Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI

BEZPEČNOSTNÉ OPATRENIA A CIELE BEZPEČNOSTI

NIS2 Roadshow, Bratislava 12.11.2024

Ivan Makatura

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:

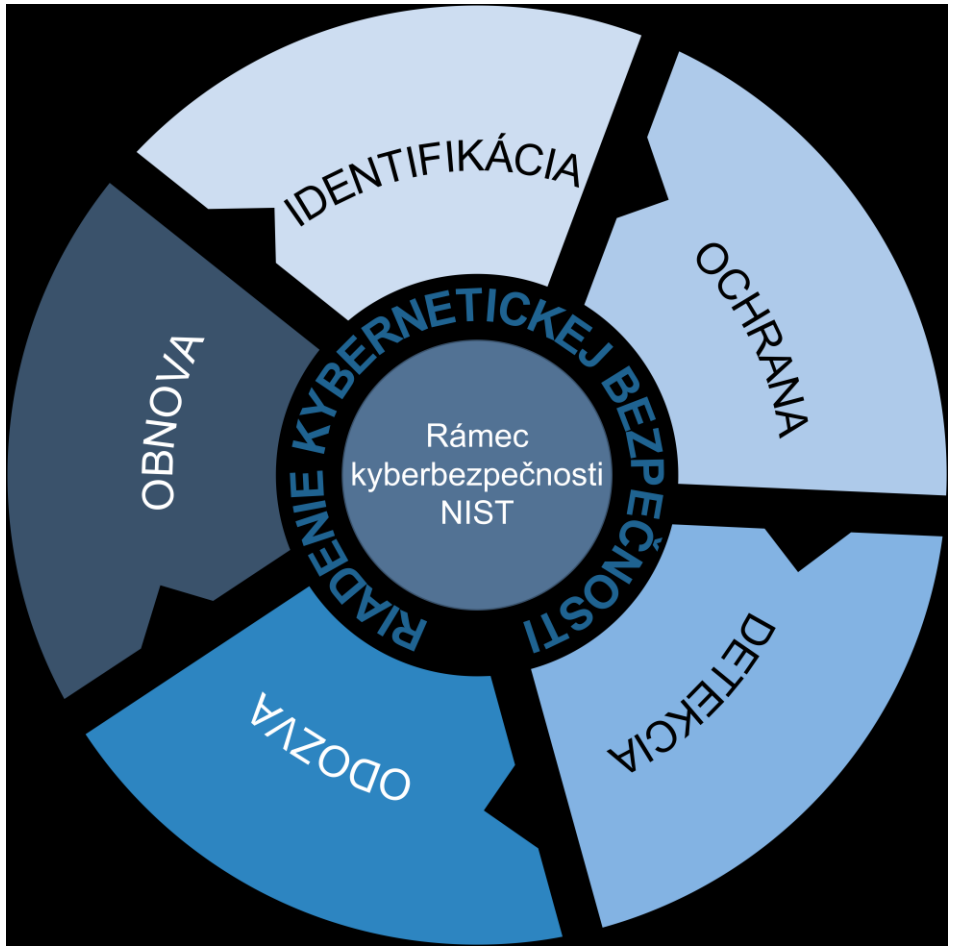
- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií
- **Certifikácia** audítorov a manažérov kybernetickej bezpečnosti
- **Vzdelávanie dospelých** v kybernetickej bezpečnosti
- Organizácia kampaní 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

Spolufinancovaný Európskou úniou

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

ČO

NIST CYBERSECURITY FRAMEWORK



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

- **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

Spolufinancovaný Európskou úniou

TYPICKÉ OBJEKTÍVNE DÔVODY PRE RIADENIE BEZPEČNOSTNÉHO RIZIKA

PREČO

OCHRANA DUŠEVNÉHO VLASTNÍCTVA 48%

OBAVA Z VÝPADKU PRODUKCIE 63%

OCHRANA REPUTÁCIE 21%

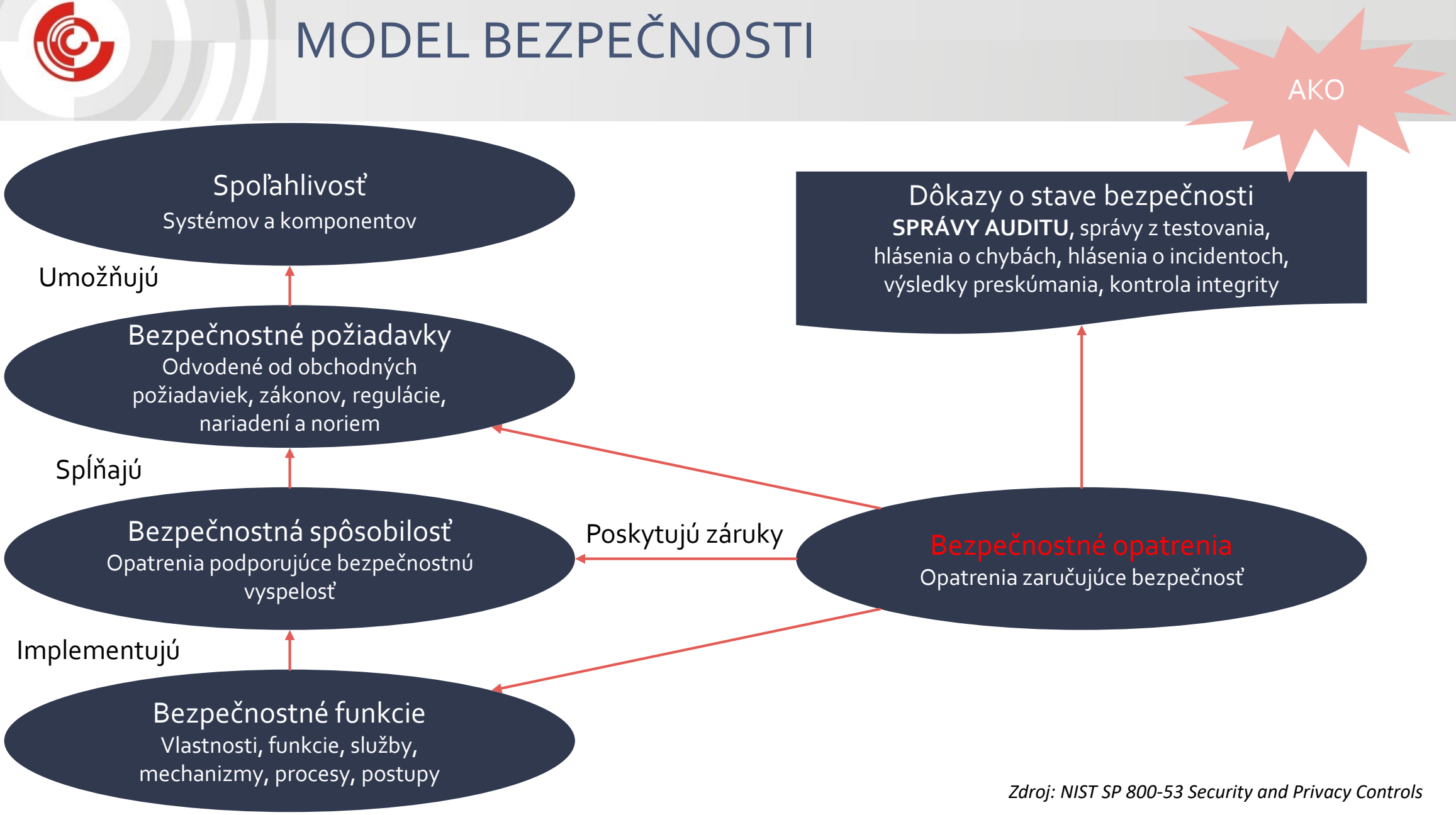
POŽIADAVKY NA SÚLAD 62%

KRITICKÁ INFRAŠTFUKTÚRA 11%

Zdroj: Ponemon's 2016 Application Security Risk Study

Spolufinancovaný Európskou úniou

MODEL BEZPEČNOSTI



Zdroj: NIST SP 800-53 Security and Privacy Controls

DEFINÍCIA BEZPEČNOSTNÉHO OPATRENIA

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

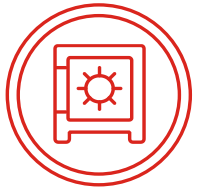
- **Úlohy, procesy, roly a technológie** v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

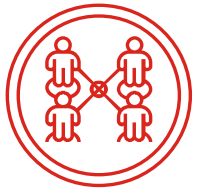
V zmysle § 19 (1) Prevádzkovateľ základnej služby je povinný do dvanástich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať:

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

GENERICKÉ ROZDELENIE OPATRENÍ

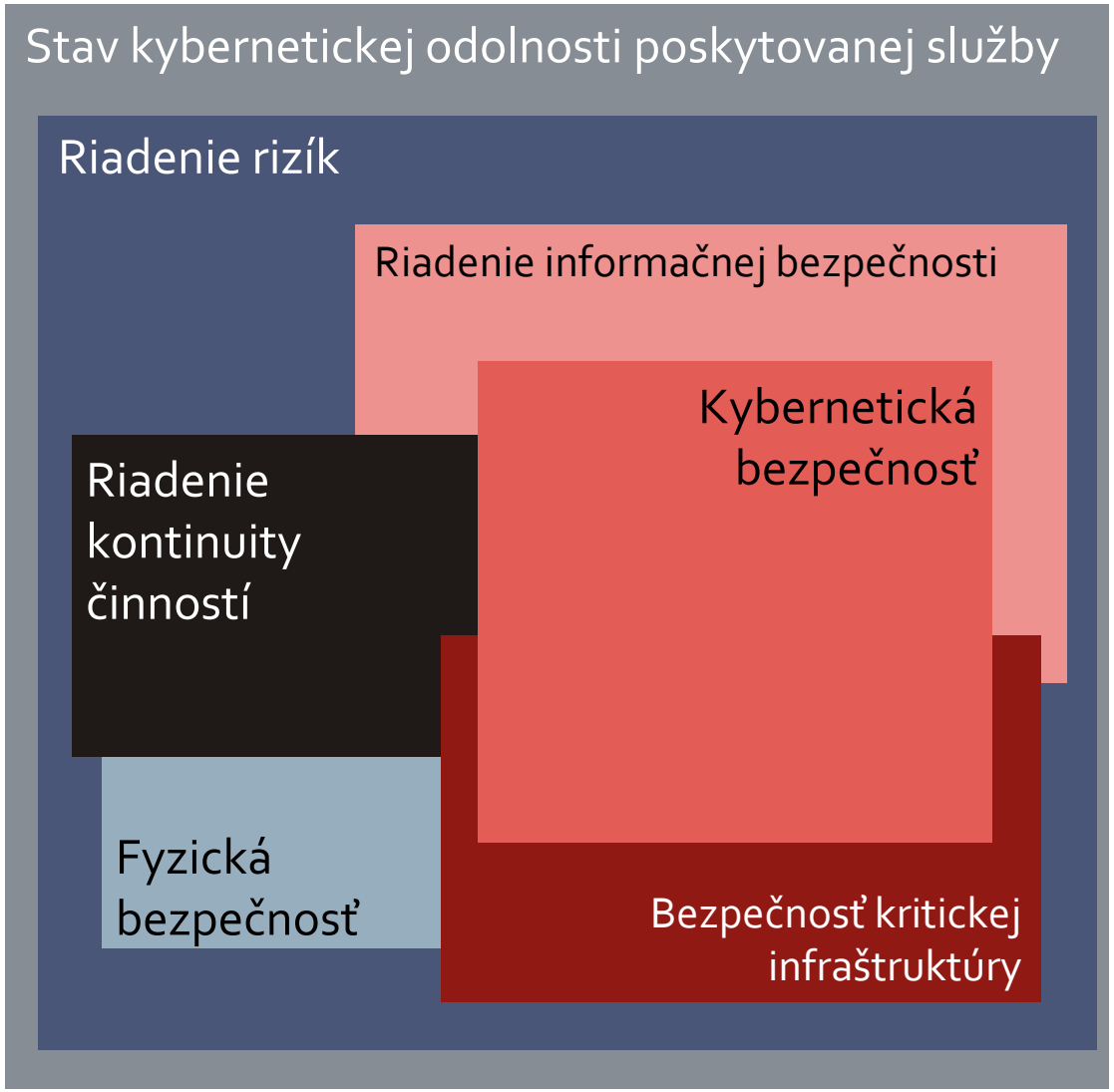
- **TECHNOLOGICKÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov technologickej povahy
- **FYZICKÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej povahy
- **ORGANIZAČNÉ OPATRENIA**
  - opatrenia na zníženie bezpečnostných rizík 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

KYBERBEZPEČNOSTNÉ DOMÉNY VS. DOBRÁ PRAX



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

PLATNÉ A PRIPRAVOVANÉ SEKTOROVÉ OPATRENIA

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

Po novele zákona sa výraznejšie uplatní právna doktrína „**Lex specialis derogat legi generali**"

Doteraz bola táto doktrína platná, avšak de-facto sa neuplatnila v aplikačnej praxi:

§ 19 (1): Prevádzkovateľ základnej služby je povinný ... prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu všeobecných bezpečnostných opatrení podľa § 20 **a sektorové bezpečnostné opatrenia, ak sú prijaté**.

ABSTRAKTNÝ AUDIT CHECKLIST PO NOVELE ZÁKONA

Opatrenie	Vyhláška č. 362/2018 Z.z.	Vyhláška č. 179/2020 Z.z.	Vykonávacie nariadenie EK Digital	RTS DORA	Iné vyhlášky o sektorových opatreniach	Auditované opatrenia (príklad: banka)
1	✓			✓		✓
2	✓			✓		✓
3	✓	✓		✓	✓	✓
4	✓	✓			✓	✓
5	✓	✓	✓		✓	✓
6	✓	✓			✓	✓
7	✓	✓				✓
8	✓	✓	✓			✓
9	✓	✓		✓		✓
.	✓		✓	✓		✓
.	✓		✓	✓		✓
.	✓		✓	✓		✓
.	✓		✓			✓
269	✓		✓			✓

Spolufinancovaný Európskou úniou

ZHRNUTIE K NOVELE ZÁKONA

- Slovensko už pri transpozícii pôvodnej Smernice NIS išlo s požiadavkami nad rámec smernice - novela zákona o kybernetickej bezpečnosti preto nie je revolúcia, ale evolúcia
- Väčšina všeobecne záväzných právnych predpisov (vrátane sektorových opatrení) je inšpirovaná uznanými technickými normami (najmä EN ISO/IEC 27002:2022)
- Pri praktickej implementácii opatrení nie je potrebné bezpodmienečne riadiť detailom právnych predpisov
  - existuje množstvo použiteľných technických noriem – legislatívci nevynašli koleso
  - podstatný je účinok primeraného opatrenia
- Pozitíva novely v kontexte bezpečnostných opatrení:
  - zdôrazňujú sa špecifiká odvetví
  - zlepšia sa procesy riadenia hrozieb a rizík, zavádza sa koordinované zverejňovanie zraniteľností
  - rozšírením pôsobnosti zákona na dodávateľské reťazce sa zvýši celková úroveň odolnosti voči hrozbám
  - zvýši sa miera kooperácie a komunikácie ohľadom hrozieb a rizík
  - zavádzajú sa mechanizmy bezpečnostnej certifikácie výrobkov, procesov a služieb

Spolufinancovaný Európskou úniou

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

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