ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen 2016**

Informační technologie – Bezpečnostní techniky –
Bezpečnost sítě –
Část 4: Zabezpečení komunikace mezi sítěmi
s využitím bezpečnostních bran

ČSN
ISO/IEC 27033-4
36 9701

Information Technology – Security techniques – Network security –
Part 4: Securing communications between networks using security gateways

Technologies de l,information – Techniques de sécurité – Sécurité de réseau –
Partie 4: Sécurisation des communications entre réseaux en utilisant des portails de sécurité

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-4:2014. 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 27033-4:2014. 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 27033-1 zavedena v ČSN ISO/IEC 27033-1:2016 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 1: Přehled a pojmy

Souvisící ČSN

ČSN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO/IEC 27002:2014 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ČSN ISO/IEC 27033-3:2015 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě –
Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení

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:

- back-to-back, cloud, cloud computing, dual-homed, end-to-end, extranet, firewall, hypervisor, man-in-

the-middle, malware, multi-homed, port, proxy, router, spam, webhosting

Pro anglický výraz „standard“ se v této normě užívá český ekvivalent „standard“, aby se tím vyjádřilo, že se jedná o nadřazený výraz zahrnující jak technické normy, tak i další související dokumenty, které nevytvářejí oficiální normalizační organizace.

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 27033-4
Bezpečnost sítě – První vydání
Část 4: Zabezpečení komunikace mezi sítěmi 2014-03-01
s využitím bezpečnostních bran

ICS 35.040

Obsah

Strana

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

copyright@iso.org

www.iso.org

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 svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. 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 technickými komisemi se rozesílají národním orgánům 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 27033-4 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Toto první vydání ISO/IEC 27033-4 zrušuje a nahrazuje ISO/IEC 18028-3:2005, které bylo technicky zrevidováno.

ISO/IEC 27033 se společným názvem *Informační technologie – Bezpečnostní techniky – Bezpečnost sítě* se
sestává z těchto samostatných částí:

- *Část 1: Přehled a pojmy*
- *Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě*
- *Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení*
- *Část 4: Zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran*
- *Část 5: Zabezpečení komunikace napříč sítěmi s využitím virtuálních privátních sítí (VPN)*

- *Část 6: Zabezpečení bezdrátového IP síťového přístupu*

(Mohou existovat i další části. Příklady možných témat, které mají být řešeny v jednotlivých částech, zahrnují lokální sítě, rozlehlé sítě, širokopásmové sítě, webhosting, Internetový e-mail a směrovaný přístup k organizacím třetích stran. Hlavními kapitolami všech takových částí by měla být Rizika, Techniky návrhu a Otázky řízení.)

Úvod

Většina komerčních i státních organizací má své informační systémy propojeny sítěmi, přičemž síťová propojení představují jedno nebo více z následujících:

- v rámci organizace,
- mezi různými organizacemi,
- mezi organizací a veřejností.

Dále, s rychlým vývojem veřejně dostupných síťových technologií (zejména Internetem) nabízejících významné obchodní příležitosti, organizace rostoucí měrou provádějí elektronické obchodování v globálním měřítku a poskytují on-line veřejné služby. Příležitosti zahrnují poskytování levnějších datových komunikací, používajících jednoduše Internet jako globální propojovací médium, až po sofistikovanější služby poskytované poskytovateli internetových služeb (ISP). To může znamenat použití od relativně levných místních připojovacích bodů na každém konci obvodu až k on-line systémům elektronického obchodování a poskytování služeb v plném rozsahu, pomocí webových aplikací a služeb. Kromě toho nová technologie (včetně integrace dat, hlasu a videa) zvyšuje příležitosti pro práci na dálku (také známou jako práci z domova). Pracovníci jsou schopni být v kontaktu prostřednictvím zařízení pro dálkový přístup k organizaci a komunitním sítím a souvisejícím informacím a službám podporujícím podnikání.

Nicméně zatímco toto prostředí podporuje významné podnikatelské výhody, jsou zde nová bezpečnostní rizika, která je třeba zvládat. Pokud organizace ve značné míře spoléhají na používání informací a souvisejících sítí pro vykonávání své podnikatelské činnosti, ztráta důvěrnosti, integrity a dostupnosti informací a služeb by mohla mít na tyto činnosti významné negativní dopady. Proto je hlavním požadavkem patřičně chránit sítě a s nimi související informační systémy a informace. Jinými slovy, zavedení a udržování odpovídající bezpečnosti sítě je zásadní pro úspěch jakékoliv podnikatelské činnosti organizace.

Průmyslová odvětví telekomunikací a informačních technologií v této souvislosti hledají nákladově efektivní, komplexní řešení bezpečnosti, zaměřené na ochranu sítí před škodlivými útoky a neúmyslnými nesprávnými činnostmi a na splnění podnikatelských požadavků na důvěrnost, integritu a dostupnost informací a služeb. Zabezpečení sítě je rovněž nezbytné pro dosažení přesnosti účtování využívání sítě. Bezpečnostní vlastnosti produktů jsou rozhodující pro celkovou bezpečnost sítě (včetně aplikací a služeb). Jak je však více výrobků kombinováno pro poskytnutí celkového řešení, bude úspěch řešení určován interoperabilitou, nebo jejím nedostatkem. Bezpečnost nesmí být pouze částí zájmu o každý výrobek nebo službu, ale musí být vybudována způsobem, který podporuje úzké propojení bezpečnostních schopností v celkovém řešení bezpečnosti.

Účelem ISO/IEC 27033-4 Zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran je poskytnout návod, jak identifikovat a analyzovat hrozby bezpečnosti sítě spojené s bezpečnostními bránami, definovat požadavky bezpečnosti sítě pro bezpečnostní brány na základě analýzy hrozeb, představit techniky návrhu pro dosažení technické architektury bezpečnosti sítě pro řešení hrozeb a aspektů řízení spojených s typickými scénáři sítě a řešení otázek spojených s implementací, provozem, monitorováním a přezkoumáváním kontrolních opatření bezpečnosti sítě pomocí bezpečnostních bran.

Je třeba zdůraznit, že ISO/IEC 27033-4 je relevantní pro všechny pracovníky, kteří jsou zapojeni do podrobného plánování, navrhování a implementace bezpečnostních bran (například architekti a projektanti sítí, správci sítí a řídící pracovníci síťové bezpečnosti).

1 Předmět normy

Tato část ISO/IEC 27033 poskytuje návod pro zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran (firewall, aplikační firewall, systém prevence průniku atd.) v souladu s dokumentovanou politikou bezpečnosti informací bezpečnostních bran, včetně:

a. identifikace a analýzy hrozeb bezpečnosti sítě spojených s bezpečnostními branami;

b. definice požadavků bezpečnosti sítě na bezpečnostní brány založených na analýze hrozeb;

c. použití technik pro návrh a implementaci pro řešení hrozeb a aspektů řízení spojených s typickými scénáři sítí; a

d. řešení otázek spojených s implementací, provozem, monitorováním a přezkoumáváním kontrolních opatření bezpečnostních bran sítě.