ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 2:
Zodpovednosť regulovaných subjektov, Časť. 2

JUDr. Michal Rampášek

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

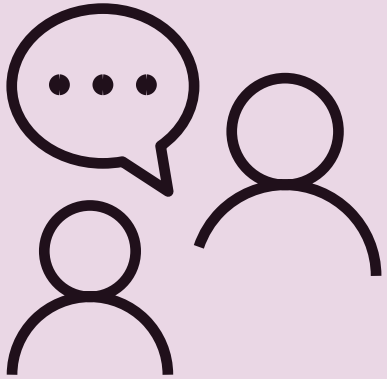
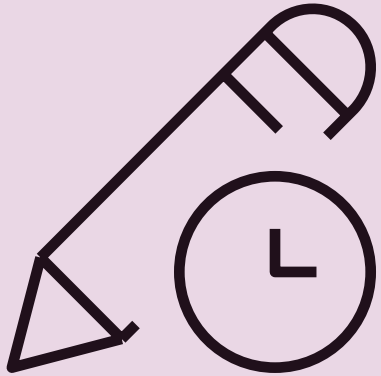
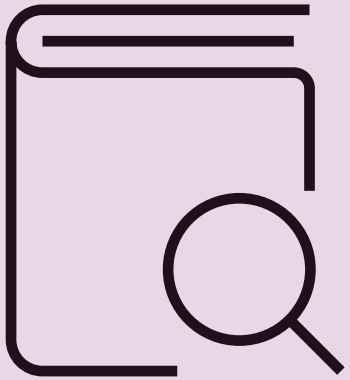
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

- Bezpečnosť dodávateľského reťazca a tretích strán
- KB incidenty, hrozby, udalosti
- Zraniteľnosti a Koordinované zverejňovanie zraniteľností
- Národná jednotka SK-CERT a iné jednotky
- Audit a samohodnotenie
- Dohľad a právomoci NBÚ
- Poistenie kybernetických rizík

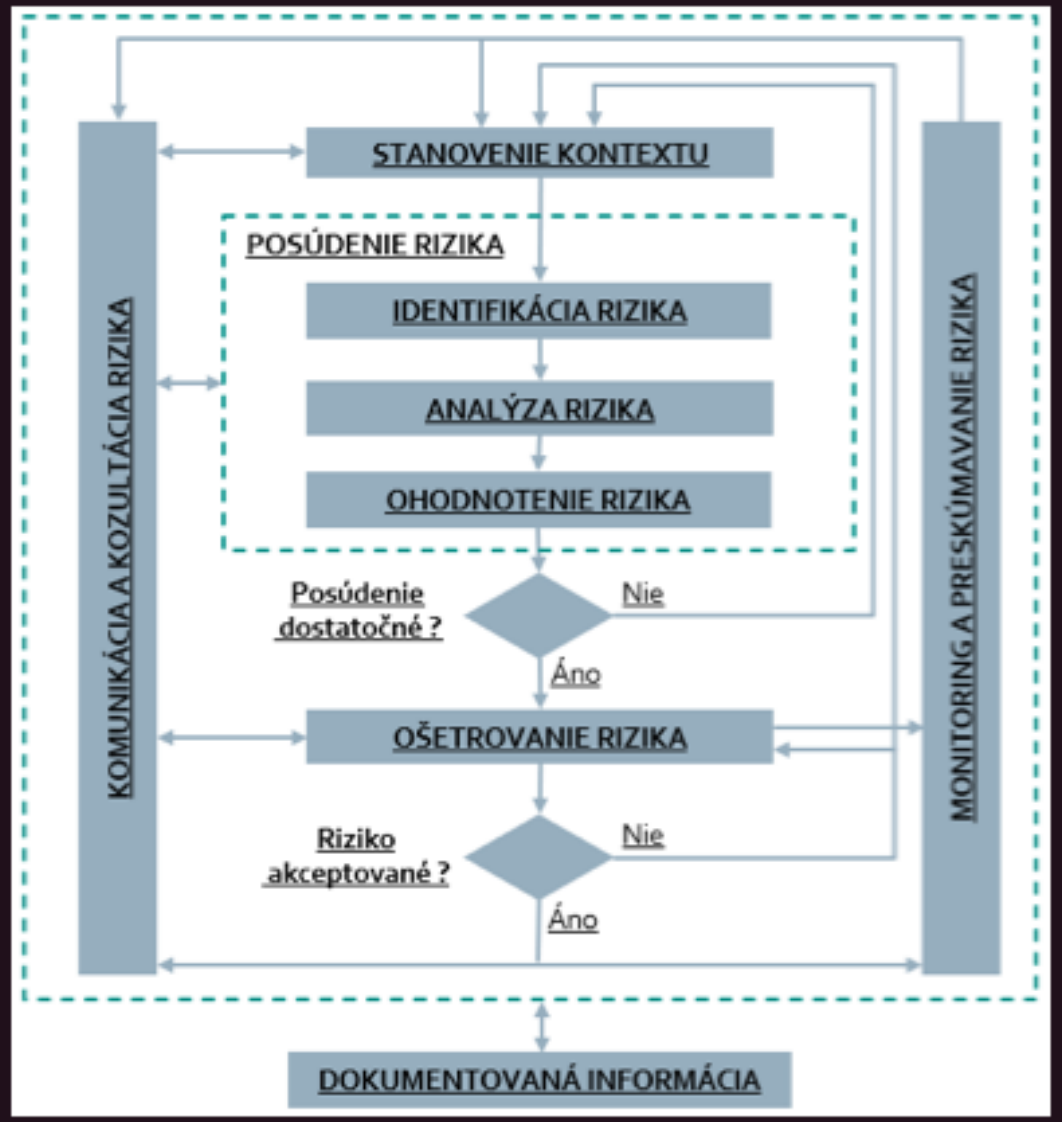
ÚVOD

RIADENIE RIZÍK DODÁVATEĽSKÉHO REŤAZCA

Proces riadenia rizika

- štatutárne vedenie organizácie je vlastníkom rizika, rozhoduje aj o akceptovaní rizika



https://www.nbu.gov.sk/data/att/3446.pdf

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

Povinnosti PZS – Analýza rizík ako súčasť riadenia rizík organizácie

- Analýza rizík organizácie - Analýza rizík má slúžiť k podrobnému rozboru stavu kybernetickej a informačnej bezpečnosti v organizácii. Cieľom analýzy rizík má byť identifikácia, analýza a evaluácia okolností, ktoré potenciálne môžu narušiť bezpečnosť (t. j. hrozieb, zraniteľností, scenárov rizík a škodlivých udalostí).

- PZS je povinný ...**v závislosti od vykonanej analýzy rizík** prijať, dodržiavať a vykonávať ... bezpečnostné opatrenia (§ 19 ods. 1 ZoKB, § 7 ods. 1 Vyhlášky č. 227/2025),
  - Rozsah všeobecných bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona je uvedený v prílohe č. 1 a určuje sa na základe analýzy rizík (§ 3 ods. 2 Vyhlášky č. 227/2025).
  - **Bezpečnostná dokumentácia obsahuje aj vykonanú analýzu rizík** a určenie úrovne identifikovaných rizík, akceptovaných rizík a zvyškových rizík pre aktíva spolu so zoznamom aktív (§ 4 ods. 1 písm. e) Vyhlášky č. 227/2025).
  - **Riadenie rizík** obsahuje a) identifikáciu aktív b) identifikáciu rizík, **c) analýzu rizík,** d) hodnotenie rizík, e) prijatie bezpečnostných opatrení, f) preskúmavanie identifikovaných rizík najmenej raz ročne a v závislosti od výsledkov aj aktualizáciu rizík a revíziu prijatých bezpečnostných opatrení. **(**§ 5 ods. 1 písm. e) Vyhlášky č. 227/2025**)**

