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.

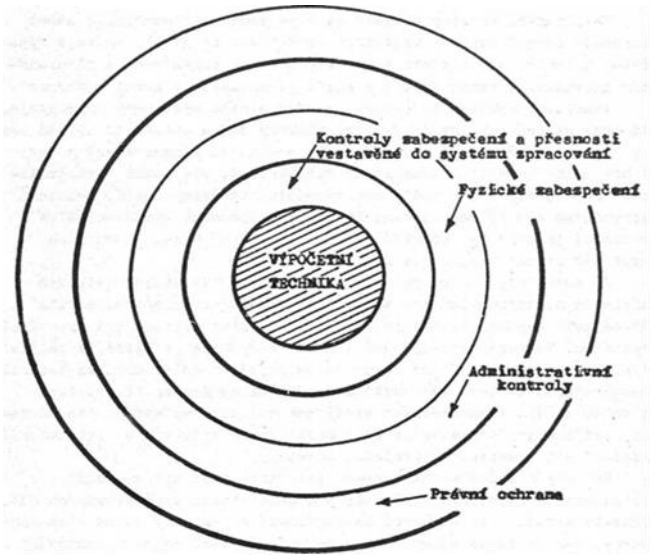
Tato kapitola obsahuje vymezení základních pojmů a zásad, které se vztahují k bezpečnosti informací a zkoumá základní součásti systému zabezpečení informací při návrhu a provozování informačních systémů. Jednotlivé kapitoly jsou zaměřeny na celou dobu životního cyklu informačního systému – od jeho návrhu, 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.