

## Michael A. Goedecker

Adam Lamser, Daniela Seigová

Rozhovor s autorem přednášky na téma „Hybridní válka: Zbraň doby kybernetické aneb co činí Vaši organizaci cílem“ na mezinárodní konferenci IS2. V rozhovoru odpovídá na otázky týkající se umělé inteligence, výhod a nevýhod online kurzů, vývoje trendů kyberbezpečnosti a další.



strana

6

## Forenzní analýza šifrovaných dat

Radek Hranický

Článek se zabývá automatizovanou kryptoanalýzou zabezpečeného obsahu. Diskutuje různé typy útoků a význam akcelerace pomocí GPU a distribuovaného zpracování. Jednotlivé techniky jsou ilustrovány na konkrétních nástrojích.



strana

14

## První rok Aktu o kybernetické bezpečnosti aneb co je nového?

Václav Stupka, Jakub Vostoupal

Druhý díl série věnující se problematice certifikace kybernetické bezpečnosti, která se stává pro Českou republiku i Unii stále více důležitou, seznamuje čtenáře s tím, co se událo důležitého za více než rok od přijetí Aktu o kybernetické bezpečnosti. Pozornost je přitom věnována nejen chystaným certifikačním schémátům, ale i přípravě Průběžného pracovního programu, klíčového dokumentu celého certifikačního rámce, a vysokým ambicím, které chce Česká republika v rámci unijního certifikačního trhu naplnit.



strana

26

## Průzkum: Bezpečné zdravotnictví v ČR 2020 – část I.

Karolína Kubínová, Michal Wojnar

Společnost PricewaterhouseCoopers zkoumala ve spolupráci s TATE International úroveň kyberbezpečnosti ve zdravotnickém sektoru. Průzkum se zaměřil na vývoj technologií ve zdravotnictví v příštích letech, jejich zabezpečení a určení nejvýznamnějších překážek zabraňujícím v řádném kyberbezpečnosti zdravotnických zařízení. Součástí průzkumu byly mimo jiné také otázky na ovlivnění situace virem COVID-19, na vnímání citlivosti dat nebo identitu aktérů hrozeb mířících proti zdravotnictví. Tento dvoudílný seriál přináší první část přehledu nejzajímavějších výsledků, které průzkum nabídl.



strana

10

## Likvidace nosičů dat a jejich obsahu v teorii a praxi – část II.

Vladimír Smejkal

Článek uvádí výsledky průzkumu, který provedla redakce DSM v odborných kruzích o tom, jak je v praxi prováděna likvidace nosičů dat. Hlavními výsledky jsou: zdaleka ne všechny firmy mají provedenu klasifikaci informací, neexistuje dostatečná odpovědnost za proces likvidace a firmy se příliš spoléhají na externí poskytovatele služeb. Další průzkum se zaměřil na tyto poskytovatele a konstatoval, že jejich informace mají vysloveně marketingový charakter, většina společností nemá žádnou certifikaci a nenabízejí kontrolu zákazníka nad procesem likvidace. V závěru je kriticky zhodnocen konkrétní příklad z praxe.



strana

19

## Akcelerace analýzy síťového provozu

Jan Kořenek, Lukáš Kekely, Pavol Korček

Chtěli byste vědět, jak zajistit zpracování síťového provozu, aniž by docházelo ke ztrátě dat? Odpověď najdete v článku, který popisuje, jak využít hardwarovou akceleraci při analýze aplikačních protokolů. Článek ukazuje, jak se dá využít charakteristika síťového provozu a dosáhnout pomocí hardwarové akcelerace vysokou propustnost i flexibilitu. Techniky akcelerace jsou ukázány na příkladu sondy pro zákonné odposlechy pracující na úrovni aplikačních protokolů.



strana

30

## Je Windows server 2019 pro vás to pravé?

Oldřich Šrubař, Jan Žák



strana

35

Windows Server 2019 prošel řadou inovací v oblasti bezpečnosti, těsnějšího propojení s Microsoft Azure, lepší kontejnerizací a vylepšeními na Hyper-Converged infrastruktuře. Všechny tyto oblasti postupně probereme v následujícím článku včetně novinek a toho co se změnilo oproti předchozí verzi systému. Podrobněji se zaměříme na vylepšení v bezpečnosti a jak vám může tento operační systém pomoci ochránit vaše firemní data a zdroje.

## Hodnocení zranitelností – část I.

Lubomír Almer, David Pecl



strana

47

Většina databází zranitelností dnes pracuje s hodnocením zranitelností založených na Common Vulnerability Scoring Systemu (CVSS). Výrobci technologií typu Vulnerability Management k doplnění hodnocení používají proprietární metody, u kterých však není zveřejněn detailní princip jejich fungování. V článku budou detailněji rozebrány dvě neznámější metody CVSS a OWASP Risk Rating, princip, na kterém fungují, jejich výhody a nevýhody. Druhá část bude zaměřena na návrh nové metodiky pro hodnocení zranitelností, která bude minimalizovat identifikované nedostatky.

# RUBRIKY

Virová stránka

53

Normy a publikace

55

Informace z partnerských společností

56

Konference IS2

57

Právní rubrika

58

Management summary

60

Tiráž

62

## Co přináší ITIL 4 – část I.

Vladimír Kufner



strana

42

Článek popisuje účel nejlepší praktiky ITIL a důvody vzniku aktualizace ITIL na verzi 4 a sumarizuje historii u předchozích verzí. Zároveň vysvětluje hodnotový systém služeb SVS.

**„Zpracování není možné plně automatizovanou umělou inteligencí. Jednoduše nemůžete nahradit vyškolené operátory, kteří procházejí data. Zkoušel jsem to se svým systémem. Může přinejlepším urychlit analýzu dat na první úrovni a vyřešit spoustu pracovní zátěže, ale poté stále potřebujete lidi, aby prošli zbytkem dat a opatrně je vyladili na základě daného způsobu použití...“**

...Rozhovor s Michaelem A. Goedekerem najdete na str. 6.