

Rozhovor: Tomáš Halajčuk

Martin Haloda

Mgr. Tomáš Halajčuk, Ph.D. je mimo jiné absolventem Lékařské fakulty Univerzity Palackého v Olomouci v magisterském oboru Ekonomika a řízení ve zdravotnictví a doktorského studijního oboru Sociální lékařství na Lékařské fakultě Masarykovy Univerzity v Brně. Od roku 2003 do roku 2022 působil na různých funkcích ve vojenském zdravotnictví. Od roku 2014 do roku 2017 pracoval na Generálním štábu Armády České republiky. Od roku 2017 do roku 2021 sloužil v Belgii na vrchním velitelství sil NATO v Evropě, na pozici hlavního důstojníka pro plánování a řízení výcviku ve vojenském zdravotnictví NATO. Od roku 2022 je předsedou představenstva Zdravotnického holdingu Královéhradeckého kraje. V rozhovoru se jej ptáme na jeho historii v NATO, vzdělávání personálu, telemedicínu, umělou inteligenci ve zdravotnictví a další.



strana

7

Aréna kybernetické války ukrajinskýma očima – část II.

Yehor Safonov

V textu je kladen důraz na vývoj kybernetických útoků proruských hackerů na Ukrajinu na pozadí právě probíhajících válečných střetů. Článek se zaměřuje na sofistikované vektory útoků, které se v rámci ruské invaze na Ukrajinu vyskytly, a na propojenost útoků kybernetického a fyzického světa. Následně je zde nastíněna historie hlavních technik a mechanismů útoků od počátku konfliktu s důrazem na využití co nejaktuálnějších informací. Závěr textu, který mimo jiné zahrnuje i efektivní techniky obrany, se věnuje preventivním opatřením, s jejichž pomocí by bylo možné útokům předejít. Zmíněny jsou i kritické body českých kybernetických prostorů, které je nutné mít na zřeteli při implementaci a provozu bezpečnostního monitoringu.



strana

16

Rozhovor: David Doležal

Martin Zbořil

Ing. David Doležal je Director of Security ve startupu Productboard. Jeho hlavním úkolem je pomoci chránit data klientů v cloud-based SaaS prostředí s kontinuálním vývojem platformy a současně získání potřebných certifikací (SOC2, ISO 27k) pro přesvědčení i enterprise zákazníků, že data nemusí být jen u nich v budově na jejich serveru a přesto budou v bezpečí. V rozhovoru se jej ptáme na aktuální bezpečnostní výzvy, bezpečnostní požadavky, IT bezpečnost u startupů a další.



strana

27

Kde jsou slabá místa měkkých cílů a jak je odhalit?

Jiří Slabý, Tomáš Fröhlich

Výchozím a zároveň nezbytným krokem pro nastavení adekvátní ochrany měkkého cíle je proces posouzení rizik, který se v této oblasti nazývá vyhodnocením ohroženosti. Hlavním cílem tohoto procesu je zhodnotit konkrétní měkký cíl a následně odhalit jeho nejzranitelnější místa ve vztahu k relevantním násilným útokům, které mohou skutečně nastat. Tento článek přináší bližší pochopení toho, co si představit pod slabým místem měkkého cíle včetně návodu, jakým způsobem tato místa poznat. Jedná se o druhý díl z volné série zaměřené na problematiku současné ochrany měkkých cílů na území České republiky.



strana

11

EIA Blockchain – průmyslová blockchainová platforma – část III.

Otto Havle, Roman Jašek, Věra Šmídová, Jakub Kozák, Jakub Vodsedálek

Ve třetím díle článku autoři představí českou průmyslovou blockchainovou platformu EIA blockchain provozovanou společností ELA Blockchain Services a.s. Na ní lze vytvořit zákaznický průmyslový blockchain, konsorciální nebo privátní. Naplňuje ideu blockchainu jako decentralizované nezávislé technologie. Není možné jej zničit, vypnout, konfiskovat, nebo ovládnout. To je zajištěno unikátními koncepty BaAC (Blockchain as Asisted Consortium) a nAA (non-Aligned Administration), které byly vyvinuty a aplikovány společností ELA Blockchain Services a.s.



strana

21

Jak na bezpečnost pomocí ChatGPT – část I.

David Pecl, Matěj Kačic

V článku se budeme zabývat chatbotem ChatGPT postaveném na umělé inteligenci. Jak vlastně taková umělá inteligence funguje a jak byla vytvořena? K čemu všemu je možné ChatGPT využít na poli bezpečnosti? Podíváme se také na jeho nedostatky a možný budoucí vývoj umělé inteligence v nejbližších měsících.



strana

31

Nařízení EU o digitálních službách: možné právní nebezpečí – část I.



strana

36

Ivo Telec

Příspěvek podrobně právně rozebírá některá právní rizika, která vyplývají z nařízení EU o digitálních službách (DSA) z roku 2022. Zvláštní kritická pozornost je věnována systémovému riziku, které má nově spočívat v závažném negativním dopadu šířených textů, fotografií a videí na tělesnou a duševní pohodu lidí. Autor dospívá k právnímu závěru o rozporu takového přístupu s mezinárodními smlouvami o lidských právech a s českou Listinou základních práv a svobod.

Deset neměnných zákonů kyberbezpečnosti



strana

46

Jan Pilař

Tempo změn v našich životech je čím dál rychlejší. A v digitálním světě to platí více než kdekoli jinde. Přibývá mobilních zařízení i důležitých sdílených dat. A útočníci to vědí. Jsou rychlí a schopní. Co se však nemění, jsou zákony kybernetické bezpečnosti. Projděme si společně deset neměnných zákonů a podívejme se na trendy, které se týkají nás všech.

(Ne)bezpečnost cloudu a cesty k němu



strana

40

Lukáš Klášterský

Každá cesta do cloudu je spojena s pozitivními překvapeními i negativními emocemi. Seznámíte se jakými kroky musí týmy IT a bezpečnosti projít, aby cesta do cloudu dopadla podle očekávání – cloud byl úspěšně adoptovaný a zabezpečený.

Nejnovější trendy a výzvy kybernetické bezpečnosti

strana

50

ChatGPT

Chceme-li se účinně bránit kybernetickým útokům, je nezbytné sledovat nejnovější technologie a bezpečnostní trendy. Tento článek by se zaměřuje na nové metody a nástroje v oblasti kybernetické bezpečnosti a na to, jak mohou společnosti a organizace tyto technologie využít ke zlepšení svého zabezpečení.

„Pro podporu klinických rozhodnutí budou nepochybně lékaři do určité míry využívat i umělou inteligenci. A tato doba je zjevně za rohem...“

...rozhovor s Tomášem Halajčkem najdete na str. 7.

R I I R R I K Y

Virová stránka

54

Normy a publikace

56

Metamorfosa 2022: Zabijačka anebo workshop?

57

Právní rubrika

58

Management summary

60

Tiráž

62