


Články označené  prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

## Rozhovor s Karlem Řehkou – část II.

Daniela Seigová

strana  
7

Brigádní generál Ing. Karel Řehka byl 20. března 2020 jmenován ředitelem Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Ve druhém dílu rozhovoru pro DSM odpovídá na otázky ohledně postavení NÚKIB v rámci světových struktur, vzdělávání mládeže, budoucnost kybernetických hrozeb, digitalizaci společností a další.



## Výzva jménem DSAR ...aneb jak má správce postupovat, když mu přijde žádost o přístup k osobním údajům – část II.

Petra Věžníková

strana  
18

Článek se zabývá právem subjektu údajů na přístup a kopii údajů (dle č. 15 GDPR). Druhá část příspěvku obsažená v tomto vydání přináší pohled na procesní aspekty práva na přístup z pohledu správce osobních údajů a představuje vzorový návod postupu pro správce osobních údajů při vyřízení žádosti o přístup.

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

Vladimír Smejkal

strana  
28

První díl článku o likvidaci nosičů dat a jejich obsahu se zabývá především právními a technickými normami, které ukládají povinnosti nebo informují o různých způsobech likvidace dat. Je zde popsána likvidace nosičů s utajovanými informacemi a podle zákona o kybernetické bezpečnosti, resp. jejich prováděcích předpisů. V závěru jsou popsány technické normy týkající se likvidace nosičů dat a dat samotných, jako jsou U.S DoD, NIST, EN BS, DIN, ISO/IEC apod.

## Cloudové služby z hlediska ochrany osobních údajů

Lenka Suchánková

strana  
11

Článek pojednává o některých dopadech Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), dále jen obecné nařízení nebo GDPR, na poskytování cloudových služeb. Zamýšlí se nad postavením zákazníka a poskytovatele cloudové služby z perspektivy GDPR a rozebírá některé důsledky vyplývající z postavení správce, zpracovatele, společných správců a subzpracovatelů. Ve své druhé části se článek zamýšlí nad některými aktuálními problémy spojenými s přeshraničním zpracováním osobních údajů v cloudu, zejména nedostatečností smluvních a jiných nástrojů jako jsou standardní smluvní doložky a nedávno zrušený Privacy Shield.

## IT bezpečnost v agilním světě

Radovan Vacek

strana  
22

IT bezpečnost je v agilním světě „enabler“, který jednotlivým týmům a tribeům umožňuje dosahovat jejich business cíle při zachování akceptovatelné míry IT rizik. Téma agilního řízení, a to nejen ve vztahu k software, nepopíratelně přinesla světu množství progresivních technologií a postupů, které však sebou nesou i změnu paradigmatu, a to jak v rovině technické, tak v rovině organizační a kulturní. Článek se pokouší tvrzení zasadit do reálného prostředí agilně řízených a na technologie silně orientovaných společností a pojmenovat kulturní i technické aspekty činnosti týmu IT bezpečnosti.

## Pojistné podmínky pojištění kybernetické bezpečnosti

Petr Dobiáš

strana  
34

Článek obsahuje analýzu pojištění kybernetických rizik nabízených vybranými pojišťovnami. Pozornost je věnována pojistným podmínkám v České republice, Německu a Spojeném království. Pojistné podmínky jednotlivých pojišťoven se podstatně liší z hlediska rozsahu pojistného krytí, což je třeba mít na paměti při volbě vhodného pojištění. Kromě toho jsou předmětem rozboru také aktivity vládních a nevládních organizací v oblasti pojištění kybernetických rizik. Tyto aktivity jsou v současnosti zaměřeny především na vypracování zpráv a doporučení založených na konzultacích s pojišťiteli a dotazníkových šetřeních.

DSM 3 | 2020

DSM Obsah

## Příčiny a dopady SSRF zranitelnosti

Jozef Karlík

strana  
39

Útok, při kterém útočník přiměje nějakou serverovou službu k odeslání požadavku na jinou serverovou službu a následné přeposlání odpovědi útočníkovi, se nazývá Server Side Request Forgery (SSRF). Byť SSRF útoky prošly značnou evolucí, zůstávají relevantní zejména díky implicitní důvěře nebo obecně laxnímu přístupu k bezpečnosti, který vede k ponechání zneužitelných cílů v dosahu útočníků. Článek rozebírá podstatu SSRF útoků, příčiny a dopady zranitelnosti serverů na tento útok.

## Ochrana proti kyberútokům nejen ve zdravotnictví: klíčový je nový pohled na zabezpečení

PR VMware

strana  
50

## Ransomware – aneb poznejte kybernetického čísla 1

Jakub Alimov

strana  
44

Článek předkládá fakta o vyděračském software, tzv. ransomware. Stručně popisuje historii vzniku a další vývoj tohoto typu škodlivých programů a uvádí příklady z praxe, kdy zneužití ransomware vedlo k vysokým finančním ztrátám, případně k dalšímu ohrožení lidí či majetku. V závěru shrnuje možnosti, jak se kybernetickým hrozbám a vydírání bránit.

Virová stránka	52
Normy a publikace	54
Metamorfosa: Nutné kroky k bezpečnému zdravotnictví – X dní po kyberútocích na nemocnice v Benešově, Brně, Ostravě a dalších	55
Informace z partnerských společností	56
Metamorfosa: Letní soirée	57
Právní rubrika	58
Management summary	60
Tiráž	62

**„Vedle přípravy lidí musíme také bedlivě sledovat vývoj technologií a v tomto směru smysluplně investovat do vědy a výzkumu. ČR bude kromě pasivní ochrany kyberprostoru muset nutně disponovat také aktivní obranou včetně ofenzivních schopností, které dříve či později budeme muset použít.“**

...Rozhovor s Karlem Řehkou najdete na str. 7.