


O B S A H

Články označené  prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

Rozhovor s Karlem Soukeníkem

strana

Petr Hampel

6

Finanční a provozní ředitel české pobočky Sberbank hovoří o schvalování investic, metodách výpočtu business case a posuzování výdajů na informační bezpečnost. Komentuje připravovaný zákon o kybernetické bezpečnosti a zamýšlí se nad rolí možného lidského selhání při krádežích cenných dat. Část rozhovoru je věnována cloudu a otázce, zda přenesení citlivých dat k renomovanému poskytovateli se silným bezpečnostním týmem znamená nárůst rizik nebo jejich snížení.

Politika mobilních zařízení



strana

Lukáš Bláha, Martin Tobolka

12

Text v úvodu vymezuje, jaká zařízení by měla být politikou mobilních zařízení pokryta. Dále vysvětluje model hrozeb, který má být základem politiky mobilních zařízení, a definuje minimální povinná opatření. V dalších částech se věnuje nástrojům MDM (mobile device management) a MAM (mobile application management) a vysvětluje rozdíly mezi nimi. Závěrečná část pak shrnuje možnosti kontrolování, jak jsou stanovená pravidla dodržována.

Biometrie obličeje pro autentizaci osob



strana

Tomáš Valer

18

Článek se zabývá rozdíly mezi dvourozměrnou a nově nastupující trojrozměrnou identifikací obličejů. Vysvětluje technický princip trojrozměrného snímání obličeje, informuje o softwarových i hardwarových prostředcích pro její realizaci a ukazuje některé praktické situace, kde může být modernější metoda s úspěchem využita. Druhá část článku je věnována případové studii – nasazení popisované technologie v moskevské pobočce Sberbank.

Dohled nad informačními systémy finančních institucí v podmínkách outsourcingu



strana

Martin Fleischmann

24

Expert ČNB v úvodu zpřesňuje definici pojmu outsourcing a vyvrací některé rozšířené omyly, které jsou s outsourcingem v bankách spojeny. Dále vysvětluje hlediska dohledu nad finančním trhem a uvádí, z jakých norem regulátor vychází. Podrobněji se zabývá přínosy cloudu i jeho riziky, zejména riziky právními, rizikem ztráty kontroly, rizikem omezení auditovatelnosti, rizikem závislosti na dodavateli, rizikem koncentrace a reputačním rizikem.

Rozhovor s Allanem Antem

strana

Petr Hampel

10

Viceprezident společnosti Gartner představuje model „informační bezpečnosti zaměřené na lidi“ jako protiklad k dosud převládající „informační bezpečnosti zaměřené na pravidla“. Hlavní část rozhovoru je věnována implementacím systémů pro řízení identit (IAM). Allan Ant uvádí hlavní chyby, které pozorování Gartner nejčastěji vedou k selháním takových projektů – důraz na technologii namísto procesů, snaha o příliš důslednou automatizaci a pokusy řešit pomocí IAM soulad s legislativou.

Zálohování ve společnosti Teleplan



strana

Josef Novikmec

15

Případová studie popisuje projekt zálohování obsahu desktopů a laptopů obsahujících data vitální pro chod společnosti – základní technologické volby, testování různých alternativ, výběr dodavatele a produktu, stanovení detailních funkčních požadavků, návrh technického řešení a jeho implementaci. Pozornost je věnována i posuzování návratnosti investice vypočtené na základě porovnání stávajícího a nově nasazeného řešení.

Autentizace: ani silné heslo nestačí



strana

PR Eset

22

„Spoléhat se na dodržování heslové politiky by bylo naivní. Skutečným řešením pro zásadní posílení zabezpečení přístupu k systémům a datům je nasazení dvoufaktorové autentizace,“ konstatuje se v textu, který rozebírá hlavní zásady a možnosti tohoto zabezpečení. Druhá část článku je věnována případové studii – nasazení ESET Secure Authentication v mezinárodní společnosti Allus Global BPO Center.

Behaviorální analýza datového provozu v praxi



strana

Mikuláš Labský, Pavel Minařík

28

Článek vysvětluje potřebu monitoringu provozu uvnitř LAN/WAN sítí a popisuje technologie, které k tomu nejčastěji využívány. Zvláště se věnuje tzv. behaviorální analýze. Její použití demonstrovuje na konkrétních případech nasazení ve společnosti ČD – Telematika a v pražské Thomayerově nemocnici.



ENJOY SAFER
TECHNOLOGY™



Redakce DSM děkuje za spolupráci dlouhodobým obchodním partnerům

Kompromitace dat pomocí SQL Injection – část II.



strana
32

Lukáš Antal, Maroš Barabas, Petr Hanáček

Tato část seriálu se zabývá méně standardními možnostmi útoků pomocí SQL injection a jejich dopadem na bezpečnost systémů. Postupně jsou pojednány operace nad souborovým systémem, zápis dat na disk, zneužití JavaScriptu a metoda Port Scanning pomocí SQL Injection.

Změny v nové verzi PCI DSS 3.0 – část II.



strana
36

Jakub Morávek

Text se věnuje nové verzi normy, která přináší minimální sadu opatření pro zajištění bezpečnosti dat držitelů platebních karet. Popisuje některé změny (zabývá se zejména monitoringem sítí a bezpečnostními politikami) a shrnuje hlavní dopady na požadavky na posuzované organizace a na průběh auditu. Zabývá se také novými verzemi dokumentů, které přesně definují požadavky na audit, včetně formulářů a vzorů dokumentů.

Bezpečnost bezkontaktních platebních karet



strana
41

Martin Henzl, Maroš Barabas
Radim Janča, Petr Hanáček

Úvodní část článku vysvětluje, jak probíhá autentizace karty vůči terminálu, ověření identity vlastníka a autorizace transakce, přičemž pozornost je věnována zejména bezkontaktním kartám navrženým s ohledem na standard EMV. Poté se text zabývá slabými místy v ochraně bezkontaktní karty a nejčastějšími typům útoků – PrePlay, Relay, Replay u SDA a Man-in-the-middle. Konstatuje, že nejúčinnějším způsobem obrany jsou limity na kartě.

Recenze knihy Petra Koubského Úklid, který jste si neobjednali



strana
45

Petr Hampl

RUBRIKY

Virová stránka	44
Normy a publikace	46
IS2	47
Vítání jara	48
Informace z partnerských společností	49
Právníková rubrika	50
Management Summary	51
Tiráž	52

V PŘÍŠTÍM ČÍSLE

3
2014

Data Security Management 3/2014 vyjde 25. září. Najdete v něm rozhovory s expertem na bezpečnost mobilní telefonie Kyrre Sletsjøe a významnou osobností z české veřejné správy. Budeme se věnovat metodikám hodnocení rizik při výpočtu business case pro investice do informační bezpečnosti, přineseme případovou studii o nasazení biometrických podpisů u velkého telekomunikačního operátora i článek o nejčastějších problémech při nasazení SSL certifikátů do webových stránek.