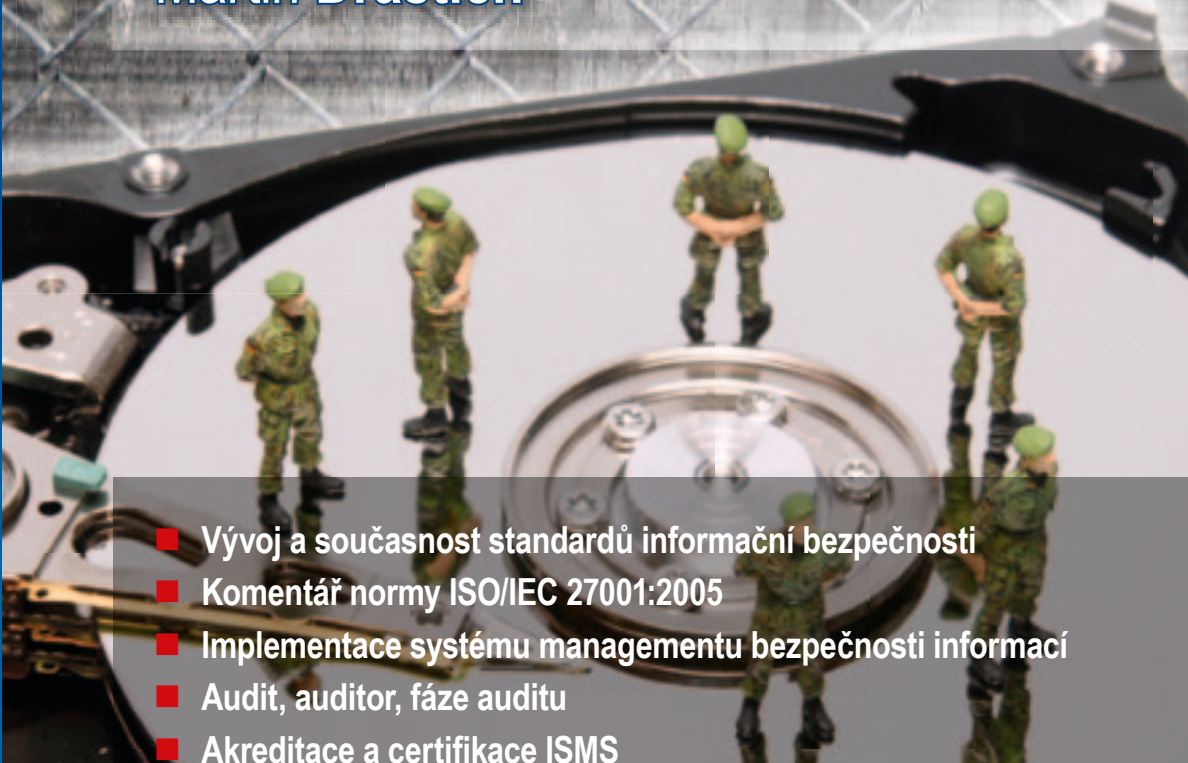




System managementu **BEZPEČNOSTI INFORMACÍ**

Martin Drastich

- 
- A photograph of a hard drive with several miniature soldiers in green uniforms standing on its surface, symbolizing security and defense.
- 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



System managementu BEZPEČNOSTI INFORMACÍ

Martin Drastich



Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována a šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude **trestně stíháno**.

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

© Grada Publishing, a.s., 2011

V knize použité názvy programových produktů, firem apod. mohou být ochrannými známkami nebo registrovanými ochrannými známkami příslušných vlastníků.

Vytiskla Tiskárna PROTISKA, 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)

Úvod	13
------------	----

ČÁST I.: Geneze vývoje a současnost standardů informační bezpečnosti 15

1.

Vývoj informační bezpečnosti

1.1 Historie v souvislostech	16
1.1.1 Období do konce 80. let	16
1.1.2 Období 90. let	16
1.1.3 Hodnocení úrovně bezpečnosti informačních systémů	17
1.1.4 Globalizace a úrovně bezpečnosti	18
1.2 Současný stav informační bezpečnosti	18
1.2.1 Standardizace informační bezpečnosti	19
1.2.2 Průzkum stavu informační bezpečnosti v České republice	20
1.3 Důvody zavedení systému managementu bezpečnosti informací	21

2.

Normy řady ČSN ISO/IEC 2700x

2.1 Struktura norem řady ISO 2700x	23
2.1.1 ISO 27001 – Specifikace pro systémy řízení bezpečnosti informací	23
2.1.2 ISO 27002 – Návod na implementaci opatření	23
2.1.3 ISO 27003 – Návod na zavedení ISMS v souladu s ISO/IEC 27001:2005 ...	24
2.1.4 ISO 27004 – Metriky ISMS	24
2.1.5 ISO 27005 – Management rizik bezpečnosti informací	24
2.1.6 ISO 27006 – Návod na implementaci opatření	24
2.1.7 ISO 27008 – Doporučení pro auditování ISMS tzv. „technický audit“ ...	24
2.1.8 ISO 27799 – Informační bezpečnost ve zdravotnictví	25
2.2 Připravované normy	25

ČÁST II.: ISO/IEC 27001:2005 27

3.

Obsah normy ISO/IEC 27001:2005

3.1 Cíle normy	28
3.2 Procesní model ISMS	28
3.2.1 Plánuj	29
3.2.2 Dělej	29
3.2.3 Kontroluj	30
3.2.4 Jednej	30
3.3 Povinná dokumentace	30

4.

Odpovědnost, audit, přezkoumání a zlepšování

4.1 Odpovědnost managementu	32
4.1.1 Osobní závazek vedení	32
4.1.2 Řízení zdrojů	32
4.1.3 Školení, informovanost a odborná způsobilost	32
4.2 Interní audit ISMS	33
4.3 Přezkoumání systému managementu ISMS	33
4.3.1 Všeobecně	33
4.3.2 Vstupy pro přezkoumání	33
4.3.3 Výstupy pro přezkoumání	33
4.4 Zlepšování ISMS	34
4.4.1 Neustále zlepšování	34
4.4.2 Opatření k nápravě	34
4.4.3 Preventivní opatření	34

5.

Bezpečnostní politika

5.1 Politika bezpečnosti informací	35
5.1.1 Dokument bezpečnostní politiky informací	35
5.1.2 Přezkoumání bezpečnostní politiky informací	35

6.

Organizace bezpečnosti informací

6.1 Vnitřní organizace	37
6.1.1 Závazek vedení organizace směrem ISMS	37
6.1.2 Koordinace bezpečnosti informací	37
6.1.3 Přidělení odpovědnosti v oblasti bezpečnosti informací	37
6.1.4 Schvalovací proces pro prostředky zpracování informací	38
6.1.5 Ujednání o ochraně důvěrných informací	38
6.1.6 Kontakt s orgány veřejné správy	38
6.1.7 Kontakty se speciálními zájmovými skupinami	38
6.1.8 Nezávislé přezkoumání bezpečnosti informací	39
6.2 Externí subjekty, partneři	39
6.2.1 Identifikace rizik vyplývajících z přístupu externích subjektů	39
6.2.2 Bezpečnostní požadavky pro přístup klientů	39
6.2.3 Zohlednění bezpečnostních požadavků v dohodách s třetí stranou	40

7.

Řízení aktiv

7.1 Odpovědnost za aktiva	41
7.1.1 Evidence aktiv	41
7.1.2 Vlastnictví aktiv	41
7.1.3 Přijatelné využívání aktiv	41
7.2 Klasifikace informací	42
7.2.1 Doporučení pro klasifikaci	42
7.2.2 Označování a zpracování informací	42

8.

Bezpečnost z hlediska lidských zdrojů

8.1 Před vznikem pracovního vztahu	43
8.1.1 Role a odpovědnosti	43
8.1.2 Prověřování osob	43
8.1.3 Podmínky a požadavky při výkonu pracovní činnosti	43
8.2 Během pracovního procesu	44
8.2.1 Odpovědnosti vedoucích pracovníků	44
8.2.2 Bezpečnostní povědomí, vzdělání a výcvik	44
8.2.3 Disciplinární řízení	44
8.3 Ukončení nebo změna pracovního vztahu	45
8.3.1 Odpovědnost při ukončování pracovního vztahu	45
8.3.2 Navrácení zapůjčených aktiv	45
8.3.3 Odebrání přístupových práv	45

9.

Fyzická bezpečnost a bezpečnost prostředí

9.1 Zabezpečení prostoru	46
9.1.1 Fyzický bezpečnostní perimetr	46
9.1.2 Fyzické kontroly vstupu osob	46
9.1.3 Zabezpečení kanceláří, místnosti a prostředků	46
9.1.4 Ochrana před hrozbami vnějšku a prostředí	47
9.1.5 Práce v zabezpečených oblastech	47
9.1.6 Veřejný přístup, prostory pro nakládku a vykládku	47
9.2 Bezpečnost zařízení	47
9.2.1 Umístění zařízení a jeho ochrana	47
9.2.2 Podpůrná zařízení, dodávky energie	48
9.2.3 Bezpečnost kabelových rozvodů	48
9.2.4 Údržba zařízení	48
9.2.5 Bezpečnost zařízení používané mimo prostory organizace	48
9.2.6 Bezpečná likvidace nebo opakované použití zařízení	48
9.2.7 Odstranění a přemístění majetku	49

10.

Řízení komunikací a řízení provozu

10.1 Provozní postupy a odpovědnost	50
10.1.1 Dokumentace provozních postupů	50
10.1.2 Řízení změn	50
10.1.3 Oddělení povinností	50
10.1.4 Oddělení vývoje, testování a provozu	51
10.2 Řízení dodávek služeb třetích stran	51
10.2.1 Dodávky služeb	51
10.2.2 Monitorování a přezkoumávání služeb zabezpečovaných třetí stranou	51
10.2.3 Řízení změn ve službách zabezpečovaných třetími stranami	51
10.3 Plánování a přejímání informačních systémů	52
10.3.1 Řízení kapacit a kapacitní plánování	52

10.3.2	Přejímání systémů	52
10.4	Ochrana proti škodlivým programům a mobilním kódům	52
10.4.1	Opatření na ochranu proti škodlivým programům	52
10.4.2	Opatření na ochranu proti mobilním kódům	53
10.5	Zálohování	53
10.5.1	Zálohování informací	53
10.6	Správa bezpečnosti sítě	53
10.6.1	Síťová opatření	53
10.6.2	Bezpečnost síťových služeb	54
10.7	Bezpečnost při zacházení s médii	54
10.7.1	Správa výměnných počítačových médií	54
10.7.2	Likvidace médií	54
10.7.3	Postupy pro manipulaci s informacemi	54
10.7.4	Bezpečnost systémové dokumentace	55
10.8	Výměna informací	55
10.8.1	Postupy a politiky při výměně informací a programů	55
10.8.2	Dohody o výměně informací a programů	55
10.8.3	Bezpečnost médií při přepravě	56
10.8.4	Elektronické zasílání zpráv	56
10.8.5	Informační systémy organizace	56
10.9	Služby elektronického obchodu	56
10.9.1	Elektronický obchod	56
10.9.2	On-line transakce	57
10.9.3	Veřejně přístupné informace	57
10.10	Monitorování	57
10.10.1	Pořizování auditních záznamů	57
10.10.2	Monitorování používání systému	57
10.10.3	Ochrana vytvořených záznamů	58
10.10.4	Administrátorský a operátorský deník	58
10.10.5	Záznam o selhání	58
10.10.6	Synchronizace hodin	58

11.

Řízení přístupu

11.1	Požadavky na řízení přístupu	59
11.1.1	Politika řízení přístupu	59
11.2	Řízení přístupu uživatelů	59
11.2.1	Registrace uživatele	59
11.2.2	Řízení privilegovaného přístupu	60
11.2.3	Správa uživatelských hesel	60
11.2.4	Přezkoumání přístupových práv uživatelů	60
11.3	Odpovědnosti uživatelů	60
11.3.1	Používání hesel	60
11.3.2	Neobsluhovaná zařízení uživatelů	61
11.3.3	Zásada prázdného stolu a prázdné obrazovky	61

11.4 Řízení přístupu k síti	61
11.4.1 Politika užívání síťových služeb	61
11.4.2 Autentizace uživatele pro externí připojení	61
11.4.3 Identifikace zařízení v sítích	62
11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci	62
11.4.5 Princip oddělení skupin v sítích	62
11.4.6 Řízení síťových spojení	62
11.4.7 Řízení směrování sítí	62
11.5 Řízení přístupu k operačnímu systému	62
11.5.1 Bezpečné postupy připojení	63
11.5.2 Identifikace a autentizace uživatelů	63
11.5.3 Systém správ hesel	63
11.5.4 Použití systémových nástrojů	63
11.5.5 Časové omezení relace	63
11.5.6 Časové omezení spojení	64
11.6 Řízení přístupu k aplikacím a informacím	64
11.6.1 Omezení přístupu k informacím	64
11.6.2 Oddělení citlivých systémů	64
11.7 Mobilní výpočetní zařízení a práce na dálku	64
11.7.1 Mobilní výpočetní zařízení a sdělovací technika	64
11.7.2 Práce na dálku	65

12.

Sběr dat, vývoj a údržba informačních systémů

12.1 Požadavky na bezpečnost informačních systémů	66
12.1.1 Analýza a specifikace požadavků na bezpečnost	66
12.2 Správný postup zpracování v aplikacích	66
12.2.1 Validace vstupních dat	66
12.2.2 Kontrola a řízení vnitřního zpracování	66
12.2.3 Celistvost zpráv	67
12.2.4 Validace výstupních dat	67
12.3 Kryptografické prostředky a opatření	67
12.3.1 Politika pro použití kryptografických prostředků a opatření	67
12.3.2 Správa klíčů	67
12.4 Bezpečnost systémových souborů	68
12.4.1 Správa provozního programového vybavení	68
12.4.2 Ochrana dat pro testování systému	68
12.4.3 Řízení přístupu do knihovny zdrojových kódů	68
12.5 Bezpečnost procesů vývoje a podpory	69
12.5.1 Postupy řízení změn	69
12.5.2 Technické přezkoumání změn operačního systému	69
12.5.3 Omezení změn programových balíků	69
12.5.4 Únik informací	69
12.5.5 Programové vybavení vyvíjené externím dodavatelem	70

12.6 Řízení technických zranitelností	70
12.6.1 Řízení, správa a kontrola technických zranitelností	70

13.

Zvládání bezpečnostních incidentů

13.1 Hlášení bezpečnostních incidentů	71
13.1.1 Hlášení bezpečnostních událostí	71
13.1.2 Hlášení bezpečnostních slabín	71
13.2 Zvládání bezpečnostních incidentů a kroky k nápravě	72
13.2.1 Odpovědnosti a postupy	72
13.2.2 Ponaučení z bezpečnostních incidentů	72
13.2.3 Shromažďování důkazů	72

14.

Řízení kontinuity organizace

14.1 Aspekty bezpečnosti informací při řízení kontinuity činnosti organizace	73
14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činnosti organizace	73
14.1.2 Kontinuita činností organizace a hodnocení rizik	73
14.1.3 Vytváření a implementace plánu kontinuity	73
14.1.4 Systém plánování kontinuity činností organizace	74
14.1.5 Testování, udržování a přezkoumávání plánu kontinuity	74

15.

Soulad a požadavky

15.1 Soulad s právními normami	75
15.1.1 Identifikace odpovídajících předpisů	75
15.1.2 Ochrana duševního vlastnictví	75
15.1.3 Ochrana záznamů organizace	75
15.1.4 Ochrana dat a soukromí osobních údajů	76
15.1.5 Prevence zneužití prostředků pro zpracování informací	76
15.1.6 Registrace kryptografických opatření	76
15.2 Soulad s bezpečnostními politikami, normami a technická shoda	76
15.2.1 Shoda s bezpečnostními politikami a normami	76
15.2.2 Kontrola technické shody	76
15.3 Hlediska auditu informačních systémů	77
15.3.1 Opatření pro audit informačního systému	77
15.3.2 Ochrana nástrojů pro audit systému	77

ČÁST III.: Implementace 79

16.

Implementace

16.1 Rozhodnutí managementu o zavedení ISMS	80
16.2 Ustanovení rozsahu a hranice ISMS	80
16.3 Vstupní analýza	80

16.4 Stanovení bezpečnostní politiky (politika ISMS)	82
16.5 Analýza rizik	82
16.6 Příklad harmonogramu implementace	84
16.7 Vypracování povinných dokumentů	86
16.7.1 Bezpečnostní příručka	87
16.7.2 Prohlášení o aplikovatelnosti POA	87
16.7.3 Směrnice řízení dokumentů a záznamů	87
16.7.4 Směrnice interní auditu	88
16.7.5 Směrnice nápravných a preventivních opatření	88
16.8 Implementace, zavádění do praxe, školení zaměstnanců	89
16.9 Systémový audit	89
16.10 Integrované systémy řízení	90

ČÁST IV.: Audit 93

Audit

17.1 Úvod do problematiky průběhu auditu	94
17.2 Důvody, cíle a odpovědnosti auditu	95
17.3 Rozsah činností auditu	95

Auditor

18.1 Charakteristika auditora	97
18.2 Etický kodex auditora	97
18.3 Příslušný výcvik auditora	98
18.4 Techniky řízení týmu	98
18.4.1 Styly řízení auditu	99
18.4.2 Řízení auditorského skupiny	99

Fáze auditu

19.1 Fáze přípravy auditu	101
19.1.1 Etapa vstupního plánování	101
19.1.2 Předběžná prohlídka	101
19.1.3 Podrobné plánování	102
19.2 Fáze auditování	102
19.2.1 Systémy dokumentace auditu	102
19.2.2 Taktika a technika auditu	102
19.2.3 Technika dotazů	103
19.2.4 Kontrolní (check) listy	103
19.2.5 Hledání objektivních důkazů	104
19.2.6 Hledání kořenových příčin	104
19.2.7 Neshody v systému	105
19.2.8 Registrace neshod	105

19.2.9	Hlášení neshod	105
19.2.10	Pozorování z auditu	106
19.3	Fáze následných opatření	106
19.3.1	Zpráva z auditu	106
19.3.2	Příprava souhrnné zprávy	106
19.3.3	Závěrečná schůzka a prezentace souhrnné zprávy	107
19.3.4	Dohoda a následná nápravná opatření	107

ČÁST V.: Akreditace a certifikace 109

20.

Akreditace a certifikace

20.1	Akreditace	110
20.2	Certifikace	110
20.2.1	Certifikační orgán	110
20.2.2	Pracovníci certifikačního orgánu	111
20.2.3	Provádění dozoru	111
20.2.4	Certifikace procesů	111
20.2.5	Certifikační dokument	111
20.3	Certifikační audit	112
20.3.1	První etapa certifikačního auditu	112
20.3.2	Druhá etapa certifikačního auditu	113
20.3.3	Zprávy a závěry z certifikačního auditu	113
20.4	Pravidla a postupy certifikačního orgánu	113
20.4.1	Žádost o prvotní audit a certifikace	113
20.4.2	Přezkoumání žádosti k provedení auditu	114
20.5	Certifikační stupeň auditu	114
20.5.1	První stupeň auditu	114
20.5.2	Druhý stupeň auditu	115
20.5.3	Závěry z prvotního certifikačního auditu	115
20.5.4	Informace pro udělení prvotní certifikace	116
20.5.5	Dozorové činnosti	116
20.6	Udržování certifikace	116
20.7	Plánování, opakování, udělení certifikace	117
20.8	Změny v certifikačním řízení	117

Závěr	120
Bibliografie	121
Pojmy	122
Zkratky	124
Summary	125
Rejstřík	126

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 vlny¹ 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 bankovníctví, e-government, 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 lvi²).

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 Physicists (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

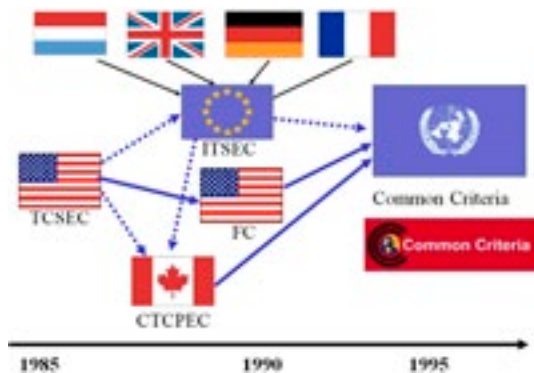
Začaly se konat první odborné konference s mezinárodní účastí Pragocrypt 1996 a Eurocrypt 1999. Ve zvýšené míře se začaly objevovat odborné články k různým aspektům informační bezpečnosti. Koncem roku 1996 nultým číslem odstartoval svoji úspěšnou dráhu specializovaný časopis DSM, v roce 1999 začal vycházet 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) rozděluje 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 prvního 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 15408–3:2002. 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 integrity¹¹ 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

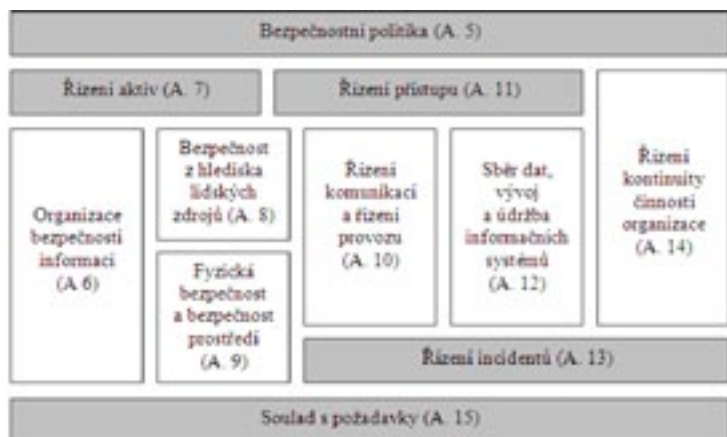
Informační bezpečnost má mnoho rovin, které jsou spolu navzájem úzce propojeny. Zdůrazněme ty hlavní, jako je ochrana informací, informačních systémů společnosti, bezpečnost komunikace, fyzická a personální bezpečnost, dále ochrana proti nebezpečím, minimalizace rizik a komplex administrativních, logických, 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 činnosti 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.

1.2.2 Průzkum stavu informační bezpečnosti v České republice

V České republice byl v roce 2009 již popáté proveden průzkum stavu informační bezpečnosti a ochrany dat v České republice. Průzkum prováděly následující organizace: Ernst and Young, časopis DSM – data security management a Národní bezpečnostní úřad. Tento průzkum probíhal od března do června 2009, bylo osloveno celkem 1 100 společností.

Výsledky průzkumu můžeme shrnout do následujících zjištění:

- Roste podíl organizací, které hodnotí vlastní úroveň řešení informační bezpečnosti jako významnou.
- Největší význam pro prosazení informační bezpečnosti má hrozba útoku.
- Ubývá společností, kde není za řešení informační bezpečnosti jasně definována ničí zodpovědnost.
- Informační bezpečnost je u naprosté většiny společností začleněna do úseků IS/IT, tento trend je ale klesající: 85 % (2003), 78 % (2005), 71 % (2007) a 70 % (2009).
- Stále přetrvává, že největší překážkou rychlejšího prosazování informační bezpečnosti je obecně nízké bezpečnostní povědomí. Roste podíl společností, které tuto překážku uvádějí na prvním místě před finanční náročností. Přitom funkční program pro zvyšování povědomí má zavedeno pouze 21 % organizací. Zvýšení bezpečnostního povědomí je také nejčastěji zmiňovanou aktivitou s potenciálem pro úspory nákladů v informační bezpečnosti ve střednědobém horizontu.
- Dvě třetiny dotázaných organizací již mají zavedenou bezpečnostní politiku.
- Nejčastěji zaznamenané bezpečnostní incidenty jsou SPAM a výpadek.
- Na 16 % klesl podíl organizací, které nikdy neprovedly analýzu rizik IS.
- Zajímavostí je, že u 63 % společností je informační bezpečnost řešena ve spolupráci s externími firmami.
- Až 66 % organizací má, nebo plánuje posoudit oblasti informační bezpečnosti externím subjektem.



Graf č. 1: Jaké mezinárodní standardy jsou využívány v oblasti informační bezpečnosti a/nebo IT governance při řešení informační bezpečnosti? (Zdroj: PSIB ČR 09)

Průzkum dále ukázal, jak jsou využívány mezinárodní standardy v oblasti informační bezpečnosti. Pokud odhlédneme od použití vlastních interních standardů a směrnic (61 %) a standardů a směrnic přejatých od mateřské společnosti (29 %), pak vidíme, že nejrozšířenějším standardem je ISO/IEC 27000:2009 (a jejich předchůdci – 27 %). Z odpovědí také vyplývá, že 31 % respondentů používá více než jeden standard.

Závěrem můžeme tedy říci, že význam normy řady ISO/IEC 27000:2009 (dříve ISO/IEC 17799 a BS 7799) zastoupených ve využívání mezinárodních standardů má vzrůstající tendenci z 25 % (2007) na 27 % (2009) a pro svoji univerzálnost je možné tuto mezinárodní normu aplikovat do různých oborů působnosti nejen do ICT organizací.

Všechny uvedené hodnoty byly převzaty z publikace průzkum stavu informační bezpečnosti v ČR za rok 2009.¹⁴

1.3 Důvody zavedení systému managementu bezpečnosti informací

Organizace by měla přistoupit k zavedení systému managementu bezpečnosti informací z mnoha důvodů, které vyplývají ze shora uvedeného textu. Zavedení systému managementu bezpečnosti informací by mělo podat důkaz o tom, že všechny citlivé informace, údaje a data jsou chráněny řízeným způsobem podle určitého standardu. Dále ukázat svým zákazníkům a dalším zainteresovaným stranám, že organizace je pro ně důvěryhodný partner a jejich citlivé informace jsou odpovídajícím způsobem chráněny. Plnit požadavky EU a legislativy ČR týkající se ochrany informací. Zavedení ISMS vede k tomu, že organizace může získat nezbytnou výhodu před konkurencí.

■ Potřeba ISMS

Trend zavedení systému managementu bezpečnosti informací je rostoucí. Tento systém potřebují:

- firmy, které poskytují služby v oblasti outsourcingu a ASP (zpracovávají informace a data – obchodní svých klientů, mají přístup do IS klientů);
- organizace, které zpracovávají informace a data občanů (nemocnice, státní správa, banky, pojišťovny a úřady);
- zákazníci, kteří předávají dodavatelům výsledky svého vývoje a know-how (žádají ISMS od svých dodavatelů);
- organizace, které se účastní výběrových řízení pro státní správu;
- organizace, které zpracovávají data a informace pro velké nadnárodní firmy;
- dodavatelé produktů a služeb, po kterých zákazníci vyžadují důkaz o uplatňování důvěryhodných postupů v oblasti bezpečnosti informací.

■ Podcenění stavu bezpečnosti informací, osob a majetku může vést k:

- úniku informací ze společnosti, včetně know-how a informací o klientech;
- opomenutí některých slabých míst v oblasti zabezpečení informací;
- vzniku škod při bezpečnostních incidentech, včetně dopadu škod vlivem jejich medializace;
- možné ztrátě image společnosti;
- sankcím za nedodržování platné legislativy;
- sankcím nebo odvolání vrcholového vedení za nedodržování bezpečnostních pravidel;
- implementaci nevhodného nebo nefunkčního bezpečnostního systému;
- možnosti vyloučení z veřejných zakázek pro nesplnění požadavků na certifikaci (např. NBÚ, ISO, ISMS apod.);
- nefunkčnosti výrobních kapacit v důsledku bezpečnostních incidentů a mimořádných událostí (IS, budovy, selhání zálohovacího zařízení apod.).

■ Přínosy zavedení a certifikace ISMS pro společnost:

- přechod od nesystémového a neuceleného řízení bezpečnosti k bezpečnosti řízené a komplexní;
- efektivní řízení investic vkládaných do bezpečnosti;
- inventura vlastních aktiv, jejich ocenění a klasifikace;
- řízené odstranění nebo snížení rizik v oblasti informačních systémů;
- zavedení systémového a systematického přístupu při používání IT/IS;
- zvýšení povědomí a odpovědnosti zaměstnanců při práci s informacemi;
- naplnění legislativních požadavků;
- zvýšení důvěryhodnosti pro partnery;
- trvalé monitorování a zlepšování systému řízení bezpečnosti informací;
- kultivace image a firemní kultury, konkurenční výhoda.

¹⁴ PSIB ČR 09, Ernst & Young, NBÚ, DSM – data security management.