ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen 2016**

Informační technologie – Bezpečnostní techniky –
Bezpečnost sítě –
Část 1: Přehled a pojmy

ČSN
ISO/IEC 27033-1
36 9701

Information Technology – Security techniques – Network security –
Part 1: Overview and concepts

Technologies de l,information – Techniques de sécurité – Sécurité de réseau –
Partie 1: Vue d,ensemble et concepts

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-1:2015. 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 27033-1:2015. 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 7498-1 dosud nezavedena

ISO 7498-2 zavedena v ČSN ISO 7498-2 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ISO/IEC 7498-3 zavedena v ČSN ISO/IEC 7498-3 (36 9614) Informační technologie – Propojení otevřených systémů – Základní referenční model: Pojmenování a adresování

ISO/IEC 7498-4 zavedena v ČSN ISO/IEC 7498-4 (36 9617) Systémy na spracovanie informácií. Prepojenie
otvorených systémov (OSI). Základný referenčný model. Časť 4: Základná štruktúra spracovania

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

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

ISO/IEC 27005 zavedena v ČSN ISO/IEC 27005:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Souvisící ČSN

ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů: Přehled

ČSN ISO/IEC 27003 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systémů řízení bezpečnosti informací

ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

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:

chat, end-to-end, extranet, firewall, helpdesk, hub, man in the broker, man in the middle, malware, port, router, spam, spyware, 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 27033-1
Bezpečnost sítě – Druhé vydání
Část 1: Přehled a pojmy 2015-08-15

ICS 35.040

Obsah

Strana

ISO copyright office

Ch. de Blandonnet 8 · CP 401

CH-1214 Vernier, Geneva, Switzerland

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

copyright@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.

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 poroznost 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 nelze činit odpovědnou 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*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27033-1:2009), 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*

Úvod

V dnešním světě má většina komerčních i státních organizací své informační systémy propojeny sítěmi (viz obrá-
zek 1), přičemž síťová propojení představují jedno nebo více z následujících:

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

Obrázek 1 – Obecné typy síťových propojení

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 na dálku“ nebo „práci z domova“), která umožňuje personálu značnou dobu pracovat mimo své základní pracoviště. Jsou schopni být v kontaktu prostřednictvím zařízení pro dálkový přístup k organizaci a komunitním sítím a souvisícím informacím a službám podporujícím podnikání.

Nicméně zatímco toto prostředí podporuje významné podnikatelské výhody, jsou zde nová bezpečnostní rizika, která je třeba řídit. Pokud organizace ve značné míře spoléhají na používání informací a souvisících 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 souvisící informační systémy a informace. Jinými slovy: *zavedení a udržování odpovídající bezpečnosti sítě je naprosto 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 zachování přesnosti účtování nebo vhodném používání informací. 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 této mezinárodní normy je poskytnout podrobné pokyny ohledně bezpečnostních aspektů řízení, provozu a používání sítí informačních systémů a jejich vzájemných propojení. Ti jedinci v organizaci, kteří jsou obecně odpovědni za bezpečnost informací, a zvláště sítí, by měli být schopni přizpůsobit látku obsaženou v této mezinárodní normě tak, aby splnila jejich specifické požadavky. Hlavní cíle normy jsou následující.

- ISO/IEC 27033-1, definovat a popsat pojetí spojená s bezpečností sítě a poskytnout pokyny pro správu/řízení bezpečnosti sítě. To zahrnuje poskytnutí přehledu o bezpečnosti sítí a souvisících definic, a pokyny jak identifikovat a analyzovat rizika bezpečnosti sítě a následně definovat požadavky na bezpečnost sítě. Rovněž uvádí, jak dosáhnout dobré kvality architektury technické bezpečnosti, a aspekty rizika, návrhu a řízení spojené s typickými scénáři sítí a oblastmi síťových „technologií“ (které jsou podrobně řešeny v dalších částech ISO/IEC 27033).

- ISO/IEC 27033-2, definovat, jak by měly organizace dosáhnout kvalitních architektur, návrhů a implementací technické bezpečnosti sítě, které zajistí bezpečnost sítě přiměřenou k podnikatelskému prostředí organizace, s použitím konzistentního přístupu k plánování, návrhu a implementaci bezpečnosti sítě, dle závažnosti, podporovaného použitím modelů/rámců (v tomto kontextu se model/rámec používá k nastínění reprezentace nebo popisu ukazujících strukturu a obecnější fungování typu architektury/návrhu technické bezpečnosti), a je relevantní pro všechny pracovníky, kteří jsou zapojeni do plánování, navrhování a implementaci aspektů architektury bezpečnosti sítě (např. architekti a projektanti sítí, správci sítí a řídící pracovníci síťové bezpečnosti).