Povinnosti PZS – Analýza rizík, BIA

- Až na základe vykonanej analýzy rizík si PZS

a) určí potrebu ošetrovania rizík a

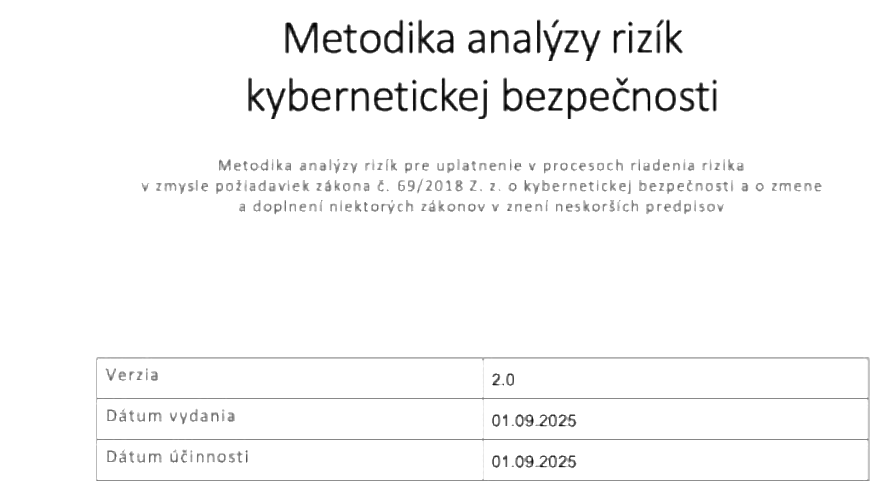
b) navrhne vhodné bezpečnostné opatrenia a vyberie tie, ktoré prijme a ktoré bude dodržiavať a vykonávať.

- Riadenie rizík okrem identifikácie aktív, identifikácie rizík, analýzy rizík, či prijatia bezpečnostných opatrení v závislosti od identifikovaných rizík obsahuje aj **analýzu funkčného vplyvu (BIA),** ktorá pozostáva z hodnotenia vplyvu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom

Metodika NBÚ 2.0

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

https://www.nbu.gov.sk/data/att/3446.pdf



Metodika analýzy rizík kybernetickej bezpečnosti

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Verzia	2.0
Dátum vydania	01.09.2025
Dátum účinnosti	01.09.2025

Riadenie rizík dodávateľského reťazca

- Organizácie často používajú rámce ako:

1. **ENISA Good practices for supply chain cybersecurity (2023)**
2. **ISO/IEC 27036 – Information security for supplier relationships**
3. **NIST SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**

Proces riadenia rizík dodávateľského reťazca

Cyklus riadenia rizík kybernetickej bezpečnosti dodávateľského reťazca IKT/OT

ENISA Good practices for supply chain cybersecurity (2023) https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

Povinnosti PZS – Analýza rizík dodávateľa

- každý dodávateľ, ktorý ovplyvňuje primárne aktíva, sa stáva súčasťou sekundárnych aktív.
- pri uzatvorení zmluvy sa vykonáva analýza rizík (§ 19 ods. 2 , veta za bodkočiarkou ZoKB, § 7 ods. 1 Vyhlášky č. 227/2025),

Povinnosti PZS – Zmluva s dodávateľom

- **Uzatvoriť** s treťou stranou zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností **(**§ 19 ods. 2) **Výnimky** z povinnosti: dodávateľ je PZS, nízke riziko dodávateľa.
- **Tretia strana je** dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre PZS.

- PKZS je povinný úradu hlásiť uzatvorenie zmluvy s treťou stranou, **ktorá má významný vplyv** pri zabezpečovaní kybernetickej bezpečnosti a aj jej ukončenie (tretia strana sa **zapisuje do registra PZS)** (§ 19 ods. 7)

Povinnosti PZS – Minimálne náležitosti zmluvy

Zmluva podľa § 19 ods. 2 zákona obsahuje najmä

- a) záväzok dodávateľa na výkon činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby (ďalej len „tretia strana“) dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
- b) vyjadrenie súhlasu tretej strany s uvedenými bezpečnostnými politikami,
- c) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany,
- d) ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení.

(§ 7 ods. 2 Vyhlášky 227/2025 Z.z.)

Bezpečnostné opatrenia v dodávateľskom reťazci

- Konkrétne položky uvádzané v prílohe č. 1 k vyhláške č. 227/2025 Z. z. (aj položky 145. až 151.) nemožno vnímať ako povinnosti, nakoľko rozsah všeobecných bezpečnostných opatrení (aj pre dodávateľský reťazec) určuje PZS následne až na základe vykonanej analýzy rizík a analýzy funkčného vplyvu (BIA).

Bezpečnostné opatrenia v dodávateľskom reťazci

Položka	Bezpečnostné opatrenia pre dodávateľský reťazec podľa § 20 ods. 2 písm. q) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
145.	sú definované a zavedené procesy a postupy na riadenie kybernetických rizík spojených s používaním produktov, procesov alebo služieb tretích strán	ÁNO	ÁNO	ÁNO	ÁNO
146.	na riadenie informačnej bezpečnosti a kybernetickej bezpečnosti vo vzťahoch s tretími stranami je s každou treťou stranou s významným vplyvom uzatvorená zmluva podľa § 19 ods. 2 zákona	ÁNO	ÁNO	ÁNO	ÁNO
147.	uzatvoreniu zmluvy podľa § 19 ods. 2 zákona predchádza analýza rizík dodávateľských služieb alebo iných dodávateľských činností	ÁNO	ÁNO	ÁNO	ÁNO
148.	súčasťou zmluvy podľa § 19 ods. 2 zákona sú bezpečnostné požiadavky špecifické pre informačné a komunikačné technológie alebo operačné technológie	ÁNO	ÁNO	ÁNO	ÁNO
149.	bezpečnostné opatrenia sú uplatnené v dodávateľskom reťazci produktov a služieb, ktorý priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
150.	sú pravidelne, najmenej raz za dva roky monitorované, preskúmavané, vyhodnocované a riadené zmeny v postupoch a v poskytovaní služieb alebo iných činností tretích strán, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
151.	sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky pre používanie cloudových služieb a riadená kybernetická bezpečnosť pri používaní cloudových služieb	ÁNO	ÁNO	ÁNO	ÁNO

Odporúčania

- uvedené aktuálne kontakty a eskalačná procedúra
- zavedený systém riadenia bezpečnosti
- mať vlastný proces risk managementu a osobitne hodnotiť riziká, ktoré môžu zasiahnuť odberateľa (napr. incidenty, výpadky, úniky).
- určené roly, prístupové oprávnenia, zodpovednosť za politiky. Právo veta na zamestnanca dodávateľa
- pravidelné bezpečnostné školenia a komunikovať zmeny
- zavedené riadenie zraniteľností a patch management, bezpečnostné testovanie a riešiť nálezy v stanovených lehotách.
- riadenie zmien v IKT a bezpečný vývoj (vrátane bezpečnostné aktualizácie)
- Subdodávatelia
- uchovávanie logov po určenú dobu
- ochrana dát a práv duševného vlastníctva
- exit plán
- ochrana a spracúvanie údajov v cloude
- osobitné opatrenia pri používaní a integrácií systémov a modelov AI
- mlčanlivosť, Zmluva NDA
- zosúladenie zo Zmluvou o spracúvaní osobných údajov (GDPR)

RIADENIE UDALOSTÍ A INCIDENTOV

Udalosti

kybernetický bezpečnostný incident

kybernetická hrozba

udalosť odvrátená v poslednej chvíli

zraniteľnosť

KB incident

„udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov "(§ 3 ods. 1)

