316/2014 Sb.

VYHLÁŠKA

ze dne 15. prosince 2014

o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

Národní bezpečnostní úřad stanoví podle § 28 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), (dále jen „zákon“) k provedení § 6 písm. a) až c), § 8 odst. 4, § 13 odst. 4 a § 16 odst. 6 zákona.

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Předmět úpravy

Touto vyhláškou se stanoví obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznámení kontaktních údajů a jeho formu.

§ 2

Vymezení pojmů

V této vyhlášce se rozumí

a) systémem řízení bezpečnosti informací část systému řízení orgánu a osoby uvedené v § 3 písm. c) až e) zákona založená na přístupu k rizikům informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, která stanoví způsob ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací,

b) aktivem primární aktivum a podpůrné aktivum,

c) primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém,

d) podpůrným aktivem technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

e) technickým aktivem technické vybavení, komunikační prostředky a programové vybavení informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a objekty, ve kterých jsou tyto systémy umístěny,

f) rizikem možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační

infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození aktiva,

g) hodnocením rizik proces, při němž je určována významnost rizik a jejich přijatelná úroveň,

h) řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,

i) hrozbou potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva,

j) zranitelností slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami,

k) přijatelným rizikem riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik,

l) bezpečnostní politikou soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv orgánem a osobou uvedenou v § 3 písm. c) až e) zákona,

m) garantem aktiva fyzická osoba pověřená orgánem nebo osobou uvedenou v § 3 písm. c) až e) zákona k zajištění rozvoje, použití a bezpečnosti aktiva,

n) uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, která využívá primární aktiva,

o) administrátorem fyzická osoba pověřená garantem aktiva zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva.

ČÁST DRUHÁ

BEZPEČNOSTNÍ OPATŘENÍ

HLAVA I

ORGANIZAČNÍ OPATŘENÍ

§ 3

Systém řízení bezpečnosti informací

(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci systému řízení bezpečnosti informací

a) stanoví s ohledem na aktiva a organizační bezpečnost rozsah a hranice systému řízení bezpečnosti informací, ve kterém určí, kterých organizačních částí a technických prvků se systém řízení bezpečnosti informací týká,

b) řídí rizika podle § 4 odst. 1,

c) vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 5 a zavede příslušná bezpečnostní opatření,

d) monitoruje účinnost bezpečnostních opatření,

e) vyhodnocuje vhodnost a účinnost bezpečnostní politiky podle § 5,

f) zajistí provedení auditu kybernetické bezpečnosti podle § 15, a to nejméně jednou ročně,

g) zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně jednou ročně,

h) aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami a

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

(2) Orgán a osoba uvedená v § 3 písm. e) zákona v rámci systému řízení bezpečnosti informací

a) řídí rizika podle § 4 odst. 2,

b) vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 5, a zavede příslušná bezpečnostní opatření a

c) provádí aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.

§ 4

Řízení rizik

(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci řízení rizik

a) stanoví metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik,

b) identifikuje a hodnotí důležitost aktiv, která patří do rozsahu systému řízení bezpečnosti informací, podle § 8 v rozsahu přílohy č. 1 k této vyhlášce a výstupy zapracuje do zprávy o hodnocení aktiv a rizik,

c) identifikuje rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce, určí a schválí přijatelná rizika a zpracuje zprávu o hodnocení aktiv a rizik,

d) zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření,

e) zpracuje a zavede plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a

f) zohlední bez zbytečného odkladu reaktivní a ochranná opatření vydaná Národním bezpečnostním úřadem (dále jen „Úřad“) v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplní plán zvládání rizik.

(2) Orgán a osoba uvedená v § 3 písm. e) zákona v rámci řízení rizik

a) stanoví metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik,

b) identifikuje a hodnotí důležitost primárních aktiv, která patří do rozsahu systému řízení bezpečnosti informací, podle § 8 minimálně v rozsahu přílohy č. 1 k této vyhlášce a výstupy zapracuje do zprávy o hodnocení aktiv a rizik,

c) identifikuje rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na primární aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce a zpracuje zprávu o hodnocení aktiv a rizik,

d) zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření,

e) zpracuje a zavede plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termíny jejich zavedení a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními a

f) zohlední bez zbytečného odkladu reaktivní a ochranná opatření vydaná Úřadem v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplní plán zvládání rizik.

(3) Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavcích 1 a 2, pokud orgán a osoba uvedená v § 3 písm. c) až e) zákona zabezpečí, že používá opatření zajišťující stejnou nebo vyšší úroveň řízení rizik.

(4) Orgán a osoba uvedená v § 3 písm. c) až e) zákona při hodnocení rizik zvažuje zejména tyto hrozby

a) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,

b) poškození nebo selhání technického anebo programového vybavení,

c) zneužití identity fyzické osoby,

d) užívání programového vybavení v rozporu s licenčními podmínkami,

e) kybernetický útok z komunikační sítě,

f) škodlivý kód (například viry, spyware, trojské koně),

g) nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

h) narušení fyzické bezpečnosti,

i) přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,

j) zneužití nebo neoprávněná modifikace údajů,

k) trvale působící hrozby a

l) odcizení nebo poškození aktiva.

(5) Orgán a osoba uvedená v § 3 písm. c) až e) zákona při hodnocení rizik zvažuje zejména

tyto zranitelnosti

a) nedostatečná ochrana vnějšího perimetru,

b) nedostatečné bezpečnostní povědomí uživatelů a administrátorů,

c) nedostatečná údržba informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

d) nevhodné nastavení přístupových oprávnění,

e) nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

f) nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování a

g) nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí.

(6) Orgán a osoba uvedená v § 3 písm. c) a d) zákona při hodnocení rizik dále zvažuje tyto hrozby

a) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů kritické informační infrastruktury,

b) pochybení ze strany zaměstnanců,

c) zneužití vnitřních prostředků, sabotáž,

d) dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,

e) nedostatek zaměstnanců s potřebnou odbornou úrovní,

f) cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik a

g) zneužití vyměnitelných technických nosičů dat.

(7) Orgán a osoba uvedená v § 3 písm. c) a d) zákona při hodnocení rizik dále zvažuje tyto zranitelnosti

a) nedostatečná ochrana prostředků kritické informační infrastruktury,

b) nevhodná bezpečnostní architektura,

c) nedostatečná míra nezávislé kontroly a

d) neschopnost včasného odhalení pochybení ze strany zaměstnanců.

§ 5

Bezpečnostní politika

(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona stanoví bezpečnostní politiku v oblastech

a) systém řízení bezpečnosti informací,

b) organizační bezpečnost,

c) řízení vztahů s dodavateli,

d) klasifikace aktiv,

e) bezpečnost lidských zdrojů,

f) řízení provozu a komunikací,

g) řízení přístupu,

h) bezpečné chování uživatelů,

i) zálohování a obnova,

j) bezpečné předávání a výměna informací,

k) řízení technických zranitelností,

l) bezpečné používání mobilních zařízení,

m) poskytování a nabývání licencí programového vybavení a informací,

n) dlouhodobé ukládání a archivace informací,

o) ochrana osobních údajů,

p) fyzická bezpečnost,

q) bezpečnost komunikační sítě,

r) ochrana před škodlivým kódem,

s) nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,

t) využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a

u) používání kryptografické ochrany.

(2) Orgán a osoba uvedená v § 3 písm. e) zákona stanoví bezpečnostní politiku v oblastech

a) systém řízení bezpečnosti informací,

b) organizační bezpečnost,

c) řízení dodavatelů,

d) klasifikace aktiv,

e) bezpečnost lidských zdrojů,

f) řízení provozu a komunikací,

g) řízení přístupu,

h) bezpečné chování uživatelů,

i) zálohování a obnova,

j) poskytování a nabývání licencí programového vybavení a informací,

k) ochrana osobních údajů,

l) používání kryptografické ochrany,

m) ochrana před škodlivým kódem a

n) nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.

(3) Orgán a osoba uvedená v § 3 písm. c) až e) zákona pravidelně hodnotí účinnost bezpečnostní politiky a aktualizuje ji.

§ 6

Organizační bezpečnost

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona zavede organizaci řízení bezpečnosti informací, v rámci které určí výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury, komunikačním systémem kritické informační infrastruktury nebo významným informačním systémem.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona určí bezpečnostní role

a) manažer kybernetické bezpečnosti,

b) architekt kybernetické bezpečnosti,

c) auditor kybernetické bezpečnosti a

d) garant aktiva podle § 2 písm. m).

(3) Orgán a osoba uvedená v § 3 písm. e) určí bezpečnostní role přiměřeně podle odstavce 2.

(4) Manažer kybernetické bezpečnosti je osoba, odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let.

(5) Architekt kybernetické bezpečnosti je osoba zajišťující návrh a implementaci bezpečnostních opatření, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let.

(6) Auditor kybernetické bezpečnosti je osoba provádějící audit kybernetické bezpečnosti, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí uvedených v odstavci 2 písm. a), b) nebo d).

(7) Výbor pro řízení kybernetické bezpečnosti je organizovaná skupina tvořená osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.

(8) Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajistí odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. b).

§ 7

Stanovení bezpečnostních požadavků pro dodavatele

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona zavede pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a zohlední je u dodavatelů nebo jiných osob, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému prokazatelně dokumentuje orgán a osoba uvedená v § 3 písm. c) až e) zákona smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona u dodavatelů uvedených v odstavci 1 dále

a) před uzavřením smlouvy provádí hodnocení rizik podle přílohy č. 2 k této vyhlášce, která jsou spojena s podstatnými dodávkami,

b) uzavírá smlouvu o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření, a

c) provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky odstraňuje nebo po dohodě s dodavatelem zajistí jejich odstranění.

§ 8

Řízení aktiv

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení aktiv

a) identifikuje a eviduje primární aktiva,

b) určí garanty aktiv, kteří jsou odpovědní za primární aktiva, a

c) hodnotí důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k této vyhlášce.

(2) Při hodnocení důležitosti primárních aktiv je třeba především posoudit

a) rozsah a důležitost osobních údajů nebo obchodního tajemství,

b) rozsah dotčených právních povinností nebo jiných závazků,

c) rozsah narušení vnitřních řídících a kontrolních činností,

d) poškození veřejných, obchodních nebo ekonomických zájmů,

e) možné finanční ztráty,

f) rozsah narušení běžných činností orgánu a osoby uvedené v § 3 písm. c) až e) zákona,

g) dopady spojené s narušením důvěrnosti, integrity a dostupnosti a

h) dopady na zachování dobrého jména nebo ochranu dobré pověsti.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) identifikuje a eviduje podpůrná aktiva,

b) určí garanty aktiv, kteří jsou odpovědní za podpůrná aktiva, a

c) určí vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy.

(4) Orgán a osoba uvedená v § 3 písm. c) až e) zákona dále

a) stanoví pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že
1. určí způsoby rozlišování jednotlivých úrovní aktiv,
2. stanoví pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv a
3. stanoví přípustné způsoby používání aktiv,

b) zavede pravidla ochrany odpovídající úrovni aktiv a

c) určí způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.

§ 9

Bezpečnost lidských zdrojů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů

a) stanoví plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny,

b) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,

c) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a

d) zajistí vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona vede o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) stanoví pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů,

b) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí,

c) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a

d) zajistí změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

§ 10

Řízení provozu a komunikací

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení provozu a komunikací pomocí technických nástrojů uvedených v § 21 až 23 detekuje kybernetické bezpečnostní události, pravidelně vyhodnocuje získané informace a na zjištěné nedostatky reaguje v souladu s § 13.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení provozu a komunikací dále zajišťuje bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem stanoví provozní pravidla a postupy.

(3) Provozní pravidla a postupy orgánu a osoby uvedené v § 3 písm. c) a d) zákona obsahují

a) práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů,

b) postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů,

c) postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech,

d) spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží,

e) postupy řízení a schvalování provozních změn a

f) postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.

(4) Řízení provozu orgánu a osoby uvedené v § 3 písm. c) až e) zákona spočívá v provádění pravidelného zálohování a prověřování použitelnosti provedených záloh.

