
ŠTRUKTÚRA BEZPEČNOSTNEJ DOKUMENTÁCIE PODĽA ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

ING. LUKÁŠ ŠURAB



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. Štruktúra a požiadavky na bezpečnostnú dokumentáciu podľa zákona o kybernetickej bezpečnosti
2. Stratégia a politiky kybernetickej bezpečnosti
3. Klasifikácia informácií a kategorizácia systémov
4. Dokumentácia plnenia bezpečnostných opatrení
5. Vykonaná analýza rizík kybernetickej bezpečnosti
6. Záverečná správa z auditu kybernetickej bezpečnosti
7. Slovník povinností
8. Životný cyklus a budúcnosť bezpečnostnej dokumentácie

ÚVOD - PREČO JE DOKUMENTÁCIA DÔLEŽITÁ?

Bezpečnostná dokumentácia nie je len administratívna formalita, ale centrálny, živý a právne vynútitel'ný nástroj riadenia kybernetickej bezpečnosti.

- **Základ pre realizáciu opatrení:** Všetky bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie.
- **Požiadavka na aktuálnosť:** Dokumentácia musí byť neustále aktuálna a musí zodpovedať reálnemu stavu technológií, procesov a rizík v organizácii.
- **Dôkaz o súlade:** Slúži ako hlavný pilier preukazovania súladu s legislatívou a efektívneho riadenia bezpečnosti.

3

ide len o "papierovanie" pre úrad alebo formálnu požiadavku zákona
Auditor sa nebude pýtať len "Máte takú a takú smernicu?", ale skôr "Ukážte mi, ako naplňate túto smernicu – napríklad záznamy z ročných kontrol prístupových práv za posledný rok". Ak nemáte dokumentáciu alebo dôkazy o jej uplatňovaní, vystavujete sa riziku sankcií aj reálnych bezpečnostných problémov.

PRÁVNÝ RÁMEC - ZÁKONY A VYHLÁŠKY

Legislatívny základ pre bezpečnostnú dokumentáciu v Slovenskej republike tvoria kľúčové predpisy:

1. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti (v znení č. 366/2024 Z. z.)
 - o Stanovuje všeobecné povinnosti, rozsah pôsobnosti a lehoty oznamovania.
2. Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach (účinná od 1. 9. 2025)
 - o Transformuje zákonné povinnosti do presnej štruktúry bezpečnostnej dokumentácie.
 - o Upravuje rámec všeobecných bezpečnostných opatrení pre IKT aj OT.
 - o Nahrádza vyhlášku č. 362/2018 Z. z.

-
- <https://www.slov-lex.sk/>

4

366/2024 Z. z. (táto novela implementuje európsku smernicu NIS2 od 1.1.2025)

Ide o zvýšenie štandardu bezpečnosti, ktoré reflektuje aktuálne hrozby a európske normy. Tento právny rámec je právne vynútiteľný: NBÚ má právomoci kontrolovať a vyžadovať nápravu a v prípade nesúladu udeľovať sankcie.

Pri najzávažnejších porušeníach môžu pokuty podľa nových pravidiel dosiahnuť až 10 miliónov eur alebo 2%

z obratu firmy, čo už každé vedenie motivuje brať túto oblasť vážne. Napríklad za nenahlásenie vážneho

kybernetického incidentu hrozia pokuty do 7 miliónov eur.

PRÁVNÝ RÁMEC - ZÁKONY A VYHLÁŠKY

Legislatívny základ pre bezpečnostnú dokumentáciu v Slovenskej republike tvoria kľúčové predpisy:

3. Vyhláška NBÚ č. 226/2025 Z. z. o podrobnostiach hlásení (účinná od 1. 9. 2025)
 - Definuje kritériá závažného narušenia a náležitosti hlásení kybernetických incidentov.

Súvisiace predpisy

- Vyhláška č. 493/2022 Z. z. o audite kybernetickej bezpečnosti – režim a ciele auditu.
- Vyhláška č. 492/2022 Z. z. o znalostných štandardoch – roly a minimálne kompetencie v KB.

-
- <https://www.slov-lex.sk/>

226 špecifikuje kedy a čo presne musíte NBÚ hlásiť.

Metodiky a regulácie

- **Dve hlavné na Slovensku – ZoKB (NBÚ) a ISVS (MIRRI)**
 - Rozdielne rozhodovanie o opatreniach.
 - Rozdielna forma hlásenia incidentov a auditov.
 - Rozdielna pôsobnosť
 - **Príklady iných regulácií**
 - DORA – finančný sektor
 - NCCS – energetika
 - EASA Part-IS & EUROCAE ED-205A/ED-201A/ED-206 – letecký sektor
 - CRA – produkty s digitálnymi prvkami
 - eIDAS2 – digitálna identita
-

pravidlá pre verejnú správu – okrem ZoKB musia orgány verejnej moci dodržiavať zákon o informačných systémoch verejnej správy (ISVS) a súvisiace vyhlášky MIRRI SR, ktoré stanovujú bezpečnostné štandardy pre štátne IT systémy.

Veľká banka na Slovensku musí mať bezpečnostnú dokumentáciu podľa ZoKB, ale zároveň musí splniť konkrétne požiadavky Národnej banky SR a európskej DORA – takže do svojej internej dokumentácie musí zabudovať aj tie. Dobře vybudovaný systém podľa ZoKB našťastie zväčša tvorí kostru, na ktorú sa dajú naviazovať sektorské požiadavky.

Pre organizáciu je dôležité poznať svoju “regulačnú mapu” – aké zákony a vyhlášky sa na ňu vzťahujú – a podľa toho prispôbiť dokumentáciu. My sa sústreďujeme na ZoKB, lebo to je univerzálny základ. Ten spravidla, ak je dobre spravený, pokryje 80% požiadaviek aj iných noriem. Zvyšných 20% sú špecifiká (napr. banky musia mať plán komunikácie s NBS pri incidente – to by ste doplnili do incident plánu).

Dobrá správa je, že všetky tie regulácie majú podobnú filozofiu – analýza rizík, opatrenia, monitoring, incidenty, audit. Takže ak zvládnete dokumentáciu podľa ZoKB, adaptácia na iné normy je už relatívne jednoduchá.

PZS A PKZS

•**Prevádzkovateľ základnej služby (PZS)** je subjekt, ktorý poskytuje základnú službu uvedenú v prílohe č. 1 zákona, a ktorý je zapísaný v registri prevádzkovateľov základnej služby, vedenom Národným bezpečnostným úradom (NBÚ).

- poskytuje službu, ktorej **výpadok by mohol mať významný** dopad na bezpečnosť alebo fungovanie spoločnosti.
- **má povinnosti podľa ZoKB**: vypracovať bezpečnostnú dokumentáciu, implementovať opatrenia, hlásiť incidenty, vykonať audit alebo samohodnotenie.

PZS A PKZS

•Prevádzkovateľ kritickej základnej služby (PKZS) je prevádzkovateľ základnej služby, ktorý prevádzkuje aspoň jednu kritickú základnú službu podľa § 18 zákona, a teda má zásadný význam pre fungovanie štátu, ekonomiky alebo spoločnosti.

- ide o subjekt, ktorý prevádzkuje **kritickú** časť infraštruktúry (napr. prenosové systavy, letiská, nemocnice, centrálné IS štátu, bankový dohľad, DNS root, QTSP).
- **má prísnejšie povinnosti:** Nižšie prahy pre incidenty, povinnosť zachovať vyššiu dostupnosť.
- jeho **kritickosť potvrdzuje alebo určuje NBÚ** zápisom do registra PKZS.

PZS VS PKZS

- **Incidenty – prahy závažného narušenia (vyhl. 226/2025):**

- PKZS: úplný výpadok > 30 min, obmedzenie činnosti > 60 min.
- PZS: úplný výpadok > 60 min, obmedzenie činnosti > 180 min.

- **Audit vs. samohodnotenie:**

- PZS môže mimo „auditových rokov“ splniť povinnosť samohodnotením v JISKB. Musí ale absolvovať audit do 5 rokov od zápisu a potom podľa periodicity zákona.
- PKZS vykonáva audit (samohodnotenie sa naň nevzťahuje).

- **Tretie strany:**

- pri zmluvách **PKZS** môže kontrolu plnenia bezpečnostných opatrení vykonávať aj **NBÚ**. Tretia strana má pre tento účel postavenie **PZS**.

ak elektrárň (PKZS) vypadne na pol hodiny, NBÚ to už považuje za významný problém, kým menšia služba by polhodinový výpadok ešte nemusela hlásiť. Pre PKZS tak platí prísnejšia povinnosť hlásiť aj kratšie výpadky, lebo sa predpokladá, že už tie môžu mať veľký Dopad.
















zákon a vyhláška dávajú NBÚ možnosť kontrolovať aj plnenie opatrení u tretích strán, ktoré sú v zmluvnom vzťahu s PKZS a podieľajú sa na prevádzke tej kritickej služby. Prakticky NBÚ môže napríklad prísť do firmy, ktorá je dodávateľom IT služieb pre PKZS, a preveriť, či dodržiava bezpečnostné opatrenia podľa zmluvy a zákona. Tieto tretie strany

majú pre účely kontroly postavenie PZS, aj keď samy o sebe PZS nie sú. To je významný rozdiel oproti bežným PZS – NBÚ takto “nekontroluje” dodávateľov každého PZS, ale pri kritických to robiť môže. Organizácia, ktorá je PKZS, teda musí do zmlúv so svojimi dodávateľmi zakomponovať bezpečnostné požiadavky a rátať s tým, že ich dodržiavanie môže NBÚ preverovať.

KTO JE PZS/PKZS?

HRANIČNÉ HODNOTY (článok 2)

Kategória podniku	Počet pracovníkov: ročná pracovná jednotka (RPJ)	Ročný obrat	Celková ročná bilančná suma
Stredné podniky	< 250	≤ 50 miliónov EUR	≤ 43 miliónov EUR
Malé podniky	< 50	≤ 10 miliónov EUR	≤ 10 miliónov EUR
Mikropodniky	< 10	≤ 2 milióny EUR	≤ 2 mil. EUR

 Energetika Kľúčová entita	 Zdravotníctvo Kľúčová entita	 Doprava Kľúčová entita	 Bankovníctvo a finančné trhy Kľúčová entita
 Pitná a odpadová voda Kľúčová entita	 Digitálna infraštruktúra Kľúčová entita	 Verejná správa Kľúčová entita	 Digitálni poskytovatelia Dôležitá entita
 Poštové služby Dôležitá entita	 Odpadové hospodárstvo Dôležitá entita	 Vesmír Kľúčová entita	 Potraviny Dôležitá entita
 Výroba Dôležitá entita	 Chemikálie Dôležitá entita	 Výskum Dôležitá entita	

Zdroje: <https://www.nbu.gov.sk/metodiky/>

<https://nis2.nbu.gov.sk/>

10

Ak si nie ste istí, či ste PZS, pozrite si zoznam sektorov v prílohe zákona a využite ten online test. NBÚ týmto nabáda na samoidentifikáciu – teda aby sa organizácie samy prihlásili, ak spĺňajú kritériá (je to ich zákonná povinnosť). Nečakať, kým NBÚ niekoho “odhalí”, ale aktívne si overiť a ak áno, podať oznámenie o zaradení do registra. Nezaradenie sa, ak na to spĺňam kritériá, by bolo porušením zákona. Takže tieto zdroje slúžia na to, aby nikto nemohol povedať “nevedeli sme, že sa nás to týka”. Z praxe: NBÚ uvádza, že novela sa dotkne minimálne 3400 organizácií na Slovensku, čo je násobne viac než pôvodný zákon. Patria tam stredne veľké podniky vo výrobe potravín, odpadoch, výrobe technológií, ďalšie

subjekty verejnej správy atď'. Čiže ak ste väčšia firma v týchto sektoroch, veľmi pravdepodobne ste sa od 2025 stali PZS. Preto NBÚ spravil maximum, aby tieto informácie šírili.

IKT a OT

Aspekt	Definícia	Príklady	Vrstvy/Zóny	Opatrenia	Dokumentácia
IKT	Bežné informačné a komunikačné technológie (IS, siete, stanice, servery, aplikácie).	e-mail, databázy, M365, webové služby identity služby.	user LAN, server LAN, DMZ	Patch & change procesy, EDR/XDR/RBA C/MFA, DLP, šifrovanie dát.	Architektúra IKT, zoznam aktív, politiky/pravidlá, zoznam prijatých/neprijatých opatrení.
OT	Technológie riadenia fyzických procesov (ICS/SCADA, PLC, DCS, HMI, senzory).	PLC, RTU, HMI/SCADA, historians, field zariadenia, bezpečnostné relé, SIS.	Purdue/ISA-95 vrstvy 0–5 Segmentácia vnútri OT a medzi IT/OT	Segmentácia IT/OT, unidirectional gateways, offline zálohy, kontrola staníc a médií.	Architektúra OT, zoznam OT aktív, špecifické postupy (na zmeny, zálohy, izoláciu), záznamy o testoch.

informačných a komunikačných technológiách (IKT) aj o technológiách prevádzkovej povahy (OT).

Vodárenská spoločnosť bude mať vo svojom zábere IT systémy (kancelárske siete, ekonomický software) aj OT systémy (čerpacie stanice, PLC automaty riadiace vodárne). Bezpečnostná dokumentácia

musí zahrnúť opatrenia pre obe – nielen chrániť servery a počítače, ale aj tie priemyselné kontroléry a siete

v továrni. V praxi to znamená, že keď robia analýzu rizík, musia analyzovať aj riziko fyzického útoku alebo

malwaru v OT zariadení, mať plány čo ak niekto napadne SCADA systém atď. Nemôžu sa tváriť, že kybernetická bezpečnosť je len záležitosť IT oddelenia – týka sa aj výrobných inžinierov, správcov budov (fyzické prístupy do strojovni) a tak ďalej.

POVINNOSŤ ZO ZÁKONA

Základným kameňom je ustanovenie § 20 ods. 3 Zákona č. 69/2018 Z. z. (stav od 1. 1. 2025):

*"Bezpečnostné opatrenia sa prijímajú a realizujú v rozsahu a spôsobom podľa § 32 ods. 1 písm. b) alebo osobitného predpisu, ak je vydaný, a na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť **aktuálna** a musí zodpovedať **reálnemu stavu**."*

Toto ustanovenie povyšuje dokumentáciu na dynamický systém, ktorý musí presne a priebežne reflektovať skutočnosť v organizácii.

12

nemôžete si len tak ľubovoľne zavádzať opatrenia, musíte ich mať

podchytené v dokumentácii. A tá dokumentácia zároveň musí vždy odrážať realitu.

Dokumentácia ako predpoklad opatrení – Najprv musíte mať schválený plán (politiky, postupy atď.) a podľa neho potom realizovať. Napríklad nemôžete povedať "urobili sme školenie zamestnancov", ak to školenie nevyplýva z ničoho. Ale ak máte v dokumentácii napísané "všetci zamestnanci budú raz ročne preškolení v kybernetickej bezpečnosti" (v politike), potom to realizujete a viete sa odvolať na to, že plníte dokumentáciu. Doležite pre auditora nie je to jednorazový produkt, ale neustále

aktualizovaný súbor dokumentov.

ARCHITEKTÚRA DOKUMENTÁCIE: PÄŤ PILIEROV SÚLADU

Vyhláška NBÚ č. 227/2025 Z. z. v § 4 ods. 1 definuje základné a neoddeliteľné súčasti bezpečnostnej dokumentácie:

1. **Stratégia a politiky** kybernetickej bezpečnosti.
2. **Klasifikácia informácií a kategorizácia systémov** sietí, IS a OT.
3. **Dokumentácia plnenia bezpečnostných opatrení.**
4. **Analýza rizík** kybernetickej bezpečnosti + **zoznam aktív.**
5. **Záverečná správa z auditu** kybernetickej bezpečnosti.

(Ďalšie povinné dokumenty podľa osobitných predpisov (ak sa vyžadujú))

Táto štruktúra kopíruje logiku cyklu **Plánuj-Rob-Kontroluj-Konaj (PDCA)**, ktorý je jadrom normy ISO/IEC 27001.

13

najvyššie riadiace dokumenty, ktoré stanovujú ciele a zásady bezpečnosti v organizácii 1

dokumentácia, ktorá opisuje, ako organizácia hodnotí citlivosť svojich informácií a kritickosť svojich Systémov 2

hlavný dokument (alebo súbor dokumentov), kde organizácia popisuje, aké bezpečnostné opatrenia má zavedené, ako ich implementuje a Udržiava 3

dokument, v ktorom je zaznamenaná identifikácia a hodnotenie rizík a plán ich ošetrovania. Sem patrí aj špecifická analýza niektorých rizík, ktorú vyžaduje zákon (politické riziko dodávateľov) 4

výstup z nezávislého auditu, ktorý overuje súlad dokumentácie a opatrení s realitou a účinnosť opatrení. Táto správa je povinnou súčasťou

Dokumentácie 5

Príklad – paralela: Predstavme si to ako bezpečnosť v budove. Pilier I – stratégia – je ako rozhodnutie vedenia “budeme chrániť budovu pred požiarom a vlámaniami, vyčleníme na to rozpočet, zodpovedný je správca budovy”. Pilier II – klasifikácia – by bolo “ktoré miestnosti/majetok sú najcennejšie alebo najcitlivejšie? (trezorová miestnosť je kritická, bežné kancelárie menej)”. Pilier III – dokumentácia opatrení – je konkrétny bezpečnostný plán budovy: aké zámky, alarmy, hasičské senzory máme, kto to kontroluje, kde sú plány evakuácie atď. Pilier IV – analýza rizík – je vyhodnotenie, čo hrozí budove (požiar, krádež, povodeň) a ako minimalizujeme riziká (postavíme protipovodňovú zábranu, dáme bezpečnostné fólie na okná atď. – a to zapracujeme do plánu). V – audit – pravidelná revízia bezpečnosti budovy, ktorú urobí nezávislý odborník, nájde slabiny (napr. zlyhávajúci alarm) a navrhne zlepšenia. Po audite vedenie aktualizuje plán, investuje do novej techniky a cyklus pokračuje.

PILIER I: STRATÉGIA A POLITIKY KB

Vrchol riadiacej hierarchie

- Tieto dokumenty nie sú technickými manuálmi, ale riadiacimi nástrojmi, ktoré definujú ciele, zodpovednosti, vzdelávanie a záväzok organizácie voči kybernetickej bezpečnosti.
- Schvaľuje vrcholové vedenie.

14

Stratégia je odpoveď na otázky ČO a PREČO chceme dosiahnuť, politiky odpovedajú AKÉ pravidlá musíme dodržiavať, aby sme ciele naplnili. Pod nimi sú potom štandardy a postupy (k tým sa dostaneme za chvíľu), ktoré riešia AKO konkrétne tie pravidlá vykonať.

Zdôrazním ešte: Tieto strategické dokumenty sú právne vynúiteľné – ak NBÚ robí kontrolu, môže si vypýtať vašu stratégiu a ak ju nemáte alebo ju neschválilo vedenie, je to porušenie vyhlášky. A zároveň ak dôjde k incidentu a vyšetrovanie ukáže, že vedenie nebolo vôbec zapojené do riadenia bezpečnosti, môže

sa

to brať ako poľahčujúca či priťažujúca okolnosť.

Napríklad európska smernica NIS2 v čl. 20 jasne hovorí, že

vrcholový manažment nesie zodpovednosť za dodržiavanie kybernetickej bezpečnosti a musí byť do nej aktívne zapojený. Slovom NIS2: členovia vedenia môžu niesť osobnú zodpovednosť za nesúlad (teoreticky pokuty, zákazy činnosti). To je ďalší dôvod, prečo majú podpisovať tieto dokumenty – dávajú tým najavo, že o nich vedia a schvaľujú ich.

BEZPEČNOSTNÁ STRATÉGIA

Základný riadiaci dokument pre celú organizáciu, ktorý musí byť schválený vrcholovým vedením (spravidla štatutárom).

- **Určuje ciele, princípy a zodpovednosti** – kto čo robí a kto nesie dohľad.
- **Dáva mandát na zdroje a opatrenia** (prečo na bezpečnosť vyčleňujeme čas a peniaze).
- **Musí byť aktuálna a zodpovedať reálnemu stavu.**

15

Vymedzuje zodpovednosti – definuje kto čo robí a kto na koho dohliada. Napríklad spomenie rolu Manažéra kybernetickej bezpečnosti (MKB), ktorého úlohou je koordinovať plnenie celej bezpečnosti; spomenie úlohu predstavenstva, že raz ročne prehodnocuje správu o stave bezpečnosti; spomenie, že vedúci IT a vedúci OT zodpovedajú za implementáciu technických opatrení vo svojich doménach; že každý zamestnanec je zodpovedný za dodržiavanie pravidiel atď.

Príklad: Povedzme, že vedenie telekomunikačnej firmy povie “Chceme byť lídrom v bezpečnosti,

naši zákazníci nám musia dôverovať, že ich dáta sú v bezpečí”. To dajú ako cieľ do stratégie. Stanovia princíp

“Security by Design – bezpečnosť už pri návrhu služieb”, určia, že Manažér KB reportuje priamo generálnemu (aby mal dostatočnú autoritu) a že budú investovať napr. 5% IT rozpočtu do bezpečnosti ročne. To všetko sa zachytí v stratégii. Následne vydajú politiky – napr. Politiku riadenia prístupu, Politiku

bezpečnosti hesiel, Politiku práce z domu, Politiku zálohovania... kde už určia konkrétne pravidlá (napr. “prístup k zákazníckym údajom majú len poverené osoby podľa princípu need-to-know, heslá musia mať min. 12 znakov a expiráciu 90 dní, každý incident sa musí nahlásiť do 24 hodín internému CSIRT tímu” a pod.). Toto schváli generálny riaditeľ. Keď príde auditor alebo NBÚ, vidí jasne záväzok a pravidlá – poďme kontrolovať, či realita zodpovedá.

POVINNÉ PRVKY STRATÉGIE (§ 4 ODS. 1 PÍSM. A) VYHL. 227/2025 Z. Z.)

Stratégia musí obsahovať najmenej:

- **Ciele kybernetickej bezpečnosti**, ktoré má organizácia dosiahnuť.
 - **Základné princípy**, podľa ktorých sa budú tieto ciele dosahovať.
 - **Určenie právomocí a zodpovedností** za systémy manažérstva, riadenie rizík a aktualizáciu bezpečnostnej dokumentácie.
 - **Merateľné ukazovatele a periodicita vyhodnocovania** (KPI/KRI).
 - **Vyhlasenie vedenia a určenie MKB.**
-

16

definovanie toho, čo považujeme za úspech v bezpečnosti – napr. ochrana osobných údajov, dostupnosť služby, zhoda s predpismi atď.

Napr. princíp primeranosti, riskbased prístup, neustáleho zlepšovania, “zero trust” architektúry atď. Organizácia povie: tieto princípy budeme dodržiavať pri všetkých aktivitách.

Toto je dôležité, lebo ak nie je jasne dané, kto má čo na

starosti, môže dochádzať k nedorozumeniam.

Stratégia povie, že osoba XY je poverená udržiavať dokumentáciu aktuálnu, takže ak v audite zistia neaktuálnosť, vedia, koho sa pýtať prečo

Napríklad stratégia prikáže: budeme sledovať počet kritických zraniteľností v systémoch a cieľ je mať ich menej než 5 ročne; budeme merať priemerný čas na zistenie incidentu; budeme každoročne

vyhodnocovať plnenie plánu školení atď. Dôležité je aj určiť periodicitu: niečo mesačne IT oddelenie, štvrťročne bezpečnostná komisia, ročne predstavenstvo

HIERARCHIA RIADIACICH DOKUMENTOV

Legislatíva vytvára logický kaskádový model, kde každý nižší stupeň konkretizuje ten vyšší:

- **Stratégia: ČO** chceme dosiahnuť a **PREČO**.
- **Politiky: Záväzné pravidlá** pre špecifické oblasti (napr. politika riadenia prístupov). Sú povinné.
- **Štandardy: AKO** technicky implementovať politiky. Určujú povinné konfigurácie (napr. štandard pre heslá). Sú voliteľné, no v praxi nevyhnutné.
- **Postupy: Krok-za-krokom** pre špecifické platformy (požadované v rámci viacerých opatrení – musia byť zavedené a uplatňované).

17

Malé organizácie zvyčajne nemajú toľko dokumentov. Často majú iba “Bezpečnostnú politiku” a v nej namiešané aj pravidlá aj nejaké technické minimum. To môže prejsť u auditu, ak pokryjú všetko. Veľké inštitúcie majú desiatky dokumentov (napr. ministerstvá majú Stratégia, Politika, potom 10 príloh – manažment bezpečnosti, kryptografická politika atď., plus pre IT adminov zoznam štandardných konfiguračných baseline). Vyhláška nestanovuje presne, koľko dokumentov, len obsah. Takže to rozdelenie je na organizácii – ak splní obsah (ciele, princípy, postupy atď.), je jedno či to je v jednom dokumente

alebo v

15.

Kľúčová vec je však: politiky sú povinné

DÔSLEDOK: PREUKÁZATEĽNÁ ZODPOVEDNOSŤ VEDENIA

- **NIS2 (čl. 20)** vyžaduje, aby vedenie schvaľovalo a dohliadalo na opatrenia riadenia kybernetických rizík; členovia vedenia môžu niesť zodpovednosť za nesúlad.
 - **Priama línia MKB ↔ štatutár:** MKB predkladá návrhy opatrení a informácie priamo štatutárnemu orgánu (Vyhláška NBÚ 227/2025, Príloha č. 1, položka 1).
 - **Dôkaz pre audit:** musí existovať schválená stratégia a politiky (§ 4 ods. 1 písm. a–b vyhlášky) a preukázateľné rozhodnutia k rizikám; audit podľa § 29 zákona overuje plnenie povinností.
 - **Nedelegovateľná zodpovednosť:** operatíva môže byť prenesená, ale dohľad a zodpovednosť zostáva na vedení (NIS2 čl. 20).
-

18

členovia najvyššieho vedenia nemôžu tvrdiť “to je vec ITčkárov, my sme o tom nevedeli”.

Musia byť do procesu zapojení, prijímať informácie o kybernetickej bezpečnosti, robiť rozhodnutia o riadení rizík a uvoľňovaní zdrojov

CISO/MKB nemá byť „zakopaný“ hlboko v IT oddelení, ale má

reportovať priamo riaditeľovi alebo predstavenstvu

To znamená, že ak príde napr. k

veľkému incidentu a vyšetrovanie ukáže, že vedenie ignorovalo varovania alebo nevyhradilo zdroje na bezpečnosť, ponesie dôsledky.

PILIER II: KLASIFIKÁCIA A KATEGORIZÁCIA

Základ pre riadenie rizík

- Tento proces organizácii pomáha pochopiť hodnotu a **význam aktív** a na základe **klasifikácie informácií a kategorizácie sietí/IS/OT** aplikovať **primerané bezpečnostné opatrenia** vyplývajúce z **analýzy rizík**.

19

Vieme čo je kritické a citlivé (tomu dáme prísnejšie opatrenia) a čo je menej dôležité (tam nemíňame zbytočne veľa zdrojov). Tento princíp sa nazýva princíp primeranosti (proporcionality) – bezpečnostné opatrenia sa neaplikujú plošne rovnako na všetko, ale ich prísnosť je úmerná hodnote chránených informácií a kritickosti systémov.

Pre poisťovňu sú údaje o klientoch a výplata poisťných udalostí kľúčové – tie by mali mať najvyššiu ochranu (sú veľmi citlivé aj z hľadiska dôvernosti, aj dôležité pre chod firmy). Na druhej strane, napríklad verejne dostupná marketingová brožúra nemá takú citlivosť – jej strata by

firme

zásadne neublížila. Klasifikácia tieto rozdiely zachytí a následne zabezpečí, že citlivé údaje budú chránené napr. šifrovaním a prísnyimi prístupmi, kým tie verejné možno netreba chrániť vôbec (aby sme zbytočne nemrhali prostriedkami).

METODIKA KLASIFIKÁCIE INFORMÁCIÍ (PRÍLOHA Č. 2)

Každé informačné aktívum musí byť ohodnotené podľa troch základných pilierov informačnej bezpečnosti (CIA triáda):

- 1. Dôvernosť (Confidentiality):** Aký je dopad neoprávneného odhalenia?
- 2. Integrita (Integrity):** Aký je dopad neoprávnenej zmeny?
- 3. Dostupnosť (Availability):** Aký je dopad nedostupnosti?

20

Napríklad: - Pre databázu klientov poisťovne by dopad nedostupnosti možno nebol taký dramatický (pár hodín výpadku by sa prežilo), ale dopad straty dôvernosti (úniku) by bol obrovský (pokuty, strata reputácie) a dopad zmeny údajov tiež (vyplatenie nesprávnych súm a pod.). Takú databázu by sme klasifikovali vysoko citlivú najmä z hľadiska dôvernosti a integrity. - Naopak verejný web s marketingovými informáciami: strata dôvernosti nevádi (veď sú to verejné info), integrita – keby tam niekto zmenil text, je to nepríjemné, ale nie kritické, dostupnosť – krátky výpadok webu tiež firmu ohrozí

minimálne. Čiže celkovo by to bolo nízko citlivé aktívum.

STUPNE KLASIFIKÁCIE

Kritérium	Stupne
Dôvernosť	Verejné, Interné, Chránené, Prísne chránené
Integrita	Nízka, Stredná, Vysoká
Dostupnosť	Nízka, Stredná, Vysoká

Poznámka: Ak informácia nie je explicitne klasifikovaná, považuje sa za internú.

21

Po klasifikácii informácií nasleduje kategorizácia systémov – tá typicky nadväzuje na klasifikáciu najdôležitejších informácií, ktoré v danom systéme sú, plus zohľadňuje, aký význam má systém pre prevádzku firmy. Aj tu sa určujú kategórie (napr. kritický systém, dôležitý systém, menej dôležitý). Napríklad e-shop pre online banku bude kategorizovaný ako kritický systém (bez neho by klienti nevedeli robiť transakcie), kým napríklad testovací server môže byť nízko kategorizovaný. Tieto kategórie potom priamo určujú, aké opatrenia musíme na daných systémoch aplikovať.

DÔSLEDOK: IMPLEMENTÁCIA PRINCÍPU PROPORCIONALITY

Kategorizácia priamo určuje rozsah **povinných** bezpečnostných opatrení podľa Prílohy č. 1 Vyhlášky 227/2025.

- **Prístup založený na riziku:** Bezpečnostné opatrenia nie sú aplikované plošne, ale ich prísnosť je úmerná hodnote chránených aktív a kritickosti systémov.
- **Logické kroky:**
 1. Ohodnotenie aktív (klasifikácia).
 2. Určenie kritickosti systémov (kategorizácia).
 3. Aplikácia primeraných opatrení (analýza rizík, vrátane zdôvodnenia neprijatých opatrení).
- **Základ pre súlad:** Nesprávna alebo povrchná klasifikácia stavia celý systém riadenia na chybných základoch a vedie k nesúladu so zákonom.

22

Správne spravená klasifikácia a kategorizácia sú základom, na ktorom stojí celý systém riadenia bezpečnosti. Ak by sme ich odflákali alebo vôbec nerobili, všetko ostatné bude postavené na chybných základoch. Nielenže by sme mohli zle nasmerovať prostriedky (napr. príliš chrániť málo dôležité veci a podceniť tie kritické), ale pri audite by to znamenalo nesúlad so zákonom. Auditor by mohol skonštatovať, že organizácia nedokáže preukázať primeranosť opatrení, lebo nemá zdokumentované, čo je pre ňu kritické.

PILIER III: DOKUMENTÁCIA BEZPEČNOSTNÝCH OPATRENÍ

Jadro prevádzkovej bezpečnosti

Popisuje, ako organizácia **reálne chráni** svoje siete a informačné systémy v praxi.

Musí byť **aktuálna a zodpovedať reálnemu stavu organizácie**.

Má obsahovať **zoznam prijatých/neprijatých opatrení a základné schémy topológií a architektúr** (IKT/OT, aplikácie, bezpečnostná architektúra).

23

Laicky, tento dokument je takým „manuálom kybernetickej bezpečnosti“ pre vašu firmu. Obsahuje všetky dôležité informácie: čo robíme, aby sme boli zabezpečení; aké technológie a procesy na to máme; kde máme aké bezpečnostné prvky nasadené. Príklad z praxe: Ak by som bol auditor a pýtal by som si dokumentáciu bezpečnostných opatrení, očakával by som, že mi predložíte hrubší spis alebo sadu súborov, kde nájdem kapitoly pre jednotlivé okruhy (sieťová bezpečnosť, riadenie prístupov, zálohovanie, fyzická bezpečnosť...). V každej kapitole bude popis: aké

konkrétne opatrenia máme (napr. „Máme centrálny firewall FortiGate, ktorý filtruje prevádzku podľa definovaných pravidiel; interná sieť je segmentovaná do VLAN oddelených ACL; vzdialený prístup je povolený len cez VPN s 2-faktorovou autentifikáciou“ a pod.). Tiež tam bude napríklad uvedené: „Opatrenie č. 14 z prílohy vyhlášky – šifrovanie uložených údajov – nie je implementované na menej kritických staniciach z dôvodu XY, namiesto toho sa uplatňuje opatrenie YZ.“ Auditor podľa toho vie posúdiť, či ste niečo nevynechali.

ROZSAH DOKUMENTÁCIE

- Vyhláška určuje obsah dokumentácie a detailne rozpisuje opatrenia pre jednotlivé oblasti.
- Dokumentácia musí preukázateľne popísať ich implementáciu.
- Rozsah všeobecných opatrení je daný pre každú oblasť podľa §20 ods.2 zákona (Príloha č. 1) a určuje sa na základe analýzy rizík.

V prílohe č. 1 vyhlášky sú vymenované oblasti bezpečnostných opatrení. Pre každú túto oblasť je v prílohe uvedené, čo minimálne treba zabezpečiť, aké evidencie viesť atď.

Dokumentácia musí preukázateľne popisovať implementáciu opatrení v každej tejto oblasti. Nestačí povedať „riešime fyzickú bezpečnosť“, treba uviesť konkrétne ako.

V praxi si môžete predstaviť obsah dokumentácie opatrení ako zoznam kapitol podľa oblastí: 1.

Organizácia a personál 2. Riadenie prístupu 3.

Prevádzková bezpečnosť a riadenie zmien 4. Sieťová a komunikačná bezpečnosť 5. Akvizícia, vývoj a údržba (bezpečný vývoj) 6. Fyzická bezpečnosť a

bezpečnosť
prostredia 7. Riešenie incidentov 8. Kryptografia a
bezpečnosť kontinuity ... plus prípadne ďalšie podľa
potreby.

KLÚČOVÉ OBLASTI I: ORGANIZÁCIA A PERSONÁL

- **Organizácia a riadenie:** Písomne definované politiky a postupy implementujúce základné zásady:
 - Najnižších privilégii (Least Privilege, pol. 6).
 - Oddelovania zodpovedností (Segregation of Duties, pol. 7).
 - Potreby poznať (Need-to-Know, pol. 8-9).
 - **Personálna bezpečnosť:** Dokumentácia pokrývajúca celý životný cyklus zamestnanca (64-75):
 - Postupy pri nástupe a odchode (pol. 64,70-71,19).
 - Písomný plán rozvoja bezpečnostného povedomia a vzdelávania (pol. 66).
 - Záznamy o vykonaných školeniach (pol. 67).
-

25

Firma mala pravidlo, že keď odchádza zamestnanec, IT oddelenie zruší jeho účty do 24 hodín. Nemali to však zdokumentované ani skontrolované – stalo sa, že odídený zamestnanec mal prístup ešte týždeň a medzitým sa s kolegom dohodol a stiahol nejaké dáta. Toto by správne nastavený a zdokumentovaný proces minimalizoval (HR by malo povinnosť informovať IT, IT by malo checklist – a auditor by si mohol hocikedy vypýtať záznamy o zrušení prístupov a overiť, že to sedí).

KLÚČOVÉ OBLASTI I: ORGANIZÁCIA A PERSONÁL

- **Roly a zodpovednosti:**

- Musia byť určené a zdokumentované.
- V zmluvách musia byť uvedené povinnosti v oblasti KB (pol. 65).
- Musí existovať preukázateľné oboznámenie s politikami (pol. 67).
- Musí byť nastolený disciplinárny proces pri porušení (pol. 69).

Taktiež, ak niektoré bezpečnostné povinnosti plnia tretie strany, aj to musí byť určené (napr. externá firma spravuje vaše servery – v zmluve a dokumentácii je uvedené, že zodpovedá za aktualizácie a monitoring tých serverov).

Ak napr. zamestnanec opakovane prichytia, že si píše heslo na papierik pri monitor, a je to v rozpore s politikou, disciplinárny proces umožní manažérovi oficiálne ho napomenúť, prípadne pri hrubom porušení (povedzme úmyselné vynesenie dát) okamžite ukončiť pracovný pomer. To všetko by malo byť podchytené, aby v kritickej situácii nenastal chaos „čo s ním teraz“.

KLÚČOVÉ OBLASTI II: PRÍSTUPY A DODÁVATELIA

- **Riadenie prístupov:** Jedna z najkritickejších oblastí.
 - Politika riadenia prístupu (pol. 76, súvisiace 82-84).
 - Zdokumentované procesy pridelovania a odoberania práv (pol. 76-79).
 - Aktuálna evidencia prístupových práv (pol. 79-80).
 - **Preukázateľný záznam** o ročnej kontrole prístupových práv (pol. 80).
 - **RBAC a Least Privilege**, bezpečná autentizácia, obmedzenie privilegovaných prístupov (pol. 81-85).
 - **Riadenie dodávateľského reťazca:**
 - Evidencia zmlúv s tretími stranami (§ 4 ods. 1 písm. f)).
 - Zmluvy musia obsahovať bezpečnostné klauzuly (povinnosť hlásiť incidenty, právo na audit).
-

27

Politiku riadenia prístupu (podľa prílohy, položka 76 a ďalšie súvisiace body 82-85). Tá stanoví princípy: napr. každý užívateľ má svoj unikátny účet, zdieľané účty sú zakázané; pridelovanie práv sa riadi princípom najmenej privilegií; administrátorské účty sa používajú len na administráciu a majú dvojfaktorové overenie; atď. - Zdokumentované procesy pridelovania a odoberania práv (body 76-79). To znamená popísaný postup: keď príde nový zamestnanec, kto vyplní žiadosť o prístupy, kto to schváli, ako IT vytvorí účet; a naopak pri odchode zamestnanca ako sa

rušia prístupy. Mali by existovať formuláre alebo ticketovací systém, cez ktorý to ide, a tie záznamy sa uchovávajú. - Aktuálna evidencia prístupových práv (body 79-80). V praxi to môže byť zoznam všetkých užívateľských účtov a ich úrovni prístupu v jednotlivých systémoch. Auditor môže chcieť vidieť, či viete zistiť, kto má kam prístup. Najlepšie je, ak to viete exportovať z IAM nástroja alebo AD. - Preukázateľný záznam o pravidelnej kontrole prístupov (body 80). Vyhláška vyžaduje minimálne raz ročne preveriť, či pridelené prístupy sú stále odôvodnené

Predstavte si, že outsourcujete správu svojich serverov externej IT firme. Vďaka opatreniam v oblasti prístupov budete mať: - Zoznam administrátorských účtov, z ktorých vidno, že tí externisti majú len tie prístupy, ktoré potrebujú (a nemajú prístupy do iných systémov). - Budete mať zmluvu, kde je napísané, že tá firma musí hlásiť incidenty – a naozaj keď sa u nej stane napr. kompromitácia jedného admin účtu, má povinnosť vám to okamžite povedať. - Raz za rok urobíte stretnutie, kde si prejdete, či všetko funguje, a to zaznamenáte. - Keď príde NBÚ alebo auditor, ukážete mu: tu sú zmluvy, tu je seznam prístupov, tu je dôkaz, že každému adminovi sme skontrolovali, či jeho

prístupy sú OK a šéf IT to odklepol.

KLÚČOVÉ OBLASTI III: PREVÁDZKA A ZRANITEĽNOSTI

- **Bezpečnosť prevádzky a riadenie zmien:**
 - Formálny, schvaľovaný proces + proces výnimiek (Change Management, pol. 95-97).
 - Zdokumentované postupy pre riadenie kapacít (pol. 92).
- **Riadenie zraniteľností a aktualizácií:**
 - Zdokumentovaný proces riadenia záplat (Patch Management, pol.12-17, 99).
 - Záznamy o zmenách a prevádzkové logy (min. 12 mesiacov, pol 96, 116-117).
 - Zdokumentované odôvodnenie pre nenasadené záplaty a kompenzačné opatrenia.
 - Požiadavky týkajúce sa práv duševného vlastníctva (pol. 142).

Každá významná zmena v IT prostredí (napr. aktualizácia aplikácie, konfigurácia servera) by mala prejsť procesom: plán -> posúdenie rizík -> schválenie -> implementácia -> dokumentácia. Vyhláška (body 95-97) to priamo vyžaduje, vrátane procesu pre výnimky (t.j. ak je nutné spraviť urgentnú zmenu bez riadneho procesu, musí byť aj to ošetrené – následne sa dodatočne schváli ako výnimka). - Postupy pre riadenie kapacít (bod 92): aby nedošlo k výpadkom z dôvodu preťaženia, firma má monitorovať a plánovať kapacity (CPU, disk, sieťová priepustnosť atď.). Dokumentácia môže napr. uvádzať, že IT oddelenie mesačne vyhodnocuje kapacitné reporty a ak nejaký server beží nad 80% dlhodobo,

plánuje
Upgrade.

Väčšina útokov využíva známe zraniteľnosti alebo zlyhanie v procesoch. Zavedený change management a patch management výrazne znižujú tieto riziká.

KLÚČOVÉ OBLASTI IV: OCHRANA A SIETE

- **Ochrana proti škodlivému kódu:**
 - Definované pravidlá pre používanie a konfiguráciu antimalvérových systémov (pol. 98–100).
 - Dokumentácia o správnej konfigurácii (napr. zapnutá real-time ochrana, pol. 38, 43, 94).
- **Sieťová a komunikačná bezpečnosť:**
 - Detailná technická dokumentácia vrátane schémy sieťovej architektúry (pol 101-115 a (§ 4 ods. 2 písm. a–d)).
 - Zdokumentovaný a pravidelne revidovaný súbor pravidiel firewallu.
 - Aktuálny zoznam vstupno-výstupných bodov siete.

29

Používa centrálné antivírusy/antimalware na všetkých staniciach a serveroch, má nastavené pravidelné skeny, aktualizácie vírusových databáz, blokovanie nebezpečných príloh atď. - Dokumentácia by mala obsahovať aj popis konfigurácie – napr. „Na všetkých PC je nasadený antivírus ESET, ktorý beží s real-time ochranou (t.j. kontroluje súbory pri prístupe)

detailnú technickú dokumentáciu siete – to znamená spomínanú schému siete a popis, aké segmenty siete existujú, ako sú od seba oddelené (firewally, VLAN, DMZ), ako je riešené zabezpečenie Wi-Fi, pripojenie pobočiek, vzdialený prístup, atď

Zoznam vstupno-výstupných bodov siete – teda všetky miesta, kadiaľ ide komunikácia dovnútra alebo von

KLÚČOVÉ OBLASTI V: VÝVOJ A MONITOROVANIE

- **Akvizícia, vývoj a údržba systémov:**
 - Zdokumentované pravidlá pre bezpečný vývoj (Secure SDLC), ktoré musia dodržiavať interní aj externí vývojári, vrátane požiadaviek pri vývoji/získavaní aplikácií, oddelenia prostredí a bezpečného nasadzovania do produkcie. (pol. 35–56, 95–97).
 - Riadenie tretích strán vo vývoji a kontrolovanie ich činnosti (pol. 54)
 - **Monitorovanie a zaznamenávanie udalostí:**
 - Politika logovania (čo, kde a ako logovať, pol. 117-119).
 - Politika uchovávaní logov (ako dlho, pol. 116).
 - Zdokumentované postupy pre pravidelnú analýzu logov (pol. 118-120).
-

30

Secure Coding Guidelines

Vo firme majú SIEM (Security Information and Event Management) – super, centrálna zbiera logy.

Auditor ale zisťuje, či tam má niekto na starosti tie alerty, čo z toho chodia. Ak by povedali „máme SIEM, ale

momentálne nemáme ľudí na jeho sledovanie“, to by bol problém. Dokumentácia by mala uvádzať, že napr. SOC tím (či interný alebo externý) monitoruje 24/7 najdôležitejšie logy a reaguje do XY minút na kritické alarmy.

KLÚČOVÉ OBLASTI VI: FYZICKÁ BEZPEČNOSŤ A INCIDENTY

- **Fyzická bezpečnosť a bezpečnosť prostredia:**
 - Plán fyzickej ochrany a zdokumentované pravidlá pre vstup do zabezpečených priestorov (napr. serverovne, pol. 121-129).
 - Bezpečné postupy pre zaobchádzanie a likvidáciu médií a zariadení (pol. 130-138).
- **Riešenie kybernetických bezpečnostných incidentov:**
 - Detailné plány reakcie na incidenty (Incident Response Plans, pol. 20-26).
 - Postupy nahlásovania incidentov (interné a externé, cez JISKB).
 - Vedenie evidencie všetkých incidentov, ich riešení a ponaučení (pol. 20-26).

31

Organizácia zaznamenala ransomvér v sieti. Podľa plánu hneď zvolali incident response tím, odpojili kritické servery od siete, začali obnovovať zo záloh. Zároveň do 24 hodín nahlásili NBÚ, že majú incident (podľa vyhlášky 226/2025 ak to bol významný výpadok). NBÚ v spätnom pohľade ocení, že firma mala tieto postupy – možno jej dá menšie sankcie, ak všetko inak spravili správne. Keby nemali nič: panika, nikomu nepovedali, NBÚ by to možno zistil až o mesiac z médií – vtedy okrem škody z incidentu majú aj právny problém.

KLÚČOVÉ OBLASTI VII: KRYPTOGRAFIA A KONTINUITA

- **Kryptografické opatrenia:**
 - Politika používania kryptografie (kedy a ako šifrovať, 61-63, 102-103).
 - Zdokumentované pravidlá pre správu kryptografických kľúčov (Key Management, pol. 61-63).
- **Riadenie kontinuity činností:**
 - Plány obnovy po havárii (DRP) a plány kontinuity činností (BCP) (pol. 27-30).
 - Detailná stratégia a postupy zálohovania (pol. 31-34).
 - **Vedenie záznamov** o pravidelnom preverení záloh a testovaní obnovy (min. raz ročne, pol. 28 a 34).

32

určiť, kedy sa má povinne šifrovať a akými prostriedkami

To znamená, že ak používate šifrovanie, musíte mať proces, ako generujete, uchováвате, rotujete a rušíte kľúče.

Ide o plány, ako udržať alebo obnoviť prevádzku v prípade závažných výpadkov či katastrof. DRP je zameraný na IT (napr. „čo spravíme, ak nám zhorí serverovňa – máme záložnú lokalitu, prepneme do cloudu“), BCP je širší (napr. „čo ak vypadne 50% zamestnancov kvôli pandémie – ako zaistíme kľúčové procesy“)

Príklad: Predstavte si banku, ktorej dátové centrum vytopí voda. Ak má DR plán, tak vie do 2 hodín

prepnúť

na záložné centrum v inom meste a klienti si možno ani nevšimnú väčší problém. Bez plánu by možno bola týždeň offline – čo je neprijateľné. Z pohľadu dokumentácie by mala mať spracovaný dokument

„DRP

dátového centra“ s postupmi, kontakty na dodávateľov generátorov, postup obnovy serverov z záloh atď.

Auditor môže kontrolovať, či existujú tie dokumenty a či sa aj cvičili

DÔSLEDOK: DÔRAZ NA PREUKÁZATEĽNÉ ZÁZNAMY

Kľúčovým zámerom legislatívy je, že nestačí mať politiky a postupy len napísané; organizácia musí byť schopná **preukázať, že sa nimi aj riadi**.

- **Požiadavka na dôkazy:** Vyhláška systematicky opakuje požiadavky na „vedenie záznamov“, „evidenciu“, „pravidelné preverovanie“ a „testovanie“.
- **Otázka audítora:** Nebude znieť "Máte politiku?", ale „Ukážte mi záznamy z revízií prístupových práv za posledných 12 mesiacov, ako to vyžaduje Prílohu č. 1 a § 4–5 Vyhlášky.“.
- **Potreba systémov:** Organizácie musia implementovať systémy (napr. ticketovacie, log management), ktoré generujú a uchovávajú tieto dôkazy.
- **Nedostatočnosť papierovej formy:** Papierová dokumentácia bez dôkazov o reálnom výkone pri audite neobstojí.

PILIER IV: ANALÝZA RIZÍK KB

Motor rozhodovania

- Analýza rizík je ústredný proces, ktorý poháňa rozhodovanie o tom, ktoré bezpečnostné opatrenia, v akom rozsahu a s akou prioritou implementovať.

Je to cyklický proces v PDCA

Povedzme, že v analýze rizík identifikujeme riziko „Zlyhanie hlavného databázového servera“. Pravdepodobnosť stredná, dopad vysoký (niekoľko dní výpadku služby). Analýza navrhne opatrenie: zaviesť clustering alebo záložný server. Ak by firma nemala analýzu, možno by ich nenapadlo investovať do redundancie, kým by reálne server neskolaboval. Vďaka analýze to zistia dopredu a predídu výpadku. To je len jeden príklad – analýza riskov systematicky prejde všetky aktíva a scenáre.

OBSAH DOKUMENTÁCIE ANALÝZY RIZÍK

Dokumentácia musí obsahovať minimálne:

- Identifikáciu aktív, hrozieb a zraniteľností.
 - Identifikáciu a analýzu rizík (ohodnotenie pravdepodobnosti a dopadu).
 - Určenie vlastníka pre každé riziko.
 - **Plán ošetrovania rizík (Risk Treatment Plan):** Najdôležitejšia časť, ktorá obsahuje informáciu, ktoré opatrenia sú a ktoré nie sú implementované, spolu s **odôvodnením**.
 - Analýzu funkčného dopadu (Business Impact Analysis - BIA).
-

35

Plán ošetrovania rizík (Risk Treatment Plan) – to je najdôležitejšia časť analýzy rizík.

Obsahuje prehľad všetkých identifikovaných rizík a informáciu, čo s nimi organizácia urobila: ktoré opatrenia

zaviedla alebo zavedie, aby riziko znížila; ktoré riziká akceptuje (napr. sú malé, netreba nič špeciálne robiť); ktoré riziká preniesla (napr. poistenie); a hlavne musí obsahovať odôvodnenie pre tie riziká, kde možno neimplementovala nejaké odporúčané opatrenie.

Napríklad: riziko X – navrhované opatrenie bolo kúpiť nový firewall, ale rozhodli sme sa riziko akceptovať, lebo existujúci firewall postačuje podľa posudku. Toto odôvodnenie musí byť jasné a schválené vedením. -

Analýzu funkčného dopadu (Business Impact Analysis – BIA) – to je pohľad zhora na dopady na biznis pri rôznych scenároch výpadku. Napríklad BIA definuje, ktoré procesy sú najkritickejšie, aké sú tolerovateľné doby ich výpadku (RTO – Recovery Time Objective) a aké množstvo dát môžeme stratiť (RPO – Recovery Point Objective). Tieto informácie sú základom pre plány kontinuity (aby sme vedeli, koľko záložných kapacít treba, aká rýchla má byť obnova). Výsledný dokument býva dosť rozsiahly – obsahuje často tabuľky rizík. Dôležité je, že vedenie ho musí schváliť. Tým vedenie schvaľuje aj, ktoré riziká sa akceptovali bez opatrení.

ŠPECIFICKÁ POŽIADAVKA: ANALÝZA POLITICKÉHO RIZIKA

Zákon v § 20 ods. 5

zavádza povinnosť vykonať analýzu **politického rizika tretích strán (dodávateľov)**, ktorá presahuje tradičnú technickú analýzu.

- **Faktory:** Posudzuje sa najmä možnosť ovplyvňovania dodávateľa štátom, ktorý nie je členom EÚ a NATO, jeho vlastnícka štruktúra a legislatíva cudzieho štátu.
- **Strategický dopad:** Riadenie bezpečnosti sa mení z technickej disciplíny na strategický proces.
- **Výber dodávateľa:** Pri výbere kľúčových technológií už nerozhoduje len cena a technické parametre, ale aj geopolitický kontext a hĺbková previerka dodávateľa.
- **Politické riziká:** Schvaľuje vláda SR (na základe stanoviska NBÚ), zverejnené v JISKB.

Dôsledok: Strategické riadenie dodávateľského reťazca

- Bezpečnostné opatrenia sa **prijímajú a realizujú** na základe analýzy rizík. Súčasťou je aj **analýza politického rizika tretej strany**.
- Riadenie kybernetickej bezpečnosti už nie je **výlučne technickou záležitosťou**, ale **strategickým procesom**, ktorý zahŕňa **geopolitické a hodnotové aspekty**.
- PZS **musí** analyzovať závislosti aktív, IS a služieb tretích strán v dodávateľskom reťazci a vyhodnocovať dopady incidentov. Výsledky tvoria **podklad pre rozhodnutia a plán ošetrovania rizík**.
- Z dôvodu **analýzy rizík** môže organizácia **vylúčiť** niektorých dodávateľov z verejného obstarávania, aj keď ich ponuka bola technicky či cenovo výhodná, ak by **predstavovali bezpečnostné riziko**.
- **Výsledky analýzy rizík**, rozhodnutia a odstránené / zmiernené riziká slúžia ako **dôkaz**, že organizácia konala **v súlade so zákonom** a bezpečnostnými záujmami SR a EÚ.

PILIER V: ZÁVEREČNÁ SPRÁVA Z AUDITU KB

Spätná väzba a overenie

- Audit slúži ako nezávislý a objektívny mechanizmus overenia, ktorý uzatvára riadiaci cyklus a poskytuje kľúčovú spätnú väzbu pre neustále zlepšovanie.

ÚLOHA AUDITU V DOKUMENTÁCI

Záverečná správa z auditu sa stáva **neoddeliteľnou súčasťou** bezpečnostnej dokumentácie (§ 4 ods. 1 písm. g) vyhl. 227/2025).

Hlavnou úlohou auditu je overiť dve kľúčové skutočnosti:

- 1. Súlad dokumentácie s realitou:** Overuje, či dokumentácia presne popisuje reálny stav.
- 2. Účinnosť implementovaných opatrení:** Posudzuje, či sú opatrenia funkčné a efektívne pri znižovaní rizík.

Audit je **odborný, nestranný a dôkazmi podložený**. Môže byť vykonávaný iba **certifikovaným audítorom KB** (vyhl. 493/2022 § 1 ods. 1–2, 5).

DÔSLEDOK: ŽIVÝ A CYKLICKÝ CHARAKTER DOKUMENTÁCIE

Zaradenie správy z auditu priamo do dokumentácie vytvára silný mechanizmus spätnej väzby.

- **Nemožno ignorovať zistenia:** Neriešené nezhody sú okamžite viditeľné pri nasledujúcom audite, keďže správa je súčasťou dokumentácie (pol. 26, 28, 34).
- **Uzatvorenie cyklu PDCA:** Nálezy z auditu sú vstupom pre nápravné opatrenia, čím sa zabezpečuje neustále zlepšovanie (pol. 58–60).
- **Požiadavka na zdroje:** Manažment musí alokovať zdroje nielen na vykonanie auditu, ale aj na odstránenie zistených nedostatkov (pol. 4).

SLOVNÍK POVINNOSTÍ - KLÍČOVÉ SLOVÁ

Klíčové slovo/Typ povinnosti	Příklad implikace
Dokumentácia, Zdokumentovať	Celý systém riadenia musí byť písomne popísaný a udržiavaný.
Stratégia, Politiky, Postup, Plán	Povinnosť vytvoriť a schváliť hierarchiu riadiacich dokumentov.
Evidencia, Záznam	Povinnosť viesť dôkazy o vykonaných aktivitách (kontroly, incidenty, zálohy).
Pravidelne preverovať, Testovať	Povinnosť nielen zaviesť, ale aj aktívne a pravidelne overovať funkčnosť.

Legislatíva používa kľúčové slová, ktoré signalizujú dokumentačnú alebo procesnú povinnosť. Príklady z registra povinností:

ŽIVOTNÝ CYKLUS DOKUMENTÁCIE

Kľúčovým posolstvom legislatívy je požiadavka na aktuálnosť. Dokumentácia je „živý“ organizmus, ktorý sa neustále vyvíja prostredníctvom:

- **Pravidelných revízií a preskúmaní:** Napr. ročná kontrola prístupových práv a ročné preskúmanie rizík
 - **Aktualizácií po zmenách:** Pri akejkoľvek významnej zmene v IT prostredí alebo procesoch.
 - **Aktualizácií po incidentoch:** Ponaučenia (lessons learned) sa musia premietnuť do aktualizácie dokumentácie.
 - **Aktualizácií po auditoch:** Odstránenie nezhôd a následná revízia dokumentov.
 - **Evidencie a schvaľovania:** verzovanie, dátum účinnosti, zodpovedná osoba, schválenie vedením
-

ZÁVEREČNÉ ZHRNUTIE

- **Robustný rámec:** Zákon o kybernetickej bezpečnosti a jeho vyhláška nepredstavujú byrokratickú záťaž, ale poskytujú logicky štruktúrovaný a medzinárodne uznávaný rámec pre riadenie rizík.
- **Kľúčový nástroj:** Komplexná, aktuálna a pravdivá bezpečnostná dokumentácia je nielen zákonnou povinnosťou, ale predovšetkým overiteľným nástrojom, ktorý umožňuje organizácii:
 - Preukázať náležitú starostlivosť.
 - Efektívne riadiť svoje bezpečnostné investície.
 - Chrániť svoje kľúčové služby a aktíva.