- ISO/IEC 27033-3, definovat konkrétní rizika, techniky návrhu a problémy řízení souvisící s typickými síťovými scénáři. Norma je relevantní pro všechny pracovníky, kteří jsou zapojeni do plánování, navrhování a implementaci aspektů architektury bezpečnosti sítě (např. architekti a projektanti sítí, správci sítí a řídící pracovníci síťové bezpečnosti).

- ISO/IEC 27033-4, definovat konkrétní rizika, techniky návrhu a problémy řízení pro zabezpečení toků informací mezi sítěmi s využitím bezpečnostních bran. Norma je relevantní pro všechny pracovníky, kteří jsou zapojeni do podrobného plánování, navrhování a implementaci bezpečnostních bran (např. architekti a projektanti sítí, správci sítí a řídící pracovníci síťové bezpečnosti).

- ISO/IEC 27033-5, definovat konkrétní rizika, techniky návrhu a problémy řízení pro zabezpečení propojení, která jsou ustavena s využitím virtuálních privátních sítí (VPN). Norma je relevantní pro všechny pracovníky, kteří jsou zapojeni do podrobného plánování, navrhování a implementaci bezpečnosti VPN (např. architekti a projektanti sítí, správci sítí a řídící pracovníci síťové bezpečnosti).

- ISO/IEC 27033-6, definovat konkrétní rizika, techniky návrhu a problémy řízení pro zabezpečení bezdrátových IP sítí. Norma je relevantní pro všechny pracovníky, kteří jsou zapojeni do podrobného plánování, navrhování a implementaci bezpečnosti bezdrátových sítí (např. architekti a projektanti sítí, správci sítí a řídící pracovníci síťové bezpečnosti).

Je třeba zdůraznit, že tato mezinárodní norma poskytuje další podrobný návod implementace kontrolních opatření bezpečnosti sítě, které jsou popsány na základní standardizované úrovni v ISO/IEC 27002.

Je třeba poznamenat, že tato mezinárodní norma není referenčním nebo normativním dokumentem pro regulatorní a legislativní požadavky na bezpečnost. Ačkoli norma zdůrazňuje význam těchto vlivů, nemůže je konkrétně uvádět, protože jsou závislé na zemi, typu podnikání atd.

Pokud není uvedeno jinak, návody odkazované v této části ISO/IEC 27033 se vztahují na aktuální a/nebo plánované sítě, ale bude na ně odkazováno jen jako na „sítě“ nebo „síť“.

1 Předmět normy

Tato část ISO/IEC 27033 poskytuje přehled o bezpečnosti sítě a souvisících definic. Definuje a popisuje pojmy spojené s bezpečností sítě a poskytuje návod na správu/řízení bezpečnosti sítě. (Bezpečnost sítě se vztahuje na bezpečnost zařízení, bezpečnost činností týkajících se správy/řízení zařízení, na aplikace/služby a na koncové uživatele, kromě bezpečnosti informací přenášených přes komunikační linky.)

Tato část je relevantní pro každý subjekt, který vlastní síť nebo ji provozuje nebo ji používá. To zahrnuje vysoce postavené manažery a jiné netechnické manažery nebo uživatele, navíc k manažerům a administrátorům, kteří mají konkrétní odpovědnosti za bezpečnost informací a/nebo bezpečnost sítě, provozování sítě, nebo kteří jsou odpovědní za celkový program bezpečnosti a rozvoj politiky bezpečnosti organizace. Je také relevantní pro každý subjekt zapojený do plánování, navrhování a implementaci aspektů architektury bezpečnosti sítě.

Tato část ISO/IEC 27033 rovněž zahrnuje následující:

- poskytuje návod, jak identifikovat a analyzovat rizika bezpečnosti sítě a definici požadavků na bezpečnost sítě na základě této analýzy,
- poskytuje přehled opatření, která podporují technické architektury bezpečnosti sítě a souvisící technická opatření, stejně jako ta netechnická opatření a technická opatření, která jsou použitelná nejen pro sítě,
- představuje, jak dosáhnout kvalitních technických architektur bezpečnosti sítě, a aspekty rizik, navrhování
  a řízení spojené s typickými scénáři sítí a oblastmi „technologií“ sítí (které jsou podrobně řešeny v dalších částech ISO/IEC 27033), a stručně se zabývá otázkami spojenými s implementací a provozováním opatření síťové bezpečnosti a průběžným monitorováním a přezkoumáváním jejich implementace.

Celkově poskytuje přehled o této mezinárodní normě a „cestovní mapu“ pro všechny ostatní části.