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.

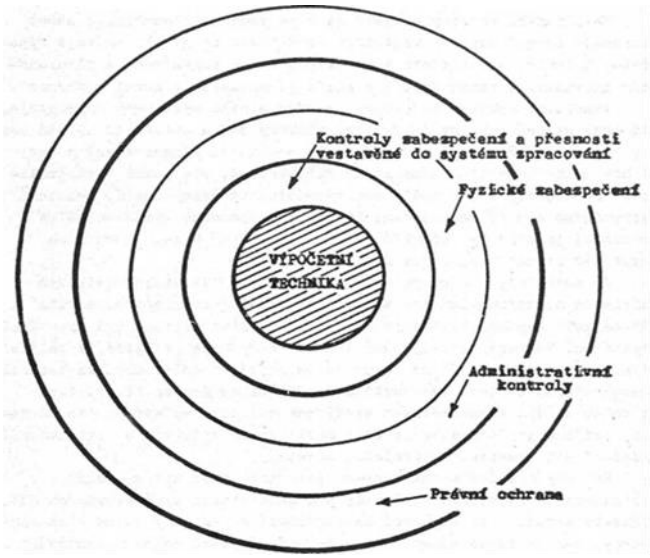
Tato kapitola obsahuje vymezení základních pojmů a zásad, které se vztahují k bezpečnosti informací a zkoumá základní součásti systému zabezpečení informací při návrhu a provozování informačních systémů. Jednotlivé kapitoly jsou zaměřeny na celou dobu životního cyklu informačního systému – od jeho návrhu,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