ČESKÁ TECHNICKÁ NORMA

ICS35.040 **Březen 2010**

Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ČSN ISO/IEC 15408-2
36 9789

Information technology – Security techniques – Evaluatution criteria for IT security – Part 2: Security functional components

Technologies de l,information – Techniques de sécurité – Criteres d,évaluation pour la sécurité TI – Partie 2: Composants fonctionnels de sécurité

Informationstechnik – IT-Sicherheitsverfahren: Evaluationskriterien für IT-Sicherheit – Teil 2: Funktionelle Sicherheitskomponnenten

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-2:2008. 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 15408-2:2008. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 15408-2 (36 9789) z listopadu 2002.

Národní předmluva

Změny proti předchozím normám

Změny v této normě oproti normě původní se týkají vypuštění některých částí původní normy, přidání nových částí a dále formálních úprav, například číslování.

Informace o citovaných normativních dokumentech

ISO/IEC 15408-1 zavedena v ČSN ISO/IEC 15408-1 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria hodnocení bezpečnosti IT – Část 1: Úvod a všeobecný model

Další informace

V této normě je použit výraz signaturní události (signature events). Jsou to takové události, které mají určité charakteristické znaky nebo rysy významné pro další postup. V použitém kontextu to znamená, že jejich výskyt izolovaný od zbytku aktivity systému svědčí o rušivých vlivech.

Pro účely této normy je přeložen:

a. anglický výraz Target of Evaluation (TOE) volně jako Předmět hodnocení

b. anglický výraz Security Target (ST) jako Bezpečnostní cíl

c. anglický výraz Management jako správa nebo řízení nebo jejich kombinace

d. anglický výraz Time Stamp jako vyznačení času.

e. Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným temínům značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky– Kritéria ISO/IEC 15408-2
pro hodnocení bezpečnosti IT – Třetí vydání
Část 2: Bezpečnostní funkční komponenty 2008-08

Obsah

Strana

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 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. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 2 směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Pozornost je věnována možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nepřebírají zodpovědnost za identifikaci jakýchkoliv nebo všech takových patentových práv.

Mezinárodní norma ISO/IEC 15408-2 byla připravena společnou technickou komisí ISO/IEC JTC 1, Informační technologie, subkomisí 27, *Bezpečnostní techniky IT*. Identický text ISO/IEC 15408-2 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 ruší a nahrazuje druhé vydání (ISO/IEC 15408-2:2005), 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 všeobecný model*
- *Část 2: Bezpečnostní funkční komponenty*
- *Část 3: Komponenty záruky bezpečnosti.*

PRÁVNÍ POZNÁMKA:

Dále uvedené vládní organizace přispěly k vývoji této verze Společných kritérií pro hodnocení bezpečnosti informačních tecchnologií. Jako společní držitelé autorských práv dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, verze 3.1, část 1 až 3 (nazývaných „CC 3.1“) přidělují tímto organizaci ISO/IEC neexkluzivní licenci k používání CC 3.1 při pokračujícím vývoji/údržbě mezinárodní normy ISO/IEC 15408. Tyto vládní organizace si však ponechávají právo používat, kopírovat, šířit, překládat nebo pozměňovat CC 3.1, jak uznají za vhodné.

Australia/New Zealand: The Defence Signals Directorate and the Government Communications Security Bureau respectively;

Canada: Communications Security Establishment;

France: Direction Centrale de la Sécurité des Systemes d'Information;

Germany: Bundesamt für Sicherheit in der Informationstechnik;

Japan: Information Technology Promotion Agency;.

Netherlands: Netherlands national Communications Security Agency;

Spain: Ministerio de Administraciones Públicas and Centro Criptológico Nacional;

United Kingdom: Communications-Electronic Security Group;

United States: The National Security Agency and the National Institute of Standards and Technology

Úvod

Bezpečnostní funkční komponenty definované v této části ISO/IEC 15408 jsou základem pro IT bezpečnostní funkční požadavky vyjádřené v Profilu ochrany (PP) nebo v Bezpečnostním cíli (ST). Tyto požadavky popisují žádoucí bezpečnostní chování očekávané Předmětem hodnocení (TOE) a jsou určeny ke splnění bezpečnostních cílů uvedených v PP nebo ST. Tyto požadavky popisují bezpečnostní vlastnosti, které uživatel může detekovat přímou interakcí (tj. vstupy, výstupy) s IT nebo odezvou IT na podnět.

Bezpečnostní funkční komponenty vyjadřují bezpečnostní požadavky, jejichž cílem je čelit hrozbám v předpo-
kládaném provozním prostředí TOE a/nebo pokrýt jakékoliv identifikované organizační bezpečnostní politiky a předpoklady.

Tato část ISO/IEC 15408 je určena spotřebitelům, pracovníkům vývoje a hodnotitelům bezpečných produktů IT. Kapitola 5 ISO/IEC 15408-1 poskytuje další informace o cílových uživatelích ISO/IEC 15408 a o použití ISO/IEC 15408 skupinami, které zahrnují tyto uživatele. Tyto skupiny mohou použít tuto část ISO/IEC 15408 následovně.

a. Spotřebitelé, kteří používají při výběru komponent tuto část ISO/IEC 15408, aby vyjádřili funkční požadavky k uspokojení bezpečnostních cílů vyjádřených v PP nebo ST. ISO/IEC 15408-1 poskytuje podrobnější informace o vztahu mezi bezpečnostními cíli a bezpečnostními požadavky.

b. Pracovníci vývoje, kteří odpovídají na aktuální nebo zaznamenané bezpečnostní požadavky při konstruování TOE, mohou nalézt v této části ISO/IEC 15408 normalizovanou metodu k pochopení těchto požadavků. Mohou také použít obsah této části ISO/IEC 15408 jako základ pro další definování bezpečnostních funkcí a mecha-
nismů TOE, které odpovídají těmto požadavkům.

c. Hodnotitelé, kteří používají funkční požadavky definované v této části ISO/IEC 15408 při ověřování, zda funkční požadavky TOE vyjádřené v PP nebo ST splňují cíle bezpečnosti IT a zda jsou objasněny a ukázány všechny závislosti, aby mohly být splněny. Hodnotitelé by také měli použít tuto část ISO/IEC 15408 jako pomoc při určení, zda daný TOE uspokojuje stanovené požadavky.

1 Předmět normy

Tato část ISO/IEC 15408 definuje požadovanou strukturu a obsah bezpečnostních funkčních komponent pro účely hodnocení bezpečnosti. Obsahuje katalog funkčních komponent, které splňují

společné bezpečnostní funkční požadavky mnoha produktů IT.