


## O B S A H

Články označené  prošly odborným recenzním řízením.

### Rozhovor s Vítězslavem Bogačem

strana

Petr Hampl

6

S CIO společnosti ČEZ o výzvách, které stojí před podnikovou informatikou, outsourcingu, komoditních službách, zdůvodňování investic do bezpečnosti i tom, kterým změnám bezpečnostní obavy brání. A také o zákonu o kybernetické bezpečnosti i o tom, jaké account manažery mají rádi informatici ČEZu.

### Rozhovor s Juvallem Ben Mošem

strana

Petr Hampl

11

Expert na forenzní zkoumání mobilních telefonů připomíná, že útočníci se mohou dostat do jakéhokoli mobilního zařízení, ale tvrdí, že přesto není třeba mít z nových sledovacích technologií obavu. Zločinci se k nim údajně hned tak nedostanou.

### Autentizace 2022



strana

Vašek Matyáš

18

Článek se po úvodní rekapitulaci fundamentálních pojmů v oblasti autentizace uživatelů věnuje rozboru některých zásadních probíhajících a očekávaných změn v oblasti autentizace uživatelů. Dále následuje pokus o rozbor zásadních faktorů s potenciálem budoucího vlivu na to, jakým způsobem bude prováděna autentizace nejen uživatelů, ale i částí systémů reagujících s uživateli.

### Využití zahraničních norem při přípravě cloudových řešení v organizacích veřejné správy



strana

Václav Žid

28

Jak postupují centrální úřady při hodnocení rizik spojených s přechodem do cloudu? Autor konstatuje, že situaci komplikuje neexistence norem a dalších závazných dokumentů. Je nicméně možné využít zahraničních norem, zejména těch, které jsou určeny pro americké federální úřady. Článek informuje o zdrojích ENISA, programu Cloud First a FedRAMP (řízení rizik). V další části se zaměřuje na popis referenčního modelu a doporučeného způsobu hodnocení rizik.

### Zamyšlení Ivana Pilného

strana

10

Orgány veřejné správy provozují v současné době 5,5 tisíc informačních systémů. Mnohé byly realizovány na základě zpackaných tendrů, chybných zadání a byly zprovozněny bez pilotního provozu. Výsledkem jsou promarněné miliardy a často i negativní dopady na občany.

### Testování nástrojů antivirové ochrany



strana

Petr Šnajdr

12

Autor se v úvodu zabývá obecnějšími problémy testování produktů a služeb IT bezpečnosti, dále diskutuje o shromažďování vzorků škodlivých kódů, na nichž by měly být antiviry testovány, k jakým chybám při tom nejčastěji dochází a co přesně z testů vyplývá. Další část se podrobněji věnuje schopnosti detekce antivirových programů a možnostem, jak sestavit pořadí testovaných produktů. Závěrečná část je věnována testování systémové náročnosti produktů.

### Změny v nové verzi PCI DSS 3.0. – část I.



strana

Jakub Morávek

22

Aktuální verze normy Payment Card Industry Data Security Standard vstoupila v platnost na konci loňského roku. Článek vysvětluje, na koho se norma vztahuje, a dále podrobně rozebírá tříletý životní cyklus normy a její aktualizace. Poté postupuje po jednotlivých kapitolách a probírá změny proti minulé verzi – úvodní ustanovení o aplikaci normy, konfigurace firewallů, ochrana uchovávaných dat, šifrování přenosu dat, ochrana proti malware, vývoj systémů a aplikací a omezení přístupu k informacím.

### Evropská direktiva o elektronických podpisech a elektronické komunikaci



strana

Martin Vondrouš

32

Nová direktiva má poskytnout konzistentní legislativní rámec a přispět k využívání elektronických prostředků mezi subjekty z různých států EU. Článek shrnuje stav dosavadní legislativy a zabývá se jednotlivými oblastmi, které návrh směrnice pokrývá – požadavky na elektronické podpisy, požadavky na archivaci, kvalifikované certifikační autority, systémy elektronické identifikace, kvalifikované doručování a ověřování certifikátů webových stránek.

# V PŘÍŠTÍM ČÍSLE

Příští číslo DSM vyjde 17. června a najdete v něm rozhovor s IT osobností z bankovníctví a případovou studii z oblasti business continuity planning. Budeme se zabývat regulacemi ČNB, přineseme recenzi knihy Petra Koubského o identity managementu a budeme se věnovat motivaci uživatelů k dodržování směrnic. Budou pokračovat seriály o útocích na weby metodou SQL injection a o nové verzi normy PCI DSS.

## Kompromitace dat pomocí SQL Injection – část I.



strana  
**36**

Lukáš Antal, Maroš Barabas, Petr Hanáček

Text vysvětluje, jakým způsobem jsou nejčastěji prováděny útoky na webové systémy napojené na databáze. Objasňuje obecný princip SQL injekce a věnuje se čtyřem konkrétním postupům: Zřetěžené dotazy, UNION dotazy, Blind SQL Injection a Time based Blind SQL Injection.

## Dvě recenze knihy Karla Burdy Aplikovaná kryptografie

strana

**46**

Tomáš Foltýnek

Michal Valášek

**47**

## Správa identit v systému Czech POINT s vazbou na základní registry



strana  
**40**

Martin Šlancar

Případová studie popisuje procesy a technologickou architekturu decentralizovaného přidělování identit, které umožňuje spravovat 100 tisíc uživatelů systému Czech POINT z 8 tisíc organizací. Dále popisuje Jednotný identitní prostor, zabývá se zadáními vzniklými v souvislosti se zavedením základních registrů a způsobem řešení těchto zadání. Závěrečná část je věnována probíhající synchronizaci dat mezi údaji o uživatelích v jednotném identitním prostoru a údaji o týchž osobách v základních registrech.

# RUBRIKY

Vírová stránka

**45**

Normy a publikace

**48**

Informace z partnerských společností

**49**

Právnícká rubrika

**50**

Management Summary

**51**

Tiráž

**52**

Redakce DSM děkuje za spolupráci dlouhodobým obchodním partnerům



ENJOY SAFER  
TECHNOLOGY™



SOLVE IT TOGETHER