

## Rozhovor s Jaroslavem Jakubčkem

strana

6

Adam Lamser

Jaroslav Jakubček působí v Evropském centru pro boj proti kyberkriminalitě, které funguje při Europolu, jako jediný zástupce z České i Slovenské republiky. Ptali jsme se ho proto především, v čem tato práce spočívá, co konkrétně je její náplní a jaké problémy v současné době řeší.



## Bezpečnost technologií mobilního zdravotnictví (mHealth)



strana

16

Zdeněk Gütter

Využívání mobilních aplikací ve zdravotnictví (mHealth) – jak profesionály, tak pacienty – je spojeno s mnoha otázkami týkajícími se bezpečnosti. Článek uvádí, jak různé druhy bezpečnosti ovlivňují účinnost, spolehlivost, důvěryhodnost a kvalitu mobilních aplikací v praxi. Přitom si klade za cíl podnítit diskusi mezi bezpečnostními odborníky v ČR k fenoménu mobilních aplikací, pro jehož komplexní otázky zatím v zemích EU se společným trhem neexistuje univerzální řešení.

## Blockchain a bezpečnost



strana

25

Jakub Jedlinský

Článek se zabývá tematikou bezpečnosti technologií distribuované účetní knihy (DLT) se zaměřením na blockchain. V první části se věnuje nepřilíh zkoumanému tématu, a sice roli důvěry v tyto DLTs. Zohledňuje širší systémové hledisko. DLTs bývají zkratkovitě označovány jako řešení odstraňující potřebu důvěry, což je přinejmenším zavádějící. Druhá část je věnována problematice nových bezpečnostních výzev, se kterými se musejí vypořádat sami uživatelé.

## Jak uživatelé přemýšlejí o bezpečnosti v kontextu mobilního bankovníctví?



strana

11

Petr Doležal, Agáta Dařbujanová, Lenka Knapová

Článek se věnuje tématu usable security. V teoretickém úvodu je představen koncept mentálních modelů a význam jejich zkoumání pro vývoj bezpečných systémů. V praktické části jsou představeny výsledky uživatelské studie autentizačních metod v rámci mobilního bankovníctví.

## Blackout – energetické společnosti se připravují na minimalizaci následků



strana

22

Pavel Veselka

Pokud nastane Blackout, lidé ocení každou pomoc a informaci. Autor popisuje zkušenosti ze společných cvičení distributora elektřiny s krajskými úřady. Zdůrazňuje důležitost rychlého přenosu kvalitních informací a vzájemnou pomoc mezi lidmi a institucemi. Energetika se snaží pomoci aktivací lokálních zdrojů elektřiny.

## Využití umělé inteligence v zabezpečení IT



strana

30

Michal Hebeda

Autor popisuje vývoj a reálné využití umělé inteligence v praxi v oblasti IT bezpečnosti. Věnuje se zejména nástupu strojového učení a jeho fázím, definuje oblasti, ve kterých může umělá inteligence pomoci ve zvýšení bezpečnosti.

## Jak na rizika – část III.

Richard Michálek

Další díl seriálu „Jak na rizika“ přináší specifika analýzy a řízení rizik bezpečnosti informací, praktický přístup k realizaci a tipy na snížení pracnosti a zvýšení srozumitelnosti.



strana

33

## DevOps – část IV.

Vladimír Kufner

Tento článek shrnuje nejlepší praktiky v oblasti implementace DevOps, upozorňuje na časté chyby a na věci, kterým je lepší se vyhnout. Popisuje odlišné požadavky a doporučení, které jsou pro DevOps specifické, jako jsou třeba organizační struktury, procesy a role.



strana

42

## RUBRIKY

Virová stránka

53

Normy a publikace

55

Informace z partnerských společností

56

Právní rubrika

57

Management summary

60

Tiráž

62

## Případová studie: implementace DLP v České průmyslové zdravotní pojišťovně

Matej Zachar

Případová studie nasazení Data Loss Prevention (DLP) systému přibližuje, jak může vypadat nasazení DLP v praxi. Na příkladu společnosti Česká průmyslová zdravotní pojišťovna jsou znázorněny jednotlivé části implementačního projektu od úvodní analýzy až po akceptaci uživateli a uvedení do ostrého provozu. Představena je jak architektura, tak konkrétní koncept implementace DLP do prostředí organizace.



strana

38

## Celostní přístup ke kybernetické bezpečnosti

Miroslav Nečas

Na kybernetickou bezpečnost nelze nadále hledět jako na problematiku ICT, ale je třeba k ní přistupovat celostně. To znamená vnímat kybernetickou bezpečnost v kontextu naplňování poslání organizace a udržování její konkurenceschopnosti, což vyžaduje posílení mezioborové komunikace uvnitř firmy a schopnost propojovat informace z ICT infrastruktury s informacemi z dalších zdrojů uvnitř i vně organizace. To je možné efektivně realizovat pomocí nadstavbové platformy, která konsoliduje informace ze SIEM systémů, monitoringu firem a osob, systémů řízení výroby a majetku a dalších informačních systémů.



strana

48