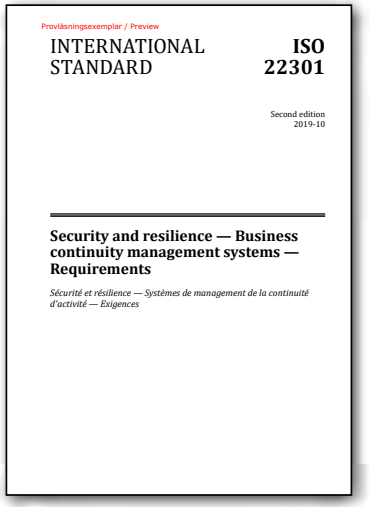
Aktuální normy a publikace o bezpečnosti


Provläsningsexemplar / Preview

INTERNATIONAL STANDARD **ISO 22301**

Second edition 2019-10

Security and resilience — Business continuity management systems — Requirements

Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences

Nová verze ISO 22301

Dne 31. října 2019 byla publikována revidovaná verze normy *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements*. Norma obsahuje povinné požadavky pro zavedení, provozování, udržování a kontinuální zlepšování systému řízení kontinuity činností (BCMS). Na to, že se jedná o revizi po sedmi letech, nejsou změny oproti předchozí verzi z roku 2012 nijak převratné. Mezi ty hlavní patří nově přidaná kapitola 6.3 (plánování změn v BMCS), předělaná kapitola 8 (hodnocení dopadů a rizik, BCM strategie, BC plány a cvičení), změny v povinné dokumentaci. Očekává se, že přechodné období bude nastaveno na tři roky, tedy do 30. 10. 2022.

https://www.iso.org/


NIST SPECIAL PUBLICATION 1800-23

Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

James McCarthy
Glen Joy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Lauren Acierto
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urbaub
John Wiltberger
Devin Wynne
The MITRE Corporation
McLean, Virginia

DRAFT

September 2019

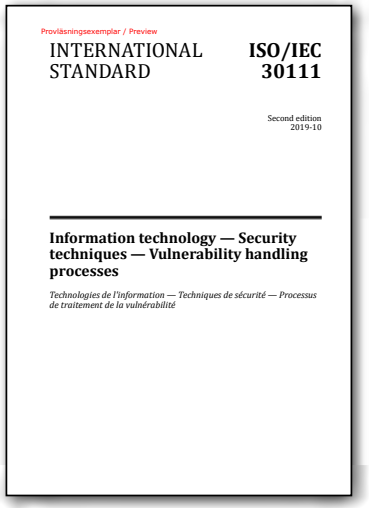
U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Řízení aktiv v energetice

Zářijový NIST *SP 1800-23 Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry (Draft)* je praktický průvodce, který má za cíl zefektivnit možnosti správy aktiv (hardwarových a softwarových) provozních technologií (Operational Technologies, OT) v energetickém sektoru. Doporučení zahrnují přístup k identifikaci nově připojených aktiv a mapování jejich atributů (výrobce, OS, MAC apod.), hodnocení souvisejících rizik, kontinuální monitoring stavu aktiv, alerty v případě připojení či odpojení aktiv. Standard také zahrnuje referenční návrh implementace, k čemuž používá komerčně dostupné technologie k vytvoření vzorového řešení, které pomůže organizacím v rámci energetiky řešit bezpečnostní výzvy při správě OT aktiv.

https://csrc.nist.gov/publications/sp800


Provläsningsexemplar / Preview

INTERNATIONAL STANDARD **ISO/IEC 30111**

Second edition 2019-10

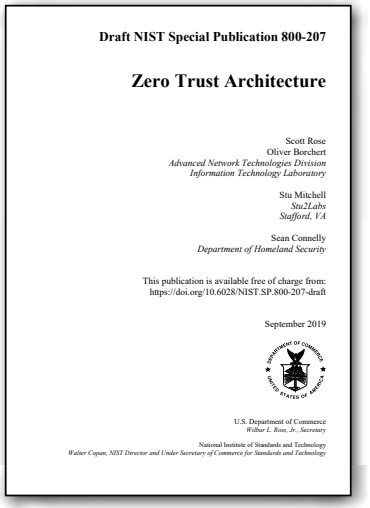
Information technology — Security techniques — Vulnerability handling processes

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

Řešení hlášených zranitelností

Další revidovanou normou je *ISO/IEC 30111:2019 Information technology – Security techniques – Vulnerability handling processes*. Norma obsahuje požadavky a doporučení pro to, jak zpracovat a odstranit potenciální zranitelnosti v dodávaných produktech nebo službách. Dokument se zabývá nastavením procesu přijetí a prověření interně nebo externě nahlášených potenciálních zranitelností, jejich potvrzením a klasifikací, návrhem a implementací nápravných opatření. Norma je určena pro obchodníky, spotřebitele a vývojáře, jako benchmark k nastavení procesu řízení zranitelností. Norma je úzce propojena s postupy popsanými v ISO/IEC 29147 (doporučení k identifikace zranitelností produktů a služeb).

https://www.iso.org/


Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Advanced Network Technologies Division
Information Technology Laboratory

Stu Mitchell
Stu2Labs
Stafford, VA

Sean Connelly
Department of Homeland Security

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

September 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Architektura s nulovou důvěrou

NIST *SP 800-207 Zero Trust Architecture (ZTA)* opravuje model architektury s nulovou důvěrou. Model nulové důvěry (Zero Trust) je založený na principu nikomu nedůvěřovat, ať jde o interní nebo externí osobu. V rámci tohoto modelu je přístup k datům a aplikacím umožněn pouze na základě explicitního povolení pouze autorizovaným a ověřeným uživatelům. Veškeré přístupy jsou prověřovány a plně logovány. ZTA je odpovědí na nové trendy, které zahrnují vzdálené uživatele a cloudová aktiva. Zaměřuje se na ochranu zdrojů, nikoli síťových segmentů, protože umístění sítě již není považováno za rozhodující kritérium zabezpečení zdroje. Dokument uvádí obecné modely nasazení a případy použití, kde by architektura s nulovou důvěrou mohla zvýšit celkovou bezpečnost podniku.

https://csrc.nist.gov/publications/sp800

Ing. Libor Široký, CISM, CRISC, AMBCI, *siroky@rac.cz*