10.15 Zvládání kybernetických bezpečnostních incidentů

Tento dokument popisuje opatření, která MUSÍ nebo BY MĚLA být implementována pro:

- **Zajištění důsledného a efektivního přístupu k řízení kybernetických bezpečnostních incidentů, včetně komunikace ohledně bezpečnostních událostí a slabých míst.**
- **Stanovení postupů při vzniku nestandardní situace, včetně stanovení eskalačního procesu uvnitř organizace a auditních požadavků (logování).**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Zvládání kybernetických bezpečnostních událostí a incidentů (§ 14), Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§ 22), Detekce kybernetických bezpečnostních událostí (§ 23), Sběr a vyhodnocování kybernetických bezpečnostních událostí (§ 24).

---

1 Definování kategorií kybernetického bezpečnostního incidentu

Pro potřeby hlášení a zvládání kybernetických bezpečnostních incidentů se MUSÍ kybernetické bezpečnostní incidenty zařadit do kategorií.

Jednotlivé kybernetické bezpečnostní incidenty se kategorizují podle významnosti při zohlednění:

a) dopadů obsažených v dopadových určujících kritériích, podle kterých byly povinné osoby určeny,
b) počtu dotčených uživatelů,
c) způsobené nebo předpokládané škody,
d) důležitosti dotčených aktiv informačního a komunikačního systému,
e) dopadů na poskytované služby informačního a komunikačního systému,
f) dopadů na služby poskytované jinými informačními a komunikačními systémy,
g) délky trvání incidentu,
h) zeměpisného rozsahu dotčené oblasti a
i) dalších dopadů.

Kategorie kybernetických bezpečnostních incidentů dle následků a negativních projevů jsou v následující tabulce:

1.1 Stupně závažnosti kybernetického incidentu (Zdroj: (1))

Kategorie	Závažnost	Reakce	Časový rámec řešení
III	**Velmi významný** (při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv)	Řešení vyžaduje neprodlené zásahy. Okamžité a trvalé úsilí s využitím všech zdrojů. MUSÍ být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	Okamžitá reakce/řešení tak rychle, jak je to jen možné. Reakce do 1 pracovní hodiny a reakční plán splněn do 4 hodin (pokud existuje řešení).
II	**Významný** (je narušena bezpečnost poskytovaných služeb nebo aktiv)	Jeho řešení vyžaduje neprodlené zásahy obsluhy. Analytici reagují okamžitě a vyhodnotí situaci. Za účelem pomoci MŮŽE BÝT využít další personál, pracující na úkolech s nízkou nebo střední prioritou.	Reakce do 2 pracovních hodin a reakční plán splněn do 1 pracovního dne (pokud existuje řešení, lhůta pro řešení se počítá od okamžiku potvrzení bezpečnostního incidentu).
I	**Méně významný** (dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv)	Uplatnění standardních postupů a provozování s běžným dohledem řídících struktur organizace.	Reakce do 4 pracovních hodin a reakční plán splněn do 2 pracovních dní (pokud existuje řešení, lhůta pro řešení se počítá od okamžiku potvrzení bezpečnostního incidentu).

**upravit dle potřeby*

1.1.1 Typy kybernetických bezpečnostních incidentů podle dopadu jsou:

a) kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv,
b) kybernetický bezpečnostní incident způsobující narušení integrity aktiv,
c) kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv, nebo
d) kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených v písmenech a) až c)

2 Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů

Cíl: Stanovit pravidla pro vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů, evidovat a analyzovat kybernetické bezpečnostní události a incidenty za účelem eliminace dalšího výskytu, stanovit auditní požadavky. Přidělit odpovědnosti a stanovit postupy pro detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů.

Společnost MUSÍ v rámci zvládání kybernetických bezpečnostních událostí a incidentů zavést proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů.

2.1 Odpovědnosti a postupy

Odpovědnosti přidělené v rámci společnosti a příslušné postupy MUSÍ být nastaveny tak, aby zajistily rychlou, efektivní a řádnou reakci na kybernetické bezpečnostní incidenty.

Implementační pokyny:

2.1.1 MUSÍ být přiděleny odpovědnosti a stanoveny postupy pro:

a) detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů,
b) koordinaci a zvládání kybernetických bezpečnostních incidentů.

2.1.2 Současně MUSÍ fungovat eskalační proces, v rámci, kterého budou přesně definovány osoby, které budou o situaci informovány, a případně na ně bude přenesena odpovědnost za její řešení.

2.1.3 MUSÍ být definovány a aplikovány postupy pro: identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.

2.2 Detekce kybernetických bezpečnostních událostí a incidentů

MUSÍ být zajištěna včasná detekce kybernetických bezpečnostních událostí a incidentů pomocí vhodného nástroje.

Společnost v rámci komunikační sítě, jejíž součástí je informační a komunikační systém:

2.2.1 MUSÍ použít nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí:

a) ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi,
b) ověření a kontrolu přenášených dat na perimetru komunikační sítě a
c) blokování nežádoucí komunikace.

2.2.2 MUSÍ zajistit detekci kybernetických bezpečnostních událostí přiměřeně s ohledem na důležitost aktiv v rámci

a) koncových stanic,
b) mobilních zařízení,
c) serverů,
d) datových úložišť a výměnných datových nosičů,
e) síťových aktivních prvků a
f) obdobných aktiv.

2.3 Reaktivní opatření

Zvládání incidentů vyžaduje zásahy (různé reakční doby) obsluhy s tím, že MUSÍ být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod. Společnost MUSÍ provádět reaktivní a ochranná opatření, která vydává NÚKIB.

Implementační pokyny:

2.3.1 MUSÍ být posouzeny očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření.

2.3.2 MUSÍ být vyhodnoceny možné negativní účinky.

2.3.3 MUSÍ být stanoven způsob rychlého provedení tohoto opatření, který minimalizuje jeho možné negativní účinky, a určí časový plán jeho provedení.

2.3.4 Způsob jejich provedení MUSÍ být neprodleně oznámen NÚKIBu prostřednictvím formuláře pro oznámení způsobu provedení reaktivního opatření (v souladu s pokyny v konkrétním opatření).

2.3.5 Vyplněné formuláře s hlášením kontaktních údajů MUSÍ být zaslány do datové schránky NÚKIB, **ID: zzfnkp3** nebo elektronicky podepsané na e-mail **regulace@nukib.cz.**

3 Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů

Řídí se pravidly pro testování a udržování Řízení kontinuity činností (BCM) viz směrnice SM Řízení kontinuity činnosti.

4 Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti

4.1 Podávání zpráv o slabých místech

Uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé využívající informační systémy a služby společnosti MUSÍ zaznamenávat a oznamovat jakékoliv zjištěné nebo předpokládané nedostatky systémů či služeb (neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti).

Implementační pokyny:

4.1.1 Všichni interní zaměstnanci, externí dodavatelé a poskytovatelé služeb MUSÍ být obeznámeni se svou povinností oznamovat nedostatky v aplikacích, systémech nebo službách tak rychle, jak je to jen možné.

4.1.2 MUSÍ být také obeznámeni:

a) s příslušnými postupy pro hlášení nedostatků bezpečnosti informací a kybernetické bezpečnosti.

b) s kontakty sloužícími k hlášení nedostatků bezpečnosti informací a kybernetické bezpečnosti.

c) s tím, že incidentem se rozumí nejen narušení integrity či důvěrnosti ale i nedostupnost informace či služby.

4.1.3 Všichni interní zaměstnanci, externí dodavatelé a poskytovatelé služeb BY MĚLI být obeznámeni s tím, že by se neměli pokoušet zjištěné nebo předpokládané bezpečnostní nedostatky prokazovat. Testování nedostatků by mohlo být interpretováno jako potenciální zneužití systému a mohlo by také způsobit poškození informačního systému nebo služby.

4.2 Sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů

Společnost MUSÍ definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu. MUSÍ vyhodnocovat účinnosti řešení kybernetického bezpečnostního incidentu. Na základě vyhodnocení MUSÍ stanovit nutná bezpečnostní opatření, popřípadě aktualizovat stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

Implementační pokyny

4.2.1 MUSÍ být použit **nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních** událostí.

4.2.2 Události MUSÍ být zaznamenávány podle podle 4.4.2.

4.2.3 Záznamy o událostech MUSÍ být uchovány nejméně po dobu 18 měsíců.

4.2.4 MUSÍ být prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu.

4.2.5 MUSÍ být vyhledávány a seskupovány související záznamy,

4.2.6 MUSÍ být poskytovány informace pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech,

4.2.7 MUSÍ být vyhodnocovány kybernetické bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí,

4.2.8 MUSÍ být omezeny případy nesprávného vyhodnocení událostí pravidelnou aktualizací nastavení pravidel pro:

a) vyhodnocování kybernetických bezpečnostních událostí,

b) včasné varování a využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.

4.3 Zlepšování kybernetické bezpečnosti

4.3.1 Postupy pro řízení kybernetických bezpečnostních incidentů BY MĚLY být doplněny o mechanismy pro shromažďování a pravidelné přezkoumávání informací o kybernetických incidentech s cílem:

a) kvantifikovat kybernetické incidenty,

b) určit vzorce a trendy kybernetických incidentů různých typů,

c) pochopit náklady a dopady s incidenty spojené,

d) identifikovat kybernetické incidenty opakující se nebo s vysokým dopadem.

4.3.2 Vyhodnocení incidentů může naznačovat potřebu rozšířených nebo dodatečných opatření za účelem omezení četnosti, škod a nákladů budoucích incidentů. Taková vyhodnocení BY MĚLA být zdokumentována a sdílena v rámci výboru kybernetické bezpečnosti.

4.3.3 Znalosti, získané analýzou a řešením úmyslných kybernetických incidentů, BY MĚLY být propojeny s informacemi z interních a externích zdrojů informací o hrozbách, a to za účelem poskytnutí informací a situačního povědomí o minulých, současných a předpokládaných útocích. Takto získané znalosti by měly podpořit rozhodování o opatřeních na základě rizik.

4.3.4 S náležitou pozorností věnovanou aspektům důvěrnosti MOHOU být případové studie ze skutečných kybernetických bezpečnostních incidentů použity v rámci názornosti pro zvýšení povědomí uživatelů či školení o bezpečnosti informací a kybernetické bezpečnosti.

4.4 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

MUSÍ být vedeny záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání.

4.4.1 Společnost MUSÍ:

a) zaznamenává bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému a

b) na základě hodnocení důležitosti aktiv aktualizuje rozsah aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.

4.4.2 Společnost MUSÍ pro zaznamenávání bezpečnostních a provozních událostí zajišťuje:

a) jednoznačnou síťovou identifikaci zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci,

b) sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává:

1. datum a čas včetně specifikace časového pásma,
2. typ činnosti,
3. identifikaci technického aktiva, které činnost zaznamenalo,
4. jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
5. jednoznačnou síťovou identifikaci zařízení původce a
6. úspěšnost nebo neúspěšnost činnosti,

c) ochranu informací získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou,

d) zaznamenávání:

1. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
2. činností provedených administrátory,
3. úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
4. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
5. činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
6. zahájení a ukončení činností technických aktiv,
7. kritických i chybových hlášení technických aktiv a
8. přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí a

e) synchronizaci jednotného času technických aktiv nejméně jednou za 24 hodin.

4.4.3 Zaznamenávání událostí se MUSÍ řídit podle směrnice SM-18 Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.

4.5 Hlášení kybernetického bezpečnostního incidentu

Společnost MUSÍ hlásit všechny kybernetické bezpečnostní incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

4.5.1 Hlášení probíhá prostřednictvím elektronického formuláře zveřejněného na internetových stránkách NÚKIB (viz editovatelný formulář Formular_hlaseni_incidentu (2)).

4.5.2 Po vyplnění všech položek a textových polí se soubor MUSÍ zaslat prostřednictvím:

- elektronické pošty Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB): na e-mail cert.incident@nukib.cz. Pro bezpečnější a důvěryhodnou komunikaci BY MĚLO být použito PGP šifrování. Předmět zprávy BY MĚL mimo jiné obsahovat typ incidentu (např. DDoS, phishing, ransomware, atd.) pro snadnější třídění incidentů mezi jednotlivé analytiky,
- datové schránky NÚKIB: ID datové schránky: **zzfnkp3.**

4.5.3 V případě nenadálé a vážné situace, kdy hrozí riziko z prodlení MŮŽE být pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777. Mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878.

4.5.4 Náležitosti hlášení kybernetického bezpečnostního incidentu jsou:
a) identifikace odesilatele,
b) identifikace informačního a komunikačního systému,
c) datum a čas zjištění incidentu a
d) popis incidentu.

5 Evidence incidentů

Informační nebo komunikační systém jako takový MUSÍ zajišťovat auditovatelnost dat i procesů. Jedná se zejména o přístupy i změny v datech pro jednotlivé objekty (princip zajištění nepopiratelnosti). Auditovatelný musí být také proces řízení identit uživatelů.

5.1.1 Soubor auditních záznamů a podobné důkazy MUSÍ být zajištěny adekvátním způsobem zabezpečeny, aby bylo možno:

1) analyzovat vnitřní problémy;
2) použít je jako forenzních důkazů v souvislosti s možným porušením smlouvy nebo porušením regulatorních požadavků nebo pro případ občansko-právního či trestně právního řízení podle odpovídající legislativy pro zneužití počítačů nebo podle zákona o ochraně osobních údajů;
3) použít je při jednání o náhradě škody s dodavateli programového vybavení a služeb.

5.1.2 Činnosti při opravách selhání systému a zotavení se z narušení bezpečnosti MUSÍ být pečlivě a formálně kontrolovány. Postupy zajišťují, aby:

1) přístup do systému a k datům byl umožněn pouze na základě jednoznačné identifikace a autorizace pracovníků;
2) všechny činnosti při mimořádné události byly detailně dokumentovány;
3) činnosti při mimořádné události byly hlášeny vedení společnosti a systematicky kontrolovány;
4) integrita systémů společnosti a opatření byly potvrzena s minimálním prodlením.

Použité zdroje

(1) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(2) Hlášení incidentů. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. NÚKIB [cit. 2022-04-25]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)