


## O B S A H

Články označené  prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

## Rozhovor se Zdeňkem Adamcem

strana

6

Petr Hampl

Náměstek ministra zemědělství hovoří o dalších záměrech rozvoje informatiky rezortu včetně možného sdílení zdrojů a dat s dalšími rezorty, např. s životním prostředím. Druhá část rozhovoru je věnována informační bezpečnosti – zásadám pro budování bezpečnostní koncepce, spolupráci mezi útvary informační a fyzické bezpečnosti, schvalování investic a praktickým zkušenostem ze skupiny PPF a Volksbank, kde Zdeněk Adamec dříve působil.

## Výkonnostní metriky ve strategiích kybernetické bezpečnosti a role CIO v kyberprostoru



strana

13

Václav Žid

První část textu vymezuje hlavní hráče, kteří se zabývají nebo by se měli zabývat zajištěním relativně bezpečného kyberprostoru. Jsou to vlády, které vytváří rámec, a manažeři IT odpovědní za chování jednotlivých organizací a uživatelů. Dále se zabývá posuzováním investic do informační bezpečnosti v organizaci a možnostmi měření přínosu takových investic. Srovnává strategii kybernetické bezpečnosti USA a EU a diskutuje o otázce, zda má být budování informační bezpečnosti ve firmě založeno na metrikách a proč. V závěru jsou probírány různé relevantní dokumenty a jsou formulována doporučení, na kterých stavět při vytváření metrik pro konkrétní organizaci.

## Nejčastější problémy při použití SSL certifikátů



strana

20

Jindřich Zechmeister

Článek rozebírá nejčastější chyby, jakých se dopouštějí administrátoři při použití bezpečnostních SSL certifikátů. Podrobněji jsou rozebírány následující oblasti: žádost o certifikát a jeho generování, specifika práce v prostředí IIS, řetězení důvěry certifikátů, provoz více domén na jednom serveru, smíšený obsah na webových stránkách, chybějící domény v certifikátu, nedostatečná ochrana vůči zranitelnosti Heartbleed a chybný výběr šifrovacího a podpisového algoritmu. V závěrečné části se pak diskutuje o pro a proti přechodu na protokol SH-2.

## Rozhovor s Kyrre Sletsjøe

strana

10

Petr Hampl

Význam odposlechů je často podceňován, zejména v malých a středních firmách. Ceny poměrně pokročilých technických zařízení klesly tak, že jsou k dispozici i malým kriminálním skupinám, tvrdí norský expert, který se řadu let zabýval bojem proti terorismu. Proto doporučuje důsledně rozlišovat, jaké informace mohou být předávány telefonem, i za cenu snížení efektivity komunikace. Věnuje se rovněž opatřením, jaká jsou finančně a organizačně dostupná i pro malé firmy a mohou významně snížit rizika.

## Představuje BYOD opravdu hrozbu?



strana

18

Dan Rosendorf

První část se zabývá novými riziky, kterým musí v souvislosti s používáním soukromých mobilů a tabletů čelit firemní informatiky. Stanoví zásady ochrany sítí s ohledem na tyto hrozby a dále se zabývá řešeními pro správu mobilních zařízení (Mobile Device Management). Navrhuje jejich rozdělení do dvou základních skupin: Exchange Active Sync (EAS) a diskutuje o omezeních, kterým podléhají oba typy MDM řešení.

## Kompromitace dat pomocí SQL Injection – část III.



strana

25

Lukáš Antal, Maroš Barabas, Petr Hanáček

Závěrečná část seriálu se zabývá rizikem kompromitace serveru na úrovni operačního systému. Popisuje dvě konkrétní metody takové kompromitace, kterými jsou MSSQL a funkce xp\_cmdshell a MySQL a User Defined Functions. Dále popisuje některé konkrétní možnosti obrany proti takovým útokům nebo alespoň zmírnění následků: využití principu nejnižších privilegií, validaci vstupů na nasazení firewallů třídy WAF (Web Application Firewall).

## Systematický přístup k zajištění bezpečnosti kritického informačního systému



strana

30

Marek Solařík

Případová studie z prostředí velkého provozovatele kritické infrastruktury s celostátní působností popisuje, jak bylo řešeno zadání zajistit bezpečnost významného systému, který se již nacházel ve finální fázi implementace. Text podrobněji popisuje výchozí situaci, implementaci systematického přístupu, analýzu síťového provozu, návrh bezpečnostních směrnic, nastavení technických zařízení, audit a testování. To vše v rámci PDCA (Plan-Do-Check-Act) cyklu.





ENJOY SAFER  
TECHNOLOGY™



Redakce DSM děkuje za spolupráci dlouhodobým obchodním partnerům

### Vlastnoruční digitální podpis a jeho implementace v O2 – část I.



strana  
**36**

Aleš Bernášek

Případová studie popisuje projekt zavedení biometrického podpisu v celé prodejní síti O2. První díl se zabývá vymezením cílů projektu, provedením analýzy dopadů, získáním podpory v rámci organizace, vytvořením funkčních požadavků a organizací výběrového řízení na dodavatele technologie. Dále se popisuje vývoj řešení, jeho technologické principy i právní argumentaci, na které je využívání biometrického podpisu založeno.

### Žádaná informační bezpečnost – utopie nebo realita?



strana  
**40**

Richard Michálek

Úvodní část textu se zabývá tím, jaké obvykle bývají cíle manažera informační bezpečnosti v organizaci a jaké konkrétní požadavky z toho vyplývají. Dále se řeší možnosti, jak získat podporu u vedení organizace a dosáhnout přidělení finančních prostředků. Uvádí praktické rady pro komunikaci s manažery, kteří o informační bezpečnosti příliš nevědí. Dalšími diskutovanými tématy jsou přidělení odpovědnosti za rizika a možnosti manažera dosáhnout reálného dodržování bezpečnostních směrnic. V závěru jsou zdůrazněny nutnost pozitivního přístupu manažera informační bezpečnosti a význam jeho schopnosti dlouhodobého zaměření na jasné cíle.

### Recenze knihy Advanced Persistent Threats: How to Manage the Risk of Your Business



strana  
**43**

Luděk Novák

## RUBRIKY

Vírová stránka	<b>44</b>
Letní soirée	<b>45</b>
Normy a publikace	<b>46</b>
Golf v Casa Serena	<b>47</b>
TOP ICT Garden Party	<b>48</b>
Informace z partnerských společností	<b>49</b>
Právnícká rubrika	<b>50</b>
Management Summary	<b>51</b>
Tiráž	<b>52</b>

## V PŘÍŠTÍM ČÍSLE

**4**  
2014 Data Security Management 4/2014 vyjde 4. prosince. Najdete v něm rozhovory s Janem Ellermannem z Europolu a významnou osobností z českého průmyslu. Budeme se věnovat systémům SIEM a praktickým aspektům biometrických řešení. Přineseme rovněž pokračování případové studie z O2 a další zkušenosti českého CISO.