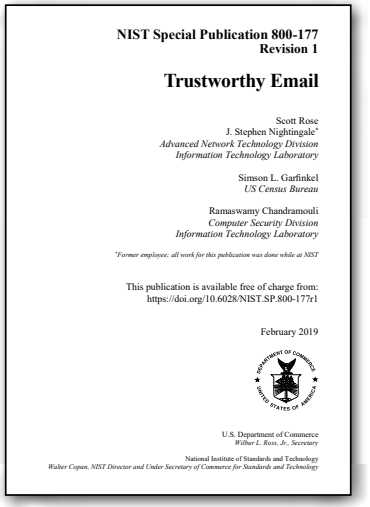
Aktuální normy a publikace o bezpečnosti

Ochrana osobních údajů v cloudu

V lednu publikované druhé vydání normy *ISO/IEC 27018:2019 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* dává doporučení na ochranu osobních údajů založené na normě ISO/IEC 27002. Norma interpretuje opatření ISO/IEC 27002 pro prostředí cloudu a měla by tak poskytnout podporu při implementaci systému řízení bezpečnosti informací v prostředí poskytovatelů veřejných cloudových služeb. Obsažená doporučení jsou zároveň relevantní pro zákazníky cloudových služeb, kteří vystupují v roli správců osobních údajů. Jednotlivá organizační a technická opatření umožní organizacím zajistit ochranu citlivých údajů svých klientů v souladu s principy normy ISO/IEC 29100.

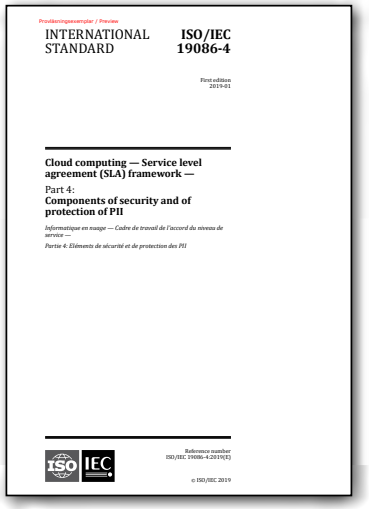
https://www.iso.org/



Důvěryhodný email

V únoru publikovaný standard *SP 800-177 Rev. 1 Trustworthy Email* poskytuje doporučení pro zabezpečení a celkové zvýšení důvěryhodnosti elektronické pošty. Primárně je určen administrátorům, síťovým správcům a specialistům na bezpečnost informací. Technologie doporučené pro podporu základního protokolu SMTP a DNS zahrnují mechanismy pro autentizaci odesílající domény: technologie ověřující odesílající server (SPF), standard využívající elektronický podpis pro ověření původu emailu (DKIM) a DMARC, který navazuje na SPF a DKIM při ověřování důvěryhodnosti zprávy. Doporučení pro zabezpečení přenosu emailů zahrnují TLS a související ověřování certifikátů. Doporučení pro zabezpečení emailového obsahu zahrnují end-to-end šifrování, ověřování obsahu zpráv a využití dalších služeb protokolu S/MIME.

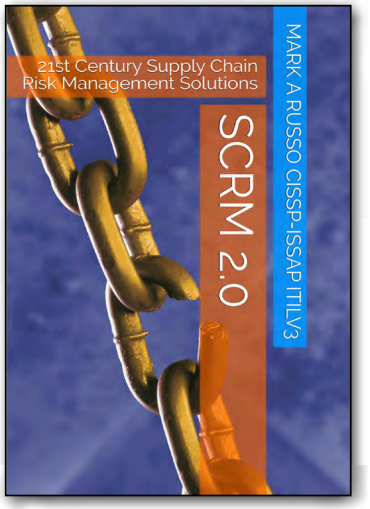
https://csrc.nist.gov/publications/sp800



SLA cloudových služeb

ISO/IEC 19086-4:2019 Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII specifikuje požadavky a doporučení pro nastavení klíčových komponent dohod o úrovni cloudových služeb (cloud SLA). Těmi jsou Service Level Objectives (SLO) a Service Quality Objectives (SQO). SLO poskytují kvantitativní prostředky k definování úrovně služeb, které zákazník cloudu může od poskytovatele očekávat. Jsou to specifické měřitelné charakteristiky SLA, jako je dostupnost, propustnost, doba odezvy atd. Mohou se skládat z jednoho nebo více měření kvality služby (SQO). V souboru norem zaměřených na SLA cloudových služeb byly od roku 2016 již vydány: *Part 1: Overview and concepts, Part 2: Metric model, Part 3: Core conformance requirements*.

https://www.iso.org/



Rizika dodavatelského řetězce

Kniha *SCRM 2.0: 21st Century Supply Chain Risk Management Solutions* je zaměřená na řízení rizik v dodavatelských řetězcích. Poskytuje doporučení pro identifikaci, hodnocení a pokrytí rizik v řetězci dodavatelů. Staví na základních konceptech standardů *NIST SP 800-30 (Risk Assessments)*, *NIST SP 800-161 (Supply Chain Risk Management)*, rozsáhlý katalog bezpečnostních opatření vychází z *NIST 800-53 (Security and Privacy Controls)*. Zatímco SCRM 1.0 je koncept zavedení efektivního a opakovatelného procesu, který lze aplikovat proti standardním aktivům dodavatelského řetězce, jako je hardware, firmware, software atd. SCRM 2.0 je zaměřený přímo na službu a její komponenty, které zahrnují výrobce, distributory, zpracovatele a další účastníky v celém dodavatelském řetězci a s nimi spojená rizika.

https://www.amazon.com/

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