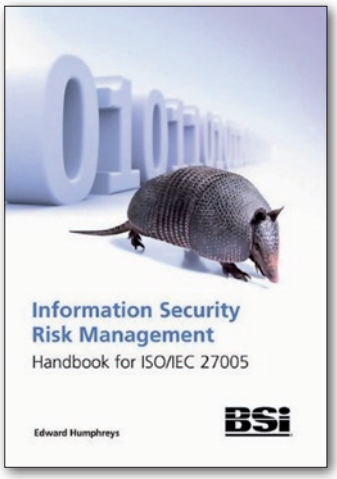
Aktuální normy a publikace o bezpečnosti

Návod k ISMS

ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance je nejnovějším přírůstkem řady 27k. Norma je především návodem a příručkou k implementaci ostatních norem této řady. Je určena všem organizacím, které mají v úmyslu zavést systém řízení bezpečnosti informací (ISMS) dle ISO/IEC 27001. Poskytuje dostatek informací a doporučení pro sestavení detailního plánu a kroků implementace ISMS. Přílohy obsahují kontrolní přehled činností, detailní přehled rolí a odpovědností, informace ke struktuře a obsahu politik ISMS.

www.iso.org

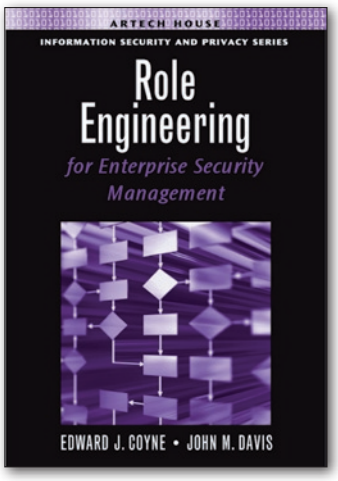
Klíč k implementaci ISO/IEC 27005



Information Security Risk Management – Handbook for ISO/IEC 27001 je praktickým návodem pro použití a aplikaci standardu pro řízení informačních rizik ISO/IEC 27005. Kniha poskytuje řadu konkrétních doporučení pro implementaci požadavků na proces řízení rizik tak, jak vyplývají z certifikační normy ISMS ISO/IEC 27001. Dostatečný prostor je věnován postupům hodnocení a zvládání rizik, výběru vhodných opatření, požadavkům na dokumentaci. Nejsou opomenuty postupy monitorování a přezkoumávání zavedeného procesu řízení rizik. Autorem dvousetstránkové publikace je známý ISMS guru Ted Humphreys.

www.bsigroup.com

Vše o řízení přístupu k informacím

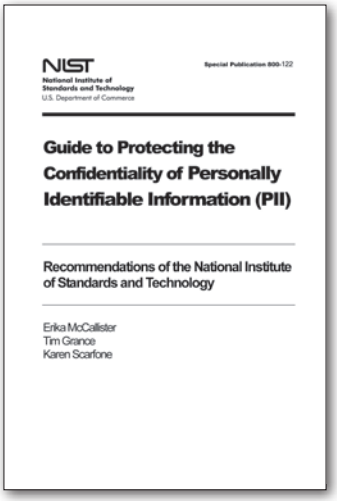


Role Engineering for Enterprise Security Management je kniha napsaná mezinárodně uznávanými autoritami na řízení přístupu. Obsahuje řadu doporučení pro správu a řízení přístupu uživatelů ke zdrojům a informacím na základě jejich rolí (Role Based Access Control – RBAC). RBAC asociuje přístupová oprávnění s rolemi, role jsou dle potřeby přidělovány uživatelům (zaměstnancům organizace). Kniha je plná praktických návodů pro navržení optimálních rolí a jim přidělených oprávnění k provozovaným systémům. Publikace patří mezi to nejlepší, co lze k nastavení efektivního RBAC v současnosti.

www.artechhouse.com

Libor Široký, *siroky@rac.cz*

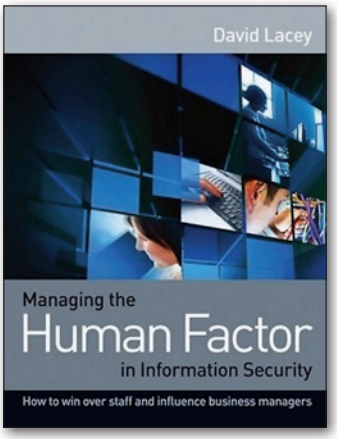
Ochrana osobních údajů



Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) je nový americký standard, který se věnuje problematice ochrany osobních údajů. Útoky zaměřené na osobní údaje mohou být nebezpečné jak pro jednotlivce, tak pro celou organizaci. Odpovídající ochrana důvěrnosti osobních údajů nemůže být efektivně zajištěna bez předchozího hodnocení rizik. Standard poskytuje doporučení pro zajištění důvěrnosti osobních údajů, založené na identifikaci všech zdrojů a úložišť důvěrných informací, potenciálních zranitelností a hrozeb, které je mohou využít. Může tak být vhodným doplňkem k českému zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

www.nist.gov

Jak vyhrát nad zaměstnanci



Managing the Human Factor in Information Security, aneb lidský faktor v bezpečnosti informací. David Lacey se v novém bestselleru věnuje významu a technikám trvalého zvyšování povědomí zaměstnanců při implementaci bezpečnosti. Jednotlivá doporučení jsou doplněna řadou příkladů a postřehů z praxe zaměřených například na to, jak motivovat zaměstnance a ovlivnit způsob jejich myšlení. Dostatečný prostor je věnován firemní kultuře, politice a dalším faktorům, které mohou mít zásadní vliv na efektivní řízení bezpečnosti informací. Autor předkládá dobře čitelný text nasycený více než dvacetiletými praktickými zkušenostmi.

www.bsigroup.com

Bezpečnost v prostředí outsourcingu

Kniha Managing Security in Outsourced and Off-shored Environments je novinkou od BSI, která je určena pro všechny, kteří hledají praxí ověřené znalosti o tom, jak řídit rizika spojená s outsourcingem a offshoringem informačních technologií a služeb. Je určena všem IT ředitelům a manažerům, risk manažerům, auditorům a konzultantům, ale také studentům a všem, kteří nemají předchozí znalost této problematiky. Je psána srozumitelným jazykem, kapitoly logicky sledují jednotlivé fáze životního cyklu outsourcingu od základních definic až po implementaci a řízení outsourcingových vztahů.

www.bsigroup.com