Název předmětu: Kybernetická bezpečnost

Téma: 6. Hrozby a rizika v kyberprostoru. Ochrana aktiv

Cíl: Cílem je seznámit studenty s hrozby a riziky v kybernetickém prostoru. Seznámit s analýzou a hodnocením rizik, řízením aktiv.

Úkoly pro samostatnou práci: naučit se a zopakovat si základní pojmy z oblasti kybernetické bezpečnosti, zopakovat si pravidla pro analýzu a hodnocení rizik, určení a řízení aktiv.

Studijní literatura:

1. SMEJKAL, V. a RAIS, K. Řízení rizik. 1. vyd. Praha: Grada Publishing, 2003. 270 s. ISBN 80-247-0198-7.
2. GRASSEOVÁ, M., DUBEC, R., ŘEHÁK, D. Analýza podniku v rukou manažera. 1. vydání. Brno: Computer Press, 2010, 325 s. ISBN 978-80-251-2621-9. (Strana 139-175)
3. Norma ISO/IEC 27005:2009 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.
4. TICHÝ, M. Ovládání rizika. Analýza a management. 1. vyd. Praha: C. H. Beck, 2006. 396 s. ISBN 80-7179- 415-5.
5. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
6. HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav; PTÁČEK, Bohumil; SKORUŠA, Leopold; SLOŽIL, Richard. *Kybernetická bezpečnost: teorie a praxe.* Praha: Powerprint s.r.o., 2015, 250 s. ISBN 978-80-87994-72-6.
7. HRŮZA, Petr; PITAŠ, Jaromír; ŠANDA, Jaroslav; BRECHTA, Bohumil. *Kybernetická bezpečnost II.* Brno: Univerzita obrany, Brno, 2013, 100 s. ISBN 978-80-7231-931-2.
8. HRŮZA, Petr. *Kybernetická bezpečnost.* Brno: Univerzita obrany, 2012, 90 s. ISBN 978-80-7231-914-5.
9. Vydané normy ISO/ČSN řady 27000, platné zákony a vyhlášky z oblasti kybernetické bezpečnosti

Obsah:

Riziko je kombinací následků, které by vyplývaly z výskytu nechtěné události a pravděpodobnosti jejího výskytu. Hodnocení rizik riziko kvantifikuje nebo kvalitativně popisuje a umožňuje vedoucím pracovníkům, aby určili prioritu rizik podle jejich vnímané důležitosti nebo jiných stanovených kritérií.

Hodnocení rizik sestává z těchto činností:

Analýza rizik zahrnuje:

- identifikaci rizik
- odhad rizik
- Vyhodnocení rizik.

Hodnocení rizik určuje hodnotu informačních aktiv, identifikuje možné hrozby a zranitelnosti, které existují (nebo by mohly existovat), identifikuje stávající opatření a jejich účinek na identifikované riziko, určuje potenciální dopady a nakonec stanoví prioritu určených rizik a řadí je proti kritériím vyhodnocení rizik určeným ve stanovení kontextu.

Hodnocení rizik se často provádí ve dvou (nebo více) opakováních. Nejprve se provádí přehledové hodnocení, aby byla identifikována potenciálně vysoká rizika, která zasluhují další hodnocení. Následující opakování může zahrnovat další důkladné zvážení potenciálně vysokých rizik odhalených v prvním kole hodnocení. Tam, kde tyto kroky neposkytnou dostatečné informace pro hodnocení rizika, provedou se další podrobné analýzy, pravděpodobně v částech celkového rozsahu, a možná za použití jiné metody. Je na organizaci, aby si vybrala svůj vlastní přístup k hodnocení rizik na základě cílů a záměru procesu.

Následujícím subprocesem po stanovení kontextu je posuzování rizik, které zahrnuje tři stěžejní činnosti, a to identifikování, analyzování a hodnocení rizik. Počáteční činností subprocesu analýzy rizik je identifikování rizik. V rámci této činnosti provádíme:

a) identifikace aktiv,

b) identifikace hrozeb,

c) identifikace stávajících opatření,

d) identifikace zranitelností,

e) identifikace následků.

Účelem identifikace rizik je určit, co by se mohlo stát, aby byla způsobena potenciální ztráta, a porozumět tomu jak, kde a proč ke ztrátě může dojít. Kroky popsané v následujících bodech by měly shromáždit vstupní data pro činnost hodnocení rizik.

Cílem tohoto kroku je vytvořit komplexní seznam rizik založený na takových událostech, které by mohly zamezit, snížit nebo zpomalit dosažení cílů. Rovněž je důležité identifikovat rizika související s nevyužitím příležitosti. Nezbytným krokem identifikování rizik je však zvážení všech možných příčin. Komplexní identifikace je totiž rozhodující, protože rizika, která nejsou identifikována na tomto stupni, nebudou zahrnuta do následující analýzy. Proto jsou při identifikování rizik důležité aktuální informace, které by měly obsahovat vhodná a podrobná data. Identifikace tak zahrnuje veškerá rizika bez ohledu na to, ať jejich zdroj již je pod kontrolou organizace, nebo ještě není.

Identifikace aktiv spočívá ve vytvoření soupisu všech aktiv ležících uvnitř hranice řízení rizik, kterou jsme si vymezili v rámci předchozího subprocesu. Při rozhodování o zařazení daného aktiva na soupis se uvede název aktiva a jeho umístění (např. automobil Tatra 815 umístěný v

podzemních garážích bloku C8). Následující stanovení hodnoty aktiva je založeno na velikosti škody způsobené zničením či ztrátou aktiva. Obvykle se při stanovení hodnoty aktiva vychází z jeho nákladových charakteristik (pořizovací ceny, reprodukční pořizovací ceny), mohou to být ale i charakteristiky výnosové (pokud aktivum přináší dobře identifikovatelné zisky či jiné významné přínosy pro subjekt). Mezi výnosové charakteristiky patří i vlastnosti aktiva, sloužící k dosahování zisků nepřímo – například postavení na trhu, ochranná známka, ale i kvalifikace a know-how zaměstnanců. Velmi podstatné je rozlišit, zda se jedná o jedinečné aktivum nebo o aktivum jednoduše nahraditelné. Do hodnoty se promítá závislost subjektu na existenci, ale i na správném fungování hodnoceného aktiva, tedy k jakým škodám dojde omezením funkčnosti nebo ztrátou aktiva, než dojde k jeho obnově. Hodnota aktiva pro analýzu rizik se může stanovit také jako vážený průměr hodnot podle všech použitých hledisek. Vzhledem k tomu, že aktiv je obvykle veliké množství, snižuje se jejich počet tak, že se provede seskupení aktiv podle různých hledisek, aby se vytvořily skupiny aktiv podobných vlastností. Seskupovat se mohou aktiva podobné kvality, ceny, účelu apod. Takto vytvořená skupina aktiv pak dále vystupuje jako jedno aktivum. Potom je nutné zabezpečit, aby protiopatření, navržená v etapě zvládání rizik pro skupinu aktiv, byla aplikována na všechna aktiva, která jsou do této skupiny sdružena (Smejkal, Rais, 2006, s. 86–87).

Aktivum je cokoli, co má pro organizaci hodnotu a co tedy vyžaduje ochranu. U identifikace aktiv je třeba mít na paměti, že informační systém se skládá z něčeho víc, než jen z hardwaru a softwaru.

Identifikace aktiv by měla být provedena na vhodném stupni podrobnosti, který poskytuje pro hodnocení rizik dostatek informací. Stupeň podrobnosti použitý pro identifikaci aktiv ovlivní celkové množství informací shromážděných během hodnocení rizik. Tento stupeň lze zpřesnit v dalším opakování hodnocení rizik.

U každého aktiva by měl být identifikován vlastník aktiva k zajištění záruky a odpovědnosti za aktivum. Vlastník aktiva k němu možná nemá vlastnická práva, ale má přiměřenou odpovědnost za jeho produkci, vývoj, údržbu, používání a bezpečnost. Vlastník aktiva je často nejvhodnější osobou pro určení hodnoty aktiva pro organizaci. Hranicí analýzy je okruh aktiv organizace, který má být zvládán procesem řízení rizik bezpečnosti informací. Výstupem je seznam aktiv, u nichž je třeba zajistit řízení rizik, a seznam procesů činností organizace, jež se vztahují k aktivům, a jejich důležitost.

Identifikace hrozeb a jejich zdrojů se provádí tak, že se vybírají ty hrozby a jejich zdroje, které mohou ohrozit alespoň jedno z aktiv subjektu. Pro identifikaci hrozeb a jejich zdrojů lze vycházet ze seznamu hrozeb, sestavených podle dostupné literatury, vlastních zkušeností, průzkumů či dříve provedených analýz. Hrozby se mohou odvozovat také od subjektu, jeho statusu (podnikatelský subjekt, státní organizace, nezisková organizace atd.), postavení na trhu, hospodářských výsledků, záměrů podnikatele (Smejkal, Rais, 2006, s. 87).

Hrozba má potenciál poškodit aktiva jako jsou informace, procesy a systémy, tedy poškodit samotnou organizaci.

Hrozby mohou být přírodního nebo lidského původu a mohou být náhodné nebo úmyslné. Měly by být identifikovány zdroje jak náhodných, tak úmyslných hrozeb. Hrozba může vyvstat zevnitř i zvenčí organizace. Hrozby by se měly identifikovat obecně podle typu (například neoprávněné akce, fyzické zničení, technické poruchy) a pak, v případě potřeby, by se měly v rámci obecné třídy identifikovat jednotlivé hrozby. To znamená, že není žádná hrozba opomenuta, včetně těch neočekávaných, avšak objem požadované práce je omezen.

Některé hrozby mohou postihnout více než jedno aktivum. V takových případech mohou mít různý dopad v závislosti na tom, která aktiva jsou postižena. Vstup k identifikaci hrozby a odhad pravděpodobnosti výskytu lze získat od vlastníků nebo uživatelů aktiv, od pracovníků lidských zdrojů, od dovednosti manažera a specialistů v oblasti bezpečnosti informací, expertů v oblasti fyzické bezpečnosti, právních oddělení a jiných organizací včetně právních orgánů, meteorologických stanic, pojišťoven a národních vládních úřadů. Při řešení hrozeb je zapotřebí brát v úvahu i aspekty životního prostředí a kultury.

Při aktuálním hodnocení by se mělo přihlížet i k vnitřním zkušenostem z incidentů a minulým hodnocením hrozeb. Tam, kde to je důležité, je možné nahlédnout i do jiných katalogů hrozeb (třeba charakteristických pro organizaci nebo zaměření organizace) za účelem doplnění seznamu obecných hrozeb. Katalogy hrozeb a statistiky jsou k dispozici u průmyslových orgánů, národních vlád, právních orgánů, pojišťoven atd.

Při použití katalogů hrozeb nebo výsledků dřívějších hodnocení hrozeb je nutné být si vědom toho, že se významné hrozby neustále mění, zejména pokud se mění obchodní prostředí nebo informační systémy.

Výstup: Seznam hrozeb s identifikací typu a zdroje hrozby.

Identifikace stávajících opatření

Aby se předešlo zbytečné práci nebo nákladům, například při duplikaci opatření, měla by být provedena identifikace stávajících opatření. Kromě toho by při identifikaci stávajících opatření měla být provedena kontrola správné funkčnosti opatření - uvedením odkazu na již existující zprávy auditu ISMS je možné snížit spotřebu času stráveného nad tímto úkolem. Pokud opatření nefunguje dle předpokladů, může to způsobit zranitelnost. V úvahu je třeba brát situace, kdy vybrané opatření (nebo strategie) selže, a proto jsou k účinnému řešení identifikovaného rizika nutná dodatečná opatření. V ISMS je podle ISO/IEC 27001 toto podporováno měřením účinnosti opatření. Způsob, jak odhadnout účinnost opatření, je poznat, jak snižuje pravděpodobnost hrozby, snadnost zneužití zranitelnosti nebo dopad incidentu. Informace o účinnosti existujících opatření poskytují také přezkoumávání vedením organizace a zprávy z auditu. Opatření, která se plánují uplatňovat v souladu s realizačními plány zvládání rizik, by měla být zvažována stejným způsobem jako ta, která jsou už uplatňována.

Existující nebo plánované opatření by mohlo být identifikováno jako neúčinné, nedostačující nebo neoprávněné. Pokud je neoprávněné nebo nedostatečné, mělo by se dané opatření zkontrolovat a určit, zda by mělo být odstraněno, nahrazeno jiným vhodnějším opatřením, nebo

zda by mělo zůstat na místě, například z finančních důvodů. Identifikaci existujících nebo plánovaných opatření mohou napomoci tyto činnosti:

- Přezkoumání dokumentů obsahujících informace o opatřeních (například implementační plány zvládání rizik). Jsou-li procesy řízení bezpečnosti informací dobře doloženy, měla by být všechna existující nebo plánovaná opatření a stav jejich uplatňování k dispozici.
- Provedení kontrol s pracovníky, kteří jsou odpovědní za bezpečnost informací (například manažerem bezpečností informací a manažerem bezpečností informačního systému, manažerem fyzické bezpečnosti nebo vedoucím provozu), a uživateli, pro něž jsou opatření pro příslušný informační proces nebo informační systém opravdu zaváděna.
- Přezkoumání fyzických opatření na místě, srovnání implementovaných a doporučených opatření a kontrola implementovaných opatření z hlediska jejich funkčnosti a účinnosti.
- Přezkoumání výsledků interních auditů.

Výstupem této činnosti je seznam existujících a plánovaných opatření, jejich zavedení a stav užívání.

Identifikace zranitelností se provádí zpravidla v těchto oblastech:

- Organizace
- Procesy a postupy
- Běžné praxe řízení
- Pracovníci
- Fyzické prostředí
- Konfigurace informačního systému
- Hardware, software nebo komunikační zařízení
- Závislost na externích stranách

Výskyt zranitelnosti nepůsobí škodu jako takový, protože musí existovat hrozba, která ho využije. Zranitelnost, která nemá odpovídající hrozbu, nemusí vyžadovat přijetí opatření, ale měla by být rozpoznána a monitorována, jestli se nemění. Je nutno poznamenat, že nesprávně přijaté nebo nefunkční opatření nebo opatření, které se používá nesprávně, by samo o sobě mohlo představovat zranitelnost. Opatření může být účinné nebo neúčinné v závislosti na prostředí, v němž funguje. Naopak, hrozba, která nemá odpovídající zranitelnost, nemusí vyústit v riziko.

Zranitelnosti mohou souviset s vlastnostmi aktiva, které lze použít způsobem nebo pro účel, který je jiný, než bylo zamýšleno, když bylo aktivum zakoupeno nebo zhotoveno. Je nutno posuzovat zranitelnosti vyplývající z různých zdrojů, například ty, které jsou pro aktivum podstatné nebo vedlejší.

Výstup: Seznam zranitelností ve vztahu k aktivům, hrozbám a opatřením; seznam zranitelností, které se nevztahují k žádné identifikované hrozbě pro přezkoumání.

Identifikace následků. Měly by být identifikovány následky, které mohou znamenat pro aktivum ztrátu důvěrnosti, integrity a dostupnosti.

Následkem může být ztráta účinnosti, nepříznivé provozní podmínky, ztráta obchodu, pověsti, škoda atd. Tato činnost identifikuje škody nebo dopady na organizaci, jež by mohly být způsobeny podle scénáře incidentu. Scénář incidentu je popis hrozby zneužívající určitou zranitelnost nebo soubor zranitelností (viz ISO/IEC 27002, kapitola 13). Je nutno určit následek incidentu a posuzovat přitom kritéria dopadu definovaná během činnosti stanovení kontextu. Následek může ovlivnit jedno nebo více aktiv nebo jen část aktiva. Aktiva tedy mohou mít stanovené hodnoty podle svých finančních nákladů nebo podle velikosti následků, jsou-li poškozena nebo kompromitována. Následky mohou být dočasného charakteru nebo mohou být stálé, jako v případě zničení aktiva.

Organizace by měly identifikovat provozní následky scénářů incidentů z hlediska (nejen):

- Vyšetřování a doby nápravy
- Ztráty času (pracovní doby)
- Ztráty příležitosti
- Zdraví a bezpečnosti
- Finančních nákladů na zvláštní dovednosti nutné pro nápravu škody
- Pověsti a důvěryhodnosti

Výstup: Seznam scénářů incidentů s jejich následky vztahujícími se k aktivům a procesům.

K identifikaci rizik můžeme používat mnoho vhodných metod a nástrojů. Přístup k jejich užití bude záviset především na povaze posuzovaných činností, druhů rizik, souvislostech organizace či účelu studia řízení rizik. Na základě toho přístupy užité k identifikování rizik mohou zahrnovat např. brainstorming, brainwriting, řízenou diskuzi, metodu CNB (společného zápisníku), dotazníkové šetření, odvětvový (funkční) benchmarking, systémovou analýzu, analýzu pomocí scénářů, předběžnou analýzu ohrožení (Preliminary Hazard Analysis – PHA) či analýzu ohrožení a provozuschopnosti (Hazard & Operability Studies – HAZOP).

Odhad rizik

Metodika odhadování rizik

Analýzu rizik lze provádět v různých stupních podrobnosti v závislosti na kritičnosti aktiv, rozsahu známé zranitelnosti a předcházejících incidentech zasahujících organizaci. Metodika odhadu může být kvalitativní nebo kvantitativní nebo kombinací obou, v závislosti na okolnostech. V praxi se často používá nejprve kvalitativní odhad k získání obecné indikace úrovně rizika a k odhalení větších rizik. Později může být nutné provést více konkrétní nebo kvantitativní analýzu větších rizik, protože je obvykle méně složité a méně nákladné provést kvalitativní než kvantitativní analýzu.

Forma analýzy by měla být v souladu s vytvořenými kritérii vyhodnocení rizik jako součásti stanovení kontextu. Další podrobnosti o metodikách odhadu jsou popsány níže: (a)

1. Kvalitativní odhad:

Kvalitativní odhad používá k popisu velikosti potenciálních následků (například nízkých, středních a vysokých) a pravděpodobnosti, že se tyto následky vyskytnou, škálu kvalifikačních atributů. Výhodou kvalitativního hodnocení je, že je všichni příslušní pracovníci mohou snadno pochopit, zatímco jeho nevýhodou je závislost na subjektivním výběru škály.

Tyto škály lze upravit nebo přizpůsobit tak, aby odpovídaly okolnostem, a pro různá

rizika lze použít různé popisy. Kvalitativní hodnocení může být použito:

- Jako počáteční prověřovací činnost k identifikaci rizik, které vyžadují podrobnější analýzu,
- V případě, kde je tento druh analýzy vhodný pro rozhodnutí,
- V případě, kde jsou číselné údaje nebo zdroje pro kvantitativní hodnocení nevhodné.

Kvalitativní analýza by měla používat skutečné informace a data, která jsou k dispozici.

2. Kvantitativní odhad:

Kvantitativní odhad používá stupnici s číselnými hodnotami (spíše než popisné stupnice používané při kvalitativním hodnocení), jak pro následky, tak pro pravděpodobnost, a využívá přitom data z různých zdrojů. Kvalita analýzy závisí na přesnosti a úplnosti číselných hodnot a platnosti použitých modelů. Kvantitativní hodnocení v mnoha případech používá historická data incidentů a má výhodu v tom, že může mít přímou souvislost s cíli bezpečnosti informací a zájmy organizace. Nevýhodou je nedostatek takových dat u nových rizik nebo slabých míst v bezpečnosti. Nevýhoda kvantitativního přístupu může vyvstat také v případě, kdy nejsou k dispozici konkrétní, kontrolovatelná data, což vytváří mylný dojem o významu a přesnosti hodnocení rizik.

Způsob, jimž jsou následky a pravděpodobnost vyjádřeny, a způsoby, jimiž jsou kombinovány, aby poskytly úroveň rizika, se budou měnit podle typu rizika a účelu, pro který má být výstup hodnocení rizik použit. Nejistota a nestálost následků i pravděpodobnosti by měly být v analýze zohledněny a účinně sděleny.

Hodnocení následků

Seznam identifikovaných scénářů incidentů, včetně identifikace hrozeb, zranitelností, ovlivněných aktiv, dopadů na aktiva a procesy.

Činnost: Měl by se hodnotit obchodní dopad na organizaci, který by mohl vyplývat z možných nebo skutečných incidentů bezpečnosti informací, s přihlédnutím k následkům porušeni bezpečnosti informací jako je ztráta důvěrnosti, integrity nebo dostupností aktiv.

Doporučení k realizaci:

Po identifikaci všech aktiv v rámci přezkoumání by měly být při hodnocení následků brány v úvahu hodnoty těchto aktiv.

Hodnotu dopadu na organizaci lze vyjádřit v kvalitativní i kvantitativní formě, ale kterákoliv metoda určující peněžní hodnotu může obecně poskytovat více informací pro přijetí rozhodnutí a tak umožnit účinnější rozhodovací proces.

Hodnocení aktiv začíná u klasifikace aktiv podle jejich kritičnosti, na základě důležitosti aktiv pro plnění obchodních cílů organizace. Hodnocení se tedy určuje za použití těchto dvou kritérií:

- Hodnoty za náhradu aktiva: náklady na obnovení a náhradu informace Je-li to vůbec možné), a
- Obchodní následky ztráty nebo kompromitace aktiva, jako jsou potenciální nepříznivé činnosti organizace a/nebo právní nebo regulační následky z vyzrazení, změny, nedostupnosti a/nebo zničení informace a jiných informačních aktiv.

Toto hodnocení lze určit z analýzy dopadů na činnost organizace. Hodnota určená dopadem na činnosti organizace je obvykle vyšší, než náklady na jednoduchou výměnu, v závislosti na důležitosti aktiva pro organizaci při plnění jejích obchodních cílů.

Hodnocení aktiv je klíčovým faktorem při hodnocení dopadu scénáře incidentu, protože incident může ovlivnit více než jedno aktivum (například další závislá aktiva), nebo pouze část aktiva. Různé hrozby a zranitelnosti budou mít na aktiva různé dopady, jako je ztráta důvěrnosti, integrity nebo dostupnosti. Hodnocení následků tak souvisí s hodnocením aktiv na základě analýzy dopadů na činnosti organizace.

Následky nebo dopady na činnosti organizace lze určit modelováním výstupů události nebo souboru událostí, nebo extrapolací z experimentálních studií nebo minulých dat.

Následky lze vyjádřit na základě peněžních, technických nebo lidských kritérií dopadu, nebo jiných kritérií vhodných pro organizaci. V některých případech je vyžadována více než jedna číselná hodnota, aby bylo možno určit následky pro různé časy, místa, skupiny nebo situace.

Finanční následky by měly být měřeny se stejným přístupem, který byl použit pro pravděpodobnost hrozeb a zranitelnost. Je nutné dodržovat důslednost v kvantitativním nebo kvalitativním přístupu. Výstupem je seznam hodnocených následků scénáře incidentu vyjádřených s ohledem na aktiva a kritéria dopadu.

Určení pravděpodobnosti incidentu

Seznam identifikovaných scénářů incidentů, včetně identifikace hrozeb, ovlivněných aktiv, využitých zranitelností a dopadů na aktiva a procesy organizace. Kromě toho seznam všech existujících a plánovaných opatření, jejich účinnost, uplatnění a stav použití.

Činnost: Měla by být určena pravděpodobnost scénářů incidentů (souvisí s ISO/IEC

Doporučení k realizaci:

Po identifikaci scénářů incidentů je nutné za použití technik kvalitativního nebo kvantitativního hodnocení určit i pravděpodobnost každého scénáře a výskytu dopadu. Přitom je nutné

zohlednit, jak často se tyto hrozby vyskytují a jak snadno lze využít zranitelnosti. Při určování pravděpodobnosti je nutné brát v úvahu:

- Zkušenosti a platné statistiky o pravděpodobnosti hrozeb
- U zdrojů úmyslných hrozeb: motivaci a schopnosti, které se časem mění, a zdroje přístupné případným útočníkům, jakož i vnímání atraktivity a zranitelnosti aktiv pro případného útočníka
- U zdrojů náhodných hrozeb: geografické faktory, například těsná blízkost chemických nebo naftových závodů, možnost extrémních atmosférických podmínek a faktory, které by mohly mít vliv na lidská selhání a funkční poruchy zařízení
- Zranitelnosti, jak jednotlivě, tak v souvislostech
- Existující opatření a jejich účinnost na snížení zranitelnosti.

Například informační systém může mít zranitelnost vůči hrozbám falšování uživatelské identity a zneužití prostředků.

Zranitelnost v důsledku falšování uživatelské identity může být kvůli nedostatku prokazování identity uživatelů vysoká. Na druhé straně může být pravděpodobnost zneužití prostředků bez ohledu na nedostatek prokazování identity uživatelů nízká, protože způsoby, jak zneužít systémové prostředky, jsou omezené.

V závislosti na potřebné přesnosti lze aktiva spojovat do skupin nebo může být nutné rozdělit aktiva na jejich prvky a přiřadit scénáře k daným prvkům. Například napříč geografickými lokalitami se může charakter hrozeb pro stejný typ aktiv měnit, nebo se může lišit účinnost existujících opatření.

Výstup: Pravděpodobnost scénáře incidentů (kvantitativní nebo kvalitativní).

Úroveň odhadu rizik

Seznam scénářů incidentů s jejich následky, jež se vztahují k aktivům a procesům týkajícím se činností organizace, a jejich pravděpodobnost (kvantitativní nebo kvalitativní).

Činnost: Měla by se odhadnout úroveň rizik u všech důležitých scénářů incidentů.

Doporučení k realizaci:

Odhad rizik přiřazuje hodnoty k pravděpodobnosti a následkům rizika. Tyto hodnoty mohou být kvantitativní nebo kvalitativní. Odhad rizik se zakládá na hodnocených následcích a pravděpodobnosti. Kromě toho může brát v úvahu poměr přínosů a nákladů, zájmy zainteresovaných stran a jiné proměnné vhodné pro hodnocení rizik. Odhadnuté riziko je kombinací pravděpodobnosti scénáře incidentu a jeho následků.

Výstupem seznamu rizik s přiřazenými úrovněmi hodnot.

Vyhodnocení rizik

Seznam rizik s přiřazenými úrovněmi hodnot a kritéria pro vyhodnocení rizik.

Činnost: Úroveň rizik by se měla porovnat s kritérii vyhodnocení rizik a kritérii akceptace rizik.

Doporučení k realizaci:

Podstata rozhodnutí patřící k vyhodnocení rizik a ke kritériím vyhodnocení rizik, jež budou použita k učinění těchto rozhodnutí, by měla být určena při stanovení kontextu. Tato rozhodnutí a kontext by měly být podrobněji revidovány v tomto stádiu, kdy se ví už více o konkrétních identifikovaných rizicích. K hodnocení rizik by organizace měly porovnat odhadnutá rizika s kritérii vyhodnocením rizik definovaných během stanovení kontextu.

Kritéria vyhodnocení rizik používaná k rozhodování by měla být v souladu s definovaným vnějším a vnitřním kontextem řízení rizik bezpečnosti informací a měla by brát v úvahu cíle organizace a hlediska zainteresovaných stran atd. Rozhodnutí učiněná v rámci činnosti vyhodnocení rizik jsou založena zejména na akceptovatelné úrovni rizik. Avšak při identifikaci rizik a v analýze by měly být brány v úvahu rovněž následky, pravděpodobnost a stupeň důvěrnosti. Nahromadění většího množství nízkých nebo středních rizik může vyústit v daleko vyšší celková rizika a potřebu tuto situaci podle toho řešit.

Úvahy by měly zahrnovat:

Vlastnosti bezpečnosti informací: jestliže jedno kritérium není pro organizaci důležité (například ztráta důvěrnosti), pak všechna rizika dopadající na toto kritérium nemusí být důležitá.

Důležitost procesu nebo činnosti podporovaných určitým aktivem nebo souborem aktiv: jestliže je určeno, že proces má malou důležitost, rizikům s ním spojeným by se měla věnovat menší pozornost, než rizikům, která mají dopad na důležitější procesy nebo činnosti.

Informací získaných o riziku v průběhu analýzy rizik je v rámci vyhodnocování rizik využito k rozhodnutí o budoucích krocích. Rozhodnutí by měla zahrnovat:

Skutečnost, zda by měla být činnost prováděna

Priority pro zvládání rizik s přihlédnutím k odhadnutým úrovním rizik.

V průběhu vyhodnocování rizik, by měly být brány v úvahu také smluvní, právní a regulační požadavky.

Výstup: Seznam rizik, kterým byla udělena priorita podle kritérií vyhodnocení rizik v souvislosti se scénáři incidentů, jež k těmto rizikům vedou.

Řízení aktiv

(1) Povinná osoba v rámci řízení aktiv

a) stanoví metodiku pro identifikaci aktiv,

b) stanoví metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,

c) identifikuje a eviduje aktiva,

d) určí a eviduje garanty aktiv,

e) hodnotí a eviduje primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b),

f) určí a eviduje vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy,

g) hodnotí podpůrná aktiva a zohledňuje přitom zejména vzájemné závislosti podle písmene f),

h) na základě hodnocení aktiv stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv,

i) stanoví přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, a

j) určí způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 k této vyhlášce.

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

a) rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,

b) rozsah dotčených právních povinností nebo jiných závazků,

c) rozsah narušení vnitřních řídicích a kontrolních činností,

d) poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,

e) dopady na poskytování důležitých služeb,

f) rozsah narušení běžných činností,

g) dopady na zachování dobrého jména nebo ochranu dobré pověsti,

h) dopady na bezpečnost a zdraví osob,

i) dopady na mezinárodní vztahy a

j) dopady na uživatele informačního a komunikačního systému.

§ 5

Řízení rizik

(1) Povinná osoba v rámci řízení rizik:

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

b) s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti; přitom zvažuje zejména kategorie hrozeb a zranitelností uvedených v příloze č. 3 k této vyhlášce,

c) provádí hodnocení rizik v pravidelných intervalech podle odstavce 2 a při významných změnách,

d) při hodnocení rizik zohlední relevantní hrozby a zranitelnosti a posoudí možné dopady na aktiva; tato rizika hodnotí alespoň v rozsahu přílohy č. 2 k této vyhlášce,

e) zpracuje zprávu o hodnocení rizik,

f) zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných touto vyhláškou, která

1. nebyla aplikována, včetně odůvodnění,

2. byla aplikována, včetně způsobu plnění,

g) zpracuje a zavede plán zvládání rizik, který 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,

h) při hodnocení rizik a v plánu zvládání rizik zohlední

1. významné změny,

2. změny rozsahu systému řízení bezpečnosti informací,

3. opatření podle § 11 zákona a

4. kybernetické bezpečnostní incidenty, včetně dříve řešených, a

i) v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.

(2) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona provádí hodnocení rizik alespoň jednou ročně a povinná osoba uvedená v § 3 písm. e) zákona alespoň jednou za tři roky.

(3) Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavci 1 písm. d), pokud povinná osoba zabezpečí, že použitá opatření zajistí stejnou nebo vyšší úroveň procesu řízení rizik.