**Scenár pre riešenie bezpečnostných incidentov**

Tento článok a scenár pre riešenie bezpečnostných incidentov je spracovaný na základe dobrej praxe a reflektuje pravidlá a postupy v oblasti riešenia bezpečnostných incidentov v kontexte požiadaviek platnej legislatívy v oblasti kybernetickej a informačnej bezpečnosti, ako aj medzinárodnej normy radu ISO/IEC 27000 v predmetnej oblasti.

**Kľúčové súvisiace predpisy a normy**

Problematika riešenia bezpečnostných incidentov je obsiahnutá nielen v medzinárodných normách v oblasti kybernetickej a informačnej bezpečnosti (normy ISO), ale aj legislatívnych predpisoch platných v Slovenskej republike, z ktorých najdôležitejšie sú:

* zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
* vyhláška č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
* vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
* zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe,
* 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,
* súbor medzinárodných noriem radu ISO/IEC 27000 (podstatná časť z nich je pre slovenské reálie prevzatá a do slovenského jazyka preložená Slovenskou národnou akreditačnou službou – SNAS).
1. **Úvod**

Pre oblasť riadenia bezpečnostných incidentov v organizácii v súlade s požiadavkami platnej legislatívy v oblasti kybernetickej a informačnej bezpečnosti, resp. s požiadavkami medzinárodných noriem (najmä radu ISO/IEC 27000) vyplýva dôležitosť pochopenia pravidiel pre zistenie (objavenie, identifikáciu) bezpečnostných incidentov, ich klasifikáciu, spôsob hlásenia, eskalácie, vyšetrovanie a reakciu na ne. Pochopením uvedeného je možné riadiť včasnú identifikáciu, preskúmanie, prešetrovanie, ako aj efektívne odstránenie vzniknutých bezpečnostných udalostí, resp. bezpečnostných incidentov, ktoré môžu mať negatívny dopad na bezpečnosť organizácie a jej aktív (teda všetkého, čo má pre organizáciu hodnotu). Výsledkom riadenia bezpečnostných incidentov je obvykle následné prijatie účinných nápravných alebo preventívnych opatrení.

Tu sa do popredia dostáva dôležitá podmienka pre riadenie bezpečnostných incidentov, ktorou je nutnosť definovať spôsob ich hlásenia. (*Pozn.: najmä pre skupinu prevádzkovateľov základných služieb je táto oblasť detailne definovaná v § 24 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, resp. pre skupinu poskytovateľov digitálnej služby je táto oblasť detailne definovaná v § 25 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Zároveň je problematike riešenia bezpečnostných incidentov venovaný § 27 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov – spolu s definovaním povinností aj pre prevádzkovateľa základnej služby.)*

1. **Ako postupovať v oblasti riešenia bezpečnostných incidentov?**
	1. **Zabezpečte proces riadenia bezpečnostných incidentov**

Pri riadení bezpečnostných incidentov je najprv potrebné v organizácii zaviesť proces ich riešenia a ďalej zabezpečiť:

* monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch,
* detekciu bezpečnostného incidentu a zber relevantných informácií,
* ohodnotenie a klasifikácia bezpečnostného incidentu (klasifikačná schéma bezpečnostného incidentu – *rozdelenie na bezpečnostný incident I., II. a III. stupňa, resp. klasifikačná schéma pre klasifikáciu informácií a kategorizáciu sietí a informačných systémov* – je definovaná v platnej legislatíve),
* zabezpečenie nahlásenia incidentu na primárny alebo sekundárny kontakt definovaným spôsobom a jeho vyhodnocovanie,
* vyriešenie bezpečnostného incidentu (definovať postupy riešenia vrátane eskalačných postupov a zaistenia i uchovania digitálnych stôp pre účely auditu, ako aj vedenia evidencie o vzniknutých incidentoch),
* realizácia/implementácia/prijatie opatrení na zabránenie opakovania bezpečnostného incidentu.

*(Pozn. Tu platí, že ak prevádzkovateľ základnej služby nemá dostatočné spôsobilosti na vyriešenie prebiehajúceho bezpečnostného incidentu, požiada o pomoc rezortný alebo sektorový útvar – ten zabezpečí pomoc organizácii prostredníctvom rezortného/sektorového tímu CSIRT.)*

* 1. **Zabezpečte dôslednú realizáciu analýzy rizík**

Pre riadenie bezpečnostných incidentov v organizácii je jednou z prvých úloh manažmentu zabezpečiť realizáciu analýzy rizík podľa vybranej metodiky ako jedného zo základov pre riešenie bezpečnostných incidentov. Metodík spracovania analýzy rizík je viacero, pre tento článok sa do úvahy vezme metodika založená na scenároch rizík.

Pre jej spracovanie je potrebné vziať do úvahy nasledovné skutočnosti:

* Spracovať zoznam aktív (informácií, sietí a informačných systémov) organizácie – teda súhrn všetkého, čo má pre organizáciu hodnotu a každému aktívu priradiť vlastníka. Pre klasifikáciu informácií a kategorizáciu sietí a informačných systémov použiť klasifikačnú schému podľa Prílohy č. 2 k vyhláške č. 362/2018 Z. z.).
* Následne spracovať **zoznam scenárov rizík** (napr. scenár rizika č. 1: Neautorizované získanie prístupu v dôsledku nedostatočnej aktualizácie hesiel).
* Spracovať zoznam/katalóg **hrozieb** (napr. získavanie, zneužitie a predstieranie cudzej identity), zoznam/katalóg **zraniteľností** (napr. neodhlásenie sa pri opúšťaní pracoviska) a zoznam/katalóg **dopadov** (napr. poškodenie alebo strata údajov).
* K predmetnému scenáru rizika priradiť **pravdepodobnosť** jeho naplnenia (napr. nízka, stredná, vysoká) a úroveň jeho **dopadu** (napr. minimálny, vážny, katastrofický).
* Pre konkrétnu pravdepodobnosť a úroveň dopadu vypočítať podľa zvolenej matice metodiky analýzy rizík hodnotu rizika (napr. akceptovateľné, závažné alebo mimoriadne závažné riziko).
* Pre každé napr. závažné alebo mimoriadne závažné riziko definovať opatrenie na jeho zníženie vytvorením katalógu **opatrení** (napr. riadenie a kontrola hesiel privilegovaných používateľov).
	1. **Vysvetlite zamestnancom v organizácii, čo bezpečnostný incident je**

Bezpečnostný incident ako taký môže byť spôsobený aktivitou užívateľa (úmyselne alebo neúmyselne), resp. iným pôsobením (napr. chyba systému, havária). Dôsledkom bezpečnostného incidentu je potom ujma na aktívach organizácie (napr. jeho nefunkčnosť, pozastavenie/nemožnosť poskytovania služby, materiálne či finančné škody atď.). Takáto ujma sa nazýva dopad (bezpečnostného incidentu), vyjadriteľný obvykle kvantitatívne (napr. finančne) alebo kvalitatívne (najmä pri ťažko merateľných dopadoch – napr. strata dobrého mena – nízka/stredná/významná).

Bezpečnostný incident je teda každá bezpečnostná udalosť, ktorá má potenciál narušiť informačnú bezpečnosť poskytovanej služby alebo organizácie.

*(Pozn. v zákone o kybernetickej bezpečnosti č. 69/2018 Z. z. v platnom znení je definovaný aj pojem „kybernetický bezpečnostný incident“ ako akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému alebo porušenia bezpečnostnej politiky, alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií.)*

Pre účely nižšie uvedených scenárov reakcie na bezpečnostné incidenty sa bude uvažovať s týmito (možnými) typmi situácií, udalostí, resp. bezpečnostných incidentov:

* **nebezpečná situácia** (napr. možné porušenie politiky alebo interných predpisov organizácie),
* **udalosť** (napr. preukázateľne porušená politika organizácie, ktorej výsledkom je hmotná alebo nehmotná škoda),
* **bežný** **bezpečnostný incident** [obvykle vyžaduje rutinný zásah, jeho dopad na aktíva nie je významný (napr. chybové hlásenia systémov, malé zavírenie, ponechanie citlivého dokumentu v tlačiarni, ponechanie návštevy bez dozoru...), môže však mať potenciál za istých predpokladov prerásť do závažného bezpečnostného incidentu].
* **závažný bezpečnostný incident** [vyžaduje si prioritný zásah, má potenciál spôsobiť organizácii významné škody, ohrozuje bezpečnosť významných aktív („zavírenie“ serverov IS, neoprávnený prístup k dôverným informáciám/neautorizovaný prístup do chráneného priestoru, výpadok klimatizácie v serverovni, skenovanie LAN, prienik na koncovú pracovnú stanicu...), má potenciál prerásť do kritického bezpečnostného incidentu].
* **kritický bezpečnostný incident** (vyžaduje okamžitý zásah; už spôsobil alebo spôsobí veľké škody, ohrozuje fungovanie kritických aktív, ohrozuje bezpečnosť poskytovaných služieb, má potenciál nekontrolovateľne sa rozšíriť).

Tu je dôležité dodať, že v rámci identifikácie následkov bezpečnostného incidentu je potrebné preskúmať poškodenie alebo potenciálne dočasné alebo trvalé následky (obchodné, finančné, prevádzkové, zdravotné, dobré meno, personálne...) pre organizáciu. Následky sú v praxi spôsobené tzv. scenárom incidentu (ide o opis hrozby využívajúci konkrétnu zraniteľnosť alebo súbor rôznych typov zraniteľností pri konkrétnom bezpečnostnom incidente). Vplyv takýchto scenárov bezpečnostného incidentu sa určuje vzhľadom na kritériá definovaných vplyvov, čo môže ovplyvniť jedno alebo viacero aktív, resp. len určitú časť aktíva.

* 1. **Všetkým pracovníkom vysvetlite ich základné povinnosti**

V oblasti riešenia bezpečnostných udalostí/incidentov v organizácii platí, že každý pracovník a tretie strany (dodávatelia, externí spolupracovníci, zákazníci a pod.) sú povinné ihneď ohlásiť akúkoľvek spozorovanú bezpečnostnú udalosť na určený kontaktný bod (ktorý je nevyhnutné vytvoriť). Následne, v prípade spozorovania vzniku bezpečnostnej udalosti/incidentu je zakázané vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu jeho dôsledkov, pričom každý pracovník je povinný poskytnúť bezodkladnú súčinnosť zodpovedným osobám pri vyšetrovaní bezpečnostných udalostí/incidentov.

* 1. **Zabezpečte koordináciu riešenia bezpečnostného incidentu v organizácii**

V organizácii je potrebné pre oblasť riešenia bezpečnostných incidentov riadiť eskalačné procesy vrátane bezpečnej výmeny informácií medzi všetkými súčasťami zapojenými do riešenia bezpečnostného incidentu.

Je tiež potrebné zabezpečiť fungovanie technickej podpory vrátane analytickej činnosti pri riešení bezpečnostných incidentov.

V neposlednom rade je dôležité udržiavať aktuálnu situačnú mapu (vedieť, v  akom aktuálnom stave riešenia bezpečnostný incident je) a následne identifikovať a realizovať/implementovať nevyhnutné (potrebné) preventívne alebo reaktívne bezpečnostné opatrenia.

Zabezpečenie súčinnosti pri riešení bezpečnostného incidentu alebo jeho predchádzaní v rozsahu adekvátnom pre danú organizáciu smerom na SK-CERT/CSIRT.SK je fundamentálnou podmienkou jeho úspešného riešenia.

* 1. **Vytvorte plány reakcie na bezpečnostné incidenty**

Je dôležité pochopiť, že reakcia na bezpečnostné incidenty je určitá forma uzatvorenia kruhu od momentu identifikácie bezpečnostných hrozieb (aktivity pred narušením) cez riešenie incidentov a implementáciu bezpečnostných opatrení (aktivity počas narušenia) až po vzdelávanie a školenia odvodené od konkrétneho bezpečnostného incidentu (aktivity po narušení).

Aktivity pre účely tvorby plánov reakcie na bezpečnostné incidenty zahŕňajú:

* kroky pre vytvorenie tímu pre reakciu na bezpečnostné incidenty,
* činnosti v rámci tvorby scenára bezpečnostného incidentu,
* aktivity v oblasti prípravy preventívnych činností,
* samotná identifikácia, riešenie a blokovanie bezpečnostných incidentov,
* záverečná analýza ako výstup po identifikovanom a vyriešenom bezpečnostnom incidente.
1. **Ako postupovať pri vzniku bezpečnostného incidentu – vzor scenára**
	1. **Fiktívny scenár č. 1 bezpečnostného incidentu**

**Fiktívny** **scenár rizika:** Neautorizované získanie prístupu v dôsledku nedostatočnej aktualizácie hesiel

**Bezpečnostná hrozba:** Získavanie, zneužitie a predstieranie cudzej identity

**Bezpečnostná** **zraniteľnosť:** Slabé riadenie hesiel

**Druh bezpečnostného incidentu:** Botnet na IP adrese XX.XXX.XXX.XXX

**Typ bezpečnostného incidentu:** bežný bezpečnostný incident

**Dopad:** Poškodenie alebo krádež/strata údajov

**Organizácia by mala postupovať nasledovne:**

* **Detekcia bezpečnostného incidentu**
* **Zistenie bezpečnostného incidentu/udalosti**

*Pozn. samostatne alebo hlásením tretej strany.*

* **Dodatočné vyhľadávanie informácií o bezpečnostnom incidente/udalosti**

*Pozn. Je potrebné vyhľadávať informácie súvisiace s bezpečnostným incidentom, ako aj snažiť sa určiť pravdepodobné príčiny jeho vzniku.*

* **Detegovanie miesta prieniku útočníka do infraštruktúry organizácie**

*Pozn. Túto časť realizovať na základe sieťovej komunikácie, spustených programov, procesov a služieb, resp. v kontexte prihlasovacích procedúr používateľov, ako aj potenciálneho zistenia použitia podsunutých dát/informácií útočníkom.*

* **Ohodnotenie a klasifikácia bezpečnostného incidentu**

Zabezpečiť identifikáciu bezpečnostného incidentu na základe dôležitosti služieb z pohľadu dôvernosti, dostupnosti, integrity a legislatívy (ochrana osobných údajov).

*Pozn. Prevádzkovateľ základnej služby identifikuje závažný kybernetický bezpečnostný incident na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov, pričom v zmysle § 24 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti sa závažné kybernetické bezpečnostné incidenty členia na kategórie prvého, druhého a tretieho stupňa. Presná špecifikácia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov je predmetom vyhlášky NBÚ č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.*

* **Hlásenie vzniku bezpečnostného incidentu/udalosti** (emailom alebo telefonicky na určené kontaktné miesto/osobu, resp. využitím Jednotného informačného systému kybernetickej bezpečnosti (<https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html>)

V rámci hlásenia vzniku bezpečnostného incidentu opísať:

* typ hlásenia (prvotné hlásenie, doplňujúce hlásenie),
* typ bezpečnostného incidentu (v prípade závažného kybernetického incidentu určiť jeho kategóriu I., II., III.),
* typ a opis zasiahnutých údajov,
* organizácia alebo jej časť, ktorej sa bezpečnostný incident týka,
* opis poskytovanej služby,
* dátum a čas zistenia a zahlásenia,
* detailný opis priebehu bezpečnostného incidentu,
* analýza prvotnej príčiny vzniku bezpečnostného incidentu,
* zoznam zasiahnutých aktív (vrátane kritických),
* informácia o aktivácii krokov v rámci kontinuity činností,
* rozsah a opis vzniknutých škôd,
* odhad dopadu bezpečnostného incidentu na chod organizácie,
* kontaktné údaje na osobu, ktorá bezpečnostný incident zistila,
* kontaktné údaje na osobu, ktorá bezpečnostný incident hlásila,
* kontaktné údaje na osobu, ktorá bezpečnostný incident rieši,
* kontaktné údaje na osobu, ktorá má právomoc pre eskaláciu bezpečnostného incidentu (*táto osoba musí byť interným zamestnancom organizácie, musí mať právomoc vypnúť/zablokovať/vykonať zmenu/obmedziť prevádzku služieb poskytovaných prostredníctvom externých sietí, musí byť odborne vzdelaná a musí mať právomoc poskytnúť kompletný prístup k dotknutej časti informačných a komunikačných technológií tímu pre riešenie bezpečnostných incidentov*),
* opis spôsobu vyrozumenia manažmentu organizácie.

*Pozn. Prevádzkovateľ základnej služby má povinnosť hlásiť každý závažný kybernetický incident, a to prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.*

* **Riešenie bezpečnostného incidentu**
* Identifikácia: záznamy z logov, aktivita na sieti (IDS/IPS, firewall...)
* Nájdenie koncovej stanice a jej (napr. forenzná) analýza
* **Realizácia opatrení na zabránenie opakovania bezpečnostného incidentu**
* Reinštalácia koncovej stanice
* Zmena hesiel, resp. následne celej metodiky tvorby hesiel
* Pridanie dvojfaktorovej autentifikácie

*Pozn. 1. Účinnosť nápravných a preventívnych opatrení musí byť v organizácii pravidelne vyhodnocovaná, za čo zodpovedá manažér kybernetickej bezpečnosti, resp. ním určený pracovník organizácie.*

*Pozn. 2. Správa o štatistike jednotlivých typov bezpečnostných incidentov a o trendoch narušenia bezpečnosti týkajúcich sa poskytovaných služieb organizácie sa vedie aspoň na ročnej báze a predkladá sa bezpečnostnému výboru organizácie. Správu schvaľuje štatutár organizácie.*

* 1. **Fiktívny scenár č. 2 bezpečnostného incidentu**

**Fiktívny** **scenár rizika:** Kompromitácia dátového úložiska s kritickými údajmi

**Bezpečnostná hrozba:** Zneužitie práv administrátora na neautorizované čítanie, modifikáciu a vymazanie dát (úmyselná činnosť administrátora alebo správcu IS vedúca k neoprávnenému použitiu IS: neautorizované čítanie, modifikácia alebo vymazanie položiek databázy alebo dátových súborov, konfiguračných súborov, lokálnych súborov elektronickej pošty, logov)

**Bezpečnostná** **zraniteľnosť:** Nesprávna alokácia prístupových práv

**Druh bezpečnostného incidentu:** Kompromitácia kritického dátového úložiska

**Typ bezpečnostného incidentu:** kritický bezpečnostný incident

**Dopad:** Neoprávnený prístup k údajom/informáciám (kompromitácia údajov, strata dobrého mena organizácie, obchodné straty, únik chránených údajov z pohľadu obchodného tajomstva)

**Organizácia by mala postupovať nasledovne:**

* **Detekcia bezpečnostného incidentu**
* **Zistenie bezpečnostného incidentu/udalosti**

Postup podľa predchádzajúceho príkladu scenára č. 1.

* **Dodatočné vyhľadávanie informácií o bezpečnostnom incidente/udalosti**

Postup podľa predchádzajúceho príkladu scenára č. 1.

* **Detegovanie miesta prieniku útočníka do infraštruktúry organizácie**

Postup podľa predchádzajúceho príkladu scenára č. 1.

* **Ohodnotenie a klasifikácia bezpečnostného incidentu**

Postup podľa predchádzajúceho príkladu scenára č. 1.

* **Hlásenie vzniku bezpečnostného incidentu/udalosti**

Postup podľa predchádzajúceho príkladu scenára č. 1.

* **Riešenie bezpečnostného incidentu**
* Identifikácia: zistenie fyzického umiestnenia kompromitovaného servera
* Záznamy z logov, aktivita na sieti (IDS/IPS, firewall...)
* **Realizácia opatrení na zabránenie opakovania bezpečnostného incidentu**
* Forenzná analýza kompromitovaného servera – prijatie opatrení na základe výsledku analýzy
* Obnova zálohy (aktivácia plánu kontinuity)
* Zmena prístupového hesla, resp. pridanie dvojfaktorovej autentifikácie
1. **Záver**

Riešenie bezpečnostných incidentov prebieha v organizácii v kontexte povinností a požiadaviek vyplývajúcich z platných legislatívnych povinností. Pre splnenie týchto požiadaviek je teda dôležité, aby organizácia mala správne implementovaný funkčný proces riešenia bezpečnostných incidentov realizovaný v praxi.

V prípade, že organizácia spadá do registra prevádzkovateľov základných služieb a nemá dostatočné kapacity, resp. spôsobilosti na vyriešenie prebiehajúceho bezpečnostného incidentu, postupuje tak, že požiada o pomoc SK-CERT (na národnej úrovni), resp. CSIRT.SK (pre sektor verejnej správy).