UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2025

Vecné pripomienky

k pripravovanému návrhu Vyhlášky MIRRI SR, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správ

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

1 Úvod ... 2
2 Oblasti podnetov a návrhov ... 3
2.1 Vymedzenie kategórií a požiadaviek pre jednotlivé subjekty verejnej správy ... 3
2.2 Nerealizovateľnosť niektorých požiadaviek pre menších správcov ... 3
2.3 Absencia rozsahu údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT ... 4
2.4 Chýbajúce rozšírené požiadavky na nové informačné technológie ... 4
2.5 Súlad s inými vykonávacími právnymi predpismi ... 5
2.6 Zapracovať opatrenia týkajúce sa koordinovaného oznamovania a zverejňovania bezpečnostných zraniteľností ... 5
2.7 URL v texte vyhlášky ... 6
3 Medzinárodný štandard ISO/IEC 27002:2022 ... 7
3.1 Kontakt s odbornými záujmovými skupinami ... 7
3.2 Spravodajstvo o hrozbách (Threat intelligence) ... 8
3.3 Overovanie spoľahlivosti pred nástupom do zamestnania ... 8
3.4 Bezpečnosť informácií pri využívaní cloudových služieb ... 8
3.5 Vymazanie informácií ... 9
3.6 Maskovanie údajov (Data masking) ... 9
3.7 Prevencia úniku údajov (Data leakage prevention) ... 9
3.8 Bezpečné programovanie (Secure coding) ... 9
3.9 Práca na diaľku (Remote working) ... 10
3.10 Riadenie kryptografických kľúčov (Key management) ... 10
3.11 Autentifikačné informácie ... 10
3.12 Koordinované oznamovanie a zverejňovanie zraniteľností (coordinated vulnerability disclosure) ... 11
Použité zdroje ... 12

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1 ÚVOD

Univerzita Pavla Jozefa Šafárika v Košiciach (ďalej len „UPJŠ“) prostredníctvom Kompetenčného centra kybernetickej bezpečnosti na UPJŠ (ďalej len „KC KB UPJŠ“) si dovoľuje reagovať na predbežnú informáciu zo dňa 5.8.2025 o začatí prípravy návrhu Vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“), ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správ (ďalej len „Návrh vyhlášky“). Predkladateľ súčasne uvádza, že zmien je toľko, že upúšťa od zmien č. 179/2020 Z. z. (ďalej len „Vyhláška č. 179/2020 Z. z.“) a pripravuje nový všeobecne záväzný právny predpis.

Podľa predbežnej informácie je cieľom pripravovanej právnej úpravy komplexne a podrobne upraviť bezpečnostné opatrenia pre informačné technológie využívané v rámci verejnej správy. Súčasne má táto úprava za cieľ posilniť kybernetickú bezpečnosť orgánov verejnej moci (štátnych orgánov, orgánov územnej samosprávy a ďalších subjektov verejnej správy), ktoré spracúvajú dáta a poskytujú dôležité verejné služby prostredníctvom informačných systémov a informačných technológií verejnej správy.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „ZoITVS“) v ustanovení § 31 písm. j) uvádza, že MIRRI vydá všeobecne záväzný právny predpis, ktorý sa v Zbierke zákonov Slovenskej republiky vyhlasuje uverejnením úplného znenia a ktorý ustanoví na úseku bezpečnosti informačných technológií verejnej správy:

1. podrobnosti o bezpečnosti informačných technológií verejnej správy,
2. bezpečnostné opatrenia,
3. rozsah a spôsob prijímania a realizácie bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov,
4. obsah a štruktúru bezpečnostného projektu,
5. rozsah údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT podľa § 18 až 23a ZoITVS,

V rámci tohto dokumentu sme si dovolili identifikovať niekoľko oblastí problémov a poskytnúť viacero návrhov pre zlepšenie kvality Návrhu vyhlášky. Súčasne sme pripravení sa zapojiť do prípravy Návrhu vyhlášky aj vo väčšom rozsahu, a to najmä v pripomienkovaní predbežných verzií a návrhu zmien a odporúčaní.

Doc. JUDr. RNDr. Pavol Sokol, PhD. et PhD.

Garant KC KB UPJŠ

2 OBLASTI PODNETOV A NÁVRHOV

Na základe analýzy aktuálne platnej **Vyhlášky č. 179/2020 Z. z.** a pripravovanej zmeny, je možné identifikovať viaceré skupiny problémov a podnetov, ktoré by mali byť predmetom úpravy Návrhu vyhlášky. Tieto problémy sú rozdelené podľa kľúčových oblastí z vyhlášky, s odkazmi na konkrétne ustanovenia. Navrhované podnety vychádzajú z praktických potrieb aplikačnej praxe, zmien v medzinárodných štandardoch a požiadaviek na zvyšovanie odolnosti subjektov voči kybernetických hrozbám. V rámci našej analýzy sme identifikovali nasledujúce oblasti podnetov a návrhov:

- vymedzenie kategórií a požiadaviek pre jednotlivé subjekty verejnej správy,
- nerealizovateľnosť niektorých požiadaviek pre menších správcov,
- absencia rozsahu údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT
- chýbajúce rozšírené požiadavky na nové informačné technológie,
- súlad s inými vykonávacími právnymi predpismi,
- zapracovať opatrenia týkajúce sa koordinovaného oznamovania a zverejňovania bezpečnostných zraniteľností,
- URL v texte vyhlášky,

2.1 VYMEDZENIE KATEGÓRIÍ A POŽIADAVIEK PRE JEDNOTLIVÉ SUBJEKTY VEREJNEJ SPRÁVY

V § 3 ods. 2 až 5 Vyhláška č. 179/2020 Z. z. sa kategorizácia správcov informačných technológií verejnej správy odvíja od počtu obyvateľov, právneho postavenia alebo organizačnej štruktúry, ale **nie je dostatočne zohľadnené reálne riziko alebo význam spracúvaných údajov**. Rovnaká kategória môže znamenať rozdielne reálne potreby na ochranu.

Podnety/návrhy:

- Zaviesť **rizikovo orientovaný prístup ku kategorizácii** informačných technológií verejnej správy systémov namiesto fixného delenia podľa veľkosti samosprávy alebo typu inštitúcie.
- Zviesť kombinovaný prístup, ktorý bude zohľadňovať povahu správcu a súčasne mieru rizika.

2.2 NEREALIZOVATEĽNOSŤ NIEKTORÝCH POŽIADAVIEK PRE MENŠÍCH SPRÁVCOV

Napriek rozdeleniu správcov do kategórií I – III sú niektoré požiadavky na správcov zaradených do **kategórie I administratívne náročné** a vyžadujú odborné znalosti, ktoré títo správcovia nemajú a reálne si ich nemôžu finančne dovoliť, resp. z povahy subjektu mu nemusia priniesť predpokladaný úžitok z požadovaného bezpečnostného opatrenia. Ide napríklad o menšie obce, materské, základné a stredné školy, školské jedálne, menšie rozpočtové organizácie obcí.

Podnety/návrhy:

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- Definovať kategóriu malých správcov a zaviesť **zjednodušené požiadavky, štandardy, postupy pre túto kategóriu** (napr. dedikovaná metodika, centrálna asistencia).
- Vyčleniť plnenie povinností, ktoré bude zo zákona zabezpečovať zriaďovateľ, orgán vedenia podľa §5 ods. 1 Zákona o ITVS (MIRRI), resp. iný orgán (NASES).

2.3 Absencia rozsahu údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT

Zákon o ITVS v ustanovení § 23 ods. 3 uvádza aj povinnosť pre orgán riadenia zasielať:

- najmenej jedenkrát do roka orgánu vedenia zoznam aktív podľa § 19 ods. 1 písm. c), ZoITVS
- spôsobom určeným orgánom vedenia vládnej jednotke CSIRT vládnou jednotkou CSIRT určené systémové informácie o aktívach, rizikách, kontaktných bodoch a evidencii kybernetických bezpečnostných incidentov informačných technológií verejnej správy v rozsahu ustanovenom všeobecne záväzným právnym predpisom vydaným ministerstvom investícií a aktualizovať zaslané údaje každých 14 dní,

Ide o dôležitý prvok správy kybernetickej a informačnej bezpečnosti vo verejnej správe, keďže súvisí so systémami, ako je Vládny informačného systém kybernetickej bezpečnosti (VISKB) a systémom na identifikovanie bezpečnostných zraniteľností Achilles.

V zmysle ustanovenia § 31 písm. j. ods. 5 MIRRI vydá všeobecne záväzný právny predpis, ktorý ustanoví rozsah údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT podľa § 18 až 23a ZoITVS.

Podnety/návrhy:

- Navrhujeme zapracovať do Návrhu vyhlášky aj časť venujúcu sa nahlasovaniu údajov podľa § 18 až 23a ZoITVS. Druhou alternatívou je vydanie samostatnej vyhlášky, ale vzhľadom na prepojenosť a dôležitosť témy, je vhodné to spojiť do jedného všeobecne záväzné právneho predpisu.
- Navrhujeme v rámci Návrhu vyhlášky špecifikovať požadované údaje podľa kategórie subjektu.
- Zosúladiť rozsah zasielaných údajov tak, aby sa týmto umožnilo plnenie aj iných bezpečnostných opatrení.

2.4 Chýbajúce rozšírené požiadavky na nové informačné technológie

Vyhláška č. 179/2020 Z. z. nereflektuje v zozname bezpečnostných opatrení aj informačné technológie, ktoré za niekoľko rokov prešli viacerými zmenami (napr. využitie cloudové aplikácie, umelej inteligencie, Internet of things).

Podnety/návrhy:

- Zvážiť zapracovanie **bezpečnostných požiadaviek na bezpečnosť cloudových aplikácií** (prístupové práva, lokalita dát, šifrovanie).
- Zohľadniť **špecifiká spracúvania dát cez systémy umelej inteligencie** a aplikovať medzinárodné normy v tejto oblasti, či už napr. odporúčania normy ISO/IEC 23894:2023 - Umelá inteligencia – usmernenia k riadeniu rizík alebo pripravovanej normy ISO/IEC DIS 27090 – usmernenia na riešenie bezpečnostných hrozieb pre systémy umelej inteligencie.

2.5 SÚLAD S INÝMI VYKONÁVACÍMI PRÁVNYMI PREDPISMI

Návrh vyhlášky by mal reflektovať existujúce, resp. pripravované zmeny v iných všeobecne záväzných právnych predpisoch, ktoré priamo upravujú oblasť kybernetickej bezpečnosti (Návrh vyhlášky NBÚ o bezpečnostných opatreniach) alebo sa obsahovo zasahujú do oblasti kybernetickej a informačnej bezpečnosti (napr. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy (ďalej len „Vyhláška UPVII o štandardoch“).

Podnety/návrhy:

- Zvážiť zosúladenie oblastí bezpečnostných opatrení v Návrhu Vyhlášky s Návrhom vyhlášky NBÚ o bezpečnostných opatreniach.
- Zadefinovať pre bezpečnostné štandardy spôsob, ako efektívne určiť minimálnu požadovanú hranicu. Napr. v prípade použitia kryptografických primitív. Príkladom by mohla byť Vyhláška UPVII o štandardoch, ktorá na viacerých miestach uvádza podporu chráneného prenosu dát cez kryptografický protokol Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group. Na druhej strane, na viacerých miestach absentujú minimálne požiadavky na iné kryptografické primitíva, ako sú šifrovacie kľúče, digitálne odtlačky a pod.

2.6 ZAPRACOVAŤ OPATRENIA TÝKAJÚCE SA KOORDINOVANÉHO OZNAMOVANIA A ZVEREJŇOVANIA BEZPEČNOSTNÝCH ZRANITEĽNOSTÍ

Podľa § 23 ods. 3 písm. e) ZoITVS je orgán riadenia je povinný zverejniť na svojom webovom sídle pravidlá na oznamovanie zraniteľností. K vykonaniu bezpečnostného útoku je nevyhnutné využitie minimálne jednej bezpečnostnej zraniteľnosti. Efektívne riadenie bezpečnostných zraniteľností zahŕňa nielen včasnú identifikáciu a odstránenie týchto zraniteľností, ale aj zavedenie procesov pre koordinované oznamovanie zraniteľností (CVD) a podporu bezpečnostnej komunity (napr. bug bounty programy). Tým sa skracuje doba medzi odhalením a nápravou bezpečnostných zraniteľnosti, znižuje sa riziko úspešného útoku a posilňuje sa dôvera zákazníkov a partnerov.

Podnety/návrhy:

- Zaviesť a udržiavať proces koordinovaného oznamovania a zverejňovania bezpečnostných zraniteľností, ktorý umožňuje interným aj externým stranám nahlásiť zistené bezpečnostné zraniteľnosti v systémoch, produktoch alebo službách organizácie. Konkrétne znenie uvádzame v nasledujúcej časti tohto dokumentu.
- Uviesť v rámci prílohy Návrhu vyhlášky jednoduchý postup na zverejňovanie bezpečnostných zraniteľností.

2.7 URL V TEXTE VYHLÁŠKY

Vyhláška č. 179/2020 Z. z. obsahuje priamy odkaz na webové sídlo vládnej jednotky CSIRT.SK ohľadne zabezpečenia webového sídla a prístupu k nemu pomocou protokolu HTTPS s využitím bezpečnej verzie protokolu TLS (https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=181). Tento odkaz nefunguje.

Podnety/návrhy:

- Neuvádzať priame URL na konkrétne odporúčania, ktoré nemusia byť časom dostupné. Navyše materiál od vládnej jednotky CSIRT.SK má odporúčací charakter a v prípade nezrovnalostí s obsahom Vyhlášky UPVII o štandardoch, má obsah tejto vyhlášky prednosť.

3 MEDZINÁRODNÝ ŠTANDARD ISO/IEC 27002:2022

V nadväznosti na pripravovaný Návrh vyhlášky a s prihliadnutím na významnú aktualizáciu medzinárodnej normy **ISO/IEC 27002:2022**, navrhujeme zapracovať nasledujúce zmeny do pripravovaného znenia Návrhu vyhlášky. Cieľom je zosúladiť národné opatrenia s medzinárodne uznávanými štandardmi v oblasti kybernetickej a informačnej bezpečnosti a zabezpečiť adekvátnu aplikáciu bezpečnostných opatrení v oblasti kybernetickej bezpečnosti vo verejnej správe.

Medzinárodná norma ISO/IEC 27002:2022 poskytuje podrobné usmernenia a odporúčania na výber, implementáciu a riadenie opatrení informačnej a kybernetickej bezpečnosti. Subjekty používajú túto normu pri tvorbe interných politík, postupov a pri zavádzaní „osvedčených praktík“ (best practices) na ochranu dôvernosti, integrity a dostupnosti svojich aktív.

Obsah Vyhlášky č. 179/2020 Z. z. čiastočne vychádzal z obsahu medzinárodnej normy ISO/IEC 27002:2013. **Zmenu v týchto medzinárodných normách je možné identifikovať už aj z názvov.** Z pôvodného „Code of practice for information security controls“ (ISO/IEC 27002:2022) na „Information security, cybersecurity and privacy protection – Information security controls“ (27002:2022) s rozšíreným zameraním aj na kybernetickú bezpečnosť a ochranu súkromia. Nová norma má aj novú štruktúru, keď sa počet bezpečnostných opatrení znížil zo 114 (2013) na 93 (2022), pričom:

- 11 bezpečnostných opatrení je úplne nových,
- 24 bezpečnostných opatrení je zlúčených z viacerých starších opatrení,
- 58 bezpečnostných opatrení bolo aktualizovaných (najmä text „Guidance“).

Súčasne nová norma ISO/IEC 27002:2022 obsahuje **štyri tematické oblasti** namiesto pôvodných 14 kapitol:

- Organizačné opatrenia (37 bezpečnostných opatrení),
- Opatrenia týkajúce sa ľudí (8 bezpečnostných opatrení),
- Fyzické opatrenia (14 bezpečnostných opatrení),
- Technologické opatrenia (34 bezpečnostných opatrení).

V rámci odbornej činnosti sme analyzovali aktuálne znenie Vyhlášky č. 179/2020 Z. z., ktoré sme namapovali na jednotlivé časti normy ISO/IEC 27002:2013. Následne sme porovnali zmeny medzi normami ISO/IEC 27002:2013 a ISO/IEC 27002:2022. Na základe týchto zmien sme navrhli možné zmeny v jednotlivých ustanoveniach Návrhu vyhlášky. Nižšie uvádzame návrh niekoľkých zmien.

3.1 KONTAKT S ODBORNÝMI ZÁUJMOVÝMI SKUPINAMI

- **Znenie aktuálnej vyhlášky:** nie je
- **Relevantné ustanovenie ISO/IEC 27002:2013:** 6.1.4 – Contact with special interest groups
- **Nové ustanovenie ISO/IEC 27002:2022:** 5.6 - Contact with special interest groups

- **Návrh paragrafového znenia:** Zabezpečiť zapojenie organizácie do činnosti odborných záujmových skupín, profesijných združení a fór relevantných pre kybernetickú a informačnú bezpečnosť s cieľom výmeny informácií a zdieľania osvedčených postupov.
- **Poznámka:** Toto bezpečnostné opatrenie by sa malo dotýkať správcov s plnením bezpečnostných opatrení vyšších kategórií.

3.2 SPRAVODAJSTVO O HROZBÁCH (THREAT INTELLIGENCE)

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** nové bezpečnostné opatrenie
- **ISO/IEC 27002:2022:** 5.7 - Threat intelligence
- **Návrh paragrafového znenia:** Zaviesť procesy na získavanie, vyhodnocovanie a využívanie informácií o kybernetických hrozbách s cieľom predchádzať kybernetickým bezpečnostným incidentom, znižovať riziká a zvyšovať pripravenosť organizácie na nové typy bezpečnostných hrozieb.
- **Poznámka:** Toto bezpečnostné opatrenie by sa malo dotýkať správcov s plnením bezpečnostných opatrení vyšších kategórií.

3.3 OVEROVANIE SPOĽAHLIVOSTI PRED NÁSTUPOM DO ZAMESTNANIA

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** 7.1.1 - Screening
- **ISO/IEC 27002:2022:** 6.1 - Screening
- **Návrh paragrafového znenia:** Pred prijatím osoby do zamestnania alebo začiatkom spolupráce overiť jej spoľahlivosť primerane jej budúcim povinnostiam a rizikám spojeným s prístupom k informáciám.

3.4 BEZPEČNOSŤ INFORMÁCIÍ PRI VYUŽÍVANÍ CLOUDOVÝCH SLUŽIEB

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** nie je
- **ISO/IEC 27002:2022:** 5.23 - Information security for use of cloud services
- **Návrh paragrafového znenia:** Zaviesť a udržiavať opatrenia na riadenie bezpečnosti informácií pri využívaní cloudových služieb, vrátane posúdenia rizík, stanovenia bezpečnostných požiadaviek a priebežného monitorovania poskytovateľa služieb.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

3.5 VYMAZANIE INFORMÁCIÍ

- **Znenie aktuálnej vyhlášky:** čiastočne (L. Fyzická bezpečnosť a bezpečnosť prostredia - Kategória II. - d) Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj pravidlá - 4. vymazávania, vyraďovania a likvidovania zariadení informačných technológií verejnej správy a všetkých typov relevantných záloh)
- **ISO/IEC 27002:2013:** nie je
- **ISO/IEC 27002:2022:** 8.10 - Information deletion
- **Návrh paragrafového znenia:** Zabezpečiť bezpečné a úplné vymazanie informácií z nosičov a systémov tak, aby sa zabránilo ich obnoveniu alebo zneužitiu.

3.6 MASKOVANIE ÚDAJOV (DATA MASKING)

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** nie je
- **ISO/IEC 27002:2022:** 8.11 – Data masking
- **Návrh paragrafového znenia:** Používať techniky maskovania údajov s cieľom minimalizovať vystavenie citlivých informácií a znížiť riziko ich zneužitia.

3.7 PREVENCIA ÚNIKU ÚDAJOV (DATA LEAKAGE PREVENTION)

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** nie je
- **ISO/IEC 27002:2022:** 8.12 - Data leakage prevention
- **Návrh paragrafového znenia:** Zaviesť opatrenia na prevenciu úniku údajov, vrátane detekcie, monitorovania a blokovania neoprávnených prenosov citlivých informácií.
- **Poznámka:** Toto bezpečnostné opatrenie by sa malo dotýkať správcov s plnením bezpečnostných opatrení vyšších kategórií.

3.8 BEZPEČNÉ PROGRAMOVANIE (SECURE CODING)

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** nie je

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- **ISO/IEC 27002:2022:** 8.28 - Secure coding
- **Návrh paragrafového znenia:** Zaviesť a uplatňovať bezpečnostné zásady a postupy pri vývoji softvéru s cieľom predchádzať zraniteľnostiam a chybám, ktoré by mohli byť zneužité.
- **Poznámka:** Toto bezpečnostné opatrenie by sa malo dotýkať správcov s plnením bezpečnostných opatrení vyšších kategórií, resp. aj pre dodávateľov informačných technológií verejnej správy.

3.9 PRÁCA NA DIAĽKU (REMOTE WORKING)

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** čiastočne 6.2.2 - Teleworking
- **ISO/IEC 27002:2022:** 6.7 - Remote working
- **Návrh paragrafového znenia:** Vypracovať a udržiavať opatrenia na zabezpečenie práce na diaľku, vrátane požiadaviek na používanie schválených zariadení, zabezpečenia komunikácie a ochrany spracúvaných informácií, tak aby sa minimalizovalo riziko ohrozenia kybernetickej a informačnej bezpečnosti.

3.10 RIADENIE KRYPTOGRAFICKÝCH KĽÚČOV (KEY MANAGEMENT)

- **Znenie aktuálnej vyhlášky:** čiastočne (N. Kryptografické opatrenia)
- **ISO/IEC 27002:2013:** 10.1.2 – Key management
- **ISO/IEC 27002:2022:** 8.24 – Use of cryptography a 8.25 – Key management
- **Zmeny:** Norma ISO/IEC 27002:2022 kladie väčší dôraz na **celoživotný cyklus kľúčov** vrátane ich generovania, distribúcie, ukladania a bezpečnej likvidácie a na zabezpečenie zhody s legislatívnymi požiadavkami.
- **Návrh paragrafového znenia:** Zaviesť a udržiavať proces riadenia kryptografických kľúčov pokrývajúci celý ich životný cyklus, vrátane generovania, distribúcie, ukladania, rotácie a likvidácie a zabezpečiť, aby bol tento proces v súlade s právnymi a regulačnými požiadavkami.
- **Poznámka:** Toto bezpečnostné opatrenie by sa malo dotýkať správcov s plnením bezpečnostných opatrení vyšších kategórií. Navrhujeme doplniť minimálne štandardy pre kryptografické primitíva, resp. uviesť, že sa majú používať kryptografické primitíva podľa aktuálneho stavu poznania (state of art).

3.11 AUTENTIFIKAČNÉ INFORMÁCIE

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- **Znenie aktuálnej vyhlášky:** čiastočné (pokryté v ustanoveniach o používaní autentifikačných prostriedkov)
- **ISO/IEC 27002:2013:** 9.3.1 - Use of secret authentication information
- **ISO/IEC 27002:2022:** 5.17 - Authentication information
- **Návrh paragrafového znenia:** Zaviesť a udržiavať proces bezpečného generovania, distribúcie, ukladania a používania autentifikačných informácií, pričom pri prístupe k citlivým systémom a údajom musí byť použité viacfaktorové overovanie.

3.12 KOORDINOVANÉ OZNAMOVANIE A ZVEREJŇOVANIE ZRANITEĽNOSTÍ (COORDINATED VULNERABILITY DISCLOSURE)

- **Znenie aktuálnej vyhlášky:** nie je
- **ISO/IEC 27002:2013:** neexistuje samostatne (čiastočne súvisí s 12.6.1 – Management of technical vulnerabilities)
- **ISO/IEC 27002:2022:** 8.8 – Management of technical vulnerabilities (rozšírené o koordinované oznamovanie)
- **Návrh paragrafového znenia:** Zaviesť a udržiavať proces koordinovaného oznamovania a zverejňovania zraniteľností, ktorý umožňuje interným aj externým stranám nahlásiť zistené zraniteľnosti v systémoch, produktoch alebo službách organizácie. Proces musí obsahovať postupy na prijatie a overenie nahlásenia, určenie priorít nápravných opatrení, bezpečné odstránenie zraniteľnosti a poskytnutie spätnej väzby oznamovateľovi.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

POUŽITÉ ZDROJE

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Geneva: ISO, 2013. 114 s.

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022. 93 s.

[3] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

[4] Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy.