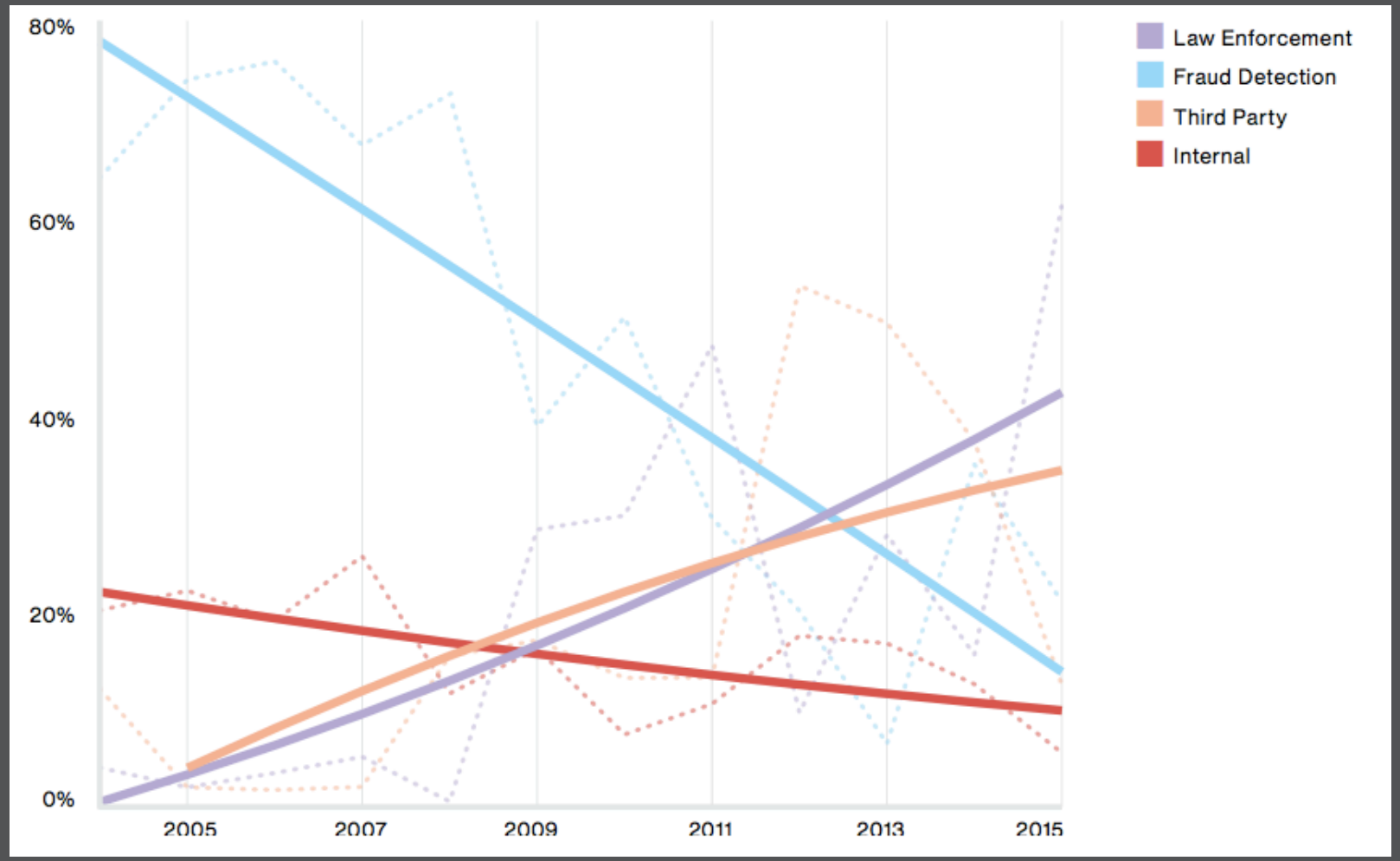
- **Network and Information Security Directive 2016/1148**
  - Podľa zoznamu firiem zapísaných v registri PZS a registri PDS
  - Regulátor – Národný bezpečnostný úrad (NBÚ)

