MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD

podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Verze 1.0, platná ke dni 17. července 2020

Obsah

1 Úvod

Tento dokument nabízí zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro organizace, které nespadají pod regulaci zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“). Je vhodný především tam, kde s nastavováním zabezpečení teprve začínají, protože ke kybernetické bezpečnosti přistupuje návodným doporučením. Pro přehlednost je dokument členěn na dvě části. První část je zaměřena manažersky, oblasti popisované v této části jsou zaměřeny procesně, zpravidla zahrnují popisy postupů, které je potřeba v rámci organizace zavést a dodržovat. Druhá část dokumentu je zaměřena technicky, je určena spíše pro IT specialisty, obsahuje konkrétní návody, jak zajistit minimální úroveň zabezpečení.

1.1 Další zdroje z oblasti kybernetické bezpečnosti

V případě potřeby zavedení komplexního systému řízení bezpečnosti informací, anebo jako zdroj inspirace lze využít vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“).

Webové stránky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) mohou rovněž sloužit jako zdroj informací o problematice kybernetické bezpečnosti. Lze je nalézt pod tímto odkazem: https://www.nukib.cz/.

NÚKIB dle potřeby vydává podpůrné materiály, které jsou primárně zaměřeny na potřeby povinných osob, ale lze z nich vycházet v rámci řešení jednotlivých oblastí kybernetické bezpečnosti. Tyto materiály jsou dostupné zde: https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/. Dalším zdrojem jsou také informace o aktuálních hrozbách, které lze nalézt zde: https://www.govcert.cz/cs/informacni-servis/hrozby/ nebo doporučení, která se nachází zde: https://www.govcert.cz/cs/informacni-servis/doporuceni/.

1.2 Kontakt

V případě dotazů se prosím obracejte na sekretariát odboru regulace NÚKIB:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

MANAŽERSKÁ ČÁST

2 Základní předpoklady

Cíl opatření: Stanovení systematického přístupu vedoucího ke zvyšování kybernetické bezpečnosti, včetně požadavků na vrcholové vedení v oblasti organizační bezpečnosti a určení odpovědností v oblasti kybernetické bezpečnosti.

Doporučení: Základním předpokladem systematického přístupu ke kybernetické bezpečnosti je podpora ze strany vrcholového vedení při jejím prosazování. Je potřeba vyčlenit potřebné zdroje, stanovit bezpečnostní role, vytvořit přiměřené bezpečnostní politiky a dokumentaci, včetně jejich schválení a následně kontrolovat jejich dodržování.

Vrcholové vedení musí projevit dostatečnou podporu a přidělit přiměřené zdroje (finanční, lidské, technické) potřebné k zavedení a udržování principů vedoucích ke zvyšování kybernetické bezpečnosti a určit osobu odpovědnou za kybernetickou bezpečnost, včetně stanovení jejích povinností, odpovědností a pravomocí. Tato role je odpovědná za řízení a rozvoj kybernetické bezpečnosti, průběžnou kontrolu stavu kybernetické bezpečnosti, dohlížení na naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti s vrcholovým vedením.

V organizaci můžou být určeny i další bezpečnostní role. Jako pomůcka pro inspiraci při stanovování bezpečnostních rolí může sloužit podpůrný materiál zveřejněný na webových stránkách NÚKIB. Přestože tento materiál je primárně určen pro určování bezpečnostních rolí u povinných osob dle zákona o kybernetické bezpečnosti, lze se jím přiměřeně inspirovat.

Materiál je dostupný zde:
https://www.govcert.cz/download/kii-vis/VKB/bezpe%C4%8Dnostn%C3%AD-role_v3.pdf.

Poznámka: *Je vhodné zajistit dostatečnou zastupitelnost bezpečnostních rolí, ale není nutné vytvářet speciální pozice pro osoby zastupující bezpečnostní role. Je důležité, aby příslušné činnosti byly řádně vykonávány i v případě, že odpovědná osoba nebude v daný okamžik k dispozici, anebo bude mít v náplni práce i další činnosti.*

Administrátoři a osoby zastávající bezpečnostní role by měli mít uzavřenou dohodu o zachování mlčenlivosti buď přímo ve formě smlouvy (NDA) nebo doložky k pracovní smlouvě.

Dále je potřeba vytvořit přiměřené bezpečnostní politiky a bezpečnostní dokumentaci. Tyto politiky a dokumenty musí být dostatečně návodné, aby bylo zajištěno, že výsledky budou reprodukovatelné – tzn., aby jiná osoba byla po jejich nastudování schopna postupovat shodným způsobem. Seznam oblastí, jež by měly bezpečnostní politiky a dokumentace zahrnovat, je uveden v příloze tohoto dokumentu. Při výběru vhodných politik a dokumentace je vždy nutné zohlednit jejich relevanci pro konkrétní prostřední organizace. Bezpečnostní politiky a dokumentace musí být schváleny na stejné úrovni jako jiné interní akty organizace (tedy nejčastěji vrcholovým vedením), a to mimo jiné i z toho důvodu, aby byla zajištěna jejich vymahatelnost.

Politiky a dokumentace by měly být v přiměřených intervalech aktualizovány tak, aby vždy reflektovaly aktuální stav.

Všechny činnosti spojené se zajišťováním kybernetické bezpečnosti by měly být v souladu se zákony a interními předpisy organizace.

Mezi bezpečnostní dokumentaci patří mimo jiné i plán zavádění bezpečnostních opatření, který je stěžejním dokumentem sloužícím k plánování zavádění bezpečnostních opatření a tedy i k zajištění kontinuálního zlepšování.

2.1 Plán zavádění bezpečnostních opatření

Využití: Přehledový dokument, který slouží jako seznam bezpečnostních opatření, která musí být zavedena, podklad pro plánování zdrojů a harmonogram pro zavádění bezpečnostních opatření.

Doporučení: Vytvořit plán zavádění bezpečnostních opatření obsahující popis bezpečnostních opatření, osoby odpovědné za zavedení jednotlivých bezpečnostních opatření, potřebné zdroje a termíny. Pravidelně plán zavádění bezpečnostních opatření aktualizovat, zohledňovat kybernetické bezpečnostní incidenty, zohledňovat aktuální dění v oblasti kybernetické bezpečnosti (např. zohledňovat opatření podle § 11 zákona o kybernetické bezpečnosti vydávané NÚKIB, informace o hrozbách vydávané vládním CERT atd.), zohledňovat výsledky auditu kybernetické bezpečnosti apod.

Plán zavádění bezpečnostních opatření by měl obsahovat všechna bezpečnostní opatření popsaná v tomto dokumentu, v případě, že je lze aplikovat.

3 Klasifikace a ochrana informací

Cíl opatření: Stanovení hodnoty informací za účelem jejich adekvátní ochrany. Tím, že dochází k jejich třídění podle hodnoty a následné ochraně dle důležitosti, může docházet ke snižování nákladů, protože není nutné chránit všechny informace na stejné úrovni.

Doporučení: Vytvořit metodiku pro identifikaci a hodnocení informací. Provést identifikaci a hodnocení informací dle důležitosti (hodnocení z pohledu důvěrnosti, integrity a dostupnosti) v souladu s metodikou. Zařadit informace do výsledných úrovní. Vytvořit a zavést pravidla pro ochranu informací dle jednotlivých úrovní. Určit odpovědné osoby za vykonání výše uvedených činností.

Jako pomůcka k hodnocení informací může sloužit například následující tabulka:

Tabulka č. 1 Úroveň hodnocení informací

Úroveň	Důvěrnost	Integrita	Dostupnost
1	Informace jsou veřejně přístupné nebo byly určené ke zveřejnění. Narušení důvěrnosti neohrožuje oprávněné zájmy organizace.	Narušení integrity neohrožuje oprávněné zájmy organizace.	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu.
2	Informace nejsou veřejně přístupné a tvoří know-how organizace.	Narušení integrity informace může vést k poškození oprávněných zájmů organizace.	Narušení dostupnosti by nemělo překročit dobu několika hodin. Výpadek je nutné řešit bez zbytečného odkladu, protože vede k ohrožení oprávněných zájmů organizace.
3	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie.	Narušení integrity vede k poškození oprávněných zájmů organizace.	Narušení dostupnosti není přípustné a i krátkodobá nedostupnost vede k vážnému ohrožení oprávněných zájmů organizace.

Následně je nutné vybrat **nejvyšší hodnotu,** čímž dojde k zařazení informace do výsledné úrovně, podle které budou aplikována pravidla pro ochranu informací.

Hodnocení by měla provádět osoba, která má detailní znalosti týkající se dané informace, je schopna kvalifikovaně ohodnotit její důležitost a je za informaci odpovědná. Tuto osobu lze nazývat garant informace.

Dále by měly být stanoveny osoby odpovědné za jednotlivé technické prostředky používané pro práci s informacemi.

