

## Rozhovor: David Mussington

strana

6

Martin Haloda

Dr. David Mussington je profesorem na prestižní Škole veřejné politiky Univerzity v Marylandu (AMD). Před svým opětovným nástupem na UMD v lednu 2025 působil jako výkonný kancléř ředitele pro infrastrukturu v Agentuře pro kybernetickou a infrastrukturu bezpečnosti (Cybersecurity and Infrastructure Agency - CISA) Ministerstva vnitřní bezpečnosti USA. V rozhovoru se ho ptáme, jaké jsou klíčové faktory pro efektivní spolupráci veřejného a soukromého sektoru v ochraně infrastruktury a jaké překážky tomu brání, jaký je potenciál kybernetických norem omezit konflikty mezi státy a další.



## Zajištění bezpečnosti chráněných osob a ochrana jejich osobních údajů ve virtuálním prostředí zdravotnického zařízení – část III.



strana

16

Lukáš Miklas, Jan Kolouch

Třetí část článku se zaměřuje na význam cloudových technologií a Evropského zdravotního datového prostoru (EHDS) pro bezpečný přenos a uchování citlivých dat a diskutují přínosy moderních technologií, jako je umělá inteligence a blockchain, pro prediktivní kybernetickou bezpečnost a ochