Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE Z POHĽADU NORIEM A REGULÁCIE

WORKSHOP: Digitálne zdravie a základy telemedicíny

27.3.2024, Bešeňová

VYHLÁSENIE O KONFLIKTE ZÁUJMOV AUTORA

☒ **Nemám potenciálny konflikt záujmov**

☐ Deklarujem nasledujúci konflikt záujmov

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Skrátene „Kompetenčné centrum", alebo „KCCKB" je štátna príspevková organizácia zriadená Národným bezpečnostným úradom podľa § 21 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy

Hlavné úlohy:

- 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
  - systémov manažérstva
  - 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

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

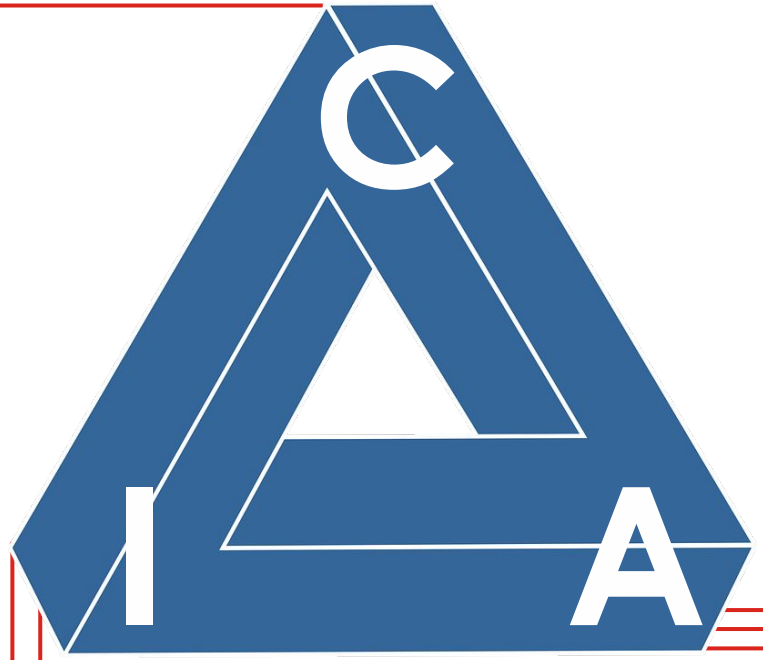
VŠEOBECNÝ VÝZNAM OCHRANY ÚDAJOV A INFORMÁCIÍ

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE
Z POHĽADU NORIEM A REGULÁCIE

ATRIBÚTY BEZPEČNOSTI INFORMÁCIÍ V ZDRAVOTNÍCTVE

Confidentiality (Dôvernosť):

- Záruka, že údaje alebo informácie nie sú prezradené neoprávneným subjektom alebo procesom
- Zdravotné údaje sú osobitnou kategóriou osobných údajov
- Môže ísť o naplnenie skutkovej podstaty trestného činu neoprávneného nakladania s osobnými údajmi



Availability (Dostupnosť)

- Záruka, že údaje alebo informácie sú pre používateľa, informačný systém, sieť, zariadenie alebo proces prístupné, keď sú potrebné a požadované
- Zdravotnícke informácie a zdravotné údaje musia byť kontinuálne dostupné
- Narušenie dostupnosti informácií má priamy vplyv na zdravotnícku starostlivosť

Integrity (Celistvosť)

- Záruka, že bezchybnosť, úplnosť alebo správnosť údajov alebo informácií neboli narušené
- Zdravotné údaje a informácie musia byť presné, správne a musia byť chránené pred neoprávneným pozmenením alebo zničením
- Chybné údaje a informácie môžu viesť ku ohrozeniu života a zdravia pacientov

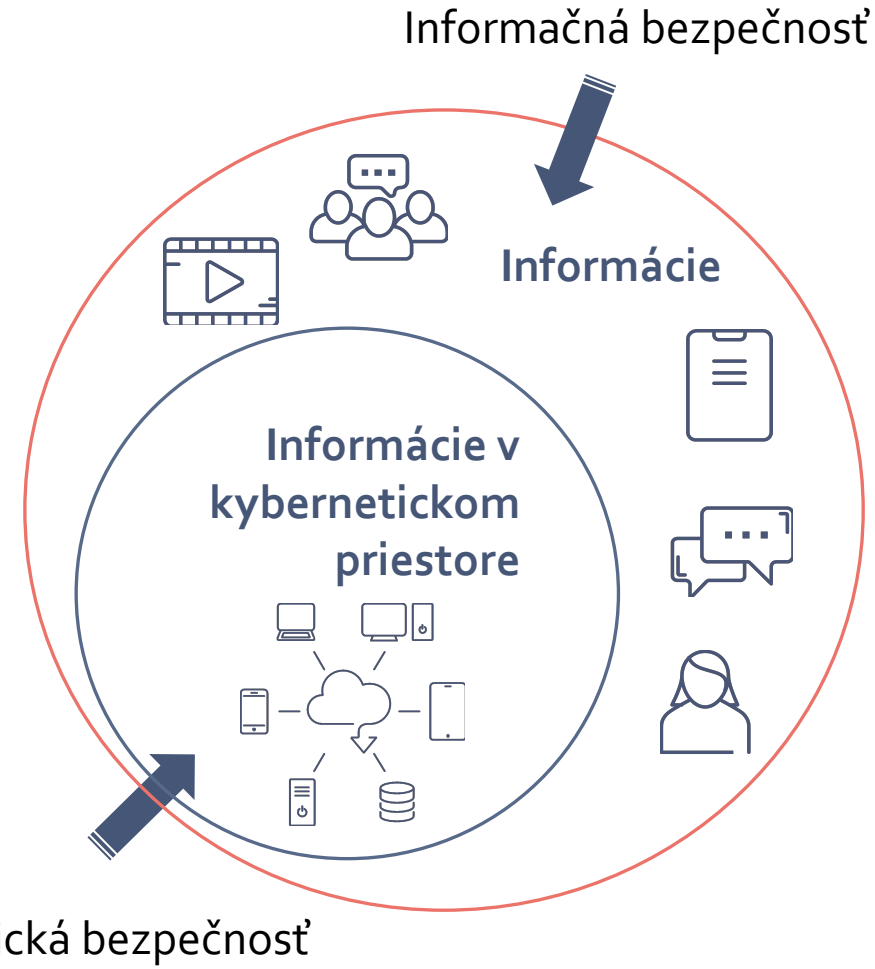
INFORMAČNÁ VS. KYBERNETICKÁ BEZPEČNOSŤ

[ISO/IEC 27032, čl. 2.33]

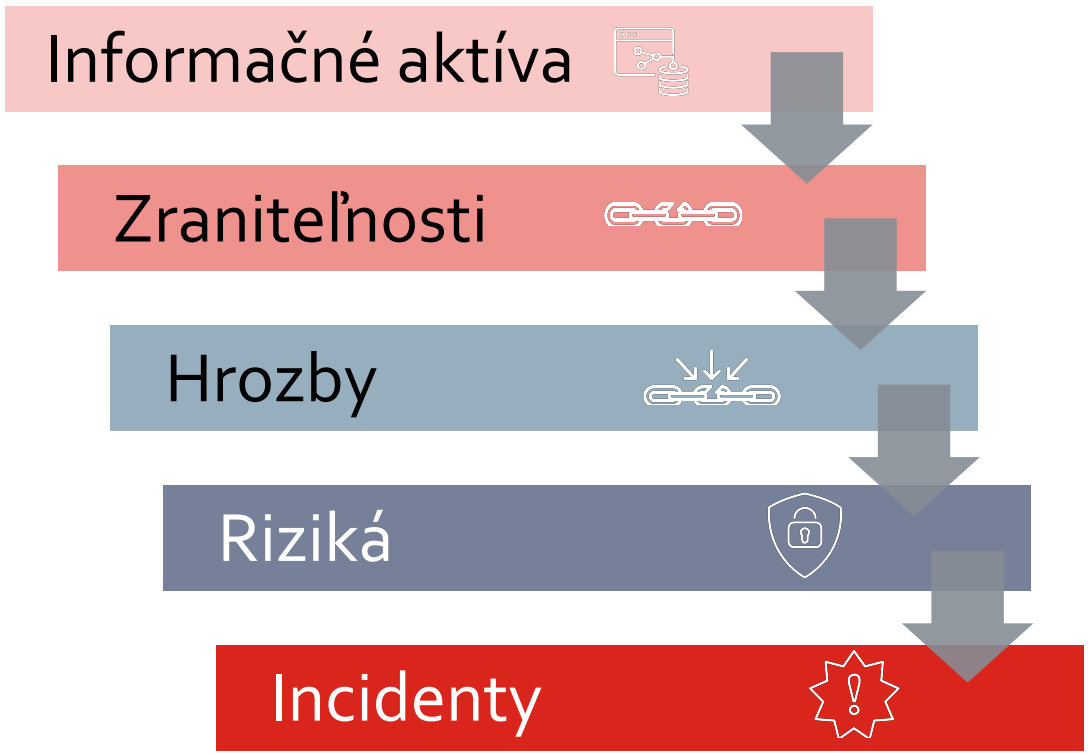
- Informačná bezpečnosť je zachovanie dôvernosti, integrity a dostupnosti informácií

[ISO/IEC 27032, čl. 4.20]

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



ŽIVOTNÝ CYKLUS INCIDENTU



Zraniteľnosť - slabé miesto informačného aktíva, slabina v informačnom systéme, v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb.

Hrozba - potenciál, že akákoľvek okolnosť či udalosť využije zraniteľnosť informačného aktíva a spôsobí negatívny následok (dopad)

