

O B S A H

Hlavní téma čísla: Bezpečnost mobilních technologií a počítačových sítí

Články na str. 10–45 prošly odbornou oponenturou redakční rady DSM.

INTERVIEW S GIDONEM PELYM

S viceprezidentem společnosti Cyber-Ark Software pro South/East Europe diskutuje na téma jeho zkušeností s eliminací rizik spojených s privilegovanými účty šéfredaktor DSM.

strana

6

TABLETY A SMARTPHONY, NASAZENÍ V KORPORÁTNÍM PROSTŘEDÍ RICHARD MICHÁLEK

Tato mobilní zařízení přinesla novou dimenzi do našeho života – být online kdykoli a kdekoli – mít možnost pracovat kdykoli a kdekoli. Zajistit bezpečnost na těchto zařízeních se stalo pro korporace novou výzvou při ochraně svých informací. Tento článek se věnuje právě této problematice z pohledu principů, praxe a zkušeností autora.

strana

10

BEZPEČNOST PODNIKOVÝCH MOBILNÍCH ZAŘÍZENÍPETR MOLÁČEK, RADEK VAJNER
JAROSLAV DOČKAL

Na trhu je dnes široká škála více či méně vyspělých řešení pro vzdálenou správu – označovány jsou akronymem MDM (Mobile Device Management). Při správě sítí se setkáme i s řadou dalších omezení, které vyplývají z odlišných schopností jednotlivých mobilních platforem a jejich verzí. Článek vysvětluje, proč je pro mobilní platformu již zavedený protokol EAS (Exchange ActiveSync) jen vhodným doplňkem, a upozorňuje, na co by se měl zákazník při volbě svého řešení pro vzdálenou správu zaměřit.

strana

14

GEOLOKACE A BEZPEČNOST POČÍTAČOVÝCH SÍTÍ

PAVEL ČELEDA, JOSEF KADERKA

Článek seznamuje s problematikou určování geografické polohy uživatelů (zařízení) na Internetu. Na vybraných příkladech jsou uvedeny hrozby využívající geolokaci k novým formám útoků. Závěr je věnován možnostem využití geolokace v oblasti bezpečnosti počítačových sítí a detekce anomálií.

strana

18

ZÁPLAVOVÉ APLIKAČNÍ ÚTOKY ODEPŘENÍ SLUŽBY

VÍT BUKAČ

V posledních letech se stále častěji setkáváme s aplikačními útoky odepření služby zaměřenými na útoky proti webovým serverům. V článku jsou proto vysvětleny jejich základní charakteristiky a je provedeno srovnání se síťovými útoky odepření služby. Detailně jsou popsány útoky typu HTTP GET flood, Slowloris, R-U-D-Y a THC SSL DoS. U každého typu útoku jsou probrány možné způsoby obrany.

strana

22

ISO 22301 NAHRAZUJE BS 25999-2

LIBOR ŠIROKÝ

První certifikační standard pro systémy řízení kontinuity (Business Continuity Management Systems, BCMS) BS 25999-2:2007 ukončí svou platnost 1. listopadu 2012. Bude nahrazen ISO 22301:2012, který se pyšní titulem první mezinárodní standard pro BCMS. Cílem článku je přiblížit čtenářům změny, které nový standard přináší, a jaké budou mít tyto úpravy dopad na organizace mající BCMS podle tohoto standardu zaveden a certifikován, popř. jsou již v pokročilé fázi implementace podle BS 25999-2.

strana

26

KE TŘEM REALIZACÍM ZPRAVODAJSKÉHO MALWARU

JAROSLAV DOČKAL

Během jednoho roku byly postupně odhaleny tři útoky nového typu – dálkově ovládaného zpravodajského malwaru. Článek popisuje, jak jsou u nich využity slabiny Windows, komunikační protokoly a kryptografické techniky. Porovnává jednotlivé útoky navzájem a uvádí do souvislosti s tolik diskutovaným Stuxnetem.

strana

30

Redakce DSM děkuje
za spolupráci dlouhodobým
obchodním partnerům

ITIL V3, EDICE 2011 – ČÁST III

VLADIMÍR KUFNER

Jak ovlivní všemi velebený, ale někdy i zatracovaný cloud implementaci procesů ITIL, resp. jak ovlivní chod oddělení IT? Dopadá nasazení cloudu na všechny etapy životního cyklu služeb, nebo pouze na některé z nich? Platí, že s implementovanými procesy nemusíme nic dělat, nebo je musíme kompletně zrekonstruovat? Autor se zamýšlí nad těmito otázkami i obecně nad faktem, zda cloud může skutečně poskytnout očekávané přínosy, jaká jsou rizika, resp. jaké jsou podmínky úspěchu.

strana
34

ZADÁVACÍ KRITÉRIA VEŘEJNÝCH ZAKÁZEK V ICT – ČÁST I

DAVID C. HÁJÍČEK

Článek pojednává o zadávacích kritériích používaných při zadávání veřejných zakázek v oblasti informačních a komunikačních technologií (ICT). Cílem článku je shrnout, jaká kvalifikační a výběrová kritéria v ICT zakázkách veřejný sektor zpravidla používá, a diskutovat o jejich vhodnosti a legálnosti. Pozornost je věnována rovněž možným dopadům porušení zákona o veřejných zakázkách a způsobu, jak by měli dodavatelé postupovat, jsou-li přesvědčeni, že k porušení došlo.

strana
38

FORMÁTY PRO ZARUČENÉ ELEKTRONICKÉ PODPISY – ČÁST IV

LIBOR DOSTÁLEK

Článek obhajuje dynamický biometrický podpis jako zaručený elektronický podpis. Dále se zabývá používáním dalších alternativních elektronických podpisů a podpisů založených na PKI. Jako alternativní elektronické podpisy zmiňuje např. podpisy, založené na sdíleném tajemství a SMS podpisy.

strana
42

ZPRÁVA IBM X-FORCE: STRUKTURA IT RIZIK SE LONI VÝRAZNĚ ZMĚNILA

PR IBM

Společnost IBM každoročně zveřejňuje zprávu o IT bezpečnosti nazvanou X-Force. Ta letošní poukazuje na překvapivé změny.

strana
46

RUBRIKY

| | |
|---|----|
| Vírová stránka | 48 |
| Informace partnerských společností, připravované konference | 49 |
| Aktuality a personálie | 50 |
| Fotoreportáž z akce „Vítání léta s...“ | 51 |
| Právní poradna - ptáme se právníka | 52 |
| Management summary | 53 |
| Tiráž | 54 |

 **ERNST & YOUNG**
Quality In Everything We Do



we protect your
digital worlds

