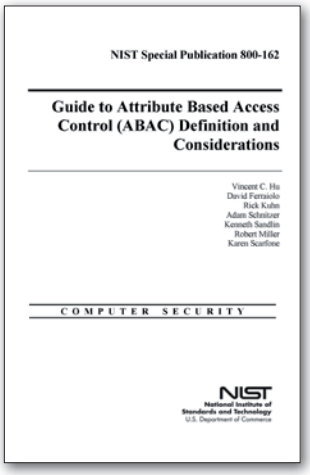
Aktuální normy a publikace o bezpečnosti

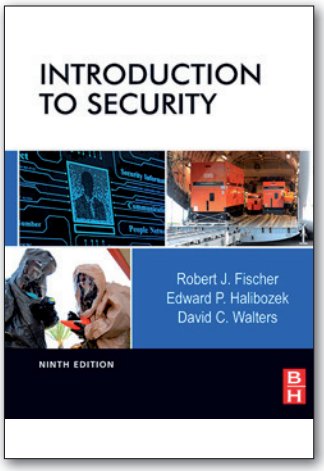
Řízení přístupu dle atributů



Guide to Attribute Based Access Control (ABAC) Definition and Considerations je prvním letošním standardem od amerického Národního institutu pro standardy a technologii (National Institute of Standards and Technology, NIST). ABAC je model řízení logického přístupu. Je založený na vyhodnocení atributů subjektu (např. jméno, role, bezpečnostní prověrka, organizace) a objektu (např. autor, datum a čas vytvoření dokumentu) a jejich porovnání s nastavenými pravidly řízení přístupu (kombinace atributů a povolené operace nad objekty). Možností je i zohlednění dalších faktorů, jako je např. čas, den v týdnu apod. Kromě podrobného vysvětlení modelu se standard také věnuje životnímu cyklu implementace (SDLC).

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

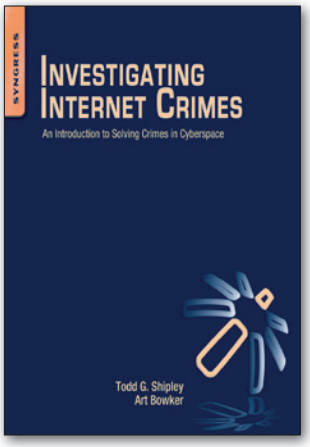
Vše o bezpečnosti



Introduction to Security je knihou, která komplexně pokrývá jednotlivé oblasti bezpečnosti. Toto již deváté vydání přináší řadu aktualizací a doplnění. Kompletně byly přepracovány kapitoly zaměřené na informační bezpečnost, krádeže identit, havarijní plánování, bezpečnost při přepravě a bezpečnost v maloobchodě. Kromě tradičních oblastí bezpečnosti (personální, fyzická, organizační, administrativní, IT atd.) se věnuje i aktuálním tématům, jako je např. kybernetická bezpečnost a ochrana kritické infrastruktury. Nadto pokrývá i takové specifické hrozby, jako je např. násilí a zneužívání alkoholu a drog na pracovišti, ekonomická kriminalita nebo špionáž.

http://www.elsevier.com/

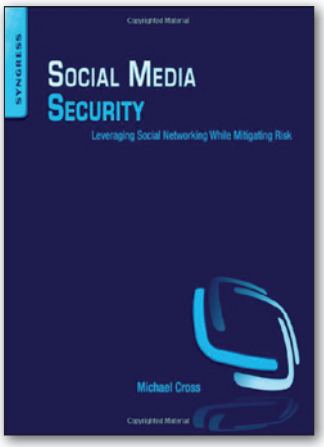
Vyšetřování zločinu na internetu



Novinka z nakladatelství Elsevier *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace* je obsáhlou (500 stran textu) a skvěle napsanou exkurzí do historie a současnosti světa počítačové kriminality. Autoři, praktici s dlouholetými zkušenostmi, čtenáře krok za krokem provází postupy vyšetřování internetových zločinů od detekce přes sběr až po dokumentování důkazního materiálu. Dle výsledků průzkumu společnosti McAfee a neziskové organizace CSIS (Center for Strategic and International Studies) jsou globální ekonomické ztráty způsobené kyberzločinci odhadovány na 300 mld. dolarů ročně. Podle stejné studie přijde jenom ve Spojených státech každoročně půl milionu lidí o práci následkem kyberšpionáže.

http://www.elsevier.com/

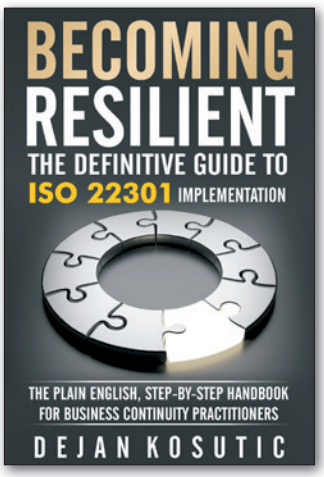
Bezpečnost v sociálních sítích



Sociální sítě poskytují zcela nové možnosti fungování podnikových procesů a obchodních činností. Včetně identifikace nových zákazníků, aktivní komunikace a získání zpětné vazby (např. Facebook, Ning, Twitter), šíření virálních videí (YouTube) nebo hledání nových zaměstnanců (LinkedIn). S ohledem na rizika s nimi spojená se plnému využití sociálních sítí řada organizací dosud brání. *Social Media Security: Leveraging Social Networking While Mitigating Risk* je knihou, která umožní organizacím se s riziky využívání sociálních sítí seznámit a nabídne doporučení, jak nastavit a udržet přijatelnou míru bezpečnosti při jejich použití. Obsahuje přehled nejoblíbenějších sociálních sítí a možností jejich využití na konkrétních příkladech.

http://www.elsevier.com/

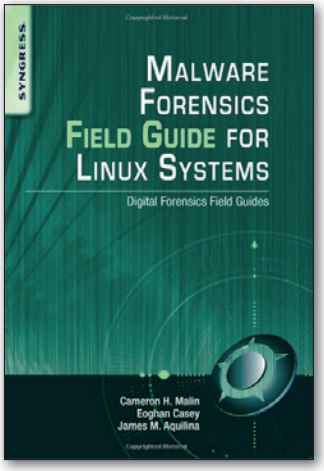
Úplný průvodce pro BCMS



Becoming Resilient: The Definitive Guide to ISO 22301 Implementation je dalším z řady praktických průvodců po požadavcích certifikační normy pro systémy řízení kontinuity činností ISO 22301:2012. Na rozdíl od jiných podobných publikací je však psána velmi srozumitelným jazykem, takže je vhodná i pro začátečníky. Autor se podrobně věnuje jednotlivým kapitolám a opatřením normy. Každý z certifikačních požadavků ISO 22301 je podrobně rozebrán a vysvětlen. Vždy je uveden účel, vstupy, možné způsoby implementace, požadavky na dokumentaci a tipy z praxe. Kniha pokrývá vše, co potřebujete vědět o BCMS a požadavcích na úspěšnou certifikaci systému řízení kontinuity.

http://www.iso27001standard.com/en/

Forenzní analýza linuxových systémů



Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides je praktickým průvodcem pro forenzní počítačové analytiky a vyšetřovatele. Kniha je psána stručnou a snadno srozumitelnou formou, obsahuje řadu případových studií, konkrétních postupů a doporučení ke zvážení. Mimo jiné pokrývá analýzu artefaktů škodlivého kódu v podezřelých programech, analýzu obrazu operační paměti včetně analýzy paměťového prostoru jednotlivých aplikací, exportování škodlivého kódu a jeho artefaktů z linuxových systémů. Věnuje se také regulatorním a legislativním otázkám spojeným se sběrem a zkoumáním důkazního materiálu. Je sestavena tak, aby dala jasný návod při řešení bezpečnostních incidentů postupy forenzní analýzy ICT.

http://www.elsevier.com/

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