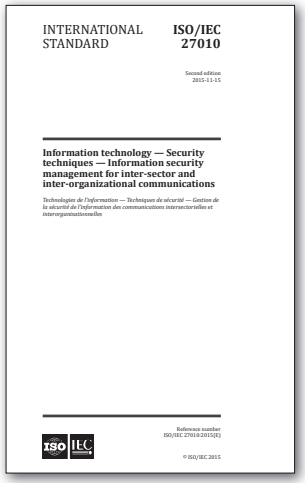
Aktuální normy a publikace o bezpečnosti

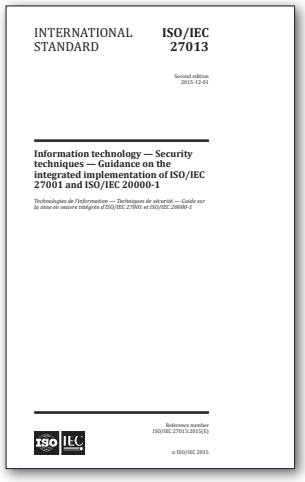
Sdílení informací o incidentech



V samém závěru loňského roku byly publikovány tři normy z rodiny 27k. První z nich je v pořadí druhé vydání normy *ISO/IEC 27010:2015 Information technology – Security techniques – Information security management for inter-sector and inter-organisational communications*. Norma nabízí doporučení směrem ke spolupráci a sdílení informací, k řešení bezpečnostních problémů, incidentů a aktuálních rizik, mezi organizacemi působícími ve stejných průmyslových odvětvích, napříč průmyslovými odvětvími a mezi vládami. A to jak v době krize, při řešení kybernetických bezpečnostních incidentů a zajišťování ochrany kritické infrastruktury, tak v rámci přípravy, při implementaci bezpečnostních opatření, plnění regulatorních, legislativních a smluvních požadavků.

http://www.iso.org/

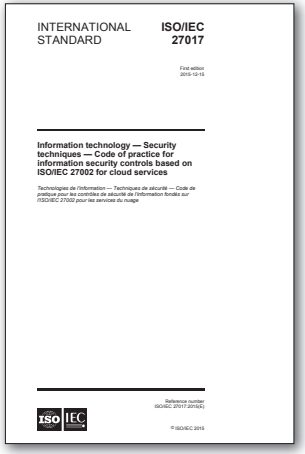
Integrace ISMS a řízení IT služeb



Druhou prosincovou normou je *ISO/IEC 27013:2015 – Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*. Norma poskytuje doporučení a návod pro zavedení integrovaného procesního přístupu k řízení bezpečnosti informací podle ISO/IEC 27001:2013 a systému řízení IT služeb podle ISO/IEC 20000-1:2011 (norma je odvozená z knihovny ITIL). Doporučení směřují k realizaci jednotlivých procesů a přípravě podpůrné dokumentace. A to jak pro organizace, které již mají jeden ze systémů zaveden, tak i pro ty, které stojí na úplném počátku řízení bezpečnosti. Příloha normy obsahuje srovnání obou výše uvedených standardů. Norma vychází ve druhém revidovaném vydání.

http://www.iso.org/

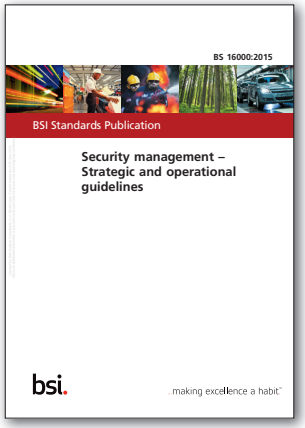
Bezpečnost cloud computingu



Poslední z prosincových přírůstků do rodiny norem 27k je *ISO/IEC 27017:2015 / ITU-T X.1631 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Jak už ze samotného názvu vyplývá, norma se věnuje konkrétním aspektům bezpečnosti informací v prostředí cloud computingu. Poskytuje doporučení k realizaci konkrétních bezpečnostních opatření v prostředí cloudu nad rámec těch, které jsou uvedeny v normě ISO/IEC 27002 a dalších standardech řady 27k. Norma je společným dílem Mezinárodní organizace pro normalizaci (ISO), Mezinárodní elektrotechnické komise (IEC) a Mezinárodní telekomunikační unie (ITU).

http://www.iso.org/

Řízení bezpečnosti obecně

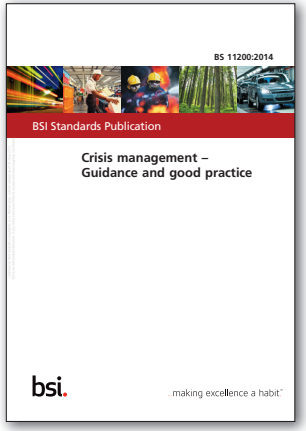


BS 16000 Security management – Strategic and operational guidelines obsahuje terminologický slovník a základní principy řízení bezpečnosti. Dává návod, jak by měla být bezpečnost v organizacích ustavena, zavedena a provozována. BS 16000 je obecný standard, kompatibilní s ostatními normami pro systémy řízení (ISO 27001, ISO 22301, ISO 9001, ISO 14001). Obsahuje také konkrétní doporučení, postupy a řešení bezpečnosti. Kromě úvodních kapitol věnujících se internímu a externímu kontextu organizace, rolím a odpovědnostem při řízení bezpečnosti, se také věnuje hodnocení rizik a v poměrně velkém detailu bezpečnostním opatřením a implementaci programu pro zvyšování úrovně bezpečnosti.

http://shop.bsigroup.com/

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

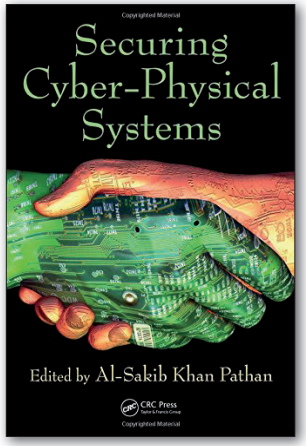
Krizové řízení



Britský standard *BS 11200:2014 Crisis management – Guidance and good practice* je věnován oblasti krizového řízení. Obsahuje užitečné informace a rady, které se mohou hodit při plánování, ustavení a kontinuálním zvyšování schopnosti organizace čelit krizovým událostem. V úvodních kapitolách se věnuje výkladu základních pojmů, rozdílům mezi incidenty a krizovými situacemi, základním principům krizového řízení a potenciálním zdrojům a varovným příznakům krizí. V dalších kapitolách poskytuje doporučení pro vytvoření rámce a nastavení postupů krizového řízení, rolím a odpovědnostem, mechanizmům rozhodování při zvládání krizových situací, krizové komunikaci a v neposlední řadě také cvičení a testování.

http://shop.bsigroup.com/

Bezpečnost CPS



Čtvrtá průmyslová revoluce (Průmysl 4.0) probíhá ve znamení kyberneticko-fyzikálních systémů (CPS), což jsou systémy schopné reagovat s fyzikálním světem. Díky těmto systémům vzniknou například chytré továrny, které se budou do značné míry řídit samy. Tento trend však s sebou kromě úspor, zvýšení produktivity, konkurenceschopnosti a flexibility firem také nese nemalá bezpečnostní rizika. Hlavním rizikem jsou kybernetické útoky a narušení bezpečnosti dat. Konkrétním hrozbám spojeným s CPS systémy a možným bezpečnostním opatřením se věnuje publikace *Securing Cyber-Physical Systems* z nakladatelství CRC Press. V celkem sedmnácti kapitolách se věnuje rizikům CPS v různých oborech a odvětvích, např. rizikům spojeným s kompromitací interních systémů autonomních vozidel.

http://www.crcpress.com