(5) Řízení provozu orgánu a osoby uvedené v § 3 písm. c) a d) zákona spočívá v

a) zajištění oddělení vývojového, testovacího a produkčního prostředí,

b) řešení reaktivních opatření vydaných Úřadem tím, že orgán a osoba uvedená v § 3 písm. c) a d) zákona
1. posoudí očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnotí možné negativní účinky a bez zbytečného odkladu je oznámí Úřadu a
2. stanoví způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určí časový plán jeho provedení.

(6) Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci řízení komunikací

a) zajišťuje bezpečnost a integritu komunikačních sítí a bezpečnost komunikačních služeb podle § 17,

b) určí pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi,

c) provádí výměnu a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla dokumentuje a

d) s ohledem na klasifikaci aktiv provádí výměnu a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.

§ 11

Řízení přístupu a bezpečné chování uživatelů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona na základě provozních a bezpečnostních potřeb řídí přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a přidělí každému uživateli jednoznačný identifikátor.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona přijme opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle § 18 a 19, a která brání ve zneužití těchto údajů neoprávněnou osobou.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále v rámci řízení přístupu

a) přidělí přistupujícím aplikacím samostatný identifikátor,

b) omezí přidělování administrátorských oprávnění,

c) přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,

d) provádí pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích,

e) využívá nástroj pro ověřování identity uživatelů podle § 18 a nástroj pro řízení přístupových oprávnění podle § 19 a

f) zavede bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.

§ 12

Akvizice, vývoj a údržba

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona stanoví bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a zahrne je do projektu akvizice, vývoje a údržby systému.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) identifikuje, hodnotí a řídí rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury; pro postupy hodnocení a řízení rizik se metodiky podle § 4 odst. 1 písm. a) použijí obdobně,

b) zajistí bezpečnost vývojového prostředí a zajistí ochranu používaných testovacích dat a

c) provádí bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.

§ 13

Zvládání kybernetických bezpečnostních událostí a incidentů

Orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů

a) přijme nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních vede záznamy,

b) připraví prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle § 21 až 23, provádí jejich vyhodnocení a identifikuje kybernetické bezpečnostní incidenty,

c) provádí klasifikaci kybernetických bezpečnostních incidentů, přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, provádí hlášení kybernetického bezpečnostního incidentu podle § 32 a zajistí sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,

d) prošetří a určí příčiny kybernetického bezpečnostního incidentu, vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu a

e) dokumentuje zvládání kybernetických bezpečnostních incidentů.

§ 14

Řízení kontinuity činností

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení kontinuity činností stanoví

a) práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role,

b) cíle řízení kontinuity činností formou určení
1. minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,
2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, a
3. dobu obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu, a

c) strategii řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností,

b) stanoví, aktualizuje a pravidelně testuje plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury,

c) realizuje opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a využívá nástroj pro zajišťování úrovně dostupnosti podle § 26 a

d) stanoví a aktualizuje postupy pro provedení opatření vydaných Úřadem podle § 13 a 14 zákona, ve kterých zohlední
1. výsledky hodnocení rizik provedení opatření,
2. stav dotčených bezpečnostních opatření a
3. vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.

§ 15

Kontrola a audit kritické informační infrastruktury a významných informačních systémů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci kontroly a auditu kritické informační infrastruktury a významných informačních systémů (dále jen „audit kybernetické bezpečnosti“)

a) posuzuje soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a určí opatření pro jeho prosazování a

b) provádí a dokumentuje pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona zajišťuje provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6, která hodnotí správnost a účinnost zavedených bezpečnostních opatření.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále pro informační systém kritické informační infrastruktury a komunikační systém kritické informační infrastruktury provádí kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reaguje na zjištěné zranitelnosti.

HLAVA II

TECHNICKÁ OPATŘENÍ

§ 16

Fyzická bezpečnost

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci fyzické bezpečnosti

a) přijme nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

b) přijme nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, a

c) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále uplatňuje prostředky fyzické bezpečnosti

a) pro zajištění ochrany na úrovni objektů a

b) pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.

(3) Prostředky fyzické bezpečnosti jsou zejména

a) mechanické zábranné prostředky,

b) zařízení elektrické zabezpečovací signalizace,

c) prostředky omezující působení požárů,

d) prostředky omezující působení projevů živelních událostí,

e) systémy pro kontrolu vstupu,

f) kamerové systémy,

g) zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a

h) zařízení pro zajištění optimálních provozních podmínek.

§ 17

Nástroj pro ochranu integrity komunikačních sítí

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavede

a) řízení bezpečného přístupu mezi vnější a vnitřní sítí,

b) segmentaci zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí,

c) kryptografické prostředky (§ 25) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií a

d) opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále využívá nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.

§ 18

Nástroj pro ověřování identity uživatelů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.

(2) Nástroj pro ověřování identity uživatelů a administrátorů zajišťuje ověření identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury a významném informačním systému.

(3) Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje

a) minimální délku hesla osm znaků,

b) minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků
1. nejméně jedno velké písmeno,
2. nejméně jedno malé písmeno,
3. nejméně jednu číslici, nebo
4. nejméně jeden speciální znak odlišný od požadavků uvedených v bodech 1 až 3,

c) maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.

(4) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) používá nástroj pro ověření identity, který
1. zamezí opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin, a
2. provádí opětovné ověření identity po určené době nečinnosti a

b) využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c).

(5) Nástroj pro ověřování identity uživatelů může být zajištěn i jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, pokud orgán a osoba uvedená v § 3 písm. c) až e) zákona zabezpečí, že používá opatření zajišťující stejnou nebo vyšší úroveň odolnosti hesla.

§ 19

Nástroj pro řízení přístupových oprávnění

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění

a) pro přístup k jednotlivým aplikacím a datům a

b) pro čtení dat, pro zápis dat a pro změnu oprávnění.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.

§ 20

Nástroj pro ochranu před škodlivým kódem

Orgán a osoba uvedená v § 3 písm. c) až e) zákona pro řízení rizik spojených s působením škodlivého kódu používá nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu

a) komunikace mezi vnitřní sítí a vnější sítí,

b) serverů a sdílených datových úložišť a

c) pracovních stanic,
přičemž provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým

kódem, jeho definic a signatur.

