3 TECHNICKÁ BEZPEČNOSTNÍ OPATŘENÍ

Proces pro řízení kybernetických bezpečnostních incidentů je součástí řízení kybernetické bezpečnosti. Primárním cílem systému řízení kybernetické bezpečnosti je zajištění bezpečnosti informací a narušení této bezpečnosti je chápáno v rámci systému jako bezpečnostní incident. Pro zajištění bezpečnosti informací a minimalizaci incidentů bezpečnosti informací existuje v systému řízení kybernetické bezpečnosti řada technických opatření. V této kapitole uvedeme základní typy technických bezpečnostních opatření. Ostatní kategorie opatření (organizační, administrativní, personální atd.) popisujeme v Compliance části (viz Část třetí).

Blíže představíme především základní technická bezpečnostní opatření, která jsou v souladu se standardy rodiny ISO27000.[31] Rozsah a forma použití norem vždy závisí na cílech, rizicích a možnostech konkrétní organizace. I ty organizace, které neusilují o příslušnou certifikaci, mohou využít některá doporučení, která odpovídají jejich potřebám a specifikům.

3.1 Klasifikace informací

Cílem klasifikace informací je, aby každá informace měla úroveň bezpečnosti odpovídající jejímu významu pro organizaci. Toto opatření je klíčové pro zajištění efektivnosti sytému řízení informační bezpečnosti a potažmo procesů řízení kybernetických bezpečnostních incidentů. Klasifikace informací by měla být založena na citlivosti a kritičnosti informace pro organizaci. Pro klasifikaci informací by mělo být vytvořeno klasifikační schéma, které by mělo být konzistentně implementováno v celé organizaci. Všechny dokumenty, které v organizaci vznikají nebo jsou zpracovávány či uchovávány, by měly mít viditelné označení úrovně zabezpečení a podle této úrovně by měly být aplikovány příslušné bezpečnostní mechanismy.

Zavedení systematické klasifikace informací se neobejde bez podpůrného systému pro zajištění ochrany klasifikovaných informací. V praxi jsou často používány systémy typu DLP (Data Loss Protection), které automaticky aplikují příslušné ochranné mechanismy v závislosti na úrovni klasifikace informace, např. automatické šifrování dokumentu nebo e-mailu, pokud je klasifikován jako Interní.

[31] Konkrétně se standardem ČSN ISO/IEC 27035-2:2018.

Příklad klasifikace informací je uveden v následující tabulce:

Úroveň klasifikace	Popis
V – veřejné	Informace jsou přístupné pro každého uvnitř i vně organizace a nevyžadují žádnou zvláštní ochranu. Tyto informace mohou zahrnovat zveřejněné marketingové materiály, zveřejněné finanční výsledky společnosti, zveřejněné nabídky volných pracovních míst a další dostupné informace o organizaci. Vzhledem k povaze těchto informací není označování externě zveřejňovaných dokumentů povinné.
I – interní	Běžné interní informace organizace, které jsou určeny pouze pro zaměstnance a oprávněné třetí strany a nejsou určeny pro veřejnost. Ztráta nebo neoprávněné zveřejnění by bylo nežádoucí, mohlo by poskytnout obchodní výhodu třetím stranám, ovlivnit pověst organizace nebo oslabit některá bezpečnostní opatření. Typickými příklady jsou běžná interní komunikace a e-maily, organizační schémata, telefonní seznamy a informace související s interními činnostmi organizace, obecné interní zásady, normy a procesy. Označení úrovně klasifikace je povinné.
D – důvěrné	Informace podléhající řízenému přístupu a kontrole po celou dobu jejich životního cyklu, včetně specifických postupů pro ukládání, přenos a zničení. Neoprávněné zveřejnění nebo ztráta těchto informací může mít za následek poškození zájmů organizace tím, že způsobí finanční ztráty, porušení zákonů nebo poškodí značku a pověst organizace. Přístup je povolen pouze na základě principu potřeby vědět (need to know) a přístup třetích stran musí být předmětem dohody o mlčenlivosti. Typickými příklady jsou: informace umožňující identifikaci osob (např. údaje o zaměstnancích, spotřebitelích, zákaznících a akcionářích), marketingová strategie, citlivé údaje o zákaznících, smlouvy s dodavateli, prognózy prodeje, zprávy o auditu a rizicích, konkrétní bezpečnostní opatření, dosud nezveřejněné finanční výsledky a podobně.

3.2 Řízení přístupu

Cílem řízení přístupu je **zajištění toho, že k informacím budou mít přístup pouze ti zaměstnanci nebo další osoby, kteří je potřebují pro výkon svojí práce nebo poskytování služeb organizaci**. Řízení přístupu zahrnuje řadu technických bezpečnostních opatření, která jsou specifická pro řízení přístupu uživatelů nebo procesů k jednotlivý vrstvám infrastruktury. V úvahu přichází řízení přístupu do sítě (k síti mohou být připojena pouze autorizovaná zařízení), řízení přístupu k operačnímu systému, databázi, specifické aplikace nebo pro využívání různých internetových služeb.

V praxi se často využívá řešení typu SSO **(Single Sign On)**, které zajišťuje řízení přístupu uživatele do různých aplikací. Uživatel, který se jednou úspěšně autentizuje, již nemusí zadávat své autentizační údaje pro přístup do dalších aplikací, autentizace je zajišťována systémem. V praxi středních a větších organizací je běžné,

že jejich IT prostředí je značně heterogenní a uživatelé pro svoji práci potřebují využívat různé aplikace. Pro řízení přístupu uživatelů v komplexním heterogenním prostředí se používají specifické nástroje typu IDM (Identity Management), které zajišťují správu identit a autentizaci uživatele ve více aplikacích a prostředích.

Specifickou oblastí je řízení **privilegovaných účtů** (např. účtů administrátorů systému). Privilegované účty se od běžných účtů liší v tom, že mají mnohem větší rozsah oprávnění, a jejich případné zneužití tedy představuje pro organizaci výrazně vyšší riziko. Privilegovaný přístup se uděluje jen na omezený časový interval a měl by procházet specifickým schvalováním. Rovněž pro podporu řízení přístupu privilegovaných uživatelů existují specifické nástroje typu PIM/PAM **(Priviledge Identity Management, Priviledge Access Management)**. Zavedení nástroje tohoto typu by měly zvážit zejména organizace, které pro svoji praxi potřebují větší počet privilegovaných uživatelů a účtů.

Relativně novou oblastí řízení přístupu je řízení přístupu nástrojů typu RPA **(Robotic Process Automation)**. Nástroje typu RPA vykonávají určité činnosti v informačním systému nebo aplikaci namísto uživatele systému. Jedná se často o opakující se činnosti, při kterých tito SW roboti vykazují vyšší účinnost a menší chybovost než člověk. RPA se v informačním systému chová podobně jako člověk (při vykonávání určitých činností), potřebuje tedy rovněž řízení přístupu k informacím. Nicméně v porovnání s reálným uživatelem systému má z pohledu řízení přístupu specifické požadavky (například stálé heslo, možnost nepřetržitého připojení do systému apod.).

Dalším technickým opatřením v oblasti řízení přístupu je samotný systém **autentizace uživatele**. Autentizace, potvrzení, že se k účtu přihlašuje oprávněný uživatel, pouze prostřednictvím hesla není v mnoha situacích považována za bezpečnou. V praxi bývá často využívaná tzv. **multifaktorová autentizace** (MFA[32]), kdy se uživatel do systému autentizuje nejen tajnou informací, kterou zná (heslo), ale také prostřednictvím něčeho, co fyzicky má (token, mobilní telefon). V prostředí cloud computing je třeba považovat MFA za standard pro autentizaci jednotlivých uživatelů.

3.3 Kryptografie

Kryptografické prostředky patří mezi silná bezpečnostní opatření, pomocí kterých lze chránit zejména důvěrnost, integritu a autenticitu informací. Různé druhy kryptografických technik se uplatňují při různých aspektech provozování informačních

[32] Obecněji řečeno, vícefázové ověření (Multi-factor authentication, MFA) je proces pro přihlášení k webové stránce nebo aplikaci za využití dvou nebo více důkazů (faktorů) potvrzujících identitu uživatele. Jedná se o kombinaci faktorů u kategorií znalost (něco, co ví pouze uživatel, např. heslo), vlastnictví (něco, co má pouze uživatel, např. mobilní zařízení, token) a charakteristika (něco, čím je pouze daný uživatel, např. biometrický údaj).

systémů: při autentizaci uživatelů, při ochraně důvěrnosti a integrity přenášených informací (šifrování v rámci komunikačních protokolů) nebo při ochraně uložených informací (šifrování paměťových médií). Zabezpečení informací pomocí šifrování bývá implementováno i v rámci dalších bezpečnostních opatření, např. systémy pro klasifikaci informací poskytují i funkcionalitu automatického zašifrování dokumentů v závislosti na úrovni klasifikace (dokumenty klasifikované jako důvěrné jsou automaticky zašifrovány).

Při využívání cloudových řešení je také nutno rozhodnout, zda organizace využije šifrování dat nabízené poskytovatelem cloudu, nebo zda využije vlastní **šifrovací klíče**, resp. šifrovací klíče od odlišného poskytovatele. První varianta je obvykle finančně i technicky dostupnější, znamená ale, že poskytovatel cloudu, který se podílí na zpracování dat v šifrované podobě, má technicky k dispozici možnost data dešifrovat. Druhá varianta posiluje bezpečnost informací a snižuje riziko neoprávněného přístupu k nim.

3.4 Provozní bezpečnost

Opatření provozní bezpečnosti zahrnuje řadu technických opatření, která jsou aplikovatelná na různých vrstvách architektury informačních systémů. Základním technických opatřením je **oddělení prostředí vývoje, testování a provozu**. Toto opatření snižuje rizika neoprávněného přístupu k informacím, riziko zavlečení nových zranitelností do systému a riziko nespravené konfigurace systému. Různá prostředí pro provoz, vývoj a testování by měla také být součástí procesů změnového řízení. Je zřejmé, že při vývoji systémů nebo testování systémových změn existuje vyšší riziko vzniku chyby, proto je nutné, aby tyto aktivity byly prováděny na prostředích oddělených od provozního prostředí.

Dalším klíčovým opatřením provozní bezpečnosti je **ochrana proti malware**. Cílem tohoto opatření je včasná detekce, prevence a zotavení z útoku využívajícím škodlivý SW. Útoky využívající nějakým způsobem zavlečení škodlivého kódu patří k nejčastějším (viz klasifikace incidentů v předchozí kapitole). Technickým řešením poskytujícím základní ochranu proti malware jsou různé antivirové systémy.

Při implementaci antimalware nástroje je důležité si uvědomit, kterými kanály může škodlivý kód do organizace proniknout. V dnešní době již není dostatečná ochrana proti malware zaměřená pouze na ochranu koncových stanic (počítačů) a serverů, ale je třeba se zaměřit i na další zařízení, která mohou být připojena do informačního systému (mobilní telefony, tablety, včetně vlastních zařízení zaměstnanců a dalších spolupracujících osob, pokud se z nich mohou připojit do systému organizace apod.), zaměřit se na ochranu mailových serverů, zamezit zavlečení škodlivého SW prostřednictvím e-mailu, a v neposlední řadě zabránit zavlečení škodlivého SW z prostředí Internetu.

Vzhledem k různým kanálům pro zavlečení škodlivého SW do systému se liší i technické systémy pro ochranu proti malware. Antivirovou ochranu poskytují

různé bezpečnostní služby typu webové proxy servery,[33] které zabraňují šíření malware prostřednictvím internetového prohlížeče a blokují webové servery se škodlivým obsahem. Dalším nástrojem jsou specifické antivirové systémy na úrovni mailového serveru, které mají schopnost zablokovat e-mail obsahující přílohu s malwarem nebo dokážou identifikovat e-mail, který obsahuje internetový link na webovou stránku se škodlivým obsahem. Existují i antivirové systémy určené pro mobilní technologie apod.

Klíčovým prvkem pro efektivnost fungování těchto technologií je pravidelná aktualizace tak, aby byly schopny identifikovat i nejnovější malware. Moderní antivirové systémy používají pokročilé metody detekce, které nejsou založeny pouze na tradičním rozpoznávání signatur známého malware, ale používají prvky umělé inteligence a behaviorální analýzy.

Současným trendem v této oblasti jsou technologie typu **EDR** (Endpoint Detection and Response), které v sobě kombinují řadu bezpečnostních funkcionalit pro ochranu koncových zařízení (ochrana proti malware, monitoring podezřelého chování systému/uživatele, scanování zranitelností). Informace získané ze systémů EDR bývají často zasílány do nástrojů pro monitoring a reakci na incidenty (nástroje typu **SIEM** – Security Information and Event Management) pro další zpracování v rámci procesu řízení incidentů kybernetické bezpečnosti. Ochrana koncových zařízení pomocí systémů typu EDR je relativně finančně náročná a vyžaduje spolupráci s nástroji typu SIEM, je tedy zřejmé, že tato bezpečnostní opatření realizují spíše střední a velké organizace, zatímco menší organizace používají klasickou ochranu proti malware (antivir).

Dalším typickým opatřením provozní bezpečnosti je **zálohování**. Jeho cílem je zamezit riziku ztráty dat. Zálohování by mělo být integrální součástí systému řízení informační bezpečnosti. U každého systému by mělo být zřejmé a jasně definované, jaká je jeho politika zálohování, tj. jak často a v jakém rozsahu má záloha proběhnout. Se zálohováním úzce souvisejí postupy pro obnovu systémů. Obnova systémů ze záloh by měla být pravidelně testována. Organizace by měla mít nadefinována pravidla, jak je se zálohami nakládáno, kde jsou uloženy, jak jsou zabezpečeny (např. šifrováním) a jak často probíhá testování obnovy ze záloh.

3.5 Logování a monitoring

Z pohledu řízení bezpečnostních incidentů patří **logování a monitoring** činnosti uživatelů mezi klíčová opatření. Organizace by měly (na základě analýzy rizik, viz Část třetí, Kapitola 4) definovat, které události v informačním systému budou zaznamenány do logu (např. záznam nových dat, jejich změna, výmaz, nebo i přístup

[33] Proxy server je HW nebo SW nástroj, který funguje jako prostředník mezi uživatelem a cílovým počítačem. Vůči cílovému počítači vystupuje sám jako uživatel a přijatou odpověď následně odesílá zpět uživateli.

k chráněným informacím) a pak dále zpracovávány v monitorovacím nástroji typu SIEM. Hlavní funkcionality systémů typu SIEM je agregace dat z různých logů (logy z aplikací, databází, síťové prvky typu firewall, bezpečnostní SW) a také korelace dat, při které se systém SIEM snaží nalézt vzájemné souvislosti mezi záznamy v lozích s cílem identifikovat potenciálně nebezpečnou událost. Systémy typu SIEM jsou založeny na implementaci pokročilých algoritmů umělé inteligence a na historických znalostech o typech útoků. Vzhledem k tomu, že každým dnem vznikají nové a nové útoky, je třeba zajistit pravidelnou aktualizaci znalostní báze systému SIEM.

3.6 Řízení zranitelností

Posledním technickým opatřením provozní bezpečnosti, které na tomto místě krátce popíšeme, je **řízení technických zranitelností (vulnerability management)**. Jeho primárním cílem je včasná identifikace zranitelnosti IT systémů organizace a zabránění jejímu zneužití. Jedná se o cyklický proces scanování, posouzení a mitigace zranitelností. Implementovat řízení technických zranitelností je nutné zejména pro systémy, které jsou přímo exponovány do sítě Internet a jsou tedy častým cílem útočníků, kteří se nejčastěji snaží k útoku využít nějakou existující, známou zranitelností systému.

Prvním krokem procesu je **scanování zranitelností**, které probíhá pomocí bezpečnostního nástroje (security scanner), který slouží k odhalení zranitelností. V dnešní době i tyto nástroje používají pokročilé algoritmy umělé inteligence a jsou rovněž založeny na rozsáhlých databázích znalostí o existujících zranitelnostech.[34] Dalším krokem systému řízení technických znalostí je jejich posouzení a prioritizace. Posouzení a prioritizace probíhá z pohledu závažnosti zranitelnosti a z pohledu náročnosti implementace opatření. Mitigace zranitelnosti probíhá nejčastěji prostřednictvím implementace bezpečnostní záplaty (patch) v rámci procesu **patch managment**. Pokud není k dispozici pro zjištěnou zranitelnost systému bezpečnostní záplata, patch, je třeba implementovat doplňková opatření, která mohou zmírnit riziko zneužití zranitelnosti, např. zvýšená intenzita monitoringu zranitelného zařízení.

Dalším technickým opatřením, které má v kybernetické bezpečnosti nezastupitelnou úlohu, je **penetrační testování**. V tomto případě se jedná o otestování odolnosti systému proti kybernetickému útoku pomocí strategií, metod a nástrojů, které používají útočníci. Vzhledem k tomu, že se jedná o použití obvyklých metod útočníků, je třeba aby penetrační testování bylo striktně řízeno z pohledu časového (v jakém období bude probíhat), z pohledu použitých technik (z penetračního testování mohou být například vyřazeny techniky, které mohou způsobit přímé

[34] Např. volně dostupný systém znalostí je databáze známých zranitelností a chyb zabezpečení provozovaná organizací MITRE. Dostupné z: www.cve.org.

škody v testovaném systému) a z pohledu rozsahu (které systémy budou předmětem testování). Cílem penetračního testování je ověřit odolnost systému proti útoku a nalezení případných slabých míst. Někdy bývá cílem testování rovněž posouzení schopnosti organizace reakce na útok a zabránění útoku. V tomto případě je o penetračních testech informován jen omezený okruh zaměstnanců organizace a sleduje se a vyhodnocuje se schopnost organizace reagovat na „reálný" kybernetický útok, zejména včasná identifikace incidentu, jeho interní oznámení, posouzení, řešení atd. (viz Část druhá).

3.7 Celkový kontrolní rámec

V předcházejících bodech jsme stručně představili základní technická opatření pro zajištění informační bezpečnosti. V praxi je vhodné tato patření a další kontrolní mechanismy (viz Část třetí, Kapitola 5 a 6) uspořádat do formalizovaného kontrolního rámce, který jednoznačně definuje kontrolní mechanismus, určí vlastníka, četnost provádění a způsob vedení evidence o provedení kontrolního mechanismu. Kontrolní rámce pro oblast informační (kybernetické) bezpečnosti jsou často vyvíjeny a publikovány organizacemi, které se zabývají tvorbou standardů v oblasti zajištění kybernetické bezpečnosti.

Inspiračním zdrojem IT kontrolního rámce může být například Cybersecurity Framework Version 1.1[35] vyvinutý organizací NIST.

Příklad části kontrolního rámce v oblasti kybernetické bezpečnosti je uveden v následující tabulce:

Tabulka č. 2 Příklad kontrolního rámce.

Rámec kontrol IT							
Oblast	**Podoblast**	**Riziko**	**Kontrolní opatření**	**Číslo kontrolního opatření**	**Vlastník kontrolního opatření**	**Frekvence provádění**	**Dokumentace/ evidence**
Kybernetická bezpečnost	Bezpečnostní politika	Nedefinované nebo v rámci organizace nekomunikované zásady v oblasti informační bezpečnosti informací mohou vést k jednání narušujícímu informační bezpečnost.	Existuje politika informační bezpečnosti, je pravidelně aktualizována, komunikována a je dostupná pro všechny zaměstnance organizace.	SP.1	Manažer kybernetické bezpečnosti	Roční	Politika dostupná pro všechny zaměstnance, evidence o komunikaci politiky zaměstnancům.

[35] https://www.nist.gov/cyberframework/framework.

Rámec kontrol IT							
Oblast	**Podoblast**	**Riziko**	**Kontrolní opatření**	**Číslo kontrolního opatření**	**Vlastník kontrolního opatření**	**Frekvence provádění**	**Dokumentace/ evidence**
Kybernetická bezpečnost	Řízení přístupu do aplikací	Neadekvátní autentizační mechanismy mohou vést k narušení bezpečnosti aplikace a informací v ní zpracovávaných.	Aplikace zpracovávající finanční informace musí mít implementovánu dvoufaktorovou autentizaci.	AC.1	Aplikační manažer	6 měsíců	Nastavení autentizační politiky aplikace.
		Nevhodná hesla mohou vést k narušení bezpečností aplikace a informací v ní zpracovávaných.	Doménová hesla musí být silná a měněna v pravidelných intervalech.	AC.2	Manažer IT infrastruktury	6 měsíců	Politika hesel na doméně.

Rámec kontrol IT							
Oblast	**Podoblast**	**Riziko**	**Kontrolní opatření**	**Číslo kontrolního opatření**	**Vlastník kontrolního opatření**	**Frekvence provádění**	**Dokumentace/ evidence**
Kybernetická bezpečnost	Bezpečnost infrastruktury	Nedostatečné zabezpečení sítě proti neoprávněnému přístupu z externích sítí.	Interní síť musí být oddělená od externí prostřednictvím firewallu. Politika nastavení firewallu musí být pravidelně kontrolována.	SM.1	Manažer síťové infrastruktury	2 měsíce	Dokument o provedené kontrole (review) adekvátnosti nastavení bezpečnostních politik.
	Ochrana proti malware	Nedostatečná ochrana proti malware může vést ke kompromitaci bezpečnosti informací.	Prostředky ochrany proti malware musí být pravidelně aktualizovány.	MP.1	Manažer koncových stanic	Měsíčně	Zpráva o úplnosti a včasnosti aktualizace antivirové ochrany.

Z uvedené tabulky je patrné, že kontrolní rámec musí reagovat na rizika, kterým je organizace vystavena, proto je důležité, aby i technická opatření (kontroly) v oblasti kybernetické bezpečnosti byla založena na analýze rizik (Část třetí, Kapitola 4).