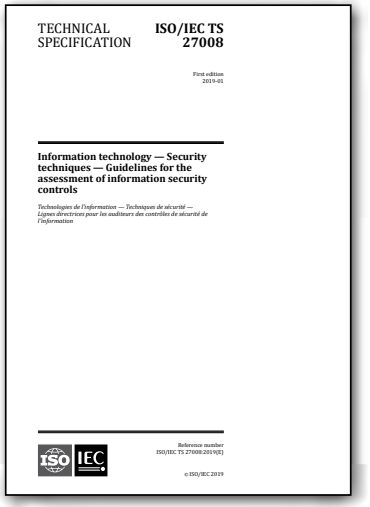
Aktuální normy a publikace o bezpečnosti

Řízení IT aktiv

Řízení aktiv je základem efektivní strategie kybernetické bezpečnosti, zcela logicky tak patří mezi top 20 kritických opatření publikovaných institutem SANS. *NIST SPECIAL PUBLICATION 1800-5 IT Asset Management* obsahuje doporučení pro efektivní monitoring a správu aktiv v oblasti informačních technologií s využitím open source a komerčních produktů. Cílem je propojit fyzická a virtuální aktiva a poskytnout tak organizaci úplný obraz o tom, kde a jak jsou jednotlivé prostředky využívány, což vede k jejich lepšímu využití a současně zvýšení kybernetické bezpečnosti. Standard je součástí rámce pro zvyšování úrovně kybernetické bezpečnosti kritické infrastruktury (Framework for Improving Critical Infrastructure Cybersecurity). Jde o soubor doporučení k ochraně informací a aktiv proti kybernetickým hrozbám, určený provozovatelům kritické infrastruktury.

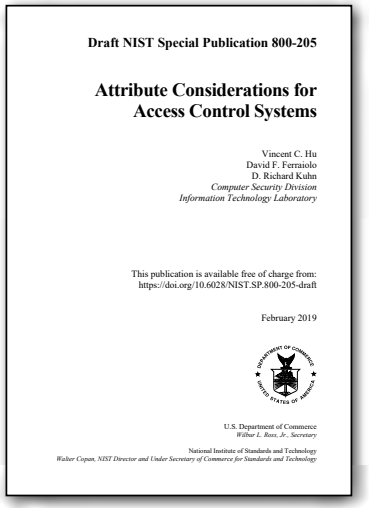
http://csrc.nist.gov/publications/



Audit opatření ISO/IEC 27001

ISO/IEC TS 27008:2019 Information technology – Security techniques – Guidelines for the assessment of information security controls je první letošní novinkou z rodiny norem 27k. Norma obsahuje doporučení jak kontrolovat opatření bezpečnosti informací, která jsou implementována a provozována v rámci zavedeného systému řízení bezpečnosti informací dle normy ISO/IEC 27001. Poskytuje metodický návod k přezkoumání a hodnocení zavedených bezpečnostních opatření z přílohy A ISO/IEC 27001, respektive normy ISO/IEC 27002. Včetně posouzení souladu organizačně-technických opatření s požadavky stanovenými organizací a kontroly technické shody s hodnotícími kritérii založenými na požadavcích bezpečnosti informací dané organizace. Příloha C normy je zaměřena na kontrolu bezpečnostních opatření normy ISO/IEC 27017 v prostředí cloudu.

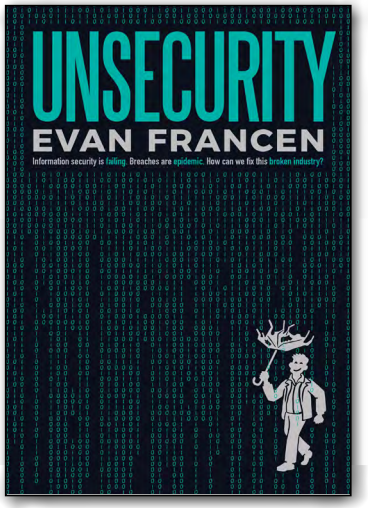
https://www.iso.org/



Řízení přístupů přes atributy

NIST *Special Publication 800-205 (draft) Attribute Considerations for Access Control Systems* poskytuje doporučení pro implementaci a vyhodnocování atributů používaných v rámci řízení přístupu z pohledu základních bezpečnostních vlastností. Publikace navazuje na NIST SP 800-162, který definoval řízení přístupu založené na atributech, neobsahoval však detailnější návod pro nastavení jednotlivých atributů. ABAC (Attribute Based Access Control) je model řízení logického přístupu založený na vyhodnocení atributů subjektu (např. jméno, oddělení, pracovní skupina, certifikace, IP adresa apod.) a objektu (např. autor, datum a čas vytvoření dokumentu) a jejich porovnáním s nastavenými pravidly řízení přístupu (kombinace atributů a povolené operace nad objekty).

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



(Ne)bezpečnost

Obor informační bezpečnosti je nemocný, protože nemluvíme stejným jazykem, tak to alespoň tvrdí autor knihy *Unsecurity: Information security is failing. Breaches are epidemic. How can we fix this broken industry?* Vychází přitom z toho, že v oblasti komunikace existují tři hlavní oblasti problémů: 1. profesionálové v rámci bezpečnostní komunity nesdílí společný jazyk, 2. bezpečnostní komunita nemluví stejným jazykem, jako běžní lidé, 3. jednotlivé organizace často mluví různým jazykem při pojmenování stejných aspektů bezpečnosti. V odvětví informační bezpečnosti jsme dle autora stále v období divokého západu. Neexistuje jednotný standard, namísto toho máme pro stejnou oblast tisíce různých standardů a doporučení (ISO 27k, NIST, COBIT, CIS, ITIL atd.), nemáme centrální profesní sdružení. Pojmenovává i další oblasti problémů a nastiňuje možnosti řešení.

https://www.amazon.com/

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