§ 21

Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajistí

a) sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a

b) ochranu získaných informací před neoprávněným čtením nebo změnou.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona dále pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému zaznamenává

a) přihlášení a odhlášení uživatelů a administrátorů,

b) činnosti provedené administrátory,

c) činnosti vedoucí ke změně přístupových oprávnění,

d) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,

e) zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,

f) automatická varovná nebo chybová hlášení technických aktiv,

g) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a

h) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle odstavce 2 uchovává nejméně po dobu 3 měsíců.

(4) Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajišťuje nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

§ 22

Nástroj pro detekci kybernetických bezpečnostních událostí

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro detekci

kybernetických bezpečnostních událostí, které zajistí ověření, kontrolu a případně zablokování komunikace

a) v rámci vnitřní komunikační sítě a

b) serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.

§ 23

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajistí

a) integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury,

b) poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury a

c) nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále zajistí

a) pravidelnou aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování, a

b) využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.

§ 24

Aplikační bezpečnost

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona provádí bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále v rámci aplikační bezpečnosti zajistí trvalou ochranu

a) aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou a

b) transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.

§ 25

Kryptografické prostředky

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona

a) pro používání kryptografické ochrany stanoví
1. úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a
2. pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat a

b) v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používá kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a průkaznou identifikaci osoby za provedené činnosti.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) stanoví pro používání kryptografických prostředků systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů, a

b) používá odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem.

§ 26

Nástroj pro zajišťování úrovně dostupnosti

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používá nástroj pro zajišťování úrovně dostupnosti informací.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro zajišťování úrovně dostupnosti informací, který zajistí

a) dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností,

b) odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost, a

c) zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury
1. využitím redundance v návrhu řešení a
2. zajištěním náhradních technických aktiv v určeném čase.

§ 27

Bezpečnost průmyslových a řídicích systémů

Orgán a osoba uvedená v § 3 písm. c) a d) zákona pro bezpečnost průmyslových a řídicích systémů, které jsou informačním systémem kritické informační infrastruktury nebo komunikačním systémem kritické informační infrastruktury anebo jsou jejich součástí, používá nástroje, které zajistí

a) omezení fyzického přístupu k síti a zařízením průmyslových a řídicích systémů,

b) omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů,

c) ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých

zranitelností a

d) obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu.

HLAVA III

BEZPEČNOSTNÍ DOKUMENTACE

§ 28

Bezpečnostní dokumentace

(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona vede a aktualizuje bezpečnostní dokumentaci, která obsahuje

a) bezpečnostní politiku podle § 5 odst. 1,

b) zprávy z auditu kybernetické bezpečnosti podle § 3 odst. 1 písm. f),

c) zprávy z přezkoumání systému řízení bezpečnosti informací podle § 3 odst. 1 písm. g),

d) metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik,

e) zprávu o hodnocení aktiv a rizik,

f) prohlášení o aplikovatelnosti,

g) plán zvládání rizik,

h) plán rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. a),

i) zvládání kybernetických bezpečnostních incidentů podle § 13 písm. e),

j) strategii řízení kontinuity činností podle § 14 odst. 1 písm. c) a

k) přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků podle § 15 odst. 1 písm. a).

(2) Orgán a osoba uvedená v § 3 písm. e) zákona vede a aktualizuje bezpečnostní dokumentaci, která obsahuje

a) bezpečnostní politiku podle § 5 odst. 2,

b) metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik podle § 4 odst. 2 písm. a),

c) zprávu o hodnocení aktiv a rizik podle § 4 odst. 2 písm. b) a c),

d) prohlášení o aplikovatelnosti podle § 4 odst. 2 písm. d),

e) plán zvládání rizik podle § 4 odst. 2 písm. e),

f) plán rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. a),

g) zvládání kybernetických bezpečnostních incidentů podle § 13 písm. e),

h) strategii řízení kontinuity činností podle § 14 odst. 1 písm. c) a

i) přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků podle § 15

odst. 1 písm. a).

(3) Orgán a osoba uvedená v § 3 písm. c) až e) zákona vede bezpečnostní dokumentaci tak, aby záznamy o provedených činnostech byly úplné, čitelné, snadno identifikovatelné a aby se daly snadno vyhledat. Opatření potřebná k identifikaci, uložení, ochraně, vyhledání, době platnosti a uspořádání záznamů o provedených činnostech dokumentuje.

(4) Doporučená struktura bezpečnostní dokumentace je stanovena v příloze č. 4 k této vyhlášce.

§ 29

Prokázání certifikace

Orgán a osoba uvedená v § 3 písm. c) až e) zákona, jejíž informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém je zcela zahrnut do rozsahu systému řízení bezpečnosti informací, který byl certifikován podle příslušné technické normy[1)] akreditovaným certifikačním orgánem, a která vede dokumenty obsahující

a) popis rozsahu systému řízení bezpečnosti informací,

b) prohlášení politiky a cílů systému řízení bezpečnosti informací,

c) popis použité metody hodnocení rizik a zprávu o hodnocení rizik,

d) prohlášení o aplikovatelnosti,

e) certifikát systému řízení bezpečnosti informací splňující požadavky příslušné technické normy zabývající se bezpečností informací[1)],

f) záznam o přezkoumání systému řízení bezpečnosti informací včetně souvisejících vstupů a výstupů přezkoumání a

g) zprávu z auditů provedených certifikačním orgánem včetně příslušných záznamů o nápravě zjištěných neshod s příslušnou normou,

splňuje požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky.

ČÁST TŘETÍ

KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT

§ 30

Typy kybernetických bezpečnostních incidentů

(1) Podle příčiny jsou kybernetické bezpečnostní incidenty rozděleny do následujících typů

a) kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb,

b) kybernetický bezpečnostní incident způsobený škodlivým kódem,

c) kybernetický bezpečnostní incident způsobený překonáním technických opatření,

d) kybernetický bezpečnostní incident způsobený porušením organizačních opatření,

e) kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb a

f) ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem.

(2) Podle dopadu jsou kybernetické bezpečnostní incidenty rozděleny do následujících typů

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).

§ 31

Kategorie kybernetických bezpečnostních incidentů

(1) Pro potřeby zvládání kybernetických bezpečnostních incidentů se podle následků a negativních projevů kybernetické bezpečnostní incidenty dělí do následujících kategorií

a) Kategorie III - velmi závažný kybernetický bezpečnostní 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 kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

b) Kategorie II - závažný kybernetický bezpečnostní 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 kybernetického incidentu včetně minimalizace vzniklých škod.

c) Kategorie I - méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona při kategorizaci jednotlivých kybernetických bezpečnostních incidentů podle odstavce 1 zohlední

a) důležitost dotčených aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

b) dopady na poskytované služby informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, nebo významného informačního systému,

c) dopady na služby poskytované jinými informačními systémy kritické informační infrastruktury, komunikačními systémy kritické informační infrastruktury, nebo významnými informačními systémy a

d) předpokládané škody a další dopady.

§ 32

Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona hlásí kybernetický bezpečnostní incident

a) v elektronické podobě prostřednictvím
1. elektronického formuláře zveřejněného na internetových stránkách Úřadu,
2. emailu na adresu elektronické pošty Úřadu určené pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněné na internetových stránkách Úřadu,
3. datové zprávy do datové schránky Úřadu, nebo
4. prostřednictvím určeného datového rozhraní, jehož popis je zveřejněn na internetových stránkách Úřadu, anebo

b) v listinné podobě na adresu Národního centra kybernetické bezpečnosti, zveřejněné na internetových stránkách Úřadu.

(2) Hlášení v listinné podobě se zasílá pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavci 1 písm. a).

(3) Náležitosti hlášení kybernetického bezpečnostního incidentu jsou uvedeny v příloze č. 5 k této vyhlášce.

ČÁST ČTVRTÁ

REAKTIVNÍ OPATŘENÍ A KONTAKTNÍ ÚDAJE

§ 33

Reaktivní opatření

Orgán a osoba uvedená v § 3 písm. c) až e) zákona oznámí provedení reaktivního opatření a jeho výsledek na formuláři, jehož vzor je uveden v příloze č. 6 k této vyhlášce.

§ 34

Kontaktní údaje

Orgán a osoba uvedená v § 3 zákona oznamuje kontaktní údaje na formuláři, jehož vzor je uveden v příloze č. 7 k této vyhlášce. Orgán a osoba uvedená v § 3 písm. c) až e) zákona oznamuje kontaktní údaje formou uvedenou v § 32 odst. 1 písm. a).

ČÁST PÁTÁ

ÚČINNOST

§ 35

Tato vyhláška nabývá účinnosti dnem 1. ledna 2015.

Ředitel:

Ing. Navrátil v. r.

Příloha 1

Hodnocení a úrovně důležitosti aktiv

Pro hodnocení důležitosti aktiv jsou použity stupnice o čtyřech úrovních. Orgán nebo osoba uvedená v § 3 písm. c) až e) zákona může používat odlišný počet úrovní pro hodnocení důležitosti aktiv, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jí používaným způsobem hodnocení důležitosti aktiv a stupnicemi a úrovněmi pro hodnocení důležitosti aktiv, které jsou uvedeny v této příloze.

V případě použití tří úrovní hodnocení důležitosti aktiv je přípustné sloučit buď úrovně nízká a střední, nebo úrovně vysoká a kritická.

Stupnice pro hodnocení důvěrnosti

Úroveň	Popis	Ochrana
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how orgánu a osoby uvedené v § 3 písm. c) až e) zákona, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje).	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.

Stupnice pro hodnocení integrity

Úroveň	Popis	Ochrana
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).

Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Ochrana
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Příloha 2

Hodnocení rizik

Hodnocení rizik je vyjádřeno jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

Pro hodnocení rizik lze použít zejména tuto funkci
riziko = dopad x hrozba x zranitelnost.

Jednoznačné určení funkce pro určení rizika je nezbytnou součástí metodiky pro identifikaci a hodnocení rizika.

Stupnice pro hodnocení dopadů	
Úroveň	Popis
Nízký	Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický. Rozsah případných škod nepřesahuje a) 10 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty do 5 000 000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob.
Střední	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí a) do 10 mrtvých nebo od 11 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 5 000 000 Kč do 50 000 000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2 500 osob.
Vysoký	Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí a) od 11 do 100 mrtvých nebo od 101 do 1 000 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 50 000 000 Kč do 500 000 000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2 501 do 25 000 osob.
Kritický	Dopad je plošný rozsahem, trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí a) 101 a více mrtvých a 1 001 a více osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty převyšující 500 000 000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25 000 osob.

Stupnice pro hodnocení hrozeb	
Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Stupnice pro hodnocení zranitelností	
Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována.Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Stupnice pro hodnocení rizik	
Úroveň	Popis
Nízké	Riziko je považováno za přijatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

V případě, že orgán nebo osoba uvedená v § 3 písm. c) až e) zákona využívá metodu pro identifikaci a hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení míry hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně postupuje i orgán nebo osoba uvedená

§ 3 písm. c) až e) zákona, které používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.

Příloha 3

Minimální požadavky na kryptografické algoritmy

(1) Symetrické algoritmy

a) Blokové a proudové šifry pro ochranu důvěrnosti a integrity

1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů Triple Data Encryption Standard (3DES) s využitím délky klíčů 168 bitů, omezené použití jen se zatížením klíče menším než 10 GB, postupně přecházet na AES.

2. Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu.

3. Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.

4. Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.

5. Twofish s využitím délky klíčů 128 až 256 bitů.

6. Serpent s využitím délky klíčů 128, 192, 256 bitů.

7. Camellia s využitím délky klíčů 128, 192 a 256 bitů.

8. SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů.

b) Módy šifrování s ochranou integrity

1. CCM,

2. EAX,

3. OCB,

4. Složená schémata typu "Encrypt-then-MAC".

Poznámka:
Schémata typu "Encrypt-then-MAC",musí používat k šifrování pouze uvedené šifrovací módy a k výpočtu MAC pouze uvedené módy pro ochranu integrity.

c) Módy šifrování

1. CTR,

2. OFB,

3. CBC,

4. CFB,

Poznámka:
Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným inicializačním vektorem, při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru, při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače, v případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

d) Módy pro ochranu integrity

1. HMAC,

2. CBC-MAC-X9.19, omezené použití jen se zatížením menším než 10^9 MAC,

3. CBC-MAC-EMAC,

4. CMAC.

(2) Asymetrické algoritmy

a) Pro technologii digitálního podpisu

1. Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů a více, délky parametru cyklické podgrupy 224 bitů a více.

2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů a více.

3. Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů a více.

b) Pro procesy dohod na klíči a šifrování klíčů

1. Diffie-Hellman (DH) s využitím délky klíčů 2048 bitů a více, délky parametru cyklické podgrupy 224 bitů a více.

2. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů a více.

3. Elliptic Curve Integrated Encryption System - Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více.

4. Provably Secure Elliptic Curve - Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 256 bitů více.

5. Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více.

6. Rivest Shamir Adleman - Optimal Asymetric Encryption Pedding (RSA-OAEP) s využitím délky klíčů 2048 a více.

7. Rivest Shamir Adleman - Key Encapculation Mechanism (RSA-KEM) s využitím délky klíčů 2048 a více.

(3) Algoritmy hash funkcí

a) SHA-2
1. SHA-224,
2. SHA-256,
3. SHA-384,
4. SHA-512,
5. SHA-512/224,
6. SHA-512/256.

b) SHA-3
1. SHA3-224,
2. SHA3-256,
3. SHA3-384,

4. SHA3-512,
5. SHAKE-128,
6. SHAKE-256.

c) Ostatní hašovací funkce
1. Whirpool,
2. RIPEMD-160,
3. SHA 1 s omezeným použitím.

Poznámka č. 1:
SHA-1 se nesmí používat pro generování nových digitálních podpisů, časových razítek, jakékoliv jiné aplikace vyžadující nekolizní SHA-1.

Poznámka č. 2:
SHA-1 lze používat pouze pro ověřování již existujících digitálních podpisů a časových razítek, generování a ověřování HMAC-SHA1,funkce pro odvozování klíčů a pseudonáhodné generátory.

Příloha 4

Struktura bezpečnostní dokumentace

Tato příloha obsahuje doporučený obsah bezpečnostní dokumentace. Navrhované struktury jednotlivých dokumentů zahrnují témata, která jednotlivé dokumenty podle této vyhlášky pokrývají, přičemž uvedené struktury dokumentů nejsou závazné a je na orgánu nebo osobě uvedené v § 3 písm. c) až e) zákona, jaký přístup k tvorbě bezpečnostní dokumentace použije. Přípustná je i změna názvů jednotlivých dokumentů nebo integrování více témat do jednoho dokumentu.

I. **Struktura bezpečnostní politiky**

(1) Politika systému řízení bezpečnosti informací*

[§ 5 odst. 1 písm. a), § 5 odst. 2 písm. a)]

a) Cíle, principy a potřeby řízení bezpečnosti informací.

b) Rozsah a hranice systému řízení bezpečnosti informací.

c) Pravidla a postupy pro řízení dokumentace.

d) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.

e) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.

f) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.

g) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

(2) Politika organizační bezpečnosti**

[§ 5 odst. 1 písm. b), § 5 odst. 2 písm. b)]

a) Určení bezpečnostních rolí a jejich práv a povinností,

1. práva a povinnosti manažera kybernetické bezpečnosti,

2. práva a povinnosti architekta kybernetické bezpečnosti,

3. práva a povinnosti auditora kybernetické bezpečnosti,

4. práva a povinnosti garanta aktiv,

5. práva a povinnosti výboru pro řízení kybernetické bezpečnosti.

b) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.

(3) Politika řízení dodavatelů**

[§ 5 odst. 1 písm. c), § 5 odst. 2 písm. c)]

a) Pravidla a principy pro výběr dodavatelů.

b) Pravidla pro hodnocení rizik dodavatelů.

c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.

e) Pravidla pro hodnocení dodavatelů.

(4) Politika klasifikace aktiv**

[§ 5 odst. 1 písm. d), § 5 odst. 2 písm. d)]

a) Identifikace, hodnocení a evidence primárních aktiv

1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta,

2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.

b) Identifikace, hodnocení a evidence podpůrných aktiv

1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta,

2. určení vazeb mezi primárními a podpůrnými aktivy.

c) Pravidla ochrany jednotlivých úrovní aktiv

1. způsoby rozlišování jednotlivých úrovní aktiv,

2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,

3. přípustné způsoby používání aktiv.

d) Způsoby spolehlivého smazání nebo ničení technických nosičů dat.

(5) Politika bezpečnosti lidských zdrojů**

[§ 5 odst. 1 písm. e), § 5 odst. 2 písm. e)]

a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

1. způsoby a formy poučení uživatelů,

2. způsoby a formy poučení garantů aktiv,

3. způsoby a formy poučení administrátorů,

4. způsoby a formy poučení dalších osob zastávajících bezpečnostní role.

b) Bezpečnostní školení nových zaměstnanců.

c) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.

d) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.

1. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,

2. změna přístupových oprávnění při změně pracovní pozice.

(6) Politika řízení provozu a komunikací**

[§ 5 odst. 1 písm. f), § 5 odst. 2 písm. f)]

a) Pravomoci a odpovědnosti spojené s bezpečným provozem.

b) Postupy bezpečného provozu.

c) Požadavky a standardy bezpečného provozu.

d) Řízení technických zranitelností.

e) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

(7) Politika řízení přístupu**

[§ 5 odst. 1 písm. g), § 5 odst. 2 písm. g)]

a) Princip minimálních oprávnění/potřeba znát (need to know).

b) Požadavky na řízení přístupu.

c) Životní cyklus řízení přístupu.

d) Řízení privilegovaných oprávnění.

e) Řízení přístupu pro mimořádné situace.

f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

(8) Politika bezpečného chování uživatelů*

[§ 5 odst. 1 písm. h), § 5 odst. 2 písm. h)]

a) Pravidla pro bezpečné nakládání s aktivy.

b) Bezpečné použití přístupového hesla.

c) Bezpečné použití elektronické pošty a přístupu na internet.

d) Bezpečný vzdálený přístup.

e) Bezpečné chování na sociálních sítích.

f) Bezpečnost ve vztahu k mobilním zařízením.

(9) Politika zálohování a obnovy**

[§ 5 odst. 1 písm. i), § 5 odst. 2 písm. i)]

a) Požadavky na zálohování a obnovu.

b) Pravidla a postupy zálohování.

c) Pravidla bezpečného uložení záloh.

d) Pravidla a postupy obnovy.

e) Pravidla a postupy testování zálohování a obnovy.

(10) Politika bezpečného předávání a výměny informací**

[§ 5 odst. 1 písm. j)]

a) Pravidla a postupy pro ochranu předávaných informací.

b) Způsoby ochrany elektronické výměny informací.

c) Pravidla pro využívání kryptografické ochrany.

(11) Politika řízení technických zranitelností**

[§ 5 odst. 1 písm. k)]

a) Pravidla pro omezení instalace programového vybavení,

b) Pravidla a postupy vyhledávání opravných programových balíčků,

c) Pravidla a postupy testování oprav programového vybavení,

d) Pravidla a postupy nasazení oprav programového vybavení.

(12) Politika bezpečného používání mobilních zařízení*

[§ 5 odst. 1 písm. l)]

a) Pravidla a postupy pro bezpečné používání mobilních zařízení.

b) Pravidla a postupy pro zajištění bezpečnosti zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.

(13) Politika poskytování a nabývání licencí programového vybavení a informací*

[§ 5 odst. 1 písm. m), § 5 odst. 2 písm. j)]

a) Pravidla a postupy nasazení programového vybavení a jeho evidence.

b) Pravidla a postupy pro kontrolu dodržování licenčních podmínek.

(14) Politika dlouhodobého ukládání a archivace informací*

[§ 5 odst. 1 písm. n)]

a) Pravidla a postupy archivace dokumentů a záznamů.

b) Ochrana archivovaných dokumentů a záznamů.

c) Politika přístupu k archivovaným dokumentům a záznamům.

(15) Politika ochrany osobních údajů*

[§ 5 odst. 1 písm. o), § 5 odst. 2 písm. k)]

a) Charakteristika zpracovávaných osobních údajů.

b) Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů.

c) Popis přijatých a provedených technických opatření pro ochranu osobních údajů.

(16) Politika fyzické bezpečnosti**

[§ 5 odst. 1 písm. p)]

a) Pravidla pro ochranu objektů.

b) Pravidla pro kontrolu vstupu osob.

c) Pravidla pro ochranu zařízení.

d) Detekce narušení fyzické bezpečnosti.

(17) Politika bezpečnosti komunikační sítě**

[§ 5 odst. 1 písm. q)]

a) Pravidla a postupy pro zajištění bezpečnosti sítě.

b) Určení práv a povinností za bezpečný provoz sítě.

c) Pravidla a postupy pro řízení přístupů v rámci sítě.

d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti.

e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.

(18) Politika ochrany před škodlivým kódem*

[§ 5 odst. 1 písm. r), § 5 odst. 2 písm. m)]

a) Pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí.

b) Pravidla a postupy pro ochranu serverů a sdílených datových uložišť.

c) Pravidla a postupy pro ochranu pracovních stanic.

(19) Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí**

[§ 5 odst. 1 písm. s), § 5 odst. 2 písm. n)]

a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí.

b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události.

c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

(20) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí**

[§ 5 odst. 1 písm. t)]

a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí.

b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.

c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

(21) Politika bezpečného používání kryptografické ochrany**

[§ 5 odst. 1 písm. u), § 5 odst. 2 písm. l)]

a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.

b) Pravidla kryptografické ochrany informací

1. při přenosu po komunikačních sítích,

2. při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat,

c) Systém správy klíčů.

II. **Struktura další dokumentace**

(1) Zpráva z auditu kybernetické bezpečnosti**

[§ 28 odst. 1 písm. b)]

a) Cíle auditu kybernetické bezpečnosti.

b) Předmět auditu kybernetické bezpečnosti.

c) Kritéria auditu kybernetické bezpečnosti.

d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily.

e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti.

f) Zjištění z auditu kybernetické bezpečnosti.

g) Závěry auditu kybernetické bezpečnosti.

(2) Zpráva z přezkoumání systému řízení bezpečnosti informací**

[§ 28 odst. 1 písm. c)]

a) Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací,

b) Identifikace změn a okolností, které mohou mít vliv na systém řízení bezpečnosti informací.

c) Zpětná vazba o výkonnosti řízení bezpečnosti informací

1. neshody a nápravná opatření,

2. výsledky monitorování a měření,

3. výsledky auditu,

4. naplnění cílů bezpečnosti,

d) Výsledky hodnocení rizik a stav plánu zvládání rizik.

e) Identifikace možností pro neustálé zlepšování.

d) Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.

(3) Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik*

[§ 28 odst. 1 písm. d), § 28 odst. 2 písm. b)]

a) Určení stupnice pro hodnocení primárních aktiv

1. určení stupnice pro hodnocení úrovní důvěrnosti aktiv,

2. určení stupnice pro hodnocení úrovní integrity aktiv,

3. určení stupnice pro hodnocení úrovní dostupnosti aktiv.

b) Určení stupnice pro hodnocení rizik

1. určení stupnice pro hodnocení úrovní dopadu,

2. určení stupnice pro hodnocení úrovní hrozby,

3. určení stupnice pro hodnocení úrovní zranitelnosti,

4. určení stupnice pro hodnocení úrovní rizik,

a) Metody a přístupy pro zvládání rizik.

b) Způsoby schvalování přijatelných rizik.

(4) Zpráva o hodnocení aktiv a rizik**

[§ 28 odst. 1 písm. e), § 28 odst. 2 písm. c)]

a) Přehled primárních aktiv

1. identifikace a popis primárních aktiv,

2. určení garantů primárních aktiv,

3. hodnocení primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.

b) Přehled podpůrných aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona)

1. identifikace a popis podpůrných aktiv,

2. určení garantů podpůrných aktiv,

3. určení vazeb mezi primárními a podpůrnými aktivy,

c) Identifikování a hodnocení rizik

1. posouzení možných dopadů na aktiva,

2. hodnocení existujících hrozeb,

3. hodnocení existujících zranitelností, hodnocení existujících opatření,

4. stanovení úrovně rizika, porovnání této úrovně s kritérii pro přijatelnost rizik,

5. určení a schválení přijatelných rizik.

d) Zvládání rizik

1. návrh způsobu zvládání rizik,

2. návrh opatření a jejich realizace.