TROCHU ŠTATISTIKY



Verizon 2016 Data Breach Investigations Report

TROCHU ŠTATISTIKY



Verizon 2016 Data Breach Investigations Report

ZAKLADNÉ AKTIVITY NAD KYBERNETICKÝM PRIESTOROM

Riešenie

- Kybernetickej kriminality
  - Kybernetická kriminalita je akékoľvek nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu
- Kybernetickej obrany
  - ZoKB novelizuje Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky – rozširuje ho o obranu štátu v kybernetickom priestore a pod.
- Kybernetického spravodajstva
  - Gestorom sú SIS/VS v rozsahu svojich pôsobností
- Kybernetickej bezpečnosti
  - **Transpozícia smernice NIS**
  - Regulácia sektorov podľa zákona
  - Bezpečnostné štandardy
  - Riadenie rizík
  - Kontrola a audit

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI

Obsah zákona

- Organizácia a pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
- Národná jednotka CSIRT
- Jednotný informačný systém kybernetickej bezpečnosti,
- Postavenie a povinnosti prevádzkovateľa základných služieb a poskytovateľa digitálnych služieb
- Jednotky CSIRT pre riešenie kybernetických bezpečnostných incidentov a ich akreditáciu,
- Systém zabezpečenia kybernetickej bezpečnosti, hlásenia a riešenie incidentov
- Kontrolu nad dodržiavaním tohto zákona, priestupky
- Určenie zoznamu všeobecne záväzných právnych predpisov pre oblasť KB
- Úprava zákona o kritickej infraštruktúre
- Odmeňovanie pracovníkov VS v oblasti kybernetickej bezpečnosti
- Určenie sektorov a VPA pre sektory a podsektory
- Novelizácia zákonov o obrane a ozbrojených silách

PREVÁDZKOVATEĽ ZÁKLADNEJ SLUŽBY

Prevádzkovateľ základnej služby (PZS)

- Smernica v prílohe 2 určuje minimálne 7 sektorov pre PZS
- Kritéria pre určenie PZS naznačuje smernica a je vhodné ich harmonizovať naprieč ČŠ
- ČŠ následne musia určiť subjekty v kategórii Prevádzkovateľ základnej služby
- ČŠ musia vytvoriť zoznam základných služieb a regulovať u PZS len tieto služby
- ČŠ by mali určiť kritéria na posúdenie závažnosti rušivého vplyvu incidentu
- ČŠ môžu prijať alebo zachovať ustanovenia, ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov

Prevádzkovateľ základnej služby (PZS)

- Zabezpečuje kontinuitu digitálnej služby
- Zavedie a vykonáva bezpečnostné opatrenia, vedie bezpečnostnú dokumentáciu
- Plní notifikačné povinnosti voči Úradu, nahlasuje incidenty a prijíma opatrenia
- Vykonáva audit a podriaďuje sa kontrole

REGULOVANÉ SEKTORY PODĽA ZÁKONA

Príloha 1: Sektory pre určenie Prevádzkovateľov základných služieb

- Energetika
- Doprava
- Bankovníctvo
- Finančné trhy
- Zdravotníctvo
- Pitná voda
- Digitálna infraštruktúra
- Chemický priemysel
- Telekomunikačný sektor
- Verejná správa

POSKYTOVATEĽ DIGITÁLNYCH SLUŽIEB

Poskytovateľ digitálnych služieb (PDS)

- Smernica v prílohe 3 určuje presne 3 druhy digitálnych služieb
- ČS podľa smernice NISE nesmú ukladať PDS žiadne ďalšie bezpečnostné alebo oznamovacie požiadavky nad rámec tých, ktoré určuje smernica

Poskytovateľ digitálnych služieb (PDS)