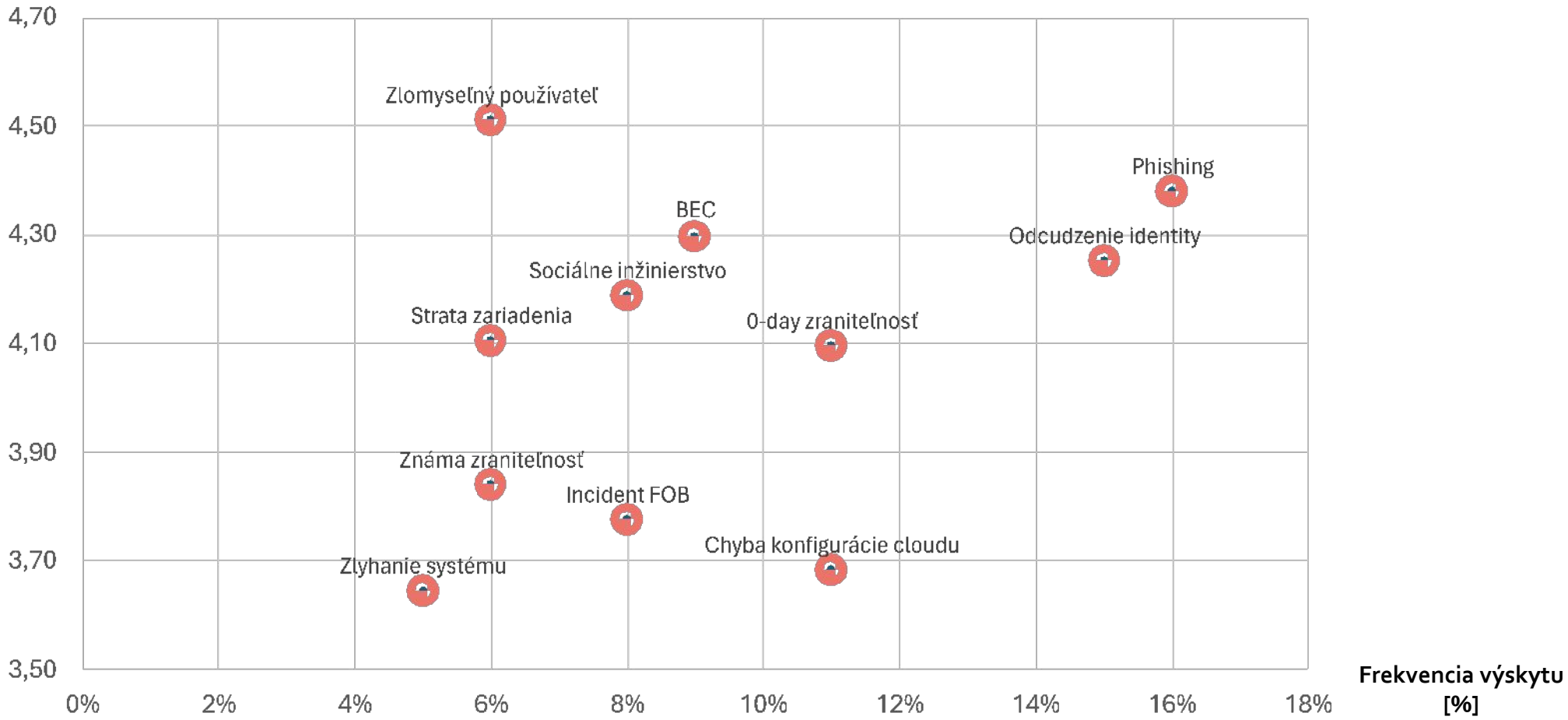
Riziko - funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody.

Incident - udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov

DOPAD A FREKVENCIA INCIDENTOV

Celosvetový priemer strát v roku 2023:

