

Rozhovor s Udo Helmbrechtem, ředitelem ENISA

Adam Lamser



strana
8

V tomto vydání jsme nahlédli do fungování Evropské agentury pro bezpečnost sítí a informací (ENISA). Jejím výkonného ředitele Udo Helmbrechta jsme se ptali, jak se daří naplňovat poslání agentury, kterým je osvěta v oblasti kybernetické bezpečnosti, a dále na připravované zavedení bezpečnostních certifikací.



Vážná zranitelnost (nejen) elektronických občanek: ROCA (CVE-2017-15361) rok poté

Petr Švenda, Václav Matyáš



strana
15

Tento článek představuje roční ohlédnutí za kritickou zranitelností ve způsobu generování kryptografických klíčů v čipových kartách („ROCA“), která se nachází v odhadem 1-2 miliardách čipů. Tato návrhová chyba byla přehlédnuta během certifikací dle NIST FIPS 140-2 i Common Criteria EAL 5+ a zůstala neodhalena po dobu více než 15 let. Vedla k široce rozšířeným zranitelným zařízením včetně průkazů totožnosti několika evropských zemí, čipů TPM využívaných pro šifrování disků pomocí Microsoft Bitlocker či tokenů pro šifrování komunikace dle PGP a zaručený elektronický podpis dle eIDAS. Zranitelnost vede k možnosti vypočítat privátní klíč z pouhé znalosti klíče veřejného. Útok lze snadno paralelizovat na více výpočetních jádrech a tím ho prakticky libovolně zrychlovat.

Jak na bezpečné zavádění cloudových služeb – část V.

Martin Zbořil, Michal Wojnar



strana
27

Společnost PricewaterhouseCoopers zkoumala ve spolupráci s TATE International, s.r.o. úroveň povědomí o bezpečnosti cloudových služeb. Průzkum se zaměřil na využívání cloudových služeb v organizacích, jejich bezpečnostních rizik, přínosů, opatření a kontrol. Součástí průzkumu byly také otázky na compliance a státní cloud. Tento článek přináší druhou část přehledu nejzajímavějších výsledků, které průzkum nabídl.

Stěhování datového centra jako „ostrý test“ Business Continuity

Josef Rech



strana
12

Může Vám pomoci zavedené Business Continuity a Disaster Recovery plánování i při takových aktivitách, jako stěhování datového centra? Samozřejmě, že může. Konkrétní situaci, přípravu na stěhování, její průběh a výsledek, včetně role BCM, lze ukázat na Raiffeisenbank, kde stěhování datového centra před pár měsíci proběhlo. Přestože za vlastním stěhováním stálo hlavně úsilí kolegů z IT, je bez pochyb, že celá akce proběhla snáze právě díky tomu, že v Raiffeisenbank je již po několik let vybudována a pravidelně testována infrastruktura umožňující převést provoz kritických aplikací do záložního datového centra a neomezovat tak klienty či zaměstnance ve využívání systémů a služeb banky. Přínos se prokazatelně ukázal i v pravidelném trénování členů krizového štábu a týmů obnovy.

Co nového přináší TLS 1.3

Jaroslav Dočkal



strana
21

Článek rozebírá, co přináší nová verze protokolu TLS z hlediska bezpečnosti a výkonosti. Dále podrobně analyzuje, jak se v něm odráží pokroky v kryptografii. Upozorňuje, že dilema mezi požadavky výkonu a bezpečnosti se promítá i do samotného TLS 1.3, a to do rozhodování mezi dvěma variantami procesu obnovy relace.

DevOps – část III.

Vladimír Kufner



strana
31

Další díl seriálu probírá klíčové principy a koncepty uplatňované v rámci DevOps, včetně asi nejznámějšího principu tzv. tří cest (Three ways). Dále se v textu rozebírají vybrané praktiky, jejich definice a podrobnější vysvětlení.

Zážitkovost a interaktivita vzdělávání dětí v oblasti kybernetické bezpečnosti



strana
38

Pavλίna Jedličková

Význam integrace problematiky kybernetické bezpečnosti do edukačního procesu nabývá v posledních letech na důležitosti. Otázkou však zůstává, jaké vzdělávací metody jsou z pohledu této problematiky nejefektivnější. Článek seznamuje s interaktivními a zážitkovými metodami vzdělávání žáků základních škol v oblasti kybernetické bezpečnosti a nabízí ukázkou vzorové interaktivní aktivity pro žáky šestých a sedmých tříd.

Dynamický biometrický podpis pro podnikovou prax



strana
42

František Hortai

Podpis je prirodzený, ľahko dostupný, používateľom dobre známy nástroj pre preukázanie svojej identity. Autentizácia osôb pomocou dynamického biometrického podpisu (DBP) dokáže zvýšiť kybernetickú bezpečnosť a paralelne zefektívniť komunikáciu v podniku. Článok sa zameriava na výhody a úskalia DBP, pričom sa reprezentujú riešenia a rady pre organizácie na úspešnú implementáciu DBP.

Informační aktiva a rizika – část II.



strana
48

Miroslav Buda

Ve druhém díle autor popisuje řešení dříve prezentovaných problémů s řízením informačních aktiv a rizik. Při něm využívá zkušeností získaných při implementaci zákaznických projektů a zaměřuje se na možnosti využití dedikovaných informačních systémů, které srovnává s manuálním zpracováním. Závěrem jsou vyjmenovány klíčové pilíře, na kterých by měla stavět každá organizace implementující moderní řízení informačních aktiv a rizik.



20 LET IS2

...bezpečnost každého z nás?!

29.–30. května 2019
PRAHA – KAROLINUM

www.is2.cz

RUBRIKY

Virová stránka

53

Normy a publikace

55

Blahopřání

56

Informace z partnerských společností

57

Právní rubrika

58

Management summary

60

Tiráž

62