- Zabezpečí kontinuitu digitálnej služby
- Plní notifikačné povinnosti voči Úradu, nahlasuje incidenty a prijíma opatrenia
- Podriaďuje sa základnej kontrole

Online trhovisko

Internetový vyhľadávač

Služby cloudcomputingu

JEDNOTKY CSIRT

Jednotky CSIRT

- ČŠ určí jedna alebo viac jednotiek spĺňajúcich požiadavky Prílohy 1 Smernice NIS, pokrývajúce aspoň odvetvia z Prílohy 2 Smernice NIS (akreditácia CSIRT)
- Jednotky CSIRT podľa Smernice možno zriadiť v rámci príslušného orgánu
- S cieľom prispieť k rozvoju dôvery medzi členskými štátmi a podporiť rýchlu a účinnú operačnú spoluprácu sa zriaďuje sieť vnútroštátnych jednotiek CSIRT

- Možnosť dobrovoľnej akreditácie CSIRTu ľubovoľnou právnickou osobou
- CSIRT musí plniť rovnaké požiadavky ako CSIRT VPA
- Získava možnosť prístupu do IS KB s právom využiť dostupné služby pre seba a svojich klientov

BEZPEČNOSTNÉ OPATRENIA PRE PZS

Bezpečnostné opatrenia sa prijímajú pre oblasť

a) riadenia bezpečnosti a rizík,
b) personálnej bezpečnosti,
c) bezpečnosti systémov a zariadení,
d) riadenia prevádzky,
e) riešenia kybernetických bezpečnostných incidentov
f) riadenia dostupnosti siete a informačného systému,
g) monitorovania, testovania bezpečnosti a bezpečnostných auditov,
h) technických opatrení.

BEZPEČNOSTNÉ OPATRENIA PRE PZS

Bezpečnostné opatrenia musia zahŕňať najmenej

a) detekciu kybernetických bezpečnostných incidentov,
b) evidenciu kybernetických bezpečnostných incidentov,
c) vnútorné postupy a predpisy pre riešenie kybernetických bezpečnostných incidentov,
d) postupy riešenia kybernetických bezpečnostných incidentov,
e) riešenie kybernetických bezpečnostných incidentov,
f) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
g) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania podľa § 10.

VŠEOBECNÉ ZÁVÄZNÉ PREDPISY

NBÚ pripraví v spolupráci s VPA a odbornou verejnosťou

- Podrobnosti o technickom, technologickom a personálnom vybavení,
- Prahové hodnoty pre identifikáciu základnej služby,
- Obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie, rozsah bezpečnostných opatrení,
- Kategórie a prahové hodnoty kybernetických bezpečnostných incidentov hlásených prevádzkovateľom základnej služby a poskytovateľom digitálnej služby,
- Podrobnosti o požiadavkách na audit a rozsahu auditu,
- Bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti,
- Klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
- Podrobnosti o vymieňaní informácií a osobných údajov s orgánmi členských štátov Európskej únie.

AKO ZÁKON VZNIKAL?

- Transpozícia smernice po jej schválení v júli 2016
- Niekoľko iterácii
- V polovici októbra medzinárodný workshop o transpozícii NIS ako súčasť aktivít predsedníctva v Bratislave
- V decembri 2016 prvý krát predstavená členom Výboru pre kybernetickú bezpečnosť Bezpečnostnej rady Slovenskej republiky
- Zapracovaná prvá časť pripomienok
- Na konci januára zákon predložený na verejné pripomienkovanie odbornej verejnosti (výbor, komisia riaditeľa a pod.)
- Zapracovaná druhá časť pripomienok
- 16.2. verejný workshop k zákonu po druhej sade pripomienok
- Máj posledné pripomienky od ÚPVII, 26.5.2017 návrh zákona uvoľnený do MPK
- Veľmi úzka spolupráca aj s SBA, SASIB, ISACA, ITAS počas celého procesu

ĎAKUJEM ZA POZORNOSŤ

rastislav.janota@nbu.gov.sk