MVŠO

BEZPEČNOST ICT A OCHRANA DAT

STUDIJNÍ OPORA PRO KOMBINOVANÉ STUDIUM

BEZPEČNOST ICT A OCHRANA DAT

Ing. Jindřich KODL, CSc.

Prof. Ing. Vladimír SMEJKAL, CSc., LL.M.

Moravská vysoká škola Olomouc, o.p.s., 2018

Autoři: Ing. Jindřich KODL, CSc.,

Prof. Ing. Vladimír Smejkal, CSc., LL. M.

Olomouc 2018

Obsah

Kapitola 1

Úvod do problematiky bezpečnosti

Po prostudování kapitoly budete umět:

- formulovat základní pojmy, týkající se systému ochrany informací v informačních a komunikačních systémech
- charakterizovat hlavní zásady při zajištění bezpečnosti informací v celém životním cyklu jejich správy v informačním systému
- využít metodické zásady a požadavky uváděné bezpečnostními normami řady ČSN ISO/IEC 27000.

Klíčová slova:

Systém ochrany informací, ČSN ISO/IEC řada 27000.

1.1 Vývoj problematiky v oblasti bezpečnosti

Tematicky je předmět zaměřen na zdůraznění hlavní zásady při zajištění bezpečnosti informací, tj. že vytvoření zabezpečeného informačního prostředí vyžaduje realizaci efektivního systému řízení bezpečnosti informací kombinujícího řešení pro lidi, procesy a technologie.

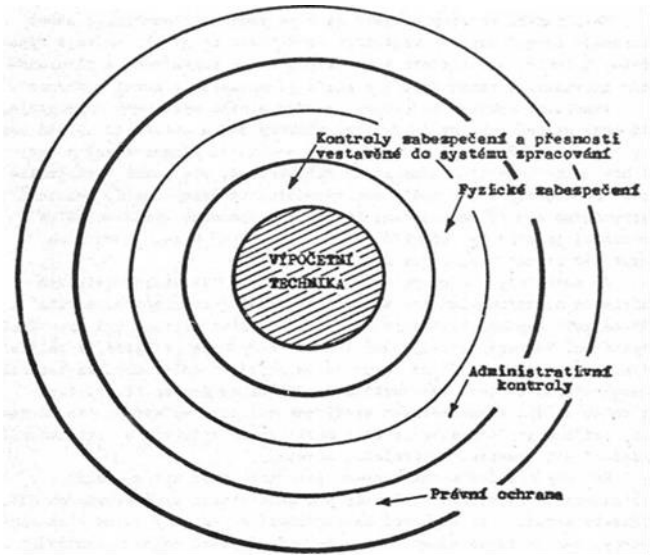
Tato kapitola obsahuje vymezení základních pojmů a zásad, které se vztahují k bezpečnosti informací a zkoumá základní součásti systému zabezpečení informací při návrhu a provozování informačních systémů. Jednotlivé kapitoly jsou zaměřeny na celou dobu životního cyklu informačního systému – od jeho návrhu, přes nasazení do prostředí ICT podniku, tak i jeho provozování. Přitom je klíčovým momentem řešení systému řízení bezpečnosti informací, dodržování souladu s platnými bezpečnostními normami (řady ČSN ISO/IEC 27000). Soulad s bezpečnostními normami, se promítá i při řešení bezpečnosti u elektronických dokumentů, kdy jsou využívány nástroje, jako jsou elektronický podpis, elektronická pečeť a časové razítko aj. Koncepční řešení systémů řízení bezpečnosti informací není již jen technickou záležitostí. Realizace zabezpečených informačních systémů musí být v souladu jak právními předpisy ČR, viz např. zákon č. 297/2016 Sb, tak musí splňovat podmínky Nařízení EU, viz např. Nařízení eIDAS.

Vývoj v přístupu k řešení problematiky bezpečnosti v informačních systémech musel reagovat na rozvoj výpočetních i komunikačních technologií.

S vývojem sálových počítačů souviselo budování výpočetních středisek. Výpočetní technika byla umístěna v uzavřených prostorách, uživatelé pracovali s daným počítačem prostřednictvím zakázek, kdy zadané úlohy uživatelé dostávali ve formě zpracovaných zakázek (výsledky zadané úlohy ve formě sjetin – na děrných páskách, štítcích nebo tisků). Následně pak komunikace uživatelů s výpočetní technikou probíhala prostřednictvím terminálů umístěných v k tomu zřízených prostorách ve výpočetním centru.

Ve výpočetních centrech ochrana dat se orientovala na bezpečnost a přesnost zpracovávaných dat a na dodržování oprávněnosti přístupu k datům zajišťované vesměs v rámci fyzické bezpečnosti.

Základy metodiky ochrany informace ve výpočetních střediscích vycházely z kontrol zabudovaných do vlastního výpočetního systému i v řešení bezpečnostního perimetru daného střediska, které tvořilo uzavřený systém. Jednotlivé kontrolní sféry při řešení ochrany zpracovávaných dat jsou ukázány na následujícím obrázku.



Obrázek 1.1 Tradiční sféry bezpečnosti podniku

Dominantní úlohu zde hrála fyzická ochrana výpočetního střediska a administrativní kontrolou uživatelů. Bezpečnostní projekty tak řešily opatření k zajištění uzavřeného prostoru, neboť zpracovávané informace se v elektronické podobě z tohoto prostoru nedostaly.

Tato koncepce bezpečnostních opatření se radikálně změnila s vývojem systému malých elektronických počítačů (např. PDP-11), osobních počítačů, komunikačních sítí a zejména Internetu.

Řešení bezpečnosti zpracovávaných informací už není možné realizovat v hranicích pevně definovaného perimetru obklopujícího uzavřený prostor. Současné podnikové útvary, které zodpovídají za systém řízení bezpečnosti informací již nemohou spoléhat na vytvoření fyzického perimetru okolo podniku, ale realizovat bezpečnostní perimetr s cílem vytvořit bezpečné rozhraní mezi podnikovou sítí a vnějším komunikačním prostředím. Fyzická ochrana přitom tvoří jen jednu z částí tohoto perimetru.

Řešení bezpečnosti již musí zahrnout všechny možné přístupy ke zpracovávaným informacím, a to jak z interního prostředí podniku, ale zejména z vnějších sítí. Součástí bezpečnostního perimetru je celá řada bezpečnostních nástrojů, které zajišťují bezpečný přístup ke zpracovávaným informacím.

1.2 Pojem bezpečnost

Lze tedy konstatovat, že pojem „bezpečnost“ se ve vztahu k výpočetním a komunikačním systémům zpracovávajícím informace de facto změnil v pojem „informační bezpečnost“.

Pojem „Informační bezpečnost“ v sobě zahrnuje komplexní systémový přístup při zajištění ochrany informací v celém jejich životním cyklu, tj. ochranu odpovídajících technologických, programových i organizačních komponent IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny.

Do takto formulované informační bezpečnosti pak spadá i komunikační bezpečnost, tj. ochrana informace přenášené mezi výpočetními prostředky (počítači, servery apod.), fyzická bezpečnost, tj. ochrana před přírodními hrozbami i hrozbami způsobenými lidským faktorem a personální bezpečnost, tj. ochrana před zaměstnanci podniku.

1.3 Podniková bezpečnost informací

U podnikové bezpečnosti informací je třeba brát zvláštní zřetel na charakter podniku.

Specifika bezpečnosti informací u podnikového informačního systému souvisí ochranou podnikových business procesů. Bezpečnostní opatření, která jsou realizována na základě analýzy rizik podnikových procesů musí být na takové úrovni, aby nebyla ohrožena kontinuita činností podniku. S tím souvisí i zajištění požadavků na podnikový informační systém ve vztahu k dostupnosti, aktuálnosti, správnosti a důvěryhodnosti realizovaných příslušných funkcí a procesů. Z pohledu bezpečnosti podnikového informačního systému, resp. aplikací a s tím souvisejícího zabezpečení zpracovávaných dat proti:

- Neoprávněnému přístupu,
- Odcizení dat,
- Zničení dat.

V případě podnikové bezpečnosti informací, resp. zpracovávaných dat je vždy významným aspektem ekonomické hledisko návrhu realizovaných opatření. Zajištění požadované bezpečnosti musí vycházet z charakteru podnikových procesů, aby „nepřiměřená bezpečnost“, neměla negativní dopad na kvalitu aplikací a s nimi souvisejících služeb poskytovaných podnikem.

1.4 Bezpečnost ICT/IS

Jedno z možných dělení informační bezpečnost vychází z prostředí, ve kterém je informační bezpečnost uplatňována, tj. prostředí ICT.

ICT je zkratka Information and Communication Technologies, tj. česky informační a komunikační technologie. Zkratka ICT se stále více používá než původní IT, neboť výpočetní prostředky jsou stále více začleněny do komunikačního prostředí. Zejména je třeba zdůraznit význam Internetu, ale i v poslední době jakýchkoliv dalších přenosných zařízení (mobilních telefonů, tabletů).

Pod pojmem ICT musíme vidět nejen zařízení (hardware počítačů, serverů nebo komunikačních prostředků), ale i programy a aplikace (software).

IS je zkratka informačního systému, nás bude provázet v podstatě všemi kapitolami, kdy úvodem lze informační systém chápat jako celek složený dvou částí – automatizované, tj. počítačového hardwaru a souvisejícího softwaru, zajišťující procesy zpracování dat, a neautomatizované, ke které patří uživatelé a informace, většinou v listinné podobě, které se zpracovávají ručně.

Do kategorie informačního systému je nutné zařadit podnikový informační systém (PIS), který lze charakterizovat jako systém, který podnik využívá k zajištění svých činností a podpoře podnikových procesů. Díky automatizaci činností tak může zvýšit kvalitu služeb, zajistit práci s velkými objemy dat apod. Podnikové informační systémy se používají ve všech úrovních podniku.

1.5 Popis základních hrozeb;

Pro zabezpečení provozu IS je nutné znát hrozby, které mohou ovlivnit jeho chod. Tyto hrozby mohou vyvolat situace, které mají negativní dopad na ICT, kdy tím, že způsobí:

- výpadek výpočetního systému,
- výpadek komunikačního systému,
- ztrátu zpracovávaných dat,
- celkový výpadek informačního systému.

Podle původu lze hrozby roztřídit na:

- hrozby přírodní – záplavy, požáry, blesky
- hrozby vyvolané lidskou činností
    - úmyslná činnost – krádeže zařízení, modifikace, znepřístupnění, krádeže dat jak ze strany zaměstnanců, tak i „nepřátel“
    - neúmyslná činnost – chybná manipulace se zařízeními, neodborná práce s daty

Problematice hrozeb, zranitelností a rizik jsou věnovány další kapitoly, kde jsou objasněny nejen samotné pojmy, ale zejména jsou zde detailně popsána bezpečnostní opatření, reagující na jednotlivé druhy hrozeb.

1.6 Právní předpisy a technické normy pro oblast bezpečnosti ICT

Problematice právních předpisů a technických norem týkajících se oblasti bezpečnosti informací jsou věnovány další kapitoly, ve kterých je podrobně uveden jejich účel i význam při budování systému řízení bezpečnosti informací spravovaných v informačních systémech.

Zde na úvod je uveden pouze výčet základních bezpečnostních předpisů a norem, které je nutné považovat jako významnou, a ve většině případů jako nutnou pomůcku při návrhu, realizaci a provozu systémů řízení bezpečnosti ICT/IS, resp. jednotlivých bezpečnostních opatření nasazených do informačních systémů.

Právní předpisy

- Nařízení Evropského parlamentu a Rady (EU) 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (General Data Protection Regulation – GDPR) – vstupuje v účinnost 25. 5. 2018,
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
- Zákon č. 480/2004 Sb., o některých službách informační společnosti,

- Zákon c. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti,
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- Zákon č. 40/2009 Sb., trestní zákoník.

Technické normy

- ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky;
- ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací;
- ČSN ISO/IEC 27005:2009 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Do výkladu je zařazena rovněž problematika kybernetické kriminality včetně jejího odhalování a vyšetřování. Současně lze tento předmět považovat za úvod do kryptologie.

1. Formulujte základní pojmy, týkající se systému ochrany informací v informačních a komunikačních systémech;
2. Charakterizujte hlavní zásady při zajištění bezpečnosti informací v celém životním cyklu jejich správy v informačním systému;
3. Popište metodické zásady a požadavky uváděné bezpečnostními normami řady ČSN ISO/IEC 27000;

Literatura k tématu:

[1] Smejkal, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9

Kapitola 2

Vícevrstvá bezpečnost informačních systémů

Po prostudování kapitoly budete umět:

- definovat základní pojmy bezpečnosti informací;
- charakterizovat systém, informační podnikový informační systém;
- vysvětlit zásady realizace vícevrstvé ochrany informací v systémech.

Klíčová slova:

Systém, informační systém, podnikový systém, bezpečnost informací vícevrstvá ochrana.

2.1 Systém

Systém je složitý reálný nebo abstraktní objekt, ve kterém jsou rozlišeny části, vztahy mezi nimi a jeho vlastnosti a který vůči okolí vystupuje jako celek. Lze jej chápat jako množinu prvků a vazeb mezi nimi, které jsou účelově definovány na nějakém objektu. S fungováním systému jsou pak spojeny vzájemně související jevy, věci a procesy. Významnou roli při fungování systémů hrají nastavená pravidla. Při definování systémů vycházíme z následujících charakteristik, kdy:

- každý systém se skládá z určité množiny prvků,
- prvky jsou části, na které je možné a účelné systém dělit,
- systém je možné členit na subsystémy,
- každý systém je součástí vyššího systému (supersystému), jehož je subsystémem,
- systém je propojen s okolím, na které reaguje, proto hovoříme o dynamickém systému,
- systém vyjadřuje interaktivnost prvků (vztahy mezi nimi),
- systém může existovat samostatně (bez určení vztahu k jinému systému).

2.2 Informační systém jako speciální případ systému

Nejdříve je třeba definovat pojmy:

Informace

Informace je poznatek, týkající se jakýchkoliv objektů, tedy faktů, událostí, myšlenek nebo pojmů, které dostávají zvláštní význam díky kontextu, do něhož jsou zařazeny. Jsou jakýmkoliv projevem, který může mít smysl pro příjemce nebo toho, kdo je vysílá. [1]

Data

V informatice tvoří informaci strukturovaná data, která lze vysílat, přijímat, uchovávat a zpracovávat technickými prostředky. Data jsou vstupem či výstupem informačního systému.

[1] Smejkal, V., Rais, K. Řízení rizik ve firmách a jiných organizacích

Metadata

Metadata jsou strukturovaná data o datech.

Informační systém

Informační systém je množina prvků ve vzájemných informačních a procesních vztazích (informační procesy). Informační systémy zpracovávají data a zabezpečují komunikaci informací mezi prvky.

Všeobjímající definice z Encyklopedie Britanica charakterizuje informační systém jako *integrovanou sadu komponent pro sběr, ukládání a zpracování dat a poskytování informací, znalostí v digitálních produktech*.

Informační systémy lze dělit podle:

ÚČELU

- systémy zpracování dat
- komunikační systémy

PROSTŘEDÍ

- podnikové informační systémy (Enterprise Information Systems, EIS)
- veřejné informační systémy (Public Information Systems) - veřejné knihovny apod.

FUNKCE

- dokumentografické (dokumentačně-rešerní – Storage and Information Retrieval Systems)
- faktografické (Management Information Systems)
- měřicí, regulační (používané v IS pro řízení technologických procesů)

REŽIMU ČINNOSTI

- individuální zpracování požadavků (např. na osobním počítači)
- dávkové zpracování dat (tradiční ASŘ na střediskových počítačích)
- zpracování dat v reálném čase (rezervace letenek, technologické procesy, diagnostické systémy)
- zpracování dat v centralizovaných databázích (serverové farmy)

Rozhodující součástí informačních systémů jsou prostředky zajišťující bezpečnost zpracovávaných a předávaných informací. Při projektování informačního systému musí bezpečnostní technologie být integrovány jak do výpočetní platformy, tak i do celé organizační struktury informačního systému. Nedílnou součástí informačních systémů se v současné době stává SIEM (Security Information and

Event Management) management bezpečnostních informací a událostí postihující problematiku zabezpečení spravovaných informací v celém jejich životním cyklu.

Podnikový informační systém

Podnikový informační systém je specifická forma informačního systému. Tvoří jej dohromady prostředky informační a komunikační technologie (hardware a software), které zajišťují pro podnikové business procesy sběr, přenos, ukládání a zpracování dat. Tvoří uzavřený systém, jehož součástí je i personál (uživatelé).

Podnikový informační systém je nedílnou součástí podniku, musí tedy být vytvářen „na míru“, který má plnit určité úlohy nikoli pro jednoho uživatele, nýbrž pro celou organizaci.

Podnikové informační systémy při provádění a řízení svých operací, komunikaci se svými zákazníky a dodavateli, a konkurenci na trhu. Přitom se informační systémy využívají k zajištění dodavatelských řetězců a elektronických trhů.

Na zajišťování informačních služeb je nutné podnikový informační systém chápat ve dvou rovinách, resp. částech:

- automatizovaná část, procesy zajišťované s využitím informační technologie (IT)
- neautomatizovaná část – tj. činnosti s dokumenty v „papírové“ podobě, zpracovávané ručně.

2.3 Vzájemná provázanost tří základních aspektů (technologie, procesy, lidé)

Zavedení programu bezpečnosti informací do prostředí podniku vyžaduje v současné době správnou a vyváženou kombinací tří základních aspektů:

- technologií;
- procesů;
- personálu podniku.

S tím jsou spojeny následující požadavky:

Investice do nových technologií musí být v souladu s tzv. úrovňovou informační bezpečností.

Řešení jednotlivých procesů, projektů i zajišťování provozu podniku musí probíhat v souladu s bezpečnostními opatřeními.

Efektivní bezpečnostní program musí vycházet z bezpečnostního vědomí a relevantních výsledků bezpečnostních hodnocení

Cílem bezpečnostních aktivit je realizace efektivního programu informační bezpečnosti, kdy jsou v rovnovážném stavu rizika podniku a vynakládané investice na jeho rozvoj.

Technologie

Technologie je základním prvkem efektivního programu zabezpečení informací, který je nejvíce zdůrazňován. Způsob řešení bezpečnosti pomocí technologických prostředků je zdůrazňován zejména dodavateli HW či SW produktů. Ale aby technologie umožnila zajistit požadavky v oblasti zabezpečení informací, nelze spoléhat na to, že technologie samotná vyřeší informační bezpečnost.

V případě nekoncepčnosti, kdy se řešitelé informačních systémů výhradně zaměřují na technologii, mohou vytvořit pocit bezpečí a mohou vystavit společnost zbytečným rizikům.

Informační technologie mají v programu informační bezpečnosti zásadní vliv na efektivnost realizovaného bezpečnostního programu.

Z pohledu bezpečnosti zpracovávaných informací plyne nutnost řešit na úrovni technologií zejména následné požadavky:

- autentičnost, dostupnost a integritu zpracovávaných informací v podnikovém informačním systému (zajištění oprávněného přístupu, problematika neodmítnutelnosti činností uživatelů systému, zabezpečené uložení);
- základní nástroje a metody správy systému ochrany informací;
- systém autentizace – např. elektronický podpis a jeho využití, PKI, certifikační autority;
- kryptografické prostředky;
- právní aspekty, normotvorné a legislativní úpravy.

Ale z pohledu zajištění systému bezpečnosti informací je třeba řešit technologické komponenty ve shodě s navrhovanými bezpečnostními procesy a s možnostmi a schopnostmi lidí (uživatelů i odborného personálu).

Procesy

Dobře definované zásady, standardy a postupy, tj. procesy informační bezpečnosti, jsou základem při řešení programu, který má zajistit požadovanou míru zabezpečení informací.

Základním atributem je vypracování a schválení bezpečnostní politiky, která vyváří základní rámec pro program zabezpečení informací v daném podniku či organizaci. Bezpečnostní politika stanoví zásady přístupu ke klíčovým interním systémům pouze vymezenému počtu autorizovaných uživatelů.

Rozpracování bezpečnostní politiky do bezpečnostních směrnic a předpisů pak dokumentuje zásadní přístup pro výběr technologií a procesů pro různé činnosti.

Vypracované normy mohou také definovat, které organizační celky mají přístup k definovaným aplikacím apod.

Vybudování systému řízení bezpečnosti informací spočívá mj. na vypracování podrobných pokynů, které stanoví uživatelům podmínky a požadavky pro zajišťování jejich činností bezpečným způsobem.

Klíčové zásady pro podnik zahrnují správu administrace, kde je důležité řízení oprávněného přístupu k daným agendám. Je důležité zajistit, aby uživatelé měli přístup pouze k systémům, které potřebují k výkonu své práce. Musí být zajištěno, aby uživatelé měli přístup k citlivým informacím pouze na základě „potřeby poznat“ (need to know). U citlivých informací je nutné při jejich zpracování vždy zajistit plnění zásady „čtyř očí“.

Efektivní procesy zabezpečení informací jsou nezbytnou součástí efektivního programu zabezpečení informací. Bezpečnostní normy (například ČSN ISO/IEC řady 27000) vyžadují při zajišťování bezpečnosti informací procesní přístup, neboť se jedná o zásadní pojítko mezi uživateli a technologickým produkty a zajišťují, že jsou dodržovány základní aspekty při řešení:

- autentizace, autorizace a správy účtů (v anglickém jazyce se uvádí jako zásada AAA – Authentication, Authorisation, Accounting);
- firewallů / virtuálních privátních sítí (VPN);
- škodlivého software;
- řízení zranitelnosti;
- detekce narušení, Prevence narušení;
- filtrování obsahu;
- šifrování – významnou kapitolu při řešení bezpečnostních aspektů zaujímá šifrová ochrana informací – v rámci řešení bezpečnostních opatření se jedná zejména o využití kryptografických metod a jejich integrace do bezpečnostních protokolů.

Lidé

Klíčové faktory, týkající se lidského faktoru, které je třeba vzít v úvahu při vytváření příslušné organizace pro zabezpečení informací v rámci podniku, zahrnují velikost, strukturu a zaměření business

procesů daného podniku. Malý podnik, tvořený několika odděleními, má např. významně odlišné organizační požadavky od velkého nadnárodního podniku.

Velikost podniku obvykle určuje, zda je realizován bezpečnostní útvar, nebo jsou v organizační struktuře určeni jen pracovníci zodpovědní za bezpečnost, nebo že je tato zodpovědnost převedena na jinou organizací (outsourcing, SaaS). Větší společnosti využívají externí organizace pro vytváření bezpečnostních strategií, zajištění vývoje, správy bezpečnostních událostí či servisu.

Z pohledu organizace podnikové informační bezpečnosti je nezbytná role bezpečnostního pracovníka informačního systému a jeho začlenění do bezpečnostních procesů;

Bezpečnostní pracovníci musí pravidelně kontrolovat a aktualizovat bezpečnostní strategie. Bezpečnostní pracovníci provádějí pravidelné interní bezpečnostní audity, vyžadují pravidelná bezpečnostní školení pro uživatele apod.

2.4 Vícevrstvé, hloubkové zabezpečení informačních systémů

Návrh a realizace nových technologií zajišťujících bezpečnost musí být v souladu s tzv. víceúrovňovou informační bezpečností.

Řešení jednotlivých procesů, projektů i zajišťování provozu podniku musí zahrnout mj.:

- architekturu funkčního modelu bezpečnostních služeb v IS;
- vytvoření bezpečnostních perimetrů (realizace demilitarizované zóny – firewaly a jejich dislokace, kontrola a správa, systémy detekce průniku, detekce obsahu transakcí, detekce zranitelností, ochrana proti škodlivému SW);
- bezpečnost komunikačních sítí podniku; architektura zabezpečení vzdáleného přístupu; bezpečnostní protokoly;

a s tím spojené zavedení systému řízení bezpečnosti informací do struktury podniku, definice postupů a procesů při řízení rizik, návrh bezpečnostních procesů a implementace bezpečnostních opatření.

Efektivní architektura pro jakýkoli program zabezpečení informací zahrnuje vrstvení zabezpečení, které poskytuje více úrovní obrany. Jedná se o tzv. hloubkovou ochranu. Ta zahrnuje strukturování

informačního prostředí do několika digitálních zón a zajištění ochrany ve všech vrstvách informačního systému, resp. sítě, při základním dělení vrstev na brány (gateway), servery a uživatele.

Brána (Gateway) je síťový uzel, tj. aktivní zařízení, které zajišťuje komunikaci a propojení mezi jednotlivými sítěmi či částmi vnitřní sítě podniku. Nejjednodušší definicí brány je kontrolované spojení mezi jednou částí prostředí a druhou. Typická společnost má více propojení mezi internetem a obvodem svého podniku a můžete je označit jako bránu.

Servery jsou sdílené počítače, které poskytují funkce pro více uživatelů, například ukládání souborů nebo spuštění sdílené aplikace, včetně plánování podnikových zdrojů (ERP) nebo řízení vztahů se zákazníky (CRM). Jednoduše řečeno, servery poskytují služby a to jak výpočetní, tak databázové. Klientské systémy jsou sestaveny z jednotlivých počítačů, které každý uživatel používá, včetně počítačů, notebooků, stolních počítačů a mobilních zařízení.

Zóny

Čtyři hlavní zóny, které existují v základní architektuře organizace (podniku), jsou externí (Internet), extranet, intranet a kritická oblast pro citlivá aktiva. Oddělení výpočetního prostředí do těchto čtyř zón pomáhá izolovat omezené a kritické oblasti (kritická oblast je místem, kde se nacházejí nejkritičtější systémy) a zajistit jim vyšší úroveň zabezpečení.

Digitální brána kolem daného podniku je součástí bezpečnostního perimetru. Servery brány jsou umístěny na obvodu sítě a oddělují je od Internetu. Brána je vstupním bodem do vnitřního síťového prostřední – Intranetu a vytváří řízený filtr vůči externím třetím stranám.

2.5 Bezpečnostní perimetr informačního systému

Ve firemním IT je nutné chápat bezpečnost komplexně, tak abychom pokryli všechny, i teoretické možnosti přístupu k datům nebo interním prostředkům. Silný bezpečnostní perimetr navržený vůči externím přístupům, se slabě zabezpečeným lokálním nebo VPN přístupem do sítě otevírá útočníkovi jednoduše cestu k proniknutí do informačního systému.

Základní způsoby komunikace nebo přístupu můžeme zjednodušeně rozdělit na:

- komunikace z interní sítě směrem do externího světa;
- vzdálený přístup z Internetu k veřejným prostředkům;

- vzdálený přístup do interní sítě pomocí některé metody VPN;
- lokální přístup do sítě.

Hranici mezi nebezpečným Internetem a podnikovou sítí tvoří bezpečnostní perimetr, který tak tvoří hranici mezi vnějším světem a informačním prostředím podniku. Tento je často v mnoha firmách již dlouhodobě řešen, Dříve vesměs na úrovni fyzické ochrany, ale v současné době stále více získává na důležitosti zabezpečení na úrovni systémové, či logické. V této oblasti existuje široká škála prostředků.

Zpravidla vždy je použit firewall, který zamezuje přímému přístupu k vnitřním síťovým segmentům. Takto pojaté zabezpečení perimetru není dostatečné, a je nutné je doplnit technologickými prostředky demilitarizované zóny.

Další stupeň zabezpečení je tvořen systémy IPS/IDS, které chrání nebo minimálně varují před útoky z Internetu mířené na servery.

Nové a specifické bezpečnostní požadavky vznikají s tím, že se stále častěji objevují osobní mobilní zařízení ve firemním prostředí – tzv. BYOD (Bring Your Own Device). Se stávající bezpečnostní politikou, cílenou na stabilní firemní komponenty informačního systému již nelze vystačit.

Zde je nutné takto koncipovanou bezpečnostní politiku aktualizovat a připravit prostředí IT na požadavek přístupu k datům z těchto zařízení. Z pohledu řízení bezpečnosti se jedná o velmi obtížný úkol, který skýtá velké množství rozmanitých hrozeb.

Zde již nelze stanovit striktně, že tato zařízení není možné v podnikovém informačním systému provozovat. Je třeba nastavit procesy řízení přístupu do informačního prostředí strukturované s využitím doménové architektury, tak aby např. synchronizaci s aplikacemi, které jsou navrženy pro mobilní platformy bylo možné řídit i z bezpečnostního hlediska, a to odděleně od vnitřní doménové struktury. Tyto nové technologie však významně zasahují do nastaveného podnikového bezpečnostního perimetru.

V oblasti zabezpečení informací v současné době před námi stojí velké a různorodé úkoly. Cílem této kapitoly je uvést studenty do problematiky budování systému řízení bezpečnosti informací v nových technologických podmínkách, vymezit základní pojmy u bezpečnostních komponent a ukázat přístupy při zajišťování vrstvené bezpečnosti informací s tím, že je důležité vycházet z provázanosti lidí, technologie a procesů.

1. Vysvětlete pojmy: systém, informační systém vrstvená bezpečnost, perimetr?
2. Jaký je rozdíl mezi informačním systémem a informační technologií?
3. Jakou úlohu v bezpečnosti informací mají lidé, procesy, technologie?
4. Co znamená pojem brána, server, kritický systém?

Literatura k tématu:

[1] Řepa,V.: *Analýza a návrh informačních systémů*. Praha: Ekopress, 1999. 404s. ISBN 80-861-1913-0.

[2] Smejkal, V., Rais*, K. Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9

Kapitola 3

Bezpečnost v informačních systémech

Po prostudování kapitoly budete umět:

- stanovit funkčnosti jednotlivých bezpečnostních nástrojů;
- popsat základní metody a přístupy při zajišťování bezpečnosti

Klíčová slova:

Firewall, autentizace, autorizace, heslo, klíč.

3.1 Specifika zajišťování bezpečnosti

Mezi hlavní kategorie bezpečnostních technologií patří firewally, antivirové systémy, detekce narušení, správa zranitelností a správa obsahu stále více soustředěné do SIEM (Security Information and Event Management), tj. managementu bezpečnostních informací a událostí. Protože hrozby, jako jsou např. viry, trojské koně, malware, ransomware apod. mohou využít zranitelností IS v bránách, serverech nebo klientských sítích, musí být všechna tato řešení implementována v každé ze tří vrstev sítě.

Pokud není poskytnuta ochrana ve všech třech vrstvách systému, tj. datové (databázové), aplikační a prezentační, vzniká v informačním prostředí díra, kterou mohou hackeři, škodlivý SW, ale aktivní či pasivní činnost uživatelů, kompromitovat. To platí zejména pro prezentační vrstvu, na které jsou využívány osobní počítače, zde je nutné zajistit v v prezentační vrstvě byla důsledně řešena oprávněnost přístupu, kontinuální ochrana zpracovávaných dat a zálohování.

Nyní budeme podrobněji zkoumat různé bezpečnostní technologie a budou uvedeny základní postupy a přístupy ochrany podnikového informačního systému.

3.2 Zajištění a správa bezpečnostních nástrojů

Informační technologie zahrnují tři hlavní nástroje pro kontrolu přístupu k počítačovým i komunikačním systémům a pro omezení uživatelů při přístupu pouze k funkcím a činnostem odpovídajícím jejich potřebám v rámci nastavené úrovni autorizace, autorizace a správy účtů.

3.2.1 Autentizace

Autentizace je proces, který určuje, kdo jste, jaké máte oprávnění k přístupu k aplikacím, do informačního systému aj. Pro kontrolu a audit autentizačních procesů jsou v informačních systémech implementovány systémy řízení oprávněného přístupu (např. Active Directory v prostředí MS Windows).

Pokročilejší autentifikační technologie poskytují další bezpečnost během autentizačního procesu. Tyto technologie zahrnují použití fyzických zařízení nebo žetonů, jako jsou čipové karty, které uchovávají další informace k identifikaci daného uživatele. Také biometrické systémy mohou využívat jedinečné biologické vlastnosti, včetně otisků prstů nebo snímků sítnice, a ve stále větší míře používaného dynamického biometrického podpisu (DBP), aby byla dosažena vyšší úroveň autentizace, tzv. vícevrstvá autentizace.

Odborníci v oblasti bezpečnosti odkazují na nezbytnost minimálního použití dvou forem ověřování, tj. dvoufaktorové autentizace. Dvoufaktorová autentizace je doporučena pro řízení přístupu již ke standardním informačním systémům nebo pro vzdálený přístup k těmto systémům, neboť tímto způsobem je eliminována zranitelnost informačních systémů v případech využívání autentizace typu „jméno, heslo“.

Tradiční faktory ověřování můžeme rozdělit následovně:

- něco, co znáte, například heslo;
- něco, co máte, například symbol;
- něco, co jste, například biometrické charakteristiky;
- kde jste, například pomocí globálních satelitů pro určování polohy.

Klientská softwarová řešení mohou též využívat dalších nástrojů, jako jsou „tokeny" nebo "certifikáty", které jednoznačně identifikují jak vlastníka příslušné pracovní stanice (např. osobního počítače), tak i samotné fyzické zařízení. Toto SW řešení umožňuje řešit úskalí vzdáleného přístupu, kdy je ověřeno, že daný oprávněný uživatel přistupuje do systému z fyzického zařízení, které je deklarováno a je tak možné kontrolovat oprávnění k vzdálenému přístupu k systému i v rozsáhlých sítích. V každém případě by organizace a podniky by měly využívat dvoufaktorovou autentizaci pro přístup do systému, protože jednoduché uživatelské ID a hesla neposkytují dostatečnou záruku, že nedošlo k přístupu neoprávněných osob, zejména při nedostatečné správě hesel.

Problematika hesel, správa klíčů

Uživatelům musí být zaručeno, že mají jedinečné uživatelské ID a hesla pro přístup k počítačům, e-mailovým účtům a jiným informačním systémům. Identifikátory uživatelů a hesla jsou nejzákladnější formou ověřování (jak bylo uvedeno i nejzranitelnější) a jsou ekvivalentní „elektronickým klíčům“ k systémům a aplikacím. Tyto klíče musí být pečlivě kontrolovány, musí být zajištěna jejich správa (kontrola kvalitních hesel, jejich periodická obměna apod.), a uživatelé musí být poučeni, že při jejich zneužití platí presumpce viny – tj. daný uživatel je za zneužití daného „klíče“ zodpovědný.

Uživatelé musí dodržovat následující nejdůležitější povinnosti při práci s hesly:

1. Hesla nesmí být jakýmkoliv způsobem sdělena jiné osobě.
2. Hesla nesmí být nikde poznamenána a musí se udržovat v tajnosti.
3. Nesmí být, jakkoliv umožněno jiné osobě seznámit se s heslem.
4. Jako hesla nesmí být použita jména blízkých osob, zvířat a další slova, která mohou být odhadnuta ze znalosti držitele hesla, nebo neobsahovalo po sobě jdoucí stejné.
5. Heslo musí být dostatečně silné, tak aby se nedalo jednoduše strojově nebo ručně prolomit (kombinace velkých a malých písmen a číslic, délka alespoň 10 znaků) a mělo by být pravidelně měněno v závislosti rizicích spojených s prolomením.
6. Hesla nesmí být zaznamenána na papíře nebo v obdobné podobě (výjimku tvoří bezpečné uložení administrátorských hesel pro případ havárií).

Hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla. Plnění těchto požadavků nelze nechat na samotných uživatelích, je nutno implementovat do informačních systémů řešení, které řádnou správu hesel vynucovat.

3.2.2 Autorizace

Funkce autorizace umožňuje správcům systému omezit některé speciální oprávnění na určité role nebo funkce, které zaměstnanci vykonávají v rámci organizace. S využitím autorizace je tak řešeno strukturování oprávnění jednotlivých uživatelů informačního systému. Například všichni uživatelé v dané společnosti mohou mít e-mailový účet pro všeobecné použití, ale pouze omezený počet zaměstnanců by měl privilegovaný přístup k definovaným aplikacím. V tomto případě systém umožňuje administrátorovi systému, aby zajistil kontrolu určitých omezených funkcí.

Jiným příkladem jsou systémy s jednotlivými aplikacemi, ve kterých jsou odděleny typy povinností a pravomocí dle dané role jednotlivých uživatelů. Např. personál, který má přístup k citlivým informacím, (například mzda).

Správa autorizačních oprávnění musí zjistit, kdo přistupuje k vymezeným systémům a jaké činnosti zde provádí. Musí být navržen systém pravidelného provádění vnitřních auditů, pro kontrolu, že nikdo nepřistupuje k systémům bez řádné autorizace nebo se záměrem nevhodného použití.

Například všichni zaměstnanci v dané finanční oblasti mohou být oprávněni k přístupu do systému plánování podnikových zdrojů (ERP) společnosti. Pokud ovšem auditor zjistí, že zaměstnanci používají systém v době mimo provozní dobu bez přítomnosti supervizorů, může být nezbytné provést další šetření, aby se zajistilo, že tyto činnosti jsou vhodné.

Správa účtů

Správa uživatelských účtů ve více systémech je obtížná úloha a software pro jednotné přihlášení je součástí řešení tohoto problému (Single Sign on – SSO). Tato řešení poskytují jediné ID uživatele a heslo pro přístup k více systémům, které mohou existovat v dané společnosti. SW pro přihlášení s jediným přístupem však přináší významné bezpečnostní zranitelnosti v případech, kdy jsou v podniku provozovány systémy s odlišnou architekturou. V těchto případech může SSO, které vytváří bezpečnější prostředí ve vztahu k uživatelům, způsobit rizika při implementaci do širokého spektra podnikových aplikací.

Správa účtů, jako třetí z nástrojů při řešení přístupu, slouží jak k auditu, a tak i kontrole využití zdrojů. Z pohledu auditu je důležité mít dobré znalosti o tom, kdo přistupuje k různým zdrojům v rámci podniku a mít přehled o činnosti uživatelů. Tento přístup spadá do „dobré praxe“, vyžadované při revizi protokolů kritických systémů (nejenom), aby bylo zajištěno, že k nim mají přístup pouze oprávnění uživatelé.

Správa účtů je těsně spojena s autorizací, kdy základem je pravidelná kontrola uživatelů, kteří mají přístup do vyhrazených oblastí, jako je datové centrum podniku apod. Navíc je nutnou podmínkou při vytváření prostředí, kde lze zajistit dohledání o činnostech s příslušnými informacemi (daty, elektronickými dokumenty) v celém jejich životním cyklu.

3.2.3 Šifrování

Šifrování je proces převodu dat do formátu, který neoprávněná osoba (ale i oprávněná osoba bez znalosti použitého klíče) nemůže snadno přečíst.

Existují dvě hlavní formy moderního šifrování: symetrické a asymetrické.

Při symetrickém šifrování používají obě strany stejný tajný klíč pro šifrování a dešifrování zpráv. Jedná se o bezpečnější a rychlejší způsob šifrovaní dat. Velkou nevýhodou tohoto způsobu je obtížná distribuce tajných klíčů, zejména v rozsáhlých systémech či sítích.

Asymetrické šifrování nevýhodu distribuce tajných klíčů v rozsáhlých systémech či sítích efektivně odstraňuje. V daném případě každá strana má veřejný klíč pro šifrování a privátní klíč pro dešifrování dat. Při asymetrickém šifrování odesílatel zprávy použije veřejný klíč příjemce s cílem zašifrovat zprávu pro něj. Příjemce této zprávy použije svůj privátní klíč k dešifrování této zprávy. Veřejný klíč nelze požít dešifrování zprávy ani k tomu, aby z něj rekonstruoval privátní klíč příslušného příjemce. I u asymetrického šifrování vyvstávají problémy s „klíčovým hospodářstvím“.

Je třeba zajistit, že:

- příslušný veřejný klíč patří deklarovanému uživateli;
- privátní klíč je bezpečně uložen, tak aby nedošlo k jeho zneužití.

V případě, že není ověřena jednoznačná vazba mezi uživatelem a jeho veřejným klíčem může dojít k narušení důvěrnosti dat, nebo nelze spoléhat na autenticitu dat. Proto účastníci komunikace nedistribuují veřejné klíče sami, ale využívá, tzv. certifikátů vydávaných nezávislými třetími stranami – certifikačními autoritami. Účastnící komunikace tak při přenosu dat využívají certifikátů - tj. potvrzení že daný veřejný klíč patří příslušnému subjektu.

S touto problematikou souvisí PKI (Public Key Infrastructure) tj. infrastruktura veřejných klíčů, kterou vytváří technické prostředky, organizační opatření a administrátoři, s cílem zajistit správu certifikátů veřejných klíčů. Využitím systému PKI lze pak zajistit důvěryhodnost elektronických identit.

Základem PKI je certifikační autorita vydávající certifikáty a seznam zneplatněných certifikátů (CRL Certificate Revocation List), které odpovídají standardu X.509. Certifikační autorita, jako vydavatel certifikátu je odpovědná za to, že certifikát k asymetrickým klíčům je vydán autentizovanému držiteli těchto klíčů, a tak je garantována platnost jednotlivých uživatelů.

První systémy PKI využívaly služeb jedné tzv. kořenové certifikační autority, která vytvářela proprietární certifikáty. V současné době musí být vydávané dokumenty v souladu s normami, což v praxi znamená, že možné vytvářet různé modely PKI od podnikových až po PKI postavené kolem certifikovaných certifikačních autorit.

K ochraně přenášených e-mailových zpráv se využívá protokol S/MIME, který využívá jak asymetrické, tak symetrické šifrování) a protokol Secure Sockets Layer (SSL), který je součástí protokolu HTTPS.

V kapitole jsou uvedeny hlavní aspekty při zajišťování bezpečnosti v informačních systémech. Jsou zde rozebrány základní typy bezpečnostních nástrojů. Samostatná část je věnována problematice šifrování.

1. Jaké bezpečnostní nástroje a metody se využívají při zajištění přístup do informačního systému?
2. Jaký je rozdíl mezi autentizací, dvoufaktorovou autentizací a autorizací?
3. Co je důležité dodržovat při správě hesel a klíčů?
4. Jaké jsou metody šifrování?

Literatura k tématu:

[1] CLARK, David, Leon. *Enterprise Security: The Manager's Defense Guide,* Addison-Wesley Professional, 2003, ISBN 780201719727, Počet stran: 264.

Kapitola 4

Bezpečnost v síti Internet

Po prostudování kapitoly budete umět:

- orientovat se v pojmu bezpečnostní protokol;
- realizovat bezpečnou e-mailovou komunikaci;
- vysvětlit specifika bezdrátové komunikace
- popsat přístup k realizaci VPN

Klíčová slova:

Bezpečnostní protokoly, VPN, Wifi, e-mail.

4.1 Bezpečnostní protokoly

Internet obsahuje obrovské množství informací, z nichž většina je užitečná a vhodná pro všechny uživatele. Na druhou stranu se internet ukázal být účinným prostředkem pro šíření nevhodného obsahu (např. pornografie) i rozmanitých typů škodlivého SW – od jednoduchých virů až sofistikované „trojské koně“, nebo vyděračských programů typu ransomware. Nástroje filtrování obsahu mohou tyto informace filtrovat a zajistit, aby uživatelé k nim nemohli jednoduše přistupovat.

Dvě hlavní kategorie nástrojů zahrnují filtrování webových (internetových) a e-mailových adres. Filtrování Internetu lze použít k zablokování zobrazení určitých webových stránek, které obsahují nevhodný obsah. Filtry na Internetu se odkazují na databáze známých webových adres nebo adres URL s nevhodným obsahem. Webové filtry musí pravidelně aktualizovat databázové adresy URL, protože firmy, které spravují nevhodné weby, při eliminaci blokování svých webových adres, často mění adresy URL nebo název webu. Webové filtry také používají klíčová slova, která jsou považována za nevhodná, a blokují přístup k těmto stránkám a zprávám.

Spam je dnes obrovský problém a může v případě standardního podniku vytvářet až polovinu e-mailových přenosů. Filtrování e-mailů je podobné filtrování webových stránek a může zablokovat nevhodné a nevyžádané komerční e-maily.

Bohužel tyto nástroje jsou dnes reaktivní a spoléhají se na databáze známých webových stránek nebo e-mailových adres k filtrování obsahu. K dispozici jsou i sofistikovanější nástroje, které se také spoléhají na heuristiku, aby identifikovaly tyto zprávy a odstranily je. Stejně jako u jiných heuristických metod, které však ještě nejsou dost spolehlivé.

Před implementací nástrojů filtrování obsahu je třeba zvážit jak právní aspekty, tak i požadavky uživatelů. Kategorie, jako je pornografie, nenávist a hazard, jsou snadno filtrovány, ale jiné kategorie, jako je nakupování online, mohou vyžadovat mnohem větší analýzu nastaveného filtrování. Pokud se program filtrování stává příliš náročným, mohou např. uživatelé – zaměstnanci podniku pociťovat výrazné omezení, které zasahuje i do jejich pracovního procesu (vyhledávání obchodních příležitostí aj,).

Filtrování obsahu je důležitou složkou informační bezpečnosti kvůli značným dopadům produktivity spamu a používání (a zneužívání) webových stránek zaměstnanců při práci. Při vytváření strategie filtrování obsahu je nutné pečlivé zvážení právních a personálních otázek.

4.2 Bezpečná e-mailová komunikace

Autentizační systémy používají pro autentizaci protokoly pro vyhodnocování přenášených zpráv s určením, zda jsou oprávněné, nebo na druhé straně škodlivé či určené k neoprávněnému průniku do podnikového informačního systému. Protokoly vycházejí ze stanovených pravidel, kde je definováno, zda je zpráva v souladu se stanovenými parametry a může být považována za autentickou.

Mezi tři základní protokoly, které se využívají pro autentizaci, patří protokoly Kerberos, RÁDIUS a 802.1x:

- Bezpečnostní systém Kerberos-A vyvinutý na MIT, který autentizuje pouze uživatele. Neuděluje povolení službám nebo databázím; zjišťuje identitu při přihlašování k použití během celé relace. Tento systém je využíván v prostředí jako jsou Novell NetWare a Microsoft Windows
- RÁDIUS (vzdálená autentizační volba uživatelské služby) - autentifikační protokol, který používá ověřovací metodu autentizaci vzdálených uživatelů. Využívá se pro zaměstnance, kteří vyžadují vzdálený přístup a je nutné identifikovat pracovní stanice, který používají, nestačí pouze uživatelské jméno a heslo, protože tento typ autentizace může být snadno zneužit a možnost neoprávněného přístupu je významná.
- Bezpečnostní protokol 802.1x-IEEE pro drátové sítě a bezdrátové místní sítě, které dodržují standard 802.11. Spoléhá na protokol Extensible Authentication Protocol (EAP) pro předávání zpráv některému z různých ověřovacích serverů, jako je například RÁDIUS nebo Kerberos.

4.3 Bezdrátové sítě

Bezdrátové sítě představují nové úkoly v zabezpečení informací. Bezdrátová technologie umožnila uživatelům se připojit přímo k jejich sítím místo toho, bez nutnosti využití síťových kabelů; tento trend bude v budoucnosti nadále růst. Vzhledem k tomu, že tato technologie byla nejprve vyvinuta pro jednotlivé uživatele pro osobní použití, a ne pro případy podnikových komunikací, byly vyšší priority kladeny na snadnost použití místo zabezpečení komunikovaných dat. Bezdrátová zařízení tedy nebyla navržena s cílem používat při přenosu dat šifrování, a dodatečně navrhované komunikační technologie často vykazovaly slabiny.

Ověřování nebo možnost určit, kdo se pokouší o přístup k systémům, je také omezeno bezdrátovou technologií a nemá měřítko na úrovni vstupů. Je také snadné, aby někdo připojil neoprávněné bezdrátové zařízení do firemní sítě, čímž dochází k možnosti neoprávněného přístupu do podnikového informačního prostředí, které může neoprávněný uživatel využít k získání přístupu k podnikovým zdrojům. Bezdrátový přístup (Wifi) a používání mobilních zařízení (smartphone), jakož i BYOD představují pro program zabezpečení informací nové úkoly.

4.4 Virtuální priváte sítě (VPN)

Nástroje VPN umožňují vytvořit bezpečné připojení mezi dvěma lokalitami pomocí veřejné sítě, jako je například Internet. VPN používá šifrování pro ochranu dat, a vytváří tak zabezpečený „tunel“ pro přenášená data, čím je chrání před neoprávněným přístupem nepovolaných osob. Připojení s využitím VPN vytváří zabezpečený spoj, který umožňuje propojit autorizované osoby, které chtějí vzdáleně přistupovat k podnikovému informačnímu prostředí, jako je například systém firemního e-mailu, nebo podnikovým serverům.

Pro vytvoření tohoto spojení VPN se používá kombinace hardwaru a softwaru. Jedná se nákladově efektivní způsob zabezpečeného rozšíření podnikového informačního systému ve srovnání s klasickou metodou využívající pronajaté linky.

Kapitola je orientovaná na realizaci bezpečnosti v nezabezpečeném komunikačním prostředí – Internetu. Jsou zde probrány základní charakteristiky bezpečné e-mailové komunikace. Jsou vysvětleny pojmy jako je VPN, Wifi.

1. Jaké jsou typy bezpečnostních protokolů, jaké jsou jejich charakteristiky?
2. Co znamená filtrování webových stránek?
3. Jak je řešena bezpečnost při komunikaci v prostředí Internetu?
4. Lze realizovat bezpečnost v prostředí Wifi?

Literatura k tématu:

[1] ŠENOVSKÝ, P. *Bezpečnostní informatika 1* [online]. 8. vydání. Ostrava: VŠB-TU Ostrava, 2017, 127 str. Dostupné z < http://homel.vsb.cz/~sen76/CMS/data/uploads/skripta/bi1_8ed_fin.pdf >.

Kapitola 5

Bezpečnost koncových zařízení

Po prostudování kapitoly budete znát:

- základní principy při stanovení bezpečnostní politiky;
- nezbytné bezpečnostní požadavky, které je nutné při řešení bezpečnosti v koncových zařízeních dodržet;
- pojmy firewall, antivirový SW, IPS, IDS;
- způsoby správy zranitelností informačního systému;
- specifika při zajištění bezpečnosti mobilních zařízení.

Klíčová slova:

Antivirová ochrana, IPS, IDS, správa zranitelnosti, SCADA.

5.1 Bezpečnostní koncepce, bezpečnostní politiky, bezpečnostní opatření

Informační technologie přináší do programu informační bezpečnosti řadu aktuálních otázek. Kromě toho rychlý rozvoj informačních technologií má zásadní vliv na efektivnost realizovaného bezpečnostního programu. Většina nastolených otázek vychází z důležitého faktu – že samotná technologie tyto požadavky a problémy nevyřeší, navíc stávající bezpečnostní opatření mohou být u nových informačních technologií neúčinná. Na druhé straně při přecenění možností technologií (deklarovaných v bezpečnostních parametrech daného produktu) se snadno přijme nesprávné rozhodnutí, které často přivede podnik do situace, kdy musí hledat opatření proti zbytečně vzniklým rizikům.

Ze systémového pohledu plyne nutnost řešit na úrovni technologií zejména následné požadavky:

- autentizace, autorizace, správa uživatelských účtů;
- firewall; VPN;
- antivirová ochrana;
- správa rizik;
- správa detekce narušení systému;
- filtrování obsahu dat;
- šifrování.

5.1.1 Firewally

Firewally tvoří "elektronický" obvod kolem podnikového počítačového prostředí. Brány firewall mají filtry, které umožňují přivádět pouze určité typy síťové komunikace do sítě podniku a zabránit přístupu jakýchkoli dalších dat, které nesplňují kritéria bezpečnosti, autenticity apod. Tímto způsobem vytvářejí firewally základní bezpečnostní propust na přístupu do podnikového informačního systému.

Při návrhu nasazení firewallů do podnikového prostředí je třeba uvažovat s kompromisem mezi rychlostí a úrovní zabezpečení. Firewally lze kategorizovat takto:

- filtrování paketů firewally;
- stavové firewally;
- ochranné metody na aplikační vrstvě nebo proxy serveru.

Metody ochrany v firewallech využívající filtrování paketů ověřují záhlaví, resp. informaci o adrese, paketu nebo zprávy pro identifikaci potenciálních problémů, na základě nastavených pravidel je buď příchozí paket blokován nebo propuštěn.

Stavové firewally sledují stav transakce, aby ověřily, že cíl příchozího paketu odpovídá zdroji a předchozímu odchozímu požadavku. Firewall kontroluje souvislost příchozích paketů proti předchozím odchozím paketům, aby byla určena jejich legitimitu. Firewall využívá korelaci s tabulkou stavových připojení a oproti paketovému firewallu zkoumá kontext datových paketů, tj. zdrojové a cílové adresy zprávy, spíše než jejich filtrování.

Nejbezpečnější firewall, jsou firewally na aplikační vrstvě nebo firewally na proxy serveru. Firewall analyzuje obsah příchozích paketů podle výsledků analýzy rozhoduje, zda budou do sítě propuštěny pouze platné zprávy. Jedná se o nejbezpečnější způsob filtrování, neboť je obtížné napsat do datové části paketů nevhodný obsah. Nevýhodou je, že tento proces snižuje významně propustnost. Existuje několik variant těchto řešení firewallu, kdy před aplikační firewall je předřazen paketový firewall, aby byla zátěž aplikačního firewallu, který zpracovává jen filtrované pakety. Představitelem aplikačních firewallů je proxy firewall, zde všechna data prochází vždy přes proxy server, který je podle nastavených podmínek filtruje. U tohoto typu aplikačního firewallu je výhodou, že jsou skryty zdrojové adresy uživatele, neboť je za něj je uvedena aplikační brána.

5.1.2 Antivirový software

Stejně jako u lidí i v elektronickém prostředí je nezbytné se chránit proti virům. Antivirový software pomáhá zabránit infikování počítačů škodlivým SW (počítačovými viry, červy, trojskými koni apod.). Souhrnně lze vymezit jako ochranu proti malware. Vzhledem k tomu, že každý den přibývají stovky nových typů škodlivého SW, je nezbytné a povinné aktualizovat antivirový software pravidelně s novými definicemi virů.

Navíc útoky jsou v průběhu let mnohem propracovanější a v dnešní době je mnohem snazší, aby malware infikoval vaše počítače, než tomu bylo v minulosti, neboť nový škodlivý SW, využívá současně několik různých zranitelností systému a vytváří nové formy pro své rozšiřování. Tyto hrozby vedly bezpečnostní průmysl k vývoji nástrojů, které pravidelně automaticky vybírají definice virů, často jednou za den, aby rychle a efektivně zabránily nákazám. V případě, že škodlivý kód infikuje počítač, dodavatelé zabezpečení nabízejí nástroje, které odstraňují infekce z počítače a pokoušejí se vyčistit jakékoli poškození způsobené virem.

Antivirový software je požadovanou součástí programu zabezpečení informací kvůli rostoucímu počtu virů. Pouze s implementovaným antivirovým software (doporučuje se od několika výrobců) lze přistoupit k bezpečnému využívání Internetu. Antiwirový software musí poskytovat komplexní

ochranu proti všem typům hrozeb v prostředí sítě Internet. Proto výrobci bezpečnostního softwaru dodávají „balíky“ antivirového programu, pokrývajícího známé spektrum škodlivého SW.

5.1.3 Vulnerability management – správa zranitelnosti

Řízení chyb zabezpečení je způsob, jak aktivně odstranit nedostatky z programu zabezpečení informací. Efektivní bezpečnostní program využívá nástroje pro automatickou správu chyb zranitelnosti pro identifikaci možných zranitelností v podnikovém informačním systému. Nástroje pro správu zranitelnosti porovnávají prostředí s databází známých zranitelností a kontrolují, jaká zranitelná místa obsahuje podnikové informační prostředí.

Existují dva typy nástrojů správy zranitelnosti: síťové a hostitelské. Pomocí nástrojů založených na síti můžete naskenovat síťovou komunikaci, abyste zjistili známá zranitelná místa a nástroje hostitele pro skenování fyzických zařízení, například počítačových serverů.

Vzhledem k narůstajícímu počtu zranitelných míst je třeba zajistit aktuální záplatování (patching) informačních programů. Jedná se o složitý úkol, neboť záplaty musí být před jejich aplikací testovány, což v případě velkých podniků, s rozsáhlým informačním prostředím (velký počet aplikací, serverů a uživatelů) vyžaduje systematický přístup, který musí být zakomponován do business procesů podniku.

Pravidelný a řízený program skenování zranitelných míst informačního prostředí a systém řešení potřebných oprav musí být součástí zajištění odpovídající úrovně bezpečnosti daného podniku. Z tohoto důvodu se do informačního prostředí začleňuje SIEM. Technologie správy chyb je tedy důležitou součástí systému řízení bezpečnosti informací. Tyto nástroje vám umožňují proaktivně identifikovat zranitelná místa a provést potřebná proaktivní bezpečnostní opatření.

5.1.4 IDS – Detekce narušení

Systémy detekce narušení (IDS) monitorují provoz a události v síti a v podnikových informačních systémech kde zjišťují příznaky možného útoku, či informace o útocích, které byly provedeny. Stejně jako v případě řízení zranitelnosti, nástroje pro detekci narušení lze zajistit ve dvou režimech, tj. v síťovém nebo hostitelském prostředí,

Nástroje založené na síti aktivně vyhledávají provoz na klíčových částech vaší sítě a hledají možné útoky.

Nástroje hostitele pracují na serverech a kontrolují informace o auditu nebo záznamu, aby detekovaly možné útoky. Protože vyhodnocování datového protokolu může být náročné na zdroje, mohou tyto nástroje negativně ovlivnit výkon serverů. V daném případě nutné průběžně sledovat „propustnost“ informačního systému, ale při jejím snížení nelze řešit danou situaci vypnutím nástrojů detekujících narušení.

Tyto nástroje se opírají o dvě metody identifikace narušení: rozpoznávání založené na popisu a detekci anomálií.

Rozpoznání založené na popisu porovnává určité vzorce činností s neznámými scénáři útoku.

Nástroje detekce narušení založené na popisu rozpoznávají vzorky nebo příznaky nestandardní činnosti. Zde detekce nestandardní situace závisí na určení vzorků pro normální chování a poté na zjištění chování, které se liší od normy.

Obě tyto metody musí reagovat na vysoký stupni variability kontrolovaného prostředí a určit co jsou standardní situace a čím může útočník disponovat.

5.1.5 IPS – prevence narušení

Typické podnikové sítě bývají připojeny k několika vnějším sítím. Vzdálené pobočky lze k centrální síti připojit pomocí různých technologií (pevné linky, DSL, různé typy VPN…), čímž vznikne rozlehlá síť. Vzhledem k různorodosti možných útoků není možné řešit bezpečnostní perimetr podniku pouze s využitím firewallů, ale je nezbytné navrhnout bezpečnostní zóny, které bezpečnostní nástroje strukturují s oddělením na jednotlivé oblasti – Internet, DMZ (demilitarizovaná zóna, Intranet aj.). Musí být nastavena pravidla pro přenos dat, přičemž základní pravidla jsou nastavena na firewallu. Na přenos a kontrolu kritických dat jsou určeny systémy detekce a prevence narušení (IDS/IPS systémy.

IPS systémy, stejně jako IDS systémy se dělí na síťové a hostitelské. Pro obě kategorie je společné sledování systému, schopnost upozornit administrátora na případný útok a provést bezpečnostní záznam (logu).

Hostitelské systémy se nasazují přímo na jednotlivé stanice nebo servery. Jedná se o softwarové produkty a jsou tudíž omezeny podporou pro OS na dané stanici. Monitorují systémová volání, logy a podobně. Chrání před útoky na OS a aplikace. Síťové systémy jsou specializovaná zařízení pro monitorování dění na síti.

Systém prevence narušení (IPS) je schopný útoky zároveň detekovat a reagovat na ně (tj. zabránit útoku nebo ho přerušit). Jsou zde nastaveny 2 druhy monitoringu“:

- útok na aplikace škodlivým SW;
- útok z Internetu – DoS, DDoS útoky.

Porovnání IPS a IDS

IPS, díky možnosti připravovat reakci na útoky, umožňují spolehlivější způsob ochrany. Tato reakce však může mít i negativní dopad. Jedná se o tzv. plané poplachy. V souvislosti s tím může odpojit oprávněného uživatele nebo zcela zablokovat síťový provoz na daném síťovém segmentu.

Některé IDS systémy dokáží, za spolupráce s firewallem, který dynamicky mění svoji politiku tak, aby zamezil komunikaci vyhodnocenou jako útok, také reagovat na útok.

Systémy detekce a prevence narušení jsou realizovány jako specializovaná zařízení, která jsou spravována z centrálního řídicího systému.

5.2 Vynucování bezpečnostních opatření na aplikační úrovni

Nejčastějšími útoky na aplikační vrstvě jsou útoky na webové služby a elektronickou poštu. Proti útokům na web se lze bránit jeho audit detekcí průniků, řízením přístupu, autentizací, elektronickými podpisy (včetně DBP) a šifrováním. Elektronickou poštu je třeba chránit šifrováním a elektronickými podpisy.

Na aplikační úrovni jsou útoky založeny zejména na přepisování webových stránek, odcizení a falšování pošty, využití phishingu apod. Jsou tak využívány nedostatky v navržených bezpečnostních opatřeních – příliš obecná bezpečnostní politika a s tím spojené nesprávná správa hesel, nedostatečně nastavené bezpečnostní komponenty nebo i nezodpovědní uživatelé.

Na aplikační úrovni se jedná zejména o útoky odmítnutí služby typu DoS (Denial of Service) a DDoS (Distributed Denial of Service). Termín DoS označuje útok, jehož cílem je zabránit oprávněným uživatelům v přístupu ke službám výpočetního systému, anebo alespoň tento přístup zpozdit. Termín DDoS označuje útok na internetovou službu či webovou stránku, jehož cílem je zahltit servery obrovským množstvím požadavků, a způsobit nedostupnost tohoto serveru i pro oprávněné uživatele.

Některé typy těchto útoků:

Ping-of-Death (smrtící ping) - použití paketů delších než 65 535 bajtů povolených IP specifikací, přičemž při jejich přijetí dojde k přetečení vyhrazené paměti.

Teardrop – využití IP fragmentů. V případě, že počítač útočníka generuje fragmenty, jejichž délka neodpovídala údaji v záhlaví, operační systémy neumí nesprávný fragment zpracovat.

Smurf attack – útočník vyšle záplavu pingů, které následně směrovač rozhlásí v cílové síti. Pokud ještě útočník uvede v IP záhlaví pingu adresu cizího odesilatele, zaplaví se odpověďmi ještě další síť.

V současné době jsou vedeny útoky typu Distributed Denial of Service (DDoS), které využívají útoků spuštěních z mnoha navíc cizích zdrojů, což neumožňuje lokalizovat útočníka.

5.3 Bezpečnost mobilních zařízení – zabezpečení a autentizace

Bezpečnostní problémy vzniknou vždy, když k datovým zdrojům získají přístup neoprávněné osoby, nebo když uživatelé překročí úroveň jim definovaného přístupu k daným systémům.

V rámci Informačních technologií lze využít metod pro kontrolu přístupu do informačních a komunikačních systémů k regulování přístupů uživatelů tak, aby se chovali ve shodě s jejich potřebami a ve vymezených oblastech. Důležité je, aby při realizaci bezpečnostního programu byla u této problematiky dána do souladu bezpečnostní opatření s hodnotou chráněných informací.

5.4 BYOD, IoT – kontrola a monitoring

V současné době dochází k významnému problému zabezpečení tzv. koncových bodů. Počítačová infrastruktura podniků bývá často zabezpečená, její slabá místa však představují vypalovací zařízení, tiskárny, média USB, laptopy uživatelů či chytré mobilní telefony. Slabými místy jsou také „chytré“ produkty, kdy důvodem jejich nasazení je automatizace rutinních činností, ať u v domácnostech (ledničky, pračky, topení), ale v podnikové struktuře, řízená vzdáleným přístupem přes Internet, který

sebou přináší nové bezpečnostní hrozby. Jedná se o nový fenomém IoT (Internet věcí) A v neposlední řadě rychle se rozšiřující BYOD, tedy využívání zařízení uživatele v podnikové síti, přičemž v tomto zařízení není instalována podniková „image“.

5.5 Bezpečnost průmyslových systémů (SCADA, PLC)

Údaje získané ze senzorů monitorujících bezpečnostní údaje je třeba zpracovávat nebo připravit k revizi určenému operátorovi. Data ze senzorů je lze zobrazit při sejmutí v jejich formátu, tj. v tabulce jako sled měření s časovou značkou. Údaje v takové formě však jsou odpovědnou osobou obtížně interpretovatelné, proto jsou tyto údaje před jejich zobrazením převedeny do jednodušší formy umožňujícími jejich vizualizaci.

K tomuto účelu jsou využívány tzv. systémy SCADA (Supervisory Control and Data Acquisition). SCADA systémy tvoří další vrstvu v logice průmyslové automatizace. Nejnižší vrstvu tvoří PLC automaty regulující proces v reálném čase. Systém SCADA, jelikož údaje musí, načíst (obvykle po síti), zpracovat a zobrazit, pracuje ve „skoro“ reálném čase. Je důležité si uvědomit, že SCADA systém informace nezískává přímo ze senzorů (prostřednictvím PLC), ale z definovaného místa, zejména z výkonného databázového serveru. Tyto servery jsou označovány jako real-timové databáze. Lze uvažovat i o přímém propojení SCADA – PLC přitom je však nutné uvažovat s tím, že PLC je přizpůsobeno regulaci, ale není schopna poskytovat informace v podobě srovnatelné s relační databází. Výhodou však je, že je jednoduché nastavit, aby PLC použil jako úložiště dat nějaký databázový server (spojení PLC – databáze) a propojit tento server se systémem SCADA (databáze – SCADA).

Kapitola pojednává o základních principech při stanovení bezpečnostní politiky a bezpečnostní strategie. Studenti jsou seznámeni s nezbytnými bezpečnostními požadavky, které je nutné při řešení bezpečnosti v koncových zařízeních dodržet. Jsou probírány bezpečnostní komponenty a metody jako je firewall, antivirový SW, IPS, IDS. Je probírána otázka správy zranitelností informačního systému. A na druhé straně jsou zde uvedeny základní vlastnosti systému SCADA.

1. Co znamená pojem IDS a jaký je rozdíl mezi IDS a IPS?
2. Vysvětlete princip SCADA.
3. Co znamená antivirová ochrana, jak lze charakterizovat škodlivý SW?
4. Co znamená správa zranitelnosti?

Literatura k tématu:

[1] ., SMEJKAL, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9

Kapitola 6

Systém řízení bezpečnosti informací

Po prostudování kapitoly budete umět:

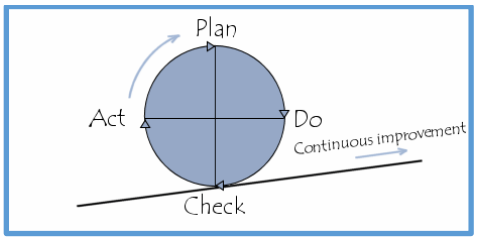
- vysvětlit účel cyklu PDCA;
- rozpoznat, proč je nutné při realizaci bezpečnosti informačního systému postupovat dle požadavků ISMS;
- základy řízení rizik;
- pojmy ITIL, COBIT, Prince 2;
  vysvětlit, proč je nutné při realizaci bezpečnosti informačního systému postupovat dle doporučení ČSN norem řady 27000.

Klíčová slova:

PDCA, ISMS, ČSN normy, řízení rizik, Prince 2

6.1 Procesní řízení bezpečnosti v cyklu PDCA

Principem celého ISMS (Information Security Management System), tedy systému řízení bezpečnosti informací je tzv. PDCA model (Demingův model), který je zobrazen na obrázku č. 6.1.



Obrázek 6.1 Demingův model

Vlastní implementace systému řízení bezpečnosti informací zahrnuje především návrh a implementaci procesů, které vedou k řízení bezpečnosti informací, kontroly způsobu jejich implementace a neustálého udržování a zlepšování (PDCA).

Postupů a metodik, jak implementaci zvládnout existuje několik, v případě informačních systémů lze v souladu PDCA postupovat podle osvědčeného postupu.

Plan – ustavení ISMS:

- Strategie informační bezpečnosti
- Management rizik
- Návrh bezpečnostní politiky, systémových směrnic, plánu řízení kontinuity činností
- Bezpečnostní plán a plán implementace ISMS

Do – zavádění a provozování ISMS:

- Implementace procesů a postupů dle bezpečnostního plánu a plánu implementace ISMS
- Zavedení postupů kontrol
- Školení
- Provoz

Check – monitorování a přezkoumání ISMS:

- Před-certifikační audit
- Penetrační testy
- Testy procesů
- Testy techniky

- Testy metodami sociálního inženýrství
- Další testy dle plánu implementace

Act – udržování a zlepšování

6.2 Normy řady ČSN ISO/IEC 27000

Spolu s rozvojem šifrové ochrany informací hrají stále důležitější roli standardizační činnosti mezinárodních i státních organizací. Přijímané normy a standardy dávají doporučení a stanovují principy a postupy vývoje, testování a ověřování parametrů i podmínky provozu šifrovacích zařízení i celých informačních systémů s integrovanou bezpečnostní nadstavbou. Zároveň jsou nezbytnou součástí při hodnocení bezpečnostních parametrů realizovaných komponent a systémů. Cílem bezpečnostních norem je též unifikace vytvářených produktů i celých systémů. Zvláštní zřetel je nyní dáván na standardizaci procesního řízení v oblasti bezpečnosti.

Normy ČSN ISO/IEC řady 27000 lze považovat za nejvhodnější technický normativní systém v oblasti bezpečnosti informací.

ČSN ISO/IEC 27000 je určena pro obecný úvod do ISMS a pro uvedení předmětů jednotlivých norem této řady. ČSN ISO/IEC 27000 poskytuje slovník, formálně definující většinu pojmů používaných v řadě norem ČSN ISO/IEC 27000, a popisuje rozsah a cíle pro každou normu této řady.

Norma ČSN ISO/IEC 27002:2014. Tato mezinárodní norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v rámci kontextu organizace. Tato mezinárodní norma také zahrnuje požadavky na posuzování a ošetření rizik bezpečnosti informací, přizpůsobené potřebám organizace. Požadavky této mezinárodní normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností.

Norma ČSN ISO/IEC 27002:2014. Tato mezinárodní norma poskytuje směrnice pro organizační normy bezpečnosti informací a postupy pro řízení bezpečnosti informací, včetně výběru, implementace a řízení opatření, s přihlédnutím k prostředí rizik bezpečnosti informací organizace. Je určena pro použití organizacemi, které mají v úmyslu:

a) vybrat opatření v rámci procesu zavádění systému řízení bezpečnosti informací založeném na normě ISO/IEC 27001 - ISMS;
b) zavést obecně uznávaná opatření bezpečnosti informací;

c) vypracovat vlastní směrnice k řízení bezpečnosti informací.

Zatímco tato norma poskytuje návod pro širokou škálu opatření v oblasti bezpečnosti informací, která se běžně uplatňují v mnoha různých organizacích, zbývající normy v řadě norem ČSN ISO/IEC 27000 poskytují doplňující doporučení či požadavky týkající se dalších aspektů celkového procesu řízení bezpečnosti informací.

6.3 Nastavení maturity bezpečnosti informačního systému

Pro řízení bezpečnostních procesů v informačním systému je vhodné postupovat podle metodologie CoBiT 5 (Control Objectives for Information and related Technology) – Řídící cíle pro oblast informačních a s nimi propojených technologií, definující kromě základních bodů řízení i tzv. modely zralosti (maturity models) pro jednotlivé bezpečnostní procesy.

Na základě analyzovaných informací o informačním systému podniku, jakož i rozboru vnitřní bezpečnostní dokumentace podniku lze zařadit daný informační systém, resp. celý podnik do příslušné úrovně bezpečnostní zralosti (tzv. enterprise maturity level of security).

Interní benchmark ilustruje stav informačního systému s hodnotami získanými počáteční analýzou v porovnání s tím, do jaké míry (procentuálně) plní požadavky normy ČSN ISO/IEC 27002:2014 ve srovnání s jejími cílovými hodnotami požadovanými pro příslušnou úroveň bezpečnostní zralosti. Od této úrovně zralosti podniku se odvíjí i výše uvedená, navrhovaná bezpečnostní opatření.

6.4 Řízení rizik

Proces řízení rizik v podniku těsně navazuje na výsledky analýzy rizik. Na základě těchto výsledků musí podnik připravit bezpečnostní projekt. V tomto projektu se řízení rizik zaměřuje na dvě úrovně rizik projektu:

- Koncepční úroveň – kdy jsou řešeny hlavní úkoly a formulují se priority bezpečnostních opatření. Zároveň je třeba skloubit tento projekt v rámci řízení projektů s projekty již realizovanými.

- Projektová úroveň – zvážení hlavních projektových rizik, které mohou být interního i externího charakteru. Musí být vytvořen soupis evidovaných rizik a stanoveny možnosti podniku při realizaci návazných opatření z hlediska finančního, personálního aj. pokrytí. V tomto případě je nezbytné posoudit, zda jsou veškerá identifikovaná rizika přijatelná či nepřijatelná. V případě nepřijatelných rizik musí být projekt upraven tak, aby, byl nastaven proces eliminace těchto rizik

6.5 Audit bezpečnosti

Účelem auditu bezpečnosti informačního systému je posouzení vhodnosti a úplnosti provozovaných bezpečnostních opatření, tj. zda funkční a technická specifikace navržených a provozovaných bezpečnostních řešení poskytuje předpoklady, že řešení tak, jak je navrhováno, splní požadavky formulované v bezpečnostních normách ČSN ISO/IEC řady 27000.

Kromě postupů uvedených v normách ČSN ISO/IEC řady 27000 lze využít v přístupu k auditu bezpečnosti IS řadu celosvětově přijímaných metodik, při kterých lze využít i vypracované SW nástroje. Mezi nejznámější metodiky a nástroje patří metodika ITIL (IT Infrastructure Library), COBIT (Control Objectives for Information and related Technology) i řada průmyslových metodik, které nich vycházejí.

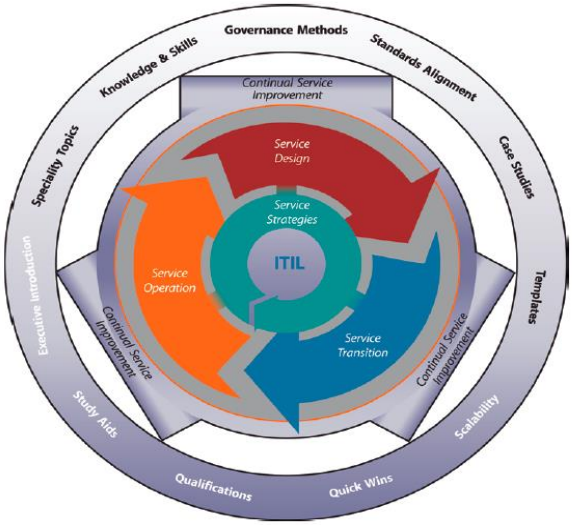
Audit bezpečnosti standardně prochází následujícími fázemi:

- popis základních cílů a zaměření auditu při stanovení hranic auditovaného systému,
- posouzení stávajících bezpečnostních parametrů systému,
- popis evidovaných hrozeb, zranitelností v jednotlivých oblastech informačního systému,
- identifikace a ocenění bezpečnostních rizik a kritických míst v systému,
- návrh bezpečnostních opatření, stanovení prioritních úkolů v postupu navrhovaného řešení příslušných opatření.

V návaznosti na vyhodnocení výsledků auditu je vhodné v rámci organizace aktualizovat stávající systémovou bezpečnostní politiku a provést celkovou revizi systému řízení bezpečnosti zpracovávaných informací, přičemž je důležité přijatá bezpečnostní opatření harmonizovat business strategií podniku.

6.6 ITIL[2]

Informace uvedené v ITIL (Information Technology Infrustructure Library) vycházejí ze zkušeností „best practice“ mnoha společností na celém světě. Jedná se de-facto o mezinárodní standard pro řízení IT služeb (IT Service Management). ITIL byl publikován poprvé v letech 1989 – 1995 u Her Majesty's Stationery Office (HMSO) v UK v rámci Central Communications and Telecommunications Agency (CCTA) – dnešní Office of Government Commerce (OGC) a měl podobu 31 knih. V letech 2000 – 2004 byla původní verze revidována a následně vyšel ITIL verze 2, který čítal již jen 7 knih. V roce 2007 se objevuje ITIL verze 3, sestávající z 5 knih, které kopírují životní cyklus služby:



Obrázek 6.2 Životní cyklus služby

ITIL v jednotlivých knihách popisuje procesy, které se většinou musí v IT vykonávat, aby jej bylo možné provozovat a jaké služby musí poskytovat podnikovým business procesům. ITIL se snaží poskytované služby formulovat z pohledu zákazníka, který služby odebírá. Vychází z procesního řízení a ze zkušeností, že společnosti, které své procesy zavedly podle ITIL, dosahují vyšší efektivity, přičemž poskytované služby splňují parametry uvedené v SLA (Service level agreement), tj. dohodě o úrovni poskytovaných služeb. Další výhoda zavedení procesů podle ITIL spočívá v tom, že společnosti v takovém případě používají stejnou terminologii, která umožňuje formalizaci přijatých opatření.

Myšlenka ITIL vychází ze skutečnosti, pro firmy je výhodné vycházet z „best practices“, tj. z tzv. nejlepší osvědčené praxe, tedy z osvědčených procesů a metod řízení. Většinou však zavádění procesního řízení se střetává s obtížemi vzhledem k tomu, že zavádění ITIL sebou nese i určitou změnu

[2] ITIL® výkladový slovník v češtině, v1.1, 6. ledna 2012 založen na výkladovém slovníku v angličtině v1.0 z 29. července 2011

struktury liniového řízení v daném podniku. To může vést k obavám z větší byrokracie a k vyvolání určitých předsudků. Nejhorší zkušenosti „worst practices“ se zaváděním ITIL jsou shrnuty v dokumentu ABC of ICT[3].

ITIL popisuje vazby mezi jednotlivými procesy a definuje, jaké by měly být vstupy, výstupy, role a metriky. Vzhledem k tomu, že nositeli každého procesu jsou lidé, musí být jasně určeno, kdo za co odpovídá. V ITIL se používá pojem role, ta je přiřazena člověku nebo týmu, který pak v rámci daného procesu vykonává jednu nebo více činností. Je zřejmé, že pokud má daná role vykonávat příslušnou činnost, musí mít nejen požadované schopnosti, ale potřebuje k tomu též nástroje, tj. HW, SW a musí být vybavena i odpovídajícími pravomocemi a nést určitou odpovědnost.

V ITILu je doporučeno pro každý proces vytvořit tzv. RACI tabulku, která bude v záhlaví obsahovat role a v řádcích jednotlivé činnosti, které se musí v rámci procesu vykonat. U každé činnosti by mělo být uvedeno, kdo ji vykonává (Responsible), kdo je odpovědný za výsledek (Accountable), s kým je nutno postup konzultovat (Consult) a koho je třeba informovat (Inform). Pro úplnost je třeba dodat, že ITIL používá ještě pojem funkce a myslí tím organizační jednotku nebo tým, který určitý proces nebo aktivity v rámci daného procesu vykonává. Ač je všech pět knih, které tvoří jádro ITIL poměrně rozsáhlých, není v nich uveden detailní popis procesů, neboť ITIL popisuje jen hlavní aktivity v rámci daných procesů.

6.7 COBIT

Standard pro postupy řízení a pro kontrolu a audit stavu ICT v organizaci.

Je určen top manažerům k posuzování fungování ICT v podniku z pohledu struktury, pravomocí a zodpovědnosti a auditorovi pro provádění auditu systému řízení ICT.

COBIT – soubor nejlepších praktik a postupů, které pomáhají organizaci dosáhnout strategických cílů pomocí efektivního využití dostupných zdrojů a minimalizaci IT rizik. Soubor praktik, pro správné postupy řízení, kontroly a auditu informačních technologií.

[3] Bernam, ABC of ICT - An Introduction to the Attitude, Behavior and Culture of ICT, ISBN-13: 978-9087531409

COBIT vzájemně propojuje:

- řízení podniku (Enterprise governance);
- řízení a správu informatiky (IT governance);.
- Realizace:
- propojení podnikových a IT cílů;
- definováním metrik a modelů zralosti pro měření dosahování cílů a
- definováním odpovědností vlastníků podnikových a IT procesů.

6.8 PRINCE2

V současnosti je nejrozšířenější metodikou řízení projektů v Evropě.

Metodika PRINCE2 definuje veškeré dokumenty, důležitá pravidla a postupy pro řízení projektu se opírá o sedm principů, tvoří ji sedm procesů a popisuje sedm témat.

Principy PRINCE2:

- průběžné zdůvodnění projektu;
- poučení se ze zkušeností;
- definované role a zodpovědnosti;
- řízení pomocí etap;
- dohled nad projektem na základě výjimek;
- důraz na produkty;
- nutnost upravit metodiku podle aktuálního prostředí.

V rámci konkrétního projektu jsou práce rozděleny do dvou základních kroků. V prvním kroku dá projektový manažer dohromady základní podklady pro to, aby mohl projektový výbor posoudit, zda se vůbec pouštět do často nákladného plánování.

Je-li projektový výbor přesvědčen o vhodnosti projektu, dává své schválení, přechází se do druhého kroku, tj. stanovování projektových strategií, plánování projektu, nastavení komunikace, projektových kontrol.

V PRINCE2 existuje jednoznačný proces určující fungování projektového výboru. Pravomoci a zodpovědnosti za vývoj projektu jsou jednoznačně stanoveny a rozděleny mezi projektového manažera a řídící výbor projektu. PRINCE2 dává dokonce plnou zodpovědnost za projekt do rukou sponzora

projektu předsedajícího řídícímu výboru, a nikoliv samotnému projektovému manažerovi. Toto rozdělení vnáší do metodiky jasný řád a zvláště méně zkušeným projektovým manažerům vymezuje pravidla hry.

Nicméně v rámci každého projektu je nutné metodiku PRINCE2 přizpůsobit konkrétnímu účelu, přičemž je nutné dodržovat principy, které jsou páteří celé metodiky.

Po naplánování projektu a vypracování obchodního případu (zdůvodnění projektu či obhájení investice) opět přichází schválení řídícího výboru, který dává pokyn k zahájení následné etapy. Právě striktní rozdělení projektu na etapy dává zodpovědným manažerům možnost včas identifikovat případné problémy a zasáhnout. V projektech PRINCE2 by tedy nemělo docházet k tomu, že vedení projektu pozná až příliš pozdě nevyhnutelné překročení rozpočtu nebo zásadní nedodržení časového harmonogramu.

Kapitola pojednává procesním řízení bezpečnosti dle cyklu PDCA. Je vysvětlen důvod řešení bezpečnosti v rámci procesního řízení. Je ukázáno, proč je nutné při realizaci bezpečnosti informačního systému postupovat dle požadavků ISMS. Studenti se seznámí s
pojmy ITIL, COBIT, Prince2. Velký důraz je kladen ne nutnost při realizaci bezpečnosti informačního systému postupovat dle doporučení ČSN norem řady 27000.

1. Co je to PDCA?
2. Co znamená ISMS?
3. Popište základní charakteristiky metodik CoBIT, ITIL a Prince2.
4. Shrňte základní oblasti řešené v jednotlivých ČS normách řady 27000.

Literatura k tématu:

[1] SMEJKAL, Vladimír. Právo informačních a telekomunikačních systémů. 2., aktualiz. a rozš. vyd. Praha: C.H. Beck, 2004. Právo a hospodářství (C.H. Beck). ISBN 8071797650.

[2] MATES, P. a V. SMEJKAL. E-*government v České republice: právní a technologické aspekty*. 2. vyd. Praha: Leges, 2012. 464 s.ISBN 978-80-875-7636-6.

Kapitola 7

Bezpečnostní analýza (analýza rizik)

Po prostudování kapitoly budete umět:

- základní pravidla a smysl analýzy rizik, tj., bezpečnostní analýzy informačního systému.

Klíčová slova:

Analýza rizik, aktivum, hrozba, zranitelnost, riziko.

7.1 Úvod do problematiky

Důležitým atributem navrhovaných systémů je správa bezpečnosti informací. Pro základní analýzu rizik se vychází z přístupů uvedených v metodice, která je v souladu s normami:

- ČSN ISO/IEC 27001:2014 – Systémy řízení bezpečnosti informací
- ČSN ISO/IEC 27002:2014 – Soubor postupů pro řízení bezpečnosti informací
- ČSN ISO/IEC 27005:2009 – Řízení rizik bezpečnosti informací

Postup, který je ve shodě s bezpečnostními normami ČSN/ISO, je klíčovým zorným úhlem při řešení analýzy rizik.

7.1.1 Definice pojmů[4]

Aktivum

Aktivum je vše, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Základní charakteristikou aktiva je hodnota aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva pro daný subjekt, popřípadě kombinaci obou přístupů. Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení.

Při hodnocení aktiva se berou v úvahu především následující hlediska:

a) pořizovací náklady či jiná hodnota aktiva,
b) důležitost aktiva pro existenci či chování subjektu,
c) náklady na překlenutí případné škody na aktivu,
d) rychlost odstranění případné škody na aktivu,
e) jiná hlediska (mohou být specifická případ od případu).

Hrozba

Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu.

[4] Smejkal, V., Rais, K. Řízení rizik ve firmách a jiných organizacích. 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9

Škoda, kterou způsobí hrozba při jejím působení na určité aktivum, se nazývá dopad hrozby. Základní charakteristikou hrozby je její úroveň. Úroveň hrozby je definována jako pravděpodobnost výskytu hrozby.

Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva odpovídá pravděpodobnosti, že se hrozba vyplní.

Opatření

Opatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Opatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.

Z hlediska analýzy rizik je opatření charakterizováno efektivitou a náklady.

Do nákladů na opatření se započítávají náklady na pořízení, zavedení a provozování opatření. Společně s efektivitou opatření jsou tyto náklady důležitými parametry při výběru opatření.

Riziko

Ve smyslu předchozích definic riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí toho, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní.

Při návrhu opatření se používá pravidlo, které stanovuje, že náklady vynaložené na snížení rizika musí být přiměřené hodnotě chráněných aktiv s cílem dosažení referenční úrovně rizika, pod kterou se riziko prohlásí za zbytkové a nepodnikají se žádná opatření.

7.2 Identifikace aktiv, vytvoření modelu aktiv informačního systému

V rámci této fáze je provedeno rozdělení aktiv do kategorií:

1. datová aktiva – informace, data,
2. fyzická aktiva – počítačové vybavení, komunikační zařízení, úložná media, další technická zařízení (napájecí zdroje, klimatizační zařízení),
3. aplikační programová aktiva – aplikační a systémové programové vybavení, vývojové nástroje a utility,
4. informační aktiva – databáze, datové soubory, systémová dokumentace, uživatelské manuály, školící materiály, archivované informace
5. služby koncovému uživateli – procesy, přístupy k datům,
6. prostory – lokality, budovy, místnosti,
7. lidé – dovednosti, zkušenosti,
8. nehmotná aktiva – pověst, image organizace.

Při zpracování analýzy rizik je výhodné i některá aktiva sdružovat do skupin. U všech aktiv pak je stanovena i jejich hodnota, závislá na hodnocení výše uvedených typů aktiv a vazeb plynoucích z vybraných aktiv. V návaznosti na stanovení hodnoty aktiv bude definována úroveň hrozeb a zranitelností pro všechna aktiva. K tomuto účelu jsou využity výsledky z řízených interview se specialisty Zadavatele. Odpovídající opatření k ošetření jednotlivých rizik vycházejí z hodnot aktiv a úrovní hrozeb a zranitelností, resp. ze zjištěné míry rizika. Dále jsou zohledněny i dostupné informace z této oblasti včetně zkušeností zpracovatelského týmu.

7.3 Stanovení zranitelnosti informačního systému, hodnocení rizik (stanovení míry rizika)

Obecně chápeme riziko jako možnost, že s určitou pravděpodobností dojde k události, jež se liší od předpokládaného stavu či vývoje. Riziko by nicméně nemělo být směšováno, respektive redukováno na pouhou pravděpodobnost, neboť zahrnuje, jak samotnou pravděpodobnost, tak kvantitativní rozsah dané události (dopad). Nejčastěji se riziko uvádí v souvislosti s negativním dopadem (i když

obecně může být odchylka i kladná, ale kladný výsledek nelze většinou považovat za riziko. Proto je nejvíce adekvátní definicí ta, podle níž riziko je situace, v níž existuje možnost nepříznivé odchylky od žádoucího výsledku, ve který doufáme nebo ho očekáváme.

V souvislosti s řízením IS/IT projektů je tedy třeba posoudit:

- jaká rizika projektu hrozí,
- jak je lze zcela eliminovat nebo alespoň snížit jejich úroveň.

Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů, a naopak umožňují využít příležitosti působení pozitivních vlivů. Součástí procesu řízení rizik je rozhodovací proces, vycházející z analýzy rizika. Po zvážení dalších faktorů, zejména ekonomických, technických, ale i sociálních, politických a jiných, management pro řízení rizik vyvíjí, analyzuje a srovnává možná preventivní a regulační opatření. Posléze z nich vybere ta, která existující riziko minimalizují.

Zpracovaná analýza rizik není konečným dokumentem, rizika musí být následně dále upřesňována, zejména z pohledu reakce na ukončení vývoje systémů podniku a reflektovat na nové požadavky vyplývající z rutinního provozu.

Lze konstatovat, že základní analýza již vymezuje bezpečnostní požadavky na realizaci systému a poskytuje podklady pro podrobnou analýzu rizik, prováděnou před nastavením systému do rutinního provozu.

V daném případě je u analytických prací výhodné využít zkušeností s postupem využívajícím řízených interview, tj. „Facilitated Risk Analysis Process“ (FRAP)[5]. Tento proces byl vypracován CSI (Computer Security Institute a vychází z metodiky Delphy, tedy z postupu založeném na řízené diskusi se zástupci Zadavatele. Hlavní důraz při jejím provádění je kladen na řízená jednání expertů a pracovníků Zadavatele jakož i Zpracovatele a na komunikaci s těmito pracovníky, kteří se na provádění analýzy podílejí.

Přitom metoda vychází z předpokladu, že obdržené výsledky analýzy jsou na úrovni odpovídající odborné fundovanosti a znalosti prostředí IS jednotlivých zúčastněných pracovníků.

S ohledem na tyto skutečnosti je třeba daný přístup považovat za první krok, kdy je třeba řešit základní požadavky spojené se stanovením bezpečnosti systému, přičemž podrobná analýza rizik může být provedena v dalším kroku (před nasazením do rutinního provozu).

[5] Thomas Peltier, Information Security Risk Analysis, CRC Press, 2001 - Počet stran: 296 ISBN: 0-8493-0880-1.

7.4 Návrh opatření – prevence proti identifikovaným hrozbám a rizikům

Metody a postupy reflektují doporučení bezpečnostních norem.

7.4.1 Fáze analýzy rizik

1. Identifikace aktiv
   Identifikace aktiv systémů v rámci podniku a jejich základní členění na:

   - informační aktiva
   - podpůrná aktiva
   - aktiva technické infrastruktury,
   - fyzická aktiva,
   - personál.

2. Ohodnocení aktiv.
   Zde jsou stanoveny hranice analyzovaného systému a definují se aktiva spravovaná v systému, kdy se u identifikovaných aktiv systému určí jejich hodnoty a ohodnotí závažnost dopadů bezpečnostních incidentů (Business Impact Analysis) podle identifikátorů hodnocení a se stanovením požadavků na obnovu aktiv v případě havárie (BCP – Business Continuity Plan), tedy zajištění nepřetržitosti provozu.
3. Analýza hrozeb a zranitelností dle metodiky stanovené v ČSN ISO/IEC 27005:2008.
4. Stanovení rizik dle vztahu:

   Riziko = funkce f (dopad hrozby, pravděpodobnost výskytu hrozby)

7.4.2 Aktiva informačního systému

Stanovení odpovědnosti za aktiva je nutnou podmínkou pro dosažení odpovídající bezpečnosti informací.

Musí být stanoven vlastník každého identifikovaného aktiva nebo skupiny aktiv a vlastníkovi musí být přiřazena odpovědnost za udržování příslušných nástrojů řízení bezpečnosti. Odpovědnost za

implementaci nástrojů řízení bezpečnosti může být delegována, ačkoliv zodpovědnost musí zůstat u určeného vlastníka aktiva.

Při tomto postupu základní analýzy můžeme aktiva seskupovat do kategorií, což umožňuje zjistit a popsat způsoby jejich zpracování. Informační aktiva zobrazují významné komponenty informačního systému s bezprostředním vlivem na informační bezpečnost.

Dané skutečnosti jsou posuzovány z pozice nejhorších případů spojených s dopady, které by mohly vyplynout zejména z následujících skupin důsledků:

- nedostupnosti dat,
- prozrazení dat,
- modifikace dat,
- zničení dat.

Bližší posouzení standardně vychází ze čtyř hlavních bezpečnostních hledisek, týkajících se i aktiv informačního systémů podniku, tj.:

- narušení důvěrnosti dat – ze strany uživatelů neoprávněných, ale i ze strany uživatelů překračujících rozsah svého oprávnění;
- modifikace dat nebo programů – vlivem chyb, poruch systému a/nebo aktivní (úmyslnou) či nedbalostní činností uživatelů;
- zničení dat nebo programů – vlivem chyb (hardware, software, správy IS nebo uživatelů, a to rovněž aktivní (úmyslnou) či nedbalostní činností);
- nedostupnost – zamezení přístupu oprávněných uživatelů do systému nebo datům.

Při základním posuzování aktiv je zásadou pomíjet stávající realizovaná opatření, aby nedošlo ke zkreslení výsledku díky jejich stávající účinnosti.

7.4.3 Ohodnocení aktiv

U všech aktiv je stanovena i jejich hodnota, závislá na hodnocení výše uvedených typů aktiv a vazeb plynoucích z kategorií aktiv.

Informační aktiva, která jsou předmětem zkoumání v této etapě projektu, byla identifikována na základě úvodních pohovorů, kdy se dané skutečnosti posuzovaly z pozice nejhorších případů, které by mohly vyplynout zejména z následujících skupin důsledků:

- nedostupnosti dat,
- prozrazení dat,

- modifikace dat,
- zničení dat.

Každé z výše uvedených hledisek je třeba hodnotit z konkrétních dílčích hledisek:

- v případě nedostupnosti je nutné hodnotit alespoň tři časové úseky specifikující dobu nedostupnosti, kdy dojde k určité formě dopadů a následků – od pouhých nepříjemností přes vážný problém až po nezvratné změny.
- u zničení se zvažuje, zda se jedná o totální zničení bez možnosti náhrady, či o zničení s možností obnovy z náhradních zdrojů – tj. v našem případě informačních aktiv o pořízení dat z náhradních zdrojů.
- v případě chybné funkce se jedná o rozlišení ve vztahu k alespoň třem časovým úsekům specifikujícím dobu chybné funkce, kdy dojde k určité formě dopadů a následků – od pouhých nepříjemností až vážným problémům.
- u modifikace je hodnocena chyba nebo úmysl.

Jelikož se ukazuje dosti obtížné, přiřadit jednotlivým aktivům finanční hodnotu, efektivní cesta k ocenění, resp. ohodnocení významu aktiv spočívá v odhadu důležitosti posuzovaných aktiv v rámci navrženého systému.

Numerické údaje tedy nevyjadřují hodnotu nebo kvantitu veličiny, ale příslušnost do dané oblasti. Tím, že se pracuje s veličinami, které spadají do definovaných intervalů, se do jisté míry eliminuje různá kvalita (různá úroveň hodnocení) získaných podkladů.

Obvyklými důsledky naplnění hrozeb jsou dopady finanční (vícenáklady, ušlý zisk, náklady na soudní spor, náhrada škody apod.). Ale mohou to být i dopady společensko-politické (neschopnost organizace zajistit určitou činnost, vyplývající ze zákona nebo z vlastního rozhodnutí příslušného orgánu veřejné moci), jakož i dopady právní (porušení zákona – např. na ochranu osobních údajů).

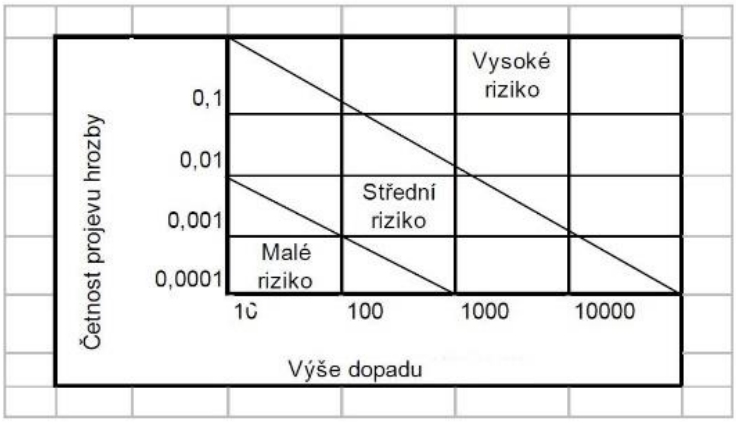
Některé lze kvantifikovat (zejména z oblasti finanční), některé nikoliv a v takovém případě nám přijde vhod výše popsaný kvalifikovaný odhad na pětistupňové stupnici.

Za klíčové dopady lze považovat již výše uvedené:

- pořizovací náklady či jiná hodnota aktiva,
- důležitost aktiva pro existenci či chování subjektu,
- náklady na překlenutí případné škody na aktivu,
- rychlost odstranění případné škody na aktivu,
- jiná hlediska (mohou být specifická případ od případu)

Hodnoty z tabulek, tj. pravděpodobnost vzniku hrozby, hodnota aktiva a zranitelnost daného aktiva jsou podkladem k výpočtu rizik. Vypočtenou míru rizik pak můžeme vyjádřit ve formě matice

rizik. Zde můžeme identifikovat pásma rizika definovaná hranicemi pro nízká (přijatelná), střední a vysoká rizika takto (měřítko je ilustrativní):



Obrázek 7.1 Matice rizik

Při identifikování hlavních informačních aktiv se vychází z procesního řízení a stanovuje se výše každého případu v rozsahu od stupně „velmi nízký“ do „kritický“.

V návaznosti na zhodnocení vlivu hrozeb na řešené prostředí informačního systému vyplývá i obsah tabulky (viz příloha), kde jsou, ve vztahu na nedostupnost či chybnou funkci aktiva, hodnoceny tři časové úseky specifikující dobu nestandardní situace, kdy dojde k určité formě dopadů a následků – od pouhých nepříjemností přes vážný problém až po nezvratné změny.

7.4.4 Analýza hrozeb a zranitelností

Pro provedení analýzy rizik je hodnota identifikovaných aktiv základním vstupem. V širším pojetí zahrnujeme do informačních aktiv i aktiva, která souvisejí s technickou infrastrukturou posuzovaných informačních systémů, i personální a objektovou oblastí.

Úroveň hrozby stanovujeme jako pravděpodobnost výskytu hrozby a úroveň zranitelnosti odpovídá pravděpodobnosti, že se hrozba vyplní s tím, že se hodnotí důležitost aktiva napadeného hrozbou.

Princip odhadu hrozeb a zranitelností

Vzhledem k množství faktorů, které mohou zapříčinit dopad hrozby na informační systém, byly jednotlivé hrozby a zranitelnosti strukturovány podle názvu příslušných aktiv, přičemž bylo dodrženo členění normy ČSN ISO/IEC 27001. Takto zvolený přístup umožnil postihnout celou šíři hrozeb a zranitelností, potenciálně směrovaných na prostředí informačního systému.

Důležité je, aby se vždy hodnocení soustředilo na možné projevy vyplývající mj. z následujících nestandardních situací a činností s ohledem na charakter daného informačního systému, zejména na:

- logická infiltrace (neoprávněný přístup, zneužití oprávněného přístupu, neoprávněné použití aplikace, viry apod.),
- infiltrace komunikace (aktivní narušení komunikace, zneužití logického propojení apod.),
- chyby lidského faktoru (chyby uživatelů, administrátorů, operátorů apod.),
- provozní závady IS,
- fyzické hrozby (krádež, úmyslné poškození, terorismus).

Posuzuje se, do jaké míry by působením hrozeb ve vztahu k identifikovaným zranitelnostem utrpěl informační systém, resp. podnik významnou újmu či případní narušitelé získali významný prospěch.

Metrika hrozeb a zranitelností

Pro stanovení úrovně hrozeb i zranitelnosti byla zvolena pětibodová stupnice, na rozdíl od tříbodové metriky použité v metodice CRAMM. Tato diference vyplynula ze zvolení jiného postupu při výpočtu míry rizika, kdy v našem případě jsou východiskem doporučení a postupy uvedené v normě ČSN ISO/IEC 27005.

Vyjádření úrovní hrozeb a zranitelností je uvedeno v následujících stupních významnosti takto:

Tabulka 7.1 Matice hrozeb a zranitelností

Hrozby	
1	velmi nízké
2	nízké
3	střední
4	vysoké
5	kritické

Zranitelnost	
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	kritická

Použitá metoda stanovení míry rizik[6]

V našem případě byla zvolena metoda analýzy rizik využívající matice aktiv, hrozeb a zranitelností.

Při této analýze rizik se využívají následující tabulky:

- tabulka, obsahující identifikovaná aktiva spolu s jejich hodnotou;

[6] Viz též Smejkal V., Rais K., Řízení rizik ve firmách a jiných organizacích. 4. vydání, Praha Grada Publishing. 2013

- tabulka, obsahující identifikované hrozby a pravděpodobnost možnosti jejich realizace;
- tabulka zranitelností systému.

Hodnoty z tabulek, tj. pravděpodobnost vzniku hrozby, hodnota aktiva a zranitelnost daného aktiva jsou podkladem k výpočtu rizik. Vypočtenou míru rizik pak můžeme vyjádřit ve formě matice rizik.

Míru rizika lze zjistit výpočtem dle vztahu:

Riziko = funkce (pravděpodobnost výskytu hrozby, výše dopadu na aktivum)

S ohledem na hodnotu aktiva je pak stanoven bezpečnostní profil pro aktiva zahrnutá do analýzy rizik a návazně pak budou definována příslušná opatření k ošetření rizik. Lze již nyní poznamenat, že srovnání bezpečnostního profilu a stávajících opatření přijatých v daném informačním systému dává relevantní podklady k vytvoření bezpečnostního modelu maturity (úrovně bezpečnostní zralosti) systému.

Ke stanovení míry rizika bude využito principů definovaných v normě ČSN ISO/IEC 27005:2009 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací) Grafické znázornění míry rizika je v daném případě velmi přehledné a lze jej dobře využít pro zpracování souborů návazných plánů pro ošetření jednotlivých rizik, jakož i podklady pro sledování navržených akčních plánů.

V návaznosti na doporučení normy ISO/IEC 27005:2008 a z pohledu efektivnosti řešení rizik v informačních systémech podniku (jakož i s ohledem na charakter získaných podkladových materiálů) je zvolena metoda využívající tedy dvou základních parametrů, kdy míra rizika je funkcí pravděpodobnosti výskytu incidentu a dopadu uskutečnění hrozby ve vztahu k příslušnému aktivu.

Nejdříve je ke každému aktivu přiřazena jeho hodnota. Tato hodnota vyjadřuje míru nepříznivého dopadu, ke kterému by došlo v případě ohrožení daného aktiva.

Pro určení pravděpodobnosti výskytu této události je možné s výhodou využít empiricky zjištěných hodnot z veřejně dostupných zdrojů.

Tyto hodnoty uvedené v příslušných tabulkách pak vyjadřují pravděpodobnost výskytu dotčené události.

Následně je pak nalezením průsečíku hodnot dopadu na aktivum a pravděpodobnosti výskytu dané události v součtové tabulce je určena míra rizika pro dotčené aktivum. Tabulkou je pak tato operace vyjádřena následovně:

Tabulka 7.2 Matice pravděpodobností

pravděpodobnost	velmi nízká	1–2	**1**
	nízká	3–4	**2**

	střední	5–6	**3**
	vysoká	7–8	**4**
	kritická	9–10	**5**

K hodnocení míry jednotlivých rizik (inherentního, reziduálního a zbytkového) je použita tzv. součtová matice.

V etapě analýzy rizik a před přijetím opatření na jejich eliminaci se realizuje ohodnocení inherentních rizik (tj. bez zohlednění již existujících či uvažovaných opatření v analyzovaném systému). Po implementaci opatření tak musí být provedeno nové hodnocení míry rizik tak, že je stanovena míra rizika reziduálního, tj. s uvažováním dopadu provedených opatření, popř. cílového rizika, které vychází ze strategického manažerského rozhodnutí, kde je stanovena míra daného rizika, která je již plně akceptovatelná.

V tabulkách jsou hodnoty pravděpodobnosti výskytu rizika definovány takto:

Tabulka 7.3 Matice pravděpodobnosti výskytu

Pravděpodobnost výskytu		
Stupeň	% za rok	Slovní vyjádření
1	<0; 5>	prakticky nepravděpodobné
2	<5; 20>	málo pravděpodobné
3	<20; 50>	příležitostné
4	<50; 70>	pravděpodobné až časté
5	<70; 100>	velmi časté

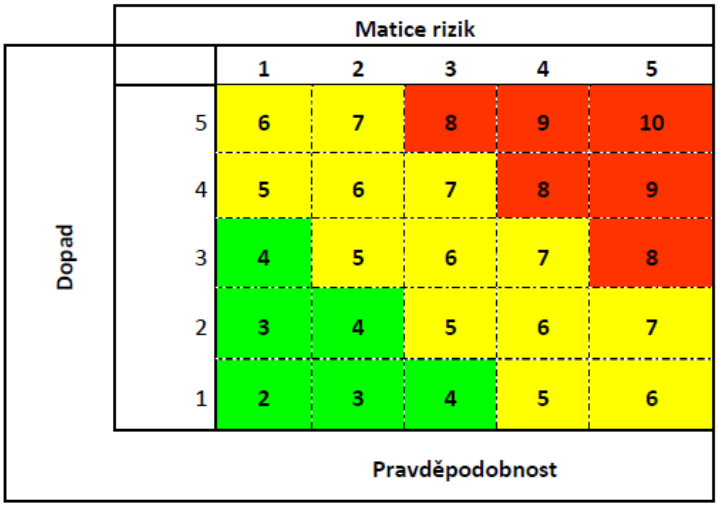
Dopad je ohodnocen mírou následků pro subjekt rovněž ve stupnici 1-5.

Tabulka 7.4 Matice dopadu

Dopad		
Stupeň	Dopad	Následek pro aktiva
1	nevýznamný	Nemá vliv na aktiva nebo je zcela zanedbatelný
2	malý	Nepodstatný, velmi malý vliv na aktiva

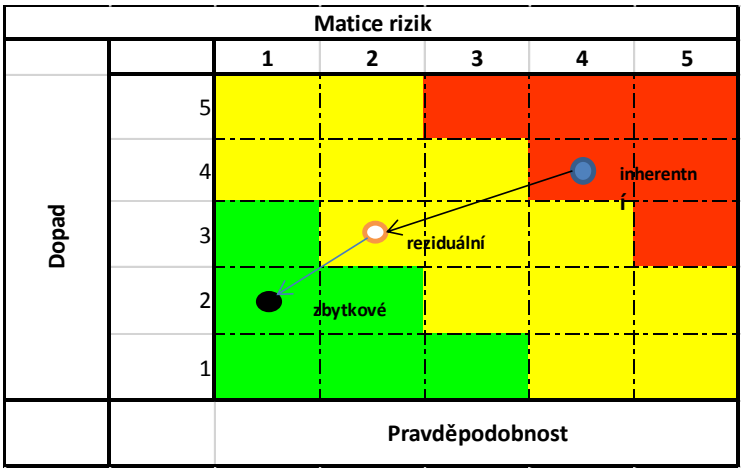
3	střední	Má vliv na aktiva a ztráty jsou řešitelné v rámci stávajících aktiv (Projektu)
4	značný	Má značný vliv na aktiva a ztráty jsou řešitelné pouze mimořádnými opatřeními (zvýšení nákladů, časového harmonogramu atd.)
5	fatální, obrovský	Má kritický vliv na aktiva a potenciální ztráty jsou tak velké, že mohou vést k zrušení Projektu, zakázky, diskreditaci Objednatele apod.

Numerické údaje tedy nevyjadřují hodnotu nebo kvantitu veličiny, ale příslušnost do dané oblasti. Tím, že se pracuje s veličinami, které spadají do definovaných intervalů, se do jisté míry eliminuje různá kvalita (různá úroveň hodnocení) získaných podkladů. V souladu s metodikou uvedenou v ČSN ISO/IEC 27005:2009 jsou evidovaná rizika strukturovaná dle své úrovně do součtové matice rizik uvedené na následujícím obrázku, kde jsou ilustrovány oblasti s danými číselnými hodnotami.



Obrázek 7.2 Součtová matice rizik

Při návrhu odpovídajících bezpečnostních opatření dochází k „posunům“ v tabulkách rizik z úrovně inherentního rizika na úroveň reziduálního rizika, kdy je nutno brát v úvahu účinnost navrhovaných opatření, která jsou v rámci informačního systému implementována. Pro ilustraci je uveden příklad posunu z úrovně inherentního rizika na úroveň reziduálního rizika.



Obrázek 7.3 Eliminace evidovaných rizik

Důležité je zdůraznit, že míru reziduálního rizika neurčují opatření, která jsou teprve uvažována či připravována. Zbytkové riziko je svázáno se strategickým manažerským rozhodnutím, kdy je stanovena míra daného rizika, která je pro podnik v dané situaci akceptovatelná.

Z toho vyplývá, že v systému správy bezpečnostních rizik musí vlastník rizika po jeho zjištění a evidenci stanovit úroveň rizika ve třech základních kategoriích:

- inherentní riziko – míra evidovaného rizika bez implementovaných opatření,
- residuální riziko – aktuální míra evidovaného rizika (při zohlednění implementovaných opatření),
- zbytkové riziko – cílový stav, který nevyžaduje žádné akce na jeho řešení.

Metrika míry rizik

Pro zpracování analýzy rizik v rámci informačních systémů může být zvolena stupnice, kde jsou hodnoty strukturovány do „oblastí“, takže můžeme danou veličinu zařadit po položku:

- 1 = velmi nízké – prakticky nepravděpodobné,
- 2 = nízké – málo pravděpodobné apod.

- Míra rizika 2–4 znamená, že je možné dané riziko akceptovat, toto riziko není vyřazeno z evidence, nejsou přijata žádná opatření, která by vedla k eliminaci tohoto rizika, většinou se jedná o rizika, u kterých by náklady spojené s odpovídajícím opatřením byly vyšší než potenciální dopad uskutečněné hrozby.

- Míra rizika 5–7 značí, že se jedná o riziko, které vyžaduje přijetí adekvátních opatření, v rámci ošetření tohoto rizika je nutné zpracovat plán mitigace (snížení) tohoto rizika a příslušné činnosti budou průběžně sledovány v rámci správy rizik. Dané riziko bude posouzeno při pravidelné kontrole (vesměs se jedná o pravidelné každoroční aktivity).

- Míra rizika 8–10 ukazuje na kritickou oblast a vyžaduje okamžité přijetí nápravy.

Numerické údaje tedy nevyjadřují hodnotu nebo kvantitu veličiny, ale příslušnost do dané oblasti.

V rámci této tabulky jsou následně stanoveny hranice pro nízká (přijatelná), střední a vysoká rizika.

Každé riziko je charakterizováno množinou {úroveň hrozby; úroveň zranitelnosti; pravděpodobnost výskytu rizika; výše škody}, přičemž v rámci návrhu systému bude k takto definovaným rizikům přiřazeno navrhované opatření.

Metodika výpočtu rizika

Míra rizika podle metody postavené na vztahu výše dopadu události (resp. uskutečnění hrozby) na dané aktivum a pravděpodobnosti výskytu takové události je relativní veličina ve stupnici 2–10. Tato hodnota vychází ze závislosti jednotlivých atributů (hrozby, zranitelnosti apod.) stanovených v předchozích etapách analýzy.

Pro další práci s evidovanými riziky systému a další činnosti svázané se správou rizik související s jejich hodnocením ve vztahu ke všem kategoriím rizik (tj. inherentnímu, reziduálnímu a zbytkovému riziku) jsou využity příslušné tabulky uvedené v příloze. Získané hodnoty jsou pak uvedeny v tabulce rizik.

Cílem analýzy rizik je evidence a stanovení míry jednotlivých základních rizik informačního systému podniku Analýza rizik je vždy směrována do výpočtu míry inherentních rizik, tj. rizik systému, kde nejsou uplatněna bezpečnostní opatření.

Dělení evidovaných rizik do příslušných matic rizik se uplatní až při evidenci a stanovení reziduálních rizik, informačních systémů, To umožní jednoznačně sledovat účinnost implementovaných bezpečnostních opatření a využít hodnoty v daných maticích při plánování procesu řízení rizik.

V příslušných tabulkách (maticích rizik) jsou rizika umístěna v závislosti na pravděpodobnost jejich výskytu a dle dopadu na aktiva podniku, které projev tohoto rizika způsobí.

ČERVENÁ OBLAST – pro rizika, která jsou začleněna do této oblasti, musí být navrženo bezpečnostní opatření k jejich zvládnutí a tvorba plánů eliminace těchto rizik má vysokou prioritu.

ŽLUTÁ OBLAST – míra rizika, umístěného v této oblasti umožňuje posouzení nezbytnosti realizace bezpečnostních opatření, jejich rozsahu a časového plánu. Nicméně je třeba zdůraznit, že navržený přístup musí být důkladně zvážen a případná akceptace tohoto rizika musí být zdůvodněna a musí podléhat periodické kontrole.

ZELENÁ OBLAST – vytváří prostor, kde rizika mohou být akceptována, neboť jejich dopad či frekvence jejich výskytu nevyžaduje realizaci opatření. Reakce na tato rizika ve většině případů spadá do organizační úrovně.

Základní analýza rizik informačních systémů podniku je koncipována tak, aby poskytla podklady pro realizaci opatření, adekvátní ke zjištěným hrozbám. Na rizika zjištěná a evidovaná v základní analýze rizik musí reagovat bezpečnostní opatření již následující etapě vývoje. Uplatněná bezpečnostní opatření se pak odrazí v maticích rizik, kdy bude možné poukázat na eliminaci inherentních rizik na hodnoty reziduálního rizika, popř. až na zbytkovou hodnotu rizika.

Kapitola obsahuje souhrnný popis jednotlivých etap analýzy rizik. Jsou zde definice hrozeb a zranitelností informačního systému, Je ukázán postup při oceňování rizik a stanovení následných opatření.

1. Popište jednotlivé kroky analýzy rizik.
2. Vysvětlete pojmy aktivum, hrozba, zranitelnost.
3. K čemu se využívá součtová matice dopadu a pravděpodobnosti?
4. Na základě, čeho jsou oceňována rizika?

Literatura k tématu:

[1] SMEJKAL, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích.* 4. aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.

Kapitola 8

Realizace bezpečnosti

Po prostudování kapitoly budete umět:

- stanovit základní přístup při zpracování bezpečnostní politiky;
- stanovit bezpečnostní opatření v návaznosti na výsledky analýzy rizik.

Klíčová slova:

Bezpečnostní politika, bezpečnostní opatření, bezpečnostní normy.

8.1 Stanovení bezpečnostní politiky

Bezpečnostní politika je základním dokumentem podniku, který vymezuje rozsah a určení nutných opatření při vybudování systému řízení bezpečnosti informací. Řeší základní organizační aspekty při formulování přístupu k budování bezpečnostních opatření. Při formulování bezpečnostních zásad je třeba při návrhu bezpečnostní politiky vycházet z toho, že realizovaný bezpečnostní systém musí zahrnovat nejrůznější úrovně i způsoby zabezpečení – od komplexních služeb a řešení na úrovni globálních sítí až k podnikovým sítím a jednotlivým koncovým zařízením s využitím nejmodernějších technologií ochrany před počítačovými viry, hackingem, útoky na dostupnost (denial of service) a nedbalostí koncových uživatelů. Samozřejmostí je zálohování důležitých dat mimo firmu. Jedná se tedy o komplexní ochranu v rámci stanoveného bezpečnostního perimetru podniku.

8.2 Bezpečnostní opatření – v návaznosti na analýzu rizik

Bezpečnostní opatření jsou realizována postupně pro zavádění jednotlivých bezpečnostních prvků podle stanovených priorit a ekonomických možností **podniku** s tím, že respektují výsledky analýzy rizik.

Návrh bezpečnostních opatření jednoznačně souvisí s mechanismy, které naplňují následující bezpečnostní funkce:

- systém identifikace a autentizace,
- řízení přístupu,
- funkce zajišťující integritu a důvěrnost,
- systém kontrol,
- mechanismy ochrany dat,
- mechanismy fyzické bezpečnosti.

Základní principy bezpečnostních opatření v rámci technologické infrastruktury jsou řízeny v souladu s doporučením dle ČSN ISO/IEC řady 27000.

Určujícím požadavkem na fungování bezpečnostních nástrojů je zajištění následujících bodů:

- vysoká dostupnost,
- aplikační load balancing,
- odolnost proti chybám a aktivním útokům,
- odolnost proti neoprávněnému přístupu,
- minimalizace škod způsobených logickou chybou => definice zálohovací strategie a obnovy,
- zajištění zabezpečené komunikace,
- zajištění informační infrastruktury splňující požadavky na integritu, dostupnost a bezpečnost zpracovávaných, distribuovaných a ukládaných informací,
- bezpečnostní monitoring,
- administrace systému.

Klíčovým principem návrhu řešení bezpečnostních opatření je procesní integrace, která je v souladu zejména s odpovídajícími postupy a doporučeními normy ČSN ISO/IEC 27001:2014.

Navrhovaná bezpečnostní protiopatření musí poskytovat ochranu v několika různých směrech:

- sníží hrozbu,
- sníží zranitelnost,
- sníží dopad nežádoucí události,
- detekují nechtěnou událost,
- umožní zotavení systému z nechtěné události.

V navržených opatřeních musí být dodrženy následující bezpečnostní principy:

- první úroveň bezpečnostních opatření se týká zajištění fyzické bezpečnosti serverů,
- přístup k databázím bude umožněn pouze pro přesně specifikované role s nezbytnými právy,
- provozované aplikace nebudou oprávněné upravovat data přímo a editace dat bude možná pouze pomocí uložených procedur, které zajistí správnou manipulaci s daty, přičemž bude využito auditní logování pro záznam přihlašování a činnosti jednotlivých uživatelů,
- požadavky na zabezpečení zpracovávaných informací i koncepce bezpečnosti informačních systémů podniku musí být v souladu s bezpečnostními předpisy podniku a s požadavky stanovenými v bezpečnostních zákonných opatřeních.

Základními dokumenty, které formují procesy a metody při zajišťování bezpečnosti v podnikových informačních systémech jsou uvedeny v bezpečnostních normách ČSN ISO/IEC řady 27000. Metodické řízení navrhovaného systému řízení bezpečnosti je obsaženo CoBit v. 5 a ITIL v. 3. Jedná se o soubory dokumentů, které vycházejí z „nejlepších přístupů“, které se při realizaci bezpečnosti využívají.

V návaznosti na tyto dokumenty lze koncipovat i realizovat správné postupy řízení, kontroly a auditu informačních technologií.

Vzhledem k tomu, že podle těchto dokumentů a zejména metodik musí realizace bezpečnosti podléhat procesnímu řízení. S tím souvisí nezbytné nastavení procesů, které zajišťují bezpečnost v informačních systémech. Je nutné tento přístup skloubit s bezpečnostními požadavky z pohledu využívaných bezpečnostních produktů (šifrovacích zařízení, zabezpečených úložišť apod.)

Procesní přístup je nutné nastavit i při řízení provozu.

V rámci realizace bezpečnosti je nutné realizovat systém správy nestandardních událostí. Ve smyslu metodiky ITIL se jedná o nastavení procesů:

- Správa incidentů
- Správa bezpečnostní problémů
- Správa změn

V kapitole je ukázán smysl návrhu, realizace a schválení bezpečnostní politiky. Následně jsou pak rozebírána jednotlivá bezpečnostní opatření pokrývající evidovaná rizika zjištěná v rámci analýzy rizik.

1. Charakterizujte účel realizace bezpečnostní politiky.
2. Jaké jsou hlavní účely při stanovení bezpečnostních opatření?
3. Jak se do návrhu bezpečnostních opatření promítají doporučení ČSN norem řady 2700?

Literatura k tématu:

[2] MATES, P., SMEJKAL, V. *E-government v České republice. Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání. Praha: Leges, 2012, 456 str., ISBN 978-80-87576-36-6.

[2] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.

Kapitola 9

Kryptografie

Po prostudování kapitoly budete umět:

- vysvětlit pojmy souvisejících s kryptografií;
- popsat základní kryptografické algoritmy;
- popsat blokové a proudové šifry;
- vysvětlit pojmy DES, AES, RSA;
- vysvětlit pojem elektronický podpis;
- charakterizovat dynamický biometrický podpis.

Klíčová slova:

Kryptografie, šifra, šifrový algoritmus, DES, RSA, AES, asymetrická šifra, symetrická šifra bloková šifra, elektronický podpis DBP.

9.1 Úvod

Jedním z nejdůležitějších institutů při studiu kryptografie je matematika.

Po probrání tematického okruhu posluchači budou seznámeni s pojmy používanými při řešení současné šifrové ochrany. Zároveň se seznámí s postupem při šifrování informace symetrickou a asymetrickou šifrou. Budou mít přehled o tvorbě a možnostech použití elektronického podpisu.

9.2 Kryptografie ve věku počítačů

Kryptologie nepojednává o kryptách, což se mnoho lidí stále ještě domnívá, ale řeší otázky šifer. Šifrování je proces převedením dat do takového formátu, který nemůže neoprávněná osoba jednoduše přečíst.

Než ale metody šifrové ochrany dospěly do tohoto stádia, musela kryptologie projít velmi dlouhým a složitým vývojem. Cílem tématu je ukázat hlavní mezníky při tomto vývoji, využití mechanizačních nástrojů a následky boje mezi tvůrci a luštiteli šifer. Zároveň je cílem pojednat o základních nevýhodách historických šifrových systémů a ukázat praktické využití některého e šifrových mechanismů

Moderní kryptografie využívá dvou základních směrů – symetrické a asymetrické šifrové algoritmy. Při symetrickém šifrování obě strany používají stejný tajný klíč, a to při šifrování i dešifrování zprávy. Asymetrické šifrování je postaveno na principu, kdy každý účastník vlastní veřejný a privátní klíč pro šifrování a dešifraci zprávy. U asymetrického šifrování zná odesilatel pouze veřejný klíč příjemce a jím zašifruje svou zprávu. Příjemce pak použije svůj privátní klíč pro dešifrování této zprávy. Nikdo jiný nemůže dešifrovat tuto zprávu např. použitím veřejného klíče ani nemá možnost odhalit privátní klíč příjemce. Vzhledem k výpočetní složitosti asymetrických algoritmů se nešifrují celé zprávy, ale jejich kryptografický kontrolní součet – tzv. otisk zprávy, který je vytvořen s využití kryptografické hash funkce. (v současnosti SHA 256)

S asymetrickým šifrováním je spojena nová služba v elektronickém světě – elektronický podpis. V tom případě odesilatel použije svůj privátní klíč pro „zašifrování“ - podepsání své zprávy, resp. otisku zprávy. Příjemce pak použije veřejný klíč odesilatele „dešifrování“ otisku zaslané zprávy. Jiným než veřejným klíčem odesilatele nelze úspěšně tuto kontrolu otisku provést.

9.3 Proudové, blokové šifry

Proudové šifry V tomto algoritmu se otevřený text zpracovává bit po bitu, tj. je odebrán jeden bit otevřeného textu a na něm je provedena řada operací pro generování jednoho bitu šifrového textu. Technicky jsou proudové šifry blokové šifry o bloku velikosti jednoho bitu. Při šifrování se využívá produkce generátoru pseudonáhodné posloupnosti bitů jako klíče. Aby implementace šifry měla odpovídající úroveň bezpečnosti, musí být produkce generátoru pseudonáhodné posloupnosti kvalitní. Důležité je, aby aktivace pseudonáhodného generátoru nezačínala ve stejných počátečních podmínkách, tj. produkovaný řetězec nesmí být znovu použit.

Z používaných proudových šifer lze zmínit algoritmus RC4, který patřil nejrozšířenější zejména v softwarových aplikacích. Vzhledem k tomu, že provedené studie odhalily zranitelnosti v RC4 byl tento algoritmus ze všech aplikací stažen a v současné době se již nevyužívá.

Blokové šifry jsou postaveny na šifrovacím algoritmu, který zašifruje blok dat otevřeného textu o velikosti n-bitů najednou. Obvyklé velikosti každého bloku jsou 64 bitů, 128 bitů a 256 bitů. Takže například 64bitová bloková šifra bude mít 64 bitů otevřeného textu a bude šifrována do 64 bitů šifrového textu. Otevřený text se tedy dělí do jednotlivých stejně velkých bloků. V případě blok otevřeného textu je kratší (vesměs poslední blok) je doplněn tzv. „zrním“, tj. náhodnou posloupností dat příslušné délky.

- V současné době se používají standardně blokové šifry. Některé z běžně používaných šifrovacích algoritmů, ze skupiny blokových šifer jsou algoritmy DES, Triple DES, AES, IDEA a Blowfish. Zajímavý je též algoritmus GOST 28147-89, který byl navržen pro státní orgány bývalého SSSR.

V dalších kapitolách jsou blíže uvedeny algoritmy DES a AES.

9.4 Symetrické algoritmy (registry kryptografických algoritmů)

Mezi hlavní představitele blokových šifer patří algoritmy:

- DES
- IDEA (International Data Encryption Algorithm) - (blok 64 B, klíč 128) - využití v systému PGP
- GOST 28147-89 - algoritmus pro státní orgány bývalého SSSR a
- AES (Advanced Encryption Standard) – algoritmus "Rijndael" (belgičtí autoři Rijmen a Daemen) - klíče 128, 192 a 256. – nová norma (nahrazuje DES)

Blíže se seznámíme s algoritmy DES a AES

Standard šifrování dat (DES)

V roce 1973 vláda USA v reakci na opakované požadavky od průmyslu a různých organizací dala svému ministerstvu úlohu stanovit jednotné federální normy pro automatické zpracování dat a v rámci tohoto oddělení byla odpovědnost předána Národnímu úřadu pro normalizaci (NBS). Jedním z konkrétních aspektů, které NBS považuje za vytvoření standardu pro šifrování dat.

Specifikace standardu šifrování dat zveřejněného NBS stanovila podmínky, které musí každý navržený algoritmus splňovat: že musí poskytovat vysokou úroveň zabezpečení, že bezpečnost nesmí být založena na tajnosti algoritmu, musí být ekonomická implementovat elektronicky, efektivně používat a k dispozici všem uživatelům a dodavatelům.

V rámci tohoto požadavku byl vytvořen návrh šifrového algoritmu IBM, který byl přijat a stal se "standardem šifrování dat" - DES.

Jedná se o blokovou šifru, kdy:

1. Algoritmus je navržen tak, aby šifroval bloky 64 bitů dat pod řízením 64bitového klíče (K).
2. Dva uživatelé, kteří chtějí komunikovat pomocí DES, se musí shodnout na (tajném) klíči, K.
3. U tajného klíče JC uživatelé vybírají sedm 8-bitových znaků (tj. Celkem 56 bitů) a DES pak sousedí s dalšími 8 bitovými bity parity, které jim dávají požadovaný 64bitový tajný klíč.

Postup zašifrování:

1. 64bitový blok dat je zadán jako počáteční permutace (IP).
2. 64 bitů dat je rozděleno na dva 32-bitové segmenty, vlevo (L) a vpravo (R).

3. Osmdesát osm bitů klíče K je kombinováno s nelineárním rozšířením 48bitové verze R ("expanze" se skládá z opakování 16 z 32 bitů R) a těchto 48 bity jsou pak "redukováno“ na 32bitový řetězec X.
4. L je nahrazeno R a R je nahrazen součtem (mod 2) X a L za účelem získání nového 32bitového R.
5. Kroky ad 6. a ad 7 se opakují 16krát pokaždé za použití různých 48bitových segmentů K v kroku 6.
6. 64 bitů finálového 16tého cyklu (rundy) je upraveno inverzní počáteční permutaci, tj. K (IP) -1.
7. Výsledkem je 64 bitů zašifrovaného bloku.

Postup dešifrování

8. Dešifrování se provádí pomocí šifrovací procedury v opačném pořadí stejným klíčem, K.

Při použití této šifry se musí uživatelé, kteří chtějí komunikovat pomocí DES, dohodnout na společném klíči a toto může být mezi nimi dohodnuto pomocí systému výměny klíčů Diffie-Hellman. Pokud třetí strana nezíská daný klíč, měla by být bezpečnost přeneseného textu zajištěna.

Co se týče bezpečnosti algoritmu DES – bylo provedeno mnoho statistických a dalších testů na šifrovaných datech s různými klíči pomocí DES a bylo zjištěno, že při využití současných technologií a při sdílení dílčích výsledků v distribuované síti počítačů nejsou výsledky uspokojivé. Chybí zde základní předpoklad pro kvalitní blokovou šifru, tj. změna jednoho bitu na vstupu vyvolá změnu ve všech bitech na výstupu.

Z tohoto důvodu je šifra DES nahrazena šifrou AES.

Algoritmus šifrování dat AES

Současným standardem, který byl zaveden v roce2002 jako Standard federální vlády USA, využívá algoritmus AES (Advanced Encryption Standard). Je doporučen jako spolehlivý prostředek šifrové ochrany v aplikacích zajišťujících bezpečnost zpracovávaných dat, neboť v současné době provedené studie neprokázaly u tohoto algoritmu slabiny. Jedná se o blokovou šifru s velikostí bloku 128 bitů a podporuje tři možné velikosti klíče - 128, 192 a 256 bitů. Platí zde, čím delší je velikost klíče, tím silnější je šifrování. Dlouhé klíče však také vedou k delším procesům šifrování, což někdy vytváří určité potíže při implementaci AES, zejména do programových aplikací.

AES je iterativní bloková šifra, která je založena na principu "síti substituční permutace". Ta zahrnuje řadu propojených operací, z nichž některé zahrnují nahrazení vstupů specifickými výstupy (operace substituce) a další zahrnují „promíchání“ s bity „rundového“ klíče (operace permutace) v rámci jednoho cyklu (rundy).

AES provádí všechny své výpočty s Byty spíše než s bity. Proto AES zachází s blokem 128 bitů otevřeného textu jako se sadou 16 Bytů. Těchto 16 Bytů je následně zpracováno při uspořádání do matice o čtyřech sloupcích.

Na rozdíl od algoritmu DES je počet rund v AES variabilní a závisí na délce klíče. AES používá 10 rund pro 128bitové klíče, 12 rund pro 192bitové klíče a 14 rund pro 256bitové klíče.

V každé z těchto rund použit jiný 128bitový rundový klíč, který se vypočítá z původního klíče AES.

9.5 Asymetrické algoritmy

Asymetrické algoritmy jsou postaveny na principu, kdy šifrovací proces, využívá různé klíče pro šifrování a dešifrování informací. Použité klíče odlišné, ale jsou matematicky spárovány, takže tedy možné, že zašifrovaný otevřený text pomocí jednoho (veřejného) klíče z daného páru může být dešifrován s využitím druhého (privátního) z páru klíčů. Významnou výhodou zejména v počítačových sítích je velmi jednoduchá distribuce klíčů. Veřejný klíč je publikován a kdokoliv jej může využít k zašifrování textu a pouze držitel privátního klíče si jej může převést zpět do čitelné podoby.

Nejznámějším a široce používaným je algoritmus RSA nazvaný dle svých tvůrců Rivesta, Shamira a Adlemana.

RSA

Tento šifrový asymetrický systém patří mezi základní šifrové systémy, které byly navrženy. Při použití tohoto systému je nutné vyřešit dvě základní operace. Jedná se o:

- vygenerování páru klíčů,
- vytvoření šifrovacího/dešifrovacího algoritmu.

Generování páru klíčů RSA

Každá osoba nebo strana, která se chce účastnit komunikace pomocí šifrování, potřebuje vygenerovat pár klíčů, jmenovitě veřejný klíč a soukromý klíč. Postup při generování klíčů vygenerování využívá principu faktorizace velkých prvočísel. Kdy výpočetně v reálném čase nemožné z vypočtené hodnoty n, která je součástí veřejného klíče, při faktorizaci velkého prvočísla nalézt dva hodnoty (p & q), které se používají k získání n.

9.6 Elektronický podpis

Návrh asymetrických kryptografických algoritmů umožnil navrhnout řešení elektronického podpisu.

S využitím algoritmu RSA lze jednoduše „podepsat“ příslušnou zprávu tím, že odesilatel použije svůj privátní klíč pro „zašifrování“ - podepsání své zprávy. Příjemce pak použije veřejný klíč odesilatele „dešifrování“ otisku zaslané zprávy, čímž získá důvěryhodnou informaci o tom, kdy danou zprávu podepsal (zašifroval privátním klíčem, který vlastní pouze dotčený odesilatel). Jiným než veřejným klíčem odesilatele (který je spárován s jeho privátním klíčem) nelze danou zprávu ověřit.

9.7 Biometrický dynamický podpis

Alternativou k Elektronickému podpisu na bázi kryptografických metod je dynamický biometrický podpis.

Systémy dynamických biometrických podpisů zaznamenávají vlastnoruční podpis s využitím speciálního „pera“ a digitalizačního tabletu, zaznamenávajícího data, která umožní analyzovat jak statické, tak zejména dynamické vlastnosti podpisu spojeného s typickým chováním podepisující se osoby. Počet a rozsah analyzovaných parametrů závisí na zvoleném tabletu a SW analyzujícím sejmutá biometrická data. Navrhované systémy tak mohou analyzovat nejen data souřadnicového systému podpisu, ale i další dynamické identifikátory.

Dynamický podpis obsahuje biometrické informace o tom, jak podpis byl vytvořen, odráží tedy charakteristické znaky podepisující se osoby, její návyky a projevy chování. Tyto vlastnosti představují biometrickou stopu, která je unikátní pro každého jednotlivce a nemůže být padělatelem reprodukována (na rozdíl od samotného obrázku podpisu, který zde tvoří pouze jeden z parametrů biometrické stopy).

Důležitým atributem dynamického biometrického podpisu je, že již sám v sobě obsahuje nejen prvek „živosti" objektu (pisatele), ale i skutečnost, že podpis vytvořil pisatel vědomě, takže není potřeba vyvíjet další mechanismy testující, zda objekt je živý či nikoliv rozdíl od statických biometrických metod (kontrola otisku prstů, dlaně, oka apod.). Můžeme také vycházet z vyvratitelného předpokladu, že osoba věděla, co podepisovala.

Verifikace osoby na základě jejího podpisu je jedna z nejpřirozenějších biometrických metod, protože jsme dennodenně zvyklí cokoliv stvrzovat naším podpisem.

V kapitole jsou uvedeny základy kryptografie. Je vysvětlen pojem kryptografický algoritmus a uvedeny jeho základní typy. Jsou zde popsány blokové a proudové šifry. Jsou popsány i hlavní představitelé symetrických a asymetrických algoritmů – DES, AES a RSA. Je zde uveden princip elektronického podpisu a jeho alternativy dynamického biometrického podpisu.

1. Co znamenají pojmy kryptografie, šifrování, šifrovací algoritmus?
2. Popište blokové kryptografické algoritmy a uveďte jejich odlišnost od proudových kryptografických algoritmů.
3. Popište princip symetrického kryptografického algoritmu.
4. Popište princip asymetrického kryptografického algoritmu.
5. Popište schéma DES, AES.
6. Popište princip RSA.
7. Co znamená pojem elektronický podpis?
8. Co znamená pojem dynamický biometrický podpis?

Literatura k tématu:

[1] http://www.tutorialspoint.com

[2] SMEJKAL, V., KODL, J., Uřičař, M. *Elektronický podpis podle nařízení eIDAS. Revue pro právo a technologie*, VI., 2015, č. 11, s. 189–235. ISSN 1804-5383 (Print), ISSN 1805-2797 (Online)

[3] CLARK, David Leon. *Enterprise Security: A Manager's Defense Guide*. 1st. ed. Boston: Addison-Wesley Longman Publishing Co., Inc., 2002. 288 s. ISBN 978-02-017-1972-7.

[4] MENEZES, Alfred, Paul C. Van OORSCHOT a Scott A. VANSTONE. *Handbook of Applied Cryptography. Rev. repr. with updates.* Boca Raton: CRC Press, 1997. 780 s. ISBN 0-8493-8523-7.

[1] SCHNEIER, Bruce. *Applied Cryptography,* Second Edition: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons, 1996. 758. ISBN 0471117099

Kapitola 10

Listiny a elektronické dokumenty

Po prostudování kapitoly budete umět:

- definovat pojem elektronický dokument;
- popsat základní principy při ochraně elektronických dokumentů;
- vysvětlit požadavky nařízení eIDAS.

Klíčová slova:

Listina, dokument, elektronický dokument.

10.1 Definování základných pojmů

10.1.1 Základní pojmy

Dokument
Je jím každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena svým původcem nebo byla původci doručena.

Listina
Dokument vesměs v papírové podobě.

Elektronický dokument (ED)
Definice: Digitálně zpracovaný dokument, který je možno zpracovávat pomocí elektronických prostředků.

10.2 Ochrana elektronických dokumentů

Elektronické originály dokumentů dnes představují rovnocennou náhradu listin, kterou je možné archivovat po neomezeně dlouhou dobu. Základem právní úpravy nakládání s elektronickými originály dokumentů, se stalo zajištění jejich věrohodnosti, neporušitelnost a čitelnost. Toto bylo umožněno nejen pokrokem na poli technologií, ale zejména na poli potřebné legislativy, která umožnila využití technologického pokroku, který byl v této oblasti učiněn.

Elektronizace business procesů jednoznačně zařadila do stávajících procesů výpočetní techniku. S tím pak souvisí i skutečnost, že pracovní dokumenty jsou již vytvářeny, přenášeny uchovávány v elektronické podobě. Dnes již platná legislativa staví naroveň elektronický dokument, který má platnost originálu a může se s ním zacházet jako s tradičním dokumentem v listinné podobě (tedy v současné době vesměs s papírovým dokumentem).

Problematiku práce s elektronickými dokumenty podporuje i stávající legislativa, která umožnuje řešit požadavky na důvěryhodnost elektronických dokumentů, tj. dokumentovat:

- Autentičnost – věrohodnost původu
- Integritu – neporušenost obsahu
- Dostupnost – čitelnost
- Důvěrnost – v případě citlivých informací

Současně byla díky výše uvedené novelizaci patřičné legislativy zavedena celá sada referenčních norem AdES vydaných Evropským institutem pro standardy v telekomunikacích ETSI, které stanovily požadavky na formáty zpracovávaných elektronických dokumentů (PAdES, XAdES, CAdES).

Z pohledu zabezpečení těchto dokumentů vyvstaly nové úkoly a agendy pro podnikové bezpečnostní útvary, které musely své činnosti rozšířit ze zajišťování fyzické bezpečnosti do problematiky bezpečnosti IT. S tím souvisí zavedení správy přístupových práv,

Přístupová práva musí být v souladu s činností jednotlivých uživatelů informačních systémů, resp. povinnostmi a pravomocemi v jednotlivých pracovních agendách. Přistupuje zde i nový požadavek na zařazení uživatelů do určité typové autorizační skupiny, kde jednotliví pracovníci ve skupině mají stejná práva, přičemž musí být řešena otázka možné anonymity.

Zpracování systému přidělování práv se dostává z organizační roviny, resp. administrativní bezpečnosti jednoznačně do bezpečnosti IT, která je spojena s:

- založením uživatele;
- založením a aktivací autorizace;
- přiřazení autorizace uživatelům apod.

V předchozích kapitolách již byly probrány nástroje a metody zabezpečení elektronických dokumentů tj.:

- autentizace;
- elektronický podpis;
- DBP;
- elektronická pečeť a časové razítko.

10.3 Nařízení eIDAS

Cílem zákona o službách vytvářejících důvěru pro elektronické transakce je adaptace právního řádu České republiky na přijetí nařízení eIDAS pro oblast služeb vytvářejících důvěru. V zákoně je upraveno pouze to, co nařízení výslovně nechává na úpravu vnitrostátním právním řádem. Úprava obsažená v zákoně proto zejména stanoví některé postupy poskytovatelů služeb vytvářejících důvěru a požadavky na služby vytvářející důvěru a pravidla elektronického podepisování, elektronického pečetění a opatřování dokumentů elektronickými časovými razítky. Zákon rovněž stanovuje Ministerstvo vnitra jako orgán dohledu nad poskytovateli služeb vytvářejících důvěru. V zákoně není upravena elektronická identifikace, která bude řešena samostatně.

Cílem předkládaného změnového zákona je reflektovat změny, které přináší nařízení eIDAS, případně i kmenový zákon – zákon o službách vytvářejících důvěru pro elektronické transakce, v příslušných zvláštních zákonech. Změnový zákon obsahuje také novelu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a novelu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Novely těchto zákonů byly připraveny v souvislosti s plněním úkolu, stanoveného Ministerstvu vnitra na základě plánu legislativních prací na rok 2015 a Akčního plánu České republiky Partnerství pro otevřené vládnutí na období let 2014 až 2016 stanovit jednotící pravidla pro poskytování informací povinnými subjekty ve formě otevřených dat.

Ministerstvo vnitra plní úkoly orgánu dohledu podle nařízení eIDAS a dále podle zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce. Zpracovává také návrhy právních předpisů týkajících se elektronického podpisu a v jeho působnosti je rovněž zajištění mezinárodní spolupráce v této oblasti a plnění úkolů plynoucích z členství ČR v mezinárodních organizacích.

V kapitole je projednána problematika elektronických dokumentů, popsán princip jejich zabezpečování během jejich celého životního cyklu. Je zde také zmíněno nařízení eIDAS a jeho určení.

1. Definujte pojmy dokument, listina, elektronický dokument.
2. V čem spočívá ochrana elektronických dokumentů?
3. Jaké jsou požadavky nařízení eIDAS?

Literatura k tématu:

[1] SMEJKAL, V., KODL, J., UŘIČAŘ, M. *Elektronický podpis podle nařízení eIDAS. Revue pro právo a technologie*, VI., 2015, č. 11, s. 189–235. ISSN 1804-5383 (Print), ISSN 1805-2797 (Online).

[2] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.

Kapitola 11

Zálohování

Po prostudování kapitoly budete umět:

- popsat smysl, důvod a účel tvorby zálohovacích systémů;
- vysvětlit rozdíly mezi zálohováním a uložením (dlouhodobým uložením) dat;
- vysvětlit architekturu RAID a účel využívání systémů RAID;
- uvést technologické prostředky používané při zálohování a ukládání dat;
- uvést základní požadavky při zabezpečení uložených citlivých dat;
- popsat proces při řízení kontinuity business procesů.

Klíčová slova:

RAID, zálohování, ukládaní, BCP, DRP havarijní plány.

11.1 Úvod

Většinou problematiku zálohování dat vnímáme jako ad hoc vytváření kopií dat na samostatný datový nosič pro případ ztráty v původním úložišti. Tento přístup lze aplikovat při správě dat na osobním počítači.

V případě informačních systémů a tím více podnikových informačních systémů musí být řešení záloh komplexní a systém záloh musí zejména zajistit

- aktuálnost záložních dat
- operativnost a dostupnost při práci se zálohami
- zabezpečení integrity a autentičnosti zálohovaných dat (v případě citlivých dat i důvěrnost)
- oprávnění přístupu

Zálohování dat musí být řešeno proaktivně a systémy zálohování musí být nedílnou součástí procesů v informačních systémech.

Zálohování dat je úzce propojeno se systémy ukládání (dlouhodobého ukládání) dat. Z tohoto pohledu je také třeba při návrhu systému zálohu tak přistupovat. Zejména u velkých informačních systémů může způsobit kolaps, neboť zpracovávané informace mohou být ztraceny:

- neúmyslnou nebo úmyslnou chybou člověka – člověk může soubory omylem smazat, přepsat, vyvolat chybu programu pro manipulaci s uloženými daty,
- chybou operačního systému – operační systém může svojí chybou způsobit přepsání některé důležité části média,
- přírodní pohromou – povodeň,
- škodlivým SW,
- zničením médií.

11.2 Architektura záložních systémů, návrh RAID

Zálohování na FTP server Zálohování na FTP (File Transfer Protocol) server poskytuje bezpečný způsob ukládání, vzhledem k možnosti uložení dat na zcela oddělené místo od zdrojových dat. Tento

způsob zálohování má však nízkou úroveň zabezpečení ukládaných dat, vzhledem k hrozbám manipulace s těmito daty během přenosu.

Online zálohování. Jedná se o metodu nahrávání dat přes internet do externího úložiště s pomocí zálohovacího softwaru od poskytovatele online služby. Soubory jsou kdykoliv k dispozici a můžeme je opět obnovit a použít.

Hlavní **výhodou** je uložení dat v jiné lokalitě, čímž je zajištěna vyšší ochrana dat proti možnému zničení záloh v důsledku požáru, povodní a jiných živelných pohrom. situací. **Nevýhody** spočívají v nutnost vysokorychlostní komunikace a delší doba uložení velkých objemů dat. připojení k internetu a delší doba nahrávání většího objemu dat. Další nevýhodou je možnost neoprávněného přístupu k datům třetí osobou., čemuž je nutné se bránit zašifrováním přenášených dat.

Software – základní podmínkou při návrhu systému zálohovaní je možnost pravidelného zálohování, tj. nutné zajistit v pravidelných intervalech ukládání záložní kopie.

Technologie RAID. Pro vytvoření záloh lze použít i RAID, což je zkratka z anglického Redundant Array of Independent Disks, (vícenásobné diskové pole nezávislých disků). Jedná se o metodu zabezpečení dat proti selhání pevného disku, na kterém jsou ukládána data. Metoda spočívá v ukládání dat na více nezávislých discích, které jsou propojeny tak, že ukládaná data jsou v případě selhání jednoho z nich zachována.

11.3 Systém zálohování dat

Způsoby zálohování a výběr vhodného typu vytváření záloh je závislá na mnoha aspektech.

Volba systému zálohování musí vycházet z výsledků analýzy, a to v některých případech i provedené analýzy rizik. Zvolený systém zálohování, který je často spojen i se systémem ukládání dat, takže při volbě způsobu, metody a systému zálohování je třeba zvážit:

- Objem zálohovaných dat.
- Charakter zálohovaných dat (citlivá, publikovatelná, systémová aj.).
- Frekvence a aktualizace zálohovaných dar.
- Offline nebo online zálohování.

Po vymezení požadavků na zálohování je třeba zajistit příslušný SW, HW, který bude schopen zálohovat požadovaná data. V případě zálohování dat lze využít:

Technologické prostředky

Páskové mechaniky. Pro zálohování velkého množství dat v informačních systémech lze použít páskové mechaniky. Tyto prostředky jsou též využívané a doporučované pro dlouhodobé ukládání dat. Provedené testy prokázaly, že digitální záznam na páskovém médiu vydrží minimálně 20 let.

REV mechaniky. REV mechanika je zálohovací systém, který využívá k zálohování výměnné pevné disky umístěné ve speciálních kazetách. Disky jsou vybaveny dvouúrovňovou ECC kontrolou chyb. Provedené testy prokázaly minimální dobu, po kterou jsou REV mechaniky schopny uchovat data na 30 let.

Zálohování a dlouhodobé uložení citlivých dat

Zálohování a dlouhodobé ukládání citlivých dat vyžaduje realizaci zabezpečeného úložiště, kde je třeba zaručit zachování integrity dat a jejich důvěrnosti a dostupnosti.

Nastavená bezpečnostní opatření ve vztahu k ochraně dat musí podléhat požadavkům stanoveným v bezpečnostních normách ČSN ISO/IES řady 27000, v případě technologického řešení pak normě ČSN ISO/IEC 15408. Tyto požadavky musí být podloženy výsledky zpracované analýzy rizik a dokumentovány vnitřními směrnicemi.

V případě dlouhodobého ukládání dat, musí být data převáděna do odpovídajících formátů.

Například elektronické dokumenty se do úložiště ukládají ve formátu PDF/A, který umožňuje integraci dat při ověřování integrity využívající elektronické podpisy.

Vzhledem ke kontinuální kontrole integrity elektronického dokumentu musí v úložišti integrovány funkcionality automatizované kontroly integrity.

Celý systémový přístup, resp. mechanismy zajištění bezpečnosti ukládaných dat musí zaručit, že v případě uložení dat do tohoto úložiště nemůže dojít k jejich ohrožení či poškození (k narušení integrity nebo k úplnému zničení).

11.4 Nastavení kontinuity procesů podnikového informačního systému

Při zabezpečení provozu informačního systému je důležitým aspektem postihnout i případy nestandardních situací. Je nutné počítat s možnými havarijními situacemi, kdy podnikový informační systém může zajišťovat pouze částečný provoz nebo být úplně mimo provoz, čímž jsou narušeny i business procesy podniku. Vzhledem k tomu, že jedním z nejdůležitějších parametrů zpracovávaných da je jejich dostupnost, je třeba mít připraveny procesy, zajistí kontinuitu informačních technologií.

BCP (Business Continuity Plan – plán kontinuity činností). Pro případ jakékoliv havárie musí mít podnik vypracovaný řídící proces, který v případě identifikace nestandardní situace, vyhodnotí možné dopady a aktivuje takové postupy a opatření, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností podniku na minimální úroveň činností, které zajistí kontinuální zajištění business aktivit.

Pro jednotný přístup k řešení této problematiky je třeba vycházet z doporučení bezpečnostních norem ČSN ISO/IEC řady 27000.

DRP (Disaster Recovery Plan – plán obnovy po havárii). Lze říci, že DRP je podmnožinou BCP, neboť zpracované procesy směřují přímo k obnově činnosti technologických prostředků. Jedná se opravu, či výměnu technologických komponent – HW i SW i využití náhradních zdrojů. Zde je nutné zdůraznit, že nelze na úkor rychlé obnovy technologického parku snížit úroveň ochrany zpracovávaných informací. Z tohoto důvodu jsou proces DRP posuzovány v rámci analýzy rizik.

11.5 Havarijní plány

Havarijní plán musí postihnout celé spektrum činností (od organizační struktury havarijního výboru až po činnosti realizované v rámci DRP). Hlavním cílem zpracovaného havarijního plánu je, na základě zjištěných skutečností, nastavit priority činnosti, které je třeba řešit k zajištění minimalizace ztrát. Z tohoto důvodu jsou v rámci zpracování havarijního plánu připraveny různé scénáře, které mohou pokrýt případy s největší pravděpodobností výskytu. Bezprostředně na havarijní plán navazuje plán obnovy.

V kapitole je rozebrán smysl, důvod a účel tvorby zálohovacích systémů. Je zde uvedena architektura zálohovacích systémů. Jsou zde nastíněny rozdíly mezi zálohováním a uložením (dlouhodobým uložením) dat a uvedeny technologické prostředky používané při zálohování a ukládání dat. Samostatnou část tvoří realizace požadavků při zabezpečení uložených citlivých dat. Je zde vysvětlena architektura RAID a účel využívání systémů RAID. Závěrečnou část kapitoly tvoří popis způsobů řízení kontinuity business procesů v nestandardních situacích.

1. Popište architekturu využívaných záložních systémů.
2. Co znamená pojem RAID?
3. Vysvětlete rozdíly mezi DRP, BCP a havarijním plánem.
4. Co je třeba zajistit při uložení citlivých dat?

Literatura k tématu:

[1] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.

Kapitola 12

Kybernetická kriminalita

Po prostudování kapitoly budete umět:

- definovat pojem kriminalita, kybernetická kriminalita,
- vysvětlit vybrané skutkové podstaty uvedené v trestním zákoníku.

Klíčová slova:

Kriminalita, počítačová kriminalita.

Kriminalita, nazývaná nejdříve počítačová, nyní pak nově kybernetická kopíruje technické vlastnosti i uživatelské možnosti počítačů, počítačových sítí, resp. celého kyberprostoru. Ze všeho nejdříve se počítače staly předmětem klasických kriminálních útoků, směřujících proti nim coby věcem movitým – krádeže, poškozování cizí věci atd., dále pak se jednání pachatelů posunulo směrem k neoprávněnému užívání. Následovaly útoky na data počítači zpracovávaná, a přes podvody jsme se dostali k dnešnímu stavu, kdy skutkových podstat spojených s počítači a počítačovými sítěmi nalezneme v současném trestním zákoníku mnoho a kdy variabilita jednání pachatelů v kyberprostoru je značná a neustále se rozšiřuje.

Označení „počítačová kriminalita“ má obdobný charakter jako pojmy „násilná kriminalita“, „kriminalita mladistvých“ apod. Takovýmito názvy jsou označovány skupiny trestných činů, mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty). Přitom ale – na rozdíl od jiných kategorií trestné činnosti – dlouho neexistovala jasná shoda v tom, co počítačovou kriminalitou je. Diskuse, která proběhla u nás v devadesátých letech, se přiklonila k názoru poprvé publikovaném kolektivem Smejkal, Sokol, Vlček[7], že pod pojmem „počítačová kriminalita“ je třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,
b) nebo jako nástroj trestné činnosti.

Počítač může být předmětem trestného činu; současně je ale také ke spáchání celé řady trestných činů ideálním prostředkem. Vzhledem k mnoha jeho vlastnostem, jakými jsou především:

- složitost principů, na nichž pracuje a nejednoduchost jeho ovládání;
- nakládání s informacemi, jež jsou nehmotné, přičemž mohou reprezentovat vysoké peněžní hodnoty nebo představovat citlivé osobní či ekonomické údaje;
- možnost jednoduchého skrývání a zahlazování těchto nehmotných stop;
- dostupnost prostředků pro utajování obsahu informací (šifrováním, přístupovými mechanismy – hesly, kartami, otisky prstů apod.);
- uplatnění distančního přístupu v prostředí počítačových sítí a elektronických komunikací, umožňující páchat trestnou činnost na dálku,

[7] Smejkal, V., Sokol, T., Vlček, M., *Počítačové právo*. Praha: C. H. Beck, 1995, s. 99.

je z hlediska páchání trestné činnosti používání počítačů pro pachatele vysoce přínosným.

Prvními trestnými činy zaměřenými na počítače, ať už si je představíme v jakékoliv podobě, byly sabotáže, které byly různě motivované – politicky i mstou zaměstnavateli.[8]

Velice brzy si ale uživatelé, kteří ani neměli přímý přístup k počítači, tehdy se nacházejícímu v klimatizovaných sálech pod dohledem vysoce kvalifikovaných specialistů, uvědomili další možnosti. Objevily se tzv. dokladové delikty, kdy stejným způsobem, jako měnili a falšovali údaje v běžných „papírových“ dokladech, začali zločinci měnit podklady připravené ke zpracování do počítače. Jednalo se o nejčastější odhalený počítačový zločin, jehož podstatou byly manipulace v mzdových účtárnách, zásobování, odbytech a na jiných pracovištích, kde pracovník měl možnost manipulovat s penězi (ať už v hotovosti nebo přes čísla účtů) či zbožím. Dnes jsou skutky tohoto typu obvykle kvalifikovány jako podvod podle § 209 trestního zákoníku obvykle v souběhu s trestným činem podle § 230 Neoprávněný přístup k počítačovému systému a nosiči informací.

Sjednocujícím kritériem takovýchto jednání je vždy více méně o využití něčího omylu ve svůj prospěch, přičemž v souvislosti s informačními systémy zde hraje nezanedbatelnou roli složitost problematiky a psychologická stránka věci. Na rozdíl od klasických manipulací s „papírovými“ doklady má manipulace s počítačovými daty pro pachatele několik výhod:

1. vymazání či přemazání údaje na magnetickém médiu je podstatně snazší a nezanechává prakticky žádné stopy;
2. člověk (zaměstnanec, auditor, zákazník apod.) z psychologického hlediska považuje výsledky z počítače za a priori správné a více jim (byť podvědomě) důvěřuje;
3. systém zpracování dat je natolik složitý, že málokdo má přehled o všech aspektech, procedurách, postupech a mechanismech, jež jsou používány a kontrola toho, co se odehrává ve výpočetním systému, je velmi obtížná;
4. objem zpracovaných, resp. přenášených dat je velmi velký;
5. zjištění stavu informačního systému v určitém, mnohdy časově vzdáleném okamžiku a prokázání odpovědnosti určité osoby za provedení operací v tomto IS je obtížné, ne-li nemožné;
6. lehkost provádění operací s počítačovými daty oproti reálnému životu; ukrást někomu z kapsy peněženku je výrazně obtížnější než napsat příkazový řádek na počítači – alespoň pro kvalifikovaného programátora;
7. morální aspekty jsou ve virtuálním světě poněkud potlačeny – daleko snadněji lze spáchat trestný čin kliknutím myši nežli namáhavým jednáním v reálném světě.

[8] Smejkal, V. a kol., *Právo informačních a telekomunikačních systémů*. 2. vydání. Praha, C. H. Beck, 2004, s. 703.

Tyto aspekty počítačové kriminality mají za následek vysokou úspěšnost trestných činů páchaných za využití výpočetní techniky. Právě značná důvěryhodnost výstupů z počítače, aniž bychom mnohdy byli schopni zjistit, jak se k těmto výstupům dospělo, je základním předpokladem úspěšného podvodu v prostředí informačních systémů.

Kromě toho se zde objevuje další aspekt podmiňující úspěchy počítačových zločinců, kterým je vysoká kvalifikace pachatelů tohoto druhu trestné činnosti. Ta se projevuje ve vysoké latenci tohoto druhu kriminality, neboť pachatelé mají daleko větší předpoklady k tomu, aby se vůbec nepodařilo spáchání trestného činu zjistit, případně aby se nepodařilo zjistit, kdo je pachatelem, a jak jsme se s tím již v nejednom případě setkali – aby nebylo podezřelému možno jeho trestnou činnost dokázat.

Teprve další dva technologické zlomy v oblasti počítačových systémů umožnily jejich hromadné využívání, a tudíž i neméně masivní trestnou činnost s počítači spojenou. Nová doba počítačového zločinu se datuje dvěma zásadními momenty:

1. nástupem osobních počítačů,
2. vznikem počítačových sítí a vzdáleného přístupu k počítačům, zejména prostřednictvím Internetu.
   K těmto dvěma faktorům musíme připojit ještě třetí, a to:
3. exponenciální růst možností mobilní telefonie a tomu odpovídající vybavenost občanů, včetně využívání anonymních, tzv. předplacených karet.

V rámci distančního přístupu prostřednictvím Internetu byly klasické podvody podle ust. § 209 TrZ zdokonaleny pomocí počítačů, případně se objevily zcela nové druhy podvodů – phishing, pharming apod.[9]

Dalšími delikty, které se objevily jako součást počítačové kriminality, byly a stále jsou:

a) padělky dokumentů, zhotovené pomocí moderních digitálních technologií;
b) padělky nosičů informací především v podobě různých karet obsahujících nosič dat – telefonních, kreditních (úvěrových), debetních (platebních), vstupních apod.

Nedlouho po masovém rozšíření počítačů a Internetu u nás se porušování autorských práv stalo takřka synonymem pro užívání počítačů. Nelegální užívání počítačů – hardware – bylo rychle dohnáno a předehnáno nelegálním užíváním software. Uvědomění si samotné existence nehmotných statků je spojeno až s pozdější dobou zhruba od poloviny devadesátých let, kdy se duševní vlastnictví ob-

[9] Smejkal, V., *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 137 a násl.

jevuje jako nehmotný majetek v obchodním majetku společností, v daňových zákonech, v novelizovaných zákonech na ochranu duševního vlastnictví a jako předmět obchodních vztahů i soudních sporů. Od té doby je ochraně práv autorských, průmyslových a práv jim podobných věnována stále větší pozornost (mj. i v důsledku intenzivnějších mezinárodních hospodářských vztahů). Dva druhy duševního vlastnictví – oba spadající pod ochranu autorským zákonem – se staly velice rychle masivním předmětem útoku zločinců: audiovizuální nahrávky a počítačové programy, později i databáze. Přitom většina počítačových programů a řada databází požívá ochrany podle autorského zákona, neboť podle § 2 odst. 2 AutZ se za dílo považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Za dílo souborné se považuje databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem.

Nelegální užívání software prošlo intenzívním nárůstem, kdy se hovořilo až o 80% nelegálně užívaného programového vybavení v České republice. Současná situace není tak dramatická a s rostoucími možnostmi zveřejňování audiových a audiovizuálních děl a jejich šíření prostřednictvím úložišť na Internetu se těžiště tr. činnosti podle § 270 stávajícího TrZ (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi) od software přesunulo k těmto dílům, případě ke zveřejňování děl literárních, zejména odborných nebo mimořádně populární beletrie obdobným způsobem[10].

S tím, jak stále více údajů je uloženo na magnetických médiích, roste zájem zločinců o obsah těchto nosičů informací. Těžiště jejich zájmu představují dnes zejména dvě oblasti:

a) osobní údaje občanů;
b) politicky nebo hospodářsky využitelné údaje (vyzvědačství a průmyslová špionáž).

Na přelomu let 1991–1992 došlo k velmi žádoucímu zařazení některých nových skutkových podstat do tehdejšího trestního zákona č. 140/1961 Sb., a to včetně skutkových podstat souvisejících s počítačovou kriminalitou. Jsou to ustanovení § 257a – Poškození a zneužití záznamu na nosiči informací a § 178 – Neoprávněné nakládání s osobními údaji.[11] Bylo to velmi prorocké, protože všechny tyto trestné činy doznaly značného rozšíření. Zejména pak neoprávněné nakládání s osobními údaji, podle stávající trestní úpravy pak § 180 tehdejšího TrZ.

Již v době platnosti předchozího tr. zákona se ale objevila další jednání, s nimiž si právní řád, a to nejen český, nevěděl příliš rady. Byly to zejména:

[10] Telec, I., *Zakázané těžení a nebezpečná situace na elektronických úložištích dat*, 2015, č. 1–2, s. 19–29; Smejkal, V., *Kybernetická kriminalita*, 2015, s. 352 a násl.

[11] Smejkal, V. a kol., *Právo informačních a telekomunikačních systémů*, 2. vydání. Praha, C. H. Beck, 2004, s. 730 a násl.

1. Obtěžování, které právě v souvislosti s ICT nabylo hrozivých rozměrů. K obtěžování dochází jednak formou elektronické pošty (e-mailů), jednak zasílám zpráv přes Internet (ICQ, chat, sociální sítě) nebo prostřednictvím mobilních telefonů (SMS), ale vyskytuje se i obtěžování formou klasických telefonických hovorů, faxů nebo různými zásilkami.
2. Tzv. hromadné útoky DoS, DDoS.[12]
3. Ještě problematičtější byl postih neoprávněného užívání počítače dálkovým způsobem, neboť podle ust. § 249 neoprávněné užívání cizí věci se předpokládalo, že se pachatel „zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu jich přechodně užívat, nebo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takových věcí, které mu byly svěřeny, přechodně užívá“. Ani jedna skutková podstata se na variantu pachatele, připojeného ze svého osobního počítače v místě A k cizímu počítači v místě B plně nehodila.
4. S tím souvisela i možnost postihu pachatele, který pronikl do cizího počítače, aniž by jakkoliv poškodil či zničil údaje, v něm uložené. Pokud se hacker dostane do počítače a „koukne se“ na data v něm uložená, aniž by je následně využil (sdělil, okopíroval, zpracoval atd.), nelze hovořit o užití, a tudíž by pravděpodobně nedošlo k naplnění skutkové podstaty ust. § 257a písm. a).
5. Jelikož delikt podle § 257a neznal nedbalostní kvalifikaci, nebylo zřejmě jednoduše a podle tohoto ustanovení možné stíhat např. zaměstnance, který vložil zavirovanou disketu do počítačového systému svého zaměstnavatele, čímž došlo k vymazání obsahu pevného disku, neboť lze podle ust. § 257a stíhat pouze ty osoby, u nichž by úmysl byl prokázán.

Dne 23. 11. 2001 byla publikována Úmluva Rady Evropy o počítačové kriminalitě (dále jen Úmluva), která vstoupila v platnost 1. 7. 2004.756 Česká republika tuto Úmluvu podepsala v roce 2005, zohlednila ji v přípravě nového trestního zákoníku, leč ratifikovala až v 23. 8. 2013 s účinností od 1. 12. 2013.757 Celkově Úmluvu ratifikovalo 41 států z celého světa, dalších 12 ji zatím pouze podepsalo. Úmluva je poměrně dobrým základem pro postihování trestné činnosti v počítačových sítích, zejména na Internetu, neboť se kromě definování skutkových podstat zabývá i otázkami jurisdikcí a mezinárodní spolupráce[13].

Kromě deliktů ve vztahu k počítačovým systémům a počítačovým datům jsou do této kategorie podle Úmluvy řazeny i delikty páchané pomocí počítačů snadněji, a tudíž častěji a pravděpodobně s vyšší společenskou nebezpečností (typicky trestné činy související s dětskou pornografií nebo porušování autorského práva).

[12] Smejkal, V. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015, s. 534 a násl.

[13] Viz např. Gřivna, T.; Polčák, R. a kol., *Kyberkriminalita a právo*, 2008, s. 162 a násl.

Na jejím základě byly formulovány „počítačové“ skutkové podstaty v současném trestním zákoníku, zákonu č. 40/2009 Sb. ve znění pozdějších předpisů, a to:

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Nová právní úprava je rozsáhlejší, pokud jde o popis postihovaných aktivit. Nadto se z původního jednoho ustanovení § 257a předchozího TrZ stala dvě ustanovení. Ustanovení § 230 postihující neoprávněný přístup k počítačovému systému a nosiči informací a § 231, který postihuje opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Přibyl i postih nedbalostního jednání podle § 232.

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat je definováno v ust. § 231 tak, že podle odst. 1 „*Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává*

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

b*ude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.*“. Detailní rozbor viz literatura. [14]

Ustanovení § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti nenalezneme v Úmluvě, ale bylo zařazeno na základě požadavků z praxe a poznatků orgánů činných v trestním řízení. U některých pachatelů bylo obtížné prokázat úmyslné jednání, přestože – vzhledem ke svému zaměstnání, postavení či funkci muselo být zřejmé, že svým jednáním způsobí škodu či jinou újmu a z kontextu vyplývalo, že si tohoto následku musel být plně

[14] Smejkal, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 411 a násl.

vědom. Rovněž zhojení se na hrubě nedbalém zaměstnanci, který svým jednáním spojeným s počítačem způsobil mnohamiliónovou škodu či mohl ohrozit samu existenci organizace, naráželo na limity dané zákoníkem práce[15].

Úmysl zákonodárců směřuje k ochraně majetku hrubě nedbalým jednáním osob, které doposud nepožívalo ochrany v rámci trestního práva a bylo je nutno řešit výlučně soukromoprávními prostředky. Důvodem je možnost značného ohrožení při nedbalém nakládání s počítačovými systémy, které dnes řídí výrobu, obchod, finance, ale i letový provoz nebo jednotky intenzivní péče, tedy kdy na jejich bezchybném provozu závisí majetek, zdraví i životy osob.

Trestnou činnost spojenou s počítačovými sítěmi a zejména s Internetem můžeme rozdělit do dvou základních kategorií:

1. zpřístupňování informací, které mohou někomu způsobit újmu nebo založit spáchání trestného činu nebo naopak shromažďování informací za účelem jejich pozdějšího nelegálního využití – neboli informační trestná činnost, neboť tato může být páchána i bez pomoci počítačů, byť značně obtížněji;
2. páchání trestné činnosti v kyberprostoru, a to takové činnosti, kterou lze páchat díky vlastnostem počítačů a počítačových sítí a jejich komponent (hardware, software, dat).

Do první oblasti ad a) lze zařadit zejména § 180 Neoprávněné nakládání s osobními údaji, § 316 Vyzvědačství, § 317 Ohrožení utajované informace, § 318 Ohrožení utajované informace z nedbalosti. Povaha Internetu jakožto prostředku, jehož prostřednictvím lze veřejně šířit informace, je významná v oblasti trestněprávní, konkrétně tam, kde se jedná o trestné činy, u nichž je veřejnost jejich znakem (např. § 184 Pomluva, § 191 Šíření pornografie, § 192 Výroba a jiné nakládání s dětskou pornografií, § 250 Manipulace s kurzem investičních nástrojů, § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, § 352 Násilí proti skupině obyvatelů a proti jednotlivci, § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, § 357 Šíření poplašné zprávy, § 364 Podněcování k trestnému činu, § 365 Schvalování trestného činu, § 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka, § 404 Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, § 405 Popírání, zpochybňování, schvalování a ospravedlňování genocidia).

Páchání trestné činnosti v kyberprostoru jiné, nežli byla popsána výše, zahrnuje zejména různé druhy útoků na zařízení ICT, a to formou kyberterorizmu, vyvoláním stavu obecné ohrožení podle §

[15] Šámal, P. a kol., *Trestní zákoník II. § 140 až 421. Komentář*, 2012, s. 2320.

272–273, poškozením a ohrožením provozu obecně prospěšného zařízení podle § 276–277, poškozováním cizích věcí podle ust. § 228 TrZ a neoprávněným užíváním cizí věci podle § 207 TrZ. V poslední době se rozmáhá vydírání v prostředí ICT, které započalo pohrůžkami o zveřejnění osobních údajů a končí zaplacením „výpalného“ za odšifrování disků s daty, tzv. ransomware.[16]

Mezi ostatní trestné činy související s počítači můžeme zařadit ještě Neoprávněné opatření, padělání a pozměnění platebního prostředku, zejména platebních karet, resp. údajů z nich (§ 234), Výroba a držení padělatelského náčiní (§ 236) tvořeného prostředky ICT, případně padělání a pozměnění veřejné listiny (§ 348). Detailní rozbor kybernetické trestné činnosti viz literatura. [17]

V blízké budoucnosti můžeme počítat s trestnou činností související s virtuálními světy (vytvořenými v kyberprostoru), která bude zaměřena na virtuální vlastnictví a virtuální majetek, včetně tzv. virtuálních měn, jako jsou např. bitcoiny. Bude docházet k prolínání klasické kriminality ve vztahu k virtuálnímu prostoru a naopak. Také nové technologické fenomény, jako např. 3D tisk, „chytré šaty“ a šperky, monitorující životní pochody nositelů, létající roboti – drony či mikrominiaturní roboti budou představovat nejen přínos pro lidstvo, ale i rostoucí bezpečnostní rizika. Čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme počítat. Proto trend IoT (Internet věcí) představuje extrémní hrozbu z hlediska kybernetické kriminality. Další velmi významnou oblastí je využívání trestné činnosti v kyberprostoru k páchání kybernetického terorizmu, útočícího na informační systémy sátu, klíčových podniků a poskytovatelů služeb obyvatelstvu včetně síťových služeb (telekomunikace, dodávky energie, vody apod.).

V kapitole je popsána problematika počítačové, resp. kybernetické kriminality. Jsou zde definovány skutkové podstaty těch trestných činů podle platného trestního zákoníku, které souvisejí s počítači a kyberprostorem. Závěrečnou část kapitoly tvoří prognóza dalšího vývoje kybernetické kriminality.

1. Jaký je rozdíl mezi počítačovou a kybernetickou kriminalitou?
2. Které jsou „počítačové“ skutkové podstaty v současném trestním zákoníku?
3. Podle jakého ustanovení trestního zákoníku jsou chráněny osobní údaje občanů?
4. Proč představuje Internet věcí vysokou hrozbu z hlediska kybernetické kriminality?

[16] Smejkal, V., *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 147 a násl.

[17] Smejkal, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015.

Literatura k tématu:

[1] SMEJKAL, V. *Kybernetická kriminalita*. 1. vyd. Plzeň: Aleš Čeněk, 2015. 640 s. ISBN 978-80-738-0501-2

[2] SMEJKAL, V. *Práva k počítačovým programům a databázím*. In: SRSTKA, Jiří a kol. *Autorské právo a práva související. Vysokoškolská učebnice.* Praha: Leges, 2017, s. 198-224. ISBN: 978-80-7502-240-0.

[3] TELEC, I., *Zakázané těžení a nebezpečná situace na elektronických úložištích dat*. *Bulletin advokacie*, 2015, č. 1–2, s. 19–29. ISSN 1210-6348.

[4] SMEJKAL, V. *Metodika vyšetřování kybernetické kriminality*. In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty*. 1. vydání. Plzeň: Aleš Čeněk, 2016, s. 786–802. ISBN 978-80-7380-589-0.

[5] SMEJKAL, V. *Metodika vyšetřování softwarového pirátství.* In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty*. 1. vydání. Plzeň: Aleš Čeněk, 2016, s. 803–824. ISBN 978-80-7380-589-0.

[6] JELÍNEK, J. a kol. *Terorismus – základní otázky trestního práva a kriminologie*. Praha: Leges, 2018, 224 str. ISBN978-80-7502-256-1.