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