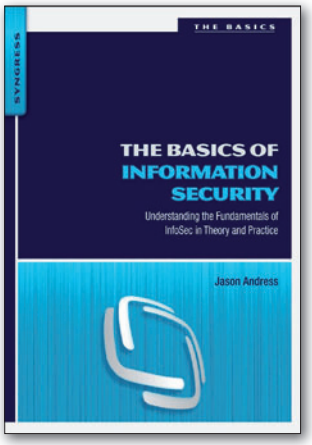
Aktuální normy a publikace o bezpečnosti

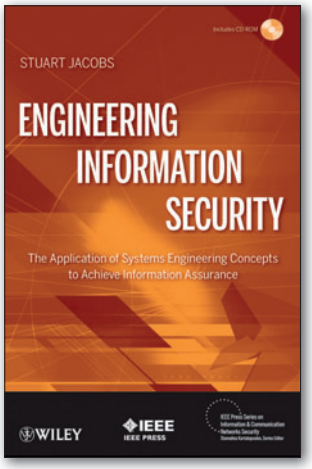
Základy bezpečnosti informací



Novinka z nakladatelství Elsevier *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* je na první pohled jen další ze stovky obdobných publikací nabízejících úvod do bezpečnosti informací. Je však výjimečná v tom, že na rozdíl od jiných je čtivá, srozumitelná a nezachází do přílišných detailů. Kromě teoretických základů je plná příkladů s odkazem na vzory z praxe. Na úvod autor osvětluje základní principy důvěrnosti, integrity a dostupnosti, aby se pak spolu se čtenářem ponořil do praktické aplikace bezpečnosti informací v oblastech fyzické, logické a administrativní bezpečnosti.

http://www.elsevier.com/

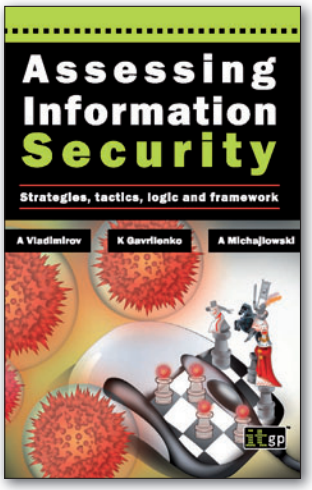
Bezpečnost informací komplexně



Kniha *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance* na úvod rozebírá základy a potřebu bezpečnosti informací. Následně pak pokrývá kompletní životní cyklus bezpečnosti systémů, od identifikace bezpečnostních požadavků a nastavení politik, přes jejich návrh, implementaci a provoz. Na rozdíl od většiny knih o bezpečnosti, které se zaměřují na konkrétní bezpečnostní mechanismy, hrozby a zranitelnosti, nabízí tato kniha metodiku pro nastavení účinné a efektivní úrovně bezpečnosti jakékoliv firmy. Metodika využívá principů systémového inženýrství k dosažení identifikovaných cílů bezpečnosti.

http://eu.wiley.com/

Bezpečnost informací a umění války

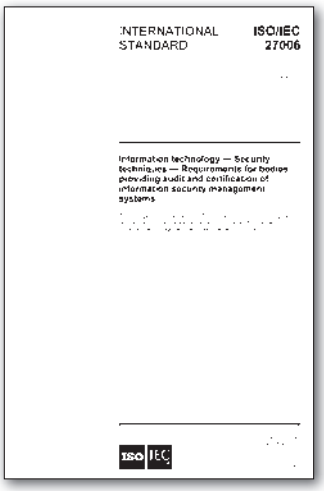


Assessing Information Security: Strategies, Tactics, Logic and Framework je knihou o filosofii, strategii a taktice efektivního hodnocení úrovně bezpečnosti ve firmách. Cílem autorů rozhodně nebylo sestavit kontrolní seznam, podle kterého provedete audit bezpečnosti od A do Z. Naopak se pokusili, nutno podotknout že úspěšně, vtisknout jednotlivým principům a doporučením lidskou tvář. Na četných příkladech dokládají, že slepá implementace jednotlivých opatření je často cestou do pekel. Navíc je kniha protkána citacemi slavných vojenských stratégů, které se slévají do jednolitého závěru – zajištění požadované úrovně bezpečnosti je nikdy nekončící válkou.

http://www.itgovernance.co.uk/

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

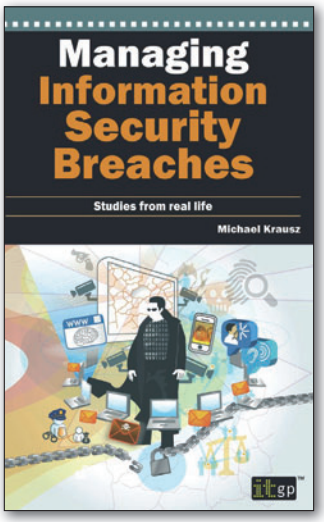
Nové vydání ISO/IEC 27006



V prosinci 2011 byla publikována první revize normy *ISO/IEC 27006:2011 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems*. Norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (ISMS) a doplňuje tak požadavky obsažené v ČSN ISO/IEC 17021 a ČSN ISO/IEC 27001. Cílem revidovaného vydání bylo zajistit soulad s revidovaným vydáním ISO/IEC 17021:2011, které stanovuje požadavky na certifikační orgány provádějící audity systémů řízení.

http://www.iso.org/

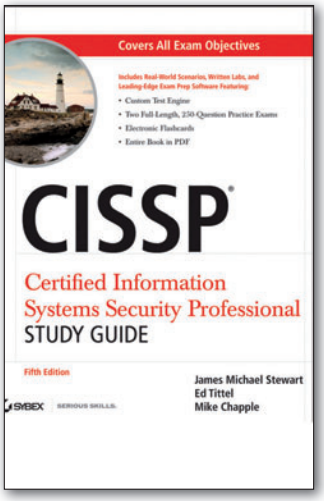
Řízení bezpečnostních incidentů



Managing Information Security Breaches: Studies from real life je publikací, která čtenáře zavede do světa bezpečnostních incidentů a postupů jejich zvládání. Kniha se zaměřuje na postupy účinného řízení závažných pokusů o prolomení bezpečnosti informací a následného obnovení odpovídající úrovně bezpečnosti. Postupy a doporučení jsou založena na opatřeních pro zvládání bezpečnostních incidentů uvedených ISO/IEC 27002:2005. Pro ilustraci jednotlivých doporučení využívá autor celou řadu případových studií. Jednotlivé případy detailně rozebírá a demonstruje na nich chyby, kterých se firmy dopustily. Následně pak nabízí doporučení pro stanovení priorit při řešení incidentů, jejich následků a přijetí preventivních opatření.

http://www.itgovernance.co.uk/

Příprava na certifikát CISSP



CISSP: Certified Information Systems Security Professional Study Guide je knihou, která čtenáře připraví na certifikaci specialisty na bezpečnost informačních systémů CISSP (Certified Information Systems Security Professional). Jedná se již o páté doplněné vydání, které na téměř tisíci stránkách pokrývá všech 10 povinných oblastí znalostí (Common Body of Knowledge, CBK), počínaje řízením přístupu až po havarijní plánování. Pro dokreslení teorie jsou v jednotlivých kapitolách uvedeny praktické příklady a doplňující vysvětlení. Na konci každé kapitoly jsou vždy shrnuty hlavní témata za danou oblast, bez jejichž znalostí nelze u zkoušky obstát, a rovněž příklady testovací otázek včetně správných odpovědí s vysvětlením.

http://eu.wiley.com/