


O B S A H

Články označené  prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

Rozhovor s Petrem Nobstem

strana

6

Petr Hampl

Finanční ředitel společnosti PLEAS hovoří o rozdílech mezi přístupy IT manažera a CFO, o schvalování investic i o tom, proč některé inovace nemohou být posuzovány jen podle měřitelné návratnosti. Vysvětluje svůj pohled na bezpečnostní aktiva textilního podniku, outsourcingu ochrany sítí a zabývá se otázkou ochrany mobilních zařízení. Oproti koncepci BYOD vyzdvihuje výhody standardizace všech zařízení v organizaci včetně mobilních telefonů.



Zaměstnanci jako bezpečnostní riziko

strana

14

Ivana Spoustová

První část textu je zaměřena na opatření, která snižují riziko neúmyslného narušení informační bezpečnosti ze strany zaměstnanců. Jedná se zejména o školení, interní komunikační kampaně, etické kodexy a závazky mlčenlivosti. Druhá část je věnována situacím, kdy k narušení informační bezpečnosti dojde úmyslně, k prevenci takových situací – výpověď, pocit křivdy, narušení psychologické smlouvy, vážná osobní či rodinná situace a specifické charakterové rysy. Součástí textu je případová studie ze zbrojovky Colt a anketa bezpečnostních manažerů velkých organizací v České republice.



strana

22

Vlastnoruční digitální podpis a jeho implementace v O2 – část II.

Aleš Bernášek

Případová studie popisuje projekt zavedení biometrického podpisu v celé prodejní síti O2. Druhý díl vysvětluje principy zabezpečení řešení, které byly implantovány na základě analýzy rizik, hrozeb a zranitelností. Dále se věnuje technické architektuře (klientská část, serverová část, integrace) a výběru technického zařízení pro zachycení podpisu. V dalších částech jsou vysvětleny procesy podporované popisovaným řešením, jeho přínosy a poučení, která z projektu vzešla.



strana

31

IP adresa v ochraně osobních údajů

Josef Prokeš

Expert Úřadu pro ochranu osobních údajů se ve svém článku vysvětluje pohled evropských dozorových orgánů. Vrací se k definici, co má být považováno za osobní údaj, ukazuje změny, ke kterým došlo v důsledku technologického vývoje a rostoucích možností identifikace uživatelů pomocí IP adresy. V další části textu se diskutuje o tzv. pseudoanonymizaci a možných dopadech očekávaného rozhodnutí soudního dvora EU.

Rozhovor s Janem Ellermannem

strana

10

Petr Hampl

Specialista informační bezpečnosti Europolu se poměrně obsírně věnuje tomu, jaké osobní údaje (zejména o pachatelích, podezřelých, svědcích a obětech trestných činů) je přijatelné uchovávat v informačních systémech a jaké procedury s tím musí být spojeny. Věnuje se rovněž klasifikaci dat, školení uživatelů a během celého rozhovoru hájí dvě základní přesvědčení – bezpečnost dat a kvalita dat jsou dvěma stranami jedné mince. Ochrana osobních dat nezdržuje vyšetřování, naopak prospívá jeho efektivitě.



Autentizace zítra a dnes



strana

20

Článek se zabývá základními trendy autentizace uživatelů (věnuje se zejména dvoufaktorové identifikaci) a perspektivám pro budoucnost v horizontu příštích několika let. Dále se věnuje možnostem, jaké jsou dostupné již dnes, představuje řešení ESET Secure Authentication. Součástí textu je stručná případová studie ze společnosti Allus Global, kde nasazení ESET Secure Authentication umožnilo splnit požadavky normy pro bezpečnost informací o držitelích platebních karet PCI DSS.

Současný stav bezpečnosti protokolu IPv6



strana

28

Petr Fojtů

Článek navazuje na stať již dříve publikované v DSM a podrobněji rozebírá jak explicitní bezpečnostní prvky (IPsec, SeND), tak také ty s implicitním dopadem (rozšiřující záhlaví, rozsáhlý adresní prostor). Dále pokrývá současný vývoj a otevírá diskusi, zda protokol IPv6 přinesl takové zvýšení bezpečnosti, jaké od něj bylo očekáváno. Závěrečná část je věnována různým praktickým aspektům přechodu z IPv4 na IPv6.



ENJOY SAFER
TECHNOLOGY™



Redakce DSM děkuje za spolupráci dlouhodobým obchodním partnerům

Zásady zabezpečení biometrických dat



strana
34

Roman Cinkais

Text je zaměřen na specifickou podoblast systémů biometrické identifikace osob – zabezpečení biometrických dat. Vyčítá způsoby, jak mohou být biometrická data kompromitována, definuje požadované vlastnosti biometrického systému, které z toho vyplývají, a zaměřuje se na dvě konkrétnější problémové oblasti – prostředí a procesy snímání dat a nedostatečné informace poskytované výrobci biometrických produktů.

Několik zásad pro úspěšnou implementaci SIEM



strana
38

Karel Šimeček

Autor znovu objasňuje základní principy, na kterých jsou založeny systémy SIEM, a ukazuje, jak opomíjení těchto základních principů vede ke zklamání z výsledků implementace. Zvláštní pozornost věnuje požadavku na zapojení SIEM do aplikační vrstvy ERP systému, se kterým přichází někteří zákazníci, a riziku zahlcení SIEM při útoku typu DDoS. Doprovodné tabulky ukazují různé možnosti licencování a nejčastější chybná nastavení SIEM.

Recenze knihy Jaye Jacobse a Boba Rudise Data-Driven Security: Analysis, Visualization and Dashboards



strana
44

Vašek Matyáš

RUBRIKY

Normy a publikace	45
Vírová stránka	46
Svatomartinská husa	47
Konference IT Governance 2014	48
Z partnerských společností	49
Právní rubrika	50
Management summary	51
Tiráž	52

V PŘÍŠTÍM ČÍSLE

1
2015

Data Security Management 1/2015 vyjde 12. března. Najdete v něm rozhovor s významnou osobností z telekomunikací, případovou studii o monitoringu provozu v sítích, článek o rizikovém chování uživatelů v sociálních sítích a další zkušenosti českého CISO. Znovu se také vrátíme k otázce cloud computingu, a pokud už budou existovat prováděcí předpisy, zaměříme se rovněž na zákon o kybernetické bezpečnosti.