PZS aj PKZS povinne hlásia len **závažný KB incident** (§ 24 ods. 2)

a) **rozsiahly** incident alebo

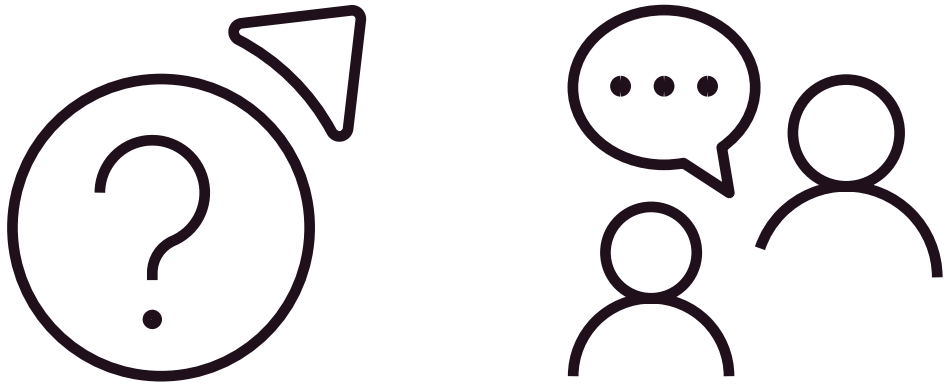
b) ak spôsobil alebo môže spôsobiť **závažné narušenie fungovania** PZS alebo škodu či ujmu **min. 650.000 EUR** alebo

c) škodu či ujmu iným osobám **min 250.000 EUR,** alebo

d) + **významný incident** podľa Vykonávacieho nariadenia 2024/2690 alebo **incident** podľa Zákona o kritickej infraštruktúre (Príloha č. 1 Vyhláška NBÚ č. 226/2025)

Dobrovoľné hlásenie

Skúmanie zavinenia incidentu



Rozsiahly KB incident

„incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť Slovenskej republiky naň reagovať, alebo ktorý má významný vplyv aspoň na dva členské štáty Európskej únie “ (§ 3 ods.1 písm. n) ZoKB)

Závažné narušenie fungovania (Príloha č. 1 k Vyhláške 226/2025)

1.Úplný výpadok alebo nedostupnosť činnosti (viac ako 30/60 minút),

2. Narušenie alebo obmedzenie činnosti (viac ako 60/180 minút)

3. Ohrozenie chránených údajov (obchodné tajomstvo, profesijne tajomstvá, utajované skutočnosti)

4. Ohrozenie uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb,

5. Spôsobenie hospodárskej straty vyššej ako 0,1 % HDP,

6. Spôsobenie škody najmenej 1 užívateľovi viac ako 250 000 eur,

7. Vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni alebo spôsobenie viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo úmrtie aspoň jednej osoby, alebo

8. Neoprávnený prístup alebo znefunkčnenie siete alebo informačného systému a ktorá by mohla spôsobiť následky uvedené v prvom až siedmom bode, alebo Významné narušenie fungovanie iného PKZS, alebo Významným incident (Digi) alebo Incidentom v KI.

Významný incident (Nariadenie 2024/2690) – horizontálne kritériá

Incident ktorý spôsobil alebo môže spôsobiť

a) priamu finančnú stratu, ktorá prevyšuje 500 000 EUR alebo 5 % celkového ročného obratu;

b) únik obchodných tajomstiev príslušného subjektu

c) smrť fyzickej osoby

d) značné poškodenie zdravia fyzickej osoby

e) došlo k úspešnému, domnelo zlomyseľnému a neoprávnenému prístupu do sietí a informačných systémov, ktorý by mohol spôsobiť vážne narušenie prevádzky;

f) opakujúci incident

g) incident spĺňa aspoň jedno z kritérií špecifických pre subjekt ako sú uvedené v čl. 5 a nasl.

Opakujúci incident (Nariadenie 2024/2690)

Opakujúce sa incidenty sa považujú za jeden významný incident, ak spĺňajú všetky tieto kritériá (kumulatívne):

a) vyskytli sa aspoň dvakrát za šesť mesiacov;

b) majú rovnakú zjavnú hlavnú príčinu;

c) spoločne spĺňajú kritérium straty, ktorá prevyšuje 500 000 EUR alebo 5 % celkového ročného obratu

Významný incident (Nariadenie 2024/2690) – vertikálne kritériá

Špecifické prahy významnosti podľa typu poskytovateľa (DNS, TLD registre, cloud, dátové centrá, CDN, MSP/MSSP, online trhy, vyhľadávače, sociálne siete, dôveryhodné služby). Tým reflektuje, že rovnaká technická udalosť má úplne iné dôsledky v cloude než v dátovom centre alebo u DNS

Príklad rozdielnych podmienok činnosti pri cloud computing - dôraz na dostupnosť služba a dopad na užívateľov , naopak pri dátových centrách je „významnosť" užšie naviazaná na fyzickú prevádzku a kontrolu prístupu, nielen na počet používateľov.

Významný incident (Nariadenie 2024/2690) – cloud computing

V prípade poskytovateľov služieb cloud computingu, ak

a) poskytovaná služba cloud computingu je **úplne nedostupná dlhšie ako 30 minút**;

b) dostupnosť služby cloud computingu poskytovateľa je počas **viac ako 1 hodiny obmedzená pre viac ako 5 %/1mil. používateľov** služby cloud computingu v Únii;

c) integrita, dôvernosť alebo pravosť údajov súvisiacich s poskytovaním služby je ohrozená v dôsledku **domnelo zlomyseľného konania**;

d) integrita, dôvernosť alebo pravosť údajov súvisiacich s poskytovaním služby je ohrozená s dosahom na **viac ako 5 %/1 mil. používateľov** tejto služby cloud computingu v Únii.

Významný incident (Nariadenie 2024/2690) – dátové centrá

V prípade poskytovateľov služieb dátového centra ak

a) služba dátového centra prevádzkovaného poskytovateľom **je úplne nedostupná**;

b) dostupnosť služby dátového centra je **obmedzená viac ako 1 hodinu**;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov je ohrozená v **dôsledku domnelo zlomyseľného konania**;

d) fyzický prístup k dátovému centru je ohrozený.

Incident v kritickej infraštruktúre

“incidentom udalosť, ktorá môže významne narušiť alebo ktorá narúša poskytovanie základnej služby kritickým subjektom, alebo ktorá ovplyvňuje vnútroštátne systémy, ktoré chránia právny štát” (§ 2 písm. e) zákona č. 367/2024)

Kritický subjekt je povinný oznámiť ústrednému orgánu **každý incident, ktorý spĺňa prahové hodnoty uvedené ústredným orgánom v posúdení rizika**, ktoré zohľadnia najmä počet a podiel používateľov dotknutých narušením, trvanie narušenia a geografické územie dotknuté narušením s prihliadnutím na to, či je toto územie geograficky izolované.

Ďalšie incidenty

11 právnych aktov Únie s oznamovacími povinnosťami so spolu 31 samostatnými povinnosťami (napr. AI Act, CRA, eIDAS/eIDAS2, DORA).

Commission Staff Working Document, (SWD(2025) 836 final, Brussels, 19.11.2025, https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal. str. 181 - 190.