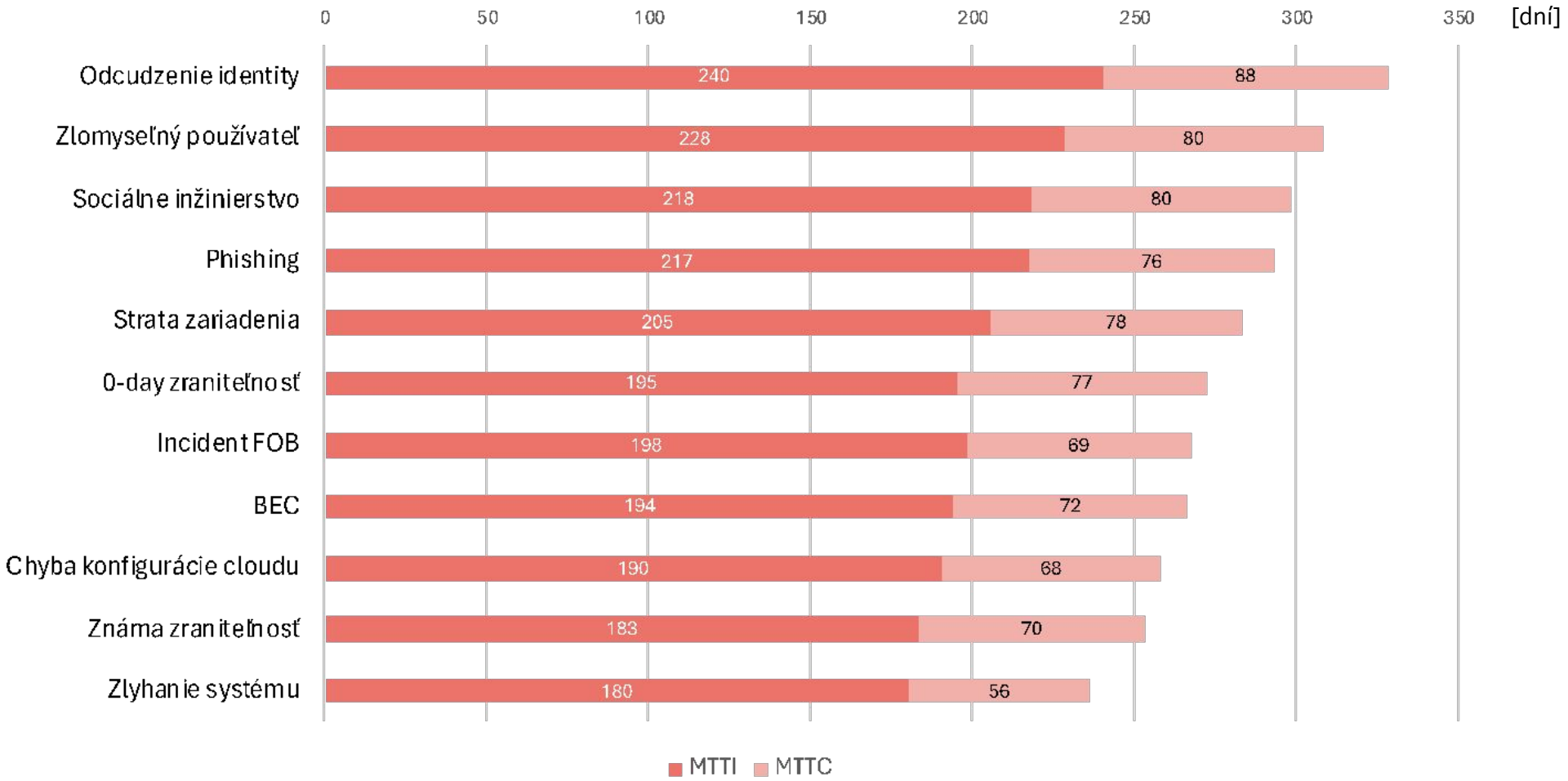
4,23 Mil EUR



Zdroj: Ponemon's Cost of Data Breach Report 2023

STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU PODĽA TYPU

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



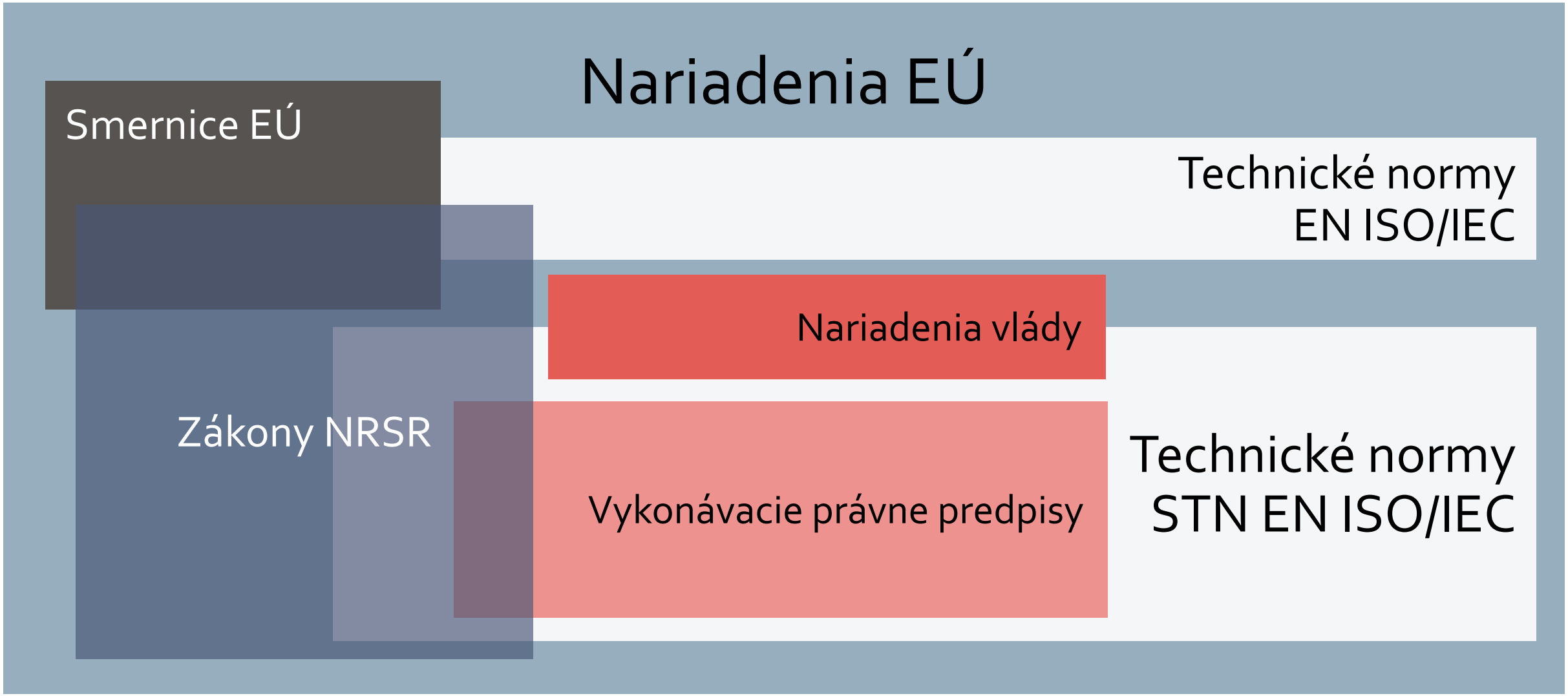
Zdroj: Ponemon Institute: The Cost of a Data Breach Report 2023

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

KDE SÚ UVEDENÉ POŽIADAVKY NA BEZPEČNOSŤ? (PRÁVNA ÚPRAVA)

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE
Z POHĽADU NORIEM A REGULÁCIE

HIERARCHIA PRÁVNYCH A TECHNICKÝCH PREDPISOV



PRÁVNE PREDPISY SR S DOSAHOM NA IB/KB

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

Zákon č. 483/2001 Z. z.
o bankách

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

Nariadenie (EÚ) 2017/745
o zdravotníckych pomôckach

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

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 umelej inteligencii

AI Act

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

CySol Act

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

eIDAS2

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

Cyber Security Act (CSA+)

Commission work programme 2024: https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2024_en

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

KDE SÚ UVEDENÉ POŽIADAVKY NA BEZPEČNOSŤ? (TECHNICKÉ NORMY)

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE
Z POHĽADU NORIEM A REGULÁCIE

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 KB:

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

TECHNICKÉ NORMY RELEVANTNÉ PRE KYBERBEZPEČNOSŤ V ZDRAVOTNÍCTVE

STN EN ISO/IEC 27002: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia - Riadenie informačnej bezpečnosti

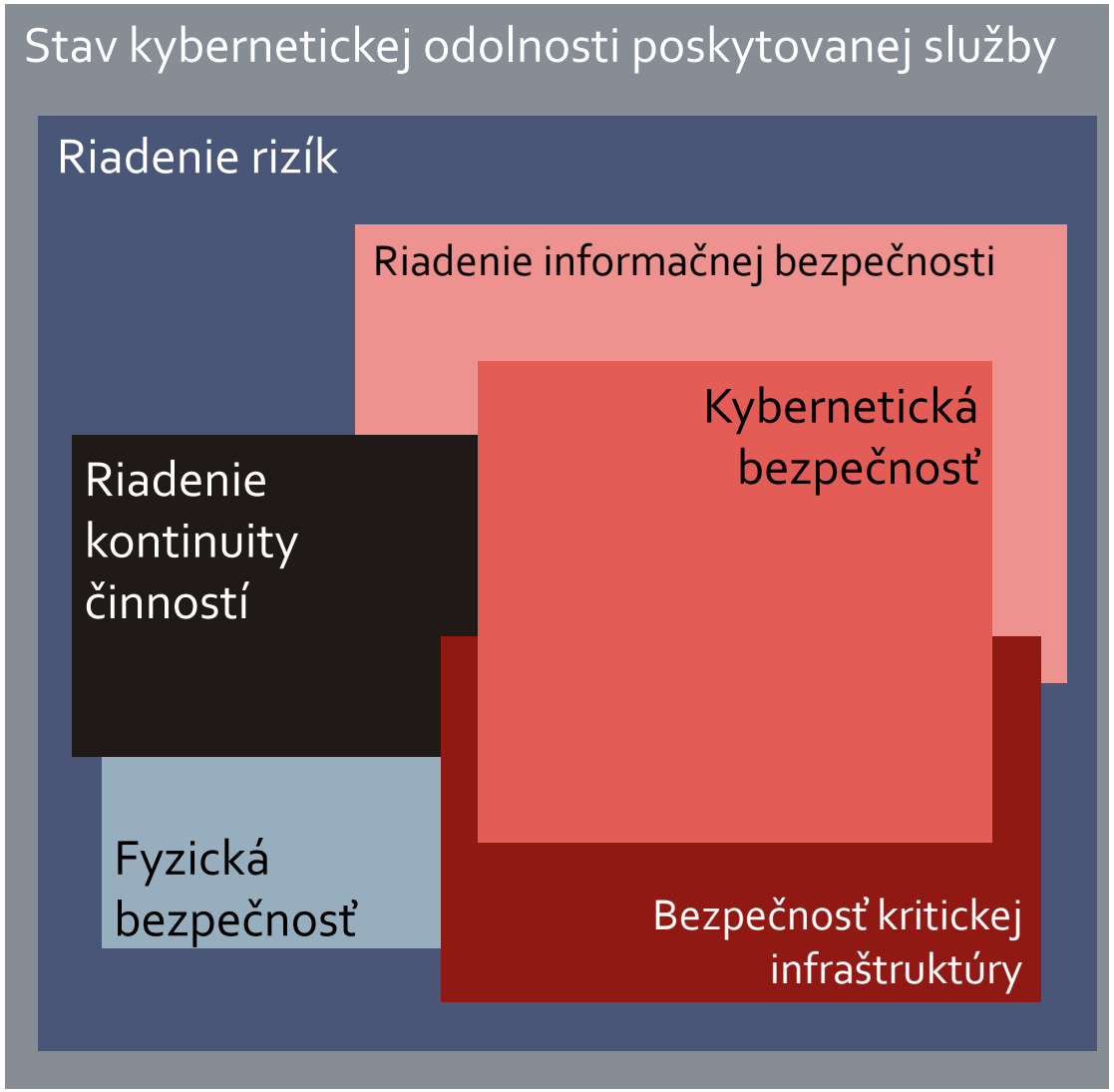
- ISO 7101:2023 Healthcare organization management - Management systems for quality in healthcare organizations - Requirements
- ISO 13131:2021 Health informatics — Telehealth services — Quality planning guidelines
- ISO 13606-4:2019 Health informatics — Electronic health record communication — Part 4: Security
- ISO 20301:2014 Health informatics — Health cards — General characteristics
- ISO 22388:2023 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents
- ISO 22857:2013 Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data
- ISO 27789:2021 Health informatics — Audit trails for electronic health records
- ISO 81001-1:2021 Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts
- ISO/IEC 24714:2023 Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance
- ISO/TR 11636:2009 Health Informatics — Dynamic on-demand virtual private network for health information infrastructure
- ISO/TR 21332:2021Health informatics — Cloud computing considerations for the security and privacy of health information systems
- ISO/TR 21548:2010 Health informatics — Security requirements for archiving of electronic health records — Guidelines
- ISO/TS 17975:2022 Health informatics — Principles and data requirements for consent in the collection, use or disclosure of personal health information
- ISO/TS 21547:2010 Health informatics — Security requirements for archiving of electronic health records — Principles
- ISO/WD 27799 Health informatics — Information security management in health using ISO/IEC 27002

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

AKO SA VYKONÁVA KYBERBEZPEČNOSŤ?

