ČESKÁ TECHNICKÁ NORMA

ICS 35.030

Únor 2026

Informační technologie – Bezpečnost sítě – Část 7: Směrnice pro bezpečnost virtualizace sítě

ČSN ISO/IEC 27033-7

36 9701

Information technology – Network security – Part 7: Guidelines for network virtualization security

Technologies de l,information – Sécurité des réseaux – Partie 7: Lignes directrices pour la sécurité de la virtualisation des réseaux

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-7:2023. 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 27033-7:2023. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN EN ISO/IEC 27017 (36 9710) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

ČSN EN ISO/IEC 27018 (36 9709) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

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

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 této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných

evropských/mezinárodních norem (včetně všech změn).

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:

botnet, anti-botnet, docker, kubernetes, white-box.

Vypracování normy

Zpracovatel odborného překladu: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

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 – Bezpečnost sítě –
Část 7: Směrnice pro bezpečnost virtualizace sítě

ISO/IEC 27033-7
První vydání
2023-11

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.

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. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives nebo www.iec.ch/members_experts/refdocs).

ISO a IEC upozorňují na možnost, že implementace tohoto dokumentu smí vyžadovat využití patentu (patentů). V souvislosti s tím ISO a IEC nezaujímají žádné stanovisko týkající se důkazů, platnosti nebo použitelnosti všech uplatňovaných patentových práv. Ke dni zveřejnění tohoto dokumentu ISO a IEC neobdržely oznámení o patentu (patentech), který smí být vyžadován pro implementaci tohoto dokumentu. ISO a IEC však upozorňují implementující organizace, že se nemusí jednat o nejnovější informace, které lze získat z databáze patentů dostupné na adresách www.iso.org/patents a https://patents.iec.ch. ISO a IEC nelze činit odpovědné za identifikaci jakéhokoliv nebo všech takových patentových práv.

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

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí*.

Seznam všech částí souboru ISO/IEC 27033 lze nalézt na webových stránkách ISO a IEC.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adresách www.iso.org/members.html a www.iec.ch/national-committees.

Úvod

Účelem tohoto dokumentu je zabývat se klíčovými výzvami a riziky bezpečnosti virtualizace sítě. Virtualizace sítě zahrnuje infrastrukturu virtuální sítě, virtuální síťovou funkci, virtuální řízení a management zdrojů. Cílem tohoto dokumentu je:

1) identifikovat bezpečnostní rizika virtualizace sítě;

2) navrhnout model bezpečnosti virtualizace sítě;

3) navrhnout bezpečnostní směrnice pro infrastrukturu virtuální sítě, virtuální síťovou funkci, virtuální řízení a mana-
gement zdrojů.

Tento dokument má za cíl pomoci zúčastněným stranám pochopit hlavní charakteristiky bezpečnosti virtualizace sítě. Tento dokument může například pomoci dodavatelům softwaru a hardwaru bezpečně navrhovat a vyvíjet produkty, které implementují virtualizaci sítě, a provozovatelům pomoci vyhodnotit bezpečnost těchto produktů a bezpečně je nasadit pro síťové služby. Navržením bezpečnostních směrnic si tento dokument klade za cíl pomoci odvětví zlepšit bezpečnost systémů, které jsou postaveny na technologii virtualizace sítě.

Cílovou skupinou mohou být dodavatelé síťových zařízení, provozovatelé sítí, poskytovatelé internetových služeb a poskytovatelé softwarových služeb.

S rychlým rozvojem IT technologií, jako je cloud computing, se IT systémy a komunikační systémy s přijetím virtualizačních technologií stále více vyvíjejí. Virtualizace umožňuje systémům vysokou agilitu, flexibilitu a škálovatelnost s nízkými náklady, ale zároveň přináší řadu bezpečnostních výzev.

1 Předmět normy

Tento dokument si klade za cíl identifikovat bezpečnostní rizika virtualizace sítě a navrhnout směrnice pro implementaci bezpečnosti virtualizace sítě.

Celkově má tento dokument významně napomoci komplexní definici a implementaci bezpečnosti všech virtualizačních prostředí organizace. Je určen uživatelům a implementátorům, kteří jsou zodpovědní za implementaci a údržbu technických opatření potřebných k zajištění bezpečných virtualizačních prostředí.