ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor 2013**

Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model

ČSN ISO/IEC 15408-1
36 9789

Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

Technologies de l,information – Techniques de sécurité – Criteres d,évaluation pour la sécurité TI – Partie 1: Introduction et modele général

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-1:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15408-1:2009. It was translated by the Czech Office for Standards, Metrology a Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 15408-2 zavedena v ČSN ISO/IEC 15408-2 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ISO/IEC 15408-3 zavedena v ČSN ISO/IEC 15408-3 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty záruky bezpečnosti

ISO/IEC 18045 dosud nezavedena

Souvisící ČSN

ČSN IEC 27001:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN ISO/IEC 17799:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 15408-1 vypracovala společná technická komise ISO/IEC JTC 1, *Informační technologie*, subkomise 27, *Bezpečnostní techniky IT*. Identický text ISO/IEC 15408 je zveřejněn organizacemi sponzorujícími projekt Common Criteria pod názvem Společná kritéria pro hodnocení bezpečnosti informačních technologií. Společný zdroj XML pro obě publikace je uveden v *http://www.oc.ccn.cni.es/xml*

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 15408-1:2005), které bylo technicky

revidováno.

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

- *Část 1: Úvod a obecný model*
- *Část 2: Bezpečnostní funkční komponenty*
- *Část 3: Komponenty záruky bezpečnosti*

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 15408-1
Kritéria pro hodnocení bezpečnosti – 3. vydání
Část 1: Úvod a obecný model 2009-12

Obsah

Strana

Úvod

Tato část ISO/IEC 15408 umožňuje srovnatelnost výsledků nezávislých bezpečnostních hodnocení. ISO/IEC 15408 to činí poskytnutím obecné sady požadavků pro bezpečnostní funkčnost IT produktů a pro úrovně záruk aplikované na tyto IT produkty v průběhu bezpečnostního hodnocení. Tyto IT produkty mohou být implementovány v hardwaru, firmwaru nebo softwaru.

Proces hodnocení ustavuje úroveň důvěry, že bezpečnostní funkčnost těchto IT produktů a záruka opatření aplikovaná na tyto produkty IT splňují tyto požadavky. Výsledky hodnocení mohou pomoci spotřebitelům určit, zda tyto produkty IT splňují jejich bezpečnostní potřeby.

ISO/IEC 15408 je užitečná jako návod pro vývoj, hodnocení a/nebo získání IT produktů s bezpečnostní funkčností.

ISO/IEC 15408 je záměrně pružná, umožňující, aby byl určitý rozsah metod hodnocení aplikován na rozsah bezpečnostních vlastností rozsahu IT produktů. Proto uživatelé této mezinárodní normy jsou upozornění, aby věnovali pozornost tomu, že pružnost není nesprávně použita. Použití ISO/IEC 15408 společně s nevhodnými metodami hodnocení, irelevantními bezpečnostními vlastnostmi nebo nevhodnými IT produkty může například vyústit v nesmyslné výsledky hodnocení.

Následně skutečnost, že IT produkt byl ohodnocen, má význam pouze v kontextu bezpečnostních vlastností, které byly hodnoceny a metod hodnocení, které byly použity. Autoritám provádějícím hodnocení se doporučuje, aby pečlivě kontrolovaly produkty, vlastnosti a metody a mohly tak určit, že hodnocení poskytne smysluplné výsledky. Navíc kupujícím hodnocených produktů se doporučuje pečlivě zvažovat tento kontext a tak určit, zda je hodnocený produkt užitečný a aplikovatelný na jejich specifickou situaci a potřeby.

ISO/IEC 15408 se zabývá ochranou aktiv před neautorizovaným odhalením, modifikací nebo nemožností využití. Kategorie ochrany souvisící s těmito třemi druhy selhání bezpečnosti jsou obecně nazývány důvěrnost, integrita a dostupnost, v tomto pořadí. ISO/IEC 15408 je také možné aplikovat na další aspekty bezpečnosti IT. ISO/IEC 15408 je aplikovatelná na rizika vznikající v důsledku lidské činnosti (ať už zlomyslné nebo neúmyslné) a na rizika vznikající v důsledku činnosti nikoliv lidské. Kromě bezpečnosti IT může být ISO/IEC 15408 aplikována v dalších oblastech IT, ale nečiní si nárok na aplikovatelnost v těchto oblastech.

