

Duben 2002

	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření	ČSN ISO/IEC TR13335-4 36 9786
---	---	---

Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards

Technologies de l'information - Lignes directrices pour la gestion de sécurité IT - Partie 4: Sélection de sauvegardes

Tato norma je českou verzí mezinárodní normy ISO/IEC TR 13335-4:2000. Mezinárodní norma ISO/IEC TR 13335-4:2000 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC TR 13335-4:2000. The International Standard ISO/IEC TR 13335-4:2000 has the status of a Czech Standard.

© Český normalizační institut,
2002

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány
a rozšiřovány jen se souhlasem Českého normalizačního institutu.

63634

Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT

ISO/IEC TR 13335-2:1997 zavedena v ČSN ISO/IEC TR 13335-2 (36 9786) Informační technologie -
Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT

ISO/IEC TR 13335-3:1998 zavedena v ČSN ISO/IEC TR 13335-3 (36 9786) Informační technologie -
Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT

ISO/IEC 10181-2:1996 zavedena v ČSN ISO/IEC 10181-2 (36 9694) Informační technologie - Propojení
otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura autentizace

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1 (36 9785) Informační technologie - Bezpečnostní
techniky - Správa klíčů - Část 1: Struktura správy klíčů

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky k textu.

Národní poznámka

Pro účely této normy se anglické slovo „security“ překládá jako „bezpečnost“.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA
Informační technologie -
Směrnice pro řízení bezpečnosti IT -
Část 4: Výběr ochranných opatření

ISO/IEC TR 13335-4
První vydání
2000-03-01

ICS 35.040

Obsah

Strana

Úvod

..... 7

1 Předmět
normy

	 8
2	
	Odkazy
	 8
3	
	Termíny a definice
	 8
4	
	Cíl
	 8
5	
	Přehled
	 9
6	
	Úvod do výběru ochranných opatření a koncepce základní úrovně bezpečnosti..... 11
7	
	Základní odhady
	 15
7.1	
	Identifikace typu systému IT
	 15
7.2	
	Identifikace fyzikálních podmínek / podmínek okolního prostředí..... 15
7.3	
	Posouzení existujících / plánovaných ochranných opatření..... 16
8	
	Ochranná opatření
	 16
8.1	
	Organizační a fyzická ochranná opatření..... 16
8.1.1	
	Řízení bezpečnosti IT a politiky bezpečnosti IT..... 16

8.1.2	Kontrola bezpečnostní shody	17
8.1.3	Řešení incidentů	18
8.1.4	Zaměstnanci	18
8.1.5	Provozní problémy	18
8.1.6	Plánování kontinuity činnosti organizace	20
8.1.7	Fyzická bezpečnost	20
8.2	Ochranná opatření specifická pro systém IT	25
8.2.1	Identifikace a autentizace (I&A)	25
8.2.2	Řízení logického přístupu a audit	26
8.2.3	Ochrana před škodlivým programovým kódem	26
8.2.4	Správa sítí	27
8.2.5	Kryptografie	28
9	Přístup na základní úrovni: Výběr ochranných opatření podle typu systému	

IT.....	31
9.1 Všeobecně aplikovatelná ochranná opatření.....	32
9.2 Ochranná opatření specifická pro systém IT.....	32
10 Výběr ochranných opatření v závislosti na bezpečnostních problémech a hrozbách.....	33
10.1 Posouzení bezpečnostních problémů.....	34
10.1.1 Ztráta důvěrnosti.....	34

Strana 4

Strana

10.1.2 Ztráta integrity.....	35
10.1.3 Ztráta dostupnosti.....	35
10.1.4 Ztráta individuální odpovědnosti.....	35
10.1.5 Ztráta autentičnosti.....	36
10.1.6 Ztráta spolehlivosti.....	36
10.2 Ochranná opatření zajišťující důvěrnost.....	36
10.2.1	

Odposlouchávání	36
10.2.2 Elektromagnetická radiace	37
10.2.3 ©kodlivý programový kód	37
10.2.4 Předstírání identity uživatele	37
10.2.5 Nesprávné směrování / přesměrování zpráv	37
10.2.6 Chyba software	38
10.2.7 Krádež	38
10.2.8 Neautorizovaný přístup k počítačům, datům, službám a aplikacím	38
10.2.9 Neautorizovaný přístup k paměťovým médiím	39
10.3 Ochranná opatření zajišťující integritu	39
10.3.1 Zhoršení kvality paměťového média	39
10.3.2 Chyba údržby	39
10.3.3 ©kodlivý programový kód	39

10.3.4	Předstírání identity uživatelé	40
10.3.5	Nesprávné směrování / přesměrování zpráv.....	40
10.3.6	Nepopiratelnost	40
10.3.7	Chyba software	40
10.3.8	Poruchy napájení (elektrická energie, klimatizace).....	41
10.3.9	Technické poruchy	41
10.3.10	Chyby přenosu	41
10.3.11	Neautorizovaný přístup k počítačům, datům, službám a aplikacím.....	41
10.3.12	Použití neautorizovaných programů a dat.....	42
10.3.13	Neautorizovaný přístup k paměťovým médiím.....	42
10.3.14	Chyba uživatelé	42
10.4	Ochranná opatření zajišťující dostupnost.....	42
10.4.1	Destruktivní útok	43

10.4.2	Zhoršení kvality paměťových médií.....	43
10.4.3	Chyby a poruchy komunikačních zařízení a služeb.....	43
10.4.4	Požár, voda	44
10.4.5	Chyba údržby	44
10.4.6	©kodlivý programový kód	44
10.4.7	Předstírání identity uživatele 44	
10.4.8	Nesprávné směrování / přesměrování zpráv.....	45
10.4.9	Zneužití zdrojů	45
10.4.10	Přírodní katastrofy	45
10.4.11	Chyby software	45
10.4.12	Poruchy napájení (elektrická energie, klimatizace).....	46

10.4.13	Technické poruchy	
		
		46
10.4.14	Krádež	
		
		46
10.4.15	Přetížení provozu	
		
		46
10.4.16	Chyby přenosu	
		
		47
10.4.17	Neautorizovaný přístup k počítačům, datům, službám a aplikacím.....	47
10.4.18	Použití neautorizovaných programů a dat.....	47
10.4.19	Neautorizovaný přístup k paměťovým médiím.....	47
10.4.20	Chyba uživatele	
		
		48
10.5	Ochranná opatření zajišťující individuální odpovědnost, autentičnost a spolehlivost.....	48
10.5.1	Individuální odpovědnost	
		
	...	48
10.5.2	Autentičnost	
		
		48
10.5.3	Spolehlivost	
		
		48
11	Výběr ochranných opatření podle podrobných	

posouzení.....	49
11.1 Vztah mezi částí 3 a částí 4 ISO/IEC TR 13335.....	49
11.2 Zásady výběru.....	49
12 Vývoj základní úrovně pro celou organizaci.....	50
13 Shrnutí.....	51
Bibliografie.....	52
Příloha A Code of Practice for Information Security Management.....	53
Příloha B ETSI Baseline Security Standard - Features and Mechanisms.....	55
Příloha C IT Baseline Protection Manual.....	57
Příloha D NIST Computer Security Handbook.....	59
Příloha E Medical Informatics: Security Categorisation and Protection for Healthcare Information Systems.....	61
Příloha F TC68 Banking and Related Financial Services - Information Security Guidelines.....	63
Příloha G Protection of sensitive information not covered by the Official Secrets Act - Recommendations for computer workstations.....	65
Příloha H Canadian Handbook on Information Technology Security.....	67
Národní příloha NA (informativní).....	

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 3 direktiv ISO/IEC.

ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání návrhu jako mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Ve výjimečných případech, pokud technická komise shromáždila data různé povahy z těch, která jsou obvykle publikována jako mezinárodní norma ("state of the art" např.), může prostou většinou hlasů podílejících se členů rozhodnout o vydání Technické zprávy. Technická zpráva je svou povahou výhradně informativní a nemusí být revidována, dokud nejsou data, která poskytuje, již považována za neplatná nebo neužitečná.

Pozornost je nutno věnovat možnosti, že některé prvky této části ISO/IEC TR 13335 mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

ISO/IEC TR 13335-4 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, podkomise SC 27, *Bezpečnostní techniky*.

ISO/IEC TR 13335 se skládá z následujících částí se společným názvem *Informační technologie - Směrnice pro řízení bezpečnosti IT*:

- Část 1: *Pojetí a modely bezpečnosti IT*
- Část 2: *Řízení a plánování bezpečnosti IT*
- Část 3: *Techniky pro řízení bezpečnosti IT*
- Část 4: *Výběr ochranných opatření*
- Část 5: *Ochranná opatření pro externí spojení*

Úvod

Účelem této technické zprávy (ISO/IEC TR 13335) je poskytnout směrnice, ne řešení, týkající se řídicích aspektů bezpečnosti IT. Pracovníci, kteří jsou v organizaci zodpovědní za bezpečnost IT, by měli být schopni přejmout materiál uvedený v této zprávě takovým způsobem, aby vyhovoval jejich specifickým potřebám.

Hlavní cíle této technické zprávy jsou:

- definovat a popsat pojetí spojená s řízením bezpečnosti IT,
- identifikovat vztahy mezi řízením bezpečnosti IT a mezi řízením IT všeobecně,
- prezentovat několik modelů, které mohou být použity k vysvětlení bezpečnosti IT, a
- poskytnout všeobecnou směrnici o řízení bezpečnosti IT.

ISO/IEC TR 13335 je rozdělena do pěti částí. Část 1 poskytuje přehled základních pojetí a modelů, použitých k popisu řízení bezpečnosti IT. Tento materiál je vhodný pro manažery odpovědné za bezpečnost IT a pro ty, kdo jsou odpovědní za celkový bezpečnostní program organizace.

Část 2 popisuje řídicí a plánovací aspekty. Tato část má význam pro manažery s odpovědnostmi souvisejícími se systémy IT organizace. Těmi mohou být:

- manažeři IT, kteří jsou odpovědní za dohled nad návrhem, implementací, testováním, pořízením nebo provozováním systémů IT, nebo
- manažeři, kteří jsou odpovědní za činnosti, které využívají podstatným způsobem systémy IT.

Část 3 popisuje bezpečnostní techniky vhodné pro použití pracovníky, kteří jsou zapojeni do manažerských činností v průběhu životního cyklu projektu, jako je plánování, návrh, implementace, testování, získání nebo provozování.

Část 4 poskytuje směrnice pro výběr ochranných opatření a jak může být tento výběr podporován použitím základních modelů a kontrol. Rovněž popisuje, jak takový výběr doplňuje bezpečnostní techniky popsané v části 3 a jak mohou být pro výběr ochranných opatření použity doplňkové metody posuzování.

1 Předmět normy

Tato část ISO/IEC TR 13335 poskytuje směrnice pro výběr ochranných opatření s ohledem na potřeby činnosti organizace a problémy bezpečnosti. Popisuje proces výběru ochranných opatření podle bezpečnostních rizik a problémů a specifického prostředí organizace. Ukazuje, jak dosáhnout odpovídající ochrany a jak může být tento proces podporován aplikací základní úrovně bezpečnosti. Poskytuje i vysvětlení, jak přístup naznačený v této části ISO/IEC TR 13335 podporuje techniky pro řízení bezpečnosti IT předložené v ISO/IEC TR 13335-3.

-- Vynechaný text --