Zákon o ITVS (nemá vlastnú definíciu KB incidentu, ale odkazuje na definíciu KB incidentu podľa ZoKB)

Hrozba

„každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby " (čl. 2 ods. 8 nariadenia CSA)

„významnou kybernetickou hrozbou kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál spôsobiť závažný kybernetický bezpečnostný incident alebo môže mať iný závažný vplyv na sieť a informačný systém subjektu alebo používateľov služieb subjektu tým, že spôsobí škodu 250 000 EUR. (§ 3 písm. k) ZoKB)

PZS aj PKZS povinne hlásia len **významnú hrozbu** (§ 24 ods. 5 píms. a) ZoKB)

Udalosť odvrátená

„udalosťou odvrátenou v poslednej chvíli udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo"(§ 3 písm. p) ZoKB)

PZS aj PKZS povinne hlásia len **udalosť , ktorá mohla spôsobiť závažný KBI** (§ 24 ods. 5 píms. b) ZoKB)

Zraniteľnosť

„zraniteľnosťou akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou " (§ 3 písm. q ZoKB)

„slabá stránka, náchylnosť alebo chyba produktov IKT alebo služieb IKT, ktorá môže byť zneužitá kybernetickou hrozbou " (čl. 16 ods. 15 NIS2)

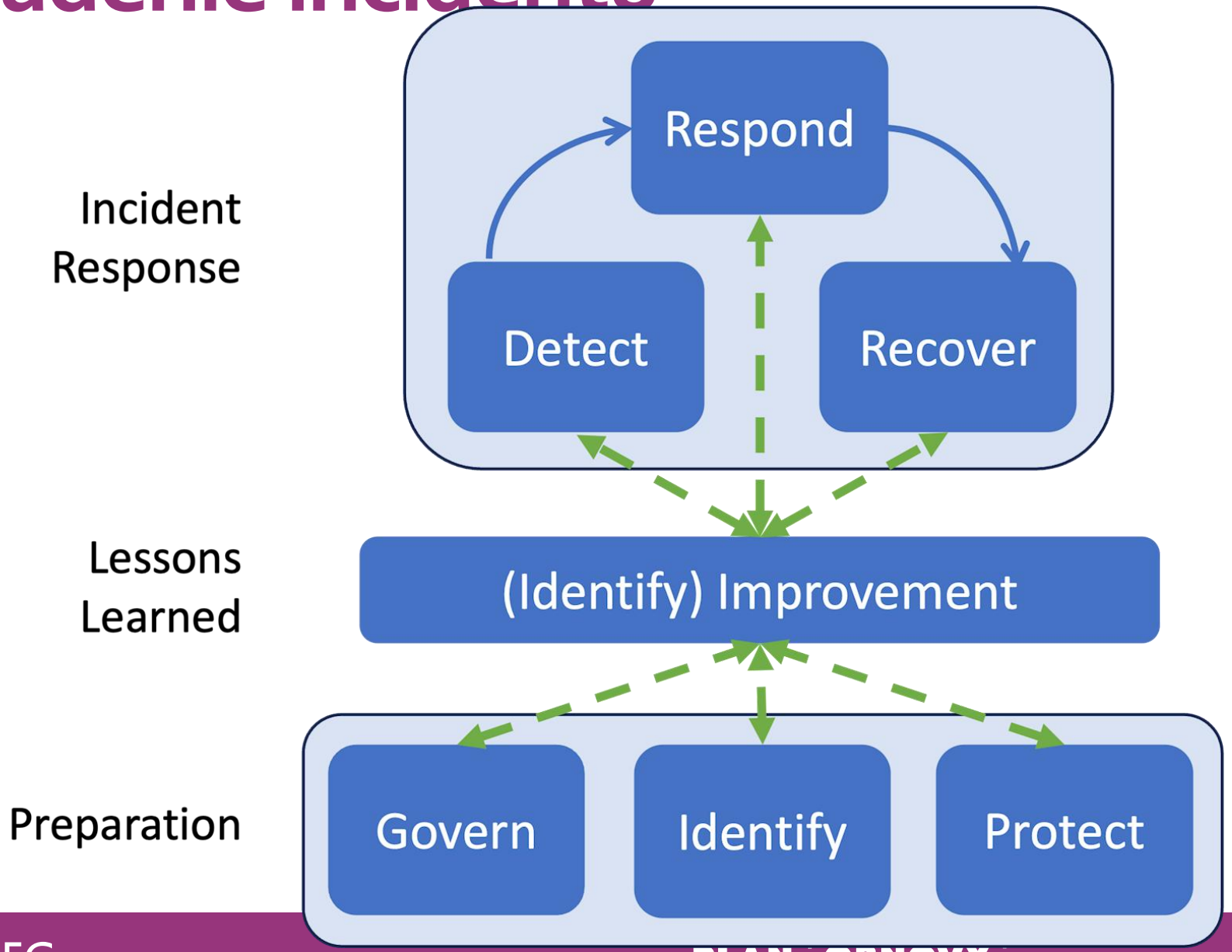
PZS aj PKZS povinne hlásia len **zraniteľnosť,**

a) **ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá**
b) **podľa dostupných informácií a technických znalostí**
c) **môže byť zneužitá na spôsobenie závažného KBI a**
d) **prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika**(§ 24 ods. 5 píms. c) ZoKB)

Bezpečnostné opatrenia –Riadenie udalostí

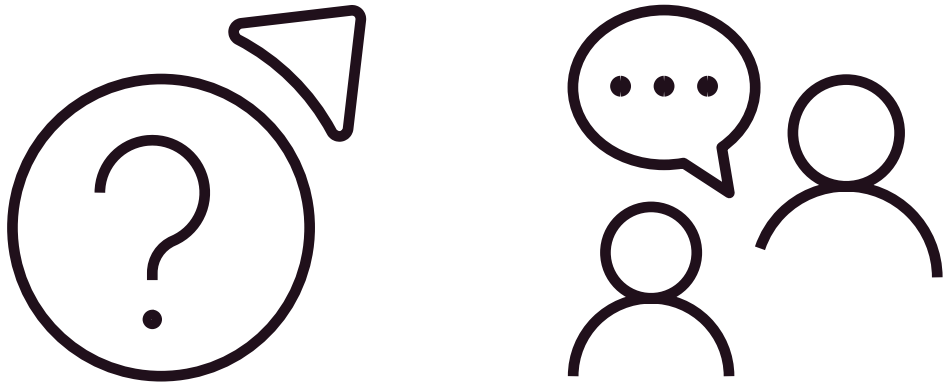
Položka	Bezpečnostné opatrenia pre riadenie udalostí a kybernetických bezpečnostných incidentov podľa § 20 ods. 2 písm. d) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
20.	je zabezpečené plánovanie a testovanie riešenia kybernetických bezpečnostných incidentov aspoň raz za kalendárny rok a sú definované, prijaté a oznámené procesy, úlohy a zodpovednosti v oblasti riešenia kybernetických bezpečnostných incidentov	ÁNO	ÁNO	ÁNO	ÁNO
21.	je zabezpečené posúdenie udalostí kybernetickej bezpečnosti a určenie ich priorít	ÁNO	ÁNO	ÁNO	ÁNO
22.	je definovaný systém reakcie na kybernetické bezpečnostné incidenty	ÁNO	ÁNO	ÁNO	ÁNO
23.	poznatky získané z riešených kybernetických bezpečnostných incidentov sú preukázateľne zohľadnené v procese riadenia kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
24.	sú zavedené a uplatňované postupy na identifikáciu, zhromažďovanie, získavanie a uchovávanie digitálnych stôp súvisiacich s kybernetickými bezpečnostnými incidentmi	ÁNO	ÁNO	ÁNO	ÁNO
25.	v prípade kybernetického bezpečnostného incidentu sú dodržiavané všetky stanovené bezpečnostné opatrenia a postupy	ÁNO	ÁNO	ÁNO	ÁNO
26.	sú definované a pravidelne, aspoň raz ročne testované pravidlá pre izoláciu kritických komponentov sietí, informačných systémov a operačných technológií počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	ÁNO	ÁNO	ÁNO	ÁNO

Riadenie incidentu



- NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (2025)

Role a zodpovednosti



Príklady

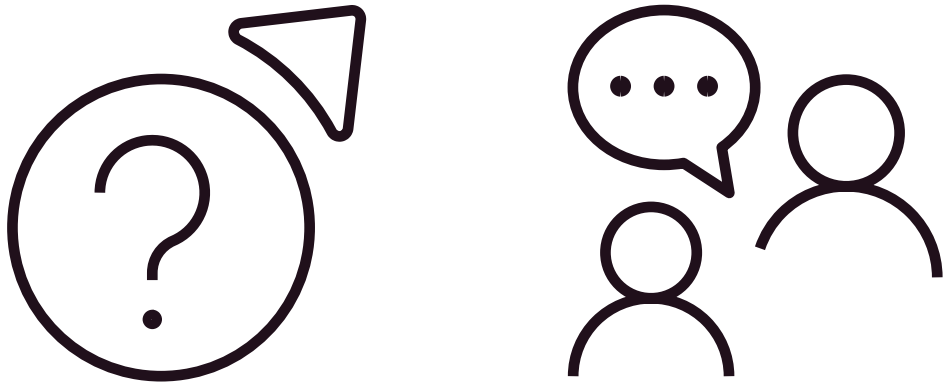
- Ľudské zdroje
- IT profesionály
- Vlastníci aktív
- Tlačové/mediálne oddelenie
- Fyzická bezpečnosť
- Právne
- Incident handlery
- Štatutárne vedenie

Role

- **Vedenie (Leadership):** riadi incident response na úrovni organizácie, prideľuje zdroje a rozhoduje o zásadných krokoch (napr. odstavenie alebo obnova kritických služieb).
- **Incident handleri / tím reakcie na incidenty:** potvrdzujú incident, zbierajú a analyzujú dôkazy, určujú priority zásahu, obmedzujú škody, hľadajú príčinu a obnovujú prevádzku; môžu byť interní alebo externí (SOC/MSSP).
- **IT/kybernetickí profesionáli :** bezpečnostní a systémoví architekti, správcovia sietí/cloudov, vývojári a ďalší technickí špecialisti, ktorí realizujú technické opatrenia pri zvládaní incidentu a obnove.
- **Právne oddelenie:** kontrolujú súlad postupov s právom (vrátane ochrany súkromia), posudzujú zmluvy s dodávateľmi, radia pri právnych dôsledkoch incidentu (reportovanie, trestné oznámenia, apod.).
- **Tlačové/mediálne oddelenie:** pripravujú a koordinujú externú komunikáciu, komunikáciu s médiami a verejnosťou; zabezpečujú konzistentné správy pri úniku informácií aj z iných zdrojov.
- **Ľudské zdroje:** riešia personálne procesy s dopadom na bezpečnosť (screening, onboarding/offboarding, zmeny rolí) a spolupracujú pri podozrení na interné zavinenie.
- **Fyzická bezpečnosť a správa budov :** riešia incidenty s fyzickým prvkom, koordinujú prístup do priestorov a k zariadeniam počas vyšetrovania (napr. uzamknutie kancelárie, serverovne).
- **Vlastníci aktív :** vlastníci systémov/dát/procesov určujú priority obnovy a požadovanú úroveň funkčnosti a priebežne dostávajú informácie o stave zásahu a obnovy.

NIST SP 800-61 Rev. 3

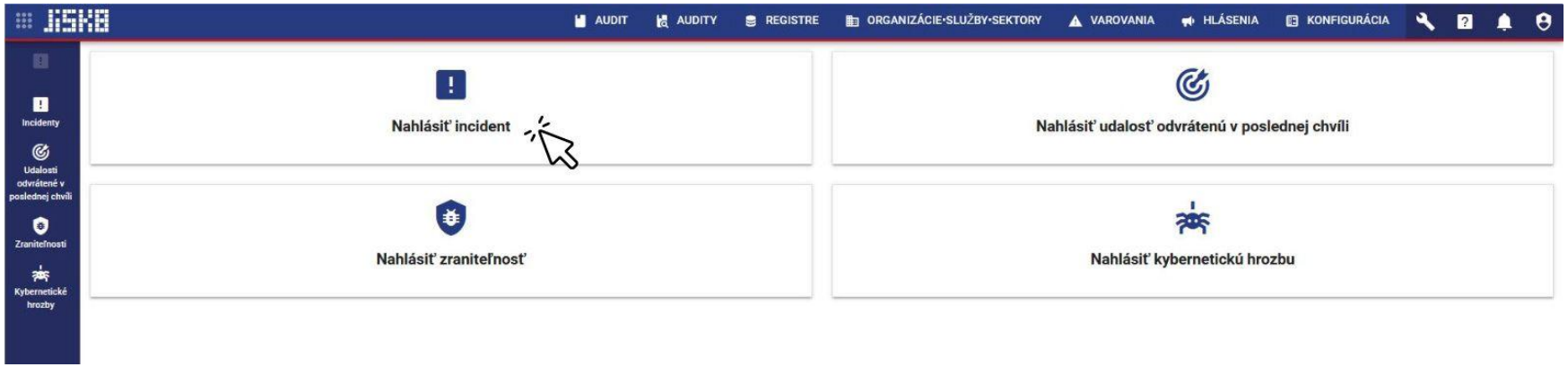
Politika riešenia incidentov



Odporúčania pre politiku

1. Vyhlásenie o záväzku vedenia
2. Účel a ciele politiky
3. Role a zodpovednosti
4. Definícia udalostí, incidentov v oblasti kybernetickej bezpečnosti, vyšetrovaní a súvisiacich pojmov
5. Záznam a monitorovania bezpečnosti IT
6. Hlásenia udalostí a eskalačné procedúry, kategorizácia incidentov
7. Riešenie KB incidentu a oznamovanie incidentov na CSIRT
8. Väzby na riadenie kontinuity činnosti (BCM)
9. Metrika riešenia incidentov (reakčné časy)

JISKB



PZS prostredníctvom jednotného informačného systému kybernetickej bezpečnosti hlási všetky udalosti

Digital Omnibus a revízia NIS2

- Návrh nariadenia **Digital Omnibus (COM/2025/837 final)**
- používanie **jednotného kontaktného miesta pre nahlasovania incidentov** stanovených v NIS 2 , GDPR, DORA, eIDAS a CER, a zefektívniť obsah nahlasovaných informácií **pri vypracúvaní spoločných vzorov** na podávanie správ pre NIS2 (čl. 23 ods. 11), CER alebo GDPR.
- Komisia môže prijať vykonávacie akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia (čl. 23 ods. 11 NIS2)
- Navrhuje sa výslovne **uvádzať údaje k ransomvérovému útoku:**

a) či subjekt zistil útok ransomware;

b) vektor útoku ransomware;

c) či boli vykonané opatrenia na zmiernenie následkov.

- na žiadosť CSIRT aj a) či subjekt dostal žiadosť o výkupné a prípadne od koho; b) či bolo výkupné zaplatené, a ak áno, v akej výške, akým spôsobom platby a komu alebo na aký účet, vrátane poskytovateľa kryptoaktív a poskytovateľa služieb kryptoaktív, ak je to relevantné.

Reaktívne opatrenia

- Reaktívne opatrenie je priama odpoveď na závažný kybernetický bezpečnostný incident a zabezpečuje sa službami jednotky CSIRT
- **Incident Handling** – ide o detekciu, riešenie incidentov, ich analýza, odozdva, ohraničenie a náprava následkov.
- **PZS má plniť povinnosti uloženej NBÚ prípade závažného KBI alebo významnej kybernetickej hrozby**

a) vykonať reaktívne opatrenie (pri nečinnosti alebo zjavnej neúspešnosti),

b) poskytnúť návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu („ochranné opatrenie“) (§ 27 ods. 1)

- PZS má povinnosť bezodkladne oznámiť a preukázať prostredníctvom JISKB **vykonanie reaktívneho opatrenia a jeho výsledok** (§ 27 ods. 6)

ÚLOHY NÁRODNEJ JEDNOTKY CSIRT

Jednotky CSIRT

- (3 akreditované) **Národná jednotka CSIRT** - NBÚ (SK-CERT), **Vládna jednotka** CSIRT - MIRRI (CSIRT.SK), Jednotka CSIRT – **Centrum pre kybernetickú obranu SR** (CSIRT.MIL.SK)
- Postavenie a úlohy (najmä § 6, § 15 a § 16 ZoKB)
- Reaktívne služby (§ 15 ods. 3 ZoKB)

Národná jednotka CSIRT (SK-CERT)

- Národné centrum kybernetickej bezpečnosti ako organizačná zložka NBÚ, ktorá má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku
- plní úlohy jednotky CSIRT pre všetky sektory a podsektory uvedené v prílohe č. 1 alebo v prílohe č. 2 okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán.
- Plnenie úloh NBÚ (SK CERT) nezbavuje PZS ani ústredný orgán zodpovednosti za plnenie povinností podľa ZoKB ani za plnenie povinností vo vzťahu k sieťam a informačným systémom podľa osobitných predpisov.
- Koordinátor v rámci procesu koordinovaného oznamovania zraniteľností
- Vykonáva neinvazívne zisťovanie a hodnotenie zraniteľností verejne prístupnej siete a informačného systému v kybernetickom priestore Slovenskej republiky, ktoré nemá negatívny vplyv

Preventívne služby

- vytváraním bezpečnostného povedomia, výcvikom,
- monitorovaním a evidenciou zraniteľností, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov,
- poskytovaním pomoci s monitorovaním siete a informačného systému alebo vykonávaním takéhoto monitorovania po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,
- vykonávaním neinvazívneho zisťovania a hodnotenia zraniteľností verejne prístupnej siete a informačného systému v rozsahu pôsobnosti jednotky CSIRT, ktoré nemá negatívny vplyv na tieto siete a informačné systémy, ako ani na služby, ktoré poskytujú a činnosti, ktoré zabezpečujú,
- vykonávaním hodnotenia zraniteľností, ktoré boli zistené podľa písmena h), po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,

Reaktívne služby

- výstraha a varovanie,
- detekcia kybernetických bezpečnostných incidentov,
- analýza kybernetických bezpečnostných incidentov,
- odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,
- asistencia pri riešení kybernetického bezpečnostného incidentu na mieste,
- reakcia na kybernetický bezpečnostný incident,
- podpora reakcií na kybernetické bezpečnostné incidenty,
- koordinácia reakcií na kybernetické bezpečnostné incidenty,
- návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

SPRÁVA ZRANITEĽNOSTÍ A HROZIEB

Zraniteľnosti a hrozby

- Povinnosť PZS analyzovať závislosti svojich aktív vrátane produktov IKT a služieb IKT tretích strán s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu. Mapovanie závislostí umožňuje: (i) správne vyhodnotiť relevanciu hrozby, (ii) určiť zraniteľné systémy a rozsah dopadu, (iii) nastaviť priority patchovania a mitigácií podľa rizika a vplyvu.
- Monitoring hrozieb (ICT/OT): Sledovanie informácií o nových typoch útokov špecifických pre informačné (ICT) aj operačné technológie (OT) v reálnom čase.
- Identifikácia zraniteľností: Pravidelné skenovanie aktív, auditovanie systémov a odoberanie bezpečnostných oznámení od dodávateľov a CSIRT jednotiek. To zahŕňa aj využívanie spravodajských informácií o hrozbách (threat intelligence)
- Hodnotenie: Analýza, do akej miery sú zistené zraniteľnosti zneužiteľné v kontexte konkrétnej infraštruktúry a aký majú vplyv na prevádzku.
- Mitigácia: Prijatie opatrení, ako sú aktualizácie (patching), izolácia zraniteľných systémov, zmena konfigurácie, alebo zavedenie dodatočných bezpečnostných prvkov.
- Spolupráca: Zdieľanie informácií o incidentoch a hrozbách (vrátane IOC) s relevantnými subjektami (napr. MISP).

Bezpečnostné opatrenia

Položka	Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb podľa § 20 ods. 2 písm. b) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
12.	je zabezpečená informovanosť o identifikovaných kybernetických hrozbách s cieľom prijať primerané bezpečnostné opatrenia vrátane kybernetických hrozieb špecifických pre informačné a komunikačné technológie a operačné technológie	ÁNO	ÁNO	ÁNO	ÁNO
13.	sú získavané informácie o zraniteľnostiach používaných informačných systémov vrátane hodnotenia, do akej miery sú tieto systémy zraniteľné a prijímania vhodných opatrení na ich mitigáciu	ÁNO	ÁNO	ÁNO	ÁNO
14.	je najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností	ÁNO	-	ÁNO	ÁNO
15.	je najmenej raz za 6 mesiacov vykonávané pravidelné posudzovanie zraniteľností	-	ÁNO	-	-
16.	sú určené priority aktualizácií na základe posúdenia rizík a analýzy vplyvov	ÁNO	ÁNO	ÁNO	ÁNO
17.	na webovom sídle sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností	-	ÁNO	-	ÁNO

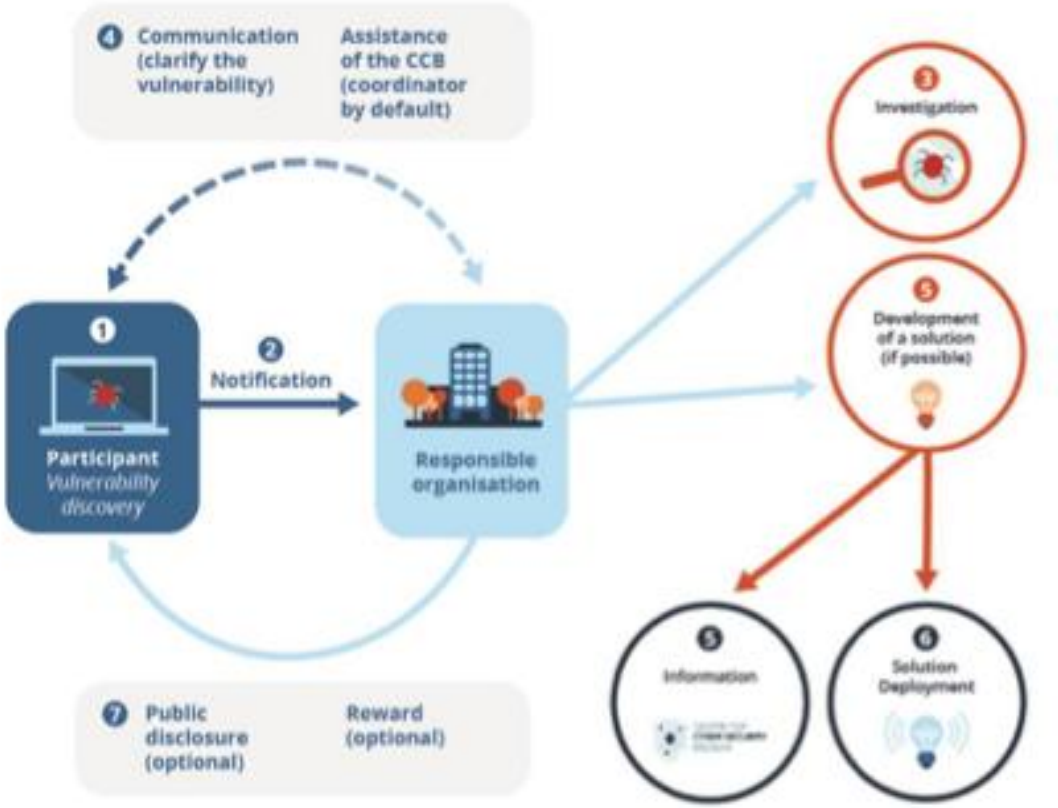
Koordinované zverejňovanie zraniteľností

- Koordinované zverejňovanie zraniteľností (Coordinated Vulnerability Disclosure, CVD) je kľúčové pre ochranu používateľov ako aj výskumu kybernetickej bezpečnosti. Tento mechanizmus zabezpečuje, že zraniteľnosti sú zverejnené až po tom, ako zodpovedné strany vyvinuli opravu, záplatu alebo poskytli opatrenia na zmiernenie hrozby, ktorú predstavuje zneužitie zraniteľnosti.

