ČESKÁ TECHNICKÁ NORMA

ICS 35.040 ~~Návrh~~

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.

63634

Národní předmluva

Citované normy

ISO/IEC TR 13335-1:1996 zavedena v ČSN ISO/IEC TR 13335-1 (36 9786) Informační technologie -

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

---

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

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 obyčejně 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 řídících 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 řídící 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 --