ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Únor**
2019

Informační technologie – Bezpečnostní techniky – Bezpečnost sítě –
Část 6: Zabezpečení přístupu k bezdrátové IP síti

ČSN
ISO/IEC 27033-6

36 9701

Information technology – Security techniques – Network security –
Part 6: Securing wireless IP network access

Technologies de l,information – Techniques de sécurité – Sécurité de réseau –
Partie 6: Sécurisation de l,acces réseau IP sans fil

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-6:2016. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27033-6:2016. It was translated
by the Czech Agency for Standardization. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

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

ISO/IEC 27033-1 zavedena v ČSN ISO/IEC 27033-1 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 1: Přehled a pojmy

ISO/IEC 27033-2 zavedena v ČSN ISO/IEC 27033-2 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě

Vysvětlivky k textu převzaté normy

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

back-end, bluebugging, bluebumping, bluedumping, bluejacking, bluesmacking, bluesnarfing, bluestabbing,
Bluetooth, End-to-End, fuzzing, hotspot, malware, man-in-the-middle, peer-to-peer, per-hop, phishing, ping, ping of death, scrambling, source routing, spam, Warchalking, Wardriving, Warflying, Warwalking

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 6: Zabezpečení přístupu k bezdrátové IP síti

ISO/IEC 27033-6
První vydání
2016-06-01

ICS 35.030

Obsah

Strana

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 oborech společného zájmu. Práce se zúčastňují také další vládní i 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.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: Foreword – Supplementary information.

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

ISO/IEC 27033 se společným názvem *Informační technologie – Bezpečnostní techniky – Bezpečnost sítě* se
sestává z následujících 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 komunikací mezi sítěmi s využitím bezpečnostních bran*
- *Část 5: Zabezpečení komunikací napříč sítěmi použitím virtuálních privátních sítí (VPN)*
- *Část 6: Zabezpečení přístupu k bezdrátové IP síti*

Úvod

V dnešním světě má většina komerčních i vládních organizací své informační systémy propojené sítěmi, přičemž síťová propojení jsou jedním nebo více z následujících typů:

- v rámci organizace;
- mezi různými organizacemi;
- mezi organizací a širokou veřejností.

Dále, s rychlým vývojem veřejně dostupných síťových technologií (zejména s Internetem), nabízejících významné obchodní příležitosti, provádějí organizace stále častěji elektronické obchodování v celosvětovém měřítku a poskytují on-line veřejné služby. Mezi tyto příležitosti patří poskytování datových komunikací s nižšími náklady, využívajících jednoduše Internet jako globální propojovací médium, a dále i propracovanější služby poskytované poskytovateli internetových služeb (ISP). To může znamenat použití od relativně levných místních připojovacích bodů na každém konci okruhu až k plnohodnotným systémům on-line elektronického obchodování a poskytování služeb s využitím webových aplikací a služeb. Kromě toho nová technologie (včetně integrace dat, hlasu a videa) zvyšuje možnosti práce na dálku (také známé jako „práce z domova“), které zaměstnancům umožňují pracovat daleko od základního místa vykonávání práce po významně delší dobu. Jsou schopni být v kontaktu prostřednictvím použití vzdálených zařízení pro přístup k sítím organizace a komunitním sítím a souvisícím informacím a službám pro podporu podnikatelské činnosti.

Nicméně přestože toto prostředí umožňuje významné podnikatelské výhody, přináší nová bezpečnostní rizika, která je třeba řídit. Vzhledem k tomu, že organizace k provozování své podnikatelské činnosti silně spoléhají na používání informací a přidružených sítí, ztráta důvěrnosti, integrity a dostupnosti informací a služeb by mohla mít významné nepříznivé dopady na podnikatelské činnosti. Je zde tedy zásadní požadavek na patřičnou ochranu sítí a souvisících informačních systémů a informací. Jinými slovy, *zavedení a udržování přiměřené bezpečnosti sítě je naprosto zásadní pro úspěch podnikatelských činností kterékoli organizace*.

V tomto kontextu se odvětví telekomunikací a informačních technologií snaží hledat nákladově efektivní komplexní bezpečnostní řešení zaměřená na ochranu sítí před škodlivými útoky a neúmyslnými nesprávnými akcemi, která splňují podnikatelské požadavky na důvěrnost, integritu a dostupnost informací a služeb. Zabezpečení sítě je také podle potřeby nezbytné pro zachování přesnosti fakturačních údajů nebo informací o používání. Bezpečnostní schopnosti produktů jsou zásadní pro celkovou bezpečnost sítě (včetně aplikací a služeb). Nicméně v případě kombinace více produktů k poskytnutí úplných řešení bude úspěšnost řešení určovat interoperabilita nebo její nedostatek. Bezpečnost by neměla být pouze záležitostí týkající se jednotlivého produktu nebo služby, ale měla by být rozvíjena způsobem, který podporuje úzké propojování bezpečnostních schopností do celkového řešení bezpečnosti.

Účelem ISO/IEC 27033 je poskytnout podrobné pokyny týkající se aspektů bezpečnosti správy, provozu a používání sítí informačních systémů a jejich vzájemného propojení. Jednotlivé osoby v rámci organizace, které jsou odpovědné za bezpečnost informací obecně, a zejména bezpečnost sítě, by měly být schopny přizpůsobit obsah tohoto dokumentu tak, aby byly splněny jejich specifické požadavky. Jeho hlavní cíle jsou následující.

- cílem ISO/IEC 27033-1 je definovat a popsat koncepce spojené s bezpečností sítě a poskytnout pokyny pro řízení bezpečností sítě. To zahrnuje poskytnutí přehledu bezpečnosti sítě

a souvisících definic, a pokyny pro identifikaci a analýzu rizik bezpečnosti sítě a následné definování požadavků na bezpečnost sítě. Rovněž uvádí, jak dosáhnout kvalitních architektur technické bezpečnosti a aspekty rizik, návrhu a řízení spojených s typickými síťovými scénáři a oblastmi síťových technologií (které jsou podrobněji řešeny v následujících částech ISO/IEC 27033).

- cílem ISO/IEC 27033-2 je definovat, jak by organizace měly dosahovat kvalitních architektur, návrhů a implementací technické bezpečnosti sítě, které zajistí bezpečnost sítě odpovídající jejich podnikatelskému prostředí, a to za použití konzistentního přístupu k plánování, návrhu a implementaci bezpečnosti sítě, pomocí použití modelů/rámců (v tomto kontextu se model/rámec používá k nastínění reprezentace nebo popisu struktury a obecnější úrovně fungování typu architektury/návrhu technické bezpečnosti) a je relevantní pro všechny pracovníky podílející se na plánování, návrhu a implementaci aspektů architektury bezpečnosti sítě (například pro síťové architekty a projektanty, správce sítě a vedoucí pracovníky bezpečnosti sítě).

- ISO/IEC 27033-3 se zaměřuje na definování specifických rizik, technik návrhu a záležitostí řízení spojených s typickými síťovými scénáři. Je relevantní pro všechny pracovníky, kteří se podílejí na plánování, návrhu a implementaci aspektů architektury bezpečnosti sítě (například pro síťové architekty a projektanty, správce sítě a vedoucí pracovníky bezpečnosti sítě).

- ISO/IEC 27033-4 se zaměřuje na definování specifických rizik, technik návrhu a záležitostí řízení pro zabezpečení toků informací mezi sítěmi používajícími bezpečnostní brány. Je relevantní pro všechny pracovníky, kteří se podílejí na podrobném plánování, návrhu a implementaci bezpečnostních bran (například pro síťové architekty a projektanty, správce sítě a vedoucí pracovníky bezpečnosti sítě).

- ISO/IEC 27033-5 se zaměřuje na definování specifických rizik, technik návrhu a záležitostí řízení pro zabezpečení připojení, vytvářených pomocí virtuálních privátních sítí (VPN). Je relevantní pro všechny pracovníky, kteří se podílejí na podrobném plánování, návrhu a implementaci zabezpečení VPN (například pro síťové architekty a projektanty, správce sítě a vedoucí pracovníky bezpečnosti sítě).

- ISO/IEC 27033-6 se zaměřuje na definování specifických rizik, technik návrhu a záležitostí řízení pro zabezpečení bezdrátových IP sítí. Je relevantní pro všechny pracovníky, kteří se podílejí na podrobném plánování, návrhu a implementaci bezpečnosti pro bezdrátové sítě (například pro síťové architekty a projektanty, správce sítě a vedoucí pracovníky bezpečnosti sítě).

Je třeba zdůraznit, že ISO/IEC 27033 poskytuje další podrobné pokyny pro implementaci opatření bezpečnosti sítě, které jsou popsány na základní normalizované úrovni v ISO/IEC 27002.

Je třeba poznamenat, že tato část ISO/IEC 27033 není referenčním nebo normativním dokumentem pro regulatorní a legislativní požadavky na bezpečnost. Ačkoli zdůrazňuje významnost těchto vlivů, nemůže je konkrétně stanovit, protože jsou závislé na zemi, druhu podnikání atd.

Není-li v této části ISO/IEC 27033 uvedeno jinak, jsou zmiňované pokyny platné pro současné a/nebo plánované sítě, ale budou odkazovat pouze na „sítě“ nebo „síť“.

1 Předmět normy

Tato část ISO/IEC 27033 popisuje hrozby, požadavky bezpečnosti, opatření bezpečnosti a techniky návrhu týkající se bezdrátových sítí. Poskytuje směrnice pro výběr, implementaci a monitorování technických opatření potřebných pro zajištění bezpečné komunikace pomocí bezdrátových sítí. Informace v této části ISO/IEC 27033 jsou určeny k použití při přezkoumávání nebo výběru voleb architektury/návrhu technické bezpečnosti, které zahrnují použití bezdrátové sítě v souladu s ISO/IEC 27033-2.

Celkově bude ISO/IEC 27033-6 výrazně napomáhat komplexní definici a implementaci bezpečnosti pro prostředí bezdrátových sítí jakékoli organizace. Je určena uživatelům a implementátorům, kteří jsou odpovědní za implementaci a údržbu technických opatření nezbytných pro zajištění bezpečných bezdrátových sítí.