Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Online přednáška portal.nukib.gov.cz
TLP: CLEAR

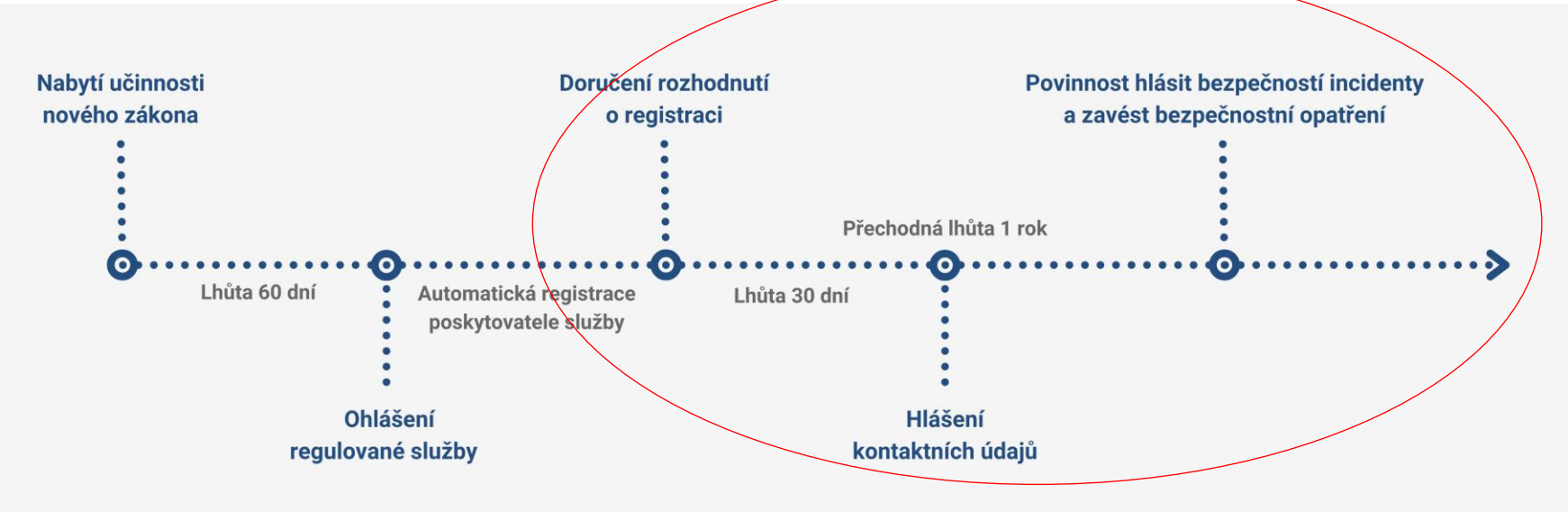
Lucie Syrovátková
Pavel Mazánek
Odbor kontroly

Informace na úvod

Tento materiál slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů.
Tento materiál se primárně zaměřuje na oblast bezpečnostních opatření pro poskytovatele v režimu vyšších povinností.
Tento materiál nenahrazuje a nepokrývá všechny detaily zákona o kybernetické bezpečnosti a jeho prováděcích předpisů.

Vyhláška o kybernetické bezpečnosti

- Vychází ze základních principů řízení kybernetické bezpečnosti, které vedou k zavádění a provádění **přiměřených bezpečnostních opatření** v rozsahu řízení kybernetické bezpečnosti, který je poskytovatel regulované služby povinen určit
- Přístup orientovaný na rizika
- Přechodná lhůta – 1 rok



Viz samostatná přednáška Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Rozsah řízení kybernetické bezpečnosti

- **Nezbytná prerekvizita pro funkční řízení bezpečnosti – je nutno vědět jaké služby jsou poskytovány a na čem jsou závislé**

Součástí rozsahu řízení kybernetické bezpečnosti jsou **aktiva související s poskytováním regulované služby**

= stanovený rozsah

Řízení aktiv – určení primárních a podpůrných aktiv

Dle § 12 zákona *č. 264/2025 Sb., o kybernetické bezpečnosti* – Stanovení rozsahu řízení kybernetické bezpečnosti

- Bezpečnostní opatření požadovaná vyhláškou je nutné implementovat v takto stanoveném rozsahu řízení kybernetické bezpečnosti

Viz samostatná přednáška Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Seznam bezpečnostních opatření

Organizační opatření

- systém řízení bezpečnosti informací,
- požadavky na vrcholné vedení,
- stanovení bezpečnostních rolí,
- řízení bezpečnostní politiky a bezpečnostní dokumentace,
- řízení aktiv,
- řízení rizik,
- řízení dodavatelů,
- bezpečnost lidských zdrojů,
- řízení změn,
- akvizice, vývoj a údržba,
- řízení přístupu,
- zvládání kybernetických bezpečnostních událostí a incidentů,
- řízení kontinuity činností a
- provádění auditu kybernetické bezpečnosti,

Technická opatření

- fyzická bezpečnost,
- bezpečnost komunikačních sítí,
- správa a ověřování identit,
- řízení přístupových práv a oprávnění,
- detekce kybernetických bezpečnostních událostí,
- zaznamenávání událostí,
- vyhodnocování kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické algoritmy,
- zajišťování dostupnosti regulované služby a
- zabezpečení průmyslových, řídících a obdobných specifických technických aktiv.

Organizační opatření

Hlava I

Změny v nVKB – organizační opatření

- Úprava struktury a textace pro lepší srozumitelnost a jednotný výklad
- Zánik pojmu provozovatel informačního nebo komunikačního systému
- Odstranění § 10 (Řízení provozu a komunikací)
  - Povinnosti rozprostřeny do jednotlivých §
- Odebrána příloha č. 1, která specifikovala doporučené požadavky na bezpečnostní role
- Odebrána příloha č. 5, která upravovala požadavky na dokumentaci
  - Méně administrativní zátěže
  - Vedení relevantních politik a dokumentace
  - Nově vznikne jako podpůrný materiál (doporučená struktura)
- Nová příloha
  - Doporučená témata pro rozvoj bezpečnostního povědomí (Příloha č. 7)

§ 3 Systém řízení bezpečnosti informací

Povinná osoba v rámci systému řízení bezpečnosti informací

a) **stanoví cíle systému řízení bezpečnosti informací** směřující k zajištění kybernetické bezpečnosti regulované služby,

b) **řídí rizika podle § 8,**

c) zavede a provádí přiměřená bezpečnostní opatření směřující k zajištění kybernetické bezpečnosti regulované služby na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik,

d) **stanoví bezpečnostní politiku a bezpečnostní dokumentaci** ve vztahu k řízení kybernetické bezpečnosti, která obsahuje hlavní zásady, cíle systému řízení bezpečnosti informací, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku a bezpečnostní dokumentaci v dalších oblastech podle § 6,

e) **zajistí provedení auditu kybernetické bezpečnosti podle § 16,**

§ 3 Systém řízení bezpečnosti informací

f) zajistí alespoň jednou ročně vyhodnocení účinnosti systému řízení bezpečnosti informací, které obsahuje
   1. vyhodnocení cílů systému řízení bezpečnosti informací směřujících k zajištění kybernetické bezpečnosti regulované služby,
   2. posouzení naplňování plánu zvládání rizik zpracovaného podle § 8 odst. 1 písm. g),
   3. hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik,
   4. posouzení výsledků provedených auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
   5. výsledky předchozího hodnocení účinnosti systému řízení bezpečnosti informací provedených podle tohoto písmene,
   6. posouzení dopadů kybernetických bezpečnostních incidentů na oblast kybernetické bezpečnosti a na poskytované služby podle § 15 a
   7. posouzení významných změn podle § 11,

g) zpracuje zprávu o přezkoumání systému řízení bezpečnosti informací na základě vyhodnocení účinnosti systému řízení bezpečnosti informací podle písmene f),

h) aktualizuje systém řízení bezpečnosti informací a relevantní dokumentaci na základě
   1. zjištění z auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
   2. výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací,
   3. dopadů kybernetických bezpečnostních incidentů na poskytované služby a
   4. prováděných významných změn,

i) řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik a

j) stanoví proces řízení výjimek z pravidel stanovených v bezpečnostní politice podle písmene d).

§ 4 Požadavky na vrcholné vedení

(1) Statutární orgán povinné osoby nebo jiná osoba anebo skupina osob v obdobném řídícím postavení u povinné osoby (dále jen „vrcholné vedení“) s ohledem na systém řízení bezpečnosti informací

a) prokazatelně absolvuje školení podle § 10 odst. 3 písm. a),

b) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 3, slučitelných se strategickým směřováním povinné osoby,

c) zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,

d) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,

e) informuje zaměstnance a všechny dotčené osoby o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky,

f) zajistí podporu k dosažení cílů systému řízení bezpečnosti informací,

g) vede a podporuje zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací,

h) se podílí na vypracování analýzy dopadů podle § 15,

i) zajistí testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů,

§ 4 Požadavky na vrcholné vedení

j) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,
k) podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
l) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,
m) zajistí, aby byla zachována mlčenlivost všech relevantních osob zejména administrátorů, osob zastávajících bezpečnostní role a dodavatelů a
n) zajistí pro osoby zastávající bezpečnostní role pravomoci potřebné pro naplňování jejich rolí a zdroje, včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů.

(2) Vrcholné vedení se prokazatelně seznamuje
a) se zprávou o přezkoumání systému řízení bezpečnosti informací,
b) se zprávou o hodnocení rizik,
c) s plánem zvládání rizik,
d) s výsledky analýzy dopadů a
e) s výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.

§ 4 Požadavky na vrcholné vedení

(3) Vrcholné vedení **zřídí výbor pro řízení kybernetické bezpečnosti a určí jeho členy**, přičemž
a) zajistí, že členem výboru pro řízení kybernetické bezpečnosti bude alespoň 1 člen vrcholného vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti,
b) určí práva a povinnosti výboru pro řízení kybernetické bezpečnosti a jeho členů, související se systémem řízení bezpečnosti informací,
c) zajistí konání pravidelných jednání výboru pro řízení kybernetické bezpečnosti alespoň jednou ročně,
d) zajistí vyhotovení záznamu o průběhu jednání výboru pro řízení kybernetické bezpečnosti a
e) zajistí, že výbor pro řízení kybernetické bezpečnosti je složen z osob s pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osob významně se podílejících na řízení a koordinaci činností spojených s kybernetickou bezpečností.

(4) Vrcholné vedení určí osoby, včetně vymezení jejich práv a povinností souvisejících se systémem řízení bezpečnosti informací, které budou zastávat bezpečnostní role
a) manažera kybernetické bezpečnosti,
b) architekta kybernetické bezpečnosti,
c) garanta aktiva a
d) auditora kybernetické bezpečnosti.

(5) Vrcholné vedení zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 4 písm. a) a b).

§ 5 Stanovení bezpečnostních rolí

(1) **Manažer kybernetické bezpečnosti**

a) je pověřen řízením systému řízení bezpečnosti informací, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací po dobu alespoň 3 let,

b) odpovídá za pravidelné informování vrcholného vedení o
   1. činnostech vyplývajících z rozsahu jeho odpovědnosti a
   2. stavu systému řízení bezpečnosti informací,

a) nesmí být pověřen výkonem rolí odpovědných za provoz technických aktiv regulované služby.

(2) **Architekt kybernetické bezpečnosti** je pověřen k zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura regulované služby, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním bezpečné architektury v délce alespoň 3 let.

(3) **Garant aktiva** je pověřen k zajištění rozvoje, použití a bezpečnost aktiva.

(4) **Auditor kybernetické bezpečnosti**

a) je pověřen prováděním auditu kybernetické bezpečnosti, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací v délce alespoň 3 let,

b) zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné a

c) nesmí být pověřen výkonem jiných bezpečnostních rolí.

§ 6 Řízení bezpečnostní politiky a bezpečnostní dokumentace

(1) Povinná osoba **stanoví bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti a vede bezpečnostní politiku a bezpečnostní dokumentaci** k relevantním bezpečnostním opatřením uvedeným v § 3 až 27.

(2) Povinná osoba **dodržuje** pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci podle odstavce 1.

(3) Povinná osoba pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajišťuje jejich aktuálnost a jejich relevantní oblasti zahrnuje do provozní dokumentace, pravidel a postupů.

(4) Povinná osoba **určí osobu odpovědnou za pravidelný přezkum a aktualizaci** bezpečnostní politiky a bezpečnostní dokumentace podle odstavce 3.

(5) Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly

a) dostupné v elektronické nebo listinné podobě,
b) dotčené osoby v rámci povinné osoby informovány o právech, povinnostech a postupech v nich obsažených,
c) přiměřeně dostupné dotčeným osobám,
d) chráněny z pohledu důvěrnosti, integrity a dostupnosti a
e) informace v nich obsažené úplné, čitelné, snadno identifikovatelné a vyhledatelné.

§ 7 Řízení aktiv

a) Povinná osoba v návaznosti na stanovení rozsahu řízení kybernetické bezpečnosti podle § 12 zákona
b) stanoví metodiku pro určování aktiv,
c) stanoví metodiku pro hodnocení aktiv včetně stanovení úrovní aktiv, alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,
d) eviduje garanty aktiv podle § 4 odst. 4 písm. c),
e) hodnotí primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b),
f) posuzuje při hodnocení primárních aktiv alespoň oblasti uvedené v příloze č. 1 k této vyhlášce,
g) určuje a eviduje vazby mezi aktivy, která mají vliv na bezpečnost regulované služby,
f) hodnotí podpůrná aktiva a vychází přitom zejména z určených vazeb na primární aktiva a
g) pro jednotlivé úrovně aktiv podle písmene b) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, integrity a dostupnosti, která obsahují alespoň

1. přípustné způsoby používání aktiv,
2. pravidla pro manipulaci s aktivy, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,
3. pravidla pro klasifikaci informací,
4. pravidla pro označování aktiv,
5. pravidla správy výměnných médií a
6. pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidace technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 2 k této vyhlášce.

§ 8 Řízení rizik

(1) Povinná osoba při řízení rizik v návaznosti na § 7

a) stanoví metodiku pro určování a hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik,

b) při určování rizik s ohledem na aktiva určuje relevantní hrozby a zranitelnosti; přitom zvažuje alespoň kategorie hrozeb a zranitelností uvedených v příloze č. 3 k této vyhlášce,

c) provádí hodnocení rizik v pravidelných intervalech alespoň jednou ročně a při významných změnách určených podle § 11 odst. 1 písm. c), při kterém zohlední

1. relevantní hrozby a zranitelnosti podle písmene b) a posoudí možné dopady na aktiva, přičemž vychází z hodnocení aktiv podle § 7,
2. významné změny,
3. změny stanoveného rozsahu podle § 12 zákona,
4. protiopatření podle § 20 zákona,
5. kybernetické bezpečnostní incidenty, včetně dříve řešených,
6. výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
7. výsledky penetračního testování a skenování zranitelností a
8. výsledky vyhodnocení účinnosti systému řízení bezpečnosti informací,

§ 8 Řízení rizik

d) při hodnocení rizik postupuje alespoň v rozsahu přílohy č. 4 k této vyhlášce,
e) na základě provedeného hodnocení rizik podle písmene c) zpracuje zprávu o hodnocení rizik,
f) zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik **prohlášení o aplikovatelnosti**, které obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která

1. nebyla aplikována, včetně odůvodnění a uvedení případných přijatých náhradních bezpečnostních opatření, a

2. byla aplikována, včetně způsobu plnění,

§ 8 Řízení rizik

g) na základě provedeného hodnocení rizik podle písmene c) a v souladu se stanovenými kritérii pro akceptovatelnost rizik zpracuje **plán zvládání rizik**, který obsahuje

1. popis bezpečnostních opatření pro zvládání rizik,
2. cíle a přínosy bezpečnostních opatření pro zvládání rizik,
3. určení osoby zajišťující zavedení bezpečnostních opatření pro zvládání rizik,
4. předpokládané lidské, finanční a technické zdroje pro zavedení bezpečnostních opatření,
5. požadovaný termín zavedení bezpečnostních opatření,
6. popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a
7. konkrétní způsob realizace bezpečnostních opatření.

(2) Povinná osoba v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.

(3) Hodnocení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavci 1 písm. c), pokud povinná osoba zajistí stejnou nebo vyšší úroveň procesu hodnocení rizik a postupuje v souladu s odstavcem 5 přílohy č. 4 k této vyhlášce.

(4) Povinná osoba nemusí uplatňovat některá bezpečnostní opatření stanovená touto vyhláškou pouze na základě provedeného řízení rizik.

§ 9 Řízení dodavatelů

(1) Povinná osoba při řízení dodavatelů

a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,

b) prokazatelně seznamuje své dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel,

c) řídí rizika spojená s dodavateli,

d) identifikuje a eviduje své významné dodavatele ve smyslu § 2 písm. h),

e) prokazatelně písemně informuje své významné dodavatele o jejich evidenci podle písmene d),

f) zajistí v souvislosti s řízením rizik spojených s významnými dodavateli, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní ustanovení uvedená v příloze č. 5 k této vyhlášce a

g) pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

§ 9 Řízení dodavatelů

(2) Povinná osoba u významných dodavatelů dále

a) provádí v rámci výběrového řízení podle zákona o zadávání veřejných zakázek nebo před uzavřením smlouvy hodnocení rizik souvisejících s plněním podle přílohy č. 4 k této vyhlášce,

b) stanoví v rámci uzavíraných smluvních vztahů způsoby a úrovně realizace bezpečnostních opatření a smluvně určí obsah vzájemné odpovědnosti za zavedení a kontrolu bezpečnostních opatření,

c) provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a

d) zajistí v reakci na rizika a zjištěné nedostatky jejich řešení, která budou přijata bez zbytečného odkladu.

§ 9 Řízení dodavatelů

(3) Náležitosti prokazatelného informování podle odstavce 1 písm. e) jsou

a) identifikační údaje povinné osoby, včetně uvedení, že povinná osoba je poskytovatelem regulované služby v režimu vyšších povinností,
b) název regulované služby povinné osoby,
c) identifikační údaje významného dodavatele a
d) prohlášení, že dodavatel je pro povinnou osobu významným dodavatelem.

§ 10 Bezpečnost lidských zdrojů

(1) Povinná osoba v rámci bezpečnosti lidských zdrojů s ohledem na stav a potřeby systému řízení bezpečnosti informací stanoví **plán rozvoje bezpečnostního povědomí**, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí včetně formy, obsahu a rozsahu poučení a školení podle odstavce 2.

(2) Povinná osoba zahrne do plánu rozvoje bezpečnostního povědomí

a) poučení vrcholného vedení o jeho povinnostech a bezpečnostní politice, zejména v oblastech systému řízení bezpečnosti informací a řízení rizik,
b) poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice,
c) potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role,
d) pravidla tvorby bezpečných hesel v souladu s § 19 a
e) relevantní témata uvedená v příloze č. 6 k této vyhlášce.

§ 10 Bezpečnost lidských zdrojů

(3) Povinná osoba v rámci bezpečnostního povědomí zajistí

a) poučení vrcholného vedení o jeho povinnostech, o bezpečnostní politice zejména v oblasti systému řízení bezpečnosti informací, řízení rizik a řízení kontinuity činností formou vstupních a pravidelných školení k získání znalostí a dovedností vedoucích k určování rizik a posouzení vhodnosti zvolených postupů při řízení rizik a jejich dopadů na regulovanou službu,

b) poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,

c) pravidelná odborná školení osobám zastávajícím bezpečnostní role, přičemž vychází z aktuálních potřeb povinné osoby v oblasti kybernetické bezpečnosti a

d) pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní nebo služebním zařazením.

§ 10 Bezpečnost lidských zdrojů

(4) Povinná osoba v rámci bezpečnosti lidských zdrojů

a) určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu rozvoje bezpečnostního povědomí uvedeny,
b) zajistí v souladu s plánem rozvoje bezpečnostního povědomí provedení poučení a školení podle odstavce 3,
c) pravidelně hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených poučení, školení a dalších činností spojených se zlepšováním bezpečnostního povědomí,
d) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role,
e) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a
f) zajistí plynulost výkonu činností v případě ukončení nebo změny smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.

(5) Povinná osoba vede o poučení a školení podle odstavce 3 přehledy, které obsahují předmět poučení a školení včetně seznamu osob, které poučení a školení absolvovaly.

§ 11 Řízení změn

(1) Povinná osoba při řízení změn u aktiv

a) stanoví pravidla, postupy a kritéria pro určení významných změn,
b) určí změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost,
c) určuje u změn určených podle písmene b) významné změny v souladu se stanovenými pravidly, postupy a kritérii pro určení významných změn podle písmene a).

(2) Povinná osoba u významných změn

a) dokumentuje jejich řízení,
b) řídí rizika spojená s významnými změnami,
c) přijímá bezpečnostní opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,
d) aktualizuje bezpečnostní a provozní dokumentaci,
e) zajistí jejich testování před uvedením do provozu a
f) zajistí možnost navrácení do původního stavu.

(3) Povinná osoba na základě výsledků řízení rizik podle odstavce 2 písm. b) rozhoduje o provedení penetračního testování; pokud rozhodne o provedení penetračního testování, postupuje podle § 24 odst. 5.

§ 12 Akvizice, vývoj a údržba

(1) Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou aktiv

a) řídí rizika,
b) řídí významné změny podle § 11,
c) stanoví bezpečnostní požadavky, které zohlední i relevantní bezpečnostní opatření stanovená touto vyhláškou,
d) zahrne bezpečnostní požadavky stanovené podle písmene c) do plánované akvizice, vývoje a údržby a
e) zajistí oddělení provozního, zálohovacího, vývojového, testovacího, administrátorského a jiného specifického prostředí, a zajistí ochranu informací a dat, které se v něm vyskytují.

(2) Povinná osoba zajistí při provedení akvizice nebo vývoje technického aktiva

a) využívajícího autentizační mechanismus, zejména za účelem ověření identity uživatelů nebo administrátorů, plnění požadavků podle § 19 odst. 2,
b) využívajícího kryptografické algoritmy, plnění požadavku podle § 25 odst. 1 písm. a) a § 25 odst. 3 písm. a) a
c) dostupnost bezpečnostních aktualizací po dobu jeho životního cyklu.

§ 13 Řízení přístupu

(1) Povinná osoba na základě bezpečnostních a provozních potřeb řídí přístup k aktivům a přijímá bezpečnostní opatření, která slouží k zajištění ochrany přístupových a autentizačních údajů, které jsou používány pro ověření identity podle § 19 a 20.

(2) Povinná osoba dále při řízení přístupu k aktivům

a) řídí přístup na základě skupin nebo rolí,

b) přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu práce a jedinečný identifikátor daného typu účtu, **přičemž odděluje uživatelské a administrátorské účty jedné osoby,**

c) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,

d) zavádí v souladu s písmenem c) bezpečnostní opatření pro řízení přístupu technických aktiv,

e) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě,

f) omezí a kontroluje používání programových prostředků a vybavení, které mohou být schopné překonat systémové nebo aplikační kontroly,

§ 13 Řízení přístupu

g) přiděluje a odebírá přístupová práva a oprávnění v souladu s politikou řízení přístupu,
h) provádí pravidelné přezkoumání veškerých přístupových práv a oprávnění včetně rozdělení do skupin a rolí,
i) zajistí bezodkladné odebrání nebo změnu přístupových práv a oprávnění při změně pozice nebo zařazení na základě skupin a rolí,
j) zajistí deaktivaci účtů a bezodkladné odebrání nebo změnu přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na základě kterého došlo ke zřízení přístupu k aktivům,
k) dokumentuje přidělování a odebírání přístupových práv a oprávnění a
l) využívá nástroj pro správu a ověřování identity podle § 19 a nástroj pro řízení přístupových práv a oprávnění podle § 20.

§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů

(1) Povinná osoba při zvládání kybernetických bezpečnostních událostí a incidentů

a) zavede procesy, pravidla a postupy pro detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí v souladu s § 21 až 23,

b) zavede procesy, pravidla a postupy pro koordinaci a zvládání kybernetických bezpečnostních incidentů,

c) přidělí odpovědnosti pro

1. detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí a
2. koordinaci a zvládání kybernetických bezpečnostních incidentů,

d) definuje a dodržuje pravidla a postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,

e) zajistí detekci kybernetických bezpečnostních událostí podle § 21,

f) zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování technických aktiv a podezření na zranitelnosti,

§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů

g) zajistí posuzování kybernetických bezpečnostních událostí, při kterých musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty,

h) zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,

i) přijímá bezpečnostní opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,

j) zajistí hlášení kybernetických bezpečnostních incidentů podle § 15 zákona,

k) prošetří a určí příčiny kybernetického bezpečnostního incidentu,

l) vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,

m) zajistí vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona, včetně popisu příčiny vzniku kybernetického bezpečnostního incidentu s významným dopadem, pokud je známa, a

n) vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu, popřípadě aktualizuje stávající bezpečnostní opatření.

(2) Povinná osoba dále při detekci a vyhodnocování kybernetických bezpečnostních událostí používá nástroje podle § 21 a 23.

§ 15 Řízení kontinuity činností

Povinná osoba při řízení kontinuity činností

a) stanoví metodiku pro provedení analýzy dopadů,

b) provádí analýzu dopadů, vyhodnocuje a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 8,

c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení

1. **minimální úrovně poskytovaných služeb**, která je přijatelná pro užívání, provoz a správu regulované služby,
2. **doby obnovení chodu**, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby, a
3. **bodu obnovení dat** jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání technického aktiva,

d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,

e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a

f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 26.

§ 16 Provádění auditu kybernetické bezpečnosti

(1) Povinná osoba stanoví plán provádění auditu kybernetické bezpečnosti.

(2) Povinná osoba při auditu kybernetické bezpečnosti

a) posuzuje, zda byla zavedena bezpečnostní opatření požadovaná zákonem a touto vyhláškou,
b) posuzuje soulad zavedených bezpečnostních opatření s právními předpisy, vnitřními předpisy, smluvními závazky a nejlepší praxí a
c) provádí a dokumentuje audit dodržování pravidel a postupů stanovených v bezpečnostní politice, včetně přezkoumání technické shody a dříve stanovených nápravných opatření podle odstavce 3 písm. b).

(3) Povinná osoba

a) zahrne výsledky auditu kybernetické bezpečnosti podle odstavce 2 do
    1. plánu rozvoje bezpečnostního povědomí,
    2. řízení rizik a
b) stanoví na základě výsledku auditu kybernetické bezpečnosti podle odstavce 2 případná nápravná opatření, která budou přijata bez zbytečného odkladu.

§ 16 Provádění auditu kybernetické bezpečnosti

(4) Audit kybernetické bezpečnosti podle odstavce 2 je prováděn

a) při významných změnách, a to v rámci jejich rozsahu,
b) v pravidelných intervalech alespoň jednou za 2 roky a
c) v souladu s plánem auditu kybernetické bezpečnosti.

(5) Není-li v odůvodněných případech možné provést audit v celém rozsahu podle odstavce 2 ve lhůtě podle odstavce 4 písm. b), je možné audit kybernetické bezpečnosti provádět průběžně po systematických celcích tak, aby byl naplněn celý rozsah auditu podle odstavce 2 alespoň jednou za 5 let.

(6) Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 5 odst. 4, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

Technická opatření

Hlava II

Změny v nVKB – technická opatření

- Fyzická bezpečnost
  - dokumentace perimetrů
- Bezpečnost komunikačních sítí
  - dokumentace segmentace a topologie
- Správa a ověřování identit
  - evidence autentizačních mechanismů pouze na bázi hesla
- Detekce KBU
  - součástí ochrana před škodlivým kódem
- Zaznamenávání událostí
  - nástroj pro sběr a uchovávání
- Aplikační bezpečnost
  - podpora, skenování zranitelností
- Kryptografické algoritmy
  - zabezpečení komunikace
- Zajišťování dostupnosti regulované služby
  - zálohování

§ 17 Fyzická bezpečnost

Povinná osoba v rámci fyzické bezpečnosti

a) předchází poškození, odcizení, zneužití aktiv, neoprávněným zásahům do nich a narušení bezpečnosti poskytování regulované služby,
b) stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a data, nebo ve které jsou umístěna technická aktiva regulované služby,
c) rozdělí fyzické bezpečnostní perimetry stanovené podle písmene b) s ohledem na hodnocení umístěných technických aktiv do jednotlivých úrovní fyzické ochrany a tyto stanovené fyzické bezpečnostní perimetry a jejich úrovně fyzické ochrany dokumentuje a

§ 17 Fyzická bezpečnost

d) přijme u každého fyzického bezpečnostního perimetru s ohledem na jeho úroveň fyzické ochrany stanovenou podle písmene c) relevantní bezpečnostní opatření fyzické ochrany

1. k zamezení neoprávněnému vstupu,
2. k zamezení poškození, odcizení, zneužití aktiv, neoprávněným zásahům do nich a narušení bezpečnosti poskytování regulované služby,
3. k zajištění fyzické ochrany budov a jiných ohraničených prostor,
4. pro zajištění detekce narušení fyzického bezpečnostního perimetru a
5. k evidenci vstupů a přístupů do fyzického bezpečnostního perimetru.

§ 18 Bezpečnost komunikačních sítí

Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to včetně jejího síťového perimetru

a) zajistí a dokumentuje segmentaci komunikační sítě, včetně oddělení provozního, zálohovacího, vývojového, testovacího, administrátorského a jiného specifického prostředí,
b) zajistí řízení komunikace v rámci komunikační sítě,
c) zajistí řízení vzdáleného přístupu ke komunikační síti,
d) zajistí řízení vzdálené správy technických aktiv,
e) povoluje v souladu s písmeny b) až d) pouze takovou komunikaci, která je nezbytná pro řádné zajištění regulované služby,
f) zajistí v souladu s písmeny c) a d) časové omezení komunikace a opětovné ověření identity administrátorů a uživatelů po stanovené době,
g) zajistí pomocí aktuálně odolných kryptografických algoritmů upravených v § 25 a síťových protokolů důvěrnost a integritu při přenosu informací a dat,
h) využívá nástroj, který zajistí ochranu integrity komunikační sítě a
i) dokumentuje topologii komunikační sítě a infrastruktury.

§ 19 Správa a ověřování identit

(1) Povinná osoba používá nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv, který zajišťuje

a) ověření identity před zahájením jejich aktivit,
b) řízení počtu možných neúspěšných pokusů o přihlášení,
c) odolnost uložených a přenášených autentizačních údajů vůči hrozbám a zranitelnostem, které by mohly narušit jejich důvěrnost nebo integritu,
d) opětovné ověření identity po stanovené době nečinnosti,
e) dodržení důvěrnosti při vytváření výchozích autentizačních údajů a při obnově přístupu a
f) centralizovanou správu identit s ohledem na vazby mezi aktivy.

§ 19 Správa a ověřování identit

(2) Povinná osoba při ověření identity administrátorů, uživatelů a technických aktiv

a) využívá autentizační mechanismus, který je založen na vícefaktorové autentizaci s alespoň dvěma různými typy faktorů, nebo využívá autentizační mechanismus, který je založen na aktuálně odolné kontinuální autentizaci založené na modelu nulové důvěry a

b) do doby splnění požadavků podle písmene a), využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.

(3) Povinná osoba do doby splnění požadavků podle odstavce 2 písm. a) vede evidenci technických aktiv, účtů a autentizačních mechanismů, které tyto požadavky nesplňují, a to včetně odůvodnění.

§ 19 Správa a ověřování identit

(4) Povinná osoba do doby splnění požadavku podle odstavce 2 využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla, kdy tento nástroj musí vynucovat pravidlo

a) délky hesla alespoň
   1. 12 znaků pro účty uživatelů,
   2. 17 znaků pro účty administrátorů,
   3. 22 znaků pro účty technických aktiv,
b) umožňující zadat heslo o délce alespoň 64 znaků,
c) neomezující použití malých a velkých písmen, číslic a speciálních znaků,
d) umožňující uživatelům a administrátorům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut,
e) povinné změny hesla v intervalu alespoň jednou za 18 měsíců a
f) neumožňující uživatelům a administrátorům
   1. zvolit si jednoduchá a často používaná hesla,
   2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, adresy elektronické pošty, názvu systému nebo obdobným způsobem a
   3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.

§ 19 Správa a ověřování identit

(5) Povinná osoba v souladu s odstavcem 4 zajistí

a) bezodkladné vynucení změny výchozího hesla uživatelů a administrátorů po prvním přihlášení,
b) bezodkladné vynucení změny výchozího hesla technického aktiva,
c) vytváření hesla účtu technického aktiva složeného z náhodného řetězce malých a velkých písmen, číslic a speciálních znaků,
d) bezodkladné vynucení změny přístupového hesla v případě důvodného podezření na narušení jeho důvěrnosti,
e) vytvoření náhodného výchozího hesla nebo identifikátoru sloužícího k vytvoření nebo k obnovení přístupu a zajistí jeho důvěrnost a
f) bezodkladné zneplatnění hesla nebo identifikátoru sloužícího k vytvoření nebo k obnovení přístupu po jeho prvním použití nebo uplynutí nejvýše 24 hodin od jeho vytvoření.

§ 19 Správa a ověřování identit

(6) Povinná osoba u administrátorského účtu zejména určeného pro případ obnovy po kybernetickém bezpečnostním incidentu, musí zajistit

a) bezodkladnou změnu výchozího hesla,
b) vytvoření hesla náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,
c) délku hesla složeného alespoň z 22 znaků,
d) bezpečné uložení hesla,
e) omezení manipulace s účtem a jeho heslem, kdy s tímto účtem a jeho heslem mohou manipulovat pouze pověřené osoby, a to v nezbytně nutných případech,
f) změnu hesla po jeho použití, při jakékoli změně pověřených osob, v případě důvodného podezření na jeho kompromitaci nebo v intervalu alespoň jednou za 18 měsíců a
g) evidování manipulace a pokusy o manipulaci s tímto účtem a jeho heslem.

§ 20 Řízení přístupových oprávnění

Povinná osoba pro řízení přístupových práv a oprávnění využívá nástroj,

a) který je centralizovaný s ohledem na vazby mezi aktivy,
b) kterým řídí práva pro přístup k jednotlivým aktivům a
c) kterým řídí oprávnění pro čtení a zápis informací a dat a změnu oprávnění.

§ 21 Detekce kybernetických bezpečnostních událostí

(1) Povinná osoba používá nástroj pro detekci kybernetických bezpečnostních událostí, který zajišťuje

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

§ 21 Detekce kybernetických bezpečnostních událostí

(2) Povinná osoba používá s ohledem na vazby mezi aktivy pro detekci kybernetických bezpečnostních událostí centrálně spravovaný nástroj, který u jednotlivých relevantních technických aktiv zajišťuje

a) nepřetržitou a automatickou ochranu před škodlivým kódem,
b) řízení a sledování používání vyměnitelných zařízení a datových nosičů,
c) řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,
d) řízení oprávnění ke spouštění kódu,
e) řízení a sledování komunikace aplikací, jejich služeb a procesů,
f) detekci kybernetických bezpečnostních událostí technických aktiv a
g) detekci kybernetických bezpečnostních událostí na základě chování technických aktiv, administrátorů a uživatelů.

(3) Povinná osoba provádí pravidelnou a bezodkladnou aktualizaci nástroje používaného podle odstavců 1 a 2, a to včetně jeho nastavení a detekčních pravidel.

§ 22 Zaznamenávání událostí

(1) Povinná osoba na základě hodnocení aktiv a svých bezpečnostních potřeb

a) určí technická aktiva, u kterých je zaznamenávání bezpečnostních a relevantních provozních událostí prováděno, a
b) aktualizuje rozsah technických aktiv podle odstavce 1 písm. a) v pravidelných intervalech a při významných změnách.

(2) Povinná osoba zaznamenává bezpečnostní a relevantní provozní události

a) detekované podle § 21,
b) v rámci komunikační sítě,
c) na síťovém perimetru a
d) technických aktiv určených podle odstavce 1 písm. a).

§ 22 Zaznamenávání událostí

(3) Povinná osoba v rámci zaznamenávání událostí podle odstavce 2, zaznamenává

a) přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
b) provedení a neúspěšné pokusy o provedení privilegované činnosti,
c) manipulace a neúspěšné pokusy o manipulaci s účty, oprávněními a právy,
d) neprovedení činností v důsledku nedostatku přístupových práv nebo oprávnění,
e) zahájení a ukončení činností technických aktiv,
f) kritická a chybová hlášení technických aktiv,
g) přístupy a neúspěšné pokusy o přístupy k záznamům událostí,
h) manipulace a neúspěšné pokusy o manipulaci se záznamy událostí,
i) změny a neúspěšné pokusy o změny nastavení nástrojů pro zaznamenávání událostí a
j) další činnosti uživatelů, které mohou mít vliv na bezpečnost regulované služby.

§ 22 Zaznamenávání událostí

(4) Povinná osoba v rámci zaznamenávání událostí podle odstavce 2 zaznamenává následující informace o události

a) datum a čas včetně specifikace časového pásma,
b) typ činnosti,
c) jednoznačnou identifikaci technického aktiva, které činnost zaznamenalo, a to i v případě, kdy v komunikační síti dochází ke změně této síťové identifikace,
d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, a to i v případě, kdy v komunikační síti dochází ke změně této síťové identifikace,
e) jednoznačnou identifikaci zařízení původce, a to i v případě, kdy v komunikační síti dochází ke změně této síťové identifikace, a
f) úspěšnost nebo neúspěšnost činnosti.

§ 22 Zaznamenávání událostí

(5) Povinná osoba dále s ohledem na události zaznamenané podle odstavce 2

a) zajistí důvěrnost a integritu získaných informací, včetně ochrany před neoprávněným čtením a jakoukoliv změnou,
b) používá s ohledem na vazby mezi aktivy centralizovaný nástroj pro sběr a uchovávání záznamů těchto událostí a
c) uchovává záznamy těchto událostí alespoň po dobu 18 měsíců.

(6) Povinná osoba zajišťuje nepřetržitou synchronizaci jednotného času technických aktiv.

§ 23 Vyhodnocování kybernetických bezpečnostních událostí

(1) Povinná osoba používá nástroj pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí detekovaných podle § 21, který zajišťuje

a) sběr, vyhledávání a seskupování souvisejících záznamů za účelem detekce kybernetických bezpečnostních událostí,
b) nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech, včasné varování vybraných bezpečnostních rolí a dalších relevantních osob a
c) vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů.

§ 23 Vyhodnocování kybernetických bezpečnostních událostí

(2) Povinná osoba při používání nástroje pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí v souladu s odstavcem 1 zajistí

a) omezení případů nesprávného nebo nežádoucího vyhodnocování kybernetických bezpečnostních událostí,
b) pravidelnou aktualizaci nastavení nástroje včetně jeho pravidel pro detekci a vyhodnocování kybernetických bezpečnostních událostí a
c) pravidelnou aktualizaci pravidel pro nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech včetně včasného varování vybraných bezpečnostních rolí a dalších relevantních osob.

(3) Povinná osoba zajistí využívání informací získaných nástrojem pro vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení systému řízení bezpečnosti informací regulované služby.

§ 24 Aplikační bezpečnost

(1) Povinná osoba pro zajištění bezpečnosti regulované služby užívá technická aktiva, která jsou jejich výrobcem, dodavatelem nebo jinou osobou podporována a zajistí aplikování schválených bezpečnostních aktualizací vydaných pro tato aktiva.

(2) Povinná osoba do doby plnění podle odstavce 1 zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv a eviduje technická aktiva

a) která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a
b) na která není možné aplikovat poslední schválenou bezpečnostní aktualizaci.

(3) Povinná osoba v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před

a) neoprávněnou činností a
b) popřením provedených činností.

§ 24 Aplikační bezpečnost

(4) Povinná osoba v rámci skenování zranitelností technických aktiv

a) provádí pravidelné skenování zranitelností technických aktiv regulované služby

   1. z vnitřní a vnější komunikační sítě a
   2. alespoň jednou ročně.

b) zohlední výsledky skenování zranitelností technických aktiv v rámci řízení rizik podle § 8 a zavádí bezpečnostní opatření na základě zjištěných výsledků.

§ 24 Aplikační bezpečnost

(5) Povinná osoba v rámci penetračního testování

a) provádí penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik
b) z vnitřní a vnější komunikační sítě,
c) před jejich uvedením do provozu a
d) v souvislosti s významnou změnou podle § 11 odst. 3,
e) zohlední výsledky penetračního testování při řízení rizik podle § 8 a zavádí bezpečnostní opatření na základě zjištěných výsledků,
f) provádí v souladu s odstavcem 5 písm. a) bodem 1 pravidelně penetrační testování, a to alespoň jednou za 2 roky,
g) v odůvodněných případech, pokud nemůže provést penetrační testování v rozsahu nebo intervalu stanoveném v odstavci 5 písm. c), může rozdělit toto penetrační testování do systematických celků. V takovém případě je nutno provést penetrační testování v rozsahu stanoveném v odstavci 5 písm. a) nejpozději do 5 let,
h) u penetračních testů v souladu s odstavcem 5 písm. a) eviduje termín provedení a konkrétní fyzické osoby provádějící toto penetrační testování.

(6) Povinná osoba provede opětovné otestování nálezu zjištěného na základě provedeného skenování zranitelností nebo penetračního testování za účelem ověření funkčnosti zavedených bezpečnostních opatření.

§ 25 Kryptografické algoritmy

(1) Povinná osoba při zajištění bezpečnosti technických aktiv a jejich komunikace

a) používá pouze aktuálně odolné kryptografické algoritmy,

b) prosazuje bezpečné nakládání s kryptografickými algoritmy a

c) zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Národním úřadem pro kybernetickou a informační bezpečnost.

(2) Povinná osoba zajišťuje bezpečnou

a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a

b) nouzovou komunikaci v rámci organizace.

(3) Povinná osoba v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě používá

a) pouze aktuálně odolné kryptografické klíče a certifikáty a

b) nástroj pro správu kryptografických klíčů a certifikátů, který

1. zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů,
2. umožní kontrolu a audit a
3. zajistí důvěrnost a integritu kryptografických klíčů.

§ 26 Zajišťování dostupnosti regulované služby

(1) Povinná osoba zavede bezpečnostní opatření pro zajišťování dostupnosti regulované služby, kterými zajistí

a) dostupnost regulované služby podle cílů stanovených podle § 15,
b) odolnost regulované služby vůči hrozbám a zranitelnostem, které by mohly snížit její dostupnost a
c) redundanci aktiv nezbytných pro zajišťování dostupnosti regulované služby.

(2) Povinná osoba pro zajišťování dostupnosti regulované služby v souladu s odstavcem 1 vytváří pravidelné zálohy konfigurací a nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby v případě kybernetického bezpečnostního incidentu.

§ 26 Zajišťování dostupnosti regulované služby

(3) Povinná osoba u záloh vytvářených podle odstavce 2 zajistí

a) pravidelné testování jejich integrity, dostupnosti a obnovitelnosti,

b) dokumentování výsledků testů provedených podle odstavce 3 písm. a),

c) ochranu ukládaných záloh a dat v nich obsažených před narušením jejich integrity a důvěrnosti, a to alespoň šifrováním těchto záloh v souladu s § 25 a

d) ochranu ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti.

(4) Povinná osoba pro zajišťování dostupnosti regulované služby zajistí bezpečnou správu konfigurací a nastavení technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik.

(5) Povinná osoba za účelem omezení šíření kybernetického bezpečnostního incidentu a snížení jeho dopadu odděluje zálohovací prostředí od jiných prostředí podle § 18 písm. a).

§ 27 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Povinná osoba včetně požadavků uvedených v § 3 až 26 pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických technických aktiv dále využívá nástroje a zavádí bezpečnostní opatření, která zajistí

a) omezení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,
b) omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,
c) segmentaci a oddělení komunikačních sítí průmyslových, řídicích a obdobných specifických technických aktiv od jiných prostředí a segmentaci a oddělení těchto komunikačních sítí podle § 18,
d) omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv, včetně omezení komunikace mimo komunikační síť povinné osoby,
e) ochranu jednotlivých průmyslových, řídicích a obdobných specifických technických aktiv před využitím známých zranitelností a hrozeb a
f) dostupnost a obnovu průmyslových, řídicích a obdobných specifických technických aktiv pro zajištění dostupnosti regulované služby.

Děkuji za pozornost

https://portal.nukib.gov.cz/

regulace@nukib.gov.cz