

Informační technologie - Bezpečnostní techniky -

Bezpečnost sítě -

Část 5: Zabezpečení komunikace napříč sítěmi použitím virtuálních privátních sítí (VPN)

ČSN

ISO/IEC 27033-5

36 9701

Information technology - Security techniques - Network security -

Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

Technologies de l'information - Techniques de sécurité - Sécurité de réseau -

Partie 5: Sécurité des communications au travers des réseaux utilisant des réseaux privés virtuels (VPNs)

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-5:2013. 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 27033-5:2013. 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 27001:2005 nezavedena1)

ISO/IEC 27002:2005 nezavedena2)

ISO/IEC 27005:2011 zavedena v ČSN ISO/IEC 27005:2013 (36 9790) Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací

ISO/IEC 27033-1:2009 nezavedena

Související ČSN

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

ČSN ISO/IEC 27033-3 (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:

point-to-cloud, point-to-point, man-in-the-middle, web hosting, firewall

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 27033-5

Bezpečnost sítě - První vydání

Část 5: Zabezpečení komunikace napříč sítěmi použitím 2013-08-01
virtuálních privátních sítí (VPN)

ICS 35.040

Obsah

Strana

Předmluva 5

1 Předmět normy 6

2 Citované dokumenty 6

3 Termíny a definice 6

4 Zkratky 6

5 Struktura dokumentu 7

6 Přehled 7

6.1 Úvod 7

6.2 Typy VPN 8

7 Bezpečnostní hrozby 8

8 Bezpečnostní požadavky 9

8.1 Přehled 9

8.2 Důvěrnost 9

8.3 Integrita 10

8.4	Autenticita	10
8.5	Autorizace	10
8.6	Dostupnost	10
8.7	Bezpečnost koncových bodů tunelu	10
9	Bezpečnostní opatření	10
9.1	Bezpečnostní aspekty	10
9.2	Virtuální okruhy	10
10	Techniky návrhu	11
10.1	Přehled	11
10.2	Regulatorní a legislativní aspekty	11
10.3	Aspekty správy a řízení VPN	12
10.4	Architektonické aspekty VPN	12
10.4.1	Přehled	12
10.4.2	Bezpečnost koncových bodů	12
10.4.3	Bezpečnost zakončení	13
10.4.4	Ochrana proti škodlivému softwaru	13
10.4.5	Autentizace	13
10.4.6	System detekce a prevence průniku (IPDS)	13
10.4.7	Bezpečnostní brány	13
10.4.8	Návrh sítě	13
10.4.9	Další připojení	14
10.4.10	Rozdělené tunelování	14
10.4.11	Auditní záznamy a monitorování sítě	14
10.4.12	Správa technických zranitelností	14
10.4.13	Šifrování trasy veřejnými sítěmi	14
10.5	Technické úvahy týkající se VPN	14
10.5.1	Základní informace	14

10.5.2	Správa VPN zařízení	15
10.5.3	Monitorování bezpečnosti VPN	15
11	Zásady pro výběr produktu	15
11.1	Volba nosného protokolu	15
11.2	VPN zařízení	15
	Bibliografie	16



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2013

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

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 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 jakéhokoli nebo všech patentových práv.

ISO/IEC 27033 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*,

subkomise SC 27 *IT Bezpečnostní techniky*.

Toto první vydání zrušuje a nahrazuje ISO/IEC 18028-5:2006, která byla technicky revidována.

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

- *Část 1: Přehled a pojetí*
- *Část 2: Směrnice pro návrh a implementaci zabezpečení sítí*
- *Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení*
- *Část 4: Zabezpečení komunikací mezi sítěmi s využitím bezpečnostních bran*
- *Část 5: Zabezpečení komunikace napříč sítěmi použitím virtuálních privátních sítí (VPN)*
- *Část 6: Zabezpečení přístupu k bezdrátové IP síti*

(Je nutné poznamenat, že mohou existovat další části. Příklady možných témat pro další části zahrnují lokální sítě, rozlehlé sítě, širokopásmové sítě, web hostingy, internetové e-maily a směrovaný přístup k organizacím třetích stran. Hlavními kapitolami všech těchto částí by měla být rizika, techniky návrhu a problematika řízení.)

1 Předmět normy

Tato část ISO/IEC 27033 poskytuje směrnice pro výběr, implementaci a monitorování technických opatření nezbytných k zajištění bezpečnosti sítě použitím virtuálních privátních sítí (VPN) k propojení sítí a připojení vzdálených uživatelů k sítím.

Konec náhledu - text dále pokračuje v placené verzi ČSN.