Určitá témata jsou považována za témata mimo rozsah ISO/IEC 15408, protože obsahují specializované techniky nebo protože jsou pro bezpečnost IT okrajová. Některá z nich jsou dále uvedena.

a. ISO/IEC 15408 neobsahuje kritéria pro hodnocení bezpečnosti spadající pod opatření pro administrativní bezpečnost nevztahující se přímo k funkčnosti bezpečnosti IT. Je však zjištěno, že významné bezpečnosti je často možné dosáhnout nebo je podporována administrativními opatřeními, například organizačními, personálními, fyzickými a procedurálními.

b. Hodnocení některých technických fyzických aspektů bezpečnosti IT, například kontroly elektromagnetického vyzařování není specificky pokryto, ačkoliv mnoho řešených konceptů je možné na tuto oblast aplikovat.

c. ISO/IEC 15408 se nezabývá metodologií hodnocení, pomocí které by kritéria měla být aplikována. Tato metodologie je uvedena v ISO/IEC 18045.

d. ISO/IEC 15408 se nezabývá administrativním a právním rámcem, pomocí kterých mohou být kritéria použita autoritami pro hodnocení. Očekává se však, že ISO/IEC 15408 bude použito pro účely hodnocení

v kontextu takového rámce.

e. Postupy pro použití výsledků hodnocení při akreditaci jsou mimo rozsah ISO/IEC 15408. Akreditace je administrativní proces, podle něhož je autorita poskytnuta pro provoz produktu IT (nebo jejich výběr) v jeho úplném provozním prostředí včetně všech jeho částí nespadajících pod části IT. Výsledky procesu hodnocení jsou vstupem do procesu akreditace. Jelikož pro posouzení vlastností nesouvisících s IT a jejich bezpečnostními částmi jsou vhodné jiné techniky, měli by ti, kteří provádějí akreditaci, použít pro tato hlediska jiná samostatná ustanovení.

f. Předmět kriterií pro posouzení základních vlastností kryptografických algoritmů není v ISO/IEC 15408 řešen. V případě, že by bylo požadováno nezávislé posouzení matematických vlastností kryptografie, schéma hodnocení, pomocí kterého je ISO/IEC 15408 aplikována, musí pro taková posouzení přijmout opatření.

Terminologie ISO, například „can“, „informative“, „may“, „normative“, „shall“ a „should“, používaná v dokumentu, je definovaná ve směrnicích ISO/IEC, část 2. Všimněme si, že termín „should“ má další význam aplikovatelný při použití této mezinárodní normy. Viz dále uvedenou poznámku. Následující definice je platná pro použití „should“ v ISO/IEC 15408.

should

v normativním textu „should“ označuje, „že z několika možností je jedna doporučena jako zvláště vhodná, aniž by byly zmíněny nebo vyloučeny ostatní možnosti, nebo že určitý průběh akce je preferován, ale není nutně požadován“ (směrnice ISO/IEC, část 2)

POZNÁMKA ISO/IEC 15408 interpretuje „ne nutně požadováno“ ve významu, že volba jiné možnosti vyžaduje zdůvodnění, proč nebyla vybrána preferovaná možnost.
1 Předmět normy

Tato část ISO/IEC 15408 stanoví obecné koncepty a principy hodnocení bezpečnosti IT a specifikuje obecný model hodnocení daný různými částmi mezinárodní normy, která má být v celém svém rozsahu považována za použitelnou jako základ pro hodnocení bezpečnostních vlastností produktů IT.

Poskytuje přehled všech částí ISO/IEC 15408. Popisuje různé části normy; definuje termíny a zkratky, které mají být použity ve všech částech mezinárodní normy; stanoví hlavní pojetí Cílů hodnocení (TOE); kontext hodnocení; a popisuje cílové čtenáře, kterým jsou kritéria hodnocení adresována. Je podán úvod k základním bezpečnostním pojetím nutným pro hodnocení produktů IT.

Definuje různé operace, kterými mohou být funkční komponenty a komponenty záruky uvedené v ISO/IEC 15408-2 a ISO/IEC 15408-3, upraveny s použitím povolených operací.

Jsou specifikovány základní koncepty profilů ochrany (PP), balíky bezpečnostních požadavků a předmětu shody a jsou popsány následky a výsledky hodnocení. Tato část ISO/IEC 15408 podává směrnice pro specifikaci Bezpečnostních cílů (ST) a poskytuje popis organizace komponent v rámci modelu. Obecné informace o metodologii hodnocení jsou uvedeny v ISO/IEC 18045 a je poskytnut rámec schémat hodnocení.