Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Cyber Security Framework National Institute of Standards and Technology

Bakalářská práce

Autor: Václav Buřil
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Bc. Hana Švecová

Hradec Králové Květen 2022

Prohlášení:

Prohlašuji, že jsem bakalářskou/diplomovou práci zpracoval/zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 12.8.2022 Václav Buřil

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Haně Švecové za metodické vedení práce.

Anotace

V první části bakalářské práce jsou rozpracovány dílčí části mezinárodního rámce Cyber Security Framework National Instituce of Standards and Technology. Tyto části zahrnutí především jádro, elementy, funkce, možnosti implementace a využití v oblasti informační bezpečnosti. V druhé části bakalářské práce jsou rozpracovány vybrané dílčí části vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti včetně komparativního srovnání vybraných částí frameworku a vyhlášky souvisejících s informační bezpečností. V závěru práce je provedeno shrnutí analýzy a komparace včetně doporučení.

Annotation

Title: Cyber Security Framework National Institute of Standards and Technology

The first part of the bachelor thesis elaborates on the parts of the National Institution of Standards and Technology international Cyber Security Framework. These parts mainly include the core, elements, functions, implementation options and applications in the field of information security. The second part of the bachelor thesis elaborates on selected subparts of Decree No. 82/2018 on Cyber Security, including a comparative comparison of selected framework parts and the decree related to information security. The thesis concludes with a summary of the analysis and comparison, including recommendations.

Obsah

1 Úvod

Kybernetická bezpečnost je obor v informatice, který se zabývá ochranou kritických systémů a citlivých informací před digitálním útokem. Kybernetická ochrana by měla řešit zabezpečení: sítí, aplikací, cloudu, informací a úložišť. Dále také vzdělávání koncových uživatelů a plánování či řešení případných havárií nebo kybernetických událostí. Důležitou doménou kybernetické bezpečnosti je také zabezpečení kritické infrastruktury. Kritickou infrastrukturou se rozumí taková infrastruktura, která je důležitá pro chod ekonomiky a bezpečnosti [9].

Odvětví kritické infrastruktury je tvořeno především: energetikou, vodním hospodářstvím, potravinářstvím, zemědělstvím, zdravotnictvím, dopravou, komunikačními a informačními systémy. Pro zavádění bezpečnostních pravidel a doporučení v kybernetické bezpečnosti se využívají různé frameworky či mezinárodní normy (ISO/IEC 2700x). Jedním z možných přístupů, který se nabízí pro implementaci pravidel kybernetické bezpečnosti je Cyber Security Framework National Institute of Standards and Technology, který je vyvíjen společností National Institute of Standards and Technology (NIST) a využívá společný jazyk pro nákladově efektivní správu a řešení bezpečnostních rizik v podnicích, aniž by kladl na podniky další regulační požadavky. Výše uvedený dokument byl vytvořen primárně pro zlepšení kybernetické bezpečnosti kritické infrastruktury v USA. Framework však mohou používat podniky napříč odvětvími bez ohledu na velikost, stupeň kybernetického ohrožení nebo propracovanost kybernetické bezpečnosti.

2 Cíle práce a metodika zpracování

Cílem bakalářské práce je analýza a komparativní srovnání Cyber Security Frameworku (NIST) s legislativním rámcem kybernetické bezpečnosti v České republice, konkrétně vybranými dílčími částmi vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. V první části práce byl analyzován (rozpracován) Cyber Security Framework (NIST), jeho dílčí části a možné využití organizacích. V druhé části byly rozpracovány dílčí vybrané části vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, a dále byla provedena komparace jejíchž výsledky a doporučení jsou popsány v závěru práce. Součástí komparativního srovnání je zpracování přehledové tabulky, jež je nedílnou součástí této bakalářské práce.

Vzhledem k celkovému rozsahu frameworku (cca 450 s.) byly zvoleny pro analýzu a komparaci vybrané dílčí části, které svým obsahem nejvíce zahrnovaly problematiku související s informační bezpečnosti. Analýza a komparace celého frameworku NIST svým celkovým rozsahem by byla vhodná např. pro diplomovou práci či jinou vědecky rozsáhlou práci (např. disertační práce).

3 Cyber Security Framework

Cybersecurity Framework je určen pro správu a řešení bezpečnostních rizik v podnicích, bez potřeby kladení dalších regulačních požadavků na tyto podniky. Framework mohou tedy využívat organizace po celém světě napříč odvětvími bez ohledu na velikost, stupeň kybernetického ohrožení nebo propracovanost kybernetické bezpečnosti. Existuje celá řada způsobů, jak Framework použít. Jelikož každá organizace, která implementuje Cyber Security Framework, má jedinečná rizika, priority a systémy budou se nástroje a metody používané k dosažení výsledků popsané ve Frameworku při implementaci odlišovat. O způsobu použití Frameworku si organizace rozhoduje sama podle vlastního odborného vyjádření odborníků (zaměstnanců) v organizaci. Framework obsahuje metodiku pro ochranu jednotlivců a občanských svobod. Některé organizace už mají procesy pro řešení ochrany soukromý a občanských svobod. Tato metodika je navržena tak aby doplňovala tyto procesy a poskytla pokyny pro zjednodušení řízení ochrany osobních údajů.

„Framework zůstává účinný, podporuje technické inovace, protože je technologicky neutrální, a zároveň odkazuje na řadu stávajících norem, pokynů a postupů, které se vyvíjejí s technologiemi. Spoléháním se na tyto globální normy, pokyny a postupy vyvinuté, řízené a aktualizované průmyslem se nástroje a metody dostupné k dosažení výsledků rámce budou rozšiřovat přes hranice, uznávat globální povahu kybernetických bezpečnostních rizik a vyvíjet se s technologickým pokrokem a obchodními požadavky. Využívání stávajících a nově vznikajících norem umožní úspory z rozsahu a pomůže vývoji účinných produktů, služeb a postupů, které splňují požadavky trhu. Tržní konkurence rovněž podporuje rychlejší šíření těchto technologií a postupů a realizaci mnoha přínosů zúčastněnými stranami v těchto odvětvích.

Na základě těchto standardů, pokynů a postupů poskytuje rámec společnou taxonomii a mechanismus, který organizacím umožňuje:

1) Popsat své současné postavení v oblasti kybernetické bezpečnosti;

2) Popsat svůj cílový stav kybernetické bezpečnosti;

3) Identifikovat a upřednostnit příležitosti ke zlepšení v rámci kontinuálního a opakovatelného procesu;

4) Vyhodnotit pokrok směrem k cílovému stavu;

5) Komunikovat mezi interními a externími zainteresovanými stranami o rizicích kybernetické bezpečnosti [1].*“*

3.1 Dílčí části frameworku

Framework obsahuje tři části, které popisují vztah mezi obchodními faktory/posláním a činnostmi v oblasti kybernetické bezpečnosti.

Tyto části tvoří:

Jádro rámce (Framework Core) představuje činnosti v oblasti kybernetické bezpečnosti, požadované výsledky a použitelné odkazy, které jsou společné pro všechna odvětví kritické infrastruktury. Jádro představuje standardy, pokyny a postupy. Tyto prostředky umožňují komunikaci, která se týká činností a výsledků v oblasti kybernetické činnosti napříč organizací, od vedení až po úroveň implementace. Jádro rámce se skládá z pěti souběžných a kontinuálních funkcí – identifikace, ochrana, detekce, reakce, zotavení. Pokud se tyto funkce posuzují společně, poskytují strategický pohled na životní cyklus řízení rizik kybernetické bezpečnosti v organizaci na vysoké úrovni.

Úrovně implementace rámce (Framework Implementation Tiers) určují, jak organizace vnímá riziko kybernetické bezpečnosti a jaké opatření proti těmto rizikům přímá. Jednotlivé úrovně charakterizují postupy organizace od částečné (Tier 1) až po adaptivní (Tier 4).

Rámcový profil (Framework Profile) prezentuje propojení norem, pokynů a postupů s jádrem rámce v konkrétním scénáři implementace. Dají se využívat pro identifikaci příležitostí současného stavu kybernetické bezpečnosti v organizaci. Profily lze také použít k provádění sebehodnocení a komunikaci v rámci organizace nebo mezi organizacemi navzájem.

3.1.1 Jádro frameworku

Jádro Frameworku poskytuje soubor činností, které vedou k výsledkům kybernetické bezpečnosti. Jádro není kontrolní seznam akcí, které je potřeba provést, ale představuje klíčové výsledky pro řízení kybernetických bezpečnostních rizik.

3.1.1.1 Elementy jádra frameworku

Jádro se skládá ze čtyř elementů:

Funkce (Functions) organizují základní činnosti v rámci nejvyšší úrovně kybernetické bezpečnosti. Framework dělí tyto činnosti do pěti funkcí: identifikace, ochrana, detekce, reakce a obnova. Tyto funkce pomáhají organizaci vyjádřit řízení kybernetických bezpečnostních rizik pomocí organizováním informací, umožněním rozhodováním o řízení rizik, řešením hrozeb a zlepšováním tím, že se zdokonaluje z předchozích činností.

Kategorie (Categories) rozdělují funkce do skupin výsledků kybernetické bezpečnosti úzce souvisejících s programovanými potřebami a konkrétními činnostmi.

Podkategorie (Subcategories) rozdělují kategorie do konkrétních výsledků technik a/nebo řídicích činností. Poskytují soubor výsledků, který pomáhá podporovat dosažení výsledků v každé kategorii.

Informativní odkazy (Informative references) jsou specifické části norem, postupů a pokynů, které jsou běžné v kritické infrastruktuře a popisují způsob dosažení výsledků pro každou podkategorii. Informativní odkazy v jádru Frameworku jsou ilustrativní a nejsou vyčerpávající.

3.1.1.2 Funkce jádra Frameworku

Funkce jádra frameworku nemají tvořit sériovou cestu nebo vést k požadovanému statickému konečnému stavu. Tyto funkce by se měli provádět souběžně a nepřetržitě, to povede k vytvoření provozní kultury, která zajišťuje dynamická rizika kybernetické bezpečnosti.

Jádro frameworku obsahuje pět funkcí:

Identifikace (Identify) – Cíle identifikace je rozvíjet organizační znalosti pro řízení kybernetické bezpečnosti pro systémy, lidi, aktiva a schopnosti. Činnosti v této funkci jsou základem pro efektivní používání frameworku. Tato funkce pomáhá pochopit business kontext, zdroje podporující kritické funkce a kybernetická bezpečnostní rizika. Toto umožňuje organizaci soustředit se a upřednostňovat své úsilí v souladu s se strategií řízení rizik a obchodními cíli.

Ochrana (Protect) - Cílem ochrany je vyvinout a zavést vhodná ochranná opatření k zajištění poskytování kritických služeb. Tato funkce podporuje schopnost zmírnění následků případné kybernetické události.

Detekce (Detect) - Cílem detekce je vyvinout a zavést vhodné činnosti k identifikaci výskytu kybernetické bezpečnostní události. Tato funkce zajišťuje včasné odhalení kybernetické bezpečnostní události.

Reakce (Respond) – Cílem reakce je Vyvinout a realizovat vhodné činnosti k přijetí opatření týkajících se zjištěného kybernetického bezpečnostního incidentu. Tato funkce podporuje schopnost omezení dopadu potenciálního kybernetického bezpečnostního incidentu.

Obnova (Recover) - Cílem obnovy je vyvinout a implementovat činnosti k obnovení funkcí nebo služeb, které byly narušeny kybernetickým incidentem. Tato funkce podporuje včasné obnovení běžného provozu, který byl omezen kybernetickým incidentem, za co nejmenšího dopadu.

3.1.2 Úrovně implementace frameworku

Úrovně implementace rámce poskytují kontext, jak organizace vnímá riziko kybernetické bezpečnosti a jaké procesy jsou zavedeny pro řízení tohoto rizika. Jednotlivé úrovně popisují stupeň propracovanosti postupů při řízení těchto rizik. Také pomáhají určit, jak moc je řízení kybernetických rizik založeno na obchodních potřebách a jak moc jsou integrovány do celkových postupů řízení rizik organizace. Úvahy o řízení rizik zahrnují mnoho aspektů kybernetické bezpečnosti.

Proces výběru úrovně zohledňuje současné postupy organizace v oblasti řízení rizik, prostředí hrozeb, právní a regulační požadavky, postupy sdílení informací, obchodní cíle/mise, požadavky na kybernetickou bezpečnost dodavatelského řetězce a organizační omezení. Organizace by si měli zvolit takovou úroveň implementace rámce, aby zvolená úroveň splňovala cíle organizace, byla proveditelná a snižovala riziko kybernetické bezpečnosti kritických aktiv a zdrojů na úroveň přijatelnou pro organizaci. Organizace by měli zvážit využití externích postupů a zdrojů pro určení požadované úrovně.

„Úrovně mají podpořit rozhodování organizace o tom, jak řídit rizika kybernetické bezpečnosti, a také o tom, které dimenze organizace mají vyšší prioritu

a mohly by získat další zdroje. Postup na vyšší úrovně se doporučuje v případě, že analýza nákladů a přínosů naznačuje proveditelné a nákladově efektivní snížení rizika kybernetické bezpečnosti [1]. " Úspěšná implementace rámce není vybrat úroveň rámce, ale dosažení *výsledk*ů popsaných v cílovém profilu. Výběr úrovně pomůže v organizaci nastavit řízení kybernetických rizik.

Rámec definuje čtyři úrovně implementace:

Úroveň 1 (Částečná) - V této úrovni nejsou organizační postupy řízení kybernetických bezpečnostních rizik definována a jsou řešena ad hoc. Stanovení priorit činností kybernetické bezpečnosti nemusí řídit z cílů organizace. Implementace řízení kybernetických rizik jsou nepravidelné a organizace nemusí mít zavedeny procesy, které by sdíleli informace o kybernetických rizicích v rámci organizace. Organizace nerozumí své roli v širším ekosystému s ohledem na své závislosti nebo závislé subjekty. Organizace nespolupracuje s jinými subjekty, nezískává od nich informace o kybernetické bezpečnosti ani je nesdílí.

Úroveň 2 (Informovaný o riziku) - V této úrovní jsou postupy řízení rizik schvalovány vedením organizace, ale nemusejí být implementovány v celé organizaci. Stanovení priorit činností kybernetické bezpečnosti se řídí cíli organizace. V organizaci existuje povědomí, ale nebyl zaveden celopodnikový přistup řízení kybernetických rizik. Informace o kybernetických rizikách jsou sdíleny neformálně. Obecně platí, že organizace chápe svou roli v širším ekosystému buď s ohledem na své vlastní závislosti, nebo na závislé subjekty, ale ne na obojí. Organizace spolupracuje s jinými subjekty, od kterých přímá některé informace, ale sama je sdílet nemusí.

Úroveň 3 (Opakovatelná) - V této úrovní jsou postupy řízení rizik formálně schváleny a formulovány jako zásady. Organizace pravidelně aktualizuje kybernetické bezpečnostní postupy na základě změn v obchodních požadavcích organizace a měnící se prostředí hrozeb a technologií. V organizaci existuje celopodnikový přístup k řízení rizik kybernetické bezpečnosti." *Zásady, procesy a postupy zohledňující rizika jsou definovány a implementovány v souladu se záměrem a revidovány. Jsou zavedeny konzistentní metody, které umožňují účinně reagovat na změny rizik. Zaměstnanci mají znalosti a dovednosti pro plnění svých určených rolí a povinností. Organizace důsledně a přesně monitoruje kybernetické bezpečnostní riziko aktiv organizace. Vedoucí pracovníci v oblasti kybernetické bezpečnosti a vedoucí pracovníci mimo oblast kybernetické*

bezpečnosti pravidelně komunikují ohledně kybernetického bezpečnostního rizika. Vedoucí pracovníci zajišťují zohlednění kybernetické bezpečnosti ve všech liniích činnosti organizace. Organizace chápe svou roli, závislosti a závislosti v širším ekosystému a může přispět k širšímu chápání rizik v komunitě. Pravidelně spolupracuje s jinými subjekty a získává od nich informace, které doplňují interně vytvořenými informacemi, a sdílí je s ostatními subjekty[1].“

Úroveň 4 (Adaptivní) - V této úrovní organizace přizpůsobuje své kybernetické bezpečnostní postupy na základě předchozích a současných aktivit v oblasti kybernetické bezpečnosti. Pomocí procesu stálého zlepšování zahrnující pokročilé postupy kybernetické bezpečnosti, se organizace neustále přizpůsobuje měnícímu se prostředí hrozeb a technologií, a také včas a účinně reaguje na nové hrozby. Existuje celopodnikový přístup k řízení rizik kybernetické bezpečnosti, který využívá zásady, procesy a postupy zohledňující rizika při řešení potenciálních událostí. Je definován vztah mezi cíli organizace a kybernetickým rizikem. Kybernetická bezpečnost je chápána ve stejném kontextu jako finanční riziko a další rizika organizace. Řízení rizik kybernetické bezpečnosti je součástí organizační kultury a vyvíjí se na základě povědomí o předchozích činnostech a průběžného informování o aktivitách v jejich systémech a sítích. „*Organizace rozumí své roli, závislostem a závislým osobám v širším ekosystému a přispívá k širšímu chápání rizik v komunitě. Získává, formuluje a přezkoumává prioritní informace, které jsou podkladem pro průběžnou analýzu jejích rizik v závislosti na vývoji prostředí hrozeb a technologií. Tyto informace organizace sdílí interně i externě s dalšími spolupracovníky. Organizace využívá informace v reálném čase nebo téměř v reálném čase, aby pochopila a důsledně reagovala na rizika kybernetického dodavatelského řetězce spojená s produkty a službami, které poskytuje a které využívá. Kromě toho proaktivně komunikuje a využívá formální (např. dohody) i neformální mechanismy k rozvoji a udržování pevných vztahů v dodavatelském řetězci* [1].“

3.1.3 Rámcový profil

Profil rámce představuje propojení funkcí, kategorií a podkategorií s podnikovými požadavky, tolerancí rizik a zdroji organizace. Organizace pomocí profilu může vytvořit plán na snižování kybernetických rizik, který je sladěn s cíli organizace a zohledňuje

právní/regulační požadavky, osvědčené postupy v odvětí a priority řízení rizik. Organizace může mít více profilů.

Profile lze použít k popisu stávajícího stavu organizace. Tento profil popisuje aktuální stav kybernetické bezpečnosti organizace. Cílový profil popisuje výsledky potřebné k dosažení požadovaných cílů v oblasti kybernetické bezpečnosti. Profil pomáhá při komunikacích a využívá kybernetických rizik v organizaci nebo mezi organizacemi. Tento framework nemá žádnou šablonu profilu což umožňuje flexibilitu při implementaci.

„Porovnání profilů (např. současného a cílového profilu) může odhalit nedostatky, které je třeba odstranit, aby byly splněny cíle řízení rizik kybernetické bezpečnosti. Akční plán k odstranění těchto nedostatků pro splnění dané Kategorie nebo Podkategorie může přispět k výše popsanému plánu. Stanovení priorit pro zmírnění nedostatků se řídí obchodními potřebami organizace a procesy řízení rizik. Tento přístup založený na rizicích umožňuje organizaci posoudit zdroje potřebné (např. personální zajištění nebo financování) k dosažení cílů v oblasti kybernetické bezpečnosti nákladově efektivním a prioritním způsobem. Rámec je navíc přístupem založeným na rizicích, kdy použitelnost a naplnění dané podkategorie podléhá rozsahu profilu"[1].

3.2 Koordinace zavádění Frameworku

Koordinace probíhá mezi třemi úrovněmi organizace. Nejvyšší úroveň organizace (výkonná úroveň) sděluje priority úkolů, dostupné zdroje a celkovou míru rizika úrovni business/procesu. Tato úroveň využívá tyto informace jako vstupy do procesu řízení rizik a také spolupracuje s implementační/provozní úrovní se kterou formuluje framework profily a sděluje obchodní potřeby. Implementační/provozní úroveň využívá tyto informace k posouzení dopadů. Výsledky tohoto posouzení sděluje business/proces úroveň výkonné úrovni, aby informovala o celkovém řízení rizik v organizaci.

3.3 Využití Frameworku

Organizace může využít Framework jako součást systematického procesu identifikace, hodnocení a řízení rizik kybernetické bezpečnosti. Framework není navržen tak aby nahradil stávající bezpečnostní procesy, ale může ho použít pro zjištění nedostatků současného bezpečnostního rámce a určit činnosti, které jsou pro poskytování

kritických služeb nejdůležitější, a stanovit priority výdajů tak, aby se maximalizoval dopad investic.

3.3.1 Základní přezkoumání postupů v oblasti kybernetické bezpečnosti

Framework může sloužit organizaci k porovnání současných aktivit v kybernetické bezpečnosti s aktivitami v jádře Frameworku. Organizace může za pomoci vytvoření současného profilu zkoumat, do jaké míry dosahují výsledků popsaných v jednotlivých kategoriích jádra. Na základě tohoto zkoumání organizace zjistí, zda dosahuje požadovaných výsledků nebo že může (popřípadě potřebuje) zlepšit svoji kybernetickou bezpečnost. Na základě těchto zjištění muže vypracovat akční plán pro snížení rizika kybernetické bezpečnosti. Organizace muže toto využít i pro efektivnější nakládání prostředků.

3.3.2 Zavedení nebo zlepšení programu kybernetické bezpečnosti

Organizace může rámec použít k vytvoření kybernetického bezpečnostního programu nebo zlepšení stávajícího programu. Popsané kroky by se měly dle potřeby opakovat, aby se kybernetická bezpečnost organizace neustále zlepšovala.

Krok 1 - Stanovení priorit a rozsahu. Organizace stanoví své business cíle a priority, na základě toho organizace příjme strategická rozhodnutí tykajících se implementace kybernetické bezpečnosti a určuje rozsah systémů a aktiv, které podporují vybranou obchodní linii nebo proces. Rámec lze přizpůsobit, aby podporoval různé obchodní linie nebo procesy v rámci organizace, které mohou mít různé obchodní potřeby a související toleranci k riziku. Tolerance rizik se může odrážet v cílové úrovni implementace.

Krok 2 – Orientace. V tomto kroku organizace identifikuje související systémy a aktiva, regulační požadavky a celkový přístup k rizikům. Poté organizace konzultuje zdroje, aby identifikovala hrozby a zranitelnosti vztahující se na tyto systémy a aktiva.

Krok 3 - Vytvoření aktuálního profilu. Organizace zformuluje aktuální profil tak že uvede, kterých výsledků je současně dosahováno v jednotlivých kategoriích jádra rámce.

Krok 4 - Provedení posouzení rizik. Organizace provede analýzu provozního prostředí s cílem odhalit pravděpodobnost výskytu kybernetické bezpečnostní události

a dopadu této události na organizaci. Organizace by měla identifikovat vznikající rizika a využívat informace o kybernetických hrozbách z interních i externích zdrojů.

Krok 5 - Vytvoření cílového profilu. Organizace zformuluje cílový profil tak že se zaměří na hodnocení kategorií a podkategorií Frameworku, které popisují požadované výsledky organizace. Organizace si může vytvořit i své kategorie a podkategorie na základě svých jedinečných rizik. Také muže do cílového profilu zahrnout vlivy externích stran, jako jsou zákazníci, dodavatelé atd.

Krok 6 - Určení, analýza a stanovení priorit nedostatků. Organizace porovná současný a cílový profil. Na základě nedostatků současného profilu organizace zformuluje akční plán s prioritami k odstranění nedostatků. Organizace poté stanoví zdroje, včetně finančních prostředků a pracovní síly, které jsou nezbytné k odstranění nedostatků. Používaní profilů tímto způsobem podporuje organizaci v přijímání informovaných rozhodnutí o činnostech v oblasti kybernetické bezpečnosti, podporuje řízení rizik a umožňuje organizaci provádět nákladově efektivní a cílená zlepšení.

Krok 7 - Implementace akčního plánu. Organizace stanoví, jaké opatření příjme k odstranění nedostatků. Také upraví své postupy v oblasti kybernetické bezpečnosti. Nakonec stanoví, jaké normy, pokyny a postupy, včetně těch, které jsou specifické pro dané odvětví, nejlépe vyhovují jejich potřebám.

3.3.3 Komunikace požadavků na kybernetickou bezpečnost se zúčastněnými stranami

Framework poskytuje základní jazyk pro komunikaci o požadavcích mezi odpovědnými za poskytování produktů a služeb základní kritické infrastruktury. Např: Organizace muže použít svůj cílový profil pro vyjádření požadavků pro řízení rizik pro externí poskytovatele služeb (např. poskytovatele cloudu) nebo sektor kritické infrastruktury může vytvořit cílový profil, který mohou jeho složky používat jako výchozí základní profil pro vytvoření svých cílových profilů na míru.

Komunikace je důležitá zejména v mezi subjekty v dodavatelských řetězcích. Dodavatelské řetězce jsou složité, globálně distribuované a vzájemně propojené sady zdrojů a procesů mezi několika úrovněmi organizací. Kvůli složitým a vzájemně propojeným vztahům je řízení rizik dodavatelského řetězce (SCRM) kritickou

organizační funkcí. Kybernetický SRCM se zabývá kyberbezpečnostním vlivem organizace na externí strany i kyberbezpečnostním vlivem externích stran na organizaci. Kybernetické SRCM má hlavní cíl identifikovat, posoudit a zmírnit "produkty a služby, které mohou obsahovat potenciálně škodlivé funkce, jsou padělané nebo zranitelné v důsledku špatných výrobních a vývojových postupů v rámci kybernetického dodavatelského řetězce.

„*Kybernetické SRCM může zahrnovat tyto činnosti: Stanovení požadavků na kybernetickou bezpečnost dodavatelů, zavedení požadavků na kybernetickou bezpečnost prostřednictvím formální dohody (např. smlouvy), sdělení dodavatelům, jak budou tyto požadavky na kybernetickou bezpečnost ověřovány a validovány, ověřování splnění požadavků na kybernetickou bezpečnost prostřednictvím různých metodik hodnocení.*

Kybernetický SCRM zahrnuje dodavatele a odběratele technologií, jakož i dodavatele a odběratele ne technologií, přičemž technologie se skládají minimálně z informačních technologií (IT), průmyslových řídicích systémů (ICS), kybernetico-fyzických systémů (CPS) a obecněji z připojených zařízení, včetně internetu věcí (IoT). Tyto subjekty formulují ekosystém kybernetické bezpečnosti organizace. Vztahy, produkty a služby, které poskytují, a rizika, která představují, by měli být zohledněny v kybernetické bezpečnosti organizace [1].“

Rámec umožňuje organizacím a jejich partnerům, aby jejich nový produkt nebo služba splňovali kritické bezpečnostní požadavky. Organizace nejprve vybere výsledky, které jsou relativní pro dany kontext, pak podle těchto kritérií muže hodnotit jednotlivé partnery.

3.4 Rozhodnutí o nákupu

Cílový profil je prioritizovaný seznam požadavků na kybernetickou bezpečnost organizace a lze ho využít k nákupu služeb nebo produktů. Cílový profil by měl organizaci pomoc rozhodnout mezi několika dodavateli na základě kybernetické bezpečnosti. Ne vždy budou dodavatele splňovat veškeré cíle cílového profilu, ale profil lze využít k sledování zbývajícího rizika a organizace muže tyto rizika vyřešit dalšími opatřeními.

3.4.1 Identifikace příležitostí pro nové nebo revidované informativní odkazy

Organizace může využít rámec k identifikaci příležitostí pro nové nebo revidované normy, pokyny nebo postupy, kde by další informativní odkazy pomohly organizacím řešit vznikající potřeby. Organizaci, která vyvíjí novou podkategorií, se může stát, že je málo nebo že nejsou žádné informativní odkazy. Pro řešení této potřeby může organizace spolupracovat s vedoucími technologickými a/nebo normalizačními orgány na návrhu, vývoji a koordinaci norem, pokynů nebo postupů.

3.4.2 Metodika ochrany soukromí a občanských svobod

Ochrana soukromí a kybernetická bezpečnost spolu souvisí. Organizace svými činnostmi v oblasti kybernetické bezpečnosti mohou vytvářet rizika pro soukromí a občanské svobody, pokud jsou osobní údaje používány, shromažďovány, zpracovávány, uchovávány nebo zveřejňovány.

„Vláda a její zástupci mají povinnost chránit občanské svobody vyplývající z činností v oblasti kybernetické bezpečnosti. Vláda nebo její zástupci, kteří vlastní nebo provozují kritickou infrastrukturu, by měli mít zaveden proces podporující soulad činností v oblasti kybernetické bezpečnosti s platnými zákony, předpisy a ústavními požadavky na ochranu soukromí [1].“

Organizace by měli zvážit, jestli by jejich program kybernetické bezpečnosti měl mýt zásady ochrany soukromí, jako jsou: „*minimalizace údajů při shromažďování, zveřejňování a uchovávání osobních informací, které se týkají kybernetického bezpečnostního incidentu; omezení použití mimo činnosti v oblasti kybernetické bezpečnosti u všech informací shromážděných speciálně pro činnosti v oblasti kybernetické bezpečnosti; transparentnost určitých činností v oblasti kybernetické bezpečnosti; individuální souhlas a náprava nepříznivých dopadů vyplývajících z použití osobních informací při činnostech v oblasti kybernetické bezpečnosti; kvalita, integrita a bezpečnost údajů; a odpovědnost a audit*[1].“

*„**Řízení rizik kybernetické bezpečnosti** – Organizace při posuzování rizik kybernetické bezpečnosti a možných reakcí na rizika zohledňuje důsledky svého programu kybernetické bezpečnosti pro soukromí. Osoby odpovědné za ochranu soukromí v souvislosti s kybernetickou bezpečností podléhají příslušnému vedení a jsou*

náležitě vyškoleny. Je zaveden proces podporující soulad činností v oblasti kybernetické bezpečnosti s platnými zákony, předpisy a ústavními požadavky na ochranu soukromí. Je zaveden proces pro hodnocení provádění výše uvedených organizačních opatření a kontrol.

Přístupy k identifikaci, ověřování a autorizaci osob pro přístup k prostředkům a systémům organizace *– Přístupy k identifikaci, ověřování a autorizaci osob pro přístup k prostředkům a systémům organizace.*

Opatření v oblasti informovanosti a školení *– Příslušné informace z organizačních zásad ochrany soukromí jsou zahrnuty do školení a osvětových aktivit pracovníků v oblasti kybernetické bezpečnosti. Poskytovatelé služeb, kteří pro organizaci poskytují služby související s kybernetickou bezpečností, jsou informováni o platných zásadách ochrany osobních údajů organizace.*

Detekce anomálních aktivit a monitorování systémů a prostředků *– Je zaveden proces, který provádí přezkum ochrany osobních údajů v rámci detekce anomálních aktivit a monitorování kybernetické bezpečnosti organizace.*

Činnosti reakce, včetně sdílení informací nebo jiných snah o zmírnění dopadů *– Je zaveden proces, který posuzuje a řeší, zda, kdy, jak a v jakém rozsahu jsou osobní údaje sdíleny mimo organizaci v rámci činností sdílení informací o kybernetické bezpečnosti. Je zaveden proces pro provádění přezkumu ochrany osobních údajů v rámci úsilí organizace o zmírnění kybernetické bezpečnosti* [1].“

4 Vlastní hodnocení rizik kybernetické bezpečnosti pomocí Frameworku

Organizace využívající framework by měly být schopny měřit a přiřazovat hodnoty svým rizikům spolu s náklady a přínosy kroků přijatých ke snížení rizika na přijatelnou úroveň. Čím lépe bude tyto činnosti provádět, tím racionálnější, efektivnější a hodnotnější budou její postupy a investice do kybernetické bezpečnosti.

Pro měření efektivity investic slouží výsledky kybernetické bezpečnosti v rámci jádra frameworku, které podporují sebehodnocení efektivity investic a činností v oblasti kybernetické bezpečnosti následujícími způsoby: *„Rozhodování o tom jak by měly různé části kyberbezpečnostních operací ovlivnit: výběr cílových úrovní implementace, hodnocení přístupu organizace k řízení rizik kybernetické bezpečnosti určením aktuálních*

úrovní implementace, stanovení priorit výsledků v oblasti kybernetické bezpečnosti pomocí vytvoření cílových profilů, určení míry, jaké konkrétní kroky v oblasti kybernetické bezpečnosti dosahují požadovaných výsledků kybernetické bezpečnosti prostřednictvím hodnocení současných profilů a měření stupně implementace katalogů kontrol nebo technických pokynů uvedených jako informativní odkazy [1]."

Organizace by měli být chytré, kreativní a opatrné ve způsobech využívání měření a neměli by spoléhat na uměle ukazatele. Organizacím se doporučuje, aby inovovaly a přizpůsobily způsob, jakým začlení měření do své aplikace Frameworku, s plným vědomím jejich užitečnosti a omezení.

4.1 Identifikace (Identify)

4.1.1 Inventarizace

Organizace by měla inventarizovat hardware, software a firmware. Také se muže rozhodnout zavést centralizovaný inventář kde budou obsaženy všechny systémové komponenty se všech systému organizace. V inventáři by měli být zahrnuty tyto informace: Název systému, vlastníky softwaru, číslo verze softwaru, informace o hardwaru (datum pořízení, cenu, model, sériové číslo, výrobce, informace o dodavateli, typ komponentu, umístění), informace o licenci softwaru a u síťových zařízení ještě název a IP adresu. Ke každé komponentě by měla být taky přiřazena osoba, která je odpovědná za správu této komponenty.

V inventáři by nemělo docházet k duplikacím. Pokud je některý software využívaný ve více systémech, je uveden u každého systému, který ho využívá a musí být zaručeno, že v centralizovaném inventáři bude pouze jedna instance tohoto softwaru.

Inventář by se měl pravidelně aktualizovat, když dochází k instalování nebo odebíraní komponent a při aktualizaci systému. Měla by být zaručena aktuálnost, úplnost, přesnost a dostupnost inventáře.

Měli by se automaticky detekovat neautorizované hardwarové, softwarové a firmwarové komponenty, buď v rámci celého systému nebo u jednotlivých komponent systému. Pokud se zjistí, že se taková komponenta v systému nachází, tak by se mělo provést opatření (zakázat přístup takových komponent k síti, izolovat komponenty nebo informovat příslušné pracovníky).

4.1.2 Řízení toku informací

Řízení toku informací má na starosti, kam můžou informace v rámci systému a mezi systémy putovat, ale nestará se o následný přistup k nim. Řízeni toku informací obsahuje blokování externího provozu, který tvrdí, že pochází z organizace, zabránění přenosu informací kontrolovaných při exportu do internetu, omezení webových požadavků, které nepocházejí z interního webového proxy serveru, a omezení přenosu informací mezi organizacemi na základě datových struktur a obsahu, přenos, který obsahuje: škodlivý kód, informace, které není vhodné uvolňovat ze zdrojové sítě, nebo spustitelný kód, který by mohl narušit nebo poškodit služby nebo systémy v cílové síti.

Mechanismy, které vynucují řízení toku informací, porovnávají atributy bezpečnosti a důvěrnosti spojené s daty a zdrojovými nebo cílovými objekty a reagují, když nejsou v souladu. Měli by být použity chráněné domény zpracování, které umožňují řízení informačních toků mezi prostory zpracovaní a do/z informačních objektů. Mechanismy jednosměrného toku (jednosměrná bezpečnostní brána) lze použít k zabránění exportu dat z domény nebo systému s vyšším vlivem nebo s vyšším stupněm utajení a zároveň k povolení importu dat z domény nebo systému s nižším vlivem nebo bez stupně utajení.

Řízení toku informací by se mělo být schopno dynamicky povolovat nebo zakazovat informační toky na základě měnících se podmínek, úkolů nebo provozních hledisek. Řízení toku informací by mělo být schopno povolovat informační toky na základě metadat, definované organizací, umožňuje jednodušší a efektivnější řízení toků. Také by mělo být zajištěno logické nebo fyzické oddělení informačních toků na základě definovaných dat, tím se zesílí ochrana a umožní používaní přenosové cesty, které nejsou jinak dosažitelné. Mezi typy oddělitelných informací náleží: příchozí a odchozí komunikační provoz, požadavky a odpovědi na služby a informace s různým bezpečnostním dopadem nebo stupněm utajení.

Organice by měla definovat omezení vkládání datových typů (vkládaní datového souboru do jiného souboru nebo používání komprimovaných souborů) zohledňující úrovně vkládání a zakazující úrovně vkládání datových typů, které jsou mimo možnosti kontrolních nástrojů.

Organizace mohou definovat filtr zásad zabezpečení nebo ochrany soukromí pro datové struktury. Filtry mohou omezovat maximální délku souboru, maximální velikost

polí, typy dat/souborů, konkrétní slova, vyjmenované hodnoty rozsahy hodnot dat a skrytý obsah. Organizace mohou implementovat více než jeden filtr, aby splnily cíle řízení toku informací. O použití filtru na jednotlivých tocích by měli rozhodovat správci kteří i daný filtr mohou konfigurovat. Pokud není možnou použít automatizovaný rozhodovací proces muže být použit lidský přezkum.

Při přenosu informací by měla proběhnout autentizace zdrojového a cílového bodu toku informací. Pro správnou autentizaci domény je potřeba aby systémové štítky rozlišovali mezi systémy, organizacemi a jednotlivci zapojenými do přípravy, odesílání, přijímání nebo šíření informací. Toto opatření pomáhá organizacím lépe udržovat linii zpracování osobně identifikovatelných informací při jejich toku systémy a může usnadnit sledování souhlasu, jakož i žádostí o opravu, vymazání nebo přístup od jednotlivců.

Při přenosu citlivých dat, by měla být tato data modifikována např. maskování nebo permutaci. Při přenesu informací mezi různými doménami zabezpečením, převést příchozí data do interního normalizovaného formátu a přetvořit data tak, aby byla v souladu s jejich zamýšlenou specifikací. To vede k zastavení škodlivých útoků a exfiltrace velkých tříd.

4.1.3 Využívání externích systému

Externí systémy jsou systémy, které jsou využívány, ale nejsou součástí organizačních systémů, a u nichž organizace nemá přímou kontrolu nad prováděním požadovaných kontrol nebo nad hodnocením účinnosti kontrol. Externí systémy zahrnují také systémy vlastněné nebo provozované jinými složkami v rámci téže organizace a systémy v rámci organizace s různými hranicemi oprávnění. Organizace mají možnost zakázat používání nebo omezení jakéhokoli typu externího systému nebo jeho součásti nebo zakázat používání určitých typů externích systémů nebo jeho součásti. Veškeré externí systémy by měli být inventarizovány.

Organizace by měla vytvářet, dokumentovat a udržovat důvěryhodné vztahy s externími poskytovateli služeb na základě požadavků, vlastností, faktorů nebo podmínek. Toto může být užitečné při provádění reakce na incidenty nebo při plánování aktualizací.

Organizace by měla povolit oprávněným osobám používat externí systém k přístupu do systému nebo ke zpracování, ukládání nebo přenosu informací pouze když

otestuje že externí systém je v souladu se zásadami a plány organizace v oblasti bezpečnosti a ochrany soukromí a zavedením kontrolních mechanismu těchto zásad. Mělo by se uchovat schválených dohod o připojení k systému nebo o spolupráci se subjektem organizace, který je hostitelem externího systému. Organizace by také měla mýt kontrolu nad šifrovaní dat při přenosu nebo uložení v externím systému. Pokud jsou data uložena v externím sytému měla by být možnost ověřit integritu těchto dat bez přenosu jinam.

Organizace by měla požadovat od poskytovatelů externích systému uvedení funkcí, portů, protokolů a další služeb, které jsou pro použití těchto služeb vyžadovány. Organizace by měla používat externí systémy pouze od poskytovatelů se kterými se nerozchází v zájmech organizace a které dobře otestuje a následně pravidelně kontroluje.

4.1.4 Upřednostňování zdrojů

Identifikace kritické součásti a funkce systému se provede pomocí analýzy kritičnosti. Ne všechny komponenty, funkce, služby systému potřebují významnou ochranu. Při identifikaci kritických systémových komponent a funkcí se berou v úvahu platné zákony, prováděcí nařízení, předpisy, směrnice, politiky, normy, požadavky na funkčnost systému, rozhraní systému a komponent a závislosti systému a komponent. Kritičnost komponent a funkcí se posuzuje z hlediska dopadu selhání komponenty nebo funkce na cíle organizace, které jsou podporovány systémem, jenž tyto komponenty a funkce obsahuje. Analýza kritičnosti se provádí při vývoji, úpravě nebo modernizaci architektury nebo návrhu.

Pokud organizace stanoví že některým systémovým komponentám nelze důvěřovat může reiplementovat nebo vyvinout takovou komponentu. To muže zlepšit zabezpečení.

Procesy by měli mýt přidělenou prioritu, tím nebude docházet k zdržování procesu s větší prioritou. Kvóty zabraňují uživatelům nebo procesům získat větší než předem stanovené množství prostředků.

4.1.5 Role a odpovědnost

Organizace by měla jmenovat vedoucí pracovníka který bude mít na starost koordinovat, vyvíjet, implementovat a udržovat program bezpečnosti informací v rámci celé organizace.

Organizace by měla stanovit požadavky na personální bezpečnost u externích poskytovatelů, vyžadovat, aby dodržovali zásady a postupy personální bezpečnosti, dokumentovat tyto požadavky, vyžadovat, aby externí dodavatel informoval o všech personálních převodech nebo ukončeních externích pracovníků, kteří mají pověření organizace nebo kteří mají systémová oprávnění. Organizace by měla sledovat dodržování těchto požadavků.

4.1.6 Hodnocení rizik

Zavedení programu vnitřních hrozeb, který zahrnuje mezioborový tým pro řešení incidentů souvisejících s vnitřními hrozbami. Tento program zahrnuje kontrolní mechanismy pro odhalování a prevenci škodlivých aktivit zevnitř prostřednictvím centralizované integrace a analýzy technických i netechnických informací s cílem identifikovat potenciální problémy související s hrozbami zevnitř. Tyto programy můžou využívat existenci týmů pro řešení incidentů, které již organizace mohou mít, například týmy pro řešení počítačových bezpečnostních incidentů.

Organizace by měla vytvořit kapacitu pro nasazení vyhledávání kybernetických hrozeb, to vyhledává identifikátory narušení v organizačních systémech, odhaluje, sleduje a likviduje hrozby, které se vyhýbají stávajícím kontrolním mechanismům.

Organizace využívá k analýze rizik informace ze všech zdrojů (např. veřejně dostupné zdroje, open-source informace, měření atd.) k informování o technických rozhodnutích, akvizicích a řízení rizik. Organizace muže také sdílet informace o hrozbách, včetně událostí týkajících se hrozeb (tj. taktik, technik a postupů), s jinou organizací. Tyto informace pak používá pro dynamickou aktualizaci postupu. Pro předvídání a identifikaci rizik muže být využita automatizace např. umělá inteligence.

4.1.7 Hrozby, zranitelnost, pravděpodobnost a dopady jsou využívány k určení rizika

Organizace provádí speciální hodnocení jako je ověřování, validace, monitorování systému, hodnocení vnitřních hrozeb, testování škodlivých uživatelů a dalších forem testování. To pomáhá organizaci zlepšit připravenost tím, že potrénuje schopnosti organizace a uvedou aktuální úroveň výkonnosti jako prostředek pro zaměření opatření ke zlepšení bezpečnosti a ochrany soukromí. Toto hodnocení je prováděnou v souladu s platnými zákony, prováděcími nařízeními, směrnicemi, předpisy, politikami,

normami a pokyny. Organizace si také může nechat udělat kontrolní posouzení externí organizací. Zaměstnáním nezávislé hodnotící subjekty se zvyšuje hodnotu hodnotících kontrol.

Průběžné monitorování na úrovni systému usnadňuje průběžnou informovanost o stavu zabezpečení a ochrany soukromí systému co podporuje rozhodnutí o řízení rizik v organizaci. Podle typu kontroly se určuje frekvence monitorování. Může být použita i automatizace. Ta pomáhá udržovat přesnost, aktuálnost a dostupnost informací z monitorování. Efektivnější je, pokud jsou výstupy průběžného monitorování formátovány tak, aby poskytovaly informace, které jsou konkrétní, měřitelné, realizovatelné, relevantní a včasné.

Kontroly zabezpečení a ochrany soukromí se do systému často přidávají postupně. Tím můžou jednotlivé kontroly nefungovat konzistentně a nekoordinovaně. Při zavádění nové kontroly by mělo být ověřeno, že kontroly fungují konzistentně.

4.1.8 Reakce na rizika jsou identifikovány a upřednostněny

Vypracováním nápravného plánu sytému se dokumentuje plánovaná nápravná opatření organizace k nápravě slabých míst nebo nedostatků zjištěných během hodnocení kontrol a ke snížení nebo odstranění známých zranitelností systému. Při každém vypracování nového nápravného plánu by se měl aktualizovat akční plán.

4.2 Ochrana (Protect)

4.2.1 Správa identit a přihlašovacích údajů

Zásady a postupy identifikace a autentizace se týkají kontrolních mechanismů, které jsou implementovány v rámci systémů a organizací. Hlavní faktor při vytváření těchto zásad a postupů je strategie řízení rizik. Na vytváření by měli spolupracovat programy bezpečnosti a ochrany soukromí. Postupy popisují, jak jsou zásady nebo kontroly prováděny, a mohou být zaměřeny na jednotlivce nebo roli, která je předmětem postupu.

Každý uživatel organizace má jedinečnou identifikaci a autentizaci. K tomu jsou využívány hesla, fyzické autentizátory, biometrické údaje nebo v případě implementace více faktorového ověřování jejich kombinaci. Při implementaci více faktorového ověřování by měl být jeden faktor na samostatném zařízení. Přístup k systémům

organizace je definován jako místní přístup (přístup získán přímým připojením bez použití sítí) nebo síťový přístup (např. vzdálený přístup). Muže být využito jednotné přihlášení, což umožňuje uživateli přihlásit se jednou a získat přístup do více systému.

Pro použití sdílených účtu nebo prostředků by měla být vyžadována individuální ověření to snižuje riziko používání skupinových účtů.

Implementace mechanismu ověřování, které jsou odolné proti opakovatelným ověření. Tito mechanismy využívají protokoly, které používají nonces nebo výzvy, jako jsou časově synchronní nebo kryptografické autentizátory.

Implementace mimo pasového ověřování. Autentizace mimo pásmo znamená použití dvou oddělených komunikačních cest k identifikaci a autentizaci uživatelů nebo zařízení v informačním systému. První cesta je pro ověření uživatelů nebo zařízení a proudí zde informace. Druhá cesta je využita pro ověření autentizace (např. přes mobilní telefon).

Zařízení, které nejsou ve vlastnictví organizace vyžadují jedinečnou identifikaci a ověření. Jsou definována podle typu, zařízení nebo kombinace typu a zařízení. Systémy k tomu využívají např. Mac adresy, nebo protokol TCP/IP a organizační řešení ověřování např. 802.1x a Extensible Authentication Protocol [EAP] nebo server RADIUS. Při navázaní spojení by mělo být použito obousměrné ověřování, které je založeno na kryptografii. Při dynamickém přidělování adres (např. DHCP), by se měli standardizovat informace o pronájmu dobu trvání pronájmu přidělenou zařízením v souladu s definováním organizace.

Při správě systémových identifikátorů nejdřív příslušný pracovníci přidělí oprávnění k jednotlivým identifikátorům. Výběr identifikátoru, který identifikuje jednotlivce, skupinu, roli, službu nebo zařízení, přiřazení identifikátoru určenému jednotlivci, skupině, roli, službě nebo zařízení a zabránění opakovanému použití identifikátorů po dobu definovanou organizací.

U jednotliveckých identifikátorů identifikovat status (např. že se jedná o dodavatele atd.). Při udělování dynamicky identifikátory neznámým entitám, musejí být dodrženy zásady dynamického přidělení definované organizací. Jednotlivé atributy jednoznačně definovaných entit by měli být uloženy v chráněném centrálním úložišti.

Organizace by měla vést seznam běžně používaných, očekávaných nebo kompromitovaných hesel a aktualizovat jej a v případě podezření na přímé nebo nepřímé

kompromitování organizačních hesel a kontrolovat, zda se heslo, které je vytvořené nebo aktualizované uživatelem, nenachází na tomto seznamu. Hesla přenášet pouze kryptograficky chráněnými kanály. Hesla ukládat pomocí funkce odvozeného klíče, nejlépe klíčového hashe. Když dojde k obnovení účtu žádat okamžitou změnu hesla. Mělo být podporováno vytváření dlouhých hesel a heslových frází, včetně mezer a všech tisknutelných znaků a požívaní automatizovaných nástrojů, které pomůžou uživateli s tvorbou hesla. Vyžadovat pravidla pro tvorbu hesla, definované organizací.

Před instalaci systémových komponent by mělo být požadováno poskytnutí jedinečných autentizátorů nebo změna výchozích autentizátorů. Autentizátory by měli mýt stejný stupeň ochrany jakou mají data ke kterým povoluje přístup.

Organizace by měla definovat bezpečnostní kontroly pro řízení rizika kompromitace, když uživatel má účty ve více systémech se stejnými ověřovacími prostředky např. hesla. To může vest k tomu, když je zneužit jeden účet systému, tak můžou být zneužity i ostatní.

Identifikátor a autentizátor by měli být propojeny podle pravidel definovány organizací.

Při použití biometrické ověřování by měli být použity mechanismy které splňují kvalitu posouzení definovanou organizací. Při biometrické ověřování dochází k odchylce a míra, jak velká muže být odchylka je definována organizací. Měli by být použity mechanismy, které detekují prezentační útoky pro autentizaci založenou na biometrických údajích.

Používaní správce hesel je ulehčení zapamatování složitých hesel pro různé systémy, ale je zde nebezpečí zneužití souboru s hesly, které správce hesel vytvořil. Tento soubor se proto musí chránit včetně šifrování hesel a ukládání sbírky offline v tokenu.

Při autentizaci neorganizačních uživatelů, které se připojují do systému, které jsou přístupné veřejnost (např, webové stránky) by měli být přijmu ty takové externí autentizátory které jsou v souladu s požadavky NIST, a dokumentovat a udržovat seznam akceptovaných externích autentizátorů.

Zavést techniky nebo mechanismy, které budou vyžadovat specifické ověřovací informace, když bude zaznamenánu podezřené chování (např. přistupování k většímu množství dat nebo získávaní dat které uživatel nepotřebuje k vykonávání práce), to může znamenat napadení účtu.

4.2.2 Řízení a ochrana majetku pomocí fyzické bezpečnosti

Organizace by měla mýt definované zásady a postupy pro ochranu fyzických zařízení, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba která bude mít na starost řídit vývoj, dokumentaci a šíření zásad a postupů fyzické ochrany a přezkoumat a aktualizovat stávající zásady a postupy fyzické ochrany. Prostředí, kde je vyžadována fyzická ochrana by měli být monitorování např, kamerovým systémem nebo alarmem. Tyto prostředky pomůžou v ochraně prostředí a identifikovat podezřelé chování. Při rozpoznání narušení by měla proběhnout automatická reakce (např. vyrozumění vybraných pracovníků organizace).

Měl by být vypracován a spravován seznam osob s povolením vstupu do zařízení se systémem a těmto osobám vydávat oprávnění. Pro přístup do chráněných prostorů by mělo být vyžadováno dva typy identifikace např. karta a pin. Dále by měly být zaznamenávaný jednotlivé přístupy do těchto prostor (např. identifikační údaje, datum a čas vstupu a výstupu a účel).

Organizace by měla využívat uzamykací schránky, pro přenositelné zařízení jako jsou mobilní telefony, notebooky nebo tablety, které chrání zařízení pře krádeží. Dále by měla být implementována ochrana proti sabotáži fyzických zařízením pomocí např. plomby a nátěry proti neoprávněné manipulaci a programy proti neoprávněné manipulaci, které pomáhají odhalit změny hardwaru způsobené paděláním.

Bezpečnostní kontroly by měli být použity pro systémové rozvody a přenosová vedení zabraňují náhodnému poškození, narušení a fyzické manipulaci. Tyto kontroly mohou být rovněž nezbytné k zabránění odposlechu nebo modifikaci nešifrovaných přenosů.

4.2.3 Správa vzdáleného přístupu

Organizace by měla stanovit a zdokumentovat požadavky na konfiguraci/připojení a pokyny pro implementaci a omezení v používání pro každý typ povoleného vzdáleného přístupu. Každý typ vzdáleného přístupu by měla organizace nejdříve autorizovat a poté teprve povolit připojení takových typů.

Pro odhalování útoků a zajištění zásad pro vzdálený přístup by měli být implementovány automatizované mechanismy pro monitorování a kontrolu metod vzdáleného přístupu. Dále by měli být implementovány kryptografické mechanismy pro ochranu důvěrnosti a integrity relací. Vzdálený přistup by měl probíhat pouze přes autorizované a spravované body řízení přístupu k síti, toto opatření vede k snížení možností pro útok.

Pokud je vzdálený přístup využíván externí organizací měly by organizace zvážit zahrnout požadavky na vzdálený přístupu do dohody o výměně informací.

Před připojení přenositelných zařízení by měla proběhnout autorizace a měli by být stanoveny požadavky na konfiguraci, požadavky na připojení a pokyny pro kontrolu těchto zařízení.

4.2.4 Přístupová oprávnění

Organizace by měla mýt definované zásady a postupy pro přístup k systému, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba která bude mít na starost řídit vývoj, dokumentaci a šíření zásad a postupů přístupu k systému a přezkoumat a aktualizovat stávající zásady a postupy přístupu k systému.

Při správě účtů by nejdříve měli být definovány typy účtu, které jsou povoleny nebo zakázaný a k něm vytvořena dokumentace. Poté by měl být určen správce účtů. Následně určit oprávnění uživatelé systému, členství ve skupinách a rolích a přístupová oprávnění (tj. privilegia (např. správa klíčů nebo správa databází)) a atributy pro každý účet. Dále vyžadováno chválení žádostí o vytvoření účtů. Kromě vytváření by se měli účty upravovat, zakazovat (např. vypršela platnost, nejsou spojeny s uživatelem nebo neaktivita po definovanou dobu) nebo nepotřebné účty odstraňovat a také sledovat používaní jednotlivých účtu. Můžou být využity automatizované mechanismy pro správu účtů které pomáhají s předchozími aktivitami účtu (mohou být použity i pro dočasné účty). Automatické odhlášení po definované době nečinnosti. Ukončit síťové připojení spojené s komunikační relací na konci relace nebo po definované době nečinnosti.

Organizace muže definovat a zdokumentovat akce v systému ke kterým není potřeba identifikace nebo autentizace. Mohou být definované i akce, které běžně vyžadují

identifikaci nebo autentizaci, ale za určitých okolností mohou umožnit obejití identifikačních nebo autentizačních mechanismů. K takovému obejití může dojít například prostřednictvím softwarově čitelného fyzického přepínače, který přikazuje obejít přihlašovací funkci a je chráněn před náhodným nebo nemonitorovaným použitím. Ukončit síťové připojení spojené s komunikační relací na konci relace nebo po definované době nečinnosti.

4.2.5 Ochrana integrity sítě

Dodržování schválených oprávnění pro kontrolu toku informací v rámci systému a mezi připojenými systémy na základě zásad, které organizace schválila (např. kudy se mohou informace pohybovat v rámci systému a mezi systémy nebo omezení webových požadavků). (Viz. kap. 4.1.2 Řízení toku informací)

Organizace může omezit počet souběžných relací podle typu účtu, globálně nebo obojí. Vhodné pro osoby, které pracují v rizikových doménách např. správce systému.

K externím nebo logicky odděleným sítím od vnitřních (demilitarizované zóny nebo DMZ) se připojovat pouze prostřednictvím spravovaných rozhraní tvořených zařízeními pro ochranu (např. brány, směrovače, firewally). K správně vybranému rozhraní stanovit zásady pro provoz toku, chránit důvěrnost a integritu informací přenášených přes rozhraní, dokumentovat každou výjimku z provozu toku s uvedením důvodu (např. obchodní potřebou) a dobu trvaní výjimky následně je odstraňovat.

Na vnějších a na klíčových vnitřních rozhraních v rámci systému sledovat a kontrolovat komunikaci (zabránit neoprávněné výměně provozu s externími sítěmi a filtrovat neoprávněný provoz z vnějších sítí). Všechna síťová komunikace by nejdříve měla být zakázána a následně povolovat pouze nezbytná sítová připojení (omezovat odchozí a příchozí komunikaci na základě autorizovaných zdrojů a cílů.). Zabránit rozdělenému tunelování pro vzdálená zařízení připojující se k systémům organizace, pokud není rozdělený tunel bezpečně zajištěn pomocí ochranou definovanou organizací. Komunikace by měla probíhat pouze přes ověřené Proxy servery. Zabránit infiltraci dat (přenos dat ze systému do jiného systému, kde k nim má přistup neoprávněná osoba). Pro privilegovaný přístup by měla existovat vlastní rozhraní. Adresy rozhraní by měli být tajné (nezveřejňovat síťové adresy, používáním překladu síťových adres nebo nezadáváním adres do systémů doménových jmen). Implementovat mechanismy které

nedopustí že se systémy nedostanou do nezabezpečených stavů, v nichž již neplatí zamýšlené bezpečnostní vlastnosti v případě selhaní rozhraní.

Dále vytvořit dílčí sítě pro veřejně přístupné součásti systému, které jsou fyzicky nebo logicky odděleny od vnitřních sítí. Také izolovat bezpečnostní nástroje, mechanismy a podpůrné prvky od zbytku sítě pomocí rozhraní.

Ukončit sítové připojení na konci komunikační relace nebo při době nečinnosti určené organizací.

4.2.6 Identita (ověřování, vazba na přihlašovací údaje, uplatnění v interakcích)

Organizace by měla mýt prostředky pro propojení atributu zabezpečení a ochrany (typy definované organizací) k hodnotě (Hodnoty definované organizací) pro informace v úložišti, v procesu a/nebo při přenosu. Přiřazený atribut by měl být uložený s informací. Pro jednotlivé systémy organizace by měli být atributy přiřazeny zvlášť včetně povolených/rozsahu hodnot. Při změně charakteristiky bezpečnosti nebo ochrany informací v průběhu času je potřeba dynamicky měnit tyto atributy. Tyto změny a přiřazovaní jednotlivých atributů by měly provádět pouze určené a prověřené osoby. Mohou být využity i technologie a techniky, které poskytují různé úrovně zabezpečení. Tyto atributy by měli být zobrazovaný (na výstupných zařízení) společně s objekty které systém přenáší. (Viz. kap. 4.2.1 Správa identit a přihlašovacích údajů)

4.2.7 Zabezpečení dat

Přístup k jednotlivým typům medií (digitální: pevné disky, flash paměti, …; nedigitální, papíry, fotky, …) které organizace definuje, omezit na určité pracovníky nebo role. Systémová media by měla mýt označení s uvedením: omezení distribuce, upozornění na zacházení a případné bezpečnostní značky. Typy medií vybrané organizací by se měly fyzicky kontrolovat a bezpečně ukládat v kontrolovaných a zabezpečených oblastech organizace, kde můžou být zaznamenávané povolené přistup a jednotlivé přístupy, a takto je chránit, dokud nejsou zničená.

Při přepravě vybraných medií určit odpovědné osoby a dokumentovat proces přepravy.

Před likvidací, uvolněním mimo kontrolu organizace nebo uvolněním k opětovnému použití by se měli vymazat uložená data pomocí technik které odpovídají utajení dat. Takto vyčištěná media by měli být dokumentovány.

Organizace mohou omezit používaní přenosných zařízení.

4.2.8 Ochrana dat při přenosu

Organizace by měla chránit integritu a důvěryhodnost přenášených informací pomocí fyzické ochrany: použitím chráněných distribučních systémů zahrnuje terminály a odpovídající elektromagnetické akustické, elektrické a fyzické kontroly a logické pomocí šifrovacích technik např. techniky IPsec nebo TLS. Šifrované by měli být i externí části zprávy. Může být využito skrytí nebo náhodné uspořádání komunikačních vzorů, které zajišťuje ochranu před neoprávněným vyzrazením informací. Organizace také muže zajistit důvěryhodnou komunikační cestu (logickou nebo fyzickou) pro komunikaci mezi uživatelem a důvěryhodnými součástmi systému a tuto cestu umožnit vybraným uživatelům vyvolat k bezpečnostními funkcemi systému které má organizace přiřazené.

4.2.9 Dostatečná kapacita pro zajištění dostupnosti

Při plánování uložiště pro AUDIT LOG (dokument, který zaznamenává události v systému (obvykle obsahují cílové a zdrojové adresy, časové razítko a přihlašovací údaje uživatele)) musí organizace zvážit typ auditního logu a podle toho naplánovat dostatečnou kapacitu a tím snížit riziko že tato kapacita bude překročena a povede k potenciální ztrátě nebo omezení schopnosti vedení audit logu. Pro získání větší kapacity muže organizace zvolit frekvenci kterou bude probíhat přenos logů se systému do externího média.

Při výpadku primárního zdroje napájení zajištění náhradního zdroje napájení, který buď bezpečně vypne systém nebo ho převede na náhradní zdroj energie, který dokáže udržet alespoň minimální požadovanou provozní schopnost.

Organizace by měla mýt nasazeny mechanismy které omezení jednotlivci provádět útoky na odepření služby. Měla by být implementována taky dostatečná kapacita a šířka pásma a také vytvořena redundance spojení. Dále nasadit mechanismy pro detekci indikátorů útoků typu odepření služby (zavedení diskových kvót, konfigurace systémů tak, aby automaticky upozorňovaly správce na dosažení určitých prahových hodnot

kapacity úložiště, používání technologií komprese souborů pro maximalizaci dostupného úložného prostoru a zavedení oddělených oddílů pro systémová a uživatelská data).

4.2.10 Implementace ochrany proti uniku dat

Organizace by měla sledovat informace z otevřených zdrojů a/nebo z informační stránek které organizace definuje s pravidelnou frekvencí (doba frekvence je závislá na organizaci) pokud je zjištěno vyzrazení je potřeba uvědomit odpovědnou osobu a provést opatření definované organizací. Je možno použit automatizačních nástrojů, které pomocí skriptu prohledávají vyprané zdroje.

Systém by měl být chráněn před únikem informací v důsledku vyzařování elektromagnetických signálů.

4.2.11 Ověření integrity softwaru, firmware a informací

Organizace by měla používat nástroje pro ověřování integrity (zjištění neoprávněné změny) softwaru, firmwaru a informací a při zjištění změny provést akce definované organizací. Kontrola integrity by měla probíhat při přechodných stavů (spuštění, restart, vypnutí a přerušení systému) systému nebo událostí. Možnost využití automatizačních nástrojů (pro informovaní odpovědné osoby i pro automatické reakce systému např. vypnutí). Při zjištění potenciálního porušení integrity: vytvořit auditní záznam; upozornit aktuálního uživatele; upozornit odpovědnou osobu a provést akce. Možnost implementace kryptografické mechanismů pro detekci neoprávněných změn. Kontrola integrity před spuštěním programu instalovaného uživatelem.

Kontrola platnosti informačních vstupů (platné syntaxe a sémantiky, ověřuje, zda vstupy odpovídají stanoveným definicím formátu a obsahu). Toto opatření zabraňuje útokům, jako je cross-site scripting a různé injection útoky.

4.2.12 Oddělení testovacího prostředí od produkčního

Udržovat konfigurace pro vývojová a testovací prostředí systému odděleně od základní konfigurace. Tím organizace ochrání systémy před neplánovanými nebo neočekávanými událostmi souvisejícími s vývojovými a testovacími činnostmi.

4.2.13 Konfigurace informačních systémů

Organizace by měla mýt definované zásady a postupy pro správu konfigurace, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba která bude mít na starost: řídit vývoj, dokumentaci a šíření zásad a postupů správy konfigurace a přezkoumat a aktualizovat stávající zásady a postupy správy konfigurace.

Organizace by měla vytvořit, zdokumentovat a udržovat pod kontrolou aktuální základní konfiguraci systému. Poté by měla přezkoumávat a aktualizovat základní konfiguraci systému v určitých frekvencích, podle okolností (obojí definované organizací) a při instalaci nebo aktualizaci systémových komponent. Automatické mechanismy pomáhají udržet aktuálnost, úplnost, přesnost a dostupnost základní konfigurace systému (např. sledování čísel verzí operačních systémů, aplikací, typů nainstalovaného softwaru nebo aktuálních úrovní oprav). Uchovávat určitý počet předešlých konfigurací pro podporu zpětné obnovy.

Při změně konfigurace systému by nejdříve měly být určeny a zdokumentovány typy změn systému, které by nová konfigurace přinesla. Následně tyto změny přezkoumat (Před implementací by mělo proběhnout testování v testovacím prostředí pro odhad všech dopadů.) a buď je přijmou nebo zamítnou a vytvořit dokumentaci o těchto změnách a ty následně uchovat po určenou dobu. Implementovat schválené změny a následně sledovat a přezkoumávat činnosti spojené s těmito změnami.

Implementaci změn by měli provádět pouze kvalifikované a oprávněné osoby. Měly by se vytvářet automaticky auditní záznamy. Muže být vyžadována i dvojí autorizace.

Konfigurace systému by měla obsahovat pouze základní funkce které organizace potřebuje a zakázat nebo omezit používání funkcí, portů, protokolů, softwaru a služeb, které organizace nepotřebuje. To vede k větší ochraně. Povolené funkce by se měli dále pravidelně přezkoumávat a znovu určit, zda jsou potřebné nebo bezpečné. U vypraných programů může být určeno: zákaz funkcí automatického spouštění, omezení rolí, které mohou schvalovat spouštění programů, povolení nebo zákaz konkrétních softwarových programů nebo omezení počtu instancí programů spouštěných současně.

4.2.14 Zálohování informací

Organizace by měla mýt zřízené náhradní úložiště četně nezbytných dohod umožňujících ukládání a vyhledávání záložních informací systému a také by mělo poskytovat rovnocennou kontrolu jako primární úložiště. Náhradní uložiště by mělo být dostatečně odděleno, aby se snížila náchylnost k hrozbám. Náhradní uložiště by mělo být nakonfigurováno tak aby co nejvíce usnadňovalo obnovu.

Organizace by měla provádět zálohování systémových a uživatelských informací a systémové dokumentace v určitých frekvencích. Mělo by probíhat pravidelné testování spolehlivosti zálohovacích medií a integrit zálohovaných informací. Pro zjištění, zda je obnova informací spolehlivá je potřeba při testování havarijního plánu vybrat vzorek zálohovaných informací při obnově vybraných funkcí systému. Velikost vzorku závisí na organizaci. Při mazaní nebo úpravě zálohovaných informací může být vyžadována dvojí autentizace. Zálohované informace by měli být chráněny kryptografické mechanismy.

4.2.15 Vylepšené ochranné procesy

Krom automatizačních technik testování zranitelnosti systému je možné provádět penetrační testování. Penetrační testování je mnohem učenější než automatizované mechanismy. Penetrační testování je prováděno pracovníky nebo týmy s prokazatelnými dovednostmi a zkušenostmi. Ty se pokouší napodobit útočníky a zjistit zranitelnost systému. Tyto osoby by měli být nejlépe nezávislé na organizaci.

Pro správnou reakci na incident by měl být vyvinut plán reakce na incidenty. Plán reakce obsahuje plán zavedení schopnosti reakce, popisuje její strukturu a organizaci, jak zapadá do celkové organizace, dále definuje incidenty, metriky pro měření schopnosti reakce na incidenty, obstarává sdílení informací o incidentech a určuje odpovědnost za reakci na incident.

Organizace muže provádět testy na reakce na incidenty. Z testů mohou vyplívat dopady jednotlivých incidentů na organizaci. Toto testovaní muže probíhat mocí automatizovaných mechanismů. Na výsledcích testování muže být aktualizován plán reakce na incidenty.

4.2.16 Plány obnovy

Organizace by měla zřídit náhradní místo zpracování, včetně nezbytných dohod, které umožní přenos a obnovení systémových operací pro základní úkoly a obchodní funkce při nedostupnosti primárních zpracovatelských kapacit. V náhradním místě by měli být prováděny stejné kontroly jako v primárním místě. Náhradní místo by mělo být dostatečně odděleno, aby se snížila náchylnost k hrozbám.

Obnova sytému do určeného stavu po narušení, ohrožení nebo selhání by měla proběhnout do určené doby.

4.2.17 Údržba

Organizace by měla mýt definované zásady a postupy pro údržbu a opravy, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba která bude mít na starost: řídit vývoj, dokumentaci a šíření zásad a postupů údržby a oprav a přezkoumat a aktualizovat stávající zásady a postupy údržby a opravy.

Pro údržbu, opravy a výměny součástí systému by se mělo plánovat, dokumentovat a následně kontrolovat záznamy. Jednotlivé operace by měla schvalovat oprávněná osoba. Při opravě mimo organizaci provést sanitaci dat ze zařízení. Po údržbě, opravě nebo výměně zkontrolovat, zda všechny ovládací prvky fungují správně.

Pro jednotlivé nástroje údržby (např. hardwarové a softwarové diagnostické testovací zařízení a paketové sniffery, "ping", "ls", "ipconfig") by se mělo schvalovat, kontrolovat (zda nejsou nesprávně nebo neoprávněně upravovány, nebo na mediích není škodlivý kód nebo zda má software nejnovější aktualizace) a monitorovat (k čemu jsou nástroje používány (hlavně u nástrojů které pracují s informacemi)) používání.

Pro důležité části by se měly provádět pravidelná preventivní údržba (systematickou kontrola, zkoušky, měření, seřizování, výměnu dílů, zjišťování a odstraňování počínajících poruch) a prediktivní údržbu (systematickou kontrolu, zkoušky, měření, seřizování, výměnu dílů, zjišťování a odstraňování počínajících poruch).

4.2.18 Vzdálená údržba

Pro vzdáleno údržbu (prostřednictvím externí nebo interní sítě) by se měly schvalovat a monitorovat prováděné činnosti. Nástroje vzdálenou diagnostiku a údržbu by měly být schvalovány. Při vytváření nelokálních relací údržby a diagnostiky používat silné ověřování, vést záznamy o nelokálních činnostech údržby a diagnostiky a ukončovat relace a síťová připojení po dokončení nelokální údržby. Pro relaci údržby by měla být použity autentizátory a oddělit relaci údržby od ostatních relací bud fyzicky nebo logicky. Každá relace by měla být chválená odpovědnou osobou. Měla by být implementována kryptografická ochrana. Po ukončení relace by mělo být ověřena, zda je opravdu ukončena.

4.2.19 Ochranné technologie – audit log záznamů

Organizace by měla mýt definované zásady a postupy pro audit log záznamy, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba, která bude mít na starost řídit vývoj, dokumentaci a šíření zásad a postupů pro audit log záznamy a přezkoumat a aktualizovat stávající zásady a postupy pro audit log záznamy.

Organizace by měla určit typy událostí které se mají protokolovat a zároveň je musí umět systém sám zaznamenávat (např. změny hesel, neúspěšná přihlášení, změny bezpečnostních atributů) a pro každou událost zdůvodnit, jak muže pomoci při vyšetřování incidentu. Koordinovat funkci protokolování událostí s ostatními organizačními subjekty, které vyžadují informace související s audit logem.

Audit log my měl obsahovat: Jaký typ události nastal; Kdy k události došlo; Kde k události došlo; Zdroj události; Výsledek události a Identita všech osob, subjektů nebo předmětů spojených s událostí. Muže obsahovat další informace, které stanoví organizace. Omezit osobně identifikovatelné informace obsažené v auditních záznamech pouze na potřebné pro provozní účely.

Jednotlivé audit logy by měli být přezkoumány a analyzovány kvůli indikaci nevhodné nebo neobvyklé činnosti a potenciálního dopadu této činnost. Zjištění by mělo být oznámeno odpovědné osobě. Toto muže být prováděno automatickými mechanismy. Při zjištění změny rizika je potřeba upravit úroveň přezkoumání a analýzy. Pro potřeby

analýzy mohou být použity mechanismy, které informace z audit logu uspořádávají je do souhrnného formátu, který je pro analytiky smysluplnější. Tyto redukce nesmí měnit význam původních informací.

4.2.20 Ochrana komunikačních a řídicích prvků

Pokud je v systému použita kryptografie, zřizování a spravování kryptografických klíčů by mělo být v souladu s požadavky které definuje organizace. Tyto požadavky by měli být v souladu s platnými zákony, prováděcími příkazy, směrnicemi, nařízeními, zásadami, normami a pokyny.

Pro mobile code (zahrnuje jakýkoli program, aplikaci nebo obsah, který může být přenášen přes síť (např. vložen do e-mailu, dokumentu nebo webové stránky) a spuštěn ve vzdáleném systému) je definováno, který je přijatelný a který ne. Používání mobile code by mělo být autorizováno, monitorováno a kontrolováno. Když dojde k identifikaci nepřijatelného mobilního code měli by nastat nápravná opatření (např. zablokování) podle organizace. Mělo by být zabráněno stahování a automatickému spouštění mobile code.

Pro ověření původu a integrity informace o překladu názvu hostitele/služby na síťovou adresu získané prostřednictvím služby můžou být poskytnuty další artefakty ověřování původu dat a integrity spolu s daty autoritativního rozlišení názvů, které budou vraceny společně s odpovědí. Dále poskytnout prostředky pro označení stavu zabezpečení podřízených zón a (pokud podřízená zóna podporuje služby bezpečného rozlišení) umožnit ověření řetězce důvěry mezi nadřazenými a podřízenými doménami, pokud fungují jako součást distribuovaného hierarchického jmenného prostoru. Při překladu adres muže být vyžadováno ověření původu a integrity dat u odpovědí na překlad jmen/adres, které systém dostane z autoritativních zdrojů. Systémy pro překlad názvu a adres by měly být redundantní servery nejlépe v různých geografických oddělených podsítí. Dále mohou být rozděleny na ty které zpracovávají požadavky od interních klientu a na ty co od externích klientů.

Pro zabezpečení relace zajistit, aby při odhlášeni uživatele nebo jiného ukončení byla relace zneplatněna. Dále by pro každou relaci měl být vytvořen jedinečný identifikátor a měly by být uznávány pouze identifikátory vytvořené systémem. Při vytváření relaci povolit pouze certifikáty povolené organizací.

Analýzou a testováním skrytých kanálů může organizace zjistit kudy můžou případně unikat informace. Můžou omezit šířku pásma skrytých kanálů.

Pro organizační velení a řízení provozu systému zajistit náhradní komunikační cesty. Náhradní komunikační cesty snižují riziko, že všechny komunikační cesty budou ovlivněny stejným incidentem. Náhradní cesty značně usnadní schopnost pokračovat v činnosti a přijímat vhodná opatření během incidentu.

4.2.21 Implementace mechanismů pro dosažení požadované odolnosti

Pro vyšší odolnost systému by měla organizace zajistit používání alternativních komunikačních protokolů.

Když nastane určité podmínka, která je definována organizací, mě by systém přejít do bezpečného režimu provozu. Při tomto stavu je povoleno používat pouze funkce definované systémem. Tento režim může být aktivován automaticky nebo ručně.

Pro kritické funkce můžou být využity alternativní bezpečnostní mechanismy, které zastoupí činnost hlavních bezpečnostních mechanismů, když nejsou k dispozici nebo jsou ohroženy.

4.3 Detekce (Detect)

4.3.1 Anomálie a události

Tato část je zaměřena na skenování a monitorování zranitelností systému a využívaných aplikací. K tomu využívat nástroje a technik, které usnadňují interoperabilitu mezi nástroji a automatizují části procesu správy zranitelností pomocí standardů pro: vyjmenování platforem, chyb software a nesprávných konfigurací, formátování kontrolních seznamů a testovacích postupů a měření dopadu zranitelností. Zprávy a výsledky z těchto operací analyzovat a zjištěné zranitelnosti odstranit. Tyto informace sdílet s ostatními odpovědnými pracovníky, aby mohly být odstraněni podobné zranitelnosti v ostatních systémech. Při objevení nových zranitelností přidat novou zranitelnost do seznamu zranitelností, které mají být sledovány.

Při řešení incidentu by měla proběhnout analýza škodlivého kódu a/nebo jiných zbytkových artefaktů, které zůstaly v systému po incidentu. To může poskytnout organizaci vhled do taktiky, technik a postupů protivníka. Může také naznačit identitu

nebo některé charakteristické rysy protivníka. Kromě toho může analýza škodlivého kódu pomoci organizaci při vývoji reakcí na budoucí incidenty.

4.3.2 Shromažďování dat o událostech

Občas je potřeba k identifikování např. kybernetického útoku spojit různé informace z různých zdrojů, včetně různých hlášení. Tím pádem může organizace lépe řešit kybernetické hrozby. Organizace může korelovat a sdílet určité informace s externí organizací. To opět vede k lepšímu porozumění kybernetických útoků a pomáhá zlepšit reakce na incidenty.

Dokumentace incidentů by měla obsahovat vedení záznamu veškerých incidentů, stavu incidentu a dalších relevantních informací potřebných pro forenzní analýzu, jakož i vyhodnocování podrobností o incidentech, trendech a způsobech řešení. Tyto informace lze získat z monitorování sítě, hlášení o incidentech, týmů pro řešení incidentů, stížností uživatelů, monitorování auditů, monitorování fyzického přístupu a hlášení uživatelů a správců. Lze tomu využít automatické mechanismy.

4.3.3 Bezpečnostní monitoring

Při požívání softwaru by měli být dodrženy smluvní ujednání a zákony o autorských právech. Mělo by být sledováno používání softwaru a související dokumentace chráněné množstevními licencemi za účelem kontroly kopírování a distribuce. Také by se mělo kontrolovat a dokumentovat používání technologie sdílení souborů peer-to-peer, aby bylo zajištěno, že tato možnost nebude využívána k neoprávněnému šíření, zobrazování, předvádění nebo rozmnožování děl chráněných autorským právem. Mělo by být stanoveno omezení pro požívání open-source softwaru, kvůli problematické nápravě zranitelnosti a s tím spojeny i licenční problémy, včetně omezení pro odvozené použití takového softwaru.

Při instalaci softwaru by měli být stanoveny zásady (např. povolené instalace softwaru zahrnují aktualizace a stahování nových aplikací z "obchodů s aplikacemi" schválených organizací nebo zakázané software s neznámým nebo podezřelým původem). Tyto zásady by se měli prosazovat a sledovat. Možné využít automatické mechanismy. Instalace software může být umožněna pouze privilegovaným rolím.

4.3.4 Detekce škodlivého kódu

Pro zjištění škodlivého kódu nasadit schopnost detonační komory (umožňují organizacím otevírat přílohy e-mailů, spouštět nedůvěryhodné nebo podezřelé aplikace a provádět požadavky na univerzální vyhledávač zdrojů v bezpečí izolovaného prostředí nebo virtualizovaného sandboxu, zde dojde k identifikaci škodlivého kódu).

Implementace mechanismů ochrany proti škodlivému kódu na vstupních a výstupních bodech systému (firewally, servery pro vzdálený přístup, pracovní stanice, servery elektronické pošty, webové servery, proxy servery, notebooky a mobilní zařízení), které mají za úkol detekovat a odstranit škodlivý kód. Tyto mechanismy by se měli automaticky aktualizovat, když budou k dispozici nové verze, které splňují zásady organizace. Aktualizaci by měla provádět pouze privilegovaná osoba. Skenovat pravidelně systém a v reálném čase soubory z externích zdrojů. Při detekci provést příslušnou akci (např. blokování). Při špatné detekci škodlivého kódu se snažit přijít na důvod a definovat dopady pro společnost.

Ochrana proti spamu vyžaduje nasazení mechanismů ochrany proti spamu na vstupních a výstupních bodech systému za účelem detekce a reakce na nevyžádané zprávy. Tyto mechanismy by se měli automaticky aktualizovat. Můžou být nasazeny i mechanismy s učením např. Bayesovské filtry.

4.3.5 Monitorování činností externích služeb

Mělo by být vyžadováno, aby tvůrce systému, systémové komponenty nebo systémové služby poskytl popis funkčních vlastností kontrol, které mají být implementovány. Dále by měl být požadován plán, který popisuje monitorovaní účinnosti kontrol. Tento plán musí být v souladu s programem průběžného monitorování organizace.

Mělo by být vyžadováno, aby dodavatelé externích systémových služeb splňovali požadavky organizace na bezpečnost a používali kontrolní mechanismy, které definuje organizace. Tyto služby by měli podléhat dohledu organizace a k tomu využívat procesy, metody a techniky k průběžnému sledování dodržování kontrol ze strany poskytovatelů.

4.3.6 Detekční procesy

Organizace by měla mýt definované zásady a postupy pro posuzování, autorizaci, monitorování, integritu systému, informace, související kontroly integrity systému a informací, řízení rizik dodavatelského řetězce a souvisejících kontrolních mechanismů řízení rizik dodavatelského řetězce, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba která bude mít na starost řídit vývoj, dokumentaci a šíření zásad a postupů pro tyto aktivity a přezkoumat a aktualizovat stávající zásady a postupy pro tyto aktivity.

Zavedení programu ochrany proti neoprávněné manipulaci se systémem, systémovou komponentou nebo systémovou službou. Detekcí, identifikace a odolnost má zásadní význam pro ochranu systémů a součástí během distribuce a používání. Používat technologie, nástroje a techniky proti neoprávněnému vniknutí v průběhu celého životního cyklu vývoje systému.

4.4 Reakce (Respond)

4.4.1 Plán reakce je proveden během nebo po incidentu

Organizace by měla zavést schopnost zvládání incidentů, která je v souladu s plánem reakce na incidenty a zahrnuje přípravu, detekci a analýzu, zvládnutí, likvidaci a obnovu. Pro efektivní schopnost řešit incidenty zahrnuje koordinaci mezi mnoha organizačními subjekty. Zkušenosti nabité při řešení incidentu aplikovat do postupů reakce na incidenty. Lze pro řešení incidentů zavést automatické mechanismy. Dále je možné pro určité součásti systému zavést dynamickou rekonfiguraci (zahrnuje změny pravidel směrovače, seznamů řízení přístupu, parametrů systému detekce nebo prevence narušení a pravidel filtrování firewall) a dynamickou reakci (má na starosti včasné nasazení nových nebo náhradních organizačních schopností v reakci na incidenty). To může např. zastavit útok nebo přeměřovat útočníky. Pro jednotlivé skupiny incidentů (poruchy způsobené chybami, cílený útok atd.) by měli být definovány akce co se systémem stane (např. vypnutí nebo aktivace alternativních technologií). Schopnost řešení incidentů by se měla taky týkat vnitřních hrozeb.

4.4.2 Analýza reakcí

Organizace by měla posoudit rizika kde stanoví: identifikaci hrozeb, zranitelnosti systému, určení pravděpodobnosti a rozsahu škod způsobených: neoprávněným přístupem, použitím, vyzrazením, narušením, modifikací nebo zničením systému, informací, které zpracovává, uchovává nebo přenáší, a všech souvisejících informací. Také by měla určit jaký dopad bude na jedince při zpracování informací umožňujících osobní identifikaci. Zjištěné výsledky by měla integrovat do procesu řízení rizik a tyto výsledky zdokumentovat. Výsledky by měli být rozšířeny v rámci organizace odpovědným osobám. Tyto informace o rizicích by měla organizace buď pravidelně nebo když dojde k výrazným změnám v systému aktualizovat.

4.4.3 Procesy pro příjem, analýzu a reakci na zranitelnosti

Organizace by měla mýt definované zásady a postupy pro hodnocení rizik, které budou řešit účel, rozsah, role, odpovědnosti, závazek vedení, koordinaci mezi organizačními jednotkami a dodržování předpisů a budou v souladu s platnými zákony, směrnicemi, nařízeními a normami. Měla by být určena odpovědná osoba která bude mít na starost řídit vývoj, dokumentaci a šíření zásad a postupů pro hodnocení rizik a přezkoumat a aktualizovat stávající zásady a postupy pro hodnocení rizik.

Organizace by měla co nejvíce usnadnit zaměstnancům v oblasti bezpečnosti a ochrany soukromí průběžné vzdělávání a školení. Dále by měla udržovat aktuální doporučené postupy, techniky a technologie v oblasti bezpečnosti a ochrany soukromí. Může navázat a institucionalizovat kontakty s vybranými skupinami a sdruženími v rámci komunit zabývajících se bezpečností a ochranou soukromí. S těmi to skupinami navzájem sdílet informace o hrozbách, zranitelnostech a incidentech, jakož i kontextové poznatky, techniky zajišťování shody a problémy v oblasti ochrany soukromí v souladu s platnými zákony, prováděcími příkazy, směrnicemi, politikami, předpisy, normami a pokyny.

Při reakci na zjištění plynoucí z hodnocení bezpečnosti a ochrany osobních údajů, monitorování nebo auditů, je rekce také ovlivněna mírou tolerance organizace k riziku.

Organizace by měla průběžně přijímat bezpečnostní výstrahy, doporučení a směrnice systému od zvolených externích organizací. vytvářet interní bezpečnostní výstrahy, doporučení a směrnice podle potřeby a ty následně rozesílat v organizaci odpovědným osobám. Vykonávání bezpečnostních směrnic by mělo být vykonáváno v určitém

časovém období anebo by mělo být oznámeno vydávající organizaci míru jejich nedodržení [2].

5 Analýza legislativního kyberneticko-bezpečnostního rámce České republiky

Kybernetická bezpečnost České republiky je v současné době řešena zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který vstoupil v platnost dne 29. srpna 2014 s účinností od 1. ledna 2015. Tento zákon prošel dvěma obsahově významnými novelizacemi. První novela rozšířila okruh povinných osob spadajících pod Zákon o Kybertické Bezpečnosti o provozovatele informačních systémů a dále upravila některé sankce. Druhá novela implementovala Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS). Společně s tímto zákonem byly vypracovávány i prováděcí právní předpisy, konkrétně:

• vyhláška č. 316/2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti);

• vyhláška č. 317/2014, kterou se stanoví významné informační systémy a jejich určující kritéria;

• vyhláška č. 315/2014, novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

S novelami zákona došlo i k novelizaci prováděcích právních předpisů a vytvoření předpisu nového. Konkrétně se jedná o:

• vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti);

• vyhlášku č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Další dílčí aspekty kybernetické bezpečnosti lze nalézt i v jiných právních předpisech.

5.1 Vstupní analýza legislativního rámce kybernetické bezpečnosti ČR

Zákon o kybertické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Dále zpracovává předpisy Evropské unie a upravuje zajištění bezpečnosti sítí elektronických komunikací a informačních systémů. Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

5.1.1 Subjekty patřící pod legislativní rámec kybernetické bezpečnosti ČR

Poskytovatel služby elektronických komunikací („spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize[4]“) **nebo subjekt zajištující sít elektronických komunikací**(„přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, které umožňují přenos signálů po vedení, rádiem, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace“[4])

orgán nebo osoba zajišťující významnou síť („zajišťují přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře“ [5])

správce („orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému [5]“) **a provozovatel informačního a komunikačního systému kritické informační infrastruktury**(„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu [3].“)

správce a provozovatel významného informačního systému („informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci [5]“)

správce a provozovatel informačního systému základní služby („jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností např. v energetice nebo dopravě [5]“)

provozovatel základní služby („je určena Národním úřadem pro kybernetickou a informační bezpečnost“[5])

poskytovatel digitální služby (on-line tržiště, internetového vyhledávače, cloud computingu)

Krom výše uvedených subjektů mohou se do kybernetické bezpečnosti připojit i další právnické nebo fyzické osoby.

5.1.2 Vybraná dílčí ustanovení z legislativního rámce kybernetické bezpečnosti ČR

5.1.2.1 Bezpečnostní opatření

Bezpečnostní opatření jsou úkony, který mají za cíl zajistit bezpečnost informací v informačních systémech a dostupnost a spolehlivost služeb a sítí elektronických komunikací v kybernetickém prostoru. Bezpečnostní opatření se dělí na organizační a technická opatření. Subjekty c) až e) mají povinnost zavést a provádět bezpečnostní opatření v takovém rozsahu, který zajití kybernetickou bezpečnost informačních a komunikačních sytému. Pro zavedené bezpečnostní opatření mají povinnost vést dokumentaci. Tyto bezpečnostní požadavky jsou povinny zohlednit ve výběru dodavatele informačního nebo komunikačního systému a tyto požadavky uvést ve smlouvě s dodavatelem.

Poskytovatel digitální služby je povinen zavést a provádět taková bezpečnostní opatření týkajících se sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby. Tyto bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.

Orgány veřejné moci jsou povinny zařadit poptávaný cloud computing do bezpečnostní úrovně na základě informačního nebo komunikačního systému podle

prováděcího právního předpisu a zajistit dodržování bezpečnostních pravidel a dále že budou k dispozici na základě žádosti, informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. Orgán veřejné moci a poskytovatel cloud computingu si ve smlouvě dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel a realizaci bezpečnostní politiky odběratele.

5.1.2.2 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací1) v důsledku kybernetické bezpečnostní události [5]. *“*

Subjekty b) až e) mají povinnost detekovat kybernetické bezpečnostní události. Tyto subjekty mají taky povinnost hlásit kybernetické bezpečnostní incidenty bezodkladně (*„není určeno v jakém konkrétním časovém okamžiku je třeba konat“*[3]) po jejich detekci. Pokud dopad incidentu má dopad na poskytování základní služby musí to provozovatel této služby ohlásit Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Subjekty b) a g) hlásí tyto incidenty provozovateli národního CERT (Computer Emergency Response Team) a subjekty c) až f) hlásí NÚKIB. Subjekty nepodléhající tomuto zákonu mohou také hlásit incidenty buď CERT nebo NÚKIB.

NÚKIB vede evidenci kybernetických incidentů. Tato evidence obsahuje: hlášení kybernetického bezpečnostního incidentu, identifikační údaje systému, ve kterém se kybernetický bezpečnostní incident vyskytl, údaje o zdroji kybernetického bezpečnostního incidentu a postup při řešení kybernetického bezpečnostního incidentu a jeho výsledek.

5.1.2.3 Kontrola a náprava opatření

NÚKIB provádí kontroly v oblasti kybernetické bezpečnosti. Kontrola spočívá v zjištění jak subjekty a) až f) plní své povinnosti definované v tomto zákoně. Kontrola probíhá podle kontrolního řádu a kontrolu provádějí pověření zaměstnanci NÚKIB.

Pokud NÚKIB zjistí nedostatky dá subjektu lhůtu, do které má být nedostatek odstraněn a může být určen i způsob. Pokud je kvůli nedostatkům ohrožen, informační nebo komunikační systém kyberneticky bezpečnostním incidentem tak že může dojít k jeho poškození nebo zničení může kontrolní orgán zakázat kontrolovanému subjektu používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.

5.2 Vyhláška o kybernetické bezpečnosti (VoKB)

„Tato vyhláška zapracovává Směrnici NIS a pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje:

- *obsah a strukturu bezpečnostní dokumentace,*
- *obsah a rozsah bezpečnostních opatření,*
- *typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,*
- *náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,*
- *náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,*
- *vzor oznámení kontaktních údajů a jeho formu,*
- *způsob likvidace dat, provozních údajů, informací a jejich kopií.* [6]“

5.3 Vybraná dílčí ustanovení z vyhlášky o kybernetické bezpečnosti

5.3.1 Systém řízení bezpečnosti informací

VoKB definuje Systém řízení bezpečnosti informací (ISMS – Information Security Management System) jako „*část systému řízení, která je založená na přístupu k rizikům informačního a komunikačního systému a stanovuje způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat*[7]“.

Povinná osoba stanoví rozsah systému řízení bezpečnosti informací a určí organizační části a aktiva, kterých se systém týká, stanoví cíle systému, pro stanovený rozsah zavede bezpečnostní opatření, řídí rizika viz. dále, vytvoří a schválí bezpečnostní politiku (obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu

k řízení bezpečnosti informací), zajistí provedení auditu, zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, průběžně identifikují a řídí významné změny, aktualizují systém řízení bezpečnosti informací a příslušnou dokumentacím řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenávají.

5.3.2 Řízení rizik

Povinná osoba stanoví metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik, podle aktiv identifikuje relevantní hrozby a zranitelnost, provádí hodnocení rizik v pravidelných intervalech (subjekty c) a e) alespoň 1x ročně a subjekty d) 1x za tři roky) i při významných změnách.

Identifikované hrozby a zranitelnost zhodnotí a posoudí možné dopady na aktiva a na základě tohoto hodnocení zpracuje zprávu, dále zpracuje prohlášení o aplikovatelnost, která bezpečnostní opatření požadovaných VoKB nebyla aplikována (důvod) a která byla aplikována (způsob plnění).

Zpracuje a zavede plán zvládání rizik (obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření), v souladu s tímto plánem zavadí bezpečnostní opatření.

5.3.3 Organizační bezpečnost

Povinná osoba pro systém řízení bezpečnosti informace zajistí: stanovení bezpečnostní politiky a cílů, integrací systému do procesu, dostupnost zdrojů pro systém, podporu k dosažení požadovaných výstupů systému.

Dále informuje zaměstnance o významu systému, vede je k rozvíjení efektivity sytému, osoby, které zastávající bezpečnostní role podporuje při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti, pro tyto osoby zajisti příslušné pravomoci a zdroje které jim umožní naplňovat jejich role a úkoly.

Zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role a zajistí, aby byla zachována mlčenlivost těchto administrátorů.

Prosazuje neustálé zlepšování sytému a zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

5.3.4 Bezpečnostní role

Ve VoKB jsou definované 4 typy rolí:

*„**Manažer kybernetické bezpečnosti**: osoba která je zodpovědná za systém řízení bezpečnosti informací, musí být vyškolená a musí mít za sebou minimálně 3 roky praxe nebo 1 rok, pokud má absolvovanou vysokou školu, je zodpovědný za informování o činnostech z jeho rozsahu odpovědnosti vrcholového vedení. Tato role musí být oddělena od rolí odpovědných za provoz informačního a komunikačního systému i s dalšími provozními nebo řídicími rolemi.*

***Architekt kybernetické bezpečnosti**: osoba zajišťující návrh implementace bezpečnostních opatření (pro zajištění bezpečné architektury informačního a komunikačního systému), musí být vyškolená a musí mít za sebou minimálně 3 roky praxe nebo 1 rok, pokud má absolvovanou vysokou školu.*

***Auditor kybernetické bezpečnosti:** osoba, která provádí audit kybernetické bezpečnosti, musí být vyškolená a musí mít za sebou minimálně 3 roky praxe nebo 1 rok, pokud má absolvovanou vysokou školu. Svoji roli vykonává nestraně a jeho výkon je oddělený od ostatních výkonů jiných bezpečnostních rolí.*

***Garantem aktiva:** fyzická osoba odpovědná za zajištění: rozvoje, použití a bezpečnost aktiva* [8].*“*

5.3.5 Řízení dodavatelů

Povinná osoba pro dodavatele stanoví pravidla, které se týkají požadavků systému řízení bezpečnosti informací a s těmito pravidly dodavatelé seznamuje a vyžaduje je. Vede evidenci významných dodavatelů a tyto dodavatel je o tom písemně informuje. V rámci výběrového řízení a před uzavřením smlouvy provádí hodnocení rizik souvisejících s plněním předmětu výběrového řízení. Řídí rizika spojená s dodavateli a souvislosti s tím zajistí, aby uzavřena smlouva s dodavatelem obsahoval relevantní záležitosti spojené s kybernetickou bezpečností a plnění této smlouvy pravidelně přezkoumávat. Případné nedostatky zajistí jejich nápravu.

5.3.6 Řízení provozu a komunikací

Povinná osoba zajišťuje bezpeční provoz informačního a komunikačního systému a stanoví provozní pravidla a postupy obsahující:

- *„práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role*
- *postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů*
- *postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech*
- *pravidla a postupy pro ochranu před škodlivým kódem*
- *řízení technických zranitelností*
- *spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory*
- *postupy řízení a schvalování provozních změn,*
- *postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů*
- *pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu*
- *pravidla a postupy pro instalaci technických aktiv*
- *provádění pravidelného zálohování a kontroly použitelnosti provedených záloh*
- *pravidla a postupy pro zajištění bezpečnosti síťových služeb* [7]*“*

Tyto pravidla jsou dodržována a aktualizována se změnami sytému. Dále by mělo být zajištěno vývojové, testovací a provozní prostředí.

5.3.7 Řízení změn

Povinná osoba přezkoumává možné dopady změn a určuje významné změny a u nich: „*dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí jejich testování a zajistí možnost navrácení do původního stavu* [7].*“*

5.3.8 Přístupy do systému

Povinná osoba řídí přístup k informačnímu a komunikačnímu systému na základě bezpečnostních a provozních potřeb. K tomu zavádí bezpečnostní opatření, a to včetně mobilních telefonů nebo jiných technických zařízení včetně tech co nemá ve správě. Požívá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění (přistup k aktivům systému, čtení dat, zápis dat a změnu oprávnění).

Přistup řídí na základě rolí a skupin. Každému, kdo přistupuje k systému přidělí přístupová práva, oprávnění a jedinečný identifikátor a ty následně řídí. Přidělování privilegovaná opaření omezit na nezbytnou úroveň nutnou k výkonu práce. Přidělovat nebo odebírat oprávnění na základě politiky řízení přístupu. Nastavení přístupových oprávnění pravidelně přezkoumávat a aktualizovat. Zajistí změnu nebo odeprání přístupových oprávnění pří změně pozice nebo zařízení a při vypovědění smluvního vztahu.

Omezit a kontrolovat programové prostředky, které mohou překonat systémové nebo aplikační kontroly.

Používá nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému. Nástroj musí zajišťovat: ověření identity před zahájením aktivit v systému, omezovat počet neúspěšných pokusů o přihlášení, znovu ověřovat identitu po určené době nečinnosti, odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, ukládat tyto údaje tak aby byly odolné proti offline útokům a dodržovat důvěryhodnost při obnově přístupu, centralizovanou správu identit.

Ověření identity musí být více faktorové. Pokud to není splněno musí být využívány kryptografické klíče. A pokud není ani to dodrženo musí být vynucována následující pravidla: délka hesla 12 znaků pro uživatele a 17 pro administrátora, umožnit zadat heslo až o délce 64 znaků, neomezovat malá a velká písmena, číslice a speciální znaky, jednotlivé obnovy hesla nesmí být kratší než 30 minut, vynucovat změnu hesla minimálně po 18 měsících, neumožňovat: zvolit si nejčastěji používaná hesla, 2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a 3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel. Dále musí vynutit změnu výchozího hesla po prvním použití, heslo pro obnovu zneplatnit po prvním použití nebo 60 minutách od vytvoření.

5.3.9 Zvládání kybernetických bezpečnostních událostí a incidentů

Povinná osoba zavede proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů. Přidělí odpovědnost a postupy pro detekci a vyhodnocování kybernetických bezpečnostních

událostí a incidentů a zároveň koordinací a zvládání kybernetických bezpečnostních incidentů. Definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetických bezpečnostních incidentů. Zajistí, aby jednotlivé subjekty (role, zaměstnanci atd.) oznamovali podezřivé chování systém nebo podezření na zranitelnost.

Zaznamenává bezpečnostní a důležité provozní události významných aktiv systému. Podle hodnocení aktiv je aktualizováno, u kterých aktiv se sledují události. Subjekty c) a e) musejí informace o událostech musí archivovat nejméně 18 měsíců a subjekty d) minimálně 12 měsíců.

Pro zaznamenávání událostí musí být zajištěno: jednoznačnou síťovou identifikaci zařízení původce při použití nástroje který mění síťovou identifikaci, sběr informací („*datum a čas včetně specifikace časového pásma, typ činnosti, identifikaci technického aktiva, které činnost zaznamenalo, jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, jednoznačnou síťovou identifikaci zařízení původce a úspěšnost nebo neúspěšnost činnosti*“[7]), tyto informace chránit před neoprávněním čtením a změnou, má se zaznamenávat („*přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů, činností provedených administrátory, úspěšné i neúspěšné manipulace s účty, oprávněními a právy, neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, zahájení a ukončení činností technických aktiv, kritických i chybových hlášení technických aktiv a přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí*“[7]), synchronizovat čas technických aktiv minimálně jednou za 24 hodin.

Zajistí detekci kybernetických bezpečnostních událostí pomocí nástroje pro detekci událostí. Ten zajistí kontrolu přenášených dat v rámci komunikační sítě a mezi nimi, na obvodu komunikační sítě a blokuje nežádoucí komunikaci. Detekce kybernetických bezpečnostních událostí v rámci koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, síťových aktivních prvků a obdobných aktiv.

Subjekty c) a d) musí využívat nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí. Tento nástroj umožní: sběr a vyhodnocení zaznamenaných událostí, vyhledávat a seskupovat záznamy, při detekci kyberneticky

bezpečnostní události informovat oprávněné role, vyhodnocovat kyberneticky bezpečnostní události pro případ výskytu kyberneticky bezpečnostní incidentu a včasného varování odpovědných rolí, pravidelně aktualizovat vyhodnocování a včasné varování. Informace získané pomocí tohoto nástroje využít k optimalizaci systému.

Zajistí zvládání kyberneticky bezpečnostní incidentů podle stanovených postupů. Přímá taková opatření, která odvrátí a zmírní účinnost kyberneticky bezpečnostní incidentů. Prošetří a určí příčiny kyberneticky bezpečnostní incidentu a analyzuje účinnost řešení kyberneticky bezpečnostní incidentu, případně aktualizuje stávající postupy.

5.3.10 Řízení kontinuity činností

Povinná osoba stanoví práva a povinnosti pro osoby zastávající bezpečnostní role a administrátory. Na základě hodnocení rizik a analýzy dopadů kyberneticky bezpečnostních incidentů, dokumentuje dopady a na základě nich stanoví ohrožení kontinuity činností. Na základě tohoto určení stanoví: *„minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému, doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání* [7]. *“*

Dále stanoví politiku, která obsahu předchozí cíle. Vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a havarijní plány, které souvisejí s provozováním systému a souvisejících služeb. Realizuje opatření pro zvýšení odolnosti systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti.

5.3.11 Technické opatření

Některá technická opatření uváděná ve VoKB byla už zmíněná výše např. Správa a ověřování identit nebo Detekce kybernetických bezpečnostních událostí.

Fyzická bezpečnost – povinná osoba předchází krádeži, zneužití nebo poškození technických aktiv nebo přerušení dostupnosti systému tak že stanoví fyziko bezpečnostní hranici, která ohraničuje oblast, kde dochází k zpracování a uchovávání informací a jsou zde umístěná technická aktiva systému. V této oblasti jsou přijímány nezbytná opatření a uplatňovány prostředky fyzické bezpečnostní ochrany: zamezení neoprávněnému

vstupu, zamezení poškození a neoprávněné zásahy a pro zajištění ochrany na úrovni objektů a v rámci objektů.

Bezpečnost komunikačních sítí – povinná osoba zajistí: segmentaci komunikační sítě a pro komunikaci mezi jejími segmenty využívá nástroj, který ochrání integraci sítě, řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě, důvěryhodnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií pomocí kryptografie, aktivní blokování nežádoucí komunikace.

Ochrana před škodlivým kódem – povinná osoba zajistí nepřetržitou automatickou ochranu u těchto zařízení: koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, komunikační sítě a prvků komunikační sítě a obdobných zařízení. U výměnných zařízení a datových nosičů řídí a monitoruje používání a u těchto zařízení/nosičů řídí automatické spuštění obsahu. Řídí oprávnění ke spouštění kódu. U nástroje pro ochranu před škodlivým kódem provádí pravidelnou a účinnou aktualizaci.

Kryptografické prostředky – Povinná osoba používá aktuálně odolné kryptografické algoritmy a kryptografické klíče. Využívá systém správy klíčů a certifikátů, který zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů a umožní kontrolu a audit. Prosazuje bezpečné nakládání s kryptografickými prostředky. Zohledňuje doporučení úřadu v oblasti kryptografických prostředků.

Zajišťování úrovně dostupnosti informací – povinná osoba zajistí: dostupnost systému pro splnění cílů, odolnost systémů vůči kybernetickým bezpečnostním incidentům, které by mohly narušit jeho dostupnost, dostupnost důležitých aktiv systému a redundanci aktiv systému, které jsou nezbytné pro dostupnost.

6 Shrnutí výsledků a doporučení

V první části bakalářské práce byly rozpracovány vybrané dílčí části Cyber Security Framework NIST, v druhé části práce byl stručně rozpracován legislativní rámec kybernetické bezpečnosti (povinné subjekty, bezpečnostní opatření a charakteristika bezpečnostních incidentů), dále byly rozpracovány vybrané dílčí části vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, které souvisely s informační bezpečností.

Dále byla vytvořena přehledová tabulka, která obsahuje vybraná dílčí ustanovení z vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. K těmto ustanovením byly přiřazeny odpovídající dílčí části Cyber Security Framework (NIST), přičemž přehledová tabulka je součástí této bakalářské práce.

Na základě provedeného srovnání lze konstatovat, že Cyber Security Framework od NIST je svým rozsahem velmi rozsáhlý a obsahuje velké množství informací, které je popsáno převážně obecným způsobem, tak aby tento rámec bylo možné implementovat v jakékoliv organizaci (instituci).

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti a její vybraná ustanovení, která byla zvolena pro analýzu a následnou komparaci obsahuje detailnější informace pro implementaci pravidel informační bezpečnosti. Legislativní rámec kybernetické bezpečnosti (zákon o kybernetické bezpečnosti a prováděcí vyhláška o kybernetické bezpečnosti) tvoří komplexní celek obsahující detailní informace včetně charakteristiky technických opatřeních, která jsou nedílnou součástí příloh.

Cyber Security Framework lze tedy využít při implementaci u subjektů povinných podle legislativního rámce kybernetické bezpečnosti ČR pouze jako doplnění či rozšíření možností pro zvýšení informační bezpečnosti, avšak pouze na základě individuálního přístupu v každé organizaci, protože Cyber Security Framework je tvořen převážně obecnými pravidly a doporučeními.

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti		Framework NIST
Systém řízení bezpečnosti informací	§3	Koordinace zavádění frameworku 3.2, Využití frameworku 3.3, Rozhodnutí o nákupu 3.4
Řízení rizik	§5	Idenfitikace 4.1
Organizační bezpečnost	§6	Role a odpovědnost 4.1.5
Bezpečnostní role	§7	Role a odpovědnost 4.1.5
Řízení dodavatelů	§8	Standard NIST neobsahuje
Řízení provozu a komunikací	§10	Řízení toku informací 4.1.2
Řízení změn	§11	Konfigurace informačních systémů 4.2.13
Řízení přístupů	§12	Správa identit a přihlašovacích údajů 4.2.1, Přístupová oprávnění 4.2.4
Zvládání bezpečnostních rizik a incidentů	§14	Detekce 4.3, Plány obnovy 4.2.16
Řízení kontinuity činností	§15	Detekce 4.3, Plány obnovy 4.2.16
Technická opatření	§17 - §29	Ochrana 4.2

Tabulka 1: Porovnání vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti a Cybersecurity Frameworku NIST (vlastní tvorba)

7 Závěr

V bakalářské práci byla provedena analýza vybraných dílčích částí Cyber Serurity Frameworku NIST, a dále vybraných dílčích částí vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti s následnou komparací včetně sestavení stručné přehledové tabulky, která je nedílnou součástí této bakalářské práce.

Problematika Cyber Security Frameworku NIST je velmi rozsáhlá a zajímavá, avšak detailní analýza a komparace v rámci legislativního rámce kybernetické bezpečnosti ČR by byla zajímavá např. pro vědeckou – výzkumný projekt, který by bylo možné rozšířit navíc ještě o legislativní rámec kybernetické bezpečnosti Evropské Unie na základě čehož by vznikly zřejmě velmi zajímavé výstupy, se kterými by bylo možné nadále pracovat.

8 Seznam použité literatury

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [online]. 2018. [vid. 2021-10-23]. Dostupné z: doi: 10.6028/NIST.CSWP.04162018

[2] JOINT TASK FORCE INTERAGENCY WORKING GROUP. *Security and Privacy Controls for Information Systems and Organizations* [online]. 2020 [vid. 2021-11-21]. Dostupné z: doi:10.6028/NIST.SP.80053r5

[3] Jan Kolouch, Pavel Bašta a kol. *Cybersecurity* [online]. [vid. 2022-02-17]. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[4] *Pojem telekomunikace* [online]. [vid. 2022-02-24]. Dostupné z: https://publi.cz/books/86/01.html

[5] Česká republika*. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. [vid. 2022-02-24]. Dostupné z: https://www.nukib.cz/images/icons/2021-08-31_novelizace_zneni_zakona_181_2014.pdf

[6] *Národní úřad pro kybernetickou a informační bezpečnost – Legislativa* [online]. [vid. 2022-02-27]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[7] Česká republika. *Vyhláška č. 82 ze dne 21. května 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* [online]. [vid. 2022-02-27]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[8] KROUPOVÁ, Hana. *BEZPEČNOSTNÍ ROLE a jejich začlenění v organizaci* [online]. [vid. 2022-03-05]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/bezpe%C4%8Dnostn%C3%AD-role_v3.pdf

[9] Česká republika. *Zákon č. 240/2000 Sb. ze dne 28. června 2000 o krizovém řízení a o změně některých zákonů (krizový zákon)* [online]. [vid. 2022-08-04]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240?citace=1#f4394839

9 Seznam tabulek

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor: **Václav Buřil**

Studium: I1900157

Studijní program: B1802 Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Název bakalářské práce: **Cyber Security Framework National Institute of Standards and Technology**

Název bakalářské práce AJ: Cyber Security Framework National Institute of Standards and Technology

Cíl, metody, literatura, předpoklady:

Cílem práce je analýza a komparativní srovnání rámce Cyber Security Framework NIST s legislativním rámcem v oblasti kybernetické bezpečnosti v České republice.

Zásady:

- Úvod.
- Analýza Cyber Security Framework NIST a legislativního rámce v oblasti kybernetické bezpečnosti v České republice.
- Komparace Cyber Security Framework NIST a legislativního rámce v oblasti kybernetické bezpečnosti v České republice.
- Využití výstupu komparace v oblasti kybernetické bezpečnosti.
- Závěr

BRUCKNER, Tomáš, 2012. *Tvorba informačních systémů: principy, metodiky, architektury*. Praha: Grada. ISBN 978-80-247-4153-6.

KOLOUCH, Jan, 2019. *CyberSecurity*. ISBN 978-80-88168-34-8.

NICOLE.KELLER@NIST.GOV, 2013. Cybersecurity Framework. *NIST* [online] [vid. 2021-01-29]. Dostupné z: https://www.nist.gov/cyberframework

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. ISBN 978-80-7380-765-8.

Zadávající pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Ing. Hana Švecová

Oponent: Ing. Lubomír Almer, Ph.D.

Datum zadání závěrečné práce: 9.9.2021