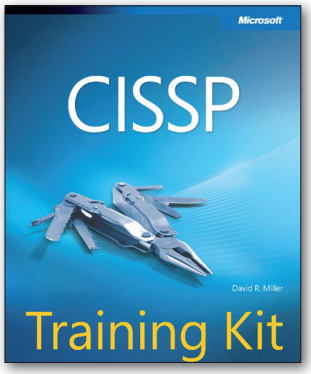
Aktuální normy a publikace o bezpečnosti

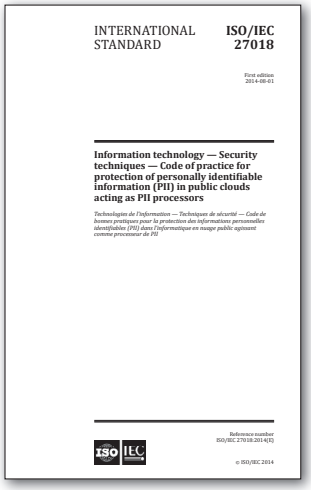
Příprava na zkoušku CISSP



CISSP Training Kit je publikací, která vám pomůže se připravit na certifikaci specialisty na bezpečnost informačních systémů CISSP (Certified Information Systems Security Professional). Kniha na téměř osmi stech stránkách pokrývá všech deset povinných znalostních oblastí (Common Body of Knowledge, CBK) od řízení přístupu přes kryptografii, business continuity, bezpečnost vývoje až po fyzickou bezpečnost. Na konci každé kapitoly jsou vždy shrnuta hlavní témata za danou oblast doplněná o dvě cvičení a osm testovacích otázek. Cvičení i otázky jsou vždy doplněny o správná řešení a odpovědi s vysvětlením. Ke knize patří také CD s dalšími testovacími otázkami.

http://www.amazon.com/

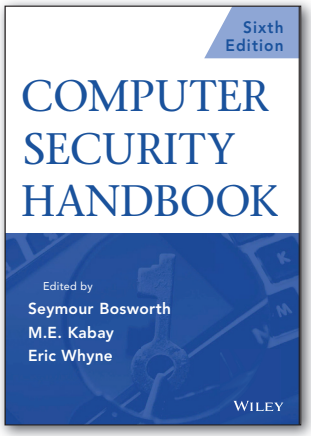
Ochrana informací v cloudu



V srpnu publikovaná norma *ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* obsahuje doporučení na ochranu osobních údajů určená poskytovatelům cloudových služeb (např. Amazon nebo Google). Norma poskytuje cíle opatření, opatření a doporučení, která umožní organizacím zajistit ochranu citlivých údajů svých klientů v souladu s principy normy ISO/IEC 29100 Information technology – Security techniques – Privacy framework. 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.

http://www.iso.org/

Příručka bezpečnosti



Šesté revidované a doplněné vydání knihy *Computer Security Handbook* je velmi podrobným zdrojem o bezpečnosti informačních a komunikačních technologií. Kniha je rozdělena do osmi částí a 75 kapitol. Na zpracování jednotlivých kapitol a témat se podílelo téměř 100 autorů. Na více než 2 000 stranách čtenář nalezne snad vše, co souvisí s počítačovou bezpečností. Od počátků informační bezpečnosti přes dnes aktuální hrozby v kyberprostoru, biometrickou autentizaci, zranitelnosti webových aplikací, zabezpečení VoIP komunikace, informační války, psychologii počítačových zločinců až po velmi detailní a přehledný výčet existujících profesních certifikací. První vydání knihy vyšlo již v roce 1973, mělo 12 kapitol, 162 stran textu a bylo zaměřeno na bezpečnost mainframů.

http://eu.wiley.com/

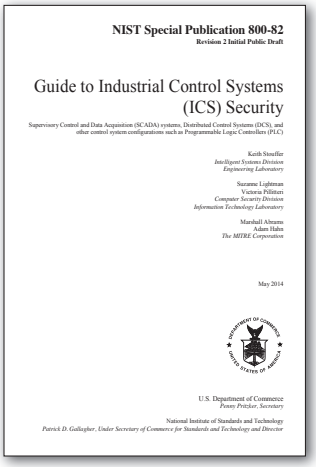
Ing. Libor Široký, CISM, CRISC, AMBCI *siroky@rac.cz*

Hrozby v kyberprostoru

V souvislosti s novým zákonem o kybernetické bezpečnosti (zákon 181/2014 Sb.), který nabývá platnosti 1. května 2015, může být zajímavým zdrojem informací o kyber hrozbách kniha *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks*. Publikace je hloubkovým exkurzem do světa reálných kybernetických hrozeb, jimž dnes jednotlivé subjekty v kybernetickém prostoru čelí. Autor se v detailu věnuje celé škále aktuálních hrozeb, jako je např. kyber špionáž či zneužití sociálních médií. Jednotlivé hrozby jsou doloženy na reálných případech výskytu z poslední doby (např. útoky na americké finanční instituce či na zpravodajské servery). Jedna z kapitol je také věnována technikám vyčíslení následků kybernetických útoků.

http://eu.wiley.com/

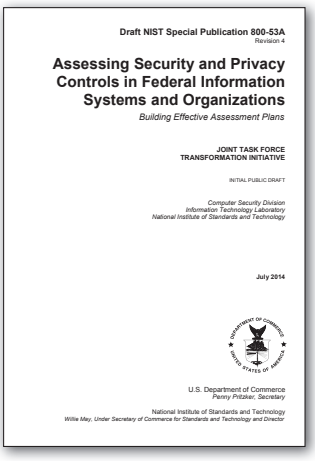
Bezpečnost SCADA systémů



Americký národní institut pro standardy a technologii (National Institute of Standards and Technology, NIST) vydal v květnu revizi normy SP 800 – 82 (Revision 2 Initial Public Draft) Guide to Industrial Control Systems (ICS) Security. Standard je zaměřen na bezpečnost průmyslových řídicích systémů (ICS). Mezi novinky druhé revize patří aktualizace hrozeb a zranitelností průmyslových řídicích systémů, revize a doplnění metodik a principů procesu řízení a hodnocení rizik ICS, aktualizace současných bezpečnostních mechanismů a trendů. Nově je také doplněn rozsáhlý katalog bezpečnostních opatření, který vychází z SP 800-53 Rev. 4. Jednotlivá opatření jsou rozšířena o doporučení k implementaci pro průmyslové systémy.

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

Hodnocení efektivnosti opatření



V červenci byla publikována již čtvrtá revize NIST standardu pro hodnocení efektivnosti bezpečnostních opatření *SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (k dispozici je prozatím verze draft). Primárním cílem aktualizace bylo promítnout změny provedené v rámci loňské revize katalogu bezpečnostních opatření *SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. Aktuální vydání také přináší větší granularitu na úrovni jednotlivých cílů hodnocení efektivnosti opatření. Co se týče samotné *SP 800-53*, byla v srpnu vydána revize Přílohy H. Účelem bylo aktualizovat mapování opatření NIST na novou verzi ISO 27001.

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