

Obsah

1. Základní principy bezpečnosti při použití IT	9
1.1 Motivace pro zabezpečování při použití IT	9
1.2 Výklad základních pojmů z oblasti bezpečnosti IT	12
1.2.1 Použitý model	12
1.2.2 Zranitelné místo, hrozba, riziko, útok, útočník	13
1.2.2.1 Zranitelné místo	13
1.2.2.2 Hrozba	14
1.2.2.3 Útok	15
1.2.2.4 Útočník	16
1.2.2.5 Riziko	17
1.2.3 Bezpečnost IT	17
1.2.4 Bezpečnostní funkce	19
1.2.5 Bezpečnostní mechanismy	21
1.3 Zásady výstavby bezpečnostní politiky IT	21
1.3.1 Cíle bezpečnostní politiky IT	22
1.3.2 Typy bezpečnostních politik	23
1.3.3 Principy určující charakter bezpečnostní politiky	24
1.3.4 Celková a systémová bezpečnostní politika IT	25
1.3.4.1 Celková bezpečnostní politika IT	25
1.3.4.2 Systémová bezpečnostní politika IT	28
1.3.4.3 Metodika procesu vytváření bezpečnostních politik	30
1.3.5 Analýza rizik	31
1.3.6 Havarijný plán	34
1.3.6.1 Účel a struktura	34
1.3.6.2 Plán činnosti po útoku	34
1.3.6.3 Průběh reakce na incident	35
1.3.6.4 Plán obnovy	35
1.3.7 Bezpečnostní audit	38
2. Bezpečnostní funkce	39
2.1 Bezpečnostní funkce podle kritérií ITSEC	39
2.1.1 Třídy funkčnosti ITSEC	39
2.1.2 Specifikace funkcí prosazujících bezpečnost podle ITSEC	40
2.1.2.1 Identifikace a autentizace	40
2.1.2.2 Řízení přístupu	40
2.1.2.3 Účtovatelnost	40
2.1.2.4 Audit	41
2.1.2.5 Opakované užití	41
2.1.2.6 Přesnost	41
2.1.2.7 Spolehlivost a dostupnost služeb	41
2.1.2.8 Výměna dat	41
2.2 Bezpečnostní funkce podle kritérií CTCPEC	41
2.2.1 Bezpečnostní funkce zajišťující důvěrnost	42
2.2.2 Bezpečnostní funkce zajišťující integritu	42
2.2.3 Bezpečnostní funkce zajišťující dostupnost	43

2.2.4	Bezpečnostní funkce zajišťující účtovatelnost	43
2.3	Bezpečnostní funkce podle CC	44
2.3.1	Rozšiřování a údržba funkčních požadavků	44
2.3.2	Organizace dokumentu ISO/IEC 15408-2	45
2.3.3	Model funkčních požadavků	45
2.3.4	Katalog komponent funkčních požadavků	49
2.3.5	Třída FAU: Bezpečnostní audit	51
2.3.6	Třída FCO: Komunikace	51
2.3.7	Třída FCS: Kryptografická podpora	51
2.3.8	Třída FDP: Ochrana uživatelských dat	51
2.3.9	Třída FIA: Identifikace a autentizace	52
2.3.10	Třída FMT: Správa bezpečnosti	53
2.3.11	Třída FPR: Soukromí	53
2.3.12	Třída FPT: Ochrana bezpečnostní funkcionality	53
2.3.13	Třída FRU: Využití zdrojů	54
2.3.14	Třída FTA: Přihlášení do HP	55
2.3.15	Třída FTP: Důvěryhodné cesty/kanály	55
2.3.16	Minimální požadavky funkčnosti v návrhu bezpečnostního standardu SIS	55
3.	Bezpečnostní mechanismy	57
3.1	Příklady bezpečnostních mechanismů	57
3.1.1.1	Hesla a osobní identifikační čísla	57
3.1.1.2	Magnetické karty	58
3.1.1.3	Čipové karty	58
3.2	Síla bezpečnostních mechanismů	59
3.3	Kryptografické bezpečnostní mechanismy	59
3.3.1	Registrace kryptografických algoritmů	60
3.3.2	Typy kryptografických algoritmů	61
3.3.3	Režimy činnosti kryptografických algoritmů	62
3.3.4	Režim ECB	63
3.3.5	Režim CBC	63
3.3.6	Režim CFB	64
3.3.7	Režim OFB	64
3.3.8	Autentizační algoritmus MAC	65
3.4	Elektronický podpis	66
3.4.1	Vlastnosti elektronického podpisu	66
3.4.2	Kryptografie a elektronický podpis	67
3.4.3	Aplikace elektronického podpisu	68
3.4.4	Bezpečnost elektronického podpisu	69
3.4.5	Podpůrné funkce	69
3.4.6	Příklad aplikace elektronického podpisu ve státní správě	70
3.4.7	Normy ISO pro elektronický podpis	70
3.4.7.1	ISO/IEC 14888	70
3.4.7.2	ISO/IEC 10118	70
3.4.7.3	ISO/IEC 13888	70
3.4.7.4	ISO/IEC 15946	71
3.5	Bezpečnostní požadavky na kryptografické moduly	71
3.5.1.1	Třída 1	71

3.5.1.2	Třída 2	72
3.5.1.3	Třída 3	72
3.5.1.4	Třída 4	72
4.	Správa bezpečnosti IT.....	73
4.1	Bezpečnostní architektura sítí podle ISO 7498-2.....	73
4.1.1	Bezpečnostní služby ISO 7498-2	74
4.1.2	Implementace bezpečnostních služeb ve vrstvách OSI.....	75
4.1.3	ISO služby pro bezpečnou komunikaci podle ISO 7498-2	76
4.1.4	Správa bezpečnosti podle ISO 7498-2	78
4.2	Norma bezpečnostních služeb IT ISO/IEC 10181	79
4.3	Důvěryhodné třetí strany (TTP)	80
4.3.1	Typy důvěryhodných třetích stran.....	81
4.3.2	Správa a provoz důvěryhodných třetích stran	82
4.3.3	Služby poskytované třetími důvěryhodnými stranami	83
4.3.3.1	Služby časových razítek	83
4.3.3.2	Služby nepopíratelnosti	84
4.3.3.3	Služby správy klíčů	84
4.3.3.4	Certifikační služby	86
4.3.3.5	Notářské služby	87
4.3.3.6	Další služby poskytované TTP.....	88
4.3.4	Relevantní normalizační materiál.....	88
5.	Normalizace bezpečnosti IT	89
5.1	Kdo je kdo ve světě norem (bezpečnosti IT).....	89
5.1.1	Mezinárodní normalizační organizace	89
5.1.2	Národní normalizační organizace.....	90
5.1.3	Ostatní standardizační organizace	90
5.2	Proces normalizace v ISO	91
5.3	ISO normy bezpečnosti IT	91
5.4	Normy síťových bezpečnostních architektur (orientační přehled).....	94
5.4.1	Normy bezpečnostních funkcí.....	95
5.4.2	Normy bezpečnostních mechanismů.....	95
5.4.2.1	Normy kryptografických algoritmů.....	96
5.4.2.2	Normy digitálních podpisů	96
5.4.2.3	Normy mechanismů řízení přístupu	96
5.4.2.4	Normy integritních mechanismů	96
5.4.2.5	Normy mechanismů výměny autentizačních dat.....	97
5.4.2.6	Normy mechanismů notarizace	97
5.5	Normy správy klíčů.....	98
5.6	Normy zaručitelnosti bezpečnosti	98
5.7	Norma bezpečnostních funkcí ISO/IEC 10181	98
5.8	Vybrané ISO/IEC normy bezpečnostních mechanismů.....	100
6.	Hodnocení bezpečnosti.....	101
6.1	Bezpečnost IT a kritéria bezpečnosti	101

6.2	Kritéria bezpečnosti ITSEC	101
6.2.1	Rozsah kritérií ITSEC	102
6.2.2	Proces hodnocení podle kritérií ITSEC	103
6.2.3	Kritické zhodnocení kritérií ITSEC.....	104
6.2.3.1	Kritika definice integrity	104
6.2.3.2	Kritika generických záhlaví definujících bezpečnostní funkcionalitu	105
6.2.3.3	Kritika příkladů tříd funkčnosti	105
6.3	Kritéria bezpečnosti CC	105
6.3.1	Čeho se CC týkají a čeho se netýkají	105
6.3.2	Pro koho jsou CC určena.....	106
6.3.3	Jak lze hodnocení podle CC uplatnit	107
6.4	Model bezpečnosti CC	108
6.5	Pojetí bezpečnosti podle CC	109
6.5.1	Prostředí produktu nebo systému IT.....	109
6.5.2	Bezpečnostní plán	110
6.5.3	Požadavky na bezpečnost IT	110
6.5.4	Profil ochrany a bezpečnostní cíl	111
6.6	Bezpečnostní funkcionalita produktu/systému IT	111
6.7	Požadavky zaručitelnosti bezpečnosti.....	112
6.7.1	Paradigma zaručitelnosti bezpečnosti IT.....	112
6.7.1.1	Základní filozofie zaručitelnosti bezpečnosti IT	112
6.7.1.2	Role hodnocení.....	112
6.7.1.3	Ošetření zranitelných míst.....	112
6.7.1.4	Vznik zranitelných míst.....	113
6.7.2	Zaručitelnost bezpečnosti IT podle CC	113
6.7.2.1	Zaručitelnost bezpečnosti je odvozená z výsledků hodnocení	113
6.7.2.2	Škálování zaručitelnosti bezpečnosti plynoucí z hodnocení	114
6.7.2.3	Úrovně zaručitelnosti bezpečnosti podle CC	114
6.7.3	Klasifikace požadavků zaručitelnosti bezpečnosti	115
6.7.3.1	Třída a rodina požadavků zaručitelnosti bezpečnosti.....	115
6.7.3.2	Příklady tříd a rodin požadavků zaručitelnosti bezpečnosti	115
6.7.4	Specifikace požadavků zaručitelnosti bezpečnosti.....	116
6.7.4.1	Komponenty a prvky zaručitelnosti bezpečnosti.....	116
6.8	Charakteristiky úrovní zaručitelnosti bezpečnosti	117
6.8.1	EAL1, funkčně testovaný produkt nebo systém IT	117
6.8.1.1	Cíle EAL1	117
6.8.1.2	Záruky EAL1	118
6.8.2	EAL2, strukturálně testovaný produkt nebo systém IT	118
6.8.2.1	Cíle EAL2	118
6.8.2.2	Záruky EAL2 (rozšíření proti EAL1).....	118
6.8.3	EAL3, metodicky testovaný a kontrolovaný produkt nebo systém.....	119
6.8.3.1	Cíle EAL3	119
6.8.3.2	Záruky EAL3 (rozšíření proti EAL2).....	119
6.8.4	EAL4, metodicky navrhovaný, testovaný a přezkoumávaný produkt nebo systém IT	119
6.8.4.1	Cíle EAL4	119
6.8.4.2	Záruky EAL4 (rozšíření proti EAL3).....	119

6.8.5	EAL5, semifórnálně navrhovaný a testovaný produkt nebo systém IT	120
6.8.5.1	Cíle EAL5	120
6.8.5.2	Záruky EAL5 (rozšíření proti EAL4).....	120
6.8.6	EAL6, testovaný produkt nebo systém IT se semifórnálně ověřovaným návrhem	121
6.8.6.1	Cíle EAL6	121
6.8.6.2	Záruky EAL6 (rozšíření proti EAL5).....	121
6.8.7	EAL7, testovaný produkt nebo systém IT s formálně ověřovaným návrhem	121
6.8.7.1	Cíle EAL7	121
6.8.7.2	Záruky EAL7 (rozšíření proti EAL6).....	122

1.3 Matrice pro zabezpečení při práci IT

Matrice pro zabezpečení při práci IT je nástroj, který umožňuje vyhodnotit riziko bezpečnosti IT v závislosti na úrovni zabezpečení a důležitosti dat.

Úroveň zabezpečení	Důležitost dat	Riziko bezpečnosti IT
1	1	1
1	2	2
1	3	3
2	1	2
2	2	4
2	3	6
3	1	3
3	2	6
3	3	9