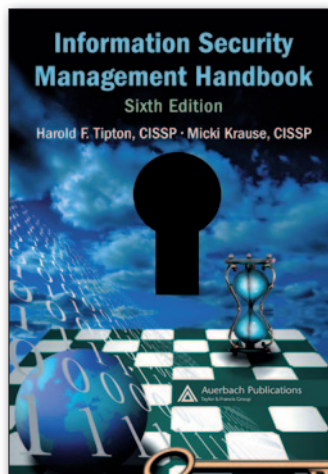


Aktuální normy a publikace o bezpečnosti

Bible informační bezpečnosti



Příručka Information Security Management Handbook bývá označována za „zlatý“ standard informační bezpečnosti. Publikace je kompilací tzv. whitepapers od více než stovky různých autorů a detailně pokrývá všechny oblasti bezpečnosti. Kromě toho, že se jedná o zásadní zdroj informací pro všechny IT profesionály, je např. také vhodným studijním zdrojem při přípravě na CISSP certifikaci. Toto již šesté vydání má 3 280 stran a 4 doplňkové svazky. Každoročně je formou nového svazku doplněna o aktuální trendy a novinky.

<http://www.auerbach-publications.com>

Bezpečnostní incidenty od A do Z



Kniha Information Security Incident Management – A Methodology staví na doporučeních ISO/IEC 18044 a ISO/IEC 27002. Poskytuje ucelený pohled na proces zvládnání incidentů bezpečnosti informací – od hlášení a detekce až po finální vyhodnocení nastalých událostí. Popsaná metodika pro zvládnání incidentů je rozdělena do celkem šesti fází, které jsou v textu do detailu rozebrány.

<http://shop.bsigroup.com>

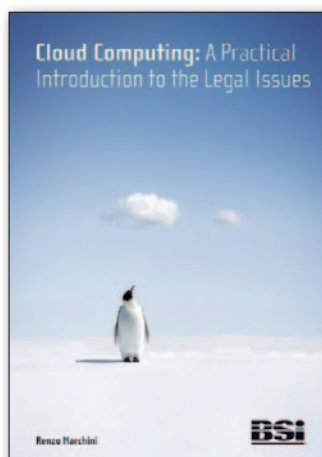
BCM s příchutí řízení rizik



AS/NZS 5050:2010 Business continuity – Managing disruption related risk je nový australský standard pro BCM. Aplikuje principy mezinárodní normy pro řízení rizik ISO 31000:2009 na rizika způsobující narušení business procesů. Oproti jiným standardům více prosazuje proaktivní přístup k BCM – od pasivního vyčkávání na havárie k aktivnímu řízení kontinuity. Modifikací rizika lze událostem způsobujícím nedostupnosti v řadě případů předejít nebo alespoň snížit pravděpodobnost jejich výskytu. Nový standard tak jen potvrzuje neustálý vývoj v této oblasti bezpečnosti.

<http://infostore.saiglobal.com/store/>

Zákony v mracích



BIP 0117:2010 Cloud Computing. A Practical Introduction to the Legal Issues je čerstvou publikací od britského normalizačního institutu (BSI). Publikace se věnuje legislativním a regulačním aspektům spojeným s cloud computingem. Po stručném úvodu do problematiky této technologie se autor věnuje souvisejícím legislativním a regulačním otázkám, např. záležitostem spojeným s ochranou soukromí, úrovní poskytovaných služeb a rizikům smluvních vztahů. Kniha přináší řadu doporučení jak těm, kdo služby cloudu kupují, tak těm, co je poskytují.

<http://shop.bsigroup.com>

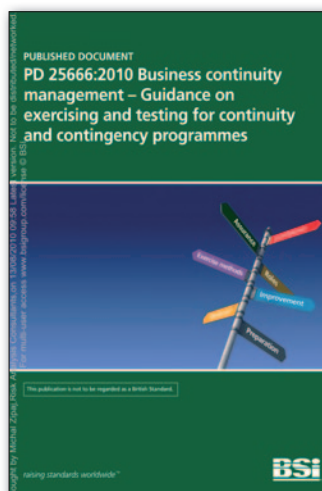
Informační bezpečnost v heslech



NIST IR 7298 (Draft), Glossary of Key Information Security Terms je první verzí nového slovníku pojmů a terminologie z oblasti informační bezpečnosti. Slovník je kompilací dílčích slovníků, které byly doposud publikovány v amerických standardech, zejména v řadě NIST (série 800) a FIPS. U každého pojmu je kromě výkladu uveden také odkaz na původní zdroj. V publikované verzi obsahuje již kolem 1 500 pojmů s tím, že bude nadále podléhat pravidelným revizím a aktualizacím.

<http://csrc.nist.gov/publications/PubsSPs.html>

Testujeme a cvičíme BCP



KPD 25666:2010, Business continuity management. Guidance on exercising and testing for continuity and contingency programmes je prvním standardem zaměřeným výhradně na cvičení programů BCM a testování souvisejících plánů kontinuity a obnovy. Je určen jako doplněk k BCM standardům BS 25999, BS 25777 a ISO/PAS 22399. Kromě samotného přístupu k testování je věnován dostatečný prostor účastníkům testů a rolím, které budou během cvičení, ale i při ostré aktivaci BCP reprezentovat.

<http://shop.bsigroup.com/>

Libor Široký, siroky@rac.cz