Rozhovor s Robertem Bigmanem

strana 6

Adam Lamser

Robert Bigman, který dlouhá léta pracoval v Central Intelligence Agency (CIA), se v rozhovoru rozpovídal o tom, jaká má tato práce specifika. Podělil se o to, jak se ve zpravodajské službě přistupuje k řízení rizik. Nastínil, jaké incidenty musel během své kariéry řešit. Vysvětlil, proč je jen velmi obtížně možné dosáhnout zlepšení v oblasti kybernetické bezpečnosti bez předchozího selhání, a vyjádřil se také ke stále aktuální kauze Huawei.

PKI v systému pro správu kryptografických klíčů – část I.

strana 18

Jiří Urbanec

První část miniseriálu se zabývá infrastrukturou veřejných klíčů jako jednou ze služeb používaných v organizaci. Rozebírá motivaci pro vytvoření systému pro správu asymetrických klíčů a diskutuje jeho použití jako jeden z možných způsobů zvýšení pružnosti organizace v řízení asymetrických klíčů a nástroje pro vyrovnání se s rozmanitostí procesů různých PKI.

Rozhovor s Jánem Urigou

strana 28

Michal Wojnar

Jána Urigy, behaviorálního psychologa, který se zaměřuje na oblast byznysu, jsme se ptali, jaký je vztah kybernetické bezpečnosti a psychologie. Vysvětlil nám, proč je výhodné mít v týmu člověka, který zná principy behaviorálních věd. Popsal význam rozpoznání hodnoty informace, která je jádrem podnikatelských aktivit každé společnosti. Uvedl i praktický příklad, jak učí zaměstnance klienta uvědomit si hodnotu informací. A představil i koncept Experience Centra společnosti PwC, které vede.

Řízení incidentů v souladu se současnou legislativou – část I.

strana 12

Jaromír Veber

Miniseriál se zaměřuje na popis toho, jakým způsobem současná legislativa zasahuje do procesu řízení incidentů. Je představen obecný popis procesu řízení bezpečnostních incidentů, a dále jsou popsány relevantní legislativní požadavky vybraných významných zákonů (v tomto díle zákonu o kybernetické bezpečnosti) včetně popisu, ve které části procesu a jakým způsobem se uplatní. Čtenáři si tak mohou ověřit, zda jejich proces je vhodným způsobem nastaven, nebo jakým způsobem proces přizpůsobit, aby vyhovoval legislativě, která se na ně uplatňuje.

Jak na rizika – část IV.

strana 23

Petr Strnad

Tento článek, jenž je čtvrtým dílem série věnované řízení rizik, tentokrát představuje hlavní druhy finančních rizik v bankách a nefinančních podnicích, jejich význam, metody řízení a měření a úskalí s nimi spojená.

Otevřená data

strana 32

Jaroslav Tajbr

Článek se zaměřuje na problematiku české právní úpravy otevřených dat. V úvodu autor článku seznamuje čtenáře s pojmem otevřených dat a následně uvádí, která právní odvětví a právní předpisy tuto problematiku v českém právním řádu upravují. Konkrétně se zabývá zákonem o svobodném přístupu k informacím, aspekty autorského práva i ochrany osobních údajů. V neposlední řadě autor uvádí příklady z české praxe ve využívání otevřených dat.

DevOps – část V. strana 36
Vladimír Kufner

Tento díl ze série článků o DevOps je zaměřen na bezpečnost v rámci DevOps („DevSecOps"). Probírá specifické zranitelnosti a možná ohrožení i největší výzvy, které DevOps pro bezpečnost IT přináší. Diskutuje, jaké další oblasti jsou DevOps ovlivněny a jaký je potenciální dopad, pokud se bezpečnost v DevOps nedaří držet pod kontrolou. V závěrečné části článek popisuje taktéž používané principy a metody.

Český telekomunikační úřad na cestě do 21. století strana 42
Jaromír Novák

Článek shrnuje vývoj telekomunikací a roli nezávislého regulátora, která se v průběhu uplynulých desetiletí měnila od dohledu nad počtem telefonních budek až po přípravu dražby frekvencí pro 5G sítě. Ve své druhé části se zaměřuje zejména na současné klíčové aktivity telekomunikačního regulátora v České republice – ČTÚ.

RUBRIKY

Virová stránka 46
Normy a publikace 50
Stalo se 52
Konference IS2: 20 LET IS2 ...bezpečnost každého z nás?! 54
Metamorfosa: Aprílové setkání 56
Informace z partnerských společností 57
Právní rubrika 58
Management summary 60
Tiráž 62