Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

BEZPEČNOSTNÉ OPATRENIA V KYBERNETICKEJ BEZPEČNOSTI

KDE ZAČAŤ?

Webinár Kyberaliancia, Bratislava, 29.4.2025

Ing. Tomáš Hettych CISA, CISM, CRISC, CDPSE, CGEIT

Člen predstavenstva KCCKB

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
- 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

NOVELA ZÁKONA č. 69/2018 Z. z. o KYBERNETICKEJ BEZPEČNOSTI

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

Nariadenie (EÚ) 2024/2487
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

Spolufinancovaný Európskou úniou

TRANSPOZÍCIA NIS2 A NADVÄZUJÚCA REGULÁCIA

Transpozícia smernice (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (**smernica NIS 2**)

Stav kľúčovej legislatívy

- (Transpozičná) novela Zákona č.69/2018 Z.z. – učinná od 1.1.2025
- Vykonávacie nariadenie EK č. 2024/2690 – účinnosť od 17.10.2024
- DORA nariadenie č. 2022/2554 – účinnosť od 17.1.2025

Spolufinancovaný Európskou úniou

KĽÚČOVÉ ZMENY

- **Rozšírenie** pôsobnosti zákona **na nové subjekty**
- **Identifikácia regulovaného subjektu** na základe jeho zaradenia do sektora
- **Aplikácia bezpečnostných opatrení** na základe analýzy rizík
- **Úprava bezpečnosti dodávateľského reťazca**
- **Úprava hlásenia incidentov**
- Koordinované zverejňovanie zraniteľností
- Audit a samohodnotenie
- **Certifikácia** bezpečnosti IKT produktov a služieb

PREVÁDZKOVATEĽ ZÁKLADNEJ SLUŽBY (PZS)

- **ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou,**
- **kritický subjekt,**
- **štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch a vyšší územný celok,** ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- **mesto,** ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- **správca ITVS** po predchádzajúcej konzultácii s príslušným ústredným orgánom,
- **osoba, ktorá poskytuje službu registrácie názvu domény** bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo
- **tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti,** má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu

ZOZNAM SEKTOROV

Smernica NIS (1)	Zákon č. 69/2018 Z.z.	Smernica NIS2	
		Kľúčové subjekty	Dôležité subjekty
Bankovníctvo	Bankovníctvo	Bankovníctvo	
Dodávka a distribúcia pitnej vody	Dodávka a distribúcia pitnej vody	Dodávka a distribúcia pitnej vody	
Doprava	Doprava	Doprava	
Energetika	Energetika	Energetika	
Infraštruktúra finančných trhov	Infraštruktúra finančných trhov	Infraštruktúra finančných trhov	
Digitálna infraštruktúra	Digitálna infraštruktúra		Poskytovatelia digitálnych služieb
	Elektronické komunikácie		Elektronické komunikácie
	Pošta		Poštové a kuriérske služby
	Priemysel		Priemysel
	Verejná správa	Verejná správa	
	Voda a atmosféra		Voda a atmosféra
	Zdravotníctvo	Zdravotníctvo	
		Odpadová voda	
		Riadenie služieb IKT	
		Vesmír	
			Odpadové hospodárstvo
			Výroba a distribúcia chemických látok
			Výroba iných dopravných prostriedkov
			Výroba elektrických strojov a zariadení
			Výroba motorových vozidiel
			Výroba počítačových elektronických a optických výrobkov
			Výroba, distribúcia a spracovanie potravín
			Výroba zdravotníckych pomôcok
			Výskum

APLIKÁCIA BEZPEČNOSTNÝCH OPATRENÍ

- Nová štruktúra všeobecných bezpečnostných opatrení (§20 ods. 1 a 2)
- **Rozsah a spôsob implementácie bezpečnostných opatrení na základe analýzy rizík**
- **Povinnosť zaviesť bezpečnostné opatrenia do 12 mesiacov odo dňa zápisu do registra PZS**
- **Aplikovateľné bezpečnostné štandardy:**
  - Všeobecné - Vyhláška, ktorou sa ustanovuje sa ustanovuje obsah bezpečnostných opatrení … – štandard pre IT systémy a osobitný štandard pre OT systémy (V PRÍPRAVE)
  - Sektor verejná správa - Zákon o ITVS a príslušná vyhláška
  - Finančný sektor - DORA a príslušné RTS(es)
  - Digitálne sektory – Vykonávacie nariadenie EK č. 2024/2690

BEZPEČNOSTNÉ OPATRENIA

DEFINÍCIA BEZPEČNOSTNÉHO OPATRENIA

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

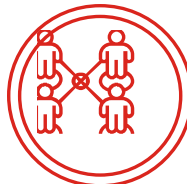
- **Úlohy, procesy, roly a technológie**
  - v #organizačnej, #personálnej #fyzickej a #technologickej oblasti
- ktorých cieľom je
  - dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií

Prevádzkovateľ základnej služby je povinný prijať a dodržiavať:

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

GENERICKÉ ROZDELENIE OPATRENÍ

- **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

Spolufinancovaný Európskou úniou

PREVENTÍVNE OPATRENIA (výber)

- Aktualizácia a záplaty (Patch management) – aktualizácia firmvérov, operačných systémov, aplikácií
- Ochrana pracovných staníc (Endpoint security) – antivírus, antispam, antimalvér
- Silné heslá (Password management) – rôzne heslá pre rôzne systémy, komplexné heslá, špeciálne znaky, časté zmeny
- Viacstupňové prihlasovanie (Multifactor authentication) – používanie kombinácie viacerých spôsobov prihlasovania
- Zálohovanie a kontrola obnovy (Backup and recovery) – pravidelne, rôzne miesta a spôsoby
- Vzdelávanie, šifrovanie komunikácie, atď.

Spolufinancovaný Európskou úniou

REAKTÍVNE OPATRENIA

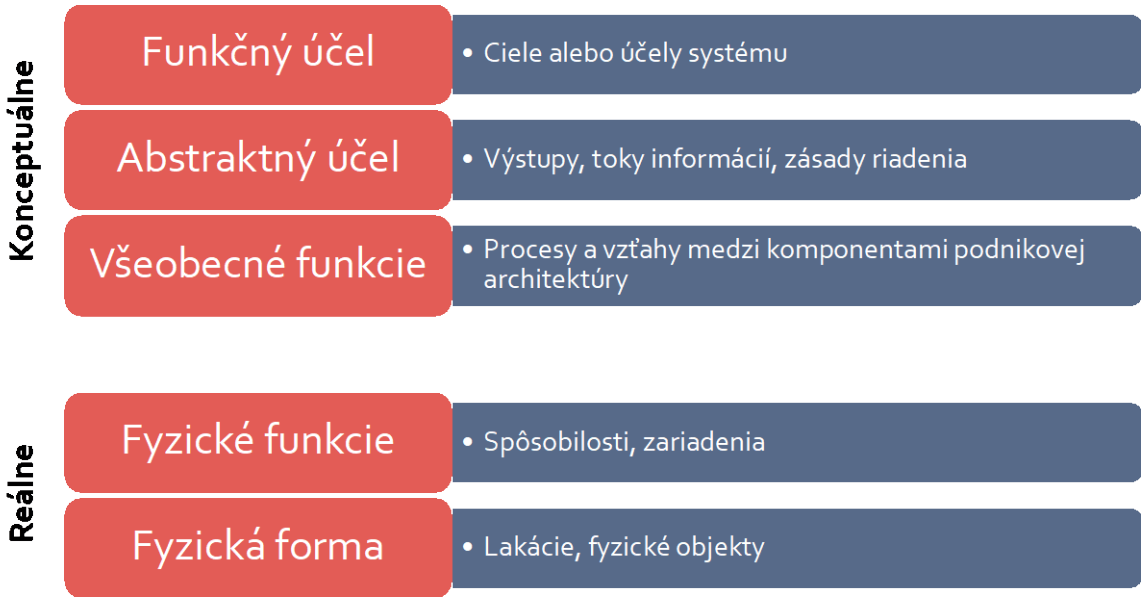
- Plány kontinuity a obnovy
  - Business Continuity Plan (BCP)
  - Disaster Recovery Plan (DRP)
- Riadenie incidentov (Incident management) – komplexný systém pre identifikáciu, klasifikáciu, riešenie a reporting incidentov
- Analýza rizík (Risk analysis)
- Analýza dopadov (Business Impact Analysis)
- Zverejňovanie zraniteľností
- Pravidelný audit

Spolufinancovaný Európskou úniou

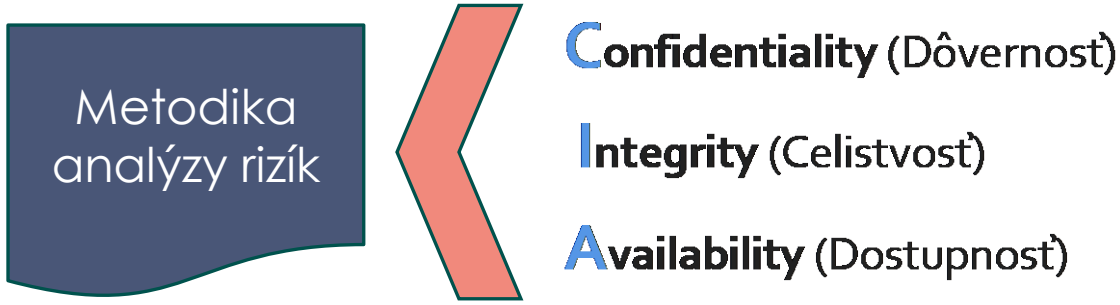
IMPLEMENTÁCIA POŽIADAVIEK KB

KDE ZAČAŤ S IMPLEMENTÁCIOU? (1/2)

1. Identifikácia informačných aktív:



2. Analýza rizík:



KDE ZAČAŤ S IMPLEMENTÁCIOU? (2/2)

3. Analýza dopadov (BIA – Business Impact Analysis)
4. Identifikované najväčšie riziká sú zároveň scenármi pre riadenie kontinuity
5. Prioritizácia
   - Postupy pre riešenie a nahlasovanie incidentov
   - Plány kontinuity (BCP) a obnovy (DRP)
6. Zapojenie najvyššieho vedenia organizácie do procesov
7. Otvorenosť a transparentnosť pri príprave podkladov

OTÁZKY?

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

www.cybercompetence.sk, kyberkomunita.sk

www.linkedin.com/company/cybercompetence

@CybercenterSk