ENISA, https://www.enisa.europa.eu/topics/vulnerability-disclosure

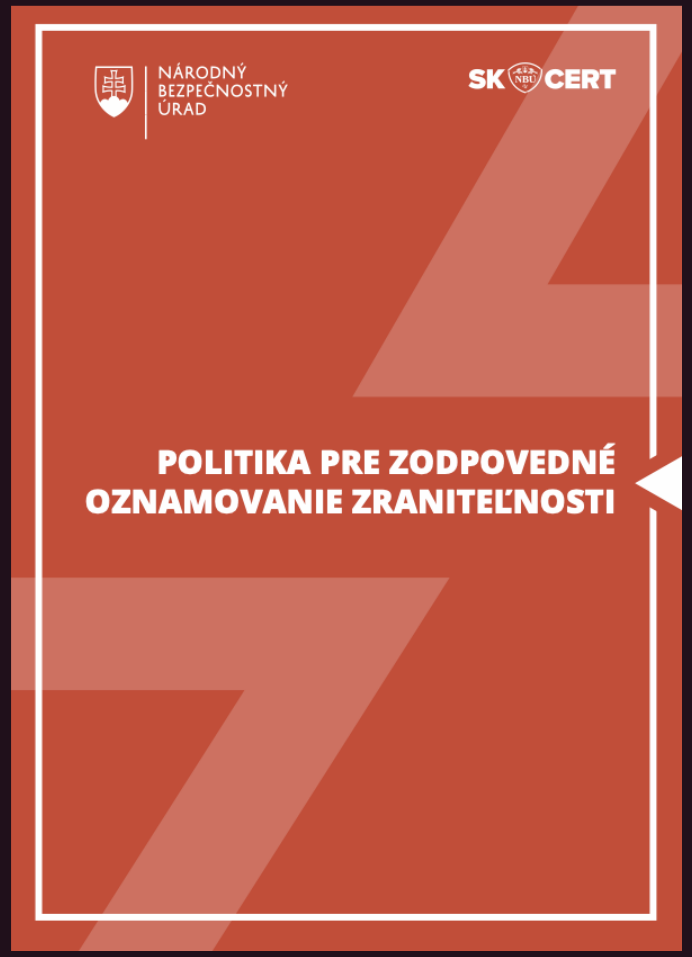
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Proces CVD



CCB BELGIUM: GUIDE TO COORDINATED VULNERABILITY DISCLOSURE POLICIES PART I: GOOD PRACTICES

Politika pre zodpovedné oznamovanie zraniteľnosti



- https://www.nbu.gov.sk/politika-pre-zodpovedne-oznamovanie-zranitelnosti/

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

AUDIT A SAMOHODNOTENIE

Audit

- Audit vykonáva **certifikovaný audítor** kybernetickej bezpečnosti podľa § 29 ods. 3 ZoKB
- Vykonať audit kybernetickej bezpečnosti **do dvoch rokov odo dňa zaradenia PZS** do registra PZS (§ 29 ods. 1), v rozsahu stanovenom podľa Vyhlášky 493/2022, a to **po každej zmene majúcej významný vplyv** na realizované bezpečnostné opatrenia **a v určenom časovom intervale** (§ 29 ods. 2 ZoKB) Audit sa vykonáva a) každé dva roky, audit sa musí začať do dvoch rokov od vydania záverečnej správy b) pri každej významnej zmene, najneskôr do dvoch mesiacov, odkedy má zmena významný vplyv (Príloha č. 2 Vyhláška 493/2022)
- Záverečná správa obsahuje **aj zhodnotenie plnenia povinností** podľa zákona a celkového stavu prijatých bezpečnostných opatrení informačných systémov súvisiacich so základnou službou, vyslovenie **súladu, čiastočného súladu alebo nesúladu** s požiadavkami na bezpečnosť sietí a informačných systémov a konkrétne uvedenie nedostatkov (§ 2 ods. 2 Vyhláška 493/2022)
- **Správa o zistených nedostatkoch s** termínami vykonania nápravných opatrení (§ 2 ods. 3 Vyhláška 493/2022)
- PZS má povinnosť predložiť **záverečnú správu o výsledkoch auditu** na NBÚ spolu s opatreniami na nápravu a s lehotami na ich odstránenie **do 30 dní od ukončenia auditu**. (§ 29 ods. 5 ZoKB)

Samohodnotenie

- PZS, ktorý nie je PKZS, **môže zabezpečiť** plnenie povinnosti vykonať audit **v lehote 2 rokov,** samohodnotením prostredníctvom JISKB (§ 29 ods. 8 ZoKB)
- Samohodnotenie vykonáva manažér kybernetickej bezpečnosti.
- PZS je povinný podrobiť sa auditu kybernetickej bezpečnosti **do 5 rokov odo dňa zaradenia do registra** prevádzkovateľov základnej služby a následne podľa periodicity určenej vyhláškou
- Vyhláška NBÚ 493/2022 o audite kybernetickej bezpečnosť sa bude novelizovať

DOHĽAD NBÚ

CUSEC

PLÁN OBNOVY

Dohľad - prehľad

- Úrad vykonáva dohľad
- a) vybavovaním sťažností,
- b) kontrolou,
- c) ukladaním opatrení na zastavenie porušovania povinností a nápravu nezákonného stavu („opatrenia na nápravu“),
- d) schvaľovaním dohody o náprave,
- e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.

Dohľad

- Primeranosť výkonu dohľadu
- Predmetom dohľadu nie je rozhodovanie sporov z právnych vzťahov
- Výkonom dohľadu nie je dotknutá povinnosti plniť povinnosti (aj počas prebiehajúcej kontroly si PZS musia plniť svoje nahlasovacie povinnosti a povinnosť riešenia incidentov)
- Sťažnosti odberateľov služby alebo záujmových združení týkajúce sa porušenia povinností PZS

Kontrola

- Kontrolou sa

a) zisťuje stav kontrolovaných skutočností a ich súlad s povinnosťami PZS podľa ZoKB alebo na jeho základe,

b) zisťujú príčiny a škodlivé následky nedostatkov zistených kontrolou,

c) zisťuje splnenie uložených alebo prijatých opatrení na nápravu („splnenie prijatých opatrení“) (§29c ZoKB)

O zistených nedostatkoch z kontroly úrad vypracuje návrh čiastkovej správy alebo návrh správy a čiastkovú správu alebo správu. Ak neboli zistené nedostatky, úrad vypracuje len čiastkovú správu alebo správu. (§29f ZoKB)

- opis nedostatkov zistených kontrolou spolu s ich odôvodnením,
- označenie konkrétnych povinností, ktoré boli porušené,
- zoznam dôkazov preukazujúcich zistené nedostatky,
- lehotu na podanie námietok k zisteným nedostatkom,
- lehotu na predloženie písomného zoznamu prijatých opatrení,
- lehotu na splnenie prijatých opatrení.

Kontrola je skončená dňom zaslania správy PZS.

Opatrenie na nápravu

- **Predbežné opatrenie** (uloží PZS, aby niečo vykonal, niečoho sa zdržal alebo niečo strpel, alebo aj nariadi zabezpečenie vecí, ktoré sú potrebné na vykonanie dôkazov)
- **Vykonať audit** kybernetickej bezpečnosti a vykonať odporúčania podľa výsledkov tohto auditu v určenej lehote,
- **Prijať opatrenia na nápravu**,
- **Informovať dotknuté osoby alebo verejnosť** o rizikách alebo následkoch porušenia povinnosti,
- **Zakázať poskytovať službu** do času nápravy (neplatí pre OVM)
- **Penále** v sume 0,5 % z najvyššej možnej sumy pokuty, za každý deň omeškania so splnením povinnosti
- **Pokutu** za správny delikt

Výnimočne ak nedochádza k náprave:

- **Zakázať štatutárnemu orgánu PZS alebo členovi, jeho vedúcemu zamestnancovi** na najvyššej úrovni riadenia zodpovednému, poverenému splnomocnencovi **vykonávať ich funkciu, zamestnanie alebo činnosť u PZS**, a to až do doby splnenia týchto povinností (neplatí pre OVM)
- **Rozhodnutím súdu** vydaným na návrh úradu **dočasne obmedziť prístup a) odberateľov k službe, alebo b) k online rozhraniu**

