ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červen**
2001

	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model	ČSN ISO/IEC 15408-1 36 9789

Information technology - Security techniques - Evaluatution criteria for IT security - Part 1: Introduction and general model

Technologies de l’information - Techniques de sécurité - Critères d’évaluation pour la sécurité TI - Partie 1: Introduction
et modèle général

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-1:1999. Mezinárodní norma ISO/IEC 15408-1:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 15408-1:1999. The International Standard ISO/IEC 15408-1:1999 has the status of a Czech Standard.

61397

Národní předmluva

Citované normy

ISO/IEC 7498-2:1989 zavedena v ČSN ISO 7498-2 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model

ISO/IEC 15408-1
První vydání
1999-12-01

ICS 35.040

Deskriptory: informační technologie, kritéria hodnocení IT, míra záruky hodnocení, schéma hodnocení, organizační bezpečnostní politika, produkt, profil ochrany, bezpečnostní atribut, bezpečnostní funkce, předmět hodnocení, model bezpečnostní politiky

Obsah

Strana

Seznam obrázků

Seznam tabulek

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 příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými 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 mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Mezinárodní norma ISO/IEC 15408-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* ve spolupráci s Organizacemi sponzorujícími projekt Společná kritéria. Identický text ISO/IEC 15408-1 je zveřejněn Organizacemi sponzorujícími projekt Společná kritéria pod názvem *Společná kritéria pro hodnocení bezpečnosti informačních technologií*. V příloze A ISO/IEC 15408-1 jsou uvedeny další informace o projektu Společná kritéria a kontaktní informace na Organizace sponzorující projekt.

ISO/IEC 15408 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT:*

– *Část 1: Úvod a všeobecný model*

– *Část 2: Bezpečnostní funkční požadavky*

– *Část 3: Požadavky na zaručitelnost bezpečnosti*

Přílohy B a C jsou normativní součástí této části ISO/IEC 15408. Přílohy A a D jsou pouze informativní.

Na základě žádosti byla do všech částí ISO/IEC 15408 umístěna tato PRÁVNÍ POZNÁMKA:

Sedm vládních organizací (společně nazývaných „Organizace sponzorující projekt Společná kritéria“), které jsou uvedené v příloze A ISO/IEC 15408-1, přidělují tímto jako společní držitelé autorských práv dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, část 1 až 3 (nazývaná „CC“) organizaci ISO/IEC neexkluzivní licenci k používání CC při vývoji mezinárodní normy ISO/IEC 15408. Organizace sponzorující projekt Společná kritéria si však ponechávají právo používat, kopírovat, šířit nebo pozměňovat CC, jak uznají za vhodné.

---

1 Předmět normy

ISO/IEC 15408, norma o více částech, vymezuje kritéria, která jsou zde z historických důvodů a pro zachování kontinuity uváděna jako Common Criteria (CC), která mají být použita jako základ pro hodnocení bezpečnostních vlastností produktů a systémů IT. Ustavením takové základny Společných kritérií budou mít výsledky hodnocení bezpečnosti IT význam pro širší veřejnost.

CC umožní srovnatelnost výsledků nezávislých hodnocení bezpečnosti. Provádějí to poskytnutím obecné množiny požadavků na bezpečnostní funkce produktů a systémů IT a na opatření týkající se záruk, která jsou aplikovaná v průběhu hodnocení bezpečnosti. Proces hodnocení ustavuje určitý stupeň důvěry, že bezpečnostní funkce takových produktů a systémů a na ně aplikovaná opatření týkající se záruk splňují tyto požadavky. Výsledky hodnocení mohou pomoci spotřebitelům určit, zdali je produkt nebo systém IT dostatečně bezpečný pro jejich zamýšlenou aplikaci a zdali je možné tolerovat bezpečnostní rizika implicitně vyplývající z jejich používání.