Pro ochranu informací lze využít například následující pravidla:

Tabulka č. 2 Výsledné úrovně hodnocení informací

Úroveň		Označení	Manipulace	Likvidace	Změny	Zálohování
1	Minimum	Dokument má na všech stranách v záhlaví označení VEŘEJNÉ	Bez omezení	Bez omezení	Evidence verzí	Zálohování podle individuální potřeby
2	Standard	Dokument má na všech stranách v záhlaví označení INTERNÍ	Pro interní potřebu, doporučujeme omezit přístup k informacím osobám, které je nepotřebují k výkonu práce, doporučujeme využívat šifrování (pokud lze)	Přepis nosiče informací, anebo jeho fyzická likvidace	Evidence verzí, omezení práv na změnu	Pravidelné zálohování podle individuální potřeby, pravidelná kontrola záloh
3	Nadstandard	Dokument má na všech stranách v záhlaví označení CITLIVÉ	Dodržování principu need-to-know, přístupné pouze pro přísně vyhrazené skupiny uživatelů, vyžadováno šifrování, šíření nutno nechat schválit garantem informace	Zajištění trvalého znehodnocení informace bez možnosti obnovy dle typu nosiče, případně fyzická likvidace nosiče	Evidence verzí, omezení práv na změnu, auditní záznamy o změnách	Pravidelné zálohování podle individuální potřeby, pravidelná kontrola záloh

4 Řízení dodavatelů

Cíl opatření: Předejití nejčastějších problémů vznikajících při využívání externích služeb, např. vendor lock-in, nedostatečná ochrana poskytnutých informací, nedostatečná bezpečnostní opatření při správě systému/ů atd.

Doporučení: V případě zajištění osoby provádějící audit či osoby odpovědné za kybernetickou bezpečnost externími dodavateli se nedoporučuje uzavírat smlouvy na tyto 2 role se stejnými dodavateli či s dodavateli zajišťujícími provozní a servisní činnosti interních informačních nebo komunikačních systémů v organizaci.

Při uzavírání smlouvy s dodavatelem s ohledem na jeho důležitost zvážit, které z následujících oblastí jsou **relevantní** a ty zohlednit ve smlouvě:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),

b) ustanovení o oprávnění užívat data,

c) ustanovení o autorství programového kódu, popřípadě o programových licencích,

d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),

e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,

f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,

g) ustanovení o řízení změn,

h) ustanovení o souladu smluv s obecně závaznými právními předpisy,

i) ustanovení o povinnosti dodavatele informovat povinnou osobu o

   1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
   2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
   3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,

j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),

k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),

l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,

m) pravidla pro likvidaci dat,

n) ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a

o) ustanovení o sankcích za porušení povinností.[1]

K této problematice je na webových stránkách NÚKIB dostupný podpůrný materiál: https://www.govcert.cz/download/kii-vis/VKB/Vyklad_pozadavku_na_smlouvy_s_dodavateli_v1.1.pdf.

V rámci řízení dodavatelských vztahů je vhodné prokazatelně seznamovat konkrétní osoby dodavatele s bezpečnostními politikami a pravidly a následně kontrolovat jejich dodržování.

[1] Jedná se o obsah přílohy č. 7 vyhlášky o kybernetické bezpečnosti.

5 Řízení lidských zdrojů

Cíl opatření: Zvyšování bezpečnostního povědomí v oblasti kybernetické bezpečnosti u všech zaměstnanců, stanovení pravidelných i jednorázových školení, zajištění seznámení dodavatelů s bezpečnostními politikami.

Doporučení: Poučit uživatele, administrátory a osoby zastávající bezpečnostní role o jejich povinnostech, teoreticky i prakticky je školit, s platnými bezpečnostními politikami seznámit nejen tyto uživatele, ale i relevantní osoby dodavatele a kontrolovat jejich dodržování.

Pro všechny zaměstnance by měla být stanovena pravidelná školení týkající se základů kybernetické bezpečnosti a to minimálně 1× ročně.

Všichni zaměstnanci musí být seznámeni s bezpečnostními politikami a je potřeba kontrolovat jejich dodržování. Pro řešení případů porušení stanovených bezpečnostních pravidel je vhodné mít nastavena přesná pravidla a postupy.

Zaměstnanci by měli být také proškoleni, jak se chovat v případě neobvyklého či podezřelého chování informačního nebo komunikačního systému, doručení nevyžádaného e-mailu, problémů s dostupností informací či služby nebo při jiné nestandardní situaci. Současně by měli být seznámeni se způsobem, jak tyto neobvyklé situace hlásit.

Dále je vhodné mít nadefinován soubor školení pro nové zaměstnance, která je nutné absolvovat při nástupu včetně specifických školení souvisejících s kybernetickou bezpečností určených pro konkrétní pracovní pozice. Pokud u zaměstnance dojde ke změně pracovního místa a vzniku potřeby proškolení na kybernetickou bezpečnost ve větším rozsahu, je nutné absolvovat odpovídající školení.

Zaměstnanci zastávající bezpečnostní role a zaměstnanci na IT pozicích by měli kromě standardních školení absolvovat i specializovaná a odborná školení související s výkonem jejich pozice, včetně školení zaměřených na kybernetickou bezpečnost. V příloze č. 6 vyhlášky o kybernetické bezpečnosti jsou uvedeny požadavky na jednotlivé bezpečnostní role a z tohoto výčtu se lze inspirovat při plánování odborných školení.

Při výskytu mimořádné události (např.: nová obecně známá hrozba, zvýšený výskyt phishingových e-mailů apod.) je vhodné zorganizovat mimořádné školení, případně zaměstnance informovat jiným vhodným způsobem.

V rámci zvyšování bezpečnostního povědomí vydává NÚKIB informační materiály, které jsou umístěny na stánkách https://www.nukib.cz/cs/vzdelavani/. Jedná se například o:

- Doporučení pro bezpečný pohyb v kybersvětě,
- Doporučení pro chování v případě spear-phishingu,
- Bezpečnostních doporučení pro administrátory a další [2].

[2] Pro zaměstnance státní správy je vytvořen online Kurz základů kybernetické bezpečnosti, pro manažery kybernetické bezpečnosti je sestaven podrobnější kurz zaměřený na vyhlášku o kybernetické bezpečnosti. Více informací k těmto kurzům je možné nalézt zde: https://www.institutpraha.cz/kurzy/kyberneticka-bezpecnost/

6 Řízení změn

Cíl opatření: Identifikování změn, které jsou podstatné z hlediska kybernetické bezpečnosti a mohou ji pozitivně nebo negativně ovlivnit. Nastavení postupů pro řízení změn tak, aby se minimalizovala možnost narušení správné funkčnosti daného informačního nebo komunikačního systému (případně bezpečnosti informací).

Doporučení: Při provozu informačního nebo komunikačního systému řešit problematiku řízení změn a konfigurací. Tato problematika zahrnuje evidenci všech změn, systematické vyhodnocování, koordinování a implementaci schválených změn a konfigurací.

V případě, že bude organizace provádět změnu, tak by měla zvážit možné dopady této změny. Změna, která by mohla mít nepříznivý dopad na informační nebo komunikační systém nebo bezpečnost informací, by měla být dokumentována.

Změny v rámci informačního nebo komunikačního systému by měly být řízeny prostřednictvím změnových požadavků, které jsou schvalovány osobou odpovědnou za kybernetickou bezpečnost.

Změny je potřeba řídit a řádně je dokumentovat.

Dále je potřeba:

- přijmout opatření za účelem snížení všech nepříznivých dopadů spojených se změnami,
- aktualizovat relevantní bezpečnostní politiky a bezpečnostní dokumentaci,
- zajistit testování změn a
- zajistit možnost navrácení do původního stavu.

V případě potřeby je vhodné provést penetrační testování.[3]

[3] Problematice penetračního testování se věnuje také kapitola 13.

7 Řízení kontinuity činností

Cíl opatření: Dostupnost aktuálních a použitelných plánů kontinuity (Business Continuity Plan – BCP), plánů obnovy (Disaster Recovery Plan – DRP) a havarijních plánů, aby v případě mimořádné situace (havárie, živelné pohromy nebo úspěšného kybernetického útoku) byla organizace schopna obnovit svoji funkčnost.

Doporučení: V případě, že BCP, DRP a havarijní plány chybí, je potřeba je vypracovat alespoň v takové míře, aby podle nich bylo možné opět zajistit správnou funkčnost informačních nebo komunikačních systémů. Plány by měly být vypracovány postupně s ohledem na důležitost informačních nebo komunikačních systémů.

V rámci řízení kontinuity by měly být řešeny tyto body:

- Práva a povinnosti administrátorů a osob podílejících se na zajištění chodu organizace. Kdo, kdy, a co má v průběhu mimořádné situace dělat. Např. eskalační postupy atd.
- Vyhodnocení a posouzení možných rizik souvisejících s ohrožením kontinuity činností. Je nutné sestavit možné elementární scénáře toho, co se může stát (nedostupnost budov, IT systémů, lidí, vznik epidemie apod.) a jaký bude dopad na důvěrnost, dostupnost a integritu dat v informačním nebo komunikačním systému a co to bude znamenat pro poskytování služeb.
- Stanovení cíle řízení kontinuity činností formou určení:
    - minimální úrovně užívání, provozu a správy informačního nebo komunikačního systému, která je akceptovatelná pro zachování poskytovaných služeb,
    - doby obnovení chodu (Recovery Time Objective – RTO), během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního nebo komunikačního systému, a
    - bodu obnovení dat (Recovery Point Objective – RPO) jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.
- Vytvoření postupů, které budou obsahovat naplnění cílů podle předchozího bodu. Tzn., jakým způsobem organizace dosáhne toho, aby udržela minimální akceptovatelnou úroveň služeb.
- Vytvoření postupů, havarijních plánů, DRP pro obnovu chodu informačního nebo komunikačního systému, na základě výše uvedených cílů.

BCP je vytvářen s ohledem na hrozící dopady do činností a nákladů na potřebná opatření.[4] Jedním ze základních parametrů dostupnosti je tzv. RTO, jenž vyjadřuje množství času potřebné pro obnovení dat a celého provozu nedostupného informačního nebo komunikačního systému. Dalším ukazatelem dostupnosti je tzv. RPO, který definuje, do jakého stavu (bodu) v minulosti lze obnovit data v informačním nebo komunikačním systému. Jinými slovy množství dat, o která lze přijít. BCP nemusí obsahovat pouze opatření týkající se samotného informačního nebo komunikačního systému, lze do něj zahrnout i jiné typy opatření, kterými zajistí organizace své fungování např. zasmluvnění potřebných služeb v období krize.

[4] K tomuto účelu lze využít metodiku BIA (Business Impact Analysis).

Samotná obnova informačního nebo komunikačního systému se provádí dle DRP. DRP vychází z požadavků stanovených BCP a obsahuje konkrétní posloupnosti a činnosti nutné pro obnovení chodu informačního nebo komunikačního systému.

Vzorový příklad BCP pro jeden scénář je uveden v příloze tohoto dokumentu.

8 Audit kybernetické bezpečnosti

Cíl opatření: Pravidelné a nezávislé zhodnocení stavu kybernetické bezpečnosti v organizaci.

Doporučení: Pro zhodnocení stavu kybernetické bezpečnosti je vhodné v pravidelných intervalech[5] provádět nezávislý audit kybernetické bezpečnosti. Audit kybernetické bezpečnosti upozorní na nalezené rozdíly, případné nedostatky a potenciální oblasti ke zlepšení.

Audit kybernetické bezpečnosti je především zodpovědností vrcholového vedení, které musí být iniciátorem procesu zlepšování.

Posuzuje soulad s:

- bezpečnostní dokumentací a bezpečnostními politikami organizace,
- právními předpisy,
- jinými předpisy a smluvní závazky, které se vztahují k informačnímu nebo komunikačnímu systému a
- nejlepší praxí.

Audit kybernetické bezpečnosti by měl být prováděn pravidelně. Je doporučeno jej provádět:

- při změnách, které mohou mít negativní dopad na kybernetickou bezpečnost a
- v pravidelných intervalech dle uvážení organizace.

Pokud nastane kybernetický bezpečnostní incident se závažným dopadem na informační nebo komunikační systém, měla by organizace provést mimořádný audit.

Výsledky těchto auditů je možné použít pro průběžné vyhodnocování bezpečnosti informací, a pro plánování zlepšování. Audit je možné provádět vlastními zdroji nebo s využitím třetí strany.

Osoba provádějící audit kybernetické bezpečnosti musí být pro tuto činnost vyškolena. Vhodná školení pro osobu zajišťující audit kybernetické bezpečnosti jsou uvedena v příloze č. 6 vyhlášky o kybernetické bezpečnosti. Je nutné, aby osoba provádějící audit kybernetické bezpečnosti byla oddělena od provozních nebo bezpečnostních rolí a byla tak zajištěna její nezávislost.

Pokud se vrcholové vedení rozhodne pověřit externí osobu prováděním auditu kybernetické bezpečnosti, tak je potřeba určit osobu v organizaci, která bude dohlížet na průběh tohoto auditu.

Výsledky auditu kybernetické bezpečnosti se následně předkládají relevantním členům vrcholového vedení a také se promítnou do plánu zavádění bezpečnostních opatření a bezpečnostní dokumentace.

[5] Vyhláška o kybernetické bezpečnosti požaduje provedení auditu kybernetické bezpečnosti u povinných osob alespoň po 3, resp. 2 letech

TECHNICKÁ ČÁST

9 Fyzická bezpečnost

Cíl opatření: Stanovení základních požadavků a principů pro zajištění bezpečnosti informací z pohledu fyzické bezpečnosti.

Doporučení: Definovat nový či rozšířit stávající soubor opatření předcházející poškození, krádeži či zneužití informací či majetku nebo přerušení poskytování služeb informačního nebo komunikačního systému, vymezit fyzický perimetr.

Fyzický bezpečnostní perimetr je oblast, ve které jsou uchovávány a zpracovávány informace a umístěny technické prostředky. Tuto oblast je nutné chránit a zabezpečit před neoprávněným vstupem a poškozením, krádeží či zneužitím. V rámci zajištění fyzické bezpečnosti je potřeba zajistit ochranu hlavně kritických míst v rámci objektů (např. serverovny, kanceláře zaměstnanců, technologické místnosti), ale také objektů samotných. Měla by být jasně definována pravidla pro návštěvy, jako je např.: vstup pouze s doprovodem, identifikace návštěvy při vstupu do objektu apod.

Příklady zajištění fyzické bezpečnosti:

- monitorování celého prostoru kamerovým systémem,
- bezpečnostní agentura zajišťující dozor,
- vstup a pohyb v rámci objektu pouze po předchozí identifikaci (např. pomocí čipové karty, resp. možnost nastavení různých oblastí, do kterých mají přístup pouze omezené skupiny zaměstnanců),
- zamykání dveří a prostor atd.

Z pohledu fyzického zabezpečení je dále vhodné mít stanovené požadavky na:

- infrastrukturu a to zejména – nezávislý zdroj napájení (alespoň UPS), přesnou klimatizaci prostor, ve kterých je informační nebo komunikační systém nebo jeho komponenty umístěny, datové rozvody dle technických norem, zajištění bezpečnosti kabelových rozvodů.

10 Řízení přístupů

Cíl opatření: Řízení přístupů na základě rolí a evidence přidělování nebo odebírání přístupových oprávnění. Specifikace parametrů pro hesla a využívání vícefaktorové autentizace.

Doporučení: Přidělit jedinečné identifikátory jednotlivým uživatelům a administrátorům přistupujících k informačnímu nebo komunikačnímu systému. Řídit a evidovat identifikátory, přístupová práva a oprávnění aplikací a technických účtů. Provádět řízení přístupu na základě skupin a rolí.

Pojem „Bring Your Own Device“ (BYOD) znamená využívání soukromých zařízení zaměstnanců, která jsou přinášena, užívána a připojena na pracovišti do počítačové sítě organizace, jako například chytré telefony, laptopy nebo tablety. Pro spravování firemních i osobních zařízení se využívá nástroje „Mobile Device Management“ (MDM), který může obsahovat například tyto funkcionality:

- konfiguraci mobilních zařízení,
- zálohu dat,
- obnovu dat,
- distribuci aktualizací operačního systému a aplikací,
- monitoring zařízení apod.

V rámci politiky řízení přístupu se musí definovat pravidla a postupy potřebné pro omezení a kontrolu používaného softwaru a hardwaru, který by mohl narušit systémovou a aplikační bezpečnost. Jedná se např. o kontrolu připojovaných USB, antivir apod.

Privilegované účty mají přiděleny samostatné přihlašovací údaje. Jednotliví administrátoři musí mít vedle privilegovaného účtu i účet běžného uživatele pro činnosti, které nevyžadují privilegovaná oprávnění.

Servisní nebo technické účty, pod kterými běží informační nebo komunikační systém nebo jeho jednotlivé komponenty, nebo prostřednictvím kterých informační nebo komunikační systém přistupuje k ostatním komponentám nebo externím informačním nebo komunikačním systémům, musí být uvedeny v dokumentaci k informačnímu nebo komunikačnímu systému. U každého účtu musí být uveden jeho účel a způsob jakým je možné účtu změnit heslo či obnovit certifikát, včetně identifikace všech míst, kde je takové heslo či certifikát bezpečně uložen/o.

Pro všechny typy účtů musí být uplatněn princip need-to-know. To znamená, že každý účet má nastavena pouze taková oprávnění, která jsou nezbytná pro provádění činností odpovídajících pracovní pozici a náplni práce uživatele. Vedení organizace by nemělo být výjimkou a mělo by využívat běžné uživatelské účty.

Přístupová oprávnění se musí pravidelně přezkoumávat a případně upravit právě podle výše zmíněného principu. Pro přidělování a odebírání přístupových oprávnění je vhodné stanovit odpovědnou osobu a tuto činnost je potřeba sladit s bezpečnostními politikami. Odpovědná osoba zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně pracovního vztahu.

Přidělování a odebírání přístupových práv je dokumentováno.

Způsob autorizace musí být zdokumentován v rámci provozně/bezpečnostní dokumentace k informačnímu nebo komunikačnímu systému. Pro informační nebo komunikační systém musí být definovány samostatné uživatelské role, které se dále člení dle aplikačních požadavků. Informační nebo komunikační systém musí zajišťovat tzv. AAA (Autentizaci, Autorizaci, Audit) v potřebné úrovni dle jeho konkrétní specifikace.

10.1 Registrace, autentizace a identifikace uživatelů

Informační nebo komunikační systém musí zajišťovat:

- registraci všech uživatelů centrálně,
- stanovit pravidla pro procesy:
    - registrace,
    - schvalování,
    - generování identit,
    - přidělování a odebírání přístupů,
    - deaktivace identit,
    - monitorování činnosti uživatelů.

Informační nebo komunikační systém musí primárně využívat stávajících informačních nebo komunikačních systémů pro podporu identifikace a autentizace používaný v prostředí organizace – tedy musí umožňovat využívat stávající informační nebo komunikační systém pro Identity management. Pro informační nebo komunikační systém přístupný pro veřejnost doporučujeme využít Národní identitní autoritu (https://www.eidentita.cz/). V případě, že implementace takového řešení by byla značně neefektivní, lze tyto funkce implementovat přímo v informačním nebo komunikačním systému.

Jestliže existují v rámci informačního nebo komunikačního systému lokální účty, je nezbytné, aby se řídily následující politikou hesel pro privilegované účty, nebo je nutné umožnit integraci s informačním nebo komunikačním systémem pro správu privilegovaných účtů.

10.2 Politika hesel pro privilegované účty

- minimální délka hesla je 17 znaků,
- heslo musí obsahovat znaky alespoň ze tří následujících skupin: velká písmena, malá písmena, číslice a speciální znak.
- maximální doba platnosti hesla je 18 měsíců,
- zákaz používaní stejného hesla (posledních 12 hesel),
- minimální platnost hesla 1 den,
- zamčení účtu po 5 neplatných pokusech zadání hesla v řadě,
- jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách.

10.3 Politika hesel pro uživatelské účty

- minimální délka hesla je 10 znaků,
- zákaz používaní stejného hesla (posledních 12 hesel),
- maximální doba platnosti hesla je 18 měsíců,
- zamčení účtu po 10 neplatných pokusech zadání hesla v řadě,
- jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách.

Tato pravidla je nutné chápat jako minimální doporučení a jejich implementace může být přísnější.

V zabezpečení řízení přístupu se pro ověření identity uživatelů, administrátorů a aplikací doporučuje maximálně využívat vícefaktorové autentizace[6], kdy je zapotřebí dvou různých typů faktorů. Primárně by tento způsob autentizace měl být zaveden u informačních nebo komunikačních systémů přístupných z internetu a u privilegovaných účtů. Organizace je tak chráněna i v případě odcizení či úniku hesla jiným způsobem, přestože se používá stejné heslo napříč informačními nebo komunikačními systémy. V případě že je jedním z použitých faktorů heslo, nemusí splňovat požadavky na hesla dle politiky hesel pro privilegované a uživatelské účty.

Pokud není možné vícefaktorovou autentizaci použít nebo by její implementace byla finančně náročná, doporučujeme pro přístup využít asymetrické kryptografie (klíče, certifikáty).

[6] Vícefaktorová autentizace je zavedena v případě, že je toto řešení v informačním nebo komunikačním systému organizace možné nebo její zavedení nepředstavuje nepřiměřené náklady.

11 Požadavky v oblasti ochrany před škodlivým kódem

Cíl opatření: Snížení pravděpodobnosti napadení škodlivým kódem, případně snížení dopadů při napadení škodlivým kódem.

Doporučení: Segmentovat síť, instalovat příslušný software a pravidelně jej aktualizovat.

V rámci informačního nebo komunikačního systému musí být navržen a implementován způsob řešení ochrany před škodlivým kódem. Správce informačního nebo komunikačního systému (společně s případným dodavatelem/provozovatelem) musí zhodnotit všechny směry, vstupy/výstupy dat a jejich uložení či další zpracování v informačním nebo komunikačním systému a navrhnout způsob ochrany před škodlivým kódem.

V rámci informačního nebo komunikačního systému musí být zavedeny minimálně následující opatření na ochranu proti škodlivým kódům:

- segmentace síťového prostředí (oddělení sítí pro provoz a pro správu), kde je to opodstatněné;
- instalace software pro detekci a odstranění škodlivých programů na informačních nebo komunikačních systémech, kde je to technicky realizovatelné;
- pravidelná aktualizace software pro detekci a odstranění škodlivých kódů včetně databáze vzorků nejméně jednou denně.

V případě služeb kritických na dostupnost doporučujeme testovat aktualizace software pro detekci a odstranění škodlivých programů včetně aktualizace souborů se vzorky s cílem ověřit, že aktualizace neovlivní služby nežádoucím způsobem. Případně je možné u těchto služeb nastavit software pouze do detekčního režimu.

Instalovat, kopírovat, užívat nebo testovat jakékoli programové vybavení, které není schválenou součástí informačního nebo komunikačního systému, doporučujeme v provozním prostředí zakázat. Tedy doporučujeme neinstalovat a nepoužívat jakékoliv programové vybavení v provozním prostředí bez toho, aby bylo ověřeno, že se nejedná o programové vybavení obsahující škodlivý kód (např. otestováním v testovacím prostředí).

V prostředí informačního nebo komunikačního systému je zakázáno vzdálené spouštění kódu ze zdroje mimo jejich prostředí.

12 Kybernetické bezpečnostní události a incidenty

Cíl opatření: Stanovení postupů při vzniku nestandardní situace, včetně stanovení eskalačního procesu uvnitř organizace a auditních požadavků (logování).

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

V organizaci by měl být stanoven proces, dle kterého se bude řídit hlášení nestandardního chování informačního nebo komunikačního systému. Zaměstnanci by měli být seznámeni s tím, co mají hlásit (např. neobvyklé či podezřelé chování informačního nebo komunikačního systému, nevyžádané e-maily, problémy s dostupností informací či služeb atd.) a mít k dispozici konkrétní kontakty, na koho se v rámci organizace obracet.

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

Primárně se řešením bezpečnostních incidentů zabývá samotná organizace, také je ale možnost incidenty hlásit vládnímu CERT týmu (kontaktní údaje k dispozici na stránkách GovCERT.CZ). Tento tým může v případě volných kapacit poskytnout při řešení incidentu metodickou podporu a pomoc. Případně je možné incident nahlásit Národnímu CSIRT.CZ týmu, zejména pokud existuje předpoklad, že by incident mohl mít plošný či jinak zásadní charakter.

Poznámka: *Za incident je považováno nejen narušení integrity či důvěrnosti ale i nedostupnost informace či služby.*

Pokud se kybernetické bezpečnostní události nebo incidenty vyskytují často, je potřeba nalézt příčinu a pokud lze, pak zavést nápravná opatření, aby k nim nadále nedocházelo. Kybernetické bezpečnostní události a incidenty je vhodné evidovat a analyzovat, zejména pro potřeby vlastního poučení a eliminaci dalšího výskytu stejného incidentu. Kybernetické bezpečnostní události je vhodné evidovat také z toho důvodu, že je někdy potřeba dohledávat informace zpětně, protože samotný kybernetický bezpečnostní incident se může objevit dlouho poté, co byla identifikována první související kybernetická bezpečnostní událost.

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

Pro ex-post analýzu kybernetického bezpečnostního incidentu je nezbytné disponovat provozními záznamy z doby jeho výskytu. Zařízení, která záznamy generují je nespočet, jedná se obecně o **bezpečnostní nástroje** (antivirus, IDS/IPS, proxy, router, switch, firewall, …), **operační systémy** (autentizace, privilegované spuštění, systémové události, …) a **aplikace** (komunikace mezi klientem a serverem, uživatelské události, přístupy, …).

Zdroje logů lze rozdělit do několika kategorií:

- **Skupinou SEC** je myšleno bezpečnostní software a nástroje, jako antivirový/antimalware software, IPS a IDS systémy, VPN, proxy, vulnerability management software, firewally a routery, autentizační servery (např. RADIUS, Single Sign-on) apod.
- **Skupina OS** zahrnuje servery, pracovní stanice a síťové prvky (routery a switche). Jde převážně o dva typy logů:
    - systémové události (spuštění/zastavení služby, vypnutí/zapnutí stanice, selhání služeb, závažné chyby apod.),
    - události auditu (pokusy o ne/úspěšné přihlášení, přístupy k souborům, změny nastavení, využití oprávnění apod.).
- **Skupina APP** označuje logování chodu aplikací. Jde především o
    - komunikace klienta se serverem (C<>S) – klientské požadavky přijaté serverem a jejich odpovědi,
    - využití účtů – informace o přihlášení k aplikaci/službě (i neúspěšné pokusy), změny v účtech, změny oprávnění apod.,
    - údaje o aktivitě uživatelů (Aktivita) – např. počty transakcí a jejich objem,
    - významné provozní akce (Akce) jako spuštění nebo ukončení aplikace, pády aplikace nebo její významné změny.

Informační nebo komunikační systém musí uchovávat jak **provozní, tak bezpečnostní logy** po dobu dle následující tabulky.

Tabulka č. 3 Minimální počet dní uchování logů pro jednotlivé skupiny

SEC				
Počet dní	60			
OS	**Systém**	**Audit**		
Počet dní	30	30		
APP	**C<>S**	**Využití účtů**	**Aktivita**	**Akce**
Počet dní	7	7	1	30

Tabulka č. 4 Standard pro kategorie

Kategorie	Standard
Rotace logů	Každý týden nebo po dosažení max. 100 MB
Jak často zasílat do log managementu	Nejméně jednou za 24 hodin
Kontrola integrity (rotace)	Volitelná
Šifrování uložených záznamů	Volitelné
Šifrovaný přenos záznamů do log managementu v rámci vnitřní sítě	Volitelné
Šifrovaný přenos záznamů do log managementu skrz veřejnou síť	Povinné (např. v rámci VPN či TLS.)

Logy informačního nebo komunikačního systému musí být integrovatelné do centrálního řešení pro vyhodnocování provozních a bezpečnostních logů. Pokud takový informační nebo komunikační systém v organizaci není zaveden, doporučujeme při výběru nových technologií vyžadovat minimálně jednou z následujících metod pro zajištění kompatibility v případě zavedení centrálního log managementu:

- Syslog (RFC 5424),
- SNMPv3 TRAP,
- JDBC,
- Microsoft Event Log.

Informační nebo komunikační systém, včetně infrastruktury, která je jeho podpůrnou součástí, a jeho další komponenty, musí být připraveny na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring.

V rámci informačního nebo komunikačního systému musí být **pořizovány a uchovávány auditní záznamy** zejména takové, které jsou uvedeny ve výčtu níže, tak, aby byly využitelné pro monitorování řízení přístupu a případné budoucí vyšetřování bezpečnostních incidentů.

Zaznamenávání událostí zohledňuje technické možnosti informačního nebo komunikačního systému a pro sběr záznamů ukládá minimálně tyto typy událostí:

- přihlášení a odhlášení uživatelů a administrátorů a to včetně neúspěšných pokusů,
- činnosti provedené administrátory, o použití privilegovaných účtů, např. účtu supervisora, administrátora,
- spuštění a ukončení informačního nebo komunikačního systému,
- změny konfigurací,
- úspěšné i neúspěšné činnosti vedoucí ke změně přístupových oprávnění,
- zahájení a ukončení činností zařízení a aplikací,
- automatická varovná nebo chybová hlášení zařízení a aplikací,

- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

Jednotlivé položky logu informačního nebo komunikačního systému nebo jeho jednotlivé řádky záznamu musí obsahovat minimálně tyto pole:

- datum a čas události (uvedený s jednoznačnou identifikací časové zóny, např. UTC nebo lokální čas s uvedením offsetu),
- síťové identifikátory komunikujících bodů (tj. např. IP adresy a porty, v případě použití proxy nebo NATu musí být síťový identifikátor předán jinou formou nebo musí být možné tyto logy korelovat),
- identifikátor uživatele, pod kterým byla činnost provedena,
- typ události,
- úspěšnost nebo neúspěšnost činnosti.

V případě, že záznamy zapisované do logu informačního nebo komunikačního systému obsahují citlivé informace (heslo, soukromý klíč či jeho prekurzor, session ID apod.) musí být před zapsáním **přepsány pseudonáhodnou sekvencí**. V žádném případě nesmí dojít k zapsání citlivých informací v čistém textu.

V informačním nebo komunikačním systému musí být zavedena **ochrana proti deaktivaci, selhání či změnám** v pořizování auditních záznamů a **ochrana proti změnám nebo zničení auditních záznamů**.

Přístup k auditním záznamům musí být chráněn, aby bylo zabráněno jeho zneužití nebo ohrožení. Informační nebo komunikační systém musí umožnit nastavení přístupových práv k auditním záznamům tak, aby mohly být auditovány samostatnou rolí (auditor, security officer apod.).

Aby bylo možné korelovat logy z více zařízení informačního nebo komunikačního systému, musí být **systémový čas synchronizován** v rámci informačního nebo komunikačního systému alespoň jednou za 24 hodin (např. pomocí protokolu NTP).

13 Požadavky v oblasti aplikační bezpečnosti

Cíl opatření: Stanovení základních požadavků a principů pro oblast aplikační bezpečnosti a jejího testování.

Doporučení: Provádět testování v odděleném prostředí, stanovit pravidla pro testovací data.

Integrační, systémové, zátěžové a akceptační testy musí vždy probíhat ve vyhrazeném testovacím prostředí nebo módu, tak aby nemohla být narušena činnost produkčních systémů. Uvedené testy jsou prováděny s ohledem na rozsah, složitost informačního nebo komunikačního systému, charakter zpracovávaných dat a informací a na okolní vazby informačního nebo komunikačního systému.

Pro zvýšení bezpečnosti jsou doporučeny penetrační a bezpečnostní testy (testy zranitelností) probíhající i na produkčním prostředí, prováděné nezávislou organizací, tak aby byl zajištěn atribut nestrannosti. Toto testování, včetně konfiguračního review, doporučujeme provést po implementaci informačního nebo komunikačního systému a musí ověřit správnost nastavení celého prostředí.

Testovací údaje (data) musí být dostatečně chráněny a kontrolovány. Je-li to možné, musí být testování prováděno na neprovozních datech. Pokud je nezbytné využít k testování provozní data, upřednostní se použití již pozměněných dat. Při výběru provozních dat k testování z provozních databází je nutné použít maskování položek, které nejsou pro potřeby testování nezbytné.

Pokud je nutné použít platná provozní data, musí být dodrženy následující zásady:

- postupy kontroly přístupu platné pro provozní data musí být uplatněny i pro testovací data,
- každé kopírování provozních dat do testovacího prostředí musí být autorizováno souhlasem odpovědné osoby (například ve schváleném zápisu),
- neveřejné informace musí být okamžitě po ukončení testů odstraněny z testovaného prostředí bezpečným způsobem, aby nebyla možná jejich dodatečná obnova,
- kopírování a užití provozních dat musí být zaznamenáváno do auditních záznamů.

Pro zvýšení bezpečnosti je doporučeno u vyvíjených aplikací provést analýzu zdrojového kódu a otestovat zranitelnost. Součástí akceptace musí být prohlášení o provedení těchto testů a jejich výsledky. Dodavatel informačního nebo komunikačního systému poskytne prohlášení o provedení těchto testů, které bude obsahovat minimálně tyto položky:

- datum provedení testu,
- použitá testovací metodika a metodika scoringu,
- název nástroje použitého pro testování,
- konfigurace profilu pro testování,
- výsledky testování, navržení opatření,
- shrnutí výsledku testování a závěrečná zpráva,
- osobní odpovědnost – jména odpovědných osob.

14 Kryptografické prostředky

Cíl opatření: Ochrana dat a informací během celého jejich životního cyklu, tedy jak při jejich uložení, tak při jejich přenosu a zálohování.

Doporučení: Zajistit šifrování přenosu dat. Šifrování uložených dat je pouze doporučeno a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.

Data a informace zpracovávaná v rámci informačního nebo komunikačního systému musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autorizovaný přístup k těmto datům a informacím.

Informační nebo komunikační systém by měl být připraven využívat aktuálně odolné kryptografické algoritmy dle doporučení NÚKIB.

Toto doporučení lze nalézt na: https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/.

V případě použití jiného než doporučeného algoritmu by mělo být toto použití řádně odůvodněno.

14.1 Šifrování disků a externích USB disků

Dle aktuálního doporučení NÚKIB je pro šifrování disků možné použít následující symetrické blokové šifrovací algoritmy:

1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů
2. Twofish s využitím délky klíčů 128 až 256 bitů
3. Serpent s využitím délky klíčů 128, 192, 256 bitů
4. Camellia s využitím délky klíčů 128, 192 a 256 bitů

Přitom mezi preferované patří AES, Camellia a Serpent (v uvedeném pořadí) a velikost klíče 256 bitů.

Nejen použitý šifrovací algoritmus zabezpečuje důvěrnost dat, ale i v jakém módu je tento algoritmus použit. Pro šifrování disků doporučení schvaluje použití následujících módů:

1. XTS – délka jednotky dat (sektoru) nesmí přesáhnout 220 bloků šifry (v případě šifry se 128-bitovým blokem je to přibližně 16 MB),
2. EME.

Tyto algoritmy jsou podporovány v novějších operačních systémech, z důvodu zpětné kompatibility je u některých OS ve výchozím nastavení zapnuto šifrování v módu CBC – pro splnění požadavků je potřeba toto nastavení změnit.

14.2 Ukládání hesel

Pokud informační nebo komunikační systém ukládá hesla, musí být takto uložená hesla odolná proti offline útokům (tedy takovým způsobem, u kterého je výpočetně náročné z uloženého hesla získat původní heslo) – nejlépe použitím k tomu určenému hašovacímu algoritmu spolu s náhodně vygenerovanou „solí“.

Pokud informační nebo komunikační systém umožňuje volbu algoritmu nebo se jedná o nově vznikající informační nebo komunikační systém, doporučujeme použít jeden z následujících algoritmů (v pořadí od nejvhodnějšího):

- Argon2 (nejlépe ve verzi „id“),
- Scrypt,
- Bcrypt,
- Pbkdf2 (s použitím schváleného hašovacího algoritmu).

„Sůl“ by měla mít velikosti minimálně 64 bitů (doporučujeme 128 bitů). Pokud je možné zvolit výpočetní náročnost algoritmu, výpočet by měl trvat výpočet minimálně 100 ms (doporučeno 500 ms) a využít minimálně 1 MB paměti.

15 Požadavky v oblasti zajišťování úrovně dostupnosti informací

Cíl opatření: Zajištění dostupnosti informačního nebo komunikačního systému a dat.

Doporučení: Stanovit základní parametry dostupnosti, navrhnout vhodnou architekturu řešení.

Dostupnost informačního nebo komunikačního systému musí být stanovena a definována správcem na požadovanou úroveň na základě plánu kontinuity činností – BCP (viz kapitola Řízení kontinuity činností).

Při stanovení dostupnosti je nutné brát zřetel na efektivnost celého řešení, neboť nadhodnocené požadavky na dostupnost mají významný dopad na architekturu řešení a v konečném důsledku pak dopad na finanční stránku. Na základě definice požadavků na dostupnost se stanoví architektura celého informačního nebo komunikačního systému. Jednou z možností jak řešit dostupnost je implementace redundantních a clusterovaných schémat v režimu vysoké dostupnosti (HA), stanovení úrovně podpory, postupy obnovy po havárii a zálohování.

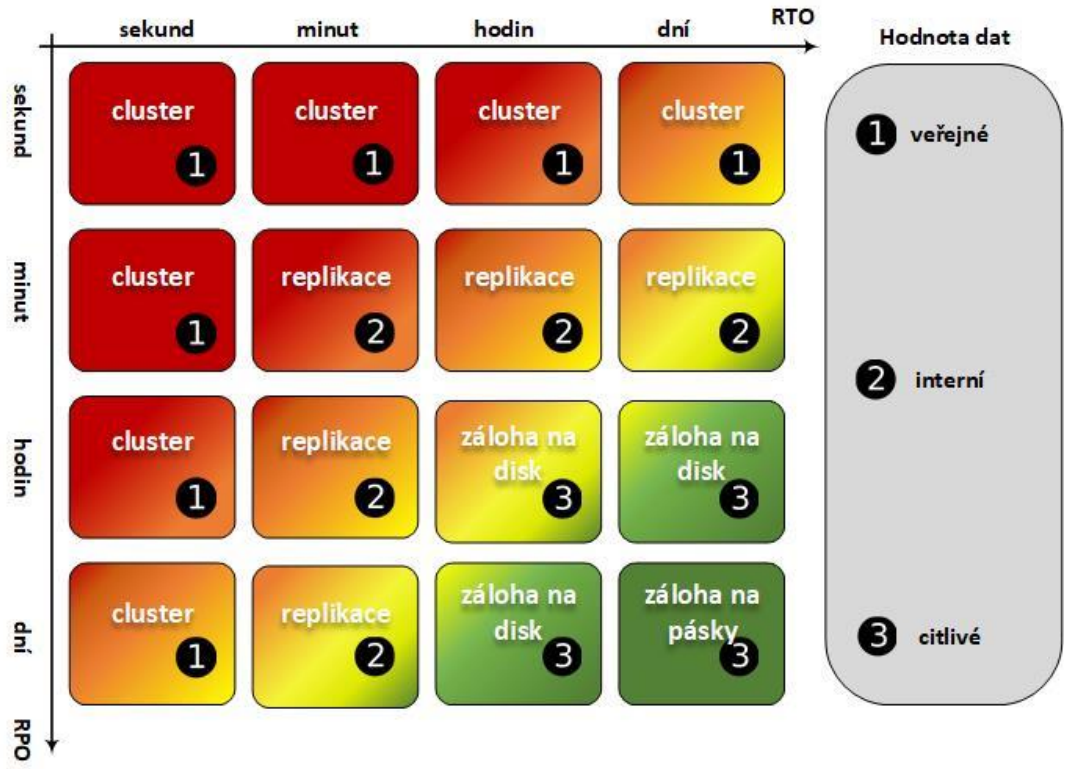
15.1 Řešení vysoké dostupnosti (HA)

Dodavatel informačního nebo komunikačního systému navrhne v rámci architektury řešení, způsob zajištění vysoké dostupnosti informačního nebo komunikačního systému dle jeho definice úrovně dostupnosti (SLA). SLA vychází z jednotlivých hodnot RPO a RTO a na základě těchto hodnot je pak nutné navrhnout a implementovat adekvátní architekturu informačního nebo komunikačního systému. Při návrhu je nutné také vycházet z ohodnocení dat. Při návrhu a realizaci řešení vysoké dostupnosti je nezbytně nutné brát zřetel především na efektivitu.

V okamžiku, kdy se požadovaná dostupnost (RPO nebo RTO) pohybuje řádově v sekundách, doporučujeme volit clusterové řešení. Pro dostupnost v řádově minutách lze provádět replikaci a v případě dostupnosti v hodinách je možno provádět zálohu na disky, a v případě dnů lze provádět zálohu na pásky.

Replikaci je možno řešit kopírováním dat do vzdálené lokality a na jiná disková úložiště. Jsou informační nebo komunikační systémy, které umožňují kopírovat jen data, která se změnila, to znamená, že se nepřenáší celý soubor, ale jen změněná část. Některé informační nebo komunikační systémy navíc umí detekovat data, která se již na diskovém úložišti vyskytují a na ty se pak pouze odkazují (deduplikace). Tímto způsobem lze výrazně snížit dobu potřebnou k vytvoření identické kopie dat produkčního prostředí a nároky na diskový prostor. V případě obnovy jsou zase tato řešení schopna obnovit data tak, že jednotlivé datové bloky jsou obnovovány postupně.[7]

[7] Převzato z: https://www.cleverandsmart.cz/analyza-rizik-kvantifikace-aktiv-z-pohledu-dostupnosti/



Obrázek č. 1 Vazba RTO a RPO na architekturu informačního nebo komunikačního systému[8]

15.2 SPOF

Již při návrhu celé architektury informačního nebo komunikačního systému (HW platformy, logické a fyzické komunikace a datových toků) je nutné v maximální možné míře zohlednit dodržování pravidla eliminace „SPOF“ (Single Point of Failure) – to znamená, že porucha jedné komponenty nezpůsobí výpadek celého informačního nebo komunikačního systému. Při zohlednění pravidla SPOF je nutné brát do úvahy efektivitu (tedy náklady) a požadavky na dostupnost.

15.3 Zálohování

Návrh informačního nebo komunikačního systému musí obsahovat požadavky na zálohování, které vychází ze SLA parametrů informačního nebo komunikačního systému (tedy dostupnosti). Vždy se požaduje vytvoření detailního návrhu zálohování celého informačního nebo komunikačního systému. Popis by měl mít strukturu, viz vzor níže:

[8] Převzato z: https://www.cleverandsmart.cz/analyza-rizik-kvantifikace-aktiv-z-pohledu-dostupnosti/

Tabulka č. 5 Ukázka popisu nastavení zálohování

Server	Co zálohovat	Interval	Kolik záloh uchovávat	Kolik dní uchovávat zálohy	Jak často provádět rozdílové zálohy	Kdy probíhá zálohování	Předpokládaná doba obnovy
Server-x	Celý server	týdně	30		denně	18:00-18:10	30 minut
Server-x	Databáze A	2 denně	28			8:00-8:10 20:00-20:10	10 minut
Server-x	Databáze A – transakční logy			730	Každou transakci	Dle transakcí	10 minut
Aktivní prvek-X	Konfigurační soubory	Při každé změně	10			Dle změn	30 minut

V rámci zálohování je doporučeno řešit i uložení médií, na která se zálohování provádí (v případě, že není využíváno centrálních zálohovacích systémů). Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3-2-1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění informačního nebo komunikačního systému („offsite“).

16 Požadavky v oblasti cloudových služeb

Cíl opatření: Zajištění kybernetické bezpečnosti při využívání cloudových služeb.

Doporučení: V případě, že je využíváno cloudových služeb pro provoz informačního nebo komunikačního systému, zajistit kybernetickou bezpečnost i z pohledu těchto služeb a to bez ohledu na to, jaký typ cloudové služby je používán (IaaS, PaaS, SaaS). Na poskytovatele cloudových služeb je potřeba vztáhnout stejná pravidla jako pro ostatní dodavatele.

Podmínky pro využívání cloudových služeb:

- deklarace místa uložení zákaznických dat v rámci jurisdikce EU,
- deklarace úrovně bezpečnosti poskytovaných cloudových služeb – (doporučujeme doložení certifikátu ČSN ISO/IEC 27001 nebo Auditní zprávu SOC 2 Type II (AT101), případně zajištění auditu na místě),
- šifrovaná komunikace (TLS/VPN) přes internet s využitím kryptografických algoritmů publikovaných v doporučení NÚKIB,
- smlouva s provozovatelem cloudových služeb obsahující vymezení provozních podmínek (SLA) a tzv. exit strategii (exit plán) včetně přádání dat,
- smluvní podmínky s provozovatelem cloudových služeb, které jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR (v případě zpracování osobních údajů v informačním nebo komunikačním systému),
- smlouva s provozovatelem cloudových obsahující povinnost informovat o bezpečnostních incidentech týkajících se daného zákazníka, a spolupracovat při jejich zvládání.

17 Další požadavky

17.1 Výjimky běhu, chyby a hlášení

Cíl opatření: Řízení výjimek a zabránění neřízeného selhání běhu informačního nebo komunikačního systému.

Doporučení: Stanovit proces řízení výjimek a jejich evidence.

Informační nebo komunikační systém musí podporovat řízení výjimek. Výjimkou je myšlena libovolná chyba nebo neočekávané chování informačního nebo komunikačního systému, které se vyskytne během vykonávání programu a je následně zpracováno a zároveň nedojde k neřízenému selhání běhu informačního nebo komunikačního systému.

Tyto výjimky musí být zaznamenány v logu, který je pravidelně vyhodnocován, přičemž zjištěné nedostatky nebo závady v informačním nebo komunikačním systému jsou v maximální možné míře ošetřeny.

17.2 Ochrana informačního nebo komunikačního systému typu webové aplikace

Cíl opaření: Ochrana webových aplikací proti nejčastějším útokům.

Doporučení: Řídit se doporučeními OWASP a věnovat pozornost zranitelnostem.

V případě, že informační nebo komunikační systém je webová aplikace, musí být tato webová aplikace chráněna proti nejčastějším útokům, které byly identifikovány nezávislým společenstvím OWASP (https://www.owasp.org). Podle tzv. best practice je nutné věnovat pozornost především následujícím známým zranitelnostem:

- Cross Site Scripting (XSS). XSS je metoda narušení webových stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).
- Injection útoky. SQL injection je technika napadnutí databázové vrstvy programu vsunutím (injection) kódu přes neošetřený vstup a vykonání vlastního, pozměněného, SQL dotazu. Vedle SQL injection existují též další podobné scénáře s jiným cílem, např. shell command injection, LDAP injection atd.
- Vzdálené spuštění kódu. Buď vlivem zranitelnosti v samotném webovém serveru, použitém frameworku či logice ve webové aplikaci.
- Nezabezpečený přímý popis objektu. Zranitelnosti této kategorie umožňují útočníkovi získat informace o jednotlivých objektech cílové aplikace bez patřičné autentizace.
- Cross Site Request Forgery (CSRF). CSFR je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.
- Únik informací nebo nedostatečné řízení chyb. Zranitelnosti tohoto typu útočníkovi zpřístupňují v případě chybového stavu aplikace informace, které lze později použít k lepšímu plánování útoku.
- Špatná autentizace a správa relace. Zranitelnosti tohoto typu umožňují útok na přihlašovací části aplikace či úplné obcházení přihlašovacího systému.

- Nezabezpečené kryptografické úložiště. Zranitelnosti tohoto typu můžou způsobit kompromitaci privátního šifrovacího klíče jedné či obou stran spojení.
- Nezabezpečená komunikace. Zranitelnosti tohoto typu umožňují útočníkům odchytávat komunikaci, která jim není určená, a provádět též aktivní útoky typu Man-in-the-Middle.
- Chybné zamezení URL přístupu. V případě, že aplikace umožňuje neautentizovaný přístup i ke stránkám, ke kterým by měl být přístup jen po příslušné autentizaci, je možnou zranitelností situace, kdy takto odkazovaná stránka zobrazí některé informace, které by měly být přístupné jen konkrétním autorizovaným uživatelům, či systémové informace citlivého charakteru.

Při zjištění některé z výše uvedených bezpečnostních zranitelností, případně jiných zranitelností známých v okamžiku vývoje webové aplikace je toto považováno za vadu aplikace (informačního nebo komunikačního systému).

17.3 Rozvoj informačních a komunikačních systémů

Cíl opatření: Zvyšování kybernetické bezpečnosti již v počátečních fázích projektů. Zahrnutím bezpečnostních požadavků od počátku dochází ke snižování nákladů, které by jinak bylo nutné vynaložit na zabezpečení v průběhu používání informačních nebo komunikačních systémů, kdy tyto náklady bývají výrazně vyšší.

Doporučení: Při tvorbě projektu v rámci akvizice, vývoje a údržby zohlednit nejen funkční, ale i bezpečnostní požadavky.

Na základě výsledků posouzení bezpečnostních aspektů vyvíjeného informačního nebo komunikačního systému musí být definovány obecné požadavky na bezpečnost informačního nebo komunikačního systému pro zjištění důvěrnosti, dostupnosti a integrity informací v informačním nebo komunikačním systému. Součástí těchto obecných požadavků musí být:

- identifikace dat vytvářených, zpracovávaných a ukládaných v informačním nebo komunikačním systému,
- definice klíčových bezpečnostních rolí včetně školení uživatelů, správců a vývojářů,
- identifikace zdrojů požadavků na informační nebo komunikační systém z hlediska bezpečnosti a regulatorních požadavků.

V případě vyvíjeného informačního nebo komunikačního systému dodavatelem musí být definovány a dokumentovány následující požadavky:

- požadavky na licenční ujednání, vlastnictví kódu a práv duševního vlastnictví,
- požadavky na osvědčení kvality a správnosti provedených prací,
- požadavky na uložení zdrojového kódu,
- požadavky na právo přístupu k vývoji pro audit bezpečnosti a správnosti provedené práce,
- požadavky na smluvní podmínky na bezpečnost a zabezpečení kódu,

- požadavky na provedení testů zranitelností před instalací v produkčním prostředí.

V případě webových aplikací je dodavatel povinen zajistit vývoj dle principů definovaných ve standardu OWASP v aktuálním znění.

Na základě posouzení bezpečnostních aspektů informačního nebo komunikačního systému definuje správce konkrétní bezpečnostní požadavky na informační nebo komunikační systém. Požadavky musí být v souladu s existujícími směrnicemi, zejména použité bezpečnostní komunikační protokoly, způsoby a možnosti šifrování. Součástí požadavků musí být i definování komunikační matice při vývoji aplikace.

Správce informačního nebo komunikačního systému definuje a dokumentuje akceptační kritéria bezpečnosti pro přechod informačního nebo komunikačního systému do produkčního provozu.

Správce informačního nebo komunikačního systému zajistí v oprávněných případech návrh splnění bezpečnostních požadavků.

Vývojové prostředí používané pro vývoj komponent informačního nebo komunikačního systému musí být zcela odděleno od provozního prostředí, a to včetně správy uživatelských oprávnění.

Pro informační nebo komunikační systém vyvíjený externím dodavatelem musí být smluvně zajištěno právo auditu zdrojového kódu a dodržování požadavků na bezpečnost. Smluvně též musí být zajištěno uložení zdrojových kódů u důvěryhodné třetí strany (code escrow) v případě, že dodavatel nepředává zdrojový kód jako součást dodávky vyvíjeného programového vybavení (informačního nebo komunikačního systému systému).

V případě vývoje aplikace (součásti informačního nebo komunikačního systému) musí mít zhotovitel formalizovanou metodiku pro vývoj, programování a kódování aplikace a testování. Tato metodika musí obsahovat mimo jiné požadavky na kybernetickou bezpečnost. V metodice musí být uvedeny principy organizační bezpečnosti pro vývoj a testování aplikace. Zhotovitel musí doložit typ metodiky, který použil pro vývoj aplikace prostřednictvím čestného prohlášení a dodání popisu nebo dokumentace této metodiky.

17.4 Komunikace

Cíl opatření: Zabezpečení komunikace s externími informačními a komunikačními systémy.

Doporučení: Dělit komunikaci s externími informačními nebo komunikačními systémy do několika skupin.

Komunikace s externími informačními nebo komunikačními systémy by měla být rozdělena podle stupně zabezpečení na:

- zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů informačního nebo komunikačního systému na úrovni infrastruktury,
- šifrování dat pro přenos a autorizací uživatele v rámci informačního nebo komunikačního systému,
- zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských informačních nebo komunikačních systémů pomocí end to end metody při přenosu dat.

18 Přílohy

Příloha č. 1: Doporučené bezpečnostní politiky a dokumentace

Tato kapitola obsahuje seznam doporučené dokumentace. Tento seznam není absolutní[9] a může se lišit podle individuálních potřeb organizace. Jednotlivé oblasti popsané v dokumentaci mohou být zapracovány do již existující dokumentace v rámci organizace, nemusí se jednat o samostatné, nově vytvořené dokumenty.

Doporučené politiky:

1. Politika organizační bezpečnosti
    a. Určení bezpečnostních rolí a jejich práv a povinností
2. Politika řízení informací
    a. Identifikace, hodnocení a evidence informací
    b. Pravidla ochrany jednotlivých úrovní informací
    c. Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií
    d. Pravidla a postupy pro ochranu předávaných informací
    e. Způsoby ochrany elektronické výměny informací
    f. Pravidla pro využívání kryptografické ochrany
3. Politika řízení dodavatelů
    a. Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti
    b. Pravidla pro provádění kontroly zavedení bezpečnostních opatření u dodavatele
4. Politika bezpečnosti lidských zdrojů
    a. Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení
    b. Bezpečnostní školení nových zaměstnanců
    c. Pravidla pro řešení případů porušení bezpečnostní politiky
    d. Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice
5. Politika řízení změn
    a. Způsob a principy řízení změn v procesech a informačních nebo komunikačních systémech
6. Politika řízení kontinuity činností
    a. Práva a povinnosti zúčastněných osob

[9] Další vhodnou dokumentaci lze nalézt např. v příloze č. 5 vyhlášky o kybernetické bezpečnosti.

   b. Cíle řízení kontinuity činností
   c. Určení a obsah potřebných plánů kontinuity činností a havarijních plánů
7. Politika řízení dokumentace
8. Politika fyzické bezpečnosti
   a. Pravidla pro ochranu objektů
   b. Pravidla pro kontrolu vstupu osob
   c. Pravidla pro ochranu zařízení
   d. Detekce narušení fyzické bezpečnosti
9. Politika řízení provozu a komunikací
   a. Postupy bezpečného provozu
   b. Požadavky a standardy bezpečného provozu
10. Politika řízení přístupu
   a. Princip minimálních oprávnění/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
11. Politika bezpečného chování uživatelů
   a. Pravidla pro bezpečné nakládání s informacemi
   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
12. Politika zálohování a obnovy a dlouhodobého ukládání
   a. Pravidla a postupy pro zálohování a obnovu
13. Politika řízení technických zranitelností
14. Politika bezpečného používání mobilních zařízení

15. Politika akvizice, vývoje a údržby
    a. Bezpečnostní požadavky pro akvizici, vývoj a údržbu
    b. Řízení zranitelností
    c. Politika poskytování a nabývání licencí programového vybavení a informací
16. Politika zvládání kybernetických bezpečnostních incidentů
    a. Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů
    b. Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti
    c. Evidence incidentů

Doporučená dokumentace:

1. Plán zavádění bezpečnostních opatření
    a. Popis bezpečnostních opatření, osoby odpovědné za zavedení jednotlivých bezpečnostních opatření, potřebné zdroje a termíny
2. Síťová topologie
3. Přehled používaných zařízení
4. Zprávy z auditu

Doporučená administrátorská dokumentace (manuály a postupy):

1. Informace o informačním nebo komunikačním systému jako celku (schéma začlenění informačního nebo komunikačního systému a komunikační mapa na úrovni L2-L3 topologie)
2. Základní popis provozní technologie vztahující se k danému informačnímu nebo komunikačnímu systému
3. Zásady a doporučení k organizaci práce s informačním nebo komunikačním systémem
4. Popis instalace, konfigurace a ovládání informačního nebo komunikačního systému
5. Popis dohledu nad funkčností informačního nebo komunikačního systému a administrace informačního nebo komunikačního systému
6. Popis řešení nestandardních stavů

Příloha č. 2: Vzorový příklad – Plán kontinuity činností (BCP)

Tabulka č. 6 Vzorový scénář

PLÁN KONTINUITY ČINNOSTÍ (BCP)	
Hrozba	Přívalová povodeň
Nebezpečí	Zničení serverovny, ztráta dat.
Pravděpodobnost vzniku	střední
OPATŘENÍ	
Prevence	
1. Umístění serverovny do vyšších pater budovy. 2. Vytvoření záloh. 3. Nasmlouvání záložní lokality. V případě vzniku mimořádné události převedení provozu informačního nebo komunikačního systému do alternativní (záložní) lokality.	
Činnosti v případě aktivace zdroje hrozby Scénář pokrývá nejhorší variantu, kdy bude nutné opustit budovu společnosti, ve které je uložena serverovna. V rámci testování i v průběhu ostrého nasazení plánu protiopatření musí být veškeré činnosti obnovy dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí určený člen týmu.	**Doba trvání**
1. Svolání krizového štábu společnosti - Svolání krizového týmu IT. - Postup dle povodňového plánu společnosti. - Rozhodnutí o aktivaci záložní lokality.	2 hod.
2. Zahájení přípravy spuštění záložní lokality - Sbalení vytvořených záloh na základě DRP. - Přesun odpovědných osob do záložní lokality – pracovníci odboru IT, a další členové týmu potřební pro zachování chodu nezbytných činností společnosti. - Aplikace opatření pro minimalizaci škod. - Evakuace zbytku osob a nařízení útlumové činnosti. - Instalace a konfigurace serverů, aplikací, síťových prvků na základě DRP.	5 hod.
3. Zahájení ostrého provozu v záložní lokalitě Informování vedení společnosti o obnovení dostupnosti aplikací v záložní lokalitě.	2 hod.
Konec (Celková doba trvání)	**9 hod.**

Doporučení pro méně závažný vývoj situace	
V případě, že se krizový štáb rozhodne neaktivovat záložní lokalitu, bude utlumena činnost organizace, budou podniknuta opatření pro minimalizaci škod (protipovodňová opatření), všechny osoby budou evakuovány.	
Další postup	
Mimořádná událost bude nadále monitorována. Po opadnutí povodně začnou likvidační práce a obnovení činností organizace v plném rozsahu.	

Příloha č. 3: Používané pojmy

Pojem	Význam
Dostupnost	Vlastnost přístupnosti a použitelnosti v požadovaném čase na žádost autorizované entity.[10]
Důvěrnost	Vlastnost, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům.[11]
Havarijní plán	Dokument, ve kterém jsou popsány činnosti a opatření, které vedou ke zmírnění nebo odstranění následků mimořádné události nebo případné havárie na životy a zdraví osob, životní prostředí, hospodářská zvířata, majetkové a kulturní hodnoty. Rozlišujeme vnější a vnitřní havarijní plán a havarijní plán kraje. [12]
Integrita	Vlastnost ochrany přesnosti a úplnosti aktiv.[13]
Krizový štáb	Pracovní orgán pro řešení krizových situací. Členové krizového štábu v době řešení vzniklé krizové situace připravují předsedovi krizového štábu podklady a návrhy řešení.
Krizový tým	Poradní orgán krizového štábu. Jeho členové jsou věcní specialisté, kteří jsou svolání v případě potřeby.
Kybernetická bezpečnostní událost	Událost, která může způsobit narušení bezpečnosti informací v informačních nebo komunikačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.[14] Jde tedy o situaci, kdy může dojít k narušení kybernetické bezpečnosti a tím ke způsobení kybernetického bezpečnostního incidentu.
Kybernetický bezpečnostní incident	Narušení bezpečnosti informací v informačních nebo komunikačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.[15] Jinými slovy dojde k situaci, kdy byla porušena kybernetická bezpečnost.
Mimořádná událost	Škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací[16].
Need-to-know	Princip, který znamená, že informace by měla být dostupná pouze tomu, kdo ji potřebuje znát, a to pouze v nezbytně nutném rozsahu.
Plán kontinuity činností	Dokumentovaný soubor postupů a informací, který je vytvořen sestaven a udržován v pohotovosti pro užití při incidentu za účelem umožnění organizaci uskutečňovat své kritické činnosti na přijatelné, předem stanovené úrovni.[17]
Správce informačního nebo komunikačního systému	Orgán nebo osoba, které určují účel informačního nebo komunikačního systému a podmínky jeho provozování.[18]

[10] Petr JIRÁSEK, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 3., doplněné a upravené vydání. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[11] tamtéž.
[12] Převzato z: https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-ke-stazeni-ff.aspx?q=Y2hudW09NA%3d%3d a https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-havarijni-planovani-havarijni-planovani.aspx.
[13] Petr JIRÁSEK, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 3., doplněné a upravené vydání. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[14] § 7 odst. 1 zákona o kybernetické bezpečnosti
[15] § 7 odst. 2 zákona o kybernetické bezpečnosti
[16] § 2 písm. b) zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů
[17] Petr JIRÁSEK, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 3., doplněné a upravené vydání. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[18] § 2 písm. e) a f) zákona o kybernetické bezpečnosti

Vendor lock-in	Závislost na konkrétním dodavateli a jeho řešení. Změny, úpravy či zpřístupnění informačního nebo komunikačního systému bez souhlasu nebo poplatků dodavateli není možné.

Příloha č. 4: Používané zkratky

Zkratka	Význam
AAA	Autentizace – Autorizace – Accounting (Auditing), tedy ověření identity – přidělení oprávnění – vytvoření záznamu o přístupu
BIA	(Business Impact Analysis) – analýza dopadů
BCP	(Business Continuity Plan) – plán kontinuity činností
BYOD	(Bring Your Own Device) – využívání soukromých zařízení zaměstnanců, která jsou přinášena, užívána a připojena na pracovišti do počítačové sítě organizace
CBC	(Cipher Block Chaining) – způsob řetězení šifrových bloků u blokových symetrických kryptografických algoritmů
CERT	(Computer Emergency Response Team) – bezpečností tým, který řeší bezpečnostní události a incidenty
CSRF	(Cross Site Request Forgery) – technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit
DRP	(Disaster Recovery Plan) – plán obnovy provozu
EME	(Encrypt-Mix-Encrypt) – způsob řetězení šifrových bloků u blokových symetrických kryptografických algoritmů
GDPR	(General Data Protection Regulation) - Obecné nařízení o ochraně osobních údajů[19]
HA	(High Availability) – řešení vysoké dostupnosti
HTTP	(Hypertext Transfer Protocol) – internetový protokol určený pro komunikaci s webovými servery
HTTPS	(Hypertext Transfer Protocol Secure) – zabezpečený protokol HTTP pomocí TLS
HW	(Hardware)
IaaS	(Infrastructure as a Service) – označuje pronájem infrastruktury, např. pro virtualizaci serverů
ID	(Identification) - identifikátor
IDS	(Intrusion Detection System) – systémy monitorující síťový provoz nebo aktivity operačního systémů provoz s cílem odhalení podezřelých aktivit
IPS	(Intrusion Prevention System) – systémy monitorující síťový provoz nebo aktivity operačního systémů provoz s cílem zablokování podezřelých aktivit
ISO/IEC 27001	Řada mezinárodních standardů zaměřená na řízení bezpečnosti informací
JDBC	(Java Database Connectivity) – základní databázové rozhraní pro aplikace vytvořené v jazyce Java
LDAP	(Lightweight Directory Access Protocol) - protokol pro ukládání a přístup k datům na adresářovém serveru nebo přímo zkratka pro adresářový server
MDM	(Mobile Device Management) – umožňuje zabezpečení, monitorování, správu i podporu mobilních zařízení používaných v rámci podnikové sítě
NAT	(Network Address Translation) – funkce routeru pro překlad síťových adres

[19] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

NDA	(Non-disclosure Agreement) – dohoda o mlčenlivosti
NTP	(Network Time Protocol) – protokol pro synchronizaci vnitřních hodin zařízení
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OWASP	(Open Web Application Security Project) – komunita zabývající se bezpečností webových aplikací
PaaS	(Platform as a Service) – poskytování komplexní platformy (aplikační a vývojové) pro tvorbu a využívání aplikací
RPO	(Recovery Point Objective) - definuje, do jakého stavu (bodu) v minulosti lze obnovit data v systému
RTO	(Recovery Time Objective) - vyjadřuje množství času potřebné pro obnovení dat
SaaS	(Software as a Service) – pronájem konkrétní softwarové aplikace, která je poskytovaná jako služba
SIEM	(Security Information and Event Management) – systémy, které nabízí monitorování, ukládání a správu bezpečnostních událostí reprezentovaných logovacími záznamy, které jsou sbírány z definovaných zařízení nacházejících se v IT infrastruktuře
SLA	(Service Level Agreement) – dohoda mezi poskytovatelem služeb IT a zákazníkem. SLA popisuje službu IT, dokumentuje cíle úrovní služeb a specifikuje odpovědnosti poskytovatele služeb a zákazníka.
SNMP	(Simple Network Management Protocol) – protokol pro monitoring sítě, který umožňuje sběr různých dat pro správu sítě a následné vyhodnocování
SOC 2	typ nezávislého systému repotingu
SPOF	(Single Point of Failure) – jediný bod selhání
SQL	(Structured Query Language) – standardní dotazovací jazyk
TLS	(Transport Layer Security) – kryptografický protokol
USB	(Universal Serial Bus) – způsob připojení periferií k zařízení
UTC	(Coordinated Universal Time) – koordinovaný světový čas
VPN	(Virtual Private Network) – virtuální privátní síť
XTS	(XEX-based tweaked-codebook mode with ciphertext stealing) – způsob řetězení šifrových bloků u blokových symetrických kryptografických algoritmů

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
17.07.2020	1.0	NÚKIB, NAKIT, MV	Vytvoření dokumentu