ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Březen 2015**

Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení

ČSN ISO/IEC 27033-3
36 9701

Information Technology – Security techniques – Network security –
Part 3: Reference networking scenarios – Threats, design techniques and control issues

Technologies de l'information – Techniques de sécurité – Sécurité de réseau –
Partie 3: Scénarios de réseautage de référence – Menaces, techniques conceptuelles et questions de contrôle

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-3:2010. 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 27033-3:2010. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27033-1 dosud nezavedena

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původním tvaru, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

backend, botnet, broadcast, chat, cross-site scripting, exploit, instant messaging, man-in-the-middle, malware, multicast, on-board, peer-to-peer, phishing, ping sweep, point-and-shoot, rootkit, spyware, SQL injection, stream, webhosting

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27033-3
Bezpečnost sítě – První vydání
Část 3: Referenční síťové scénáře – Hrozby, 2010-12-15
techniky návrhu a otázky řízení

ICS 35.040

Obsah

Strana

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 nebo 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. ISO a IEC ustavily v oblasti informačních technologií 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 27033-3 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Bezpečnostní techniky IT*.

ISO/IEC 27033 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – Bezpečnost sítě*:

- *Část 1: Přehled a pojetí*
- *Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě*

- *Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení*

Následující části se připravují:

- *Část 4: Zabezpečení komunikací mezi sítěmi s využitím bezpečnostních bran – Hrozby, techniky návrhu a otázky řízení*
- *Část 5: Zabezpečení virtuálních privátních sítí – Hrozby, techniky návrhu a otázky řízení*

V budoucnu mohou následovat další části zahrnující témata, jako jsou například lokální sítě, sítě WAN, bezdrátové a rádiové sítě, širokopásmové sítě, hlasové sítě, konvergence IP protokolu (data, hlas, video), architektury webhostingu, architektury Internetového e-mailu (včetně odchozího on-line přístupu k Internetu a příchozího přístupu z Internetu), a směrovaný přístup k třetím stranám.

1 Předmět normy

Tato část ISO/IEC 27033 popisuje hrozby, techniky návrhu a otázky řízení spojené s referenčními síťovými scénáři. Pro každý scénář poskytuje podrobné pokyny ohledně bezpečnostních hrozeb a technik návrhu bezpečnosti a opatření potřebných ke zmírnění souvisejících rizik. Pokud je to relevantní, obsahuje odkazy na ISO/IEC 27033-4 až ISO/IEC 27033-6, aby se zabránilo duplikování obsahu těchto dokumentů.

Informace uvedené v této části ISO/IEC 27033 jsou určeny pro použití při přezkoumání možností technické architektury/návrhu bezpečnosti a při výběru a dokumentování preferované technické architektury/návrhu bezpečnosti a souvisejících opatření bezpečnosti, v souladu s normou ISO/IEC 27033-2. Vybrané konkrétní informace (spolu s informacemi vybranými z ISO/IEC 27033-4 až ISO/IEC 27033-6) budou záviset na charakteristikách přezkoumávaného síťového prostředí, tj. na konkrétním síťovém scénáři (scénářích) a příslušných „technologických“ tématech.

Celkově tato část ISO/IEC 27033 podstatně pomůže komplexní definici a implementaci bezpečnosti pro síťové prostředí jakékoli organizace.