Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

REGULÁCIA A RIADENIE BEZPEČNOSTI

FEI TUKE, 6.12.2023

Ivan Makatura

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií
- **Certifikácia:**
  - audítorov a manažérov kybernetickej bezpečnosti
  - produktov v kybernetickej bezpečnosti podľa Nariadenia EÚ č. 2019/881
- **Vzdelávanie dospelých** v kybernetickej bezpečnosti
- Organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
- Publikačná činnosť
- **Audit kybernetickej bezpečnosti** podľa zákona č. 69/2018 Z. z.
- Konzultačné služby v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
- Znalecká a expertízna činnosť podľa zákona č. 382/2004 Z. z. o znalcoch

OBSAH PREDNÁŠKY

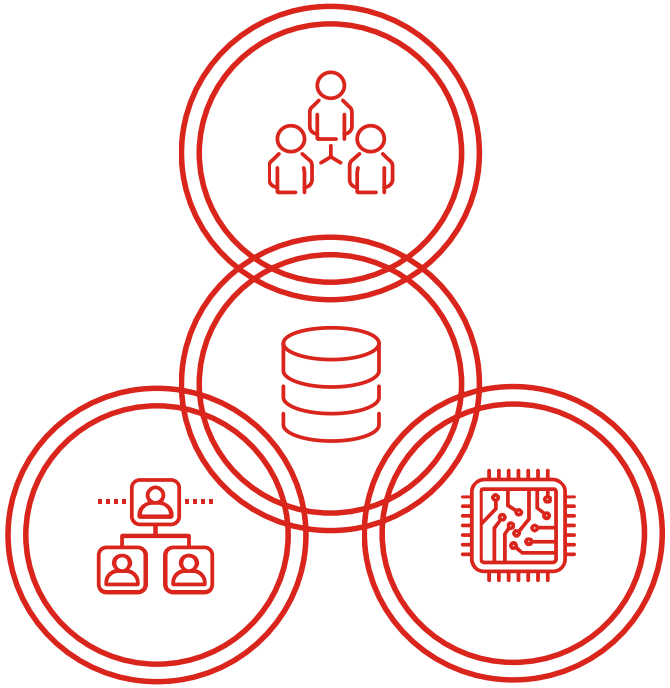
- Podstata kybernetickej bezpečnosti
- Európska a národná právna úprava v kybernetickej bezpečnosti
- Technická normalizácia v kybernetickej bezpečnosti a ochrane údajov
- Povinnosti subjektov v kontexte ochrany informačných aktív
- Organizačné štruktúry riadenia bezpečnosti
- Pracovné roly v kybernetickej bezpečnosti a obsah ich znalostných štandardov
- Princípy security governance

PREČO EXISTUJE KYBERNETICKÁ BEZPEČNOSŤ?

REGULÁCIA A RIADENIE BEZPEČNOSTI

KYBERNETICKÝ PRIESTOR

- **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

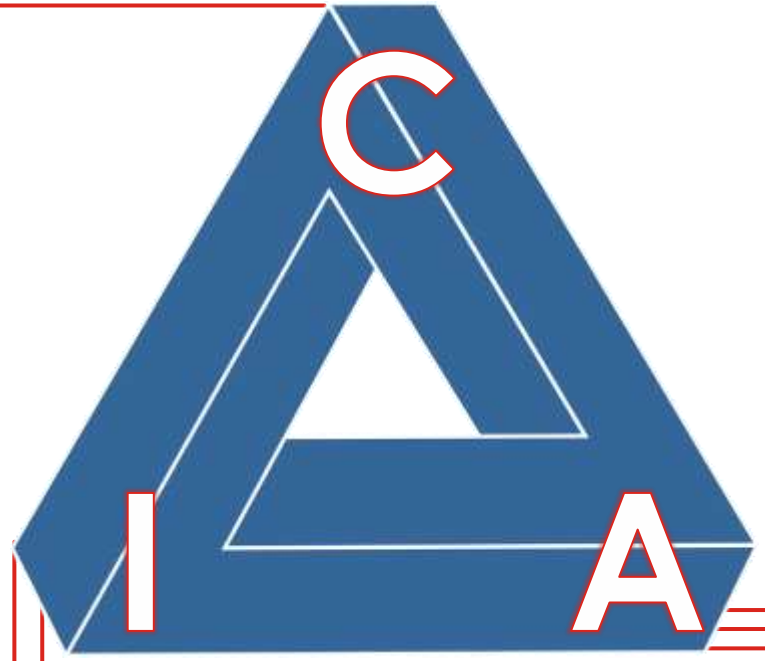


PEOPLE – PROCESS - TECHNOLOGY – (DATA)

ATRIBÚTY BEZPEČNOSTI (SPOĽAHLIVOSTI) INFORMÁCIÍ

Confidentiality (Dôvernosť):

- Záruka, že údaje alebo informácie nie sú prezradené neoprávneným subjektom alebo procesom



Availability (Dostupnosť)

- Záruka, že údaje alebo informácie sú pre používateľa, informačný systém, sieť, zariadenie alebo proces prístupné, keď sú potrebné a požadované

Integrity (Celistvosť)

- Záruka, že bezchybnosť, úplnosť alebo správnosť údajov alebo informácií neboli narušené

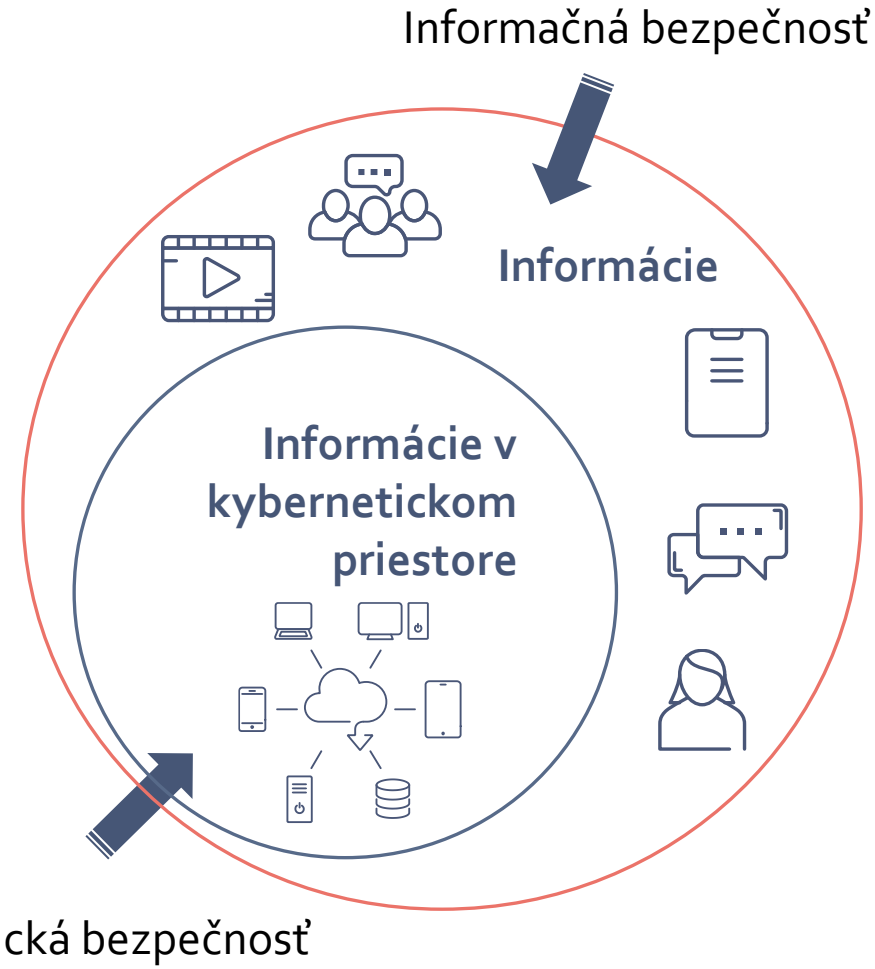
INFORMAČNÁ VS. KYBERNETICKÁ BEZPEČNOSŤ

[ISO/IEC 27032, čl. 2.33]

- Informačná bezpečnosť je zachovanie dôvernosti, integrity a dostupnosti informácií

[ISO/IEC 27032, čl. 4.20]

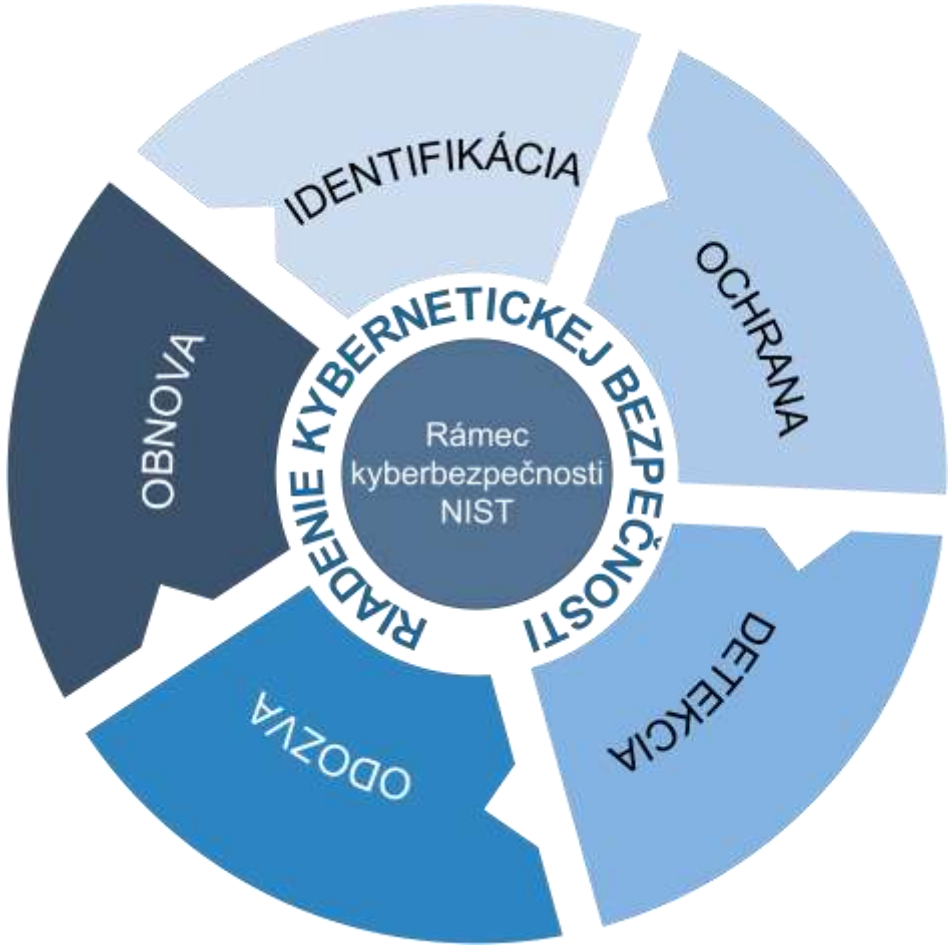
- Kybernetická bezpečnosť je zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore



CIELE BEZPEČNOSTI PODĽA NIST 800-171
NORMATÍVNY (NELEGISLATÍVNY) RÁMEC

ČO

NIST CYBERSECURITY FRAMEWORK



- **IDENTIFIKÁCIA**
  - Riadenie aktív, Identifikácia zraniteľností, Riadenie rizík
- **OCHRANA**
  - Riadenie prístupov a práv, Vzdelávanie a zvyšovanie povedomia, Implementácia preventívnych opatrení
- **DETEKCIA**
  - Monitoring udalostí, Eskalačné procedúry
- **ODOZVA**
  - Riešenie incidentov, Mitigácia, Reporting, Forenzná analýza,
- **OBNOVA**
  - Plánovanie obnovy, Plánovanie kontinuity, Zlepšovanie odolnosti

Zdroj: https://csrc.nist.gov/pubs/sp/800/171/r3/final

TYPICKÉ OBJEKTÍVNE DÔVODY PRE RIADENIE BEZPEČNOSTNÉHO RIZIKA

PREČO

OCHRANA DUŠEVNÉHO VLASTNÍCTVA 48%

OBAVA Z VÝPADKU PRODUKCIE 61%

OCHRANA REPUTÁCIE 21%

POŽIADAVKY NA SÚLAD 63%

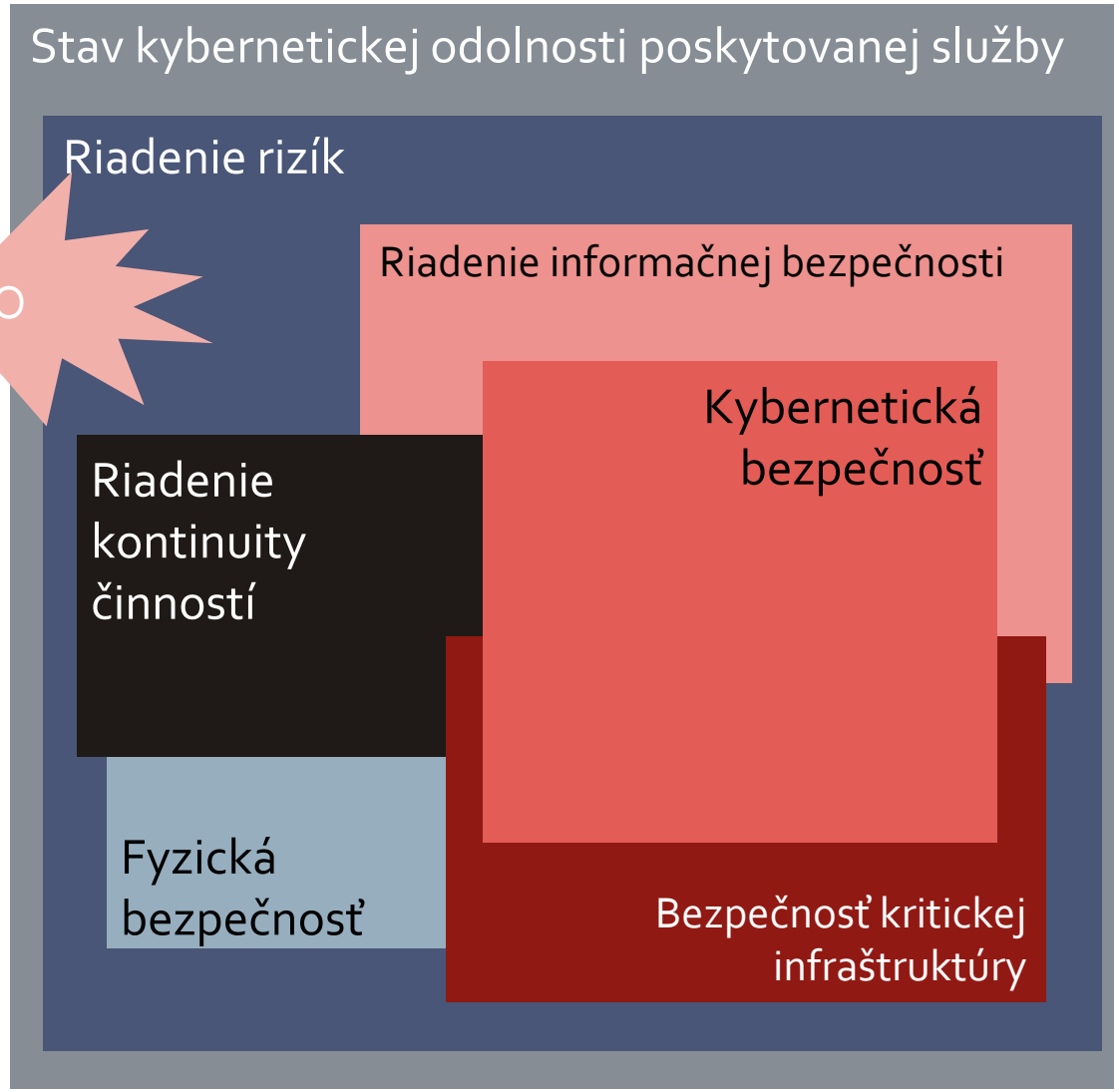
KRITICKÁ INFRAŠTFUKTÚRA 11%

Zdroj: Ponemon's 2016 Application Security Risk Study

CIELE BEZPEČNOSTI VS. DOBRÁ PRAX V KB

ČO

AKO



Organizácia	Technologické prostredie
Ochrana údajov	Klasifikácia informácií
Riadenie IT rizík	Manažment zraniteľností
Havarijné plánovanie	Security Governance
IT architektúra	Riadenie aktív
Riadenie prístupov	Riadenie zmien a konfigurácií
Riešenie incidentov	Service Level Management
Vzťahy a komunikácia	Biznis architektúra
Ekosystém partnerov	Vzdelávanie a povedomie

RIEŠENIE INCIDENTOV

REGULÁCIA A RIADENIE BEZPEČNOSTI

PROCES ODOZVY NA INCIDENT (INCIDENT RESPONSE)

Je proces:

- Preddefinovanej
- Formalizovanej
- Otestovanej

} **reakcie** na bezpečnostný incident

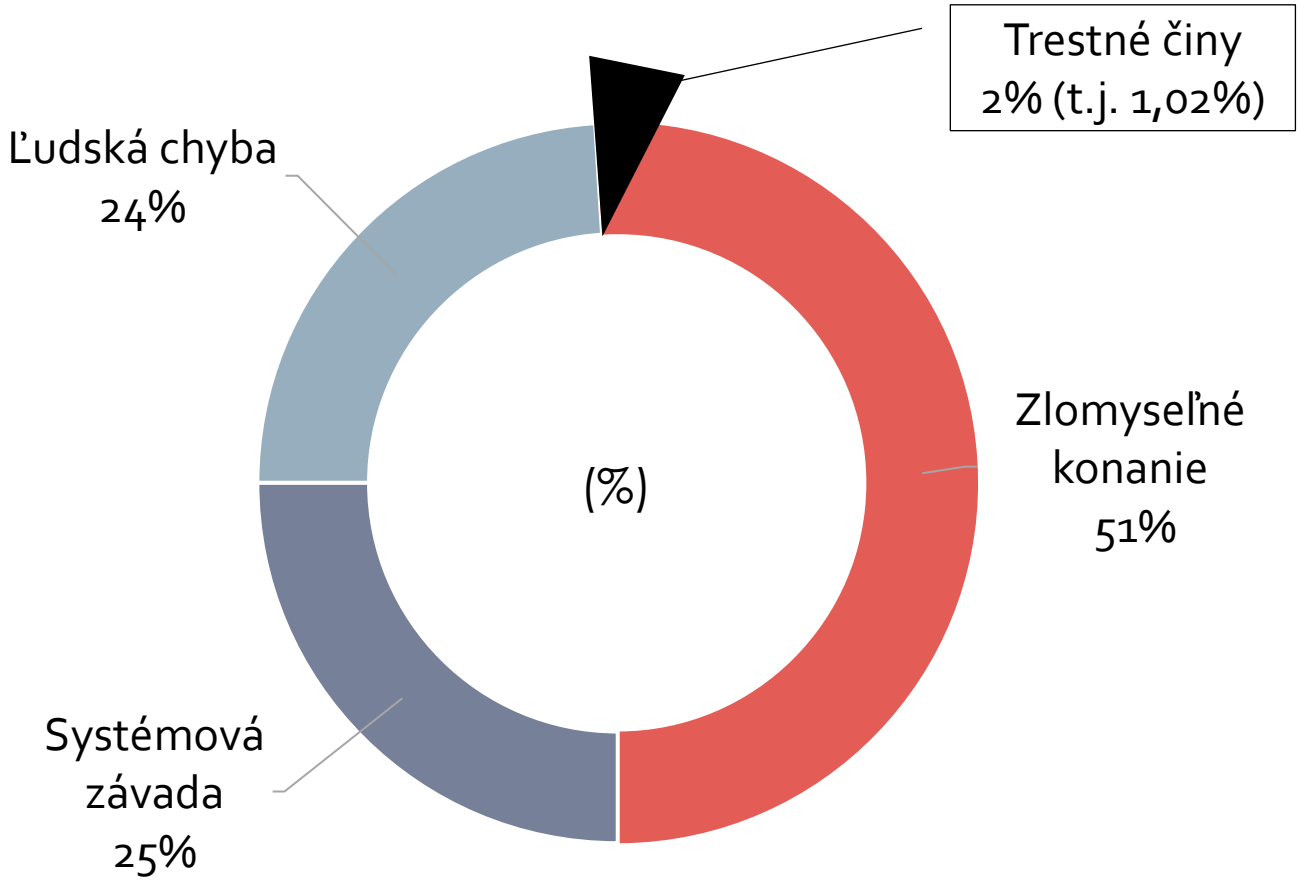
V aktivitách odozvy na incident by mali byť obsiahnuté dva základné ciele:

- **„Opraviť a pokračovať"**
  - Obnovenie funkčnosti poškodených informačných aktív a pokračovanie v činnosti.

- **„Vyšetriť a vyriešiť"**
  - Zákonná náprava a zhromaždenie digitálnych stôp na podporu postupu proti vinníkovi.

INCIDENTY NIE SÚ LEN ÚTOKY

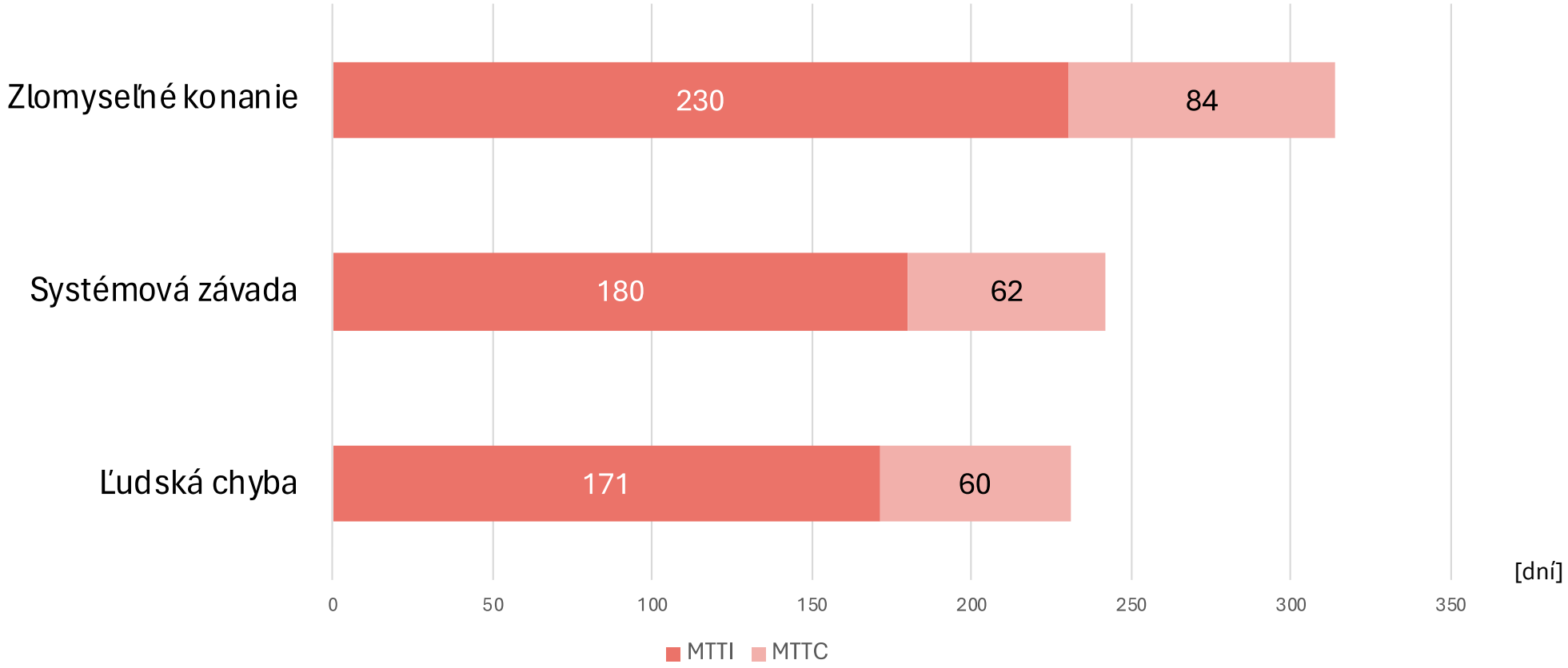
- Spôsob riešenia incidentu sa podstatne líši podľa kategórie incidentu
- Zlý úmysel môže mať aj insider - útoky zvnútra zvyčajne prevažujú
- Bolo by chybou myslieť si, že hrozby pochádzajú výhradne od hackerov
- Iba zlomok s incidentov spôsobených zlomyseľným konaním (t.j. útokov) má trestné pokračovanie



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

KOĽKO TRVÁ BEŽNÝ INCIDENT?

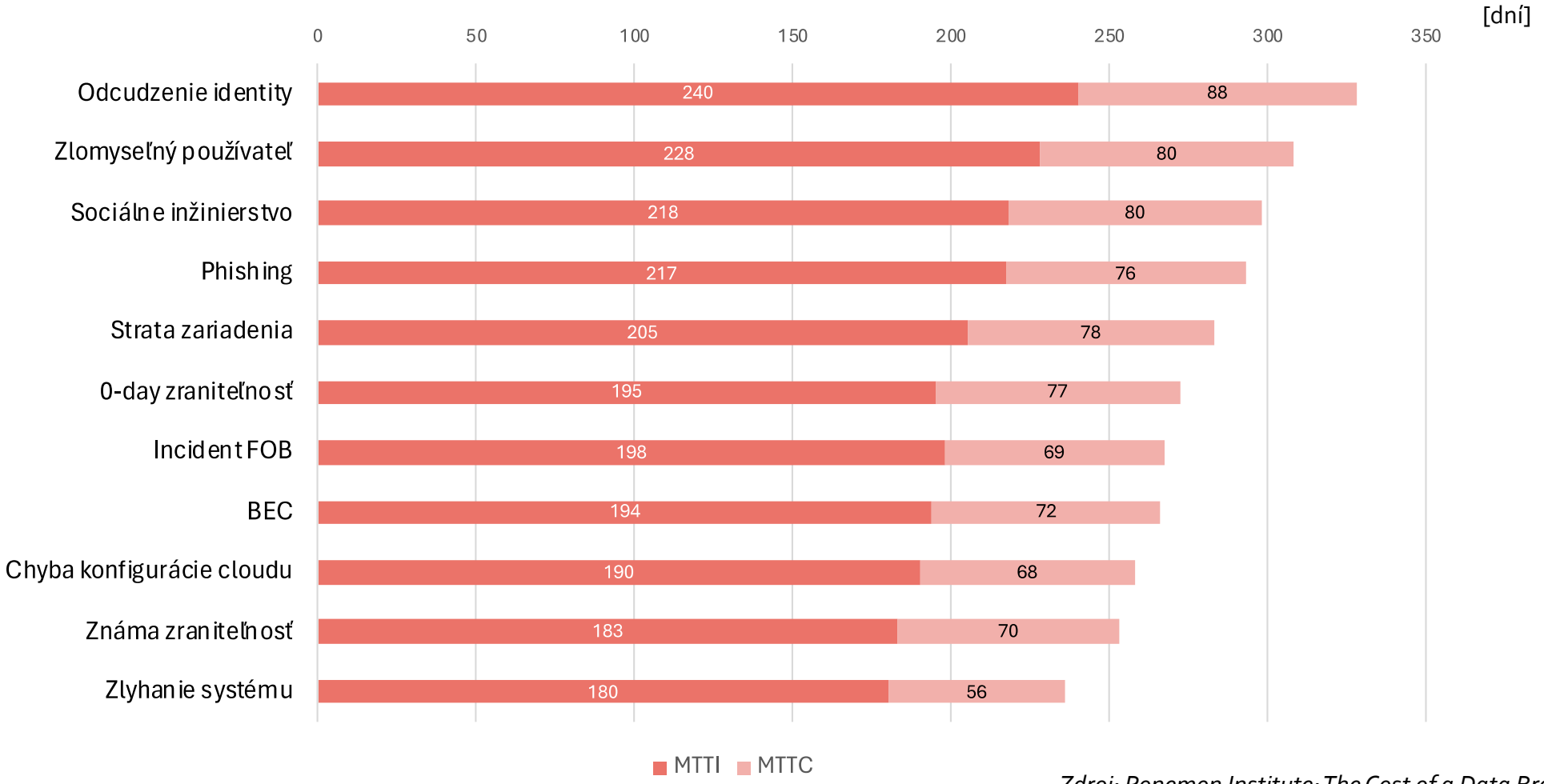
MTTI - Priemerný čas identifikácie, **MTTC -** Priemerný čas obmedzenia



Zdroj: Ponemon Institute: The Cost of a Data Breach Report 2023

STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU PODĽA TYPU

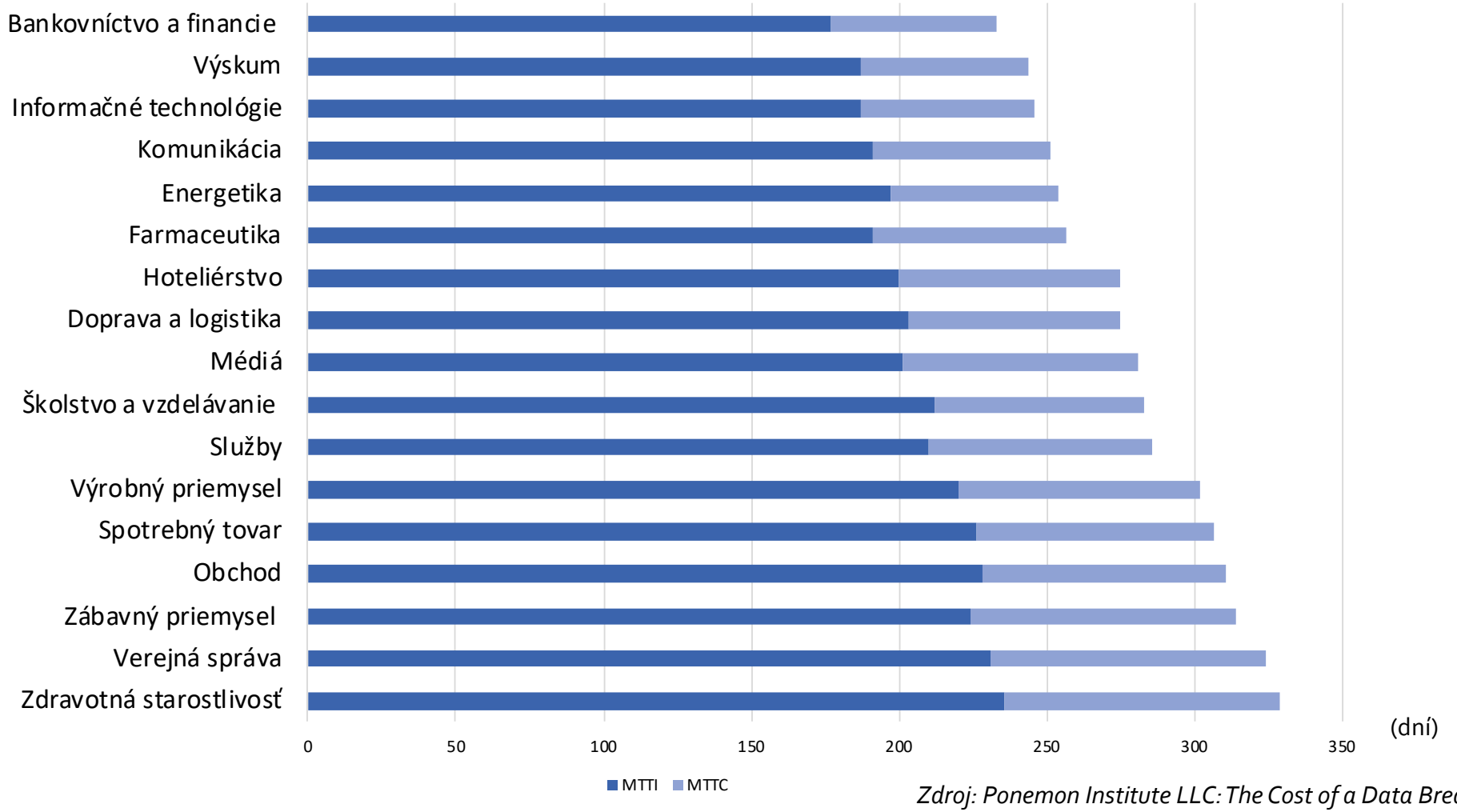
MTTI - Priemerný čas identifikácie, **MTTC -** Priemerný čas obmedzenia



Zdroj: Ponemon Institute: The Cost of a Data Breach Report 2023

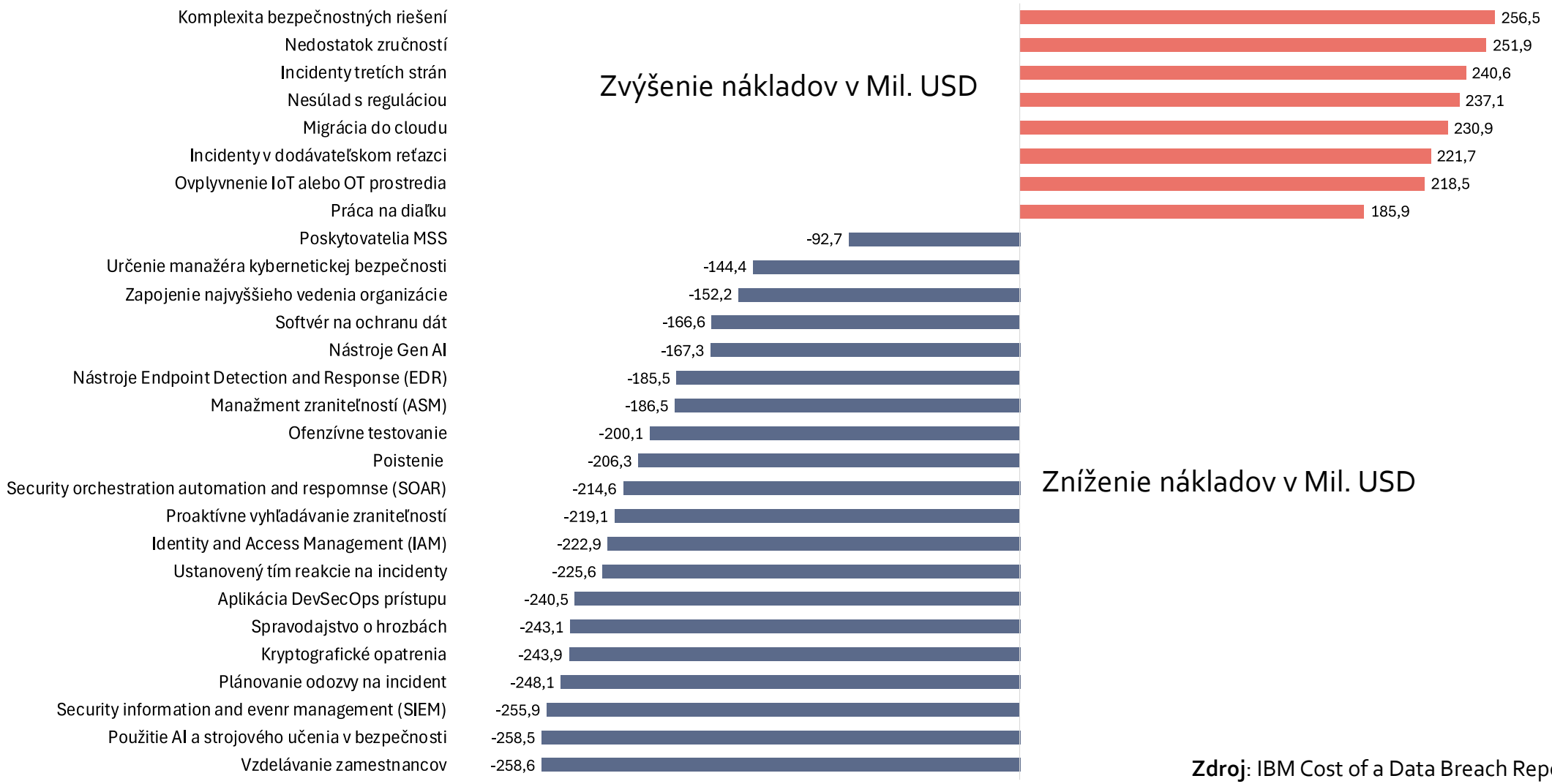
STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU PODĽA ODVETVÍ

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



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

FAKTORY OVPLYVŇUJÚCE NÁKLADY SÚVISIACE S INCIDENTOM
(Odchýlka od celosvetového priemeru - údaje normalizované na incident)



Zdroj: IBM Cost of a Data Breach Report 2024

EURÓPSKE A NÁRODNÉ PRÁVNE PREDPISY V KYBERNETICKEJ BEZPEČNOSTI

REGULÁCIA A RIADENIE BEZPEČNOSTI

PRAMENE PRÁVA A REGULÁCIA

- Zmysel zákonov (**PRAMEŇ PRÁVA**) - faktory, ktoré vyvolávajú potrebu ich prijatia
- Materiálne pramene práva:
  - ekonomické, sociálne, technologické, politické, geografické, mravné, ekologické, a mnohé iné...
  - Prameňom práva v kybernetickej bezpečnosti je **dosiahnutie stavu, kedy sú primerane ošetrené známe riziká vyplývajúce z hrozieb** pôsobiacich na informačné aktíva spoločnosti
- Regulácia sa vykonáva prostredníctvom normatívnych právnych aktov, t.j. **všeobecne záväzných právnych prepisov**
- Pravidlá a ich vynucovanie reguláciou majú za cieľ **dosiahnuť žiaduce správanie zúčastnených subjektov**
- O právach a povinnostiach dozorovaných subjektov je oprávnená rozhodovať **štátna moc**

[1] Prusák, J. Teória práva. 2. vyd. Bratislava : Vydavateľské oddelenie PF UK, 2001. 188 s. ISBN 80 – 7160 – 146 – 2

LAISSEZ-FAIRE

- Francúzska fráza, ktorá znamená „**nech sa stane** “ alebo „**nechať veci tak**“
- Doktrína, ktorá sa používa na označenie prístupu k politike bez pomoci štátu
- Laissez-faire presadzuje odolávanie vládnym zásahom pri stanovovaní politík prostredníctvom zákonov, nariadení, dotácií, ciel, daní a iných obmedzení
- Laissez-faire podporuje kapitalizmus a filozofiu voľného obchodu a slobodného správania **bez obmedzovania práv iných ľudí**

MÔŽE REGULÁCIA POMÔCŤ KYBERNETICKEJ BEZPEČNOSTI?

Cieľ regulácie:

- dosiahnutie primeranej úrovne kybernetickej bezpečnosti, ochrany informácií, ochrany údajov a ochrany súkromia

Čiastkové úlohy:

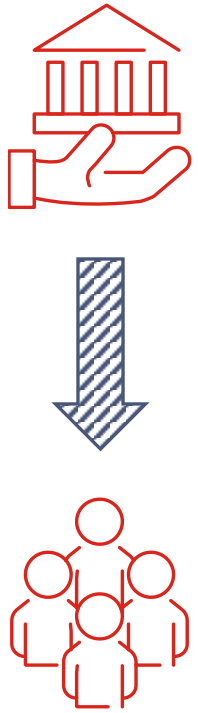
- návrh jednotných metód ochrany informácií
- návrhy na zlepšenie procesov riadenia hrozieb a rizík
- vynútenie aktivít zameraných na dosiahnutie dostatočnej úrovne ochrany dát a informácií
- tlak na dosiahnutie stavu odolnosti voči zraniteľnostiam

Nástroj dosiahnutia:

- Všeobecne záväzné právne prepisy, ktoré:
  - efektívne stanovia pravidlá a
  - dosiahnu žiaduce správanie zúčastnených subjektov

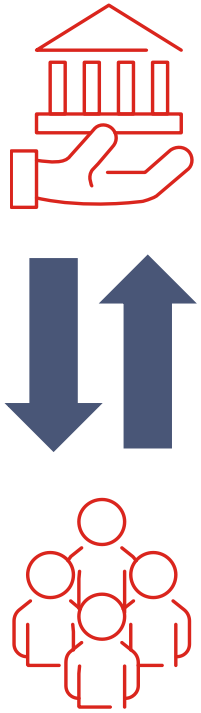
MIERA REGULÁCIE

Laissez-faire



Konajte slobodne,
bez porušenia práv tretích strán

Demokratická

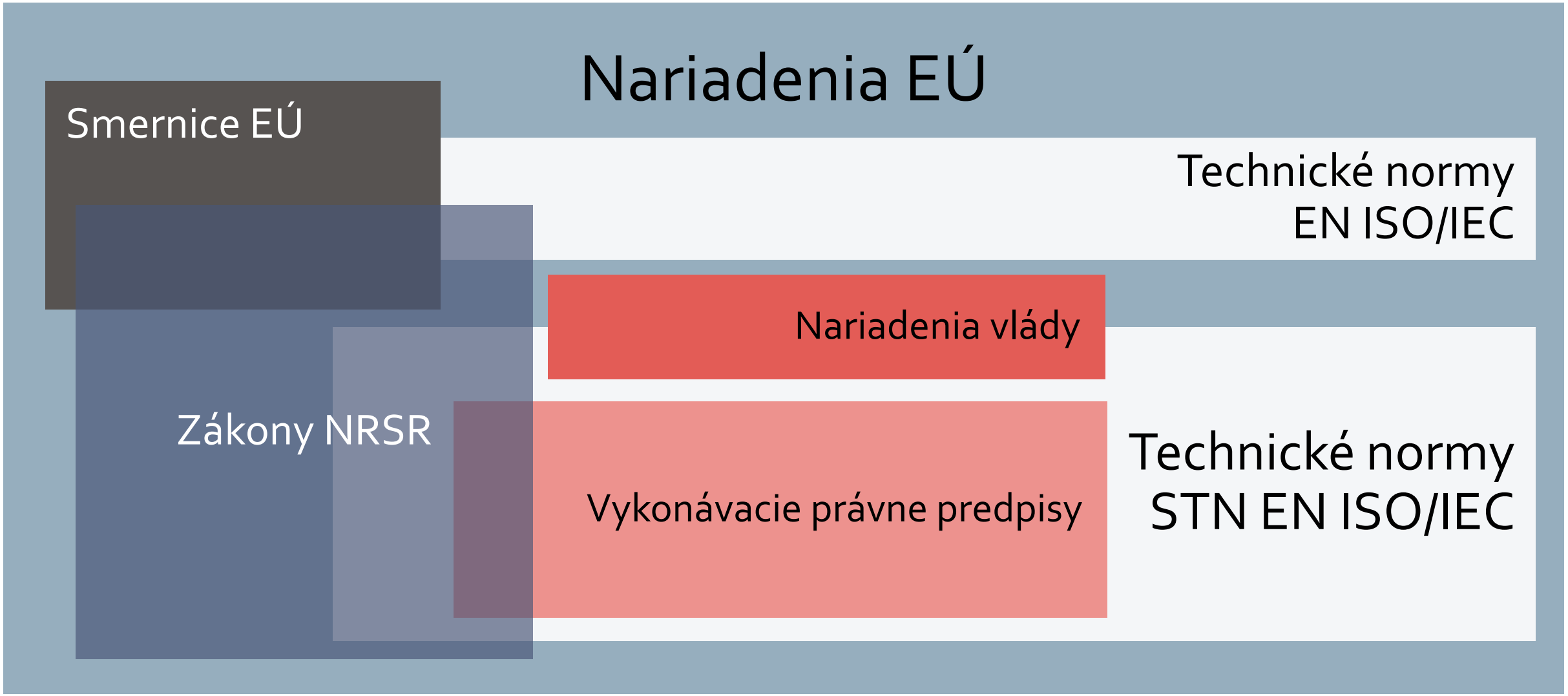


Dohodnime sa všeobecne,
ako by sme mali konať

Autokratická

Konajte tak, ako vám je nariadené

HIERARCHIA PRÁVNYCH A TECHNICKÝCH PREDPISOV



PRÁVNA ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI

Európska právna úprava

Smernica (EÚ) 2022/2555
o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

NIS2

Nariadenie (EÚ) 2019/881
o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií

Cyber Security Act (CSA)

Nariadenie (EÚ) 2019/765
ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh

Návrh nariadenia (EÚ)
o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami

Cyber Resilience Act (CRA)

Národná právna úprava

Zákon č. 69/2018 Z.z.
o kybernetickej bezpečnosti

PRÁVNE PREDPISY SR S DOSAHOM NA IB/KB

Zákon č. 483/2001 Z. z.
o bankách

Zákon č. 69/2018 Z.z.
o kybernetickej bezpečnosti

Zákon č. 452/2021 Z. z.
o elektronických komunikáciách

Zákon č. 18/2018 Z.z.
o ochrane osobných údajov

Zákon č. 95/2019 Z.z.
o informačných technológiách
vo verejnej správe

PLATNÉ PRÁVNE AKTY EÚ S DOSAHOM NA IB/KB

Smernica (EÚ) 2002/58/ES
týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií
ePD

Nariadenie (EÚ) 910/2014
o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
eIDAS

Smernica (EÚ) 2015/2366
o platobných službách na vnútornom trhu
PSD2

Nariadenie (EÚ) 2016/679
o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
GDPR

Nariadenie (EÚ) 2019/881
o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií
Cyber Security Act (CSA)

Nariadenie (EÚ) 2022/1925
o súťažeschopných a spravodlivých trhoch digitálneho sektory (akt o digitálnych trhoch)
DMA

Nariadenie (EÚ) 2022/2065
o jednotnom trhu s digitálnymi službami (akt o digitálnych službách)
DSA

Nariadenie (EÚ) 2022/2554
o digitálnej prevádzkovej odolnosti finančného sektora
DORA

Smernica (EÚ) 2022/2555
o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
NIS2

Nariadenie (EÚ) 2023/2841
o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie
EUIBAs

Nariadenie (EÚ) 2024/1689
o umelej inteligencii
AI Act

Nariadenie (EÚ) 2024/1183
o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
eIDAS2

PRIPRAVOVANÉ PRÁVNE AKTY EÚ S DOSAHOM NA IB/KB

Nariadenie (EÚ)
o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami

Cyber Resilience Act (CRA)

Nariadenie (EÚ)
o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií

Cyber Security Act (CSA+)

Nariadenie (EÚ)
o opatreniach na posilnenie solidarity a vytvorenie kapacít na odhaľovanie a reakciu na hrozby a incidenty

CySol Act

Commission work programme 2024: COM_2023_638_1_annexes_EN.pdf

PREDMET ZÁKONA č. 69/2018 Z.Z.

- Orgány verejnej moci pri výkone pôsobnosti v oblasti KB
- Národná stratégia KB
- Jednotný informačný systém kybernetickej bezpečnosti
- Organizácia a pôsobnosť jednotiek CSIRT
- Postavenie a povinnosti PZS a PDS
- Bezpečnostné opatrenia
- Systém zabezpečenia KB (identifikácia ZS, hlásenie a riešenie KBI)

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

TECHNICKÁ NORMALIZÁCIA V KYBERNETICKEJ BEZPEČNOSTI A OCHRANE ÚDAJOV

REGULÁCIA A RIADENIE BEZPEČNOSTI

TECHNICKÁ NORMALIZÁCIA

Význam technickej normalizácie:

- Nie je potrebné definovať, čo už je známe a overené najlepšou praxou
- Prostredníctvom štandardov je možné zaručiť kompatibilitu metód ochrany informačných aktív

Základné delenie ISO noriem, resp. ISO/IEC noriem v oblasti IB/KB:

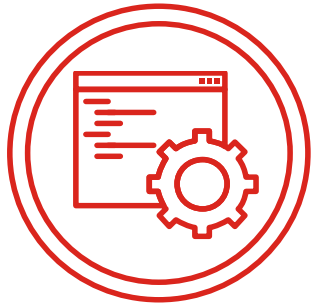
- Systém manažérstva informačnej bezpečnosti (ISMS)
- Kryptológia
- Posudzovanie a certifikácia bezpečnosti
- Bezpečnostné opatrenia
- Identifikácia a autentizácia

Trieda noriem ISO/IEC 27000 je vyhradená pre riadenie informačnej bezpečnosti

Popis ucelenej triedy noriem 27000 je uvedený napríklad na adrese: www.iso27001security.com

SYSTÉMY MANAŽÉRSTVA RELEVANTNÉ PRE IB/KB

- **Systém manažérstva** je súbor politík, procesov a postupov používaných organizáciou na zabezpečenie zlepšovania výkonnosti, stanovením opakovateľných krokov, ktoré organizácia vedome implementuje na dosiahnutie svojich cieľov a zámerov
- Typické manažérske systémy v oblasti kybernetickej bezpečnosti:
  - **Systém riadenia IT služieb** (ITSM), podľa noriem radu ISO/IEC 20 000
  - **Systém riadenia informačnej bezpečnosti** (ISMS) podľa noriem radu ISO/IEC 27 000
  - **Riadenie kontinuity činností** (BCM) podľa normy ISO/IEC 22 301
  - **Riadenie kvality** (QM) podľa normy ISO 9001



PRÁVNE PREDPISY INŠPIROVANÉ TECHNICKÝMI NORMAMI 1/2

- **V čom právne predpisy môžu súvisieť s technickými normami?**
  - Ucelená štruktúra bezpečnostných cieľov
  - Komplexný návrh bezpečnostných opatrení
  - Ustálený proces riadenia rizík
  - Metódy posudzovania a auditu informačnej bezpečnosti
  - Uznávaný systém manažérstva
  - Holistický prístup ku riadeniu procesov

PRÁVNE PREDPISY INŠPIROVANÉ TECHNICKÝMI NORMAMI 2/2

Príklady noriem premietnutých v právnych predpisoch:

- **ISO/IEC 27002** Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia - Riadenie informačnej bezpečnosti
  - Vyhláška NBÚ č. 362/2018 Z.z. o bezpečnostných opatreniach
  - Vyhláška ÚPVII č. 179/2020 Z.z o bezpečnostných opatreniach
  - NIS, NIS2, DORA
- **ISO/IEC 27008** Informačné technológie - Bezpečnostné metódy - Návod na posudzovanie opatrení informačnej bezpečnosti
  - Vyhláška NBÚ č. 493/2022 Z. z. o audite KB
- **ISO/IEC 27701** Bezpečnostné metódy - Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 o riadenie bezpečnosti osobných údajov - Požiadavky a usmernenia
  - GDPR
- **ISO/IEC 27005** Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia -Usmernenie k riadeniu rizík informačnej bezpečnosti
  - GDPR, NIS
- **ISO/IEC 17065** Posudzovanie zhody. Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb
  - GDPR, CSA, CRA

NORMY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

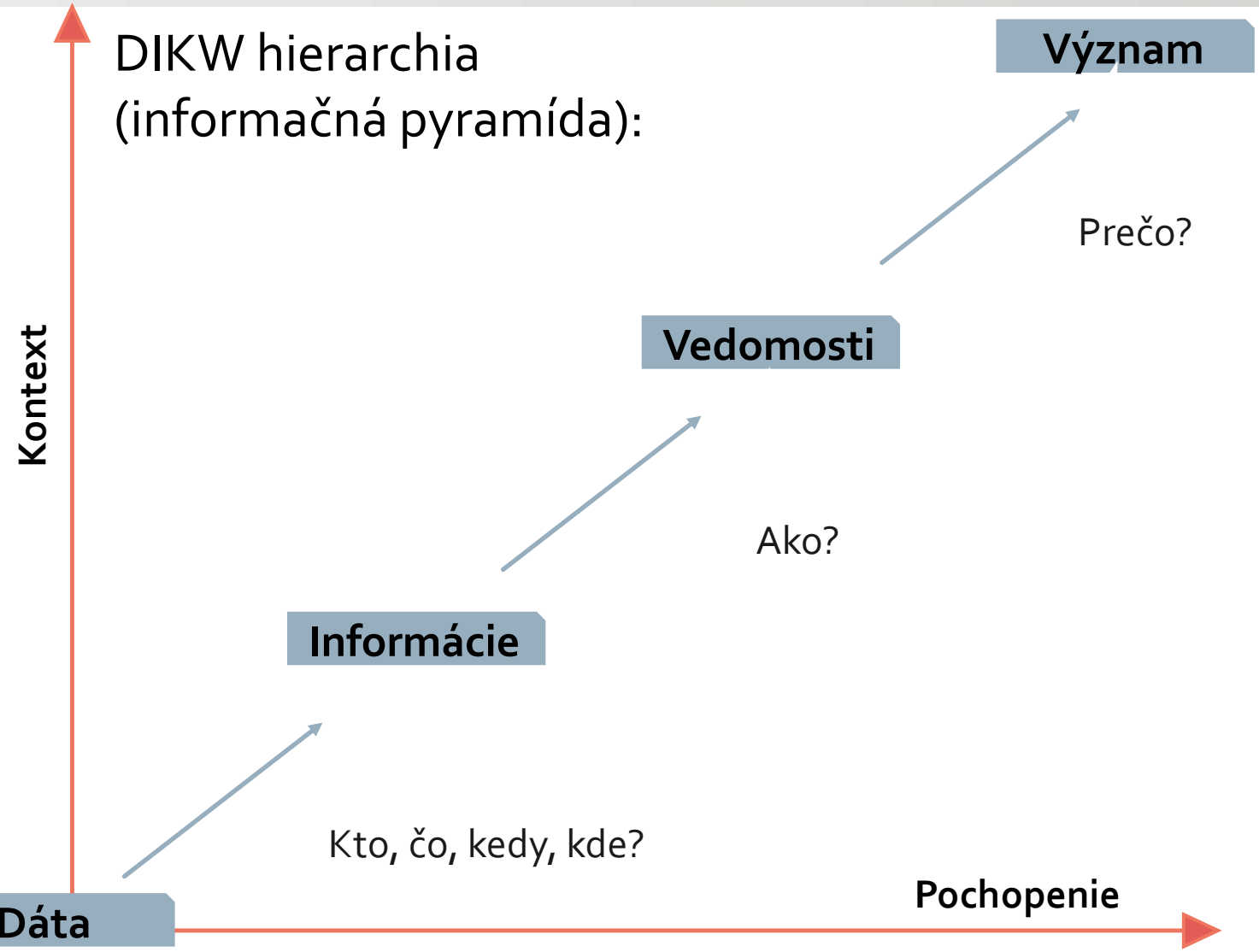
- Národný ústav technickej normalizácie ústav v pôsobnosti Ministerstva obchodu USA
- Vydáva aj niektoré štandardy „Special Publication" týkajúce sa bezpečnosti informácií:
  - NIST SP 800-30, Risk Management Guide for IT Systems
  - NIST SP 800-39, Managing Risk from Information Systems
  - NIST SP 800-14, Generally Accepted Principles and Practices for Securing IT Systems
  - NIST SP 800-18, Guide For Developing Security Plans for IT Systems
  - NIST SP 800-26, Security Self-Assessment Guide for IT Systems
  - NIST SP 800-64, Security Considerations in the System Development Life Cycle
  - NIST SP 800-27, Engineering Principles for IT Security
  - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
  - NIST SP 800-100 Information Security Handbook: A Guide for Managers

IDENTIFIKÁCIA INFORMAČNÝCH AKTÍV

REGULÁCIA A RIADENIE BEZPEČNOSTI

DÁTA VS. INFORMÁCIE

- Dáta (údaje) sa informáciami stanú, až keď nadobudnú určitý význam
- Informácia je pochopením vzťahu medzi časťami dát
- Cena informácie je daná hodnotou, ktorú musí určiť jej vlastník
- Cena dát je daná hodnotou, ktorú musí určiť ich príjemca



Kenneth Boulding, 1955

RIADENIE IT AKTÍV

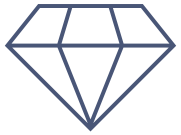
IT Aktívum – akýkoľvek finančne hodnotný komponent, ktorý sa podieľa na dodávke produktov alebo služieb

- **Aktíva (angl. Assets)** - hmotné alebo nehmotné ekonomické prostriedky, ktoré pre organizáciu priamo alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu (aktívami sú najmä: procesy, dáta, informácie, software, hardware, služby, objekty a priestory organizácie)
- **Účelom praktiky Riadenie IT aktív** (IT Asset management) je plánovať a riadiť celý životný cyklus IT aktív tak, aby pomáhala organizácii

Podľa ITIL®4 best practice – Copyright AXELOS Limited 2019

HODNOTA AKTÍV V KONTEXTE KB

Hodnotu informačných aktív je možné kvantifikovať nasledovne:



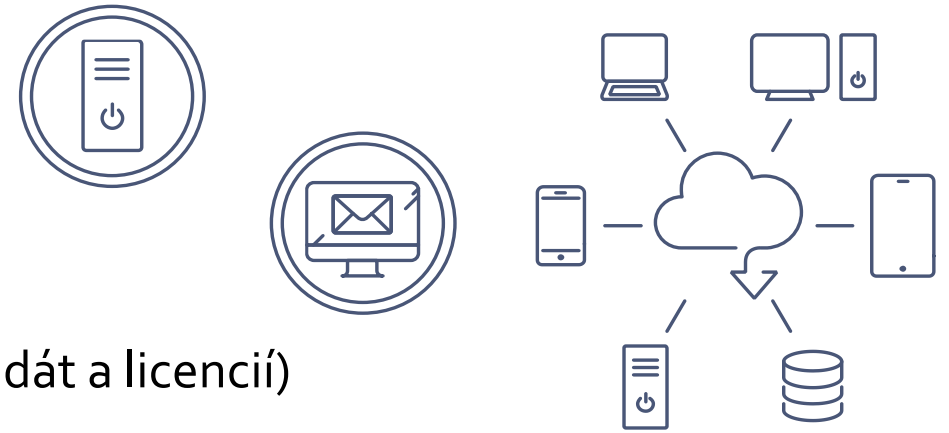
- Informačné aktíva **tvoria hodnotu**, alebo
- Hrozby pôsobiace na informačné aktíva **spôsobujú potenciálnu stratu**

Hodnotu informačných aktív vždy určuje **Vlastník aktíva** (resp. **Vlastník rizika**), odpoveďou na otázku:

- akú hodnotu informačné aktívum (napr. dokument, systém) tvorí?
- o akú hodnotu prídeme, ak aktívum (napr. dokument, systém) nemáme k dispozícii?
- aká bude potenciálna strata, ak bude informačné aktívum zneužité?
- aká hrozí pokuta, ak informačné aktívum nie je v súlade so zákonnými požiadavkami?

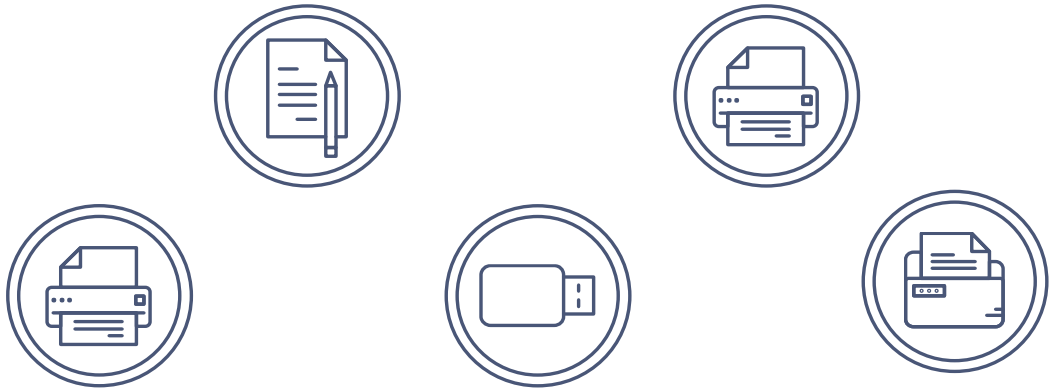
TYPY INFORMAČNÝCH AKTÍV PODĽA FYZICKEJ PODSTATY

Elektronické:



- elektronické dokumenty
- usporiadané množiny dokumentov, resp. databázy
- systémy, aplikácie (vrátane zdrojových kódov, metadát a licencií)

Fyzické:



- prenosné médiá
- tlačené a písané dokumenty

TYPY INFORMAČNÝCH AKTÍV PODĽA VÝZNAMNOSTI

ISO/IEC 27005

PRIMÁRNE AKTÍVA

- PROCESY
- INFORMÁCIE / DÁTA

PODPORNE AKTÍVA

- Technológie (HW, SW, siete)
- Lokality
- Zamestnanci (interní, externí)
- Tretie strany (dodávateľ/odberateľ)

TYPY INFORMAČNÝCH AKTÍV PODĽA RASMUSSENOVEJ HIERARCHIE

Konceptuálne

Funkčný účel	• Ciele alebo účely systému
Abstraktný účel	• Vstupy, výstupy, toky informácií, zásady riadenia
Všeobecné funkcie	• Procesy a vzťahy medzi komponentami podnikovej architektúry

Typicky elektronické

Reálne

Fyzické funkcie	• Spôsobilosti, zariadenia
Fyzická forma	• Lokácie, fyzické objekty, predmety, ľudia

Typicky fyzické

https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/introducing-component-driven-and-system-driven-risk-assessments

DEKOMPOZÍCIA SLUŽBY NA AKTÍVA

Zjednodušený príklad rozloženia základnej služby na aktíva:

- **Procesy/služby** – informovanie verejnosti, vybavovanie žiadostí autentifikovaných používateľov, poskytovanie údajov tretím stranám
- **Informácie/dáta** – štruktúrované údaje v primárnej a záložnej DB, dokumenty v DMS, zálohy na páskach, autentifikačné údaje používateľov, záznamy z monitorovania
- **Technológie** – HW (blade servery, diskové polia, pásková knižnica, sieťové prvky), SW (virtualizačná platforma, webové, aplikačné a DB servery, aplikačné moduly, active directory), siete (interná sieť, segmentované VLANy pre prvky IS, VPN)
- **Ľudia** – pracovníci pre biznis agendu, správcovia IT, zamestnanci dodávateľa
- **Lokality** – prevádzkové priestory, primárne DC, záložné DC
- **Tretie strany** – dodávateľ aplikácie, prevádzkovateľ DC, poskytovateľ pripojenia

BEZPEČNOSTNÉ OPATRENIA

REGULÁCIA A RIADENIE BEZPEČNOSTI

DEFINÍCIA BEZPEČNOSTNÉHO OPATRENIA

Opatrenia podľa **§ 20 (1)** Zákona 69/2018 Z.z. sú:

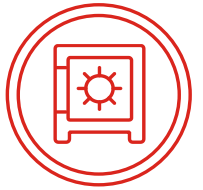
- **Úlohy, procesy, roly a technológie** v #organizačnej, #personálnej, #fyzickej a #technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií

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

- **Všeobecné bezpečnostné opatrenia** najmenej v rozsahu podľa §20
- **Sektorové bezpečnostné opatrenia**, ak sú prijaté

BEZPEČNOSTNÉ OPATRENIA

- **TECHNOLOGICKÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov technologickej povahy
- **FYZICKÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej povahy
- **ORGANIZAČNÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie
- **PERSONÁLNE OPATRENIA**
  - organizačné opatrenia týkajúce sa riadenia ľudských zdrojov

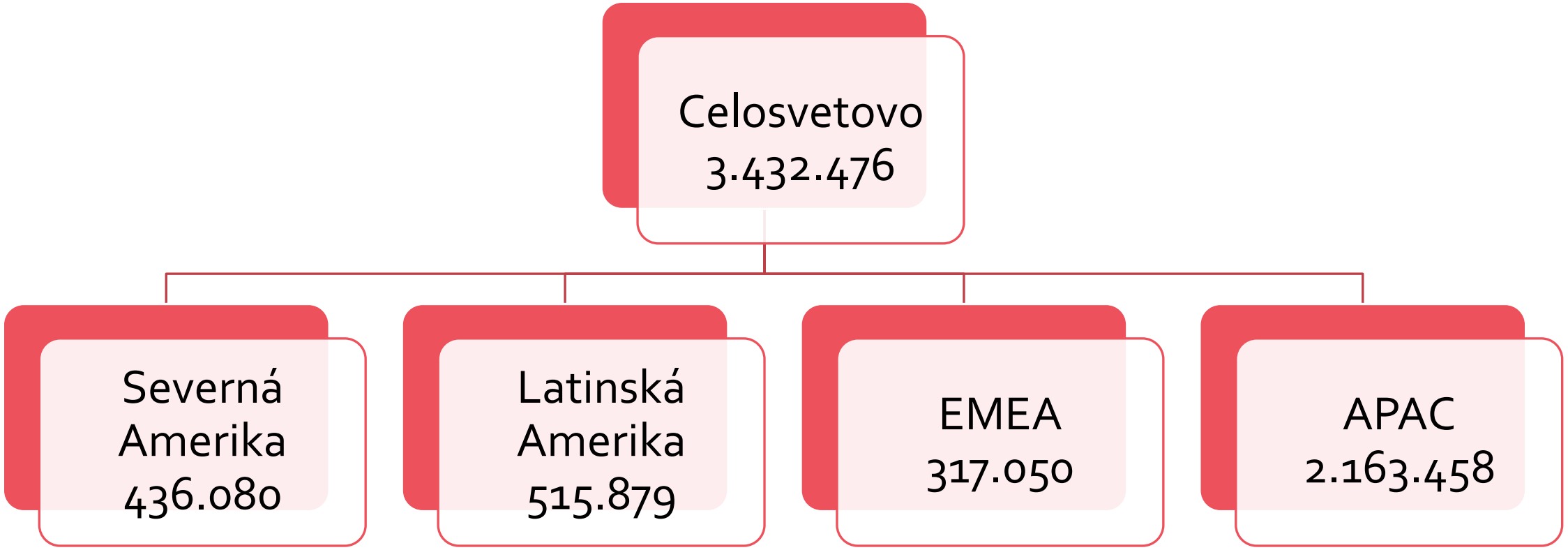


Efektívnu bezpečnosť je možné dosiahnuť
LEN POMOCOU KOMBINÁCIE
rôznych kategórií opatrení

PRACOVNÉ ROLY V KYBERNETICKEJ BEZPEČNOSTI A OBSAH ICH ZNALOSTNÝCH ŠTANDARDOV

REGULÁCIA A RIADENIE BEZPEČNOSTI

ODHAD POČTU CHÝBAJÚCICH PROFESIONÁLOV V KYBERBEZPEČNOSTI



Zdroj: *(ISC)2 Cybersecurity workforce study 2022*

CIEĽOVÉ SKUPINY VZDELÁVANIA V KB

Forma a a ciele vzdelávania	Cieľová skupina	Typické dotknuté roly
Upskilling, zvyšovanie kvalifikácie v KB	IB/KB	manažér KB, audítor KB, architekt KB, špecialista KB, analytik KB…
Upskilling, teoretické základy KB	Informatici	Všetky pracovné roly v prevádzke a vývoji IT, (študenti technických VŠ)
Zvyšovanie digitálnej gramotnosti	Zamestnanci	všetky pracovné roly, ktoré používajú k práci prostriedky IKT, (žiaci SŠ)
Zvyšovanie bezpečnostného povedomia	Laici	všetky pracovné roly, laická verejnosť, (žiaci ZŠ)

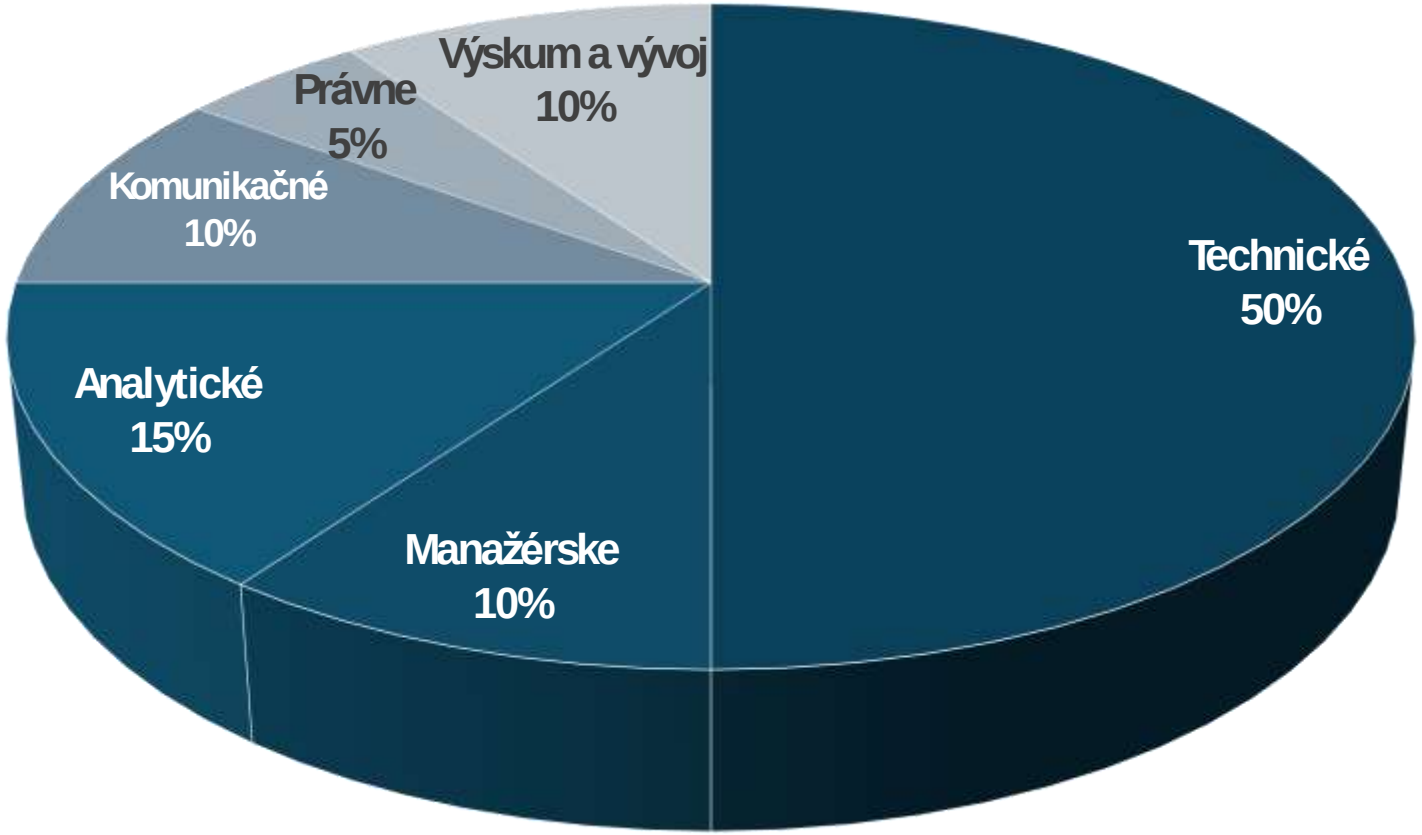
Zdroj: NIST Special Publication 800-16: Information Technology Security Training Requirements

DISTRIBÚCIA POŽIADAVIEK NA KVALIFIKÁCIE

Podľa kvalifikačného rámcy rolí v National Initiative for Cybersecurity Education (NICE)

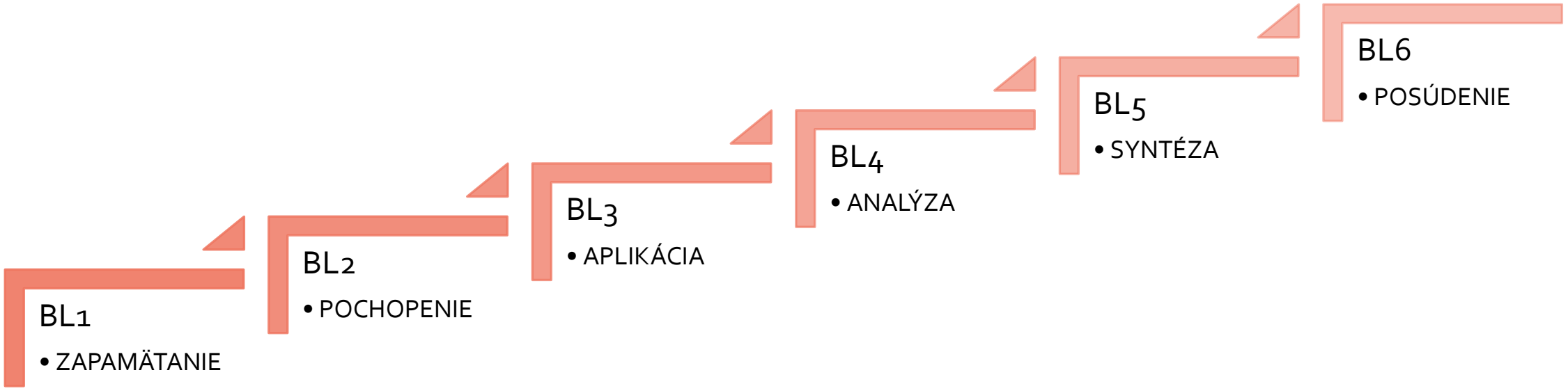
Komponenty rámca:

- **Kategórie** – Vysokoúrovňové skupiny kvalifikačných komponentov
- **Skupiny kompetencií** – Odlišné oblasti pracovnej špecializácie
- **Pracovné roly** – množiny špecifických znalostí, zručností a schopností potrebných na vykonávanie činností v konkrétnej pracovnej úlohe



BLOOMOVA TAXONÓMIA VZDELÁVANIA

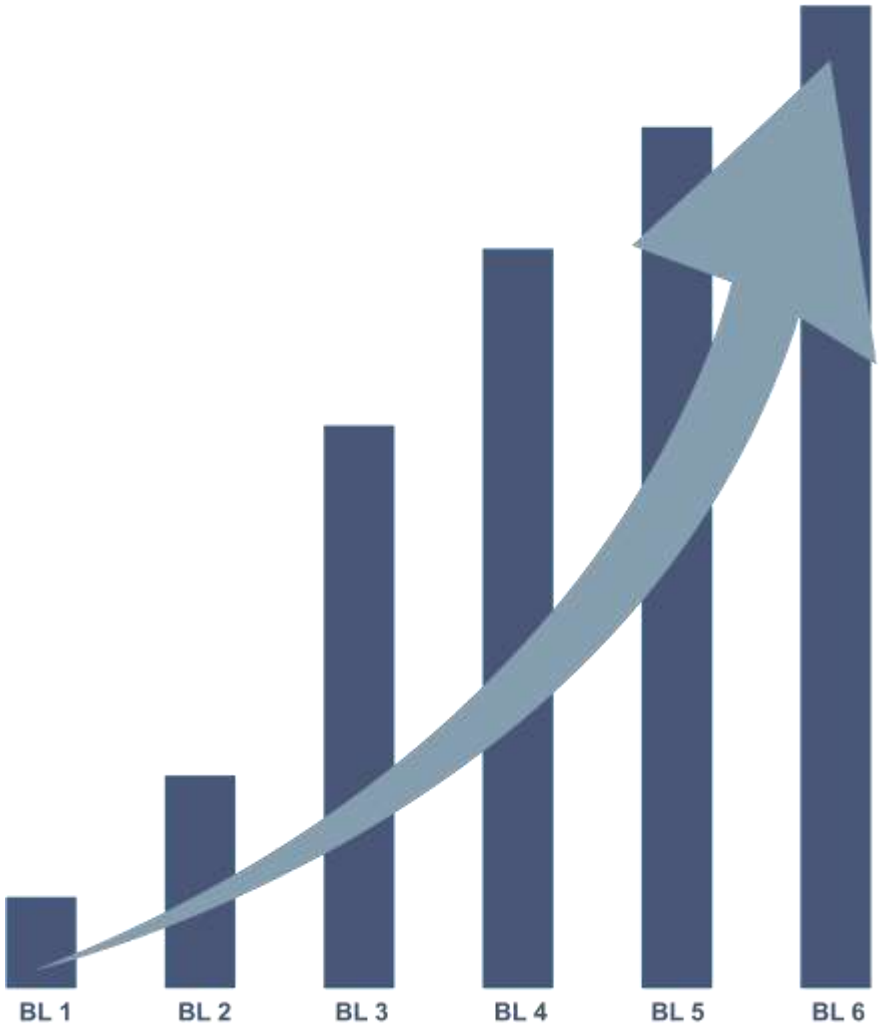
- **Taxonómia vzdelávania** je určenie miery obťažnosti učiva v procese učenia sa a vzdelávacích cieľov, ktoré majú byť prostredníctvom tohto formálneho vzdelávania dosiahnuté a ktorá môže byť použitá na štruktúrovanie cieľov, hodnotení a aktivít v učebných osnovách, vzdelávacích plánoch a v iných znalostných štandardoch
- Triedenie vzdelávacích cieľov je sekvenčné a zároveň kumulatívne
- Pre dosiahnutie vyššieho vzdelávacieho cieľa je potrebné dosiahnuť všetky predchádzajúce vzdelanostné úrovne



BLOOMOVA TAXONÓMIA

Úroveň	Vzdelávací cieľ	Popis vzdelávacieho cieľa
BL1	**ZAPAMÄTANIE**	Schopnosť zapamätať si potrebné informácie
BL2	**POCHOPENIE**	Schopnosť porozumieť alebo pochopiť význam toho, čo bolo komunikované a využiť získanú informáciu bez toho, aby ju uchádzač spájal s inými informáciami, interpretáciami alebo materiálmi
BL3	**APLIKÁCIA**	Uchádzač by mal byť schopný používať myšlienky, princípy a teórie v nových, konkrétnych situáciách
BL4	**ANALÝZA**	Uchádzač je schopný rozdeliť komunikáciu na základné časti, aby bol jasne uchopený význam informácie. V tejto úrovni sa skúma podstata jednotlivých entít, s cieľom lepšie porozumieť komplexným celkom
BL5	**SYNTÉZA**	Na tejto úrovni je uchádzač schopný opätovne spojiť rôzne časti alebo prvky konceptu do jednotného systému alebo celku
BL6	**POSÚDENIE**	V tejto fáze je uchádzač schopný dospieť k prehľadu a posúdiť hodnotu a relatívny prínos myšlienok alebo postupov pomocou vhodných kritérií

TAXONÓMIA VZDELÁVACÍCH CIEĽOV PRE ROLY V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI



Pôsobnosť vyhlášky

- Audítori a výskumníci v kybernetickej bezpečnosti
- Manažéri kybernetickej bezpečnosti
- Pracovníci v kybernetickej bezpečnosti

Ostatné kategórie rolí

- Informatici
- IT manažéri
- Manažéri
- Odborní zamestnanci
- Laici

EURÓPSKY RÁMEC ROLÍ V KB

- Zodpovednosť osôb konajúcich v kontexte kybernetickej bezpečnosti v organizácii má byť zadefinovaná jednoznačne, prostredníctvom rolí, v ktorých osoba vystupuje vo vzťahu k sieti alebo informačnému systému
- S rolami je spojená množina povinností a oprávnení pri inicializácii, návrhu, vývoji, používaní a prevádzke siete alebo informačného systému
- Charakteristika rolí patriacich do príslušnej kategórie podrobnejšie špecifikuje kľúčové činnosti, požadované vedomosti, zručnosti, špecifické kľúčové kompetencie a ďalšie podmienky, ktoré má spĺňať osoba zaradená do danej roly tak, aby bola schopná plniť svoje povinnosti vyplývajúce z roly, v ktorej je zaradená

EURÓPSKY VS. SLOVENSKÝ RÁMEC ROLÍ V KB

ENISA European Cybersecurity Skills Framework (ECSF)

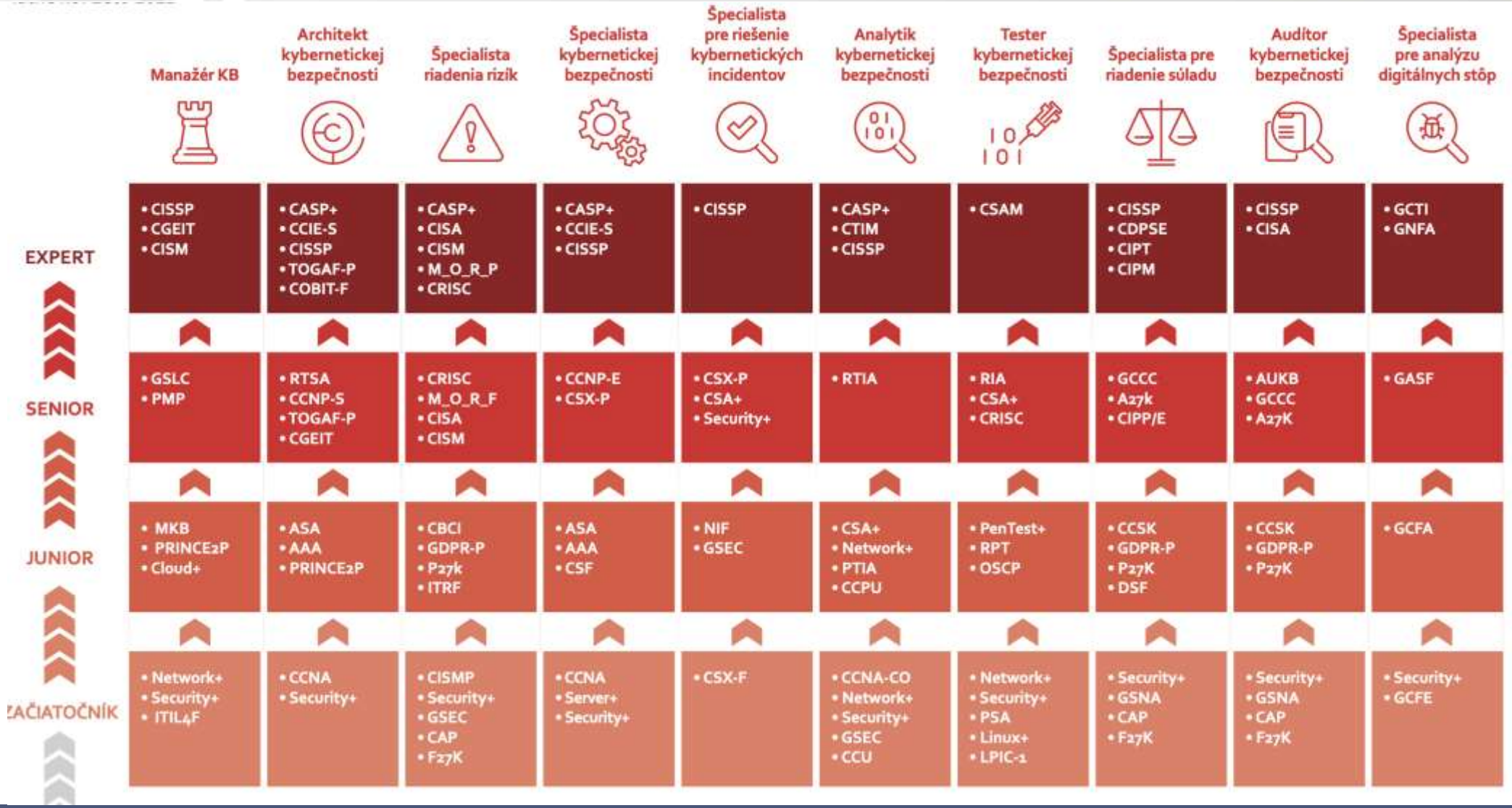
Vyhláška NBÚ č. 492/2022 o znalostných štandardoch v KB

Spolufinancovaný Európskou úniou

SUBRÁMCE KVALIFIKÁCIÍ V KONTEXTE SLOVENSKÉHO KVALIFIKAČNÉHO RÁMCA

Úroveň kvalifikácie	Všeobecnovzdelávacie kvalifikácie	Odborné kvalifikácie	Vysokoškolské kvalifikácie	Profesijné kvalifikácie
Právny základ	zákon č. 245/2008 Z.z. o výchove a vzdelávaní (školský zákon)	zákon č. 245/2008 Z.z. o výchove a vzdelávaní (školský zákon)	zákon č. 131/2002 Z. z. o vysokých školách	zákon č. 292/2024 Z. z. o celoživotnom vzdelávaní
Klasifikácia ISCED	1	2-5	6-8	2-8
Typ vzdelávacej inštitúcie	Štátne, súkromné a cirkevné základné školy	Štátne a súkromné stredné školy	Štátne a súkromné vysoké školy	Vzdelávacie inštitúcie
Cieľ vzdelávania v IB/KB	Získanie digitálnych zručností	Digitálne zručnosti, základy IKT a informačnej bezpečnosti	Stupeň vzdelania a kvalifikácia uvedená v subrámci Slovenského kvalifikačného rámca	Získanie, doplnenie, rozšírenie alebo prehĺbenie kvalifikácie a kľúčových kompetencií
Doklad	Vysvedčenie	Vysvedčenie, výučný list	Vysokoškolský diplom	Certifikát, osvedčenie o absolvovaní
Akreditácia resp. atestácia obsahu	Národný inštitút vzdelávania a mládeže (**NIVaM**)	Štátny inštitút odborného vzdelávania (**ŠIOV**)	Slovenská akreditačná agentúra pre vysoké školstvo (**SAAVŠ**)	Ministerstvo školstva, výskumu, vývoja a mládeže (**MŠVVaM**)

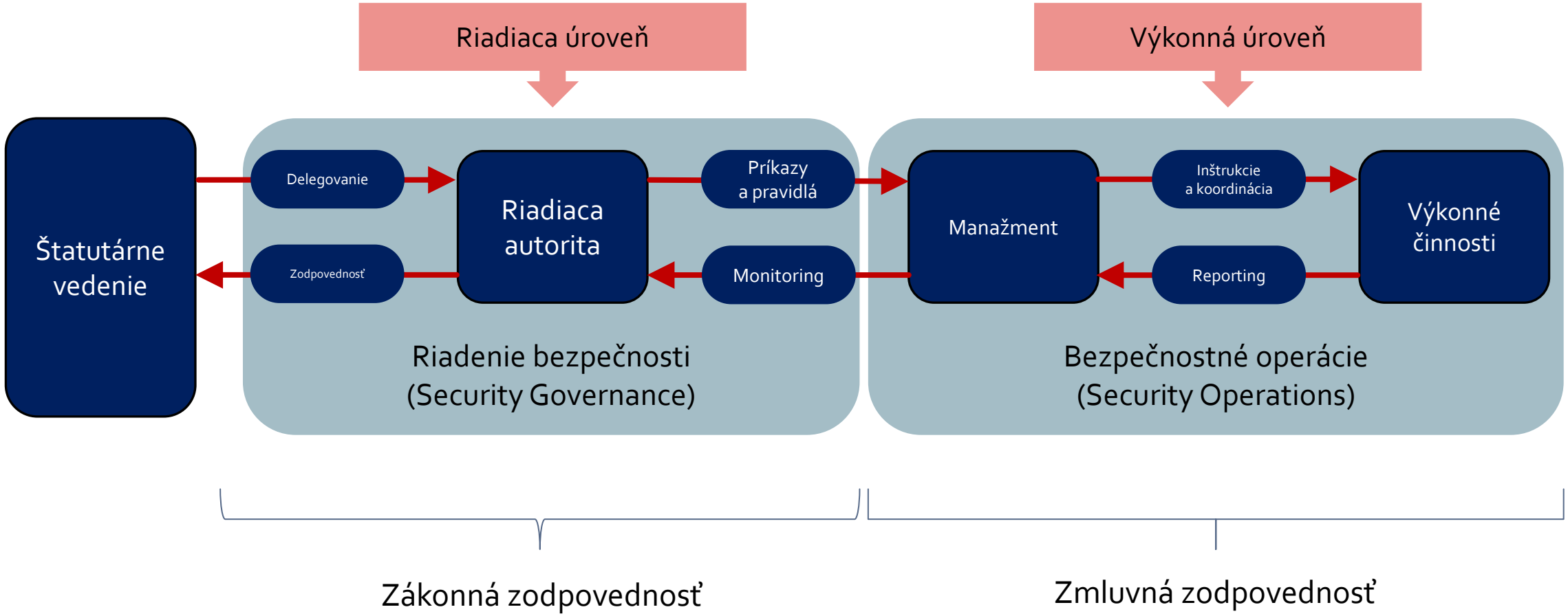
MAPOVANIE KOMERČNÝCH CERTIFIKÁTOV NA ROLY V KYBERNETICKEJ BEZPEČNOSTI



ZÁKLADNÉ PRINCÍPY SECURITY GOVERNANCE

REGULÁCIA A RIADENIE BEZPEČNOSTI

KĽÚČOVÉ ROLE A VZŤAHY V RIADENÍ A VÝKONE BEZPEČNOSTI



Zdroj: ISACA, isaca.org/cobit5

KĽÚČOVÉ PRVKY RIADENIA

Organizačné štruktúry napomáhajú definovať tri kľúčové prvky manažmentu:

Právomoci:

- Ako sú úlohy delegované
- Ako je schvaľovaná práca
- Riadiaca línia (Kto koho riadi, kto komu oznamuje úlohy)
- Ako sa oznamujú problémy, požiadavky a návrhy

Rozsah riadenia:

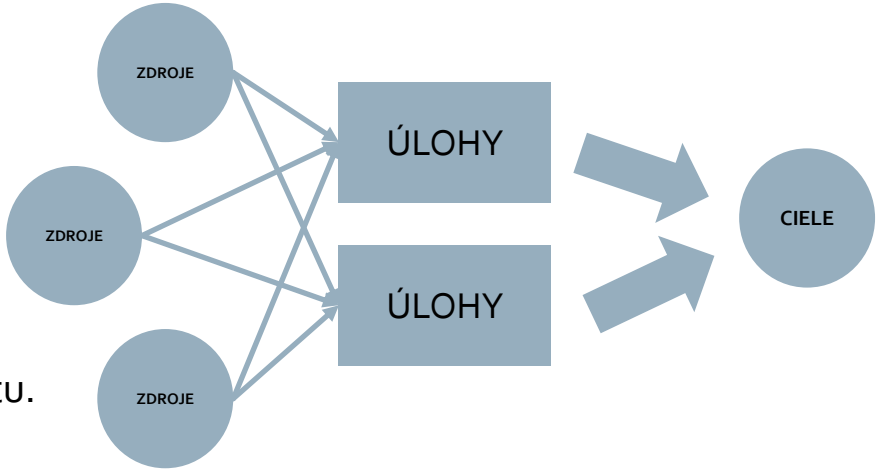
- Ktoré procesy spadajú do zodpovednosti konkrétneho manažéra
- Za ktoré úlohy zodpovedá organizačná jednotka
- Počty pracovníkov vyčlenených na jednotlivé úlohy

Úroveň centralizácie:

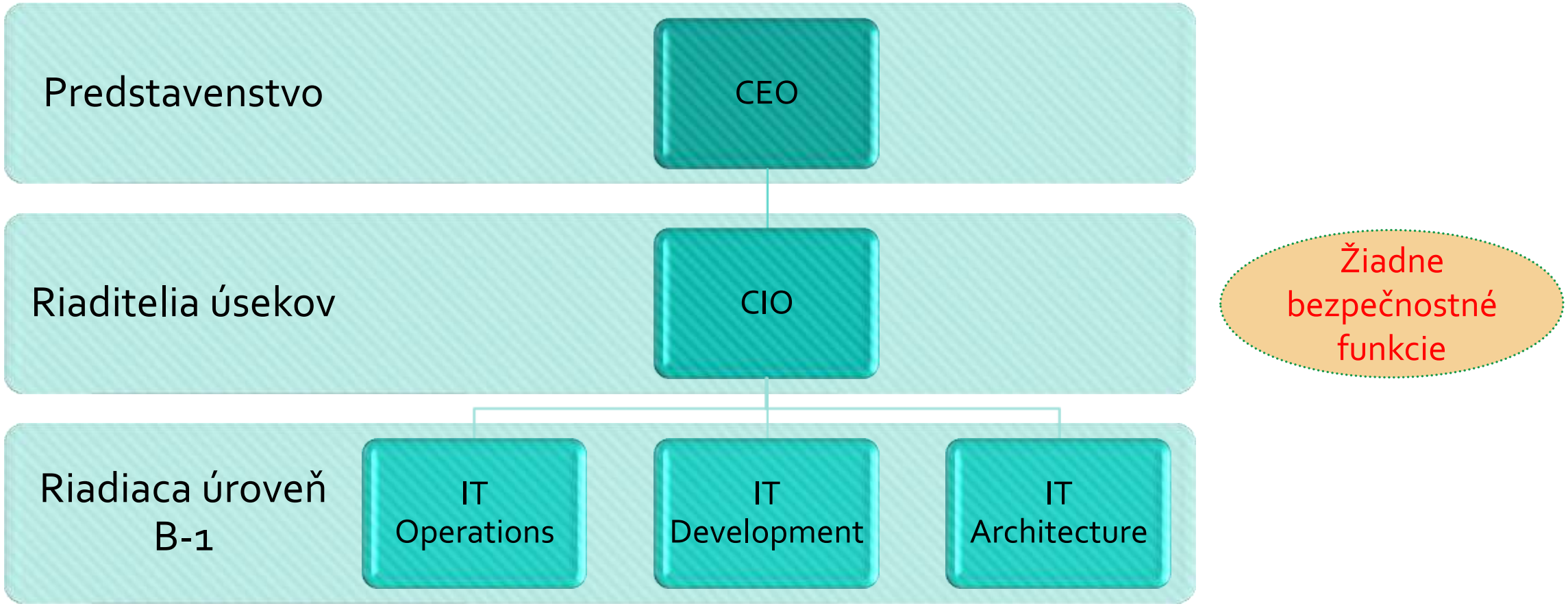
- Kontrola nad rozhodnutiami
- Ktorí ľudia v organizačnej jednotke majú slovo pri rozhodovaniach
  - **Centralizované**: konečné rozhodnutia prijíma iba jeden človek
  - **Decentralizované**: konečné rozhodnutia sa prijímajú v rámci organizačnej jednotky zodpovednej za vykonávanie úlohy

TYPOLÓGIA ORGANIZAČNÝCH ŠTRUKTÚR

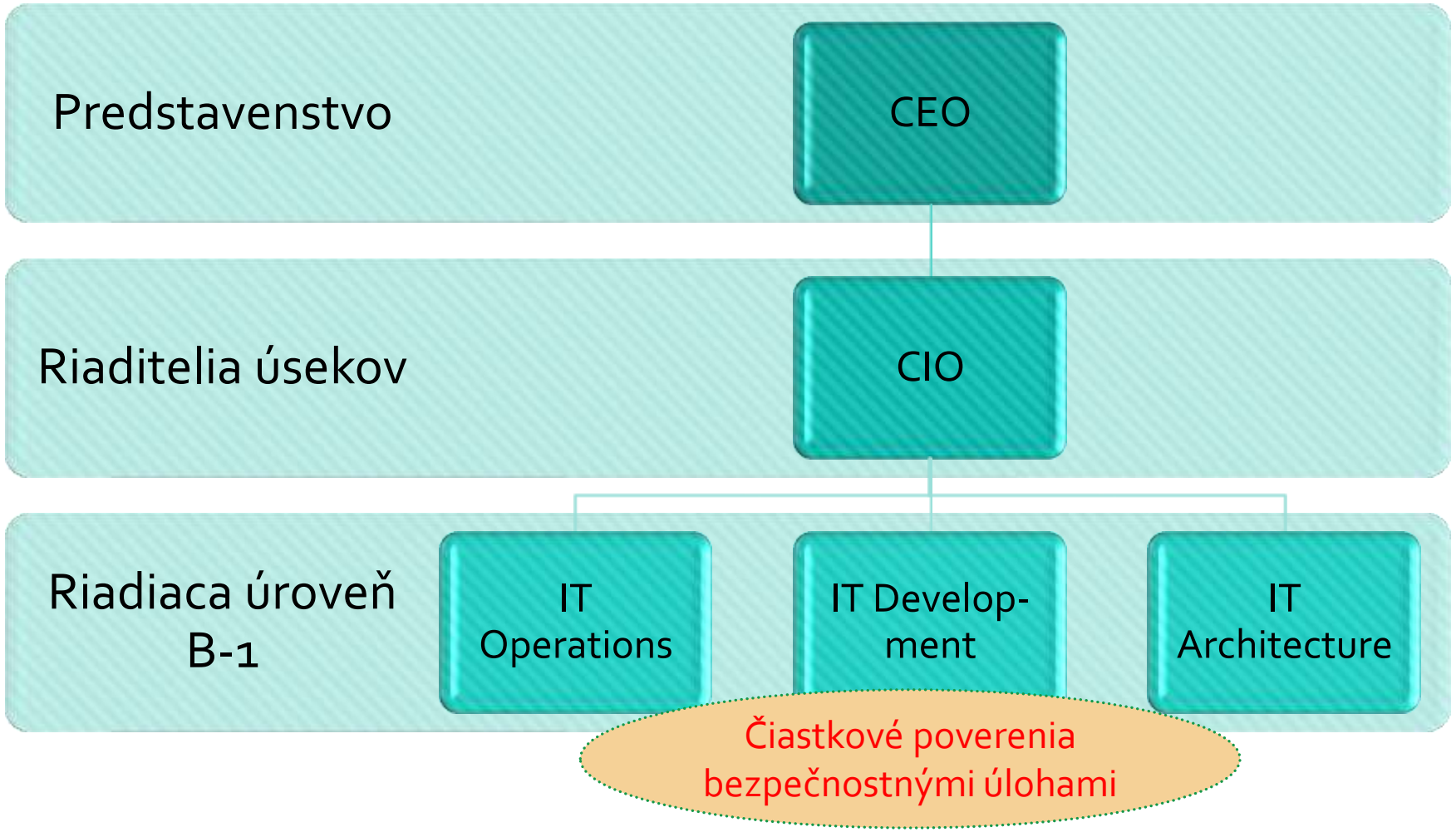
- **Plochá štruktúra**
  - Nízka úroveň hierarchie
  - Odstraňuje bariéry v rozhodovaní
  - Výhodná pre startup-y
- **Funkčná resp. líniová**
  - Vytvára odborné útvary pre jednotlivé funkčné oblasti manažmentu.
- **Divízna**
  - Typicky tri, resp. štyri úrovne riadenia: podnikovú, úsekovú, funkčnú
  - Na úrovni podniku sa rozhoduje o celkovom rozvoji aktivít
  - Na funkčnej úrovni rozhodujú funkční manažéri
- **Maticová**
  - Na úrovni podniku sa rozhoduje o celkovom rozvoji aktivít
  - Na podnikovej úrovni rozhodujú manažéri špecializovaní na vybrané produkty a oblasti
  - Na funkčnej úrovni rozhodujú funkční manažéri
- **Holdingová**
  - Podobná divíznej štruktúre, s vyšším stupňom samostatnosti základných podnikov



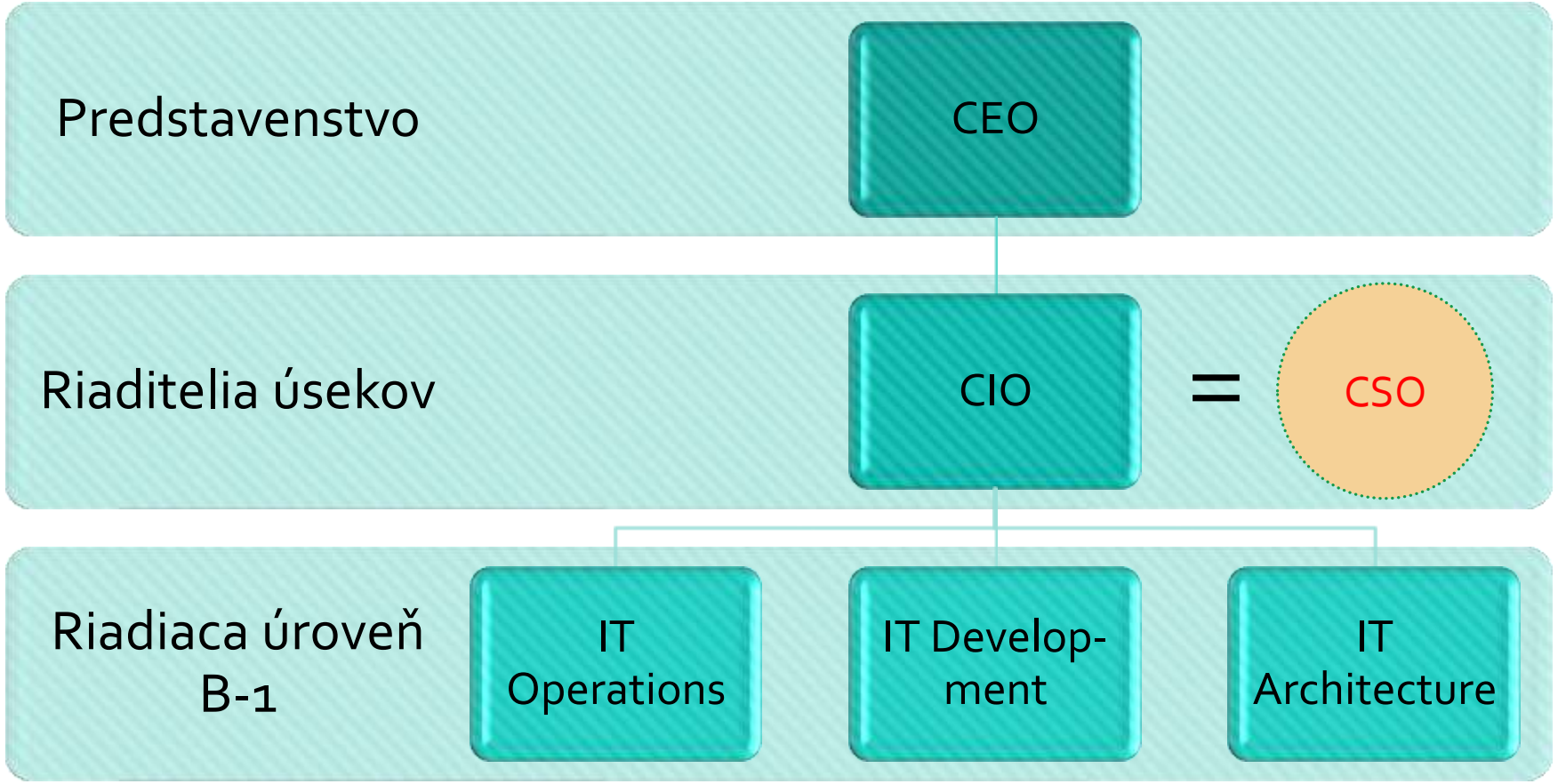
„IGNOROVANÁ“ BEZPEČNOSŤ



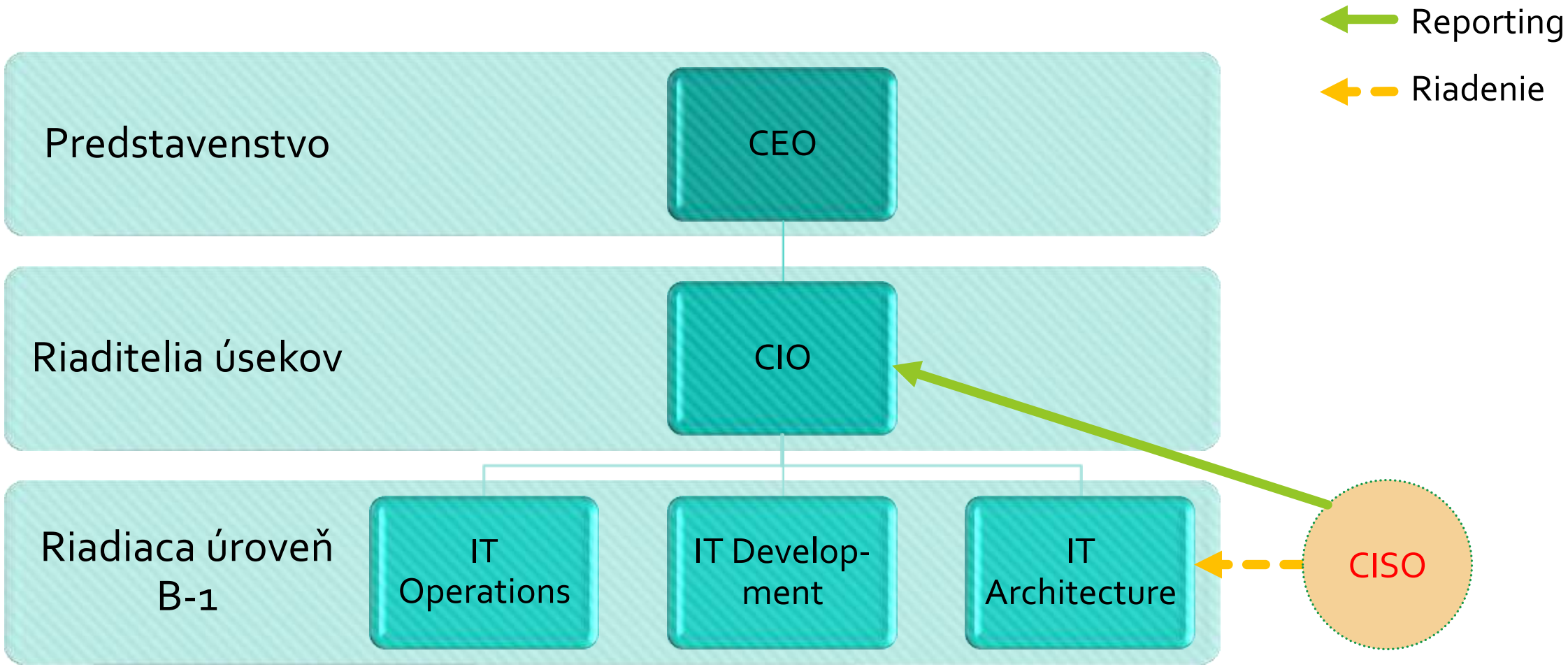
„MINIMÁLNA“ BEZPEČNOSŤ



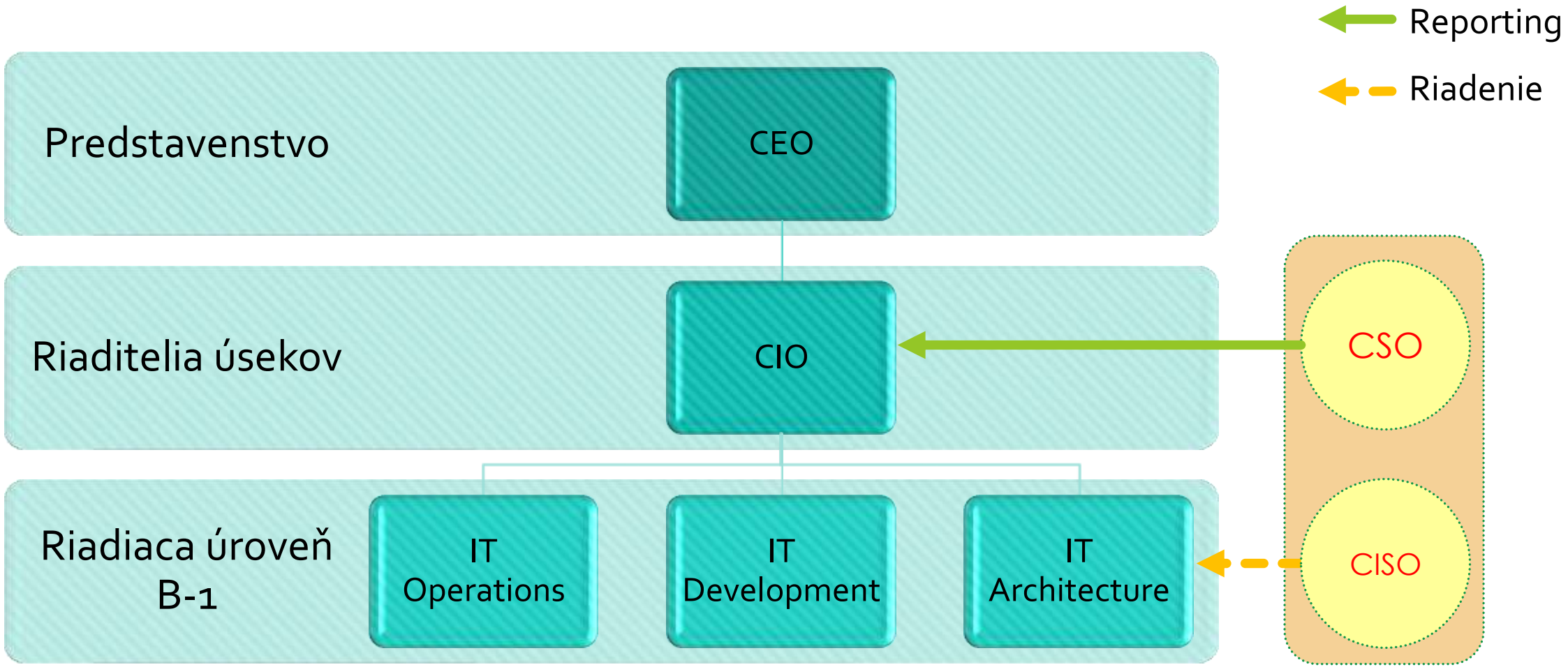
„FORMÁLNA“ BEZPEČNOSŤ



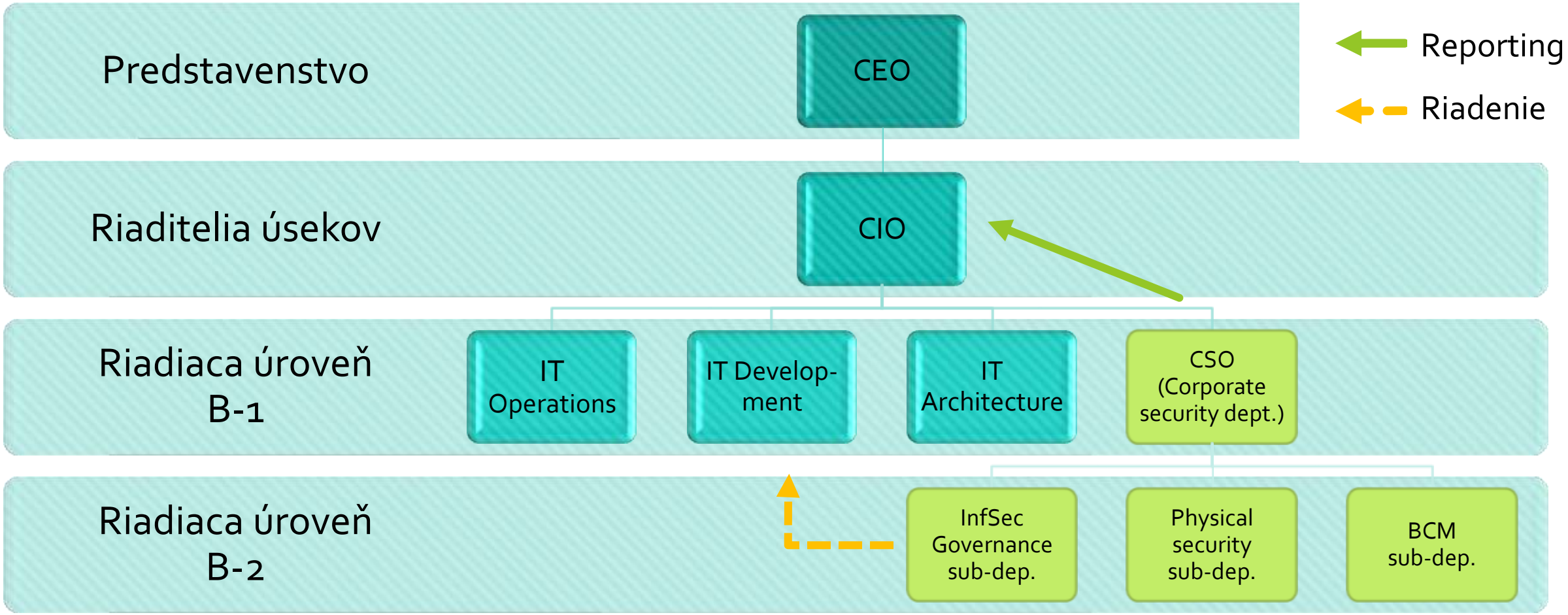
„UTOPENÁ“ BEZPEČNOSŤ



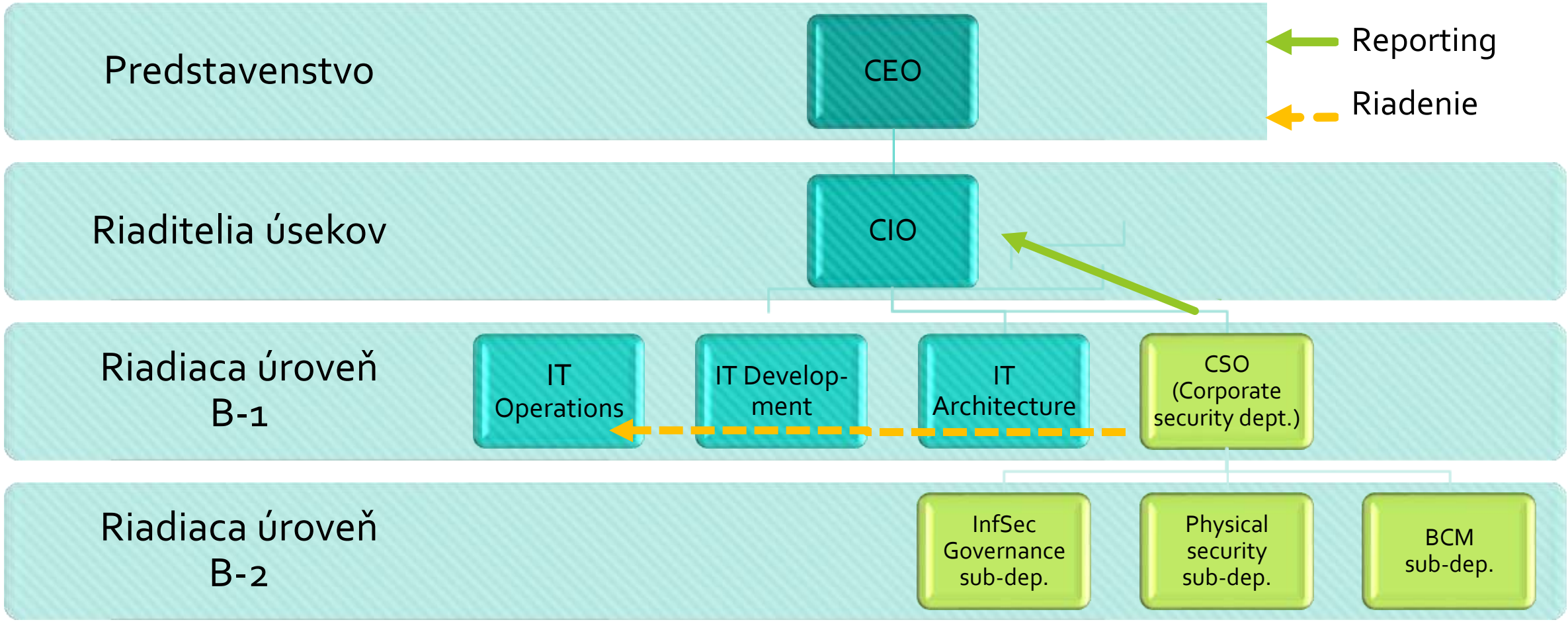
„AGILNÁ“ BEZPEČNOSŤ



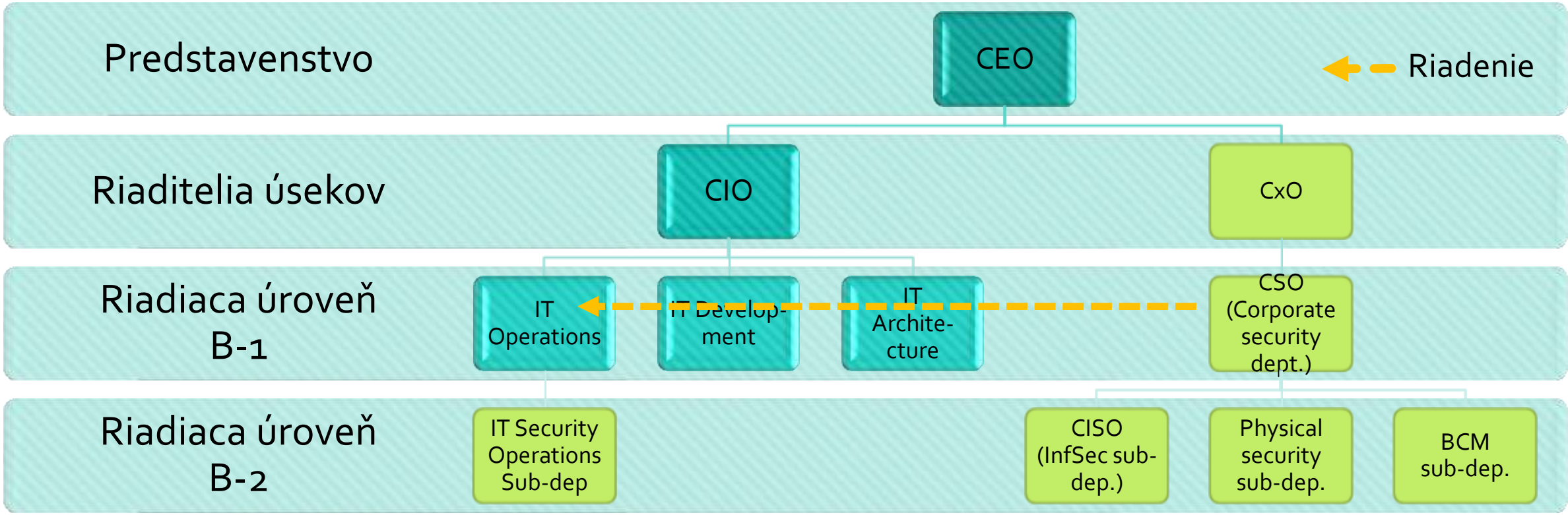
„DOZORUJÚCA“ BEZPEČNOSŤ



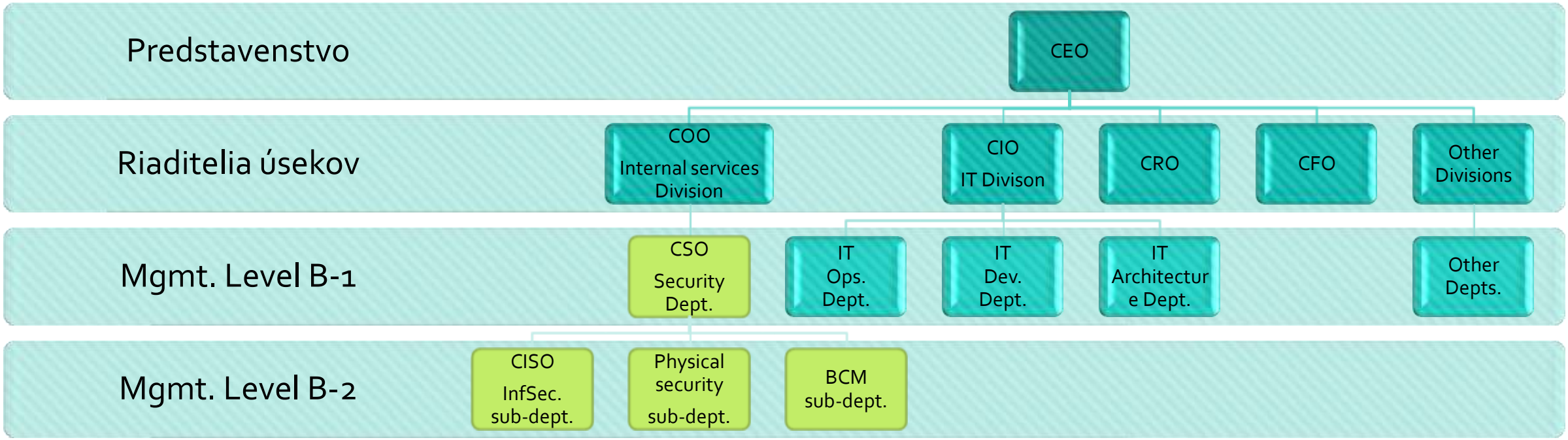
„KORPORÁTNA“ BEZPEČNOSŤ



„NEZÁVISLÁ KORPORÁTNA“ BEZPEČNOSŤ



TYPICKÁ ORGANIZAČNÁ ŠTRUKTÚRA



POROVNANIE ORGANIZAČNÝCH ŠTRUKTÚR BEZPEČNOSTI

Typ bezpečnosti	Právomoci	Rozsah riadenia	Miera centralizácie	Oddeľovanie právomocí	Vyspelosť ISMS
Ignorovaná (t.j. žiadne bezpečnostné funkcie)	N/A	N/A	N/A	N/A	0 - ISMS neexistuje
Minimálna (t.j. čiastkové poverenia)	N/A	N/A	decentralizovaná	Najhorší scenár	0 - ISMS neexistuje
Formálna (t.j. CIO=CSO)	Len formálna rola	Identický s CIO	centralizovaná	nie	1 - Počiatočná
Utopená (CISO ovplyvňuje IT, reportuje CIO)	slabá	Identický s CIO	čiastočne centralizovaná	slabé	2 - Opakovateľná
Agilná (CISO ovplyvňuje len IT, reportuje CIO)	udržateľné	slabý	čiastočne centralizovaná	čiastočné	3 - Definovaná
Dozorujúca (odbor bezpečnosti, CSO reportuje CIO)	udržateľné	dostatočný	centralizovaná	udržateľné	4 - Manažovaná
Korporátna (odbor bezpečnosti, samostatné oddelenie bezpečnostných operácií, CSO reportuje CIO)	dostatočné	dostatočný	centralizovaná	dostatočné	5 - Optimalizovaná
Nezávislá korporátna (odbor bezpečnosti, samostatné oddelenie bezpečnostných operácií, CSO reportuje v separátnej línii)	optimálne	široký	centralizovaná	Najlepší scenár	5 - Optimalizovaná

ZÁVER

"Zákony sú ako párky. Je lepšie nevedieť, ako sa vyrábajú..." (Otto von Bismarck)

- NIS, PSD, GDPR, CSA, NIS2, PSD2, DORA, DMA, DSA, AIA, CSA+, CySolA, EUIBAs, CRA, eIDAS2... vykonávacie a implementačné nariadenia COM...
  - Každý z týchto právnych predpisov EÚ pripravovala iná skupina legislatívcov, avšak zjavne bez potreby vzájomnej koordinácie
- Výsledok:
  - dokázateľne chybná terminológia v rozpore s dobrou praxou
  - právna dvojkoľajnosť
  - preregulovanosť prostredia
- **Legislatívci však nevynašli koleso:**
  - Terminológia v IB/KB je dávno ustálená v technických normách ISO/IEC (!)
  - Legislatívne pracovné skupiny sa nemajú čím iným inšpirovať, než medzinárodnými technickými normami ISO/IEC
- Praktickým rozdielom medzi požadavkami jednotlivých právnych predpisov v KB sú len **rôzne eskalačné procedúry** a **rôzni prijímatelia reportov**

Administratívna záťaž

AKO SA NEDÁ DOSIAHNUŤ ŽIADUCE SPRÁVANIE SUBJEKTOV?

- Vytváranie vlastných interpretácií odborných termínov a účinku bezpečnostných mechanizmov zo strany legislatívcov
- Nezmyselné a extenzívne regulačné požiadavky (napr. duplicitný reporting nad rámec praktickej potreby alebo len zo štatistických dôvodov)
- Zavádzanie pokút za nezavinené incidenty – tieto vytvárajú novú hrozbu a odvádzajú pozornosť od pôvodných rizík
- Povinnosti, vynucované hrozbou sankcie - likvidujú vnútornú motiváciu
- Obrátené dôkazné bremeno núti subjekty nepriznávať incidenty – čo je pravý opak zodpovedného zverejňovania zraniteľností – ak sa o hrozbe nedozvieme, nedá sa pred ňou brániť...

Právna dvojkoľajnosť je pre compliance management kontraproduktívna
(zvyčajným dôsledkom je obchádzanie pravidiel)

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB"). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

BACKLOG

REGULÁCIA A RIADENIE BEZPEČNOSTI

AKTUÁLNY STAV KYBERNETICKEJ BEZPEČNOSTI NA SLOVENSKU

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI – DOPAD NIS2 ALA. LEGISLATÍVCI NEVYNAŠLI KOLESO…

TVORBA ZISTENÍ V AUDITE KYBERNETICKEJ BEZPEČNOSTI

- Auditom kybernetickej bezpečnosti sa zisťuje:
  - Účinnosť prijatých bezpečnostných opatrení
  - Plnenie požiadaviek stanovených zákonom

Audit kyberbezpečnosti nie je sankčný mechanizmus!

Požiadavka

- Bezpečnostné opatrenie podľa príslušného právneho predpisu
- Formálne požiadavky v zmysle zákona o KB

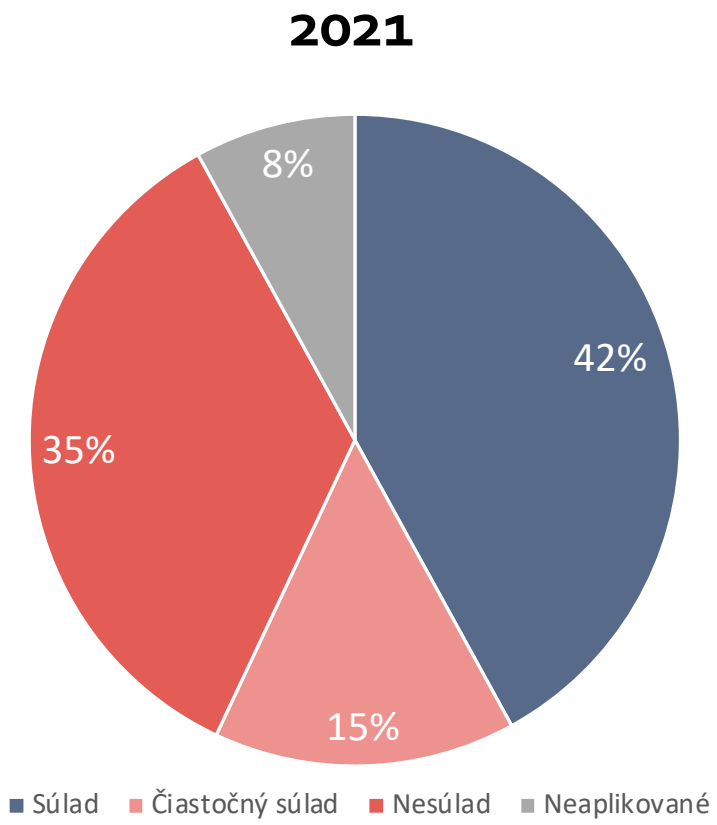
Nezhoda

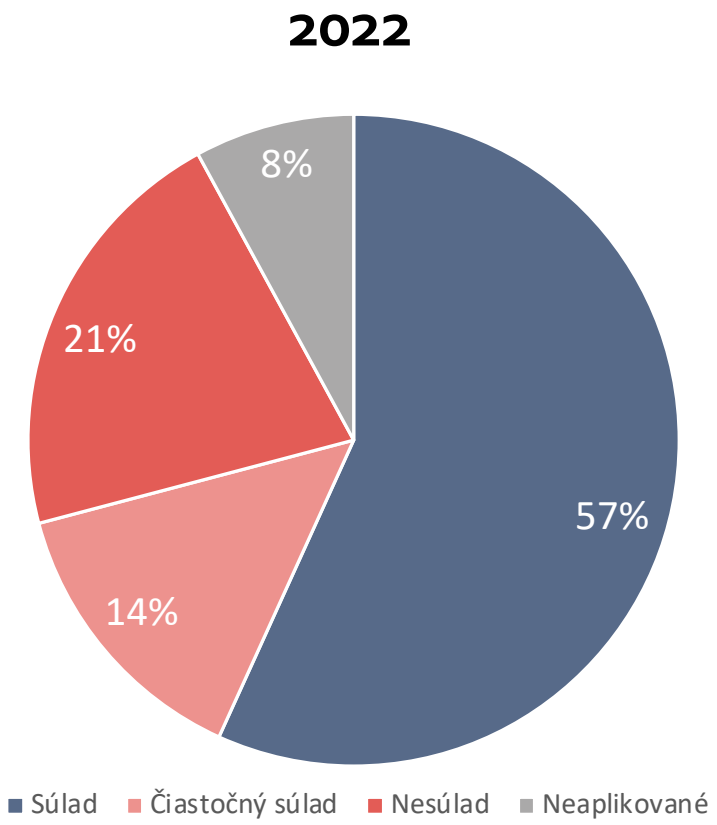
- Chýbajúce opatrenie
- Neefektívne opatrenie
- Nesplnená požiadavka
- Neplnený bezp. cieľ
- Nedostatočná kvalita alebo rozsah dokumentácie

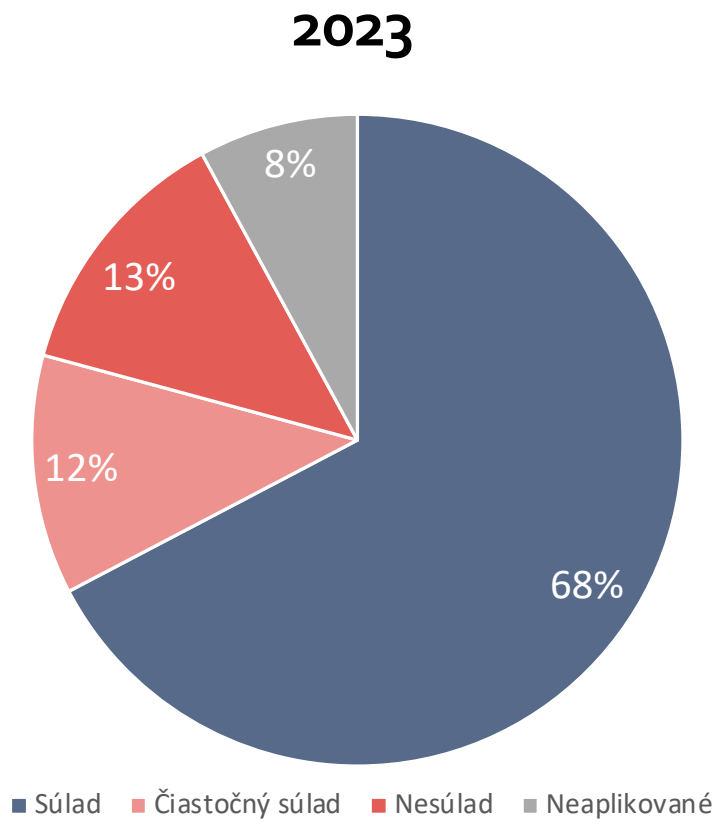
Dôkaz

- Identifikované riziko
- Identifikovaná nezhoda s požiadavkou
- Identifikovaná nízka účinnosť opatrenia

CELKOVÝ STAV SÚLADU 2021-2023

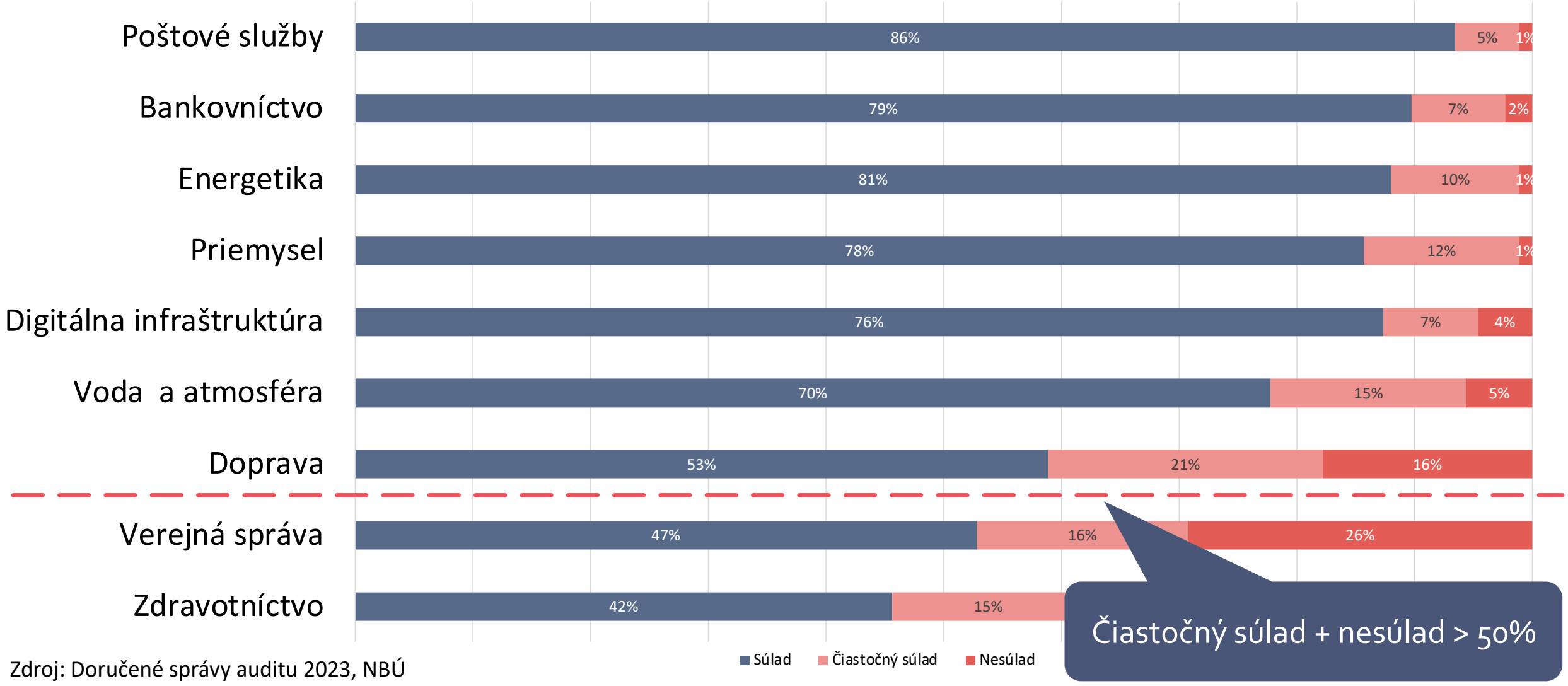






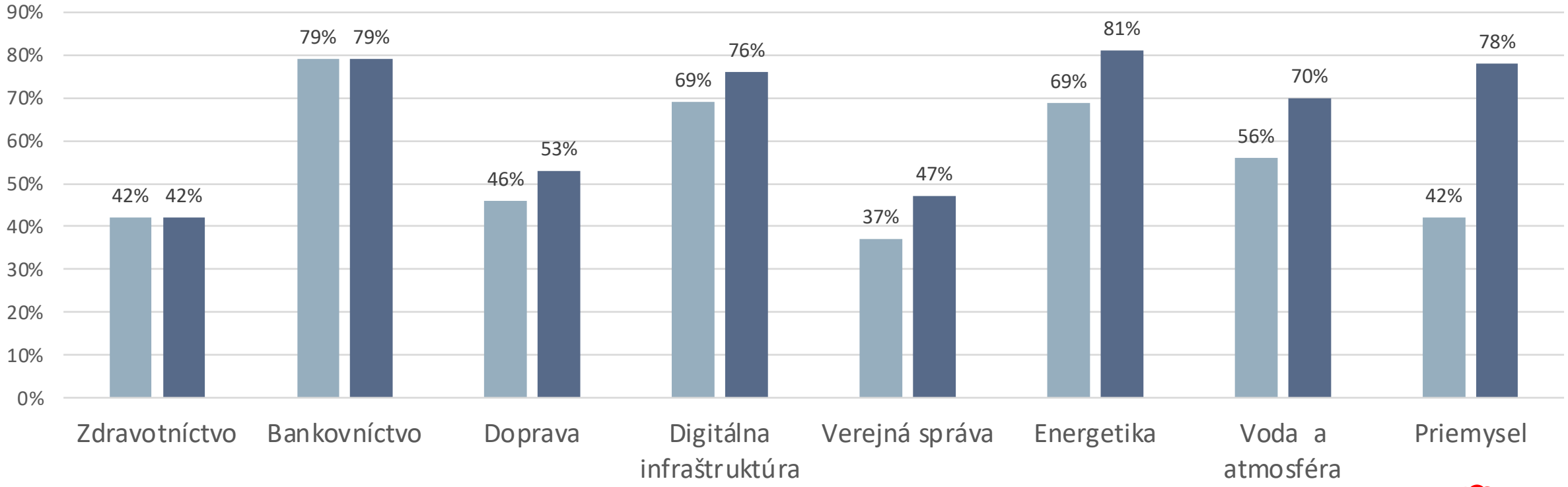
Zdroj: Doručené správy auditu 2021-2023, NBÚ

SÚLAD PODĽA ODVETVÍ 2023

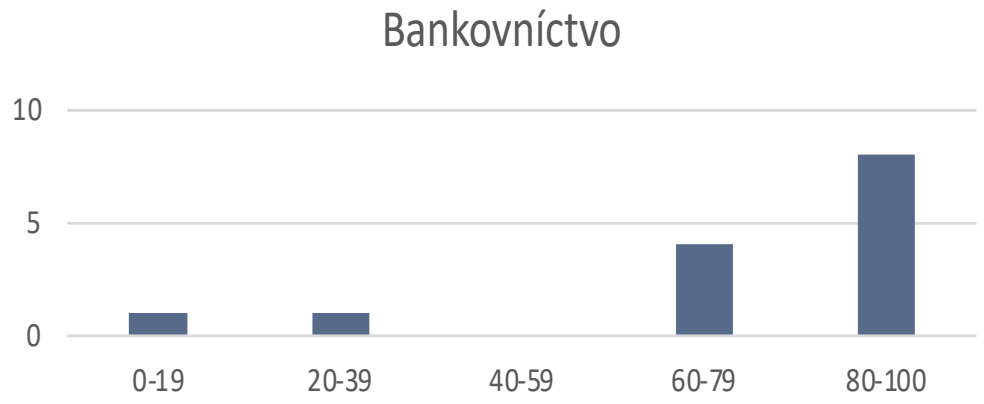


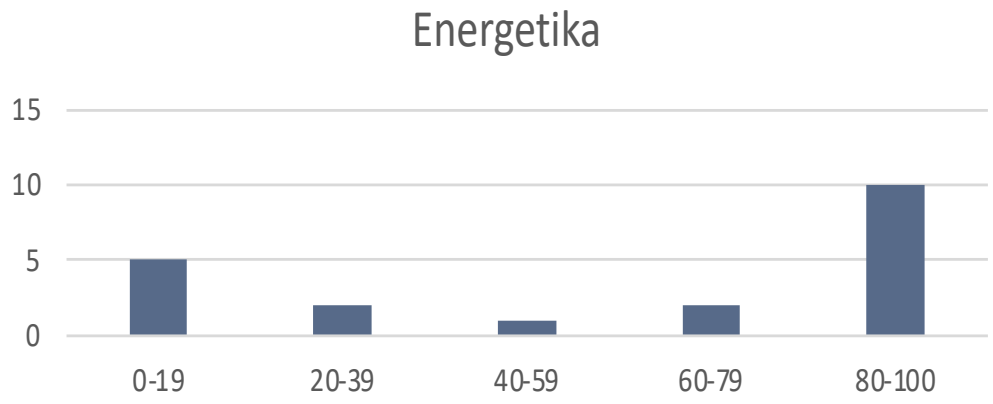
Zdroj: Doručené správy auditu 2023, NBÚ

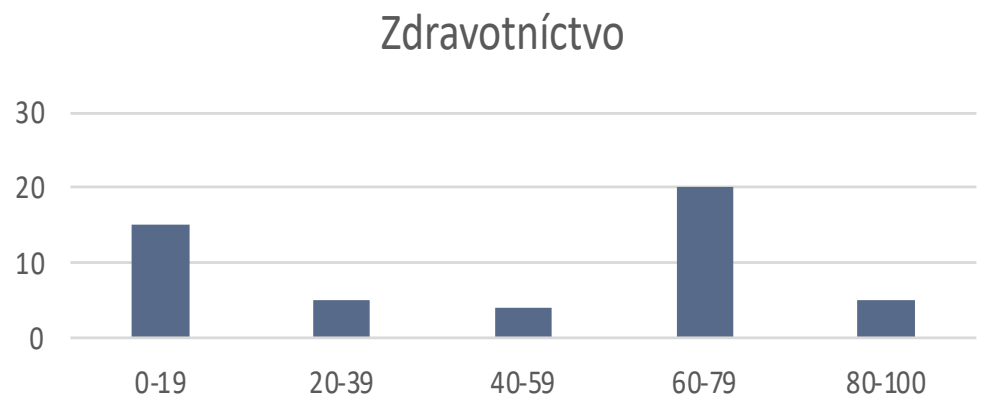
VÝZNAMNÉ ZLEPŠENIA SÚLADU PODĽA ODVETVÍ

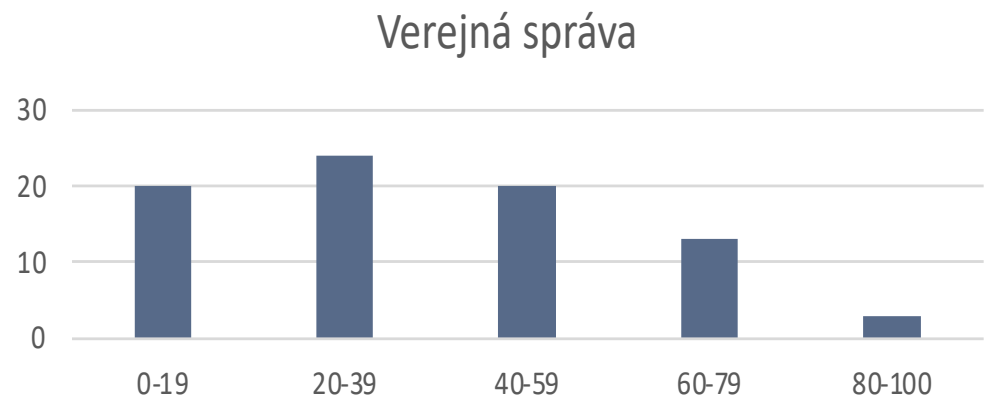


ŠTATISTICKÁ DISPERZIA SÚLADU VO VYBRANÝCH ODVETVIACH









NAJČASTEJŠIE NÁLEZY AUDITU

Riadenie bezpečnosti (Security governance):

- Nedostatočná podpora vedenia
- Nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti kybernetickej bezpečnosti
- Zodpovednosť za identifikáciu a evidenciu aktív, hrozieb a rizík
- Neexistencia analýzy rizík a analýzy dopadov
- Nedostatočná, alebo stále chýbajúca bezpečnostná dokumentácia
- Nezávislosť riadenia bezpečnosti od riadenia IT
- Vzdelávanie v oblasti informačnej bezpečnosti
- Neformálne riadenie prevádzky

Výkon bezpečnosti (Security operations):

- Chýbajúci bezpečnostný monitoring
- Nesystematické riešenie incidentov
- Vzdialený prístup do interných sietí a IS nie je zabezpečený
- Chýbajúca topológia, segmentácia, zoznamy portov
- Neexistencia procesov riadenia kontinuity činností
- Nejasné a neformálne postupy zálohovania a obnovy
- PZS nedostatočne rieši šifrovú ochranu informácií

Spolufinancovaný Európskou úniou

TYPICKÉ ZRANITEĽNOSTI A HROZBY V UNIVERZITNOM PROSTREDÍ

- Široký perimeter
- Laboratórne prostredia
- Vysoká komplexita IT architektúry

→ Zväčšená plocha útoku (Attack Surface)

- Veľké množstvo koncových zariadení
- Zdieľanie zariadení
- Súkromné zariadenia v sieti

→ Neautorizovaný prístup

- Špecifické výskumné dáta
- Spracúvanie osobných údajov
- Zložitá rekonciliácia v IAM

→ Odcudzenie údajov

ZÁSADY ORGANIZÁCIE KYBERNETICKEJ BEZPEČNOSTI

- **Najnižšie privilégiá** (least privilege)
  - každému používateľovi sú obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh
- **Oddeľovanie zodpovedností** (segregation of duties)
  - žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity
- **Vykonávanie nezávislého hodnotenia**
  - meranie a preskúmavania efektivity a účinnosti prijatých opatrení
- **Jasné vymedzenie právomoci**
  - povinnosti a zodpovednosti, sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností

OBJEKTY POSUDZOVANIA ZHODY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI