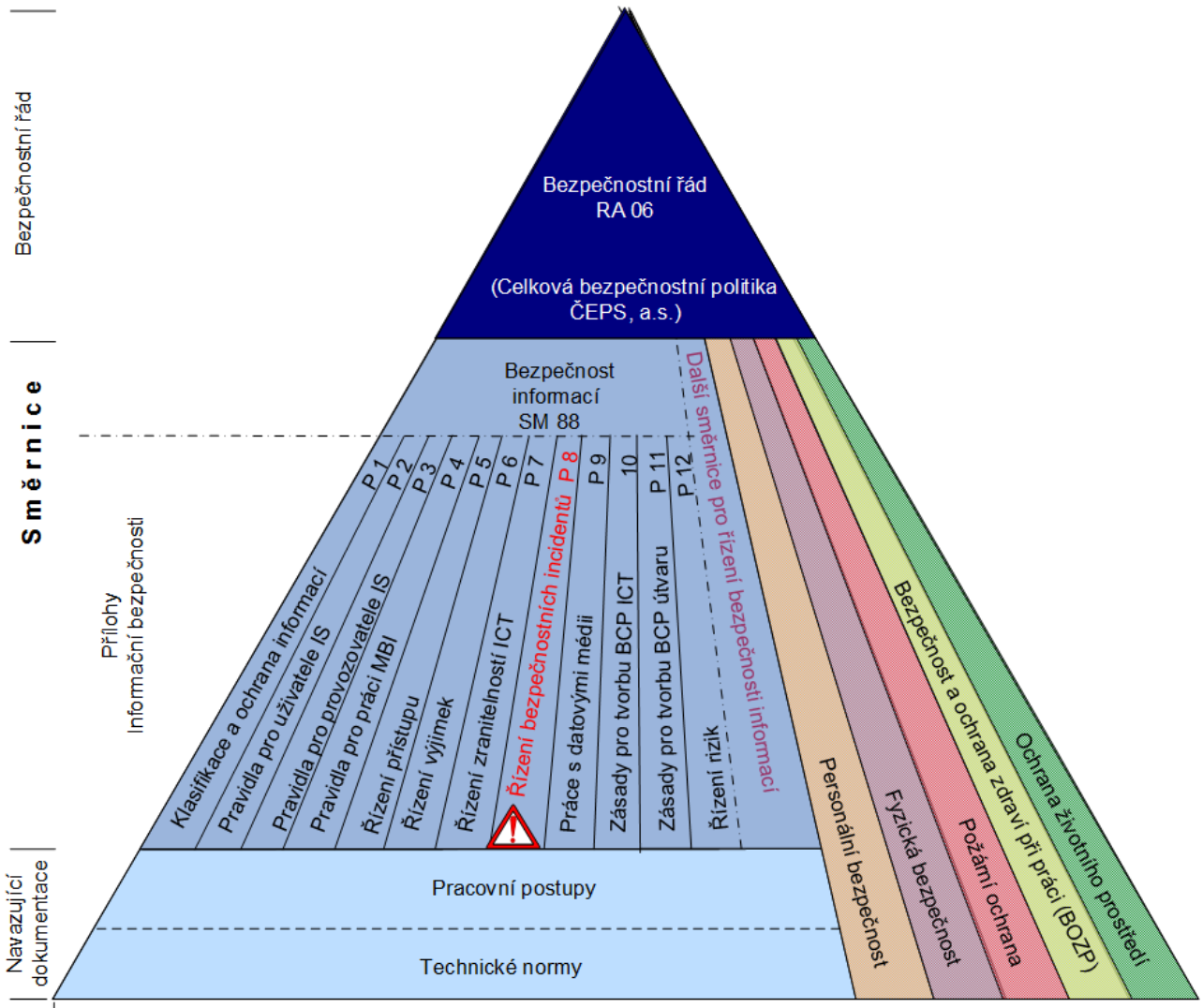
# PRAVIDLA PRO ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

**Zařazení a působnost ve struktuře bezpečnostní dokumentace**




| dokument / působnost | Klasifikace a ochrana informací | Pravidla pro uživatele IS | Pravidla pro provozovatele IS | Pravidla pro práci MBI | Řízení přístupu | Řízení výjimek | Řízení zranitelností ICT | Řízení bezp. incidentů | Práce s datovými médii | Zásady pro tvorbu BCP ICT | Zásady pro tvorbu BCP útvaru | Řízení rizik |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| uživatel IS | X | X | | | | | | | | | | |
| provozovatel IS | X | X | X | X | X | | X | X | X | X | | X |
| MBI | X | X | | X | X | X | X | X | X | X | X | X |
| vedoucí útvaru | X | X | | | | | | | | | X | X |
| personalista | X | X | | | X | | | | | | | |
| externí subjekt | X | X | X*) | | X*) | | | | | | | |

*) *Platí pro externí subjekty v roli správců/administrátorů/vývojářů IS*

*Pozn.: Uvedené názvy nejsou přesnými názvy příloh.*

# Obsah

# 1 ÚČEL A PŮSOBNOST

Tato příloha ke směrnici *Bezpečnost informací* (dále jen „SM/88“) definuje postupy pro hlášení, vyhodnocení a účinnou a efektivní reakci na informační bezpečnostní incidenty (dále také bezpečnostní incident nebo incident).

Cílem je minimalizace negativních dopadů bezpečnostních incidentů na poslání, cíle a činnosti společnosti včetně prevence opakování incidentů.

Bezpečnostní incidenty musí být rychle a efektivně zvládány na základě formalizovaných postupů, delegovaných odpovědností a připravených opatření. Směrnice popisuje systematické postupy pro účinnou a efektivní reakci na bezpečnostní incidenty.

Účelem směrnice je:

- nastavit efektivní proces řízení zvládání bezpečnostních událostí a incidentů,
- zajistit identifikaci a vyhodnocení rizik spojených s bezpečnostními incidenty,
- minimalizovat dopady bezpečnostních incidentů na činnost společnosti,
- dosáhnout zlepšení bezpečnosti informací ve společnosti prostřednictvím soustavného procesu zlepšování a prevence na základě získaných poznatků z řešení incidentů.

Tato příloha ke směrnici „*Bezpečnost informací*“ a popsaný proces řízení bezpečnostních incidentů vycházejí z mezinárodních norem ISO/IEC 27002 a ISO/IEC TR 18044 je závazná pro všechny zaměstnance ČEPS v roli provozovatele nebo administrátora informačního systému a manažera/specialisty bezpečnosti informací.

## 1.1 Role, odpovědnosti, pravomoci

**Ředitelé sekcí *Energetické řídící a informační systémy, ICT služby a Řízení provozu a údržby*** v rámci řízení bezpečnostních incidentů odpovídají za:

- monitoring a správu událostí v IS,
- vyhodnocování bezpečnostních incidentů evidovaných v Helpdesku a jejich zařazení do kategorií (méně závažný, závažný, velmi závažný),
- řešení provozních bezpečnostních incidentů a za poskytnutí specialistů pro řešení *závažných a velmi závažných* bezpečnostních incidentů,
- provoz Helpdesku ve své působnosti v roli jednotného kontaktního místa pro hlášení bezpečnostních událostí a incidentů,
- volbu prostředí pro poskytování služby Helpdesku a její provoz dle požadavků na zachování dostupnosti, důvěrnosti a integrity informací o incidentech,
- využití, údržbu a konfiguraci bezpečnostních technologií pro zaznamenávání událostí v IS a jejich vyhodnocování, a pro detekci a prevenci průniků do IS (IDS/IPS),
- spolupráci při využívání, údržbě a konfiguraci bezpečnostních technologií pro řízení zranitelností IS,
- implementaci opatření pro prevenci a za zamezení opakovaných výskytů incidentů bezpečnosti,
- zaznamenávání incidentů, které plynou z provozu IT a správy IS ČEPS.

**Manažer bezpečnosti informací**

Odpovědnost manažera bezpečnosti informací je stanovená v příloze č. 4 SM/88.

**Bezpečnostní analytik**

Bezpečnostní analytik odpovídá za:

- průběžné vyhodnocování incidentů detekovaných automatickým systémem pro správu bezpečnostních událostí (SIEM) i incidentů hlášených uživateli nebo jinými kanály. Zejména provádí následující činnosti:
  - hodnotí bezpečnostní incidenty a určuje jejich kategorii,
  - vyhodnocuje, zda je nutno aktivovat bezpečnostní radu ICT,
  - spolupracuje na řešení závažných bezpečnostních incidentů, pokud nebyla aktivována bezpečnostní rada ICT,
  - svolává bezpečnostní radu ICT z podnětu členů bezpečnostní rady nebo bezpečnostního ředitele a koordinuje její činnost,
  - provádí šetření příčin závažných bezpečnostních incidentů a kontroluje zdokumentování postupu řešení bezpečnostních incidentů,
  - koordinuje zajišťování podkladů pro forenzní analýzu,
  - navrhuje úpravy SIEM systému a provádí běžné ladění jeho funkčnosti tak, aby byla zajištěna správná a přesná detekce podezřelých chování,
  - ukládá administrátorům IT systémů, nezbytné úkoly nutné k prošetření nebo zvládnutí bezpečnostního incidentu.
- přípravu postupů pro správu bezpečnostních technologií (přístupové, autentizační, datové, zálohovací, atp.).

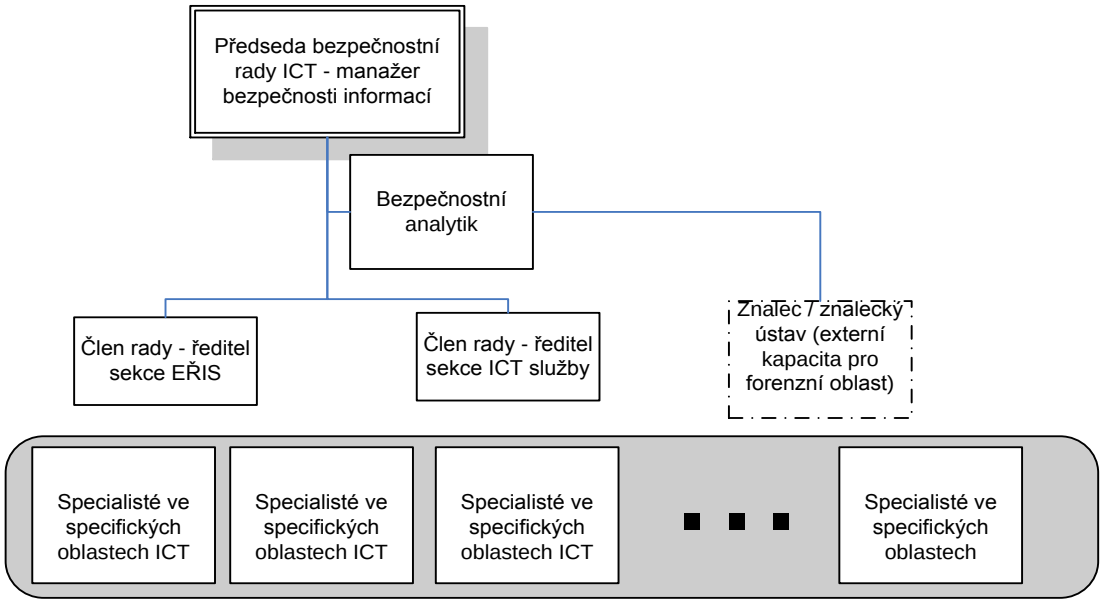
V rámci jednotlivých sekcí/oddělení mohou být určení bezpečnostní analytici, kteří provádějí činnost bezpečnostního analytika pro oblast dané sekce/oddělení.

**Bezpečnostní ředitel** odpovídá za řešení kritických bezpečnostních incidentů, v případech které nesplňují důvody pro svolání krizového štábu (viz PPŘ 09 2015).

**Bezpečnostní rada ICT v roli ISIRT**

- zajišťuje odpovídající reakci na závažné a velmi závažné bezpečnostní incidenty,
- řídí implementaci nápravných opatření k odstraňování závažných a velmi závažných bezpečnostních incidentů,
- zajišťuje vypracování postupů pro šetření jednotlivých typů incidentů a aktualizaci těchto postupů s ohledem na nové typy incidentů,
- zajišťuje vypracování komunikačního plánu jednoznačně definujícího rozhodovací a informační procesy i postupy,
- zajišťuje možnost využití odpovídajících SW a HW prostředků pro zajištění důkazů pro forenzní analýzu (kopií konfigurace, logů, diskového oddílu napadeného systému apod.),
- členové rady mají právo si pro řešení daného incidentu přizvat specialisty sekcí „Energetické řídící a informační systémy“ a “ICT služby“, externí specialisty a zástupce odborných útvarů společnosti,
- zajišťuje bezpečné uchování informací o incidentech pro účely následného šetření a možné použití důkazů pro případné soudní spory,
- odpovědnost stanovuje předseda bezpečnostní rady ICT.

## 1.2 Organizační struktura procesu řízení bezpečnostních incidentů




## 1.3 Komunikace

Pro efektivní řešení incidentu je nezbytná schopnost rychlé reakce a komunikace na všech úrovních společnosti. V případě potřeby bezpečnostní rada ICT komunikuje s vedením po přímé linii. *Při externí komunikaci* (s veřejností, zákazníky, obchodními partnery, státní správou, pracovníky záchranného systému apod.) jedná za společnost tiskový mluvčí nebo jiný zaměstnanec k tomu určený členem představenstva odpovědným za vedení úseku *„Audit, public relations a strategie“*. Předseda bezpečnostní rady ICT informuje tiskového mluvčího nebo jiného pověřeného zaměstnance hned na počátku řešení incidentu a přizve ho na jednání.

## 1.4 Povinnosti pracovníků Helpdesk

Pracovník útvaru Helpdesk přijímá od oznamovatelů hlášení o bezpečnostních událostech, provádí jejich prvotní analýzu (zejména určení priority) a má povinnost ihned zahájit kroky potřebné k jejich vyřešení podle příslušného pracovního postupu. Helpdesk sekce „ICT služby“ postupuje podle části 2.1 „Popis aktivit – operátorská činnost“ přílohy č. 6 „Správa incidentů v ICT“ směrnice SM/104 „Procesy sekce ICT služby“, ostatní Helpdesky podle vlastních schválených pracovních postupů. Není-li takový pracovní postup, řídí se operátoři Helpdesků podle těchto zásad:

- pracovníci útvaru Helpdesk odpovídají za řešení provozních dopadů incidentu, zejména s ohledem na poskytování podpory uživatelům,
- po přijetí hlášení Helpdesk zaznamenávají incident do servicedesku. V případě, kdy by se mohlo jednat o incident kategorie 3, kontaktuje Helpdesk bez zbytečného odkladu bezpečnostního analytika (oddělení *„Strategie a bezpečnost ICT“). Mimo* pracovní dobu Helpdesku, provádí tuto eskalaci pověřený pracovník pohotovosti IT.

## 1.5 Povinnosti bezpečnostního analytika

Bezpečnostní analytik vyhodnocuje incidenty detekované prostřednictvím SIEM systému. U incidentů hlášených uživateli prostřednictvím Helpdesk systému, provádí bezpečnostní analytik

detailní vyhodnocení bezpečnostních aspektů konkrétního incidentu. Při jejich zpracování má následující povinnosti:

- analyzuje situaci a po posouzení bezpečnostních aspektů rozhodne o závažnosti události**,** vyhodnotí, zda se skutečně jedná o incident a určí jeho kategorii a prioritu řešení. Příklady incidentů jsou uvedeny v dodatku č. 2,
- o incidentech kategorie 2 (viz kap. 2 Definice základních pojmů a zkratek) informuje bez zbytečného odkladu manažera bezpečnosti informací,
- o incidentech kategorie 3 (viz kap. 2 Definice základních pojmů a zkratek) informuje bez zbytečného odkladu manažera bezpečnosti informací a bezpečnostního ředitele,
- provede, nezbytná opatření, která budou bránit dalšímu šíření incidentu. Případně uloží provedení těchto opatření oznamovateli nebo provozovateli dotčeného IS.

### 1.6 Povinnosti administrátorů

Administrátor je odpovědný za řešení bezpečnostních událostí a incidentů ve své oblasti podle příslušného pracovního postupu. Administrátoři sekce *„ICT služby“* postupují podle částí 2.2 „Popis aktivit – řešení incidentu“ a 2.3 „Popis aktivit – uzavření incidentu“ přílohy 6 pracovního postupu PP 49, administrátoři ostatních Helpdesků podle vlastních schválených pracovních postupů.

Administrátoři poskytují manažeru bezpečnosti informací záznamy i o *méně závažných* incidentech prostřednictvím záznamů v HD nebo formou měsíčních hlášení a statistik/reportů (např. výskyt virových nákaz za měsíc nebo seznamu uživatelů, kterým bylo nově vygenerováno heslo, okomentované části vybraných systémových logů apod).

### 1.7 Povinnosti uživatelů

Uživatelé jsou povinni podle přílohy č. 2 SM/88 ohlásit všechny bezpečnostní události bez zbytečného odkladu na příslušný Helpdesk.

Uživatelé se sami nepokoušejí prověřovat ohlašovanou bezpečnostní událost. Zaznamenají však důležité informace a detaily (hlášení na obrazovce, chybné fungování systémů, podivné chování aplikací nebo osob apod.), případně zamezí eskalaci problému, pokud je to v jejich moci.

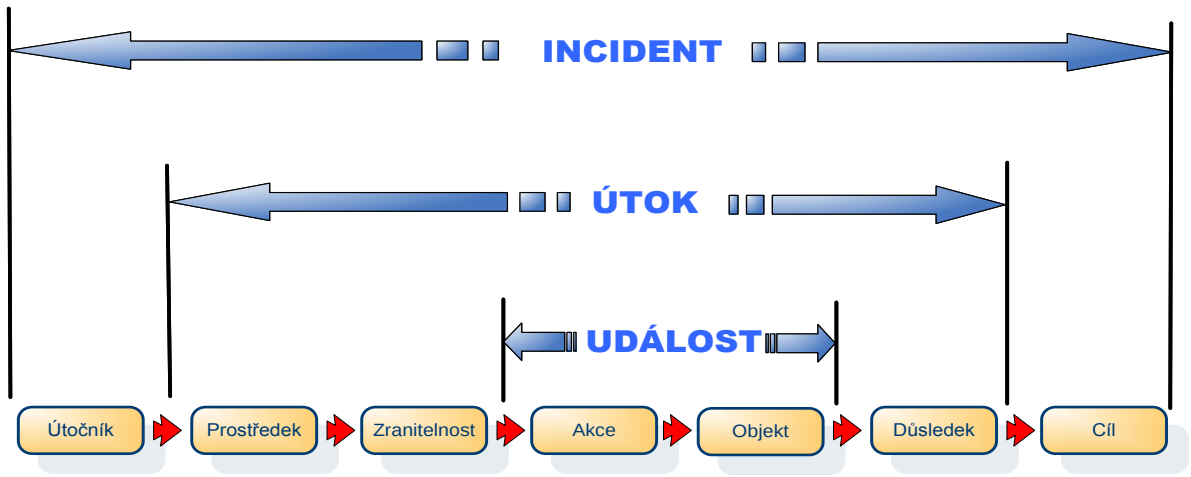
## 2 DEFINICE ZÁKLADNÍCH POJMŮ A ZKRATEK

**Bezpečnost informací -** zachování **důvěrnosti** (ochrana před neautorizovaným přístupem, odhalením nebo aktivním odposlechem), **integrity** (správnost a úplnost) a **dostupnosti** (autorizovanému uživateli dle potřeby) informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

**Bezpečnostní událost** – je identifikovaný stav systému, služby, sítě nebo aplikace, ukazující na možné porušení bezpečnosti informací nebo selhání bezpečnostních opatření.

**Bezpečnostní incident -** činnost nebo událost ohrožující aktiva nebo narušující bezpečnostní procedury.

Incident probíhá řadou objektů v následující posloupnosti:




*Schema 1 - fáze řešení Bezpečnostního incidentu*

**Útok** - je série kroků vedoucí k nežádoucím stavům provedena útočníkem s cílem narušit informační bezpečnost.

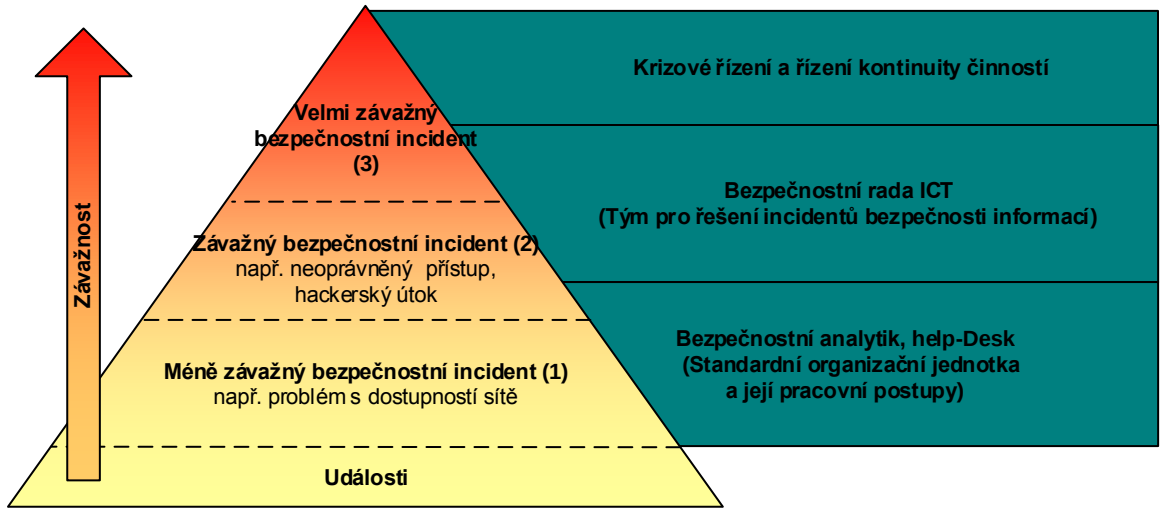
**Prostředek -** je nástroj nebo způsob, kterým byla, je nebo může být narušena bezpečnost informačního systému (počítače, sítě, prostoru apod.). Jedná se využití zranitelnosti informačního systému, které má charakter fyzického útoku, výměny informací, uživatelského příkazu, dávky nebo programu, nasazení autonomního agenta, použití sady nástrojů (toolkitu), distribuovaných nástrojů, napíchnutí dat apod.

**Zranitelnost -** je slabina, nedostatek nebo vlastnost informačního systému (počítače, sítě, prostoru, aplikace) umožňující provést neoprávněnou akci. Jedná se např. o slabinu nebo nežádoucí vlastnost v návrhu či specifikaci programového nebo technického vybavení, slabinu či chybu v implementaci programového nebo technického vybavení, nedostatečnou konfiguraci, nežádoucí hodnotu nebo kombinaci vzniklou při konfiguraci systému nebo prostředí apod.

**Důsledek** - je nežádoucí výsledek události, který může mít pro bezpečnost informací různou míru závažnosti.

Podle závažnosti a způsobu řešení se provádí následující kategorizace bezpečnostních incidentů:

- **Kategorie 1 - méně závažný bezpečnostní incident** – je takový incident, při kterém dochází k méně závažnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých škod., Zpravidla jej lze řešit v rámci pracovních postupů provozních útvarů ICT.
- **Kategorie 2 - závažný bezpečnostní incident** – je takový incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých škod.
- **Kategorie 3 – velmi závažný bezpečnostní incident** – je takový incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod. Přitom je nutno aktivovat krizové řízení a postupy Řízení kontinuity činností organizace (BCM).




*Schema 2 - priority řešení BI*

**Havárie** – je bezpečnostní incident, který má závažný dopad na kontinuitu činností a poskytovaných služeb (negativní dopad funkčnost kritických aplikací, parametrů informačního systému), na dobu delší než je kritická doba nedostupnosti vyplývající z katalogu poskytovaných služeb

**Krizová situace** – je souhrn bezpečnostních incidentů, který vede k ohrožení základních funkcí systémů ICT a tím i celé společnosti.

**ISIRT** – „information security incident response team“, tým pro řešení bezpečnostních incidentů. Podílí se na hodnocení bezpečnostních událostí a řešení bezpečnostních incidentů.

V případě potřeby mohou být do týmu přizváni externisté, např. specialisté na forenzní počítačovou analýzu. **V ČEPS roli ISIRT vykonává bezpečnostní rada ICT.**

**Plánování kontinuity činností** (Business Continuity Planning) – je proces, který v případě, že má incident negativní dopad na kontinuitu činností (procesů, IT služeb) společnosti, zajistí v požadovaných časech a úrovni jejich obnovu a obnovu podpůrných aktiv, podle předem připravených scénářů,.

**Forenzní analýza** – slouží jako prostředek k získání poznatků o původu a průběhu incidentu. Současně vyhledává důkazy o tom, zda byl či nebyl spáchán trestný čin nebo čin, který je v rozporu s vnitřními předpisy a pravidly danými obvykle řídící nebo provozní dokumentací. Je jedním z nástrojů k řešení bezpečnostních incidentů a k následnému vymáhání škod.

Výsledkem forenzní analýzy je znalecký nebo technický posudek či vyjádření mající důkazní hodnotu.

# 3 POSTUPY ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

## 3.1 Proces zvládání bezpečnostních incidentů

Bezpečnostní incidenty se zvládají v krocích tímto postupem:


*Schéma 3 – životní cyklus řešení incidentu*

Cílem **řízení a prevence** je celkové zavedení a udržování procesu řízení bezpečnostních incidentů.

Cílem **detekce a hlášení** je zjištění bezpečnostní události nebo potenciálního incidentu a předání důležitých relevantních informací příslušnému Helpdesku.

Cílem **hodnocení a určení priority** je vyhodnocení dostupných informací a kategorizace události podle její závažnosti. V návaznosti na kategorii se událost nebo incident přidělí k řešení běžnými provozními postupy nebo se aktivuje bezpečnostní rada ICT.

Cílem **řešení a reakce na incidenty** je rychlá a efektivní zabrána škodám způsobeným incidentem, zajištění stop a důkazů pro související vyšetřování incidentu, odstranění následků a příčin incidentu a obnova systémů do funkčního stavu.

Cílem **vyhodnocení a zlepšování** je využití získaných informací ke zlepšení procesu řízení incidentů a bezpečnosti informací.

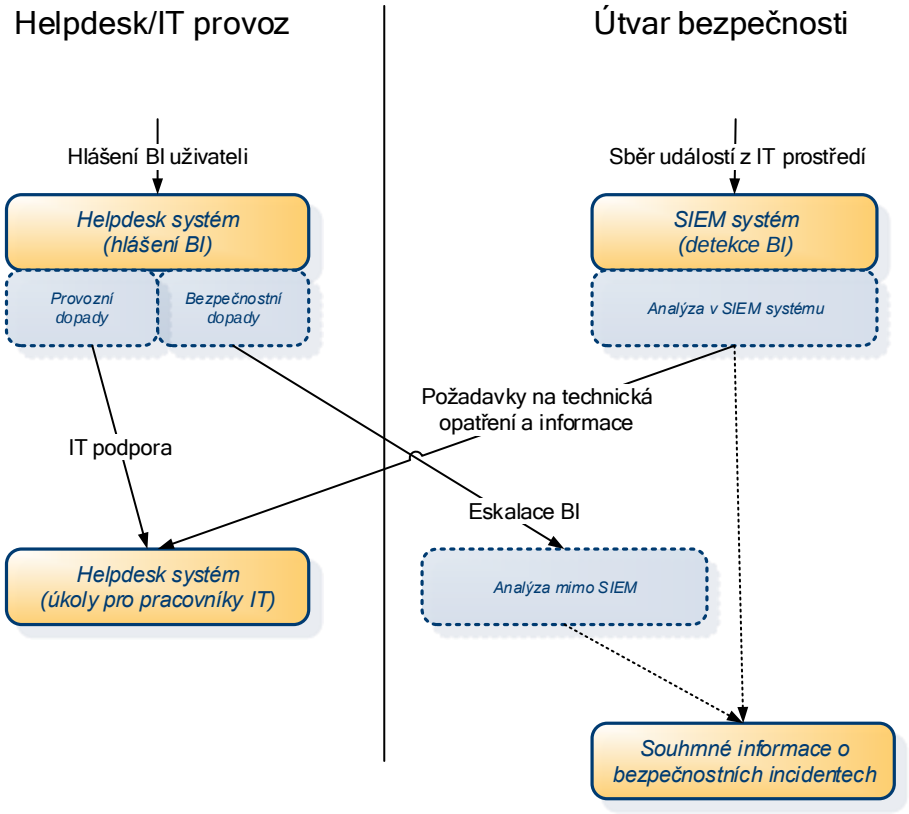



*Schéma 4 - napojení SIEM a Helpdesk systémů*

Schéma 4 zobrazuje základní vztah SIEM systému a Helpdesk systému pro sběr, vyhodnocování a zpracování bezpečnostních incidentů.

- SIEM slouží k automatizovanému sběru a vyhodnocování událostí z IT prostředí, přičemž úkoly pro IT administrátory jsou zakládány do Helpdesk systémů;
- Helpdesk slouží jako kontakt pro incidenty hlášené uživateli a distribuci těchto incidentů na IT podporu (provozní část) a útvar bezpečnosti (bezpečnostní aspekty).

Podrobnější schéma řešení bezpečnostních incidentů, včetně jejich rozdělení do priorit je uvedeno na následujícím schématu.

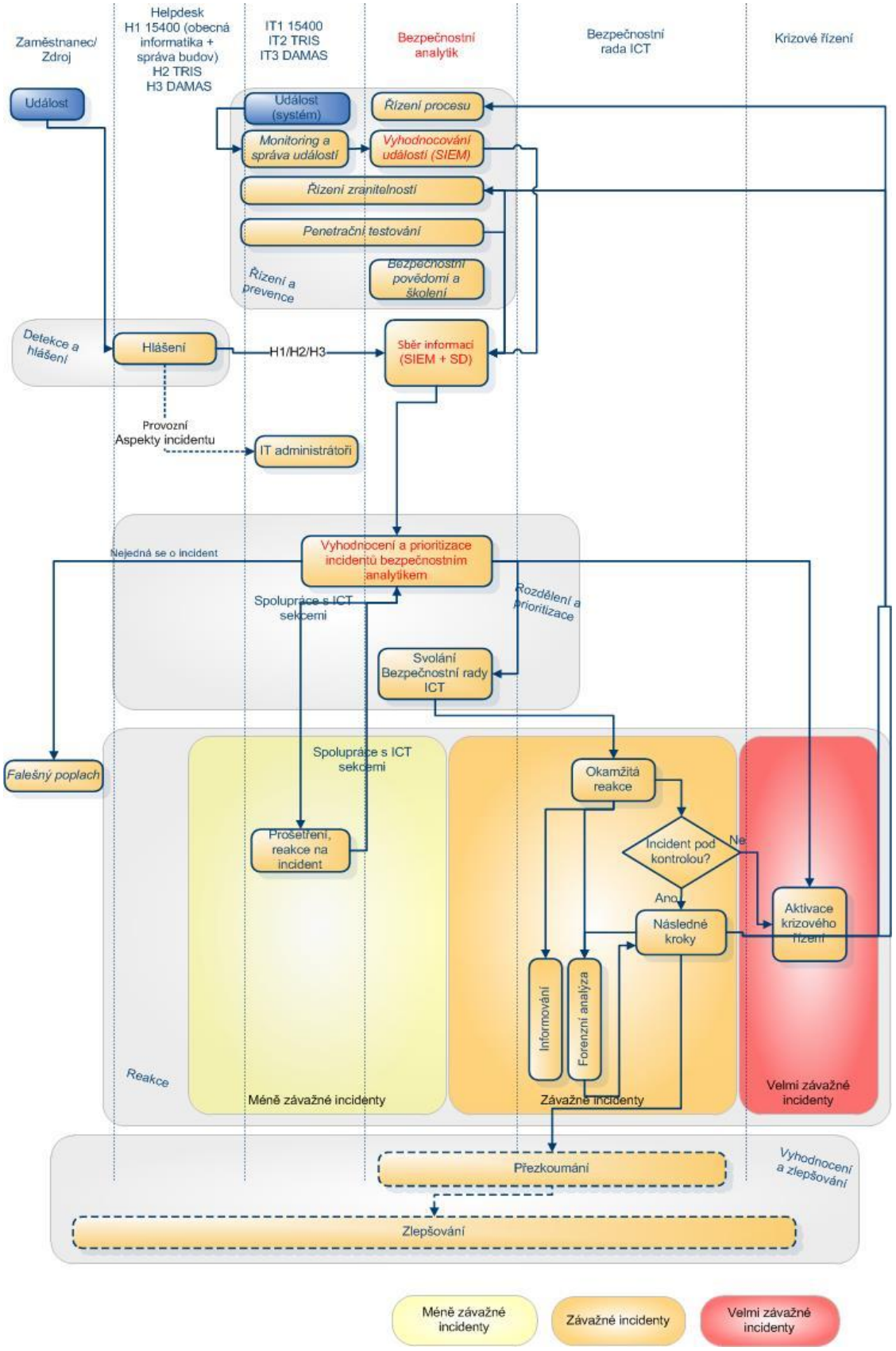



*Schéma 5 - detailní schéma zpracování incidentů*

Schéma 55 popisuje detailní workflow zpracování incidentů. Toto schéma popisuje zpracování bezpečnostních aspektů konkrétního incidentu. Detail řešení provozních dopadů a aktivity související s podporou provozu a uživatelů jsou ve schématu pro srozumitelnost zjednodušeny.

## 3.2 Řízení a prevence

Cílem je zavedení a udržování procesu řízení bezpečnostních incidentů a dále takových opatření, která jsou prevencí před vznikem možných bezpečnostních incidentů.

### *3.2.1 Řízení*

Tato činnost zajišťuje vlastní ustanovení procesu řízení incidentů a jeho popis v návaznosti na SM/88 a interní pracovní postupy sekcí *„Energetické řídící a informační systémy“, “ICT služby“ a „Řízení provozu a údržby“.*

Ustanovení zahrnuje vytvoření a popis:

- procesu řízení incidentů,
- nutné organizační struktury,
- příkladů incidentů pro účely kategorizace zejména ve fázi „rozdělení a určení priorit“,
- testování funkčnosti scénářů „od stolu“,
- vytvoření pracovních postupů nebo doplnění stávajících pracovních postupů pro zvládání konkrétních typů bezpečnostních incidentů pro pracovní skupiny např. útvary Helpdesk.

Důležitým cílem činnosti je dohled nad realizací kroků nezbytných k šetření příčin incidentu tak, aby získané důkazy byly uznatelné v případě soudního sporu. To předpokládá jejich získání způsobem, který prokazatelně nečiní změny v originálních datech, a důsledné zaznamenávání kroků při zvládání bezpečnostního incidentu. Přijatá rozhodnutí a sled navazujících kroků musí být v každém okamžiku transparentní. Tento cíl může být v přirozeném rozporu s cílem co nejrychleji obnovit službu IT, proto je nutné těmto činnostem věnovat potřebnou pozornost.

### *3.2.2 Prevence*

**Monitoring a správa událostí**

Cílem monitoringu a správy událostí je zaznamenat relevantní události v informačním systému společnosti tak, aby bylo možno odhalit bezpečnostní události a incidenty a zpětně nacházet jejich příčiny.

Pro IT systémy je monitoring, sběr a vyhodnocování bezpečnostních událostí řešeno pomocí SIEM systému. Významné nově implementované informační systémy musí být napojeny do SIEM systému.

**Vyhodnocování bezpečnostních událostí**

Cílem vyhodnocování bezpečnostních událostí je analyzovat a vyhodnotit informace získané v rámci monitoringu a správy událostí, které spadají nebo mohou ovlivňovat oblast bezpečnosti.

**Řízení zranitelností IS**

Probíhá podle přílohy č. 7 SM/88.

**Penetrační testování**

Cílem penetračního testování je:

- ohodnotit bezpečnostní odolnost IS cestou simulovaného útoku na aktiva společnosti. Proces též zahrnuje nalezení jedné nebo více zranitelností, ale na rozdíl od Řízení zranitelností tuto zranitelnost využije k modelové realizaci útoku,

- prověřit správnou a spolehlivou detekční, lokalizační, identifikační a eskalační funkci SIEM nástroje a všech komponent bezpečnostní infrastruktury.

**Školení a zvyšování bezpečnostního povědomí**

probíhá podle části 2.5 přílohy č. 4 SM/88.

### 3.3 Detekce a hlášení

Cílem je zjištění bezpečnostní události (potenciální incident) a předání důležitých relevantních informací na příslušný Helpdesk, který postupuje dle bodu 1.5.

Neobvyklé chování IS může být identifikováno monitorovacími nástroji, uživateli nebo administrátory.

Události technického charakteru jsou zpravidla detekovány a hlášeny automatizovaně monitorovacími a auditními nástroji.

Uživatel nebo administrátor, který zjistí bezpečnostní událost, má podle přílohy č. 2 SM/88 povinnost ohlásit nebo zaznamenat tuto událost na příslušný Helpdesk.

### 3.4 Hodnocení a určení priorit

Hodnocení se provádí v souladu s bodem 1.5. Součástí hodnocení je také určení priority řešení bezpečnostního incidentu. Pokud není možno rozhodnout o prioritě řešení přímo, vyhodnocuje se dopad incidentu na společnost ve škále:

- malý,
- střední,
- vysoký.

#### *3.4.1 Iniciace bezpečnostní rady ICT*

V případě, že MIB potvrdí, že bezpečnostní incident spadá do kategorií závažný nebo kritický, provede svolání bezpečnostní rady ICT. Sezve stálé členy bezpečnostní rady ICT. Tito členové pak operativně přizývají k řešení specialisty podle věcného obsahu bezpečnostních incidentu.

### 3.5 Reakce - řešení provozního bezpečnostního incidentu

Provozní bezpečnostní incidenty jsou řešeny podle interních pracovních postupů sekcí „Energetické řídící a informační systémy“ a “ICT služby“ a jsou zaznamenávány v Helpdesku tak, aby byla možná jejich následná identifikace pro účely reportingu.

Záznamy o provozních incidentech a jejich řešení jsou manažeru bezpečnosti informací k dispozici prostřednictvím odpovídajícího HelpDesku.

### 3.6 Reakce – řešení závažného a kritického bezpečnostního incidentu

Řešení závažných a kritických bezpečnostních incidentů má čtyři fáze:

1. okamžitá reakce dle příslušných pracovních postupů
2. následné kroky
3. informování okolí
4. forenzní analýza.

#### *3.6.1 Okamžitá reakce*

Cílem okamžité reakce je:

- zamezit škodám společnosti,
- zajištění stop a důkazů pro související šetření bezpečnostního incidentu.

V rámci řešení musí být zajištěna zejména:

- okamžitá nebo rychlá opatření vedoucí k získání kontroly nad incidentem a k informování příslušných osob nebo skupin, které spolupracují nebo řídí činnosti; může se jednat též o dočasná opatření jako např. odpojení systému od sítě, implementace dodatečného perimetru např. firewallem apod.,
- podrobné dokumentování situace, všech činností a rozhodnutí do formuláře „Protokol o bezpečnostním incidentu“,
- bezpečné zajištění auditních záznamů (logů) a dalších důkazních materiálů.

Po vyřešení incidentu musí být pro usnadnění řešení při opakovaní incidentu zaznamenán postup vedoucí k řešení a další informace spojené s řešením incidentu (chybné postupy, neočekávané situace apod.).

### *3.6.2 Následné kroky*

O provedení následných kroků k vyřešení incidentu rozhoduje MIB. Nepodaří-li se dostat závažný bezpečnostní incident pod kontrolu a hrozí-li další zvyšování škod společnosti, je nutno změnit klasifikaci incidentu na kritický a přizvat k řešení bezpečnostního ředitele.

Je-li incident pod kontrolou, následující kroky musí zajistit

- obnovení činnosti IS společnosti v původním rozsahu,
- přijetí opatření, která zamezí opakování incidentu v budoucnosti.

V návaznosti na okamžitou reakci bezpečnostní rada ICT odpovídá za to, že:

- provede/zajistí forenzní analýzu získaných důkazních materiálů,
- v případě, že řešení incidentu s prioritou 1 a 2 trvá déle než 7 dní, vytvoří průběžnou zprávu o incidentu pro bezpečnostní radu ČEPS.

V každém okamžiku musí být zajištěna podrobná dokumentace všech činností a rozhodnutí do „Protokolu o bezpečnostním incidentu“.

### *3.6.3 Informování okolí*

V průběhu incidentu bezpečnostní rada ICT rozhoduje o informování dalších osob v rámci společnosti.

V situacích, kdy je pravděpodobné, že dopady incidentu budou zasahovat mimo společnost, nebo je nutné v souvislosti s incidentem zahájit trestní řízení, rozhodne bezpečnostní rada ICT po konzultaci s úsekem *„Audit, public relations a strategie*“, kdo a jakým způsobem bude informován mimo společnost (subdodavatelé, partneři, média, Policie ČR apod.).

V případě velmi závažných bezpečnostních incidentů týkajících se systémů podléhajících zákonu o kybernetické bezpečnosti mají pracovníci společnosti (zejména oddělení Strategie a bezpečnost ICT) povinnost informovat Národní bezpečnostní úřad (NBÚ) v souladu s definovaným pracovním postupem.

### *3.6.4 Forenzní analýza – pravidla pro sběr důkazů*

Sběr důkazů o incidentu vykonává bezpečnostní rada ICT, případně radou určený zaměstnanec, případně dodavatel na základě smlouvy. Následující souhrnná pravidla zajišťují předpoklad pro přijatelnost a váhu důkazů v soudním a rozhodovacím procesu:

- kopie všech informací z pevných datových medií a přenosných datových medií musejí být pořízeny bezpečným způsobem tak, aby nedošlo k modifikaci (znehodnocení) originálních dat,
- kopie dat je vhodné realizovat formou vytvoření datových obrazů celých disků na k tomuto účelu vyhrazeném PC pracovišti, které není a nebude připojeno k počítačové síti. Další kopii takto zajištěných dat je třeba vytvořit před vlastním zkoumáním zajištěných dat, tak aby bylo možné se kdykoliv během šetření incidentu i po jeho skončení možno vrátit k původnímu stavu zajištěných dat,
- kopie dat jsou vytvářeny na kapacitně dostatečné a dostupné médium, které zaručí nemožnost přepisu nebo modifikace zkopírovaných dat,
- všechny úkony lze vykonávat pouze za přítomnosti svědka,
- každý úkon a rozhodnutí týmu pro zvládání bezpečnostního incidentu musí být jednoznačně zdokumentován,
- kopie informací a záznamy o vykonaných úkonech se bezpečně uloží (např. do trezoru).

Sběr důkazů o incidentu může přesahovat hranice společnosti nebo může být proces získávání důkazů za pomoci interních složek nerealizovatelný. V tomto případě musí být využito služeb externího konzultanta bezpečnosti (znalec/znalecký ústav). O jeho přizvání rozhoduje MIB v součinnosti s bezpečnostní radou ICT.

### 3.7 Vyhodnocení a zlepšování

Cílem vyhodnocení a zlepšování je získat zpětnou vazbu z procesu a poučit se ze získaných zkušeností již zvládnutých bezpečnostních incidentů.

#### *3.7.1 Přezkoumání*

Po vyřešení a uzavření bezpečnostního incidentu musí MIB v součinnosti s bezpečnostní radou ICT provést další kroky vedoucí ke zjištění příčin incidentu a snížení rizika jeho opakování:

- provedení následné forenzní analýzy pro zajištění důkazů z dat, např. obrazů disků,
- analýzu incidentu pro prevenci opakování incidentů,
- provedení analýzy souvisejících systémů a procesů, u kterých může nastat bezpečnostní incident ze stejných důvodů,
- doporučení technických nebo netechnických opatření, která mohou zamezit dalšímu vzniku incidentu,
- doporučení změny procesu zvládání incidentů a formulářů.

Dále musí být po každém incidentu vyhodnocena databáze událostí a incidentů, ve které je třeba sledovat:

- trendy ve výskytu incidentů,
- oblasti, které jsou k výskytu incidentů náchylnější,

a definovat místa, ve kterých by zavedení preventivních opatření mohlo snížit pravděpodobnost vzniku bezpečnostních incidentů.

Po přezkoumání bezpečnostního incidentu se vypracují doporučení pro zlepšování stavu bezpečnosti. Ta musí popisovat technologické a procesní změny, které je třeba zavést v návaznosti na vyřešený incident včetně finančních a lidských zdrojů a navrhnout harmonogram provedení změn.

*3.7.2 Zlepšování*

Implementace opatření definovaných v doporučeních pro zlepšování stavu bezpečnosti jsou schvalována bezpečnostní radou ICT a řízena procesem řízení změn.

*3.7.3 Testování*

Procesy zvládání bezpečnostních incidentů musí být před uvedením do praxe ověřeny a posléze zařazeny do pravidelného testování. Testovány musí být především proces hlášení, evidence bezpečnostní události, rozhodnutí o incidentu a předání incidentu k řešení (tj. funkčnost Helpdesku a připravenost řešitelů).

## Dodatek č. 1 Bezpečnostní rada ICT – Kontakty na stálé členy

| Role | Jméno | E-mail | Mobilní telefon | Pevná linka |
|---|---|---|---|---|
| **Stálí členové týmu** | | | | |
| Manažer bezpečnosti informací (MBIIB) | Šmolík Jan, Ing. | smolik@ceps.cz | 602 152 536 | 211 044 794 |
| Ředitel sekce Energetické řídící a informační systémy | Fantík Josef, Ing. | fantik@ceps.cz | 724 230 571 | 211 044 752 |
| Ředitel sekce ICT služby | Babjak Lukáš, Ing. | babjak@ceps.cz | 724 645 965 | 211 044 039 |
| Specialista bezpečnosti informací | Urbančíková Helena, Ing., | urbancikova@ceps.cz | 731 493 991 | 211 044 832 |

## Dodatek č. 2: Příklady bezpečnostních incidentů

**Méně závažné bezpečnostní incidenty**:

- problémy s přihlášením do sítě či aplikace, následné zamknutí účtu,
- nefunkční aplikace,
- potvrzené zjištění přítomnosti škodlivého softwaru, případně hlášení antiviru, že počítač byl odvirován (pouhé podezření je bezpečnostní *událostí*).

**Závažné bezpečnostní incidenty**:

(obvykle lze závažné incidenty zařadit do tří kategorií: odmítnutí služby, neoprávněný sběr dat nebo neoprávněný přístup k datům a aplikacím)

- odepření poskytnutí služby (DoS, DDoS), tj. aplikace nebo IS nejsou dostupné; zahlcení síťových aktivních prvků, zahlcení informačních systémů, útok ve vnitřní síti,
- hrozba nedostupnosti zdrojů („lehčí varianta“ předešlého, kdy jde o podezření),
- instalace a/nebo používání neautorizovaného softwaru v prostředí společnosti (možnost útoku, riziko nekompatibility, zavlečení malware, porušení autorského zákona, porušení licenčních podmínek),
- náhodné nebo úmyslné poškození výpočetní techniky (riziko nedostupnosti IS a aplikací, finanční škody),

- nepovolený přesun nebo přenos firemních dat v elektronické či papírové podobě (riziko porušení důvěrnosti nebo integrity dat),
- neoprávněné prozrazení firemních informací (porušení důvěrnosti IA),
- krádež dat, intelektuálního vlastnictví společnosti, know-how (porušení důvěrnosti informačního aktiva),
- zjištění škodlivého kódu (viry, červi, trojské koně, apod.) ve vnitřní síti, na datovém médiu nebo na zařízeních společnosti, které nebylo vyřešeno automaticky antivirovým programem,
- sdílení (neoprávněné sdělování) uživatelských jmen a hesel,
- neoprávněné získání hesla nebo pokus o získání hesla (útok hrubou silou, sociální inženýrství),
- zneužití firemních systémů; zahrnuje jakékoliv riskantní používání systémů (riziko zanesení virů, překonávání ochran daného systému za účelem porušení autorského práva nebo neoprávněné zvýšení přidělených práv) nebo takové chování, které by vedlo k žalobám a právním nárokům vůči společnosti,
- vypnutí automatických bezpečnostních opatření na zařízeních společnosti (např. neoprávněný zásah do nastavení a běhu antivirových programů, firewallů či SW aktualizací),
- poškození webových stránek společnosti (zničení nebo změna webového obsahu),
- systematické nedodržování vnitřních předpisů a bezpečnostní dokumentace,
- zneužití anebo pokus o zneužití bezpečnostní slabiny v systémech ICT (objevená slabina se musí ihned ohlásit),
- porušení směrnicemi stanovených zásad fyzické bezpečnosti,
- neautorizované změny v aplikacích a informačních systémech (překročení přidělených oprávnění, zásah do logů nebo aplikace apod.),
- nesoulad s politikami nebo směrnicemi.

Obecně se *závažným* bezpečnostním incidentem rozumí situace, ve které je vysoce pravděpodobný téměř okamžitý dopad na chod společnosti nebo událost překročí rozsah jednoho informačního systému nebo délka obnovy překročí 1 den.

**Velmi závažné bezpečnostní incidenty**

Za velmi závažné jsou považovány incidenty:

- které nelze vyřešit běžným postupem (ani prostřednictvím MIB nebo ISIRT) a je třeba aktivovat krizové řízení,
- při nichž došlo ke kumulaci velkého množství závažných incidentů,
- u kterých délka obnovy po incidentu překročí 10 dní.