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE
Z POHĽADU NORIEM A REGULÁCIE

KYBERBEZPEČNOSTNÉ DOMÉNY



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

DEFINÍCIA BEZPEČNOSTNÉHO OPATRENIA

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

- **Úlohy, procesy, roly a technológie** v organizačnej, personálnej, fyzickej 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 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

ROZDELENIE BEZPEČNOSTNÝCH OPATRENÍ PODĽA KATEGÓRIE

- **Technické opatrenia**
  - Opatrenia na zníženie rizík pomocou prostriedkov technologickej povahy
- **Organizačné opatrenia**
  - Opatrenia na zníženie rizík pomocou zmien procesov
- **Personálne opatrenia**
  - Opatrenia týkajúce sa riadenia ľudských zdrojov
- **Fyzické opatrenia**
  - Opatrenia na zníženie rizík pomocou prostriedkov fyzickej povahy a zmenami prostredia

Efektívnu bezpečnosť je možné dosiahnuť
LEN POMOCOU KOMBINÁCIE
rôznych typov opatrení

ROZDELENIE BEZPEČNOSTNÝCH OPATRENÍ PODĽA ÚČELU

- **Preventívne**
  - Opatrenia ktoré majú preventívne brániť vzniku kybernetických bezpečnostných incidentov

- **Detekčné**
  - Opatrenia, ktoré majú nastať v prípade výskytu incidentu a slúžia na zistenie jeho príčin

- **Nápravné**
  - Opatrenia, ktoré pôsobia pri vzniku incidentu a slúžia na zotavenie systému alebo organizácie z incidentu

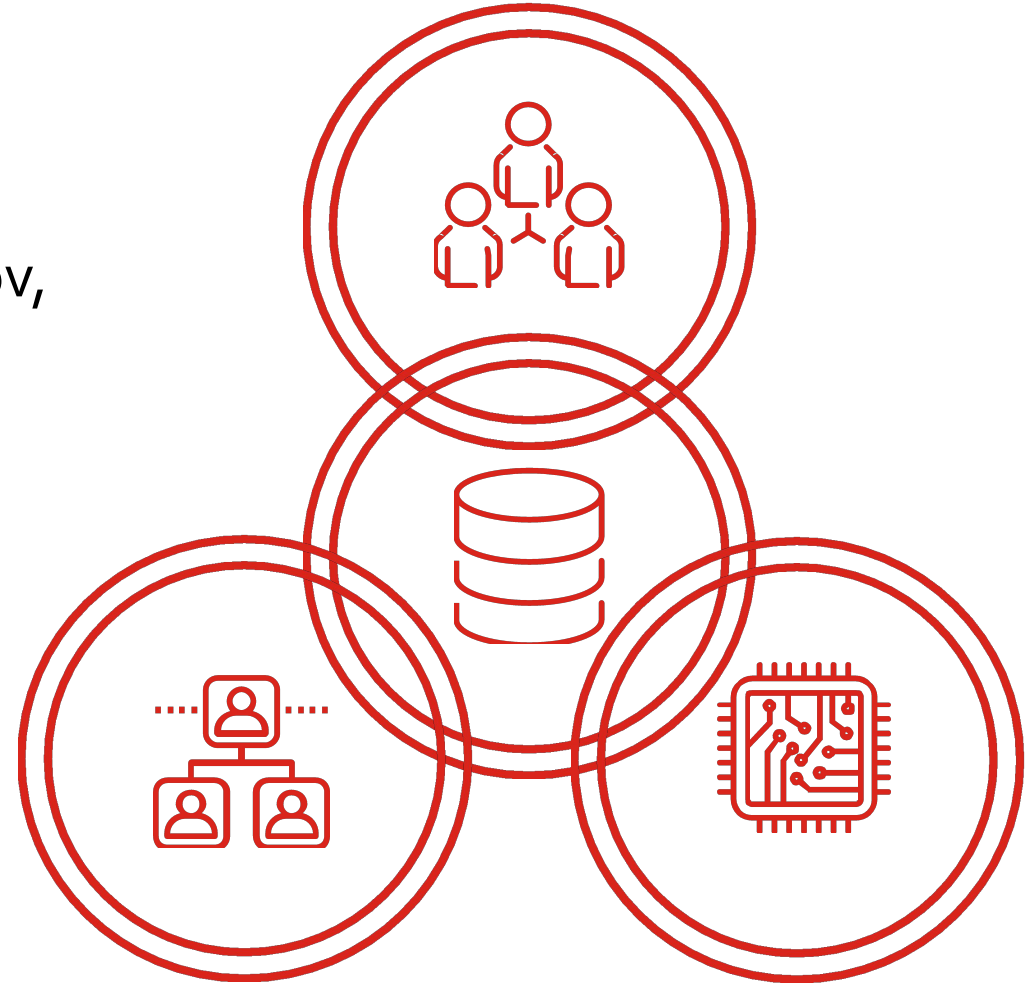
NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

KYBERBEZPEČNOSŤ V KONTEXTE ZDRAVOTNÍCTVA

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE
Z POHĽADU NORIEM A REGULÁCIE

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



TECHNOLOGICKÉ PRVKY KYBERNETICKÉHO PRIESTORU V ZDRAVOTNÍCTVE

- **Zdravotnícke technológie** hrajú kľúčovú úlohu vo všetkých aspektoch pacientskej starostlivosti
- **Zdravotnícke pomôcky** sú rozmanitou skupinou produktov, ktoré sa využívajú v zdravotníctve pre diagnózu, monitorovanie, liečbu alebo prevenciu ochorení - z hľadiska kategorizácie v IKT ide typicky najmä o:
  - prístroje,
  - zariadenia,
  - softvérové aplikácie a systémy,
  - hardvérové zariadenia (vrátane implantátov a IoT zariadení),

ZRANITEĽNÉ KATEGÓRIE ZDRAVOTNÍCKYCH TECHNOLÓGIÍ

- **Diagnostické a zobrazovacie technológie**: zariadenia určené na identifikáciu a spresnenie podstaty ochorení alebo iných zdravotných stavov
- **Terapeutické technológie**: zariadenia používané na liečbu ochorení alebo zranení
- **Monitorovacie technológie**: zariadenia a systémy na sledovanie zdravotného stavu pacienta v reálnom čase
- **Mobilné zdravotnícke technológie**: zariadenia a aplikácie pre monitorovanie a správu zdravotného stavu na diaľku
- **Laboratórne technológie**: Elektronické zariadenia používané v laboratóriách pre analýzu vzoriek a diagnostiku
- **Zdravotnícke informačné systémy**: Systémy pre správu zdravotníckych informácií, vrátane elektronických zdravotných záznamov a systémy pre správu pacientov a koordináciu zdravotnej starostlivosti

PRÍKLADY ZRANITEĽNOSTÍ ZDRAVOTNÍCKYCH TECHNOLÓGIÍ PODĽA ATRIBÚTOV CIA

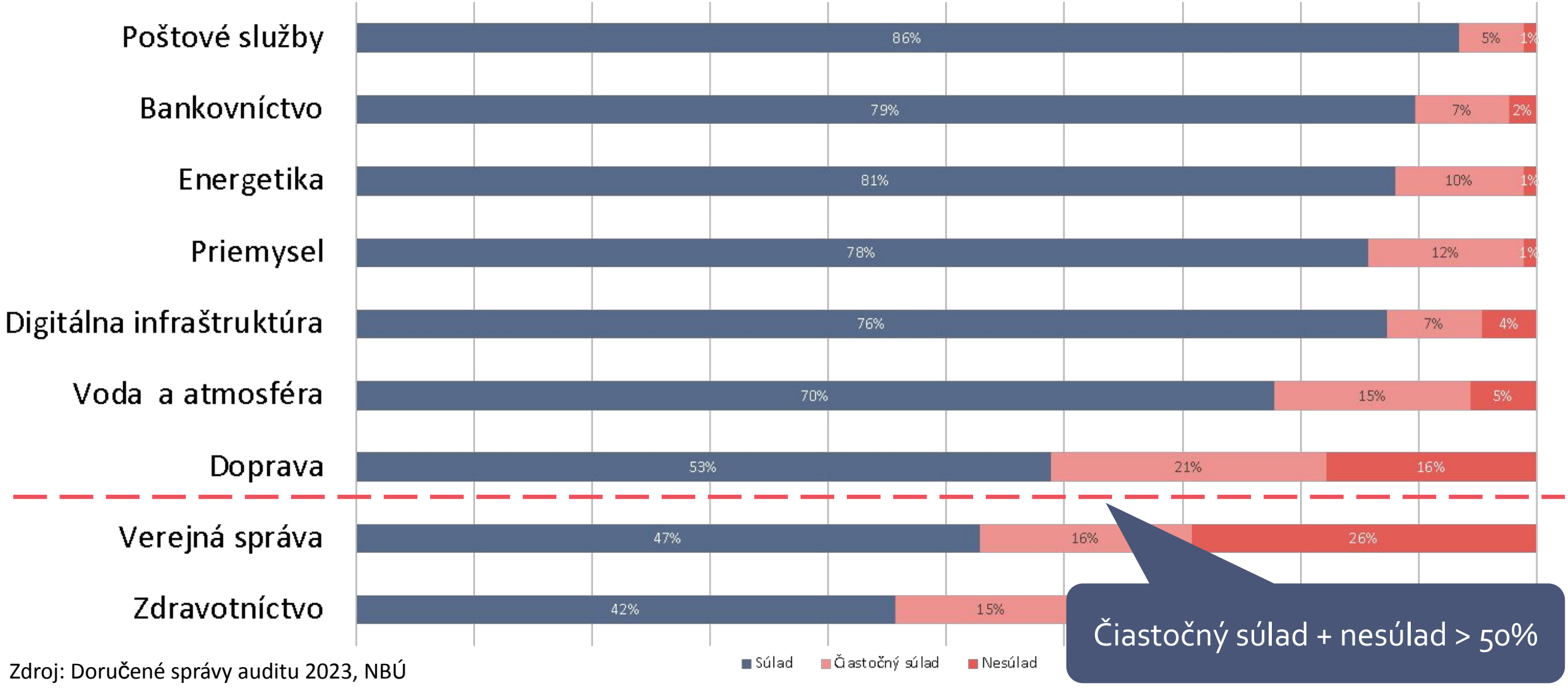
Dôvernosť	Dostupnosť	Integrita
Možné dopady narušenia dôvernosti pacientskych dát a zdravotníckych informácií	**Možné dopady obmedzenia alebo prerušenia prístupu k medicínskym systémom a technológiám**	**Možné dopady manipulácie s údajmi alebo manipulácie s funkciou zariadení:**
• porušenie práva na súkromie pacienta	• ovplyvnenie proces liečby s vážnymi následkami na zdravie pacienta	• obmedzenie poskytovania medicínskych služieb
• možné konanie o ochrane osobných údajov zo strany Úradu na ochranu osobných údajov	• obmedzenie alebo prerušenie poskytovania medicínskych služieb	• ovplyvnenie diagnostického procesu
• môže ísť o naplnenie skutkovej podstaty trestného činu neoprávneného nakladania s osobnými údajmi	• obmedzenie alebo zabránenie prístupu k diagnostickým systémom	• nesprávna diagnóza
	• obmedzenie alebo zabránenie prístupu k monitorovacím systémom	• nesprávna liečba
	• oneskorenia v diagnostike	• ohrozenie pacientovej bezpečnosti, života a zdravia
	• oneskorenie v liečbe	• presnosť laboratórnych výsledkov zásadne ovplyvňuje stanovenie diagnózy
	• prerušenie poskytovania liečby (v niektorých prípadoch aj s vážnym ohrozením života a zdravia pacienta)	

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ZÁVER

KYBERBEZPEČNOSTNÉ MINIMUM V ZDRAVOTNÍCTVE
Z POHĽADU NORIEM A REGULÁCIE

SÚLAD PODĽA ODVETVÍ 2023



Zdroj: Doručené správy auditu 2023, NBÚ

AUDITY KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKOM ZDRAVOTNÍCTVE

TYPICKÉ NEGATÍVNE ZISTENIA:

- **Nedostatočné riadenie rizík**: chýbajúce procesy riadenia rizík; chýbajúci inventár aktív, chýbajúca klasifikácia údajov
- **Chýbajúci bezpečnostný monitoring**: citlivé zdravotnícke informácie, ako sú osobné údaje pacientov, zdravotné záznamy a finančné informácie, sú vystavené rizikám; chýba monitorovanie neoprávnených prienikov, aj úniku dát
- **Nedostatočná vyspelosť dodávateľských vzťahov**: neformálne vzťahy s dodávateľským reťazcom; zmluvy ani SLA neobsahujú ustanovenia o bezpečnosti
- **Chýbajúce procesy riadenia kontinuity**: zvyšujú sa útoky pomocou ransomvéru; bez BCM procesov to môže pozastaviť poskytovanie zdravotníckej starostlivosti
- **Zraniteľnosti komplexných systémov a nových technológií**: zvýšená integrácia a zložitosť informačných systémov v zdravotníctve (vrátane telemedicíny a IoT) spôsobuje, že zlyhanie alebo zraniteľnosť jedného systému môže mať reťazové dôsledky na celú organizáciu
- **Nedostatočné bezpečnostné povedomie**: zdravotníckym pracovníkom sa nedostáva dostatočná odborná príprava na to, aby získali spôsobilosť rozpoznať a adekvátne reagovať na kybernetické hrozby

POZITÍVNE ZISTENIA:

- Bezpečnostná dokumentácia už mnohokrát dosahuje dostatočnú úroveň vyspelosti
- Väčšinou je určený Manažér kybernetickej bezpečnosti
- Sieťová bezpečnosť v posledných rokoch výrazne stúpa na vyspelosti

RÁMEC A CIEĽOVÉ SKUPINY VZDELÁVANIA V KB

Druh ďalšieho vzdelávania	Cieľová skupina	Typické dotknuté roly
Ďalšie odborné vzdelávanie	IB/KB	manažér KB, audítor KB, architekt KB, špecialista KB, analytik KB…
Upskilling, teoretické základy KB	Informatici	IT manažér, správca systému, vývojár SW, IT architekt, operátor, databázový špecialista…
Zvyšovanie digitálnej gramotnosti	Odborní zamestnanci	všetky pracovné roly, ktoré používajú k práci prostriedky IKT, s dôrazom na riadiacich zamestnancov
Zvyšovanie bezpečnostného povedomia	Všetci zamestnanci	všetky pracovné roly

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

Spolufinancovaný Európskou úniou

ZHRNUTIE

- Hlavným dôvodom pre ochranu údajov a informácií by malo byť uvedomenie si rizík

- Dokumentácia na zaručenie bezpečnosti nestačí!
  - nutné sú opatrenia:
    - #preventívne
    - # detekčné
    - # nápravné

  - v oblasti:
    - # technologickej
    - # organizačnej
    - # personálnej
    - # fyzickej

- Jedným z nepriamych opatrení v personálnej bezpečnosti je aj zvyšovanie kvalifikácie a zvyšovanie bezpečnostného povedomia

Spolufinancovaný Európskou úniou

NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Financované Európskou úniou

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.