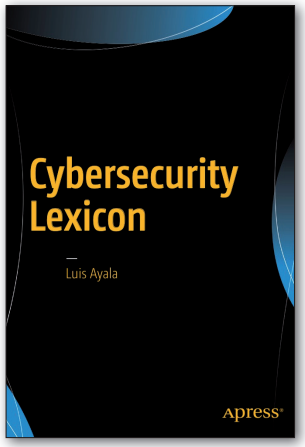
Aktuální normy a publikace o bezpečnosti

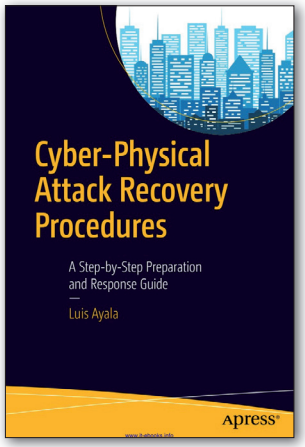
Lexikon kybernetické bezpečnosti



Cybersecurity Lexicon je poměrně rozsáhlý a užitečný zdroj pojmů a definic zaměřených na kybernetickou bezpečnost a potenciální útoky na systémy inteligentního řízení budov (BCS), systémy počítačového řízení údržby (CMMS) nebo SCADA systémy. Na téměř 200 stránkách tak čtenář najde kolem 2000 abecedně řazených technických pojmů, vysvětlení existujících hrozeb a zranitelností, ale také používaný kyber žargon. Odhadem u poloviny pojmů je jako zdroj uveden některý ze standardů NIST (National Institute of Standards and Technology), FIPS (Federal Information Processing Standard), popř. CNSS (Committee on National Security Systems), u ostatních není zdroj uveden.

http://www.springer.com/

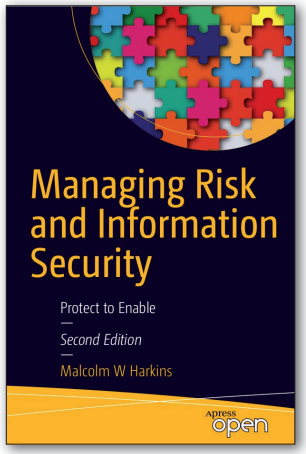
Kybernetické útoky na SCADA systémy



Cyber-Physical Attack Recovery Procedures: A Step-by-Step Preparation and Response Guide je svým zaměřením unikátní publikací. Zkraje knihy se autor věnuje útokům na řídící SCADA systémy, subsystémy a technologie automatizace a řízení moderních inteligentních budov a rozsahu možného poškození jednotlivých technologií. To co dělá publikaci výjimečnou, jsou postupy, jak se proti kyber-útokům zaměřeným na jednotlivé systémy (např. vytápění, chlazení, VZT, IRC, EPS, EZS) bránit, jak tyto útoky pokud možno v zárodku zastavit a jak se z nich následně co nejrychleji a bez dalších ztrát zotavit. Kapitola věnovaná postupům obnovy obsahuje množství detailních checklistů a konkrétních doporučení.

http://www.springer.com/

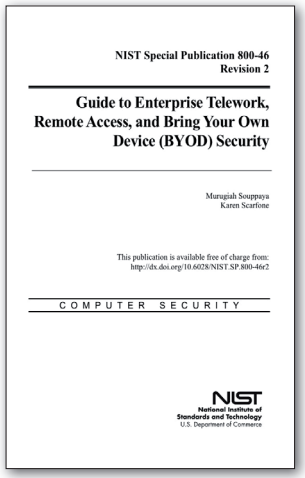
Řízení rizik a bezpečnost informací



Kniha *Managing Risk and Information Security: Protect to Enable* nabízí svěží pohled na řízení bezpečnosti podnikových informací. Jak už sám název knihy napovídá, cílem autora je ukázat potřebu změny tradičně restriktivního přístupu k řízení bezpečnosti informací, založeného na vystavení nedobytné hradby kolem informačních aktiv. Bezpečnost informací musí být vyladěna s cíli podnikání a požadavky zákazníků. Je v zájmu podniků využívat nových příležitostí, které přinášejí moderní technologie, jako jsou sociální média a zařízení v rámci internetu věcí (IoT, Internet of Things). Systém řízení bezpečnosti musí být nastaven tak, aby dokázal pružně reagovat na nové hrozby a nastavoval bezpečnostní opatření, která umožní efektivní využívání nových technologií.

http://www.apress.com/

Bezpečnost BYOD při práci na dálku


NIST Special Publication 800-46 Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-46r2

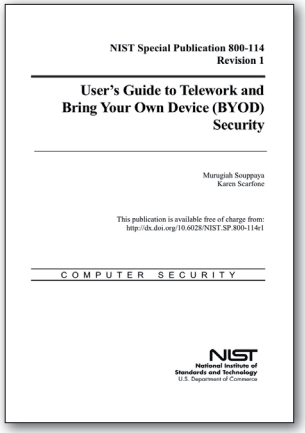
COMPUTER SECURITY

NIST National Institute of Standards and Technology U.S. Department of Commerce

SP 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security je v červenci publikovaný standard od amerického Národního institutu pro standardy a technologii (National Institute of Standards and Technology, NIST). Účelem standardu je pomoci organizacím při zvládání rizik spojených s technologiemi používanými pro práci na dálku, jako jsou servery, soukromá zařízení uživatelů používaná pro pracovní účely (BYOD) a koncová zařízení dodavatelů. Poskytuje komplexní doporučení pro vytvoření bezpečného řešení vzdáleného přístupu včetně zabezpečení serverů, komunikace mezi BYOD a vnitřní firemní sítí a výběru vhodného klientského VPN softwaru.

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

Opatření pro uživatele BYOD


NIST Special Publication 800-114 Revision 1

User's Guide to Telework and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-114r1

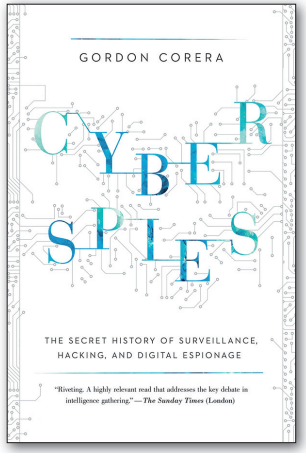
COMPUTER SECURITY

NIST National Institute of Standards and Technology U.S. Department of Commerce

Druhým červencovým přírůstkem od amerického Národního institutu je *SP 800-114, User's Guide to Telework and Bring Your Own Device (BYOD) Security*. Na rozdíl od SP 800-46 je tento standard určen přímo pro uživatele BYOD zařízení. Obsahuje doporučení pro zabezpečení soukromých zařízení používaných pro pracovní účely a to jak pro práci přímo v podniku, tak pro vzdálený přístup a práci z domova. Standard se nejprve věnuje metodám vzdáleného přístupu k firemním sítím a potenciálním rizikům při použití BYOD zařízení. Konkrétní doporučení jsou pak především zaměřena na zabezpečení uložených informací a jejich přenos, zabezpečení domácích sítí, PC, notebooků, chytrých telefonů a tabletů.

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

Historie a současnost kyber špionáže



Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage je poutavou exkurzí do světa kybernetické špionáže. Autor čtenáře provede kybernetickou špionáží od jejích počátku, kdy byly počítače využívány jako prostředek k prolomení šifry, po současnost, kdy jsou počítače naopak cílem špionáže, protože obsahují cenné informace, až po blízkou budoucnost, kdy se budou díky vzájemné propojenosti (M2M, IoT) počítače špehovat sami. Z konkrétních případů jsou popsány nejznámější aféry z období druhé světové války, studené války (např. případ německého hackera Markuse Hesse, který infiltroval informační systémy armády spojených států a získané informace o vojenských programech prodával KGB) až po současné případy kybernetické špionáže prováděné Čínou, NSA a britskou tajnou službou GCQH.

https://www.amazon.com/

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