Rozkazné konanie

- Ak bolo **vybavovaním sťažnosti, kontrolou alebo pri uložení opatrenia na nápravu, spoľahlivo zistené,** že PZS v jednotlivom prípade porušil povinnosť, úrad je príslušný **bez ďalšieho konania vydať rozkaz o uložení sankcie (**pokutu do 10 000 eur a opatrenie na nápravu.**) (**§29l ZoKB**)**
- Právo PZS podať do 15 dní od jeho doručenia písomne odpor, ktorý musí byť odôvodnený

Dohoda o náprave

- **NBÚ môže kedykoľvek počas výkonu dohľadu navrhnúť** PZS uzatvorenie dohody o náprave. (§29m ZoKB**)**
- Návrh na dohodu môže dať len NBÚ
- Podmienky pre uzatvorenie: ak opatrenia a náhrada, ktoré sú obsahom dohody sú spôsobilé odstrániť nezákonný stav a primerane nahradiť vzniknutú škodu alebo inú ujmu a ak neexistuje iný záujem na pokračovaní vo výkone dohľadu
- Dôsledok: NBÚ zastaví výkon dohľadu v rozsahu porušení povinností, ktoré sú obsahom dohody o náprave
- Zrušenie dohody a pokračovanie v dohľade:

a) došlo k podstatnej zmene ktorejkoľvek skutočnosti rozhodujúcej pre uzatvorenie dohody o náprave,

b) PZS neplní svoje záväzky z dohody o náprave, alebo

c) uzatvorenie dohody bolo založené na neúplných, nesprávnych alebo zavádzajúcich informáciách od PZS.

Priestupky fyzických osôb

- Priestupku sa dopustí fyzická osoba, ktorá
- a) poruší povinnosť uvedenú v § 12 ods. 1 (mlčanlivosť a ochrana osobných údajov),
- b) poskytla nepravdivé údaje v oznámení podľa § 17 ods. 2 (oznámenie o činnosti PZS),
- c) poruší niektorú z povinností podľa § 19 ods. 1 až 4, 6 alebo ods. 7,
- d) **nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby,**
- e) vykoná audit kybernetickej bezpečnosti v rozpore s § 29 ods. 3 (napr. audit vykoná osoba ktorá nie je certifikovaný audítor (nemá platnú certifikáciu), audit „formálne" vykoná certifikovaný audítor, ale v skutočnosti ho vykonáva niekto iný bez certifikácie), alebo
- f) vykoná samohodnotenie prostredníctvom JISKB v rozpore s § 29 ods. 8 (napr. ak samohodnotenie vykoná osoba ktorá nie je MKB).

- Za priestupok môže úrad uložiť pokutu **od 100 eur do 5 000 eur.**

Delikty právnických osôb (PZS)

- Pokuta od 300 eur do 500 000 eur za porušenie povinnosti
  - a) oznámiť začiatok vykonávania činnosti podľa § 17 ods. 2,
  - b) oznámiť zmenu údajov podľa § 17 ods. 6,
  - c) oznámiť prevádzkovanie kritickej základnej služby podľa § 18 ods. 2,
  - d) podľa § 19 ods. 2 až 4, ods. 6 písm. f) alebo ods. 7,
  - e) udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa § 20 ods. 3,
  - f) podľa § 29 ods. 1, 2, 5 alebo ods. 8,
  - g) vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29, alebo
  - h) uloženú úradom podľa § 29j ods. 1.
- Pokuta od 300 eur do 7 mil. eur alebo do výšky 1,4 % obratu za porušenie povinnosti PZS / od 500 eur do 10 mil. eur alebo do výšky 2 % obratu PKZS
  - a) podľa § 19 ods. 1 alebo ods. 6 písm. a) až e) alebo g) až i),
  - b) prijať bezpečnostnú dokumentáciu podľa § 20 ods. 3,
  - c) nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 alebo ods. 3,
  - d) zasielať automatizovaným spôsobom určené systémové informácie podľa § 24a ods. 1,
  - e) riešiť KBI, vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 3,5 alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa § 27 ods. 6, alebo
  - f) predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8.

POISTENIE

Kyberpoistenie

- Presun rizika je metóda ošetrenia rizika, pri ktorej bude určitá časť následkov rizika zdieľaná s externými subjektmi. **Typickým presunom rizika je poistenie**.
- Poistenie právnických osôb (poistenie zodpovednosti za škodu a majetkové poistenie, prípadne aj poistenie štatutára)
- Kyberpoistenie zvyčajne pokrýva externé náklady na IT služby, právne služby a PR pri reakcii na kybernetický incident, priamu finančnú stratu z prerušenia podnikania, pokuty za porušenie ochrany osobných údajov a náklady na ochranu a obranu práv spoločnosti.
- Existuje aj širšie poistené krytie, napríklad poistenie poškodenie dobrej povesti (reputácie) spoločnosti ako aj ochrana pred požiadavkami kyberzločincov na výkupné a/alebo poistné môže kryť aj náklady spojené s identifikáciou a vyjednávaním s kyberzločincami.
- Problémom však zostáva upisovanie, teda odhadovanie rizika a následne výpočet poistné-ho.
- Odlišovať od poistenia fyzických osôb - spotrebiteľov (zneužitie karty, spor s e-shopom či kyberšikana)

Rozhodnutie: Krajský súd v Tübingene (Nemecko) 2023

- Ransomvér sa dostal do systému po otvorení prílohy e-mailu (falošná faktúra) na pracovnom notebooku; notebook bol pripojený cez VPN, útok vyradil veľkú časť serverov.
- Poistený nemal zavedené bežné bezpečnostné opatrenia, chýbali aktualizácie a poskytol nepresné odpovede na otázky poisťovateľa pri hodnotení rizika.
- Poisťovateľ odstúpil od zmluvy, tvrdil porušenie predzmluvnej informačnej povinnosti a vedomé nenainštalovanie roky dostupných bezpečnostných aktualizácií. Argumentom poisťovateľa bolo že nedostatočné opatrenia (napr. chýbajúce 2FA a monitoring) mali znamenať zvýšenie rizika a hrubú nedbanlivosť.
- Podľa súdu však poisťovateľ mohol a mal tieto konkrétne bezpečnostné okolnosti preveriť už v predzmluvnej fáze; ak medzi uzavretím poistky a incidentom nenastala zmena stavu, a poisťovateľ si nevyžiadal doplňujúce informácie, implicitne akceptoval existujúce rizikové nastavenie.

Rozhodnutie Najvyššieho súdu v New Jersey vo veci Merck 2023

- Farmaceutický gigant Merck bol v júni 2017 poškodený v pravdepodobne jednom z najničivejších ransomvérových útokov NotPetya. Spoločnosť Merck si uplatnila poistný nárok z jej poistnej zmluvy na majetok. Poisťovateľ, Ace American Insurance Company (Ace) odmietol vyplatiť poistku, aj keď poistná zmluva spoločnosti Merck pokrývala „všetky riziká". Ace tvrdil, že keďže išlo o „vojnový akt" (zo strany Ruska) a tým pádom je táto udalosť vylúčená z krytia škôd súvisiacich s takýmito vojnovými činmi.
- Odvolací súd Najvyššieho súdu v New Jersey rozhodol, že útok NotPetya nespadá pod výluku „nepriateľských alebo vojnových" činov v rámci poistnej zmluvy na majetok, ktorá kryje všetky riziká.
- Od útokov NotPetya boli prijaté opatrenia s cieľom objasniť, na ktoré druhy útokov sa vzťahujú výluky z poistenia. V roku 2022 Lloyd's of London oznámil že upisovatelia budú musieť vylúčiť krytie štátom podporovaných kybernetických útokov spojených s vojnou a incidentmi, ktoré výrazne zhoršujú schopnosť štátu fungovať alebo ktoré nepriaznivo dopadajú na bezpečnostné schopnosti štátu