CC jsou užitečná jako návod pro vývoj produktů nebo systémů s bezpečnostními funkcemi IT a pro pořizování komerčních produktů a systémů s takovými funkcemi. V průběhu hodnocení je takový produkt nebo systém IT nazýván předmět hodnocení (TOE). Předmět hodnocení (TOE) zahrnuje například operační systémy, počítačové sítě, distribuované systémy a aplikace.

CC se zabývají ochranou informací před neautorizovaným zpřístupněním, změnou nebo ztrátou možnosti jejich použití. Kategorie ochrany vztahující se k těmto třem typům selhání bezpečnosti jsou obecně označovány jako důvěrnost, integrita a dostupnost. CC je možné aplikovat rovněž na další aspekty bezpečnosti. CC se soustřeďují na hrozby vůči informacím, které jsou výsledkem lidských aktivit, a» už škodlivých nebo jiných, ale mohou být aplikovatelná právě tak na některé hrozby, které nesouvisí s lidskou činností. CC mohou být kromě toho aplikována v dalších oblastech IT, nečiní si však nárok na kompetentnost mimo oblast bezpečnosti IT.

CC jsou aplikovatelná na IT bezpečnostní opatření implementovaná v hardwaru, firmwaru nebo softwaru. Bude-li záměrem aplikovat specifické aspekty hodnocení pouze na určité metody implementace, bude to vyznačeno v relevantních tvrzeních kritérií.

Určitá témata, protože zahrnují specializované techniky nebo protože jsou vzhledem k bezpečnosti IT poněkud okrajová, jsou považována za témata, přesahující rámec CC. Některá z nich jsou uvedena dále.

a) CC neobsahují kritéria pro hodnocení bezpečnosti týkající se administrativních bezpečnostních opatření, která nesouvisí přímo s IT bezpečnostními opatřeními. Často však může být významná část bezpečnosti TOE dosažena pomocí administrativních opatření jako jsou organizační, personální, fyzické a procedurální kontroly. Administrativní bezpečnostní opatření v provozním prostředí TOE jsou považována za předpoklad bezpečného použití, kdy tato opatření mají dopad na schopnost IT bezpečnostních opatření čelit identifikovaným hrozbám.

b) Hodnocení technicko-fyzických aspektů bezpečnosti IT jako je kontrola elektromagnetického vyzařování není specificky řešena, i když mnoho z uplatněných pojmů je možné na tuto oblast aplikovat. CC řeší zejména některé aspekty fyzické ochrany TOE.

c) CC se nezabývá metodologií hodnocení ani administrativním a právním rámcem, na základě kterého mohou být kritéria aplikována hodnotícími autoritami. Očekává se však, že CC budou použita pro účely hodnocení v kontextu takového rámce a takové metodologie.

d) Postupy pro použití výsledků hodnocení při akreditaci produktu nebo systému jsou mimo rámec CC. Akreditace produktu nebo systému je administrativní proces, kterým je uděleno oprávnění provozovat produkt nebo systém IT v jeho plném provozním prostředí. Hodnocení je zaměřeno na IT bezpečnostní části produktu nebo systému a na ty části provozního prostředí, které mohou přímo ovlivnit bezpečné používání prvků IT. Výsledky procesu hodnocení jsou následně cenným vstupem pro akreditační proces. Protože však pro posouzení bezpečnostních vlastností produktů nebo systémů nesouvisících s IT a jejich vztahu k bezpečnostním částem IT jsou vhodnější jiné techniky, měli by akreditační činitelé přijmout v případě takových aspektů jiná opatření.

e) CC se nezabývají předmětem kritérií pro hodnocení inherentních kvalit kryptografických algoritmů. V případě, že by bylo požadováno nezávislé hodnocení matematických vlastností kryptografie, obsažené v TOE, schéma hodnocení, na základě kterého jsou CC aplikována, musí zajistit pro taková hodnocení příslušné opatření.

-- Vynechaný text --