(5) Prohlášení o aplikovatelnosti*

[§ 28 odst. 1 písm. f), § 28 odst. 2 písm. d)]

a) Přehled vybraných bezpečnostních opatření včetně zdůvodnění jejich výběru a jejich vazby na identifikovaná rizika.

b) Přehled zavedených bezpečnostních opatření.

(6) Plán zvládání rizik**

[§ 28 odst. 1 písm. g), § 28 odst. 2 písm. e)]

a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik.

b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.

c) Osoby zajišťující jednotlivá bezpečnostní opatření pro zvládání rizik.

d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

e) Způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

(7) Plán rozvoje bezpečnostního povědomí*

[§ 28 odst. 1 písm. h), § 28 odst. 2 písm. f)]

a) Obsah a termíny poučení uživatelů.

b) Obsah a termíny poučení garantů aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).

c) Obsah a termíny poučení administrátorů (neplatí pro orgány a osoby uvedené v § 3 písm. c) a d) zákona).

d) Obsah a termíny poučení dalších osob zastávajících bezpečnostní role.

e) Obsah a termíny poučení nových zaměstnanců.

f) Formy a způsoby hodnocení plánu.

(8) Zvládání kybernetických bezpečnostních incidentů**

[§ 28 odst. 1 písm. i), § 28 odst. 2 písm. g)]

a) Definování kategorií kybernetického bezpečnostního incidentu.

b) Pravidla a postupy pro evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.

c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.

d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.

(9) Strategie řízení kontinuity činností**

[§ 28 odst. 1 písm. j), § 28 odst. 2 písm. h)]

a) Práva a povinnosti zúčastněných osob.

b) Cíle řízení kontinuity činností

1. minimální úroveň poskytovaných služeb,

2. doba obnovení chodu,

3. bod obnovení chodu.

c) Strategie řízení kontinuity činností pro naplnění cílů kontinuity.

d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.

e) Určení a obsah potřebných plánů kontinuity.

f) Postupy pro realizaci opatření vydaných Národním bezpečnostním úřadem.

(10) Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků*

[§ 28 odst. 1 písm. k), § 28 odst. 2 písm. i)]

a) Přehled obecně závazných právních předpisů.

b) Přehled vnitřních předpisů a jiných předpisů.

c) Přehled smluvních závazků.

Poznámka:

* Očekávaná důvěrnost dokumentu je na úrovni střední podle stupnice uvedené v příloze č. 1: Hodnocení a úroveň aktiv.

** Očekávaná důvěrnost dokumentu je na úrovni vysoká podle stupnice uvedené v příloze č. 1: Hodnocení a úroveň aktiv.

Příloha 5

Formulář hlášení kybernetického bezpečnostního incidentu

HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU	
MÍRA OCHRANY INFORMACE	
Úroveň ochrany	
	Osobní — seznam příjemců Omezená distribuce Neomezeno
KONTAKTNÍ ÚDAJE	
Orgán a osoba uvedená v § 3 písm. c) až e) zákona	
Email	
Telefon	
DETAILY INCIDENTU	
Datum a čas zjištění	
Časová zóna	
Kategorie incidentu	Kategorie III — velmi závažný kybernetický bezpečnostní incident Kategorie II — závažný kybernetický bezpečnostní incident Kategorie I — méně závažný kybernetický bezpečnostní incident

Typ incidentu	Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb. Kybernetický bezpečnostní incident způsobený škodlivým kódem. Kybernetický bezpečnostní incident způsobený překonáním technických opatření. Kybernetický bezpečnostní incident způsobený porušením organizačních opatření. Kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb. Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. Kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení dostupnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených shora.
Současný stav zvládání kybernetického bezpečnostního incidentu	Probíhá analýza a šetření kybernetického incidentu Kybernetický bezpečnostní incident je pod kontrolou Dotčené funkce obnoveny Neznámý
Počet zasažených systémů (odhad)	
Odhad počtu dotčených uživatelů	
Popis incidentu	
SYSTÉMOVÉ DETAILY	
Host nebo IP	
Funkce hosta (DNS server, stanice atd.)	
Pokračování	Iniciační oznámení CERTu Pokračování dříve oznámených

Příloha 6

Formulář oznámení o provedení reaktivního opatření a jeho výsledku

Část A: Údaje o orgánu a osobě uvedené v 3 písm. c) až e) zákona	
Název	
Adresa sídla	
Identifikační číslo osoby	
Část B: Údaje o fyzické osobě, která provádí hlášení	
Jméno, případně jména, příjmení a tituly	
Telefon	
Adresa elektronické pošty	
Část C: Číslo jednací reaktivního opatření	
Část D: Podrobnosti o realizaci reaktivního opatření	
Hodnocené negativní dopady reaktivního opatření a jejich možné negativní účinky	
Popis postupu možných negativních dopadů reaktivního opatření	
Problémy a negativní dopady, které se objevily během provedení reaktivního opatření	
Výsledek reaktivního opatření	
Datum a čas realizace reaktivního opatření	DD.MM.RRRR HH:MM
Datum a čas hodnocení výsledků reaktivního opatření	DD.MM.RRRR HH:MM
Poznámky	

Příloha 7

Formulář pro hlášení kontaktních údajů

Část A: Údaje o orgánu a osobě uvedené v § 3 zákona	
Název včetně odlišujícího dodatku nebo dalšího označení	
Adresa sídla	
Identifikační číslo osoby	
Část B: Identifikace informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému	
Typ informačního nebo komunikačního systému podle Š 2b) a 2d) zákona (KII / VIS)	
Základní popis systému:	
Část C: Údaje o fyzické osobě, která je za orgán nebo osobu uvedenou v 3 zákona oprávněna jednat ve věcech upravených zákonem	
Jméno, případně jména, příjmení	
Telefon — pevná linka	
Mobilní telefon	
Adresa elektronické pošty	

---

1) ISO/IEC 27001:2013, případně ČSN ISO/IEC 27001:2014