edice PRŮVODCE

GRADA

Systém managementu BEZPEČNOSTI INFORMACÍ

Martin Drastich

- Vývoj a současnost standardů informační bezpečnosti
- Komentář normy ISO/IEC 27001:2005
- Implementace systému managementu bezpečnosti informací
- Audit, auditor, fáze auditu
- Akreditace a certifikace ISMS


GRADA

edice PRŮVODCE

Systém managementu BEZPEČNOSTI INFORMACÍ

Martin **Drastich**

Systém managementu bezpečnosti informací

Martin Drastich

Vydala Grada Publishing, a.s.
U Průhonu 22, Praha 7
jako svou 4654. publikaci

Recenzoval Doc. Mgr. Roman Jašek, Ph.D.
Odpovědný redaktor Ing. Pavel Němeček
Sazba Tomáš Brejcha
Počet stran 128
První vydání, Praha 2011

Vytiskla Tiskárna PROTISK, s.r.o., České Budějovice

ISBN 978-80-247-4251-9 (tištěná verze)
ISBN 978-80-247-7616-3 (elektronická verze ve formátu PDF)
ISBN 978-80-247-7617-0 (elektronická verze ve formátu EPUB)

Obsah

8. Bezpečnost z hlediska lidských zdrojů

9. Fyzická bezpečnost a bezpečnost prostředí

10. Řízení komunikací a řízení provozu

Úvod

Objev principů zemědělství přinesl lidstvu metodu přetváření přírodních zdrojů v bohatství, jež vyvolala první vlnu civilizačních změn. Druhá civilizační vlna přinesla tovární systém tvorby bohatství, vedla k hromadné výrobě, koncentraci průmyslu, ke snaze o vytvoření stále větších trhů a masovou spotřebu.

Po zemědělské a průmyslové revoluci jsme v současné době v období nástupu třetí revoluční vlny[1] tzv. informační revoluce. Na vlastní kůži dnes prožíváme příchod třetí velké vlny změn v dějinách. Ocitáme se tak uprostřed procesu vytváření nové společnosti tzv. informační společnosti, která s sebou přináší odlišné způsoby práce a myšlení, digitální ekonomiku, internetové bankovnictví, e-goverment, firemní informační systémy, technologie B2B a B2C atp.

Třetí vlna civilizačních změn je charakteristická tím, že primárním faktorem jsou informace. Mění se celá struktura společnosti. Homogenita druhé vlny je nahrazována heterogenitou třetí vlny, která si žádá stále více výměny informací mezi jejími uživateli – firmami, státními správou, finančními úřady, soudy, dalšími institucemi a v neposlední řadě mezi jednotlivci. To vyvolává znalost informačních a komunikačních technologií.

V souvislosti s používáním informačních a komunikačních technologií vyvstává otázka nejen pro management firem, státní organizace, ale i pro jednotlivce ohledně bezpečnosti a ochrany dat a informací. Na firemní účet (resp. u přepážky na pobočce banky), vlastní peněženku, občanský průkaz nebo cestovní pas jsme se naučili si dávat pozor, vkladní knížky bývají pečlivě uchovány, ale se zabezpečením nebo ochranou dat při využívání informačních a komunikačních technologií si již rady nevíme. Zejména firmy by si měly uvědomit, že vlastní spoustu citlivých informací o vlastní výrobě, dodavatelích, odběratelích, plánech, investicích, zaměstnancích atp.

[1] TOFFLER, A., TOFFLEROVÁ, H. *Nová civilizace. Třetí vlna a její důsledky.* Praha: Nakladatelství Dokořán, 2001; s. 15.

Část I.

Geneze vývoje a současnost standardů informační bezpečnosti

1. Vývoj informační bezpečnosti

1.1 Historie v souvislostech

Pojem dnes známý jako informační bezpečnost se původně v bývalém Československu nazýval počítačová bezpečnost. Proto popis historie bude začínat obdobím nasazení prvních počítačů. Časopis Data Securite Management (DSM)[1] je dvouměsíčník, který na trhu odborné literatury problematice informační bezpečnosti věnuje velký prostor. Je zde uvedeno, že na mapách světové bezpečnosti leželo bývalé Československo v oblastech „Hic sunt leones" (zde jsou lvi[2]).

1.1.1 Období do konce 80. let

Zkoumání historie ztěžuje absence dostupných autentických faktografických zdrojů. Informační bezpečnost se v té době primárně spojovala s ochranou utajovaných skutečností. Složky ministerstva vnitra a obrany pečlivě utajovaly svoje know-how. V diplomatickém spojení se používaly šifrovací prostředky, např. šifrovací automat ŠA-1 z počátku 70. let byl navržen specialisty ministerstva vnitra. Komerční podoba v dnešním pojetí neexistovala, počítačů bylo málo a chyběla motivace o ně pečovat.

Počet zjištěných případů počítačové kriminality nebyl velký, pouhých 18 případů, o kterých věděl jen omezený okruh osob. Prvním zjištěným případem byla sabotáž vyvolávání poruch v počítačích Úřadu důchodového zabezpečení. Raritou je exotika používaného prostředku pachatele – dámského silonového prádla způsobujícího elektrostatické výboje, rušící citlivou elektroniku počítače.

Pro disciplínu informační bezpečnosti je důležitá druhá polovina 80. let. V periodikách Mechanizace a automatizace nebo Informační systémy se začaly objevovat články o aspektech ochrany počítačových systémů. V civilní sféře Československa zatím neexistoval původní výzkum ani vzdělávání v této oblasti.

Větší zájem o bezpečnost počítačů podnítila až existence počítačových virů. Postupně od roku 1985 vznikaly neformální skupiny specialistů mimo silové resorty a vytvořily předpoklady pro vznik vlastních bezpečnostních produktů a specializovaných firem.

1.1.2 Období 90. let

Společenské změny po roce 1989 přinesly obrovskou akceleraci oboru informační bezpečnosti. Část specialistů silových ministerstev přešla do komerční sféry. Byla zahájena výuka kryptografie na univerzitách. V Kriminalistickém ústavu v Praze vzniklo první oddělení počítačové kriminality. V roce 1992 byl přijat první zákon o ochraně osobních dat.

Zájemci o informační bezpečnost se začali sdružovat, v roce 1993 vznikla Asociace firem pro ochranu dat a informací (AFOI). V r. 1994 vznikla Group of Cryptology Union of Czech Mathematicians and Phsysicists (GCUCMP). Vznikly i národní pobočky mezinárodní organizace ISACA (Information

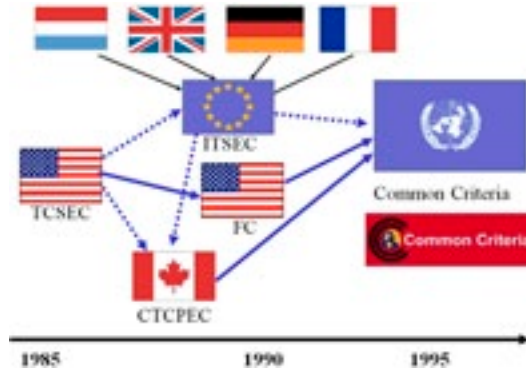
[1] Časopis DSM – Data Security Management: 6/2005; s. 8.

[2] Zde jsou lvi (latinsky). Označení neznámého neprobádaného území, na němž vládne pravděpodobně barbárie; území bez zákonů a pravidel. Používáno ve starých mapách, jako označení neprobádaného území.

Systems Audit and Control Asociation).[3] Objevili se první držitelé mezinárodně platných certifikátů CISE (Certified Information Systéme Auditor).[4]
Začaly se konat první odborné konference s mezinárodní účastí Pragocrypt 1996 a Eurocrypt 1999. Ve zvýšené míře se začaly objevovat odborné články k různým aspektům informační bezpečnosti. Koncem roku 1996 nultým číslem odstartoval svoji úspěšnou dráhu specializovaný časopis DSM, v roce 1999 začal vycházet e-zin Crypto-World. Po roce 2005 nelze opomenout vliv nové koncepce normalizace zaměřené na bezpečnost informací.

1.1.3 Hodnocení úrovně bezpečnosti informačních systémů

Nejstarším a nejrozšířenějším standardem pro hodnocení bezpečnosti informačních systémů je dokument TCSEC (Trusted Computer Evaluation Criteria),[5] který známe ovšem spíše pod názvem Orange Book. Je jednou ze série publikací ministerstva obrany USA, které se týkají bezpečnosti IS, a byla poprvé publikována v roce 1983 a později v roce 1985 podstatným způsobem upravena. Byl to první dokument, který popisoval obecné bezpečnostní požadavky. Tyto požadavky pak můžeme aplikovat na každou konkrétní část informačního systému. Části informačního systému můžeme potom rozdělit do čtyř základních tříd podle jejich bezpečnosti, a to A až D. Třída A má nejvyšší míru bezpečnosti a třída D nejnižší.
Netrvalo dlouho a objevila se i evropská kritéria pro hodnocení bezpečnosti. Jednalo se o ITSEC (Information Technology Security Evaluation Criteria).[6] Materiál vznikl jako harmonizační dokument pro národní verze, které byly přijaty ve Francii, Německu, Anglii a Holandsku. Kritéria byla v roce 1990 předložena v Bruselu k připomínkování a po úpravách byla schválena v červnu 1991. ITSEC definuje sedm tříd záruk E0 až E6 a následně v příloze definuje dalších deset tříd funkčnosti F. Třídy záruk vycházejí ze čtyř základních skupin kritérií, a to z procesu vývoje informačního systému, prostředí vývoje, provozní dokumentace a provozního prostředí. Na rozdíl od TCSEC, která původně vznikla pro vojenské prostředí a byla orientována především na důvěrnost informací, je ITSEC koncipován více obecně a pokrývá částečně i požadavky integrity a dostupnosti informace.[7]
Kanadská bezpečnostní kritéria CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) rozdělují bezpečnostní funkce do 4 velkých skupin a u každé funkce je definováno několik úrovní např. CC-0 až CC-3.



Obrázek č. 1: Přehled vzniku Common Criteria *(Zdroj: Norma ISO/IEC 15408:1999 – „Common Criteria" (CC))*

[3] *http://www.isaca.cz/*
[4] *http://www.rac.cz/*
[5] *http://www.tcsec.com/* – Trusted Computer System Evaluation Criteria (TCSEC), DoD USA, 1985.
[6] *http://www.iwar.org.uk/comsec/resources/standards/itsec.htm* – Information Technology Security Evaluation Criteria (ITSEC), EC, 1991.
[7] ANDERSON, R. J. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Wiley Publishing, 2008; s. 1080.

*

1.1.4 Globalizace a úrovně bezpečnosti

Globalizace postupuje mílovými kroky. Harmonizací výše uvedených kritérií TCSEC, ITSEC a CTCPEC byla vytvořena nejmodernější kritéria CC (Common kriteria). Tato kritéria byla přijata mezinárodním standardizačním úřadem ISO. Vznikly úrovně EAL1 až EAL7 (Evaluation Assurance Levels).
Mezinárodní norma ISO/IEC 15408:1999 má status české technické normy. Česká verze nese označení ČSN ISO/IEC 15408:2001. Český překlad prvého dílu byl Českým normalizačním institutem vydán v červnu roku 2001, překlady dalších dvou dílů byly vydány v listopadu roku 2002. Jednotlivé díly jsou ve shodě s originálem normy označeny jako 15408–1:2001, 15408–2:2002 a l5408–3:2002. Česká republika se připojila k dohodě v září roku 2004 jako certifikáty využívající účastník. V současné době je poslední vydání normy ISO/IEC 15408:2009 z roku 2009.

1.2 Současný stav informační bezpečnosti

V ČR je v oblasti informačních a komunikačních technologií řada kvalitních odborníků. Problémem však zůstává skutečnost, že se bezpečnost řeší převážně v této oblasti. Zkušenosti ze zahraničí poukazují na potřebu vnímat informační bezpečnost v daleko širším kontextu. Nejen v oblasti firemních ICT a zabezpečení jejich systémů, ale v návaznosti a ve vztazích ke zbytku firmy, včetně jejich prostor, objektů a zaměstnanců. Informační bezpečnost se nevztahuje jen k ICT, ale prakticky ke všem procesům a byznysu každé firmy.
Informační bezpečnost je nutno chápat jako základní postulát, bez kterého nelze budovat úspěšné a důvěryhodné vztahy s klienty, obchodními partnery i zaměstnanci. Veškeré osobní údaje, které budou použity v komunikaci, musí být shromažďovány, zpracovávány a uchovávány v centrální databázi s vysokou úrovní organizačního a technologického zabezpečení. Součástí bezpečnostních standardů je maximální zabezpečení elektronické komunikace mezi interními, externími počítači a serverem. Jednotlivé procesy, během nichž se odehrává přenos citlivých dat, je proto nutno zabezpečit.[8]
Informace jsou aktiva,[9] které mají pro organizaci hodnotu. Potřebují tedy být vhodným způsobem chráněny. Informační bezpečnost je zaměřena na širokou škálu hrozeb a zajišťuje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí. Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány na papíře, zachyceny na film nebo posílány elektronickou cestou, ale ať již mají jakoukoli formu, nebo ať jsou sdíleny jakýmikoli prostředky, vždy by měly být vhodně chráněny.
Informační bezpečnost je charakterizována jako zachování důvěrnosti,[10] integrity[11] a dostupnosti.[12]
Informační bezpečnosti lze dosáhnout implementací soustavy opatření, která může existovat ve formě pravidel, natrénovaných postupů, procedur, organizační struktury a programových funkcí. Tato opatření musí být zavedena proto, aby bylo dosaženo specifických bezpečnostních cílů organizace.
Informační bezpečnost je v podstatě ochrana proti možným nebezpečím, minimalizuje rizika, obsahuje komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití systému informací.

---

[8] RODRYČOVÁ, D., STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy.* Praha: Grada Publishing, 2000; s. 143.

[9] Aktivum (asset) cokoli, co má pro organizaci hodnotu [ISO/IEC 13335-1:2004].

[10] Dostupnost (availability) zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby [ISO/IEC 13335-1:2004].

[11] Integrita (integrity) zajištění správnosti a úplnosti informací a metod jejich zpracování [ISO/IEC 13335-1:2004].

[12] Důvěrnost (confidentiality) zajištění, že informace je pro oprávněné uživatele přístupná v okamžik její potřeby [ISO/IEC 13335-1:2004].

1.2.1 Standardizace informační bezpečnosti

V době zvyšujícího se konkurenčního prostředí, neustálého rozvoje a využívání informačních a komunikačních technologií, zpracovávání dat a informací klientů i partnerů je nutností veškeré informace do společností vstupující i vystupující náležitým způsobem chránit.

Definování pojmu informační bezpečnost

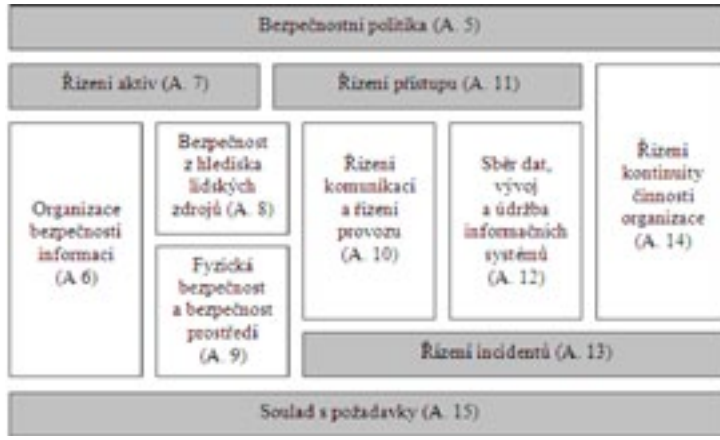
Informační bezpečnost má mnoho rovin, které jsou spolu navzájem úzce propojeny. Zdůrazněme ty hlavní, jako je ochrana informací, informačních systémů společnosti, bezpečnost komunikace, fyzická a personální bezpečnost, dále ochrana proti nebezpečím, minimalizace rizik a komplex administrativních, logických, technických, organizačních a fyzických opatření pro prevenci, detekci a opravu nesprávného použití informací a informačních aktiv. Zejména bezpečnost citlivých informací v organizaci se vztahuje na informace v elektronické i písemné formě a ošetřuje tyto informace v celém průběhu jejich koloběhu uvnitř i vně společnosti.[13]

Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System) je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že jsou určena aktiva, která se mají chránit, jsou zvolena a řízena možná rizika bezpečnosti informací, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována. ISMS je nově užívaný pojem, který v sobě zahrnuje sumu všech požadavků a opatření. Definujeme jej jako soubor opatření a požadavků k zajištění ochrany a bezpečnosti všech důležitých aktiv společnosti, tj. informací, know-how, majetku a osob, který se implementuje podle uznávaného mezinárodního standardu ISO/IEC 27001:2005.

Oblasti informační bezpečnosti

Obecně lze rozdělit informační bezpečnost do několika oblastí. Bezpečnostní politika, řízení aktiv, řízení přístupu, organizační, personální, fyzická bezpečnost, řízení komunikací a provozu, oblast vývoje a údržby informačních systémů, řízení kontinuity činností organizace, zvládání bezpečnostních incidentů a také soulad s požadavky. Přesto platí známé pravidlo informační bezpečnosti, že systém je tak bezpečný jak je zabezpečen jeho nejslabší článek. Na následujícím obrázku č. 2 (Oblasti informační bezpečnosti) můžeme vidět jednotlivé souvislosti mezi jednotlivými oblastmi.



Obrázek č. 2: Oblasti informační bezpečnosti *(Zdroj: ISO/IEC 27001:2005)*

[13] LÁTAL, I. a kol. *Ochrana informací, dat a počítačových systémů*. Praha: Eurounion, s.r.o., 1996; s. 238.