Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

KYBERNETICKÁ BEZPEČNOSŤ A SAMOSPRÁVA

Na občanoch záleží

online cyklus Úradu splnomocnenca vlády SR pre rozvoj občianskej spoločnosti

20. apríla 2021

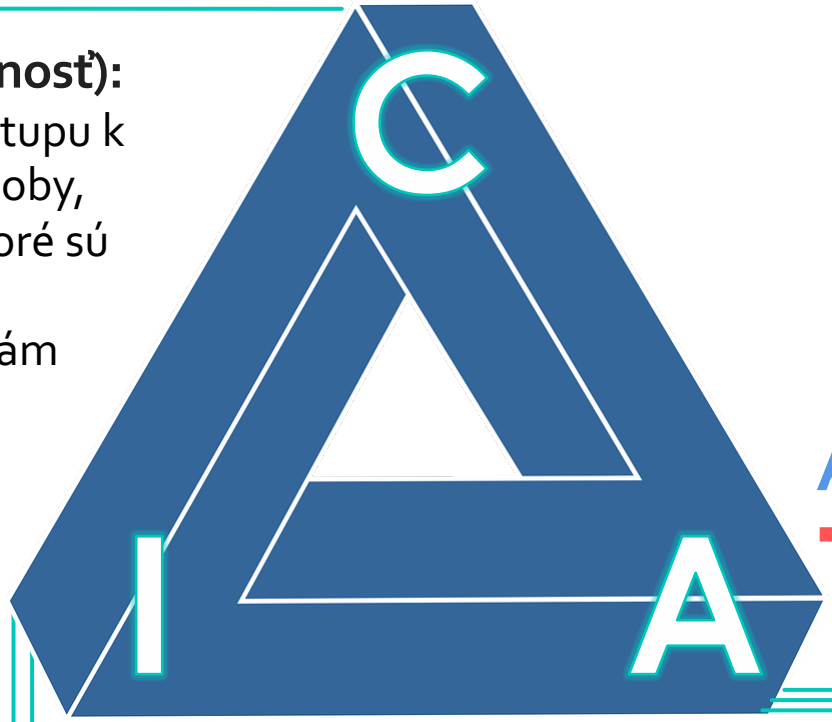
ivan.makatura@cybercompetence.sk

Kybernetická vs. informačná bezpečnosť

ZÁKLADNÉ ATRIBÚTY SPOĽAHLIVOSTI INFORMÁCIÍ

Confidentiality (Dôvernosť):

- Miera obmedzenia prístupu k informáciám len pre osoby, alebo skupiny osôb, ktoré sú oprávnené na prístup k príslušným informáciám



Availability (Dostupnosť)

- Miera dostupnosti informácie pre používateľa a systém vo chvíli, keď je informácia potrebná a požadovaná

Integrity (Celistvosť)

- Miera bezchybnosti informácie
- Charakteristikami integrity sú:
  - Úplnosť informácie
  - Správnosť informácie

DEFINÍCIA INFORMAČNEJ BEZPEČNOSTI

1. **Interdisciplinárna oblasť**, ktorá sa zaoberá skúmaním zraniteľností a hrozieb a/alebo vývojom metód a mechanizmov ochrany dát a informácií, ošetrovaním hrozieb a riadením a rizík, ktoré pôsobia na informačné aktíva
2. **Procesy a činnosti** zamerané na dosiahnutie požadovanej úrovne ochrany dát a informácií
3. **Stav systému**, kedy sú dostatočne ošetrené známe riziká vyplývajúce z hrozieb pôsobiacich na informačné aktíva

Informačná bezpečnosť (resp. bezpečnosť informácií) sa všeobecne považuje najmä za stav, v ktorom sú informácie považované za chránené voči hrozbám, bez ohľadu na:

- Fyzikálny stav dát,
- Formát dát,
- Spôsob interpretácie dát
- Médium, prostredníctvom ktorého sú dáta uchovávané a prenášané

INFORMAČNÁ vs. KYBERNETICKÁ BEZPEČNOSŤ

- **Informačná bezpečnosť** je zachovanie **dôvernosti, integrity a dostupnosti** informácií
  [ISO/IEC 27032, čl. 2.33]

- **Kybernetická bezpečnosť** je zachovanie **dôvernosti, integrity a dostupnosti** informácií v kybernetickom priestore
  [ISO/IEC 27032, čl. 4.20]

Štatistika napomáha pochopeniu

TYPICKÉ DÔVODY PRE VYKONÁVANIE PROCESU „INFORMAČNÁ BEZPEČNOSŤ“

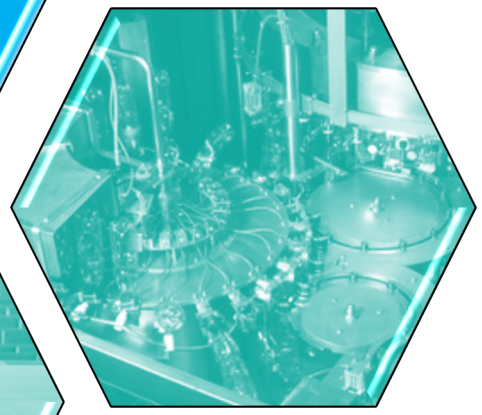
PREVENCIA INCIDENTOV 34%

OCHRANA KRITICKEJ INFRAŠTRUKTÚRY 11%

OCHRANA ZNAČKY OCHRANA REPUTÁCIE 21%

SÚLAD S REGULÁCIOU 62%

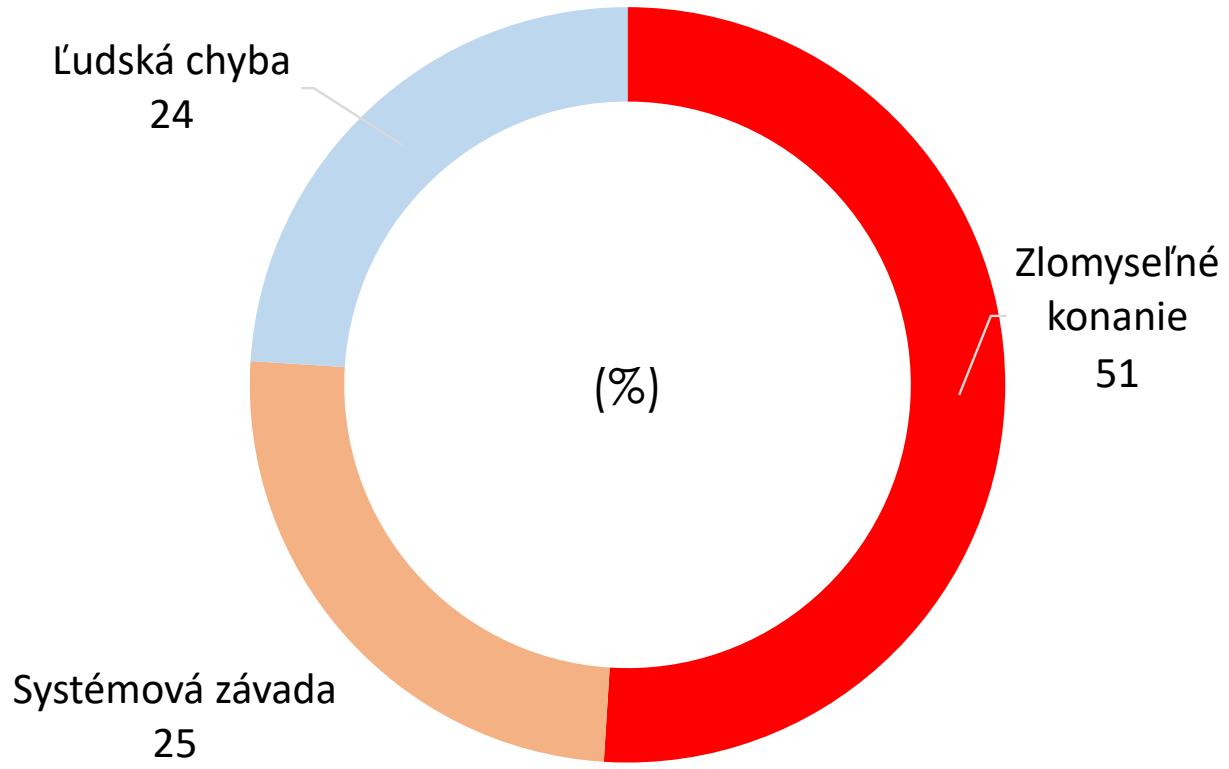
MINIMALIZÁCIA VÝPADKOV PRODUKCIE 69%



Zdroj: Ponemon’s Application Security Risk Study

PRÍČINY INCIDENTOV PODĽA ZDROJA

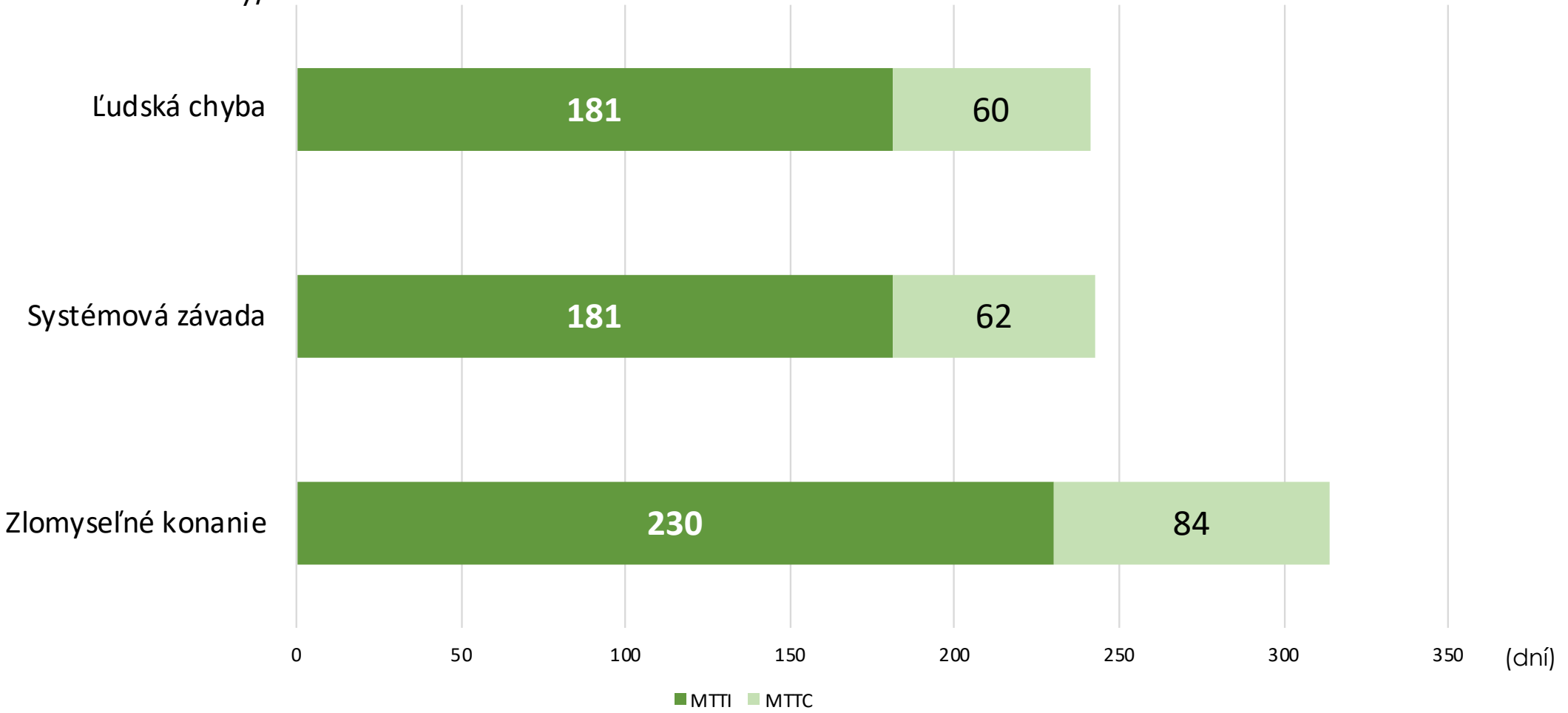
- Spôsob riešenia incidentu spôsobeného vonkajším útočníkom alebo zlomyseľným zamestnancom sa podstatne líši od riešenia incidentu spôsobeného ľudskou chybou alebo zlyhaním systému
- V reportoch zvyknú byť skúmané najmä nasledujúce tri základné príčiny incidentov



Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU PODĽA PRÍČINY

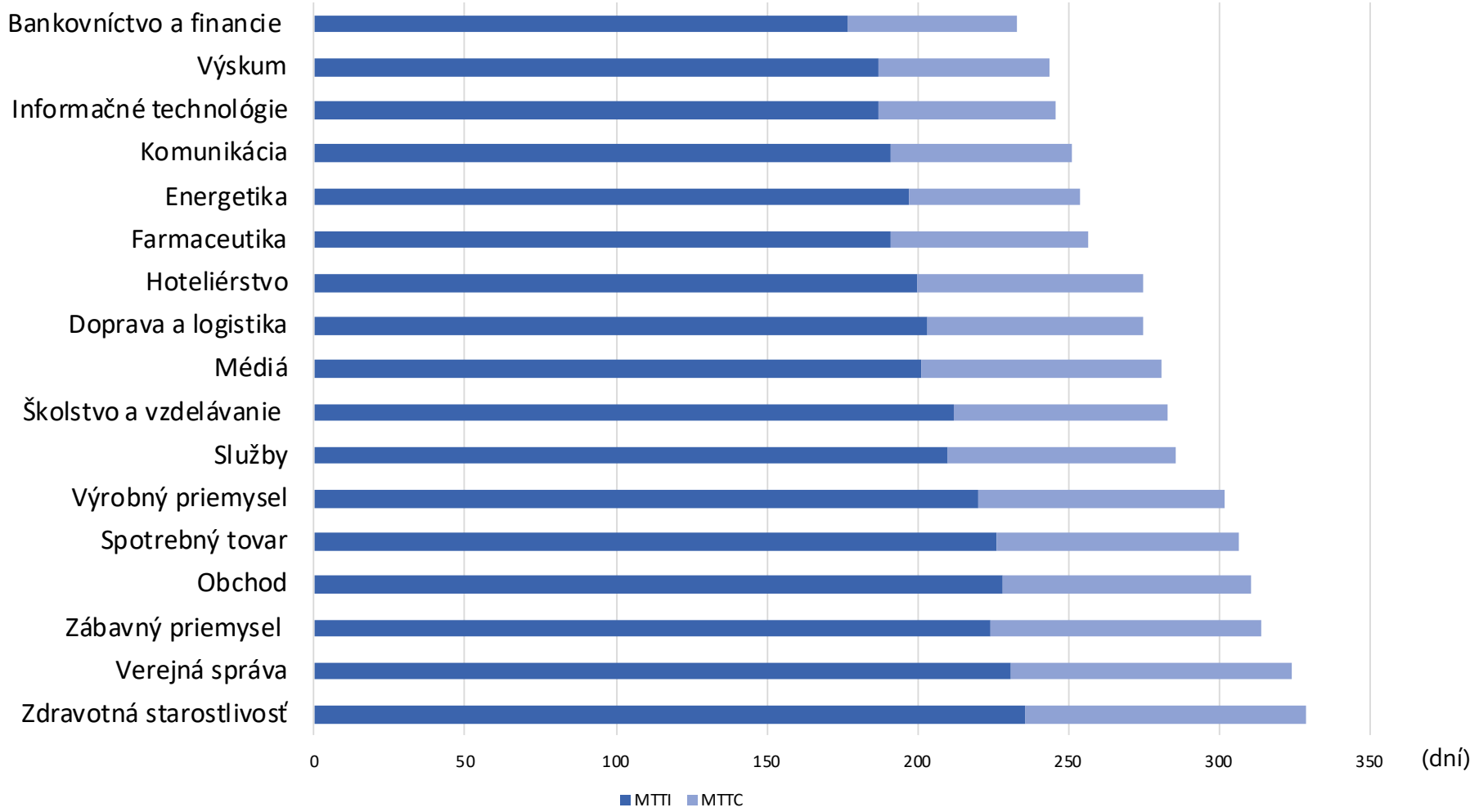
MTTI - Mean Time to Identify, **MTTC -** Mean Time to Correct



Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU PODĽA ODVETVÍ

MTTI - Mean Time to Identify, **MTTC** - Mean Time to Correct



Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

DISTRIBÚCIA KATEGÓRIÍ INCIDENTOV

Malware

Sociálne inžinierstvo (Phishing)

Trójske kone

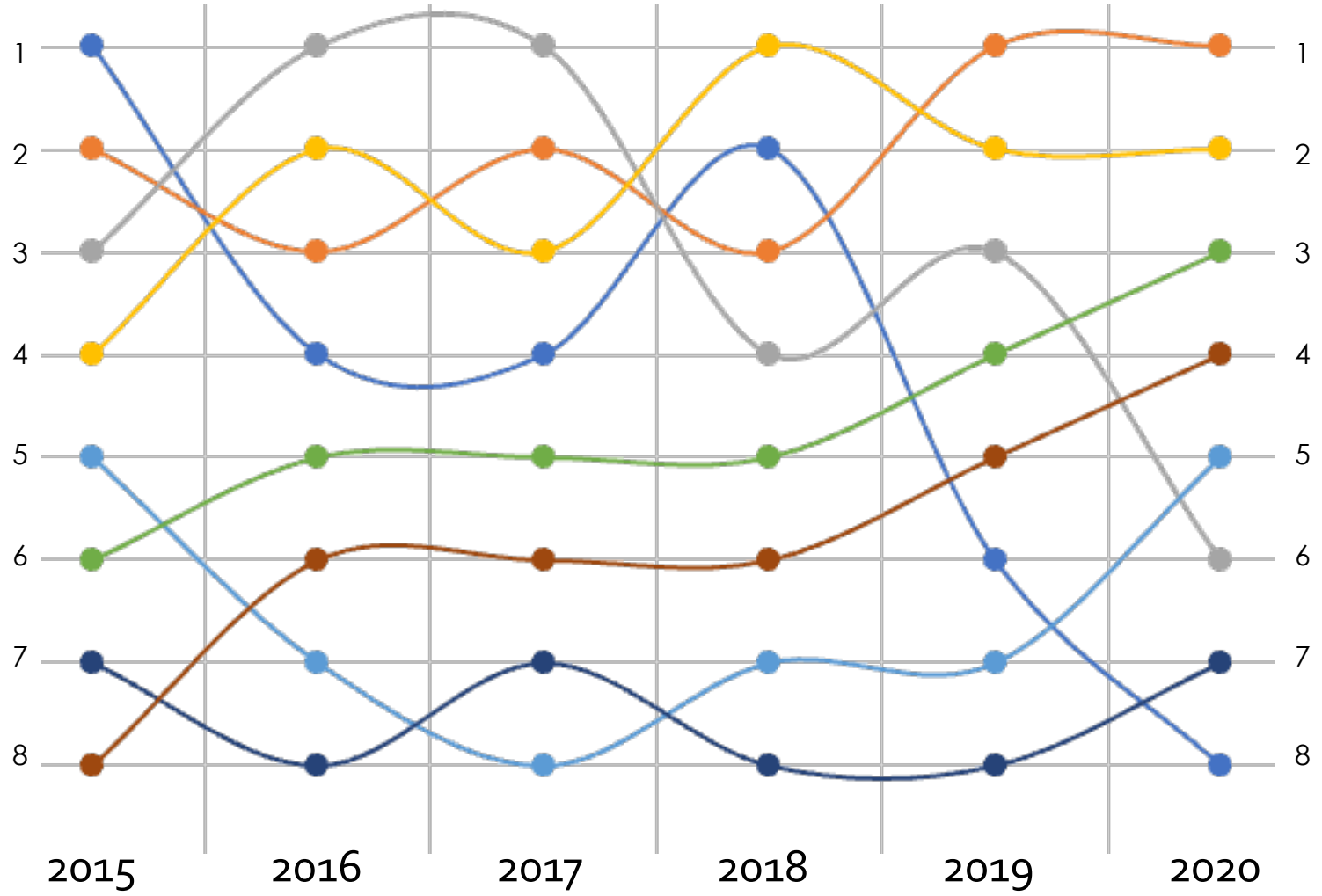
Hacking

Odcudzenie hesiel

Systémové závady

Vydieračský softvér

Ľudské chyby



Sociálne inžinierstvo (Phishing)

Hacking

Ľudské chyby

Systémové závady

Odcudzenie hesiel

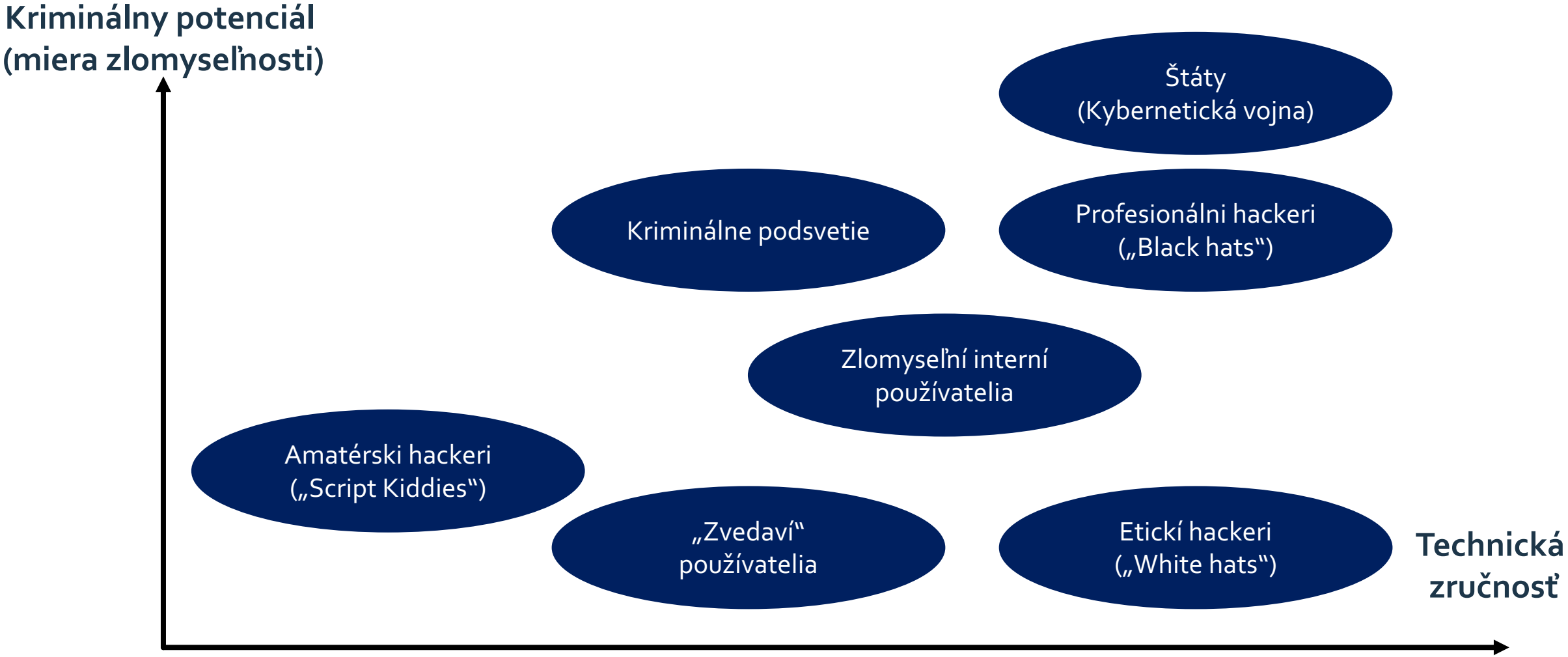
Trójske kone

Vydieračský softvér

Malware

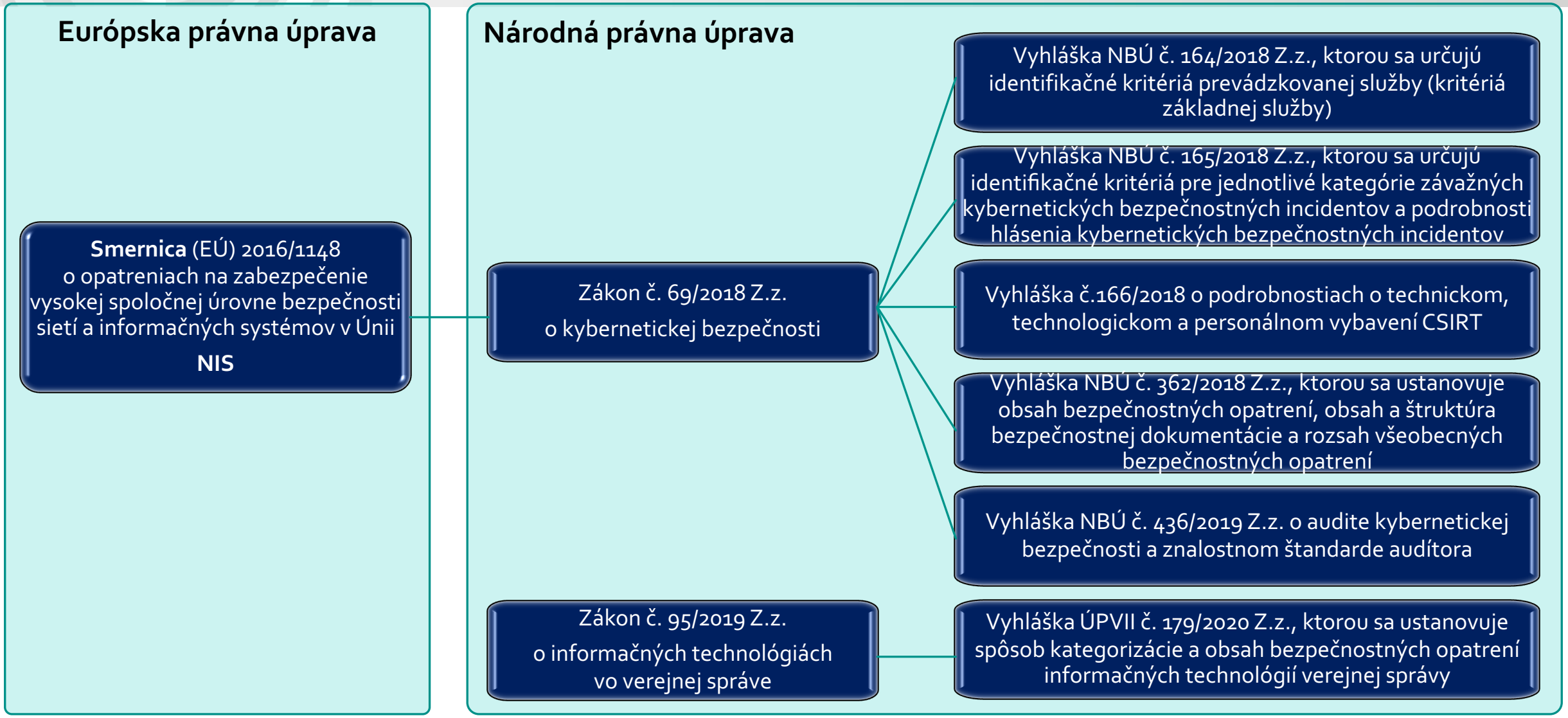
Zdroj: Verizon 2020 Data Breach Investigations Report

PROFILY ÚTOČNÍKOV



Definície kybernetickej bezpečnosti v kontexte obecnej samosprávy

SCHÉMA PRÁVNEJ ÚPRAVY KYBERNETICKEJ BEZPEČNOSTI



KYBERNETICKÝ PRIESTOR

- [§ 3 písm. b) Zákona] **Kybernetický priestor** je globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria:
  - Aktivované prvky kybernetického priestoru,
  - Osoby vykonávajúce aktivity v tomto systéme a
  - Vzťahy a interakcie medzi nimi.

ČO JE TO „ZÁKLADNÁ SLUŽBA“?

Základná služba podľa §3 písm. k) Zákona č. 69/2018 Z.z. je:

- služba, ktorá je zaradená zaradená v zozname základných služieb , závisí od sietí a informačných systémov a
  - je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, ktorá spĺňa identifikačné kritériá základnej služby
  - je informačným systémom verejnej správy, alebo
  - je prvkom kritickej infraštruktúry

IDENTIFIKAČNÉ KRITÉRIÁ ZÁKLADNEJ SLUŽBY

- Identifikačné kritériá sú v zmysle Vyhlášky NBÚ č. 164/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby):
  - Špecifické sektorové kritériá
  - Dopadové kritériá
- Základná služba musí spĺňať:
  - aspoň **jedno špecifické sektorové** a
  - aspoň **jedno dopadové** kritérium

IDENTIFIKÁCIA ZÁKLADNEJ SLUŽBY „ISVS“ PODĽA ZÁKONA č. 69/2018 Z.z.

Z Prílohy č. 1 k vyhláške č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) – sektor **VEREJNÁ SPRÁVA:**

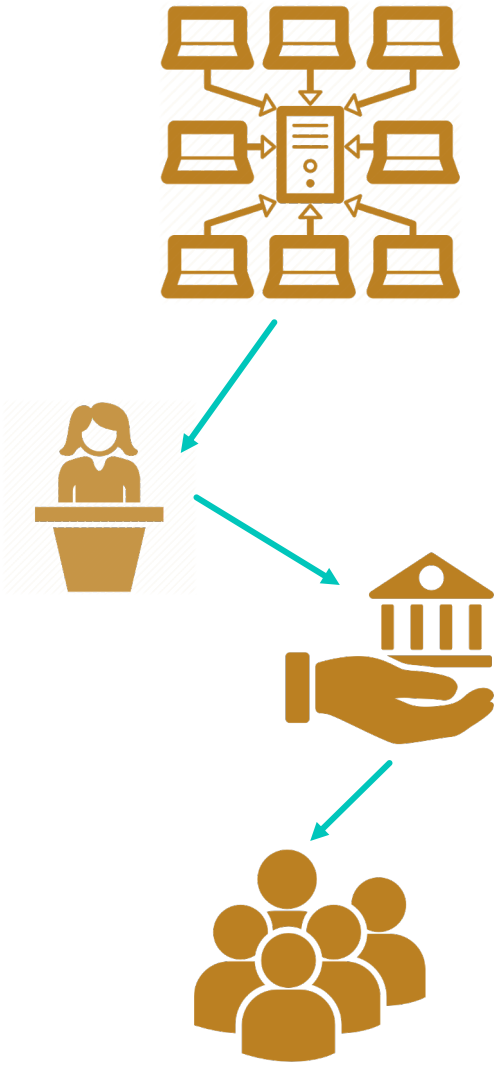
Prevádzkovateľ služieb (príloha č. 1 k zákonu)	**Špecifické sektorové kritériá** (jednotlivo)	**Dopadové kritériá** (jednotlivo) Dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť:
Orgán verejnej moci	Služba, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v jednom podsektore: a) bezpečnosti, **b) informačných systémov verejnej správy,** c) obrany, d) spravodajské služby, alebo e) utajovaných skutočností vo vzťahu k fungovaniu príslušného ústredného orgánu podľa zákona.	Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, **ktoré postihuje viac ako 1 000 osôb.** Obmedzenie či narušenie prevádzky prvku kritickej infraštruktúry. Obmedzenie či narušenie prevádzky siete a informačného systému, ktoré môže mať: • negatívny vplyv na fungovanie orgánu verejnej moci, • vplyv na výkon činnosti orgánu verejnej moci pri zaisťovaní prípravy na krízové situácie, • vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti organu verejnej moci. **Viac ako jedna zranená osoba** vyžadujúca lekárske ošetrenie. Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

PREVÁDZKOVATEĽ PODĽA ZoKB

- Zákon č. 69/2018 Z.z. **o kybernetickej bezpečnosti**:
  - § 3 písm. a): Sieť a informačný systém je elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov
  - § 3 písm. l): Prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k), Zákona (t.j. Základnú službu)

PREVÁDZKOVATEĽ PODĽA ZÁKONA O ITVS

- Zákon č. 95/2019 Z.z. **o informačných technológiách vo verejnej správe**:
  - § 2 ods. 2.: Informačný systém je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov
  - § 2 ods. 5.: Správcom je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona
    - Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby
  - § 2 ods. 6.: Prevádzkovateľom je správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba



JE OBEC PREVÁDZKOVATEĽOM ZÁKLADNEJ SLUŽBY?

Sú splnené všetky kritériá §3 písm. k) Zákona 69/2018:

1. Služba je zaradená v zozname základných služieb 
2. Služba závisí od sietí a informačných systémov 
3. je činnosťou aspoň v jednom sektore alebo podsektore 
4. je informačným systémom verejnej správy, alebo 
5. môže byť prvkom kritickej infraštruktúry (zoznam prvkov je utajovanou skutočnosťou) 

Povinnosti
Prevádzkovateľa základnej služby (PZS)

POVINNOSTI PREVÁDZKOVATEĽA ZÁKLADNEJ SLUŽBY PODĽA § 19 ZÁKONA Č. 69/2018 Z.Z.

(1)	prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.
(2)	ak sú činností vykonávané dodávateľským spôsobom, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona počas celej doby platnosti zmluvy.
(3)	informovať podnik na poskytovanie elektronických komunikačných služieb ku ktorému základná služba pripojená
(4)	informovať v nevyhnutnom rozsahu tretie strany o hlásenom kybernetickom bezpečnostnom incidente
(6a)	riešiť kybernetický bezpečnostný incident,
(6b)	bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
(6c)	spolupracovať s NBÚ a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť
(6d)	v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
(6e)	oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka
(7)	hlásiť zmeny v údajoch podľa § 17 ods. 5 prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

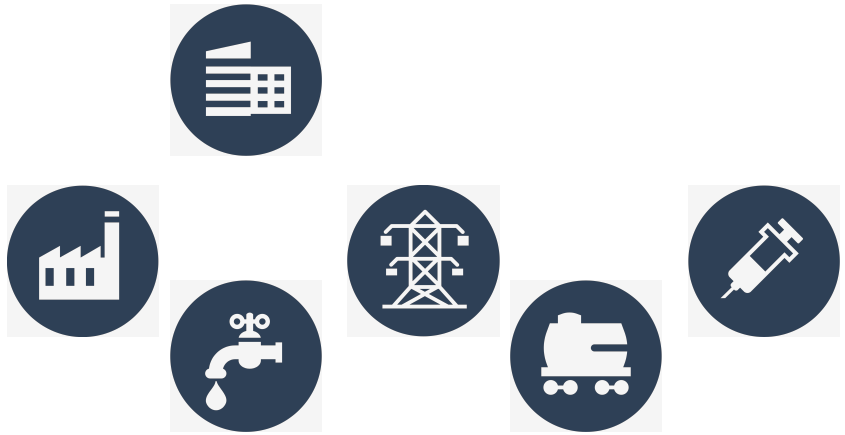
BEZPEČNOSTNÉ OPATRENIA

Opatrenia podľa § 20 (1) Zákona sú:

- **úlohy, procesy, role a technológie** v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

V zmysle § 19 (1) Prevádzkovateľ základnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať:

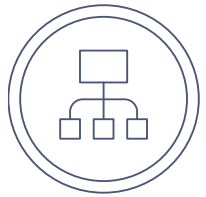
- **všeobecné bezpečnostné opatrenia** najmenej v rozsahu bezpečnostných opatrení podľa §20
- **sektorové bezpečnostné opatrenia**, ak sú prijaté.



GENERICKÉ ROZDELENIE BEZPEČNOSTNÝCH OPATRENÍ

- **Technické opatrenia**
  - Opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy

- **Organizačné opatrenia**
  - Opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie



  - **Personálne opatrenia**
    - Podkategória organizačných opatrení týkajúcich sa riadenia ľudských zdrojov

Efektívnu bezpečnosť je možné dosiahnuť
LEN POMOCOU KOMBINÁCIE
rôznych technických a organizačných opatrení

MINIMÁLNY ROZSAH BEZPEČNOSTNÝCH OPATRENÍ

Podľa §20 (4) Zákona bezpečnostné opatrenia musia zahŕňať najmenej:

a) detekciu kybernetických bezpečnostných incidentov,

b) evidenciu kybernetických bezpečnostných incidentov,

c) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,

d) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,

e) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PODĽA KATEGÓRIE SYSTÉMOV

Bezpečnostné opatrenie podľa § 20 ods. 3 zákona	Kategória I	Kategória II	Kategória III
a) organizácia informačnej bezpečnosti	Odporúčané	Odporúčané	Povinné
b) riadenie aktív, hrozieb a rizík	Odporúčané	Povinné	Povinné
c) personálna bezpečnosť	Odporúčané	Povinné	Povinné
d) riadenie dodávateľských služieb, akvizície, vývoja a údržby IS	Odporúčané	Povinné	Povinné
e) riadenie technických zraniteľností systémov a zariadení	Odporúčané	Povinné	Povinné
f) riadenie bezpečnosti sietí a informačných systémov	Odporúčané	Povinné	Povinné
g) riadenie prevádzky	Odporúčané	Povinné	Povinné
h) riadenie prístupov	Odporúčané	Povinné	Povinné
i) kryptografické opatrenia	Odporúčané	Odporúčané	Povinné
j) riešenie kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
k) monitorovanie, testovanie bezpečnosti a bezpečnostné audity	Odporúčané	Povinné	Povinné
l) fyzickej bezpečnosti a bezpečnosti prostredia	Odporúčané	Odporúčané	Povinné
m) riadenia kontinuity procesov	Odporúčané	Povinné	Povinné

JEDNOTKY CSIRT

Computer security incident response team (CSIRT); **Computer emergency response team** (CERT) = tím reakcie na kybernetické bezpečnostné incidenty

- Bezpečnostný incident je typicky neštandardná udalosť, ktorá môže mať za následok vyvolanie chaotickej reakcie – to následne zvyšuje riziko potenciálnych strát
- Administrátori bez koordinovanej podpory môžu mať nedostatok špecifických informácií pre ochranu informačných aktív
- V prípade, že je detegovaný incident, žiadaná je vhodná eskalačná procedúra (vyhľadanie správnych kontaktných osôb)
- Prvý CSIRT -> CERT Coordination Center (CERT/CC) založený na pôde Software Engineering Institute na Carnegie Mellon University,
  - O registráciu prvého CSIRT sa zaslúžil mediálne mimoriadne úspešný prvý Internetový červ (Morris, 1988)

JEDNOTKY CSIRT ZO ZÁKONA

CSIRT podľa Zákona:

- Akreditované „ex lege“
  - Národná jednotka CSIRT
  - Vládna jednotka CSIRT

- Akreditované po splnení podmienok
  - Jednotky CSIRT „ostatných“ ústredných orgánov

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

CSIRT.SK
WWW.CSIRT.GOV.SK

Požiadavky na informačné technológie verejnej správy

KATEGORIZÁCIA BEZPEČNOSTNÝCH OPATRENÍ PRE ITVS

Vyhláška č. 179/2020 Z.z. ÚPVII ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy:

§ 2 Bezpečnostné opatrenia

1) Bezpečnostné opatrenia informačných technológií verejnej správy tvoria **minimálne bezpečnostné opatrenia troch kategórií** pre jednotlivé oblasti podľa prílohy č. 2
2) Pri duplicite alebo nekompatibilite minimálnych bezpečnostných opatrení rôznych kategórií, ktoré môžu byť aplikované na konkrétne informačné technológie verejnej správy, **majú prednosť ustanovenia upravujúce opatrenia vyššej kategórie**
3) Ak sa aplikuje bezpečnostné opatrenie aj podľa osobitného predpisu, aplikuje sa bezpečnostné opatrenie podľa zákona, **ak jeho cieľom je dosiahnuť vyššiu úroveň bezpečnosti** sietí a informačných systémov ako podľa osobitného predpisu
4) Bezpečnostný projekt informačných systémov verejnej správy sa vypracuje a implementuje podľa prílohy č. 3.

KATEGÓRIE BEZPEČNOSTNÝCH OPATRENÍ V KONTEXTE SAMOSPRÁVY

Vyhláška č. 179/2020 Z.z. ÚPVII ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy:

§ 3 Minimálne bezpečnostné opatrenia

1) Minimálne bezpečnostné opatrenia upravuje príloha č. 2 a sú rozdelené do **Kategórie I**, **Kategórie II** a **Kategórie III** v rámci jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti
2) **Minimálne bezpečnostné opatrenia Kategórie I** jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na:
    a) obec do 6000 obyvateľov,
    b) obec so štatútom mesta do 6000 obyvateľov,
3) **Minimálne bezpečnostné opatrenia Kategórie I a Kategórie II** jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na:
    a) obec nad 6000 obyvateľov,
    b) obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,
    c) mestskú časť s právnou subjektivitou
4) **Minimálne bezpečnostné opatrenia Kategórie I, Kategórie II a Kategórie III** jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na
    a) obec, ktorá je aj krajským mestom,
    b) samosprávny kraj,

APLIKÁCIA POVINNOSTÍ NA SAMOSPRÁVU

Obec, ktorá je aj krajským mestom,

Samosprávny kraj

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I a Kategórie II a a Kategórie III
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec nad 6000 obyvateľov,

Obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,

Mestská časť s právnou subjektivitou

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I a Kategórie II
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec do 6000 obyvateľov,

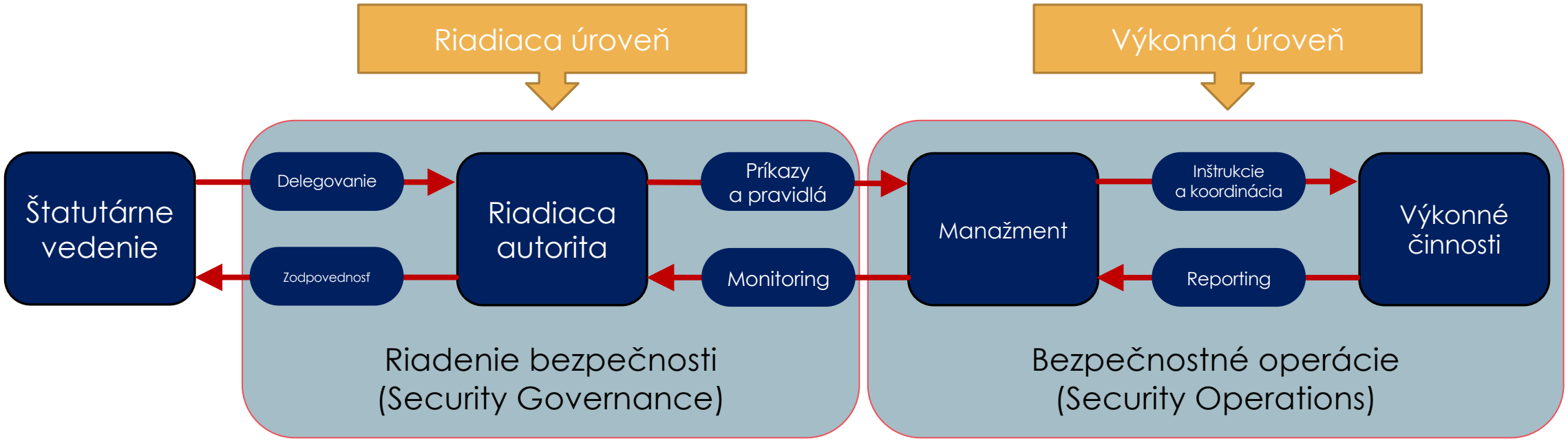
Obec so štatútom mesta do 6000 obyvateľov

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec do 1000 obyvateľov

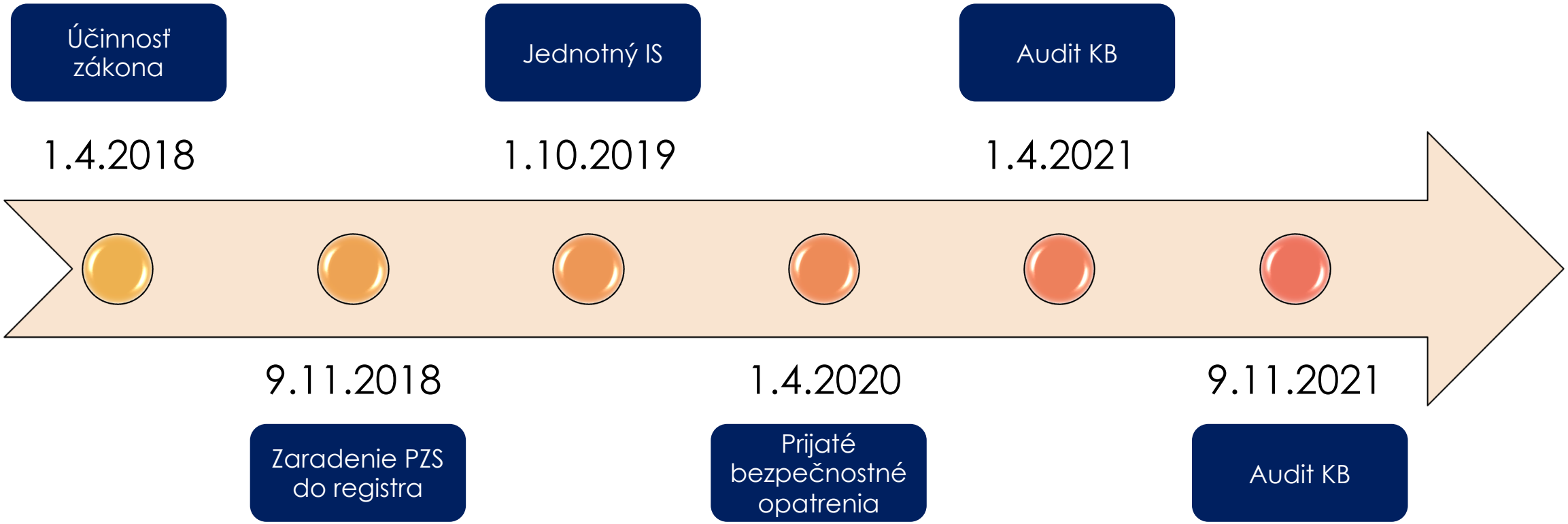
- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I
- alebo implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z. ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti

KĽÚČOVÉ ROLE A VZŤAHY V RIADENÍ A VÝKONE BEZPEČNOSTI



Zdroj: ISACA, isaca.org/cobit5

LEHOTY PODĽA ZÁKONA



KOMPONENTY BEZPEČNOSTNEJ ARCHITEKTÚRY

(Sherwood Applied Business Security Architecture)

	Aktívum (Čo)	Motivácia (Prečo)	Proces (Ako)	Ľudia (Kto)	Umiestnenie (Kde)	Čas (Kedy)
Kontext	Predmet činnosti	Model rizika	Model Procesu	Organizačné usporiadanie	Geografia	Časové závislosti základnej (obchodnej) činnosti
Koncept	Profil činnosti	Bezpečnostné ciele	Bezpečnostná stratégia a architektonické vrstvy	Model bezpečnostných entít a stanovenie dôveryhodného rámca	Model bezpečnostných domén	Termíny a životnosť prvkov súvisiacich s bezpečnosťou
Logické členenie	Model informácií	Bezpečnostné politiky	Služby bezpečnosti	Schéma entít a profily právomocí	Definícia bezpečnostných domén a ich prepojenia	Cyklus bezpečnostných operácií
Fyzické členenie	Dátový model	Bezpečnostné štandardy	Bezpečnostné mechanizmy	Používatelia, aplikácie a používateľské rozhrania	Platformy a sieťová infraštruktúra	Výkon riadiacej štruktúry
Komponenty	Detailné dátové štruktúry	Bezpečnostné procedúry a návody	Bezpečnostné produkty a nástroje	Identity, funkcie, role, ACL	Procesy, uzly, adresy, protokoly	Časovanie a postupnosť aktivít
Prevádzka	Zaistenie kontinuity činností	Riadenie operačného rizika	Riadenie a podpora služieb bezpečnosti	Riadenie a podpora používateľov a aplikácií	Bezpečnosť objektov, sietí a platforiem	Rozvrh výkonu bezpečnostných operácií

Ochrana vlastníckych práv

Vlastnícke práva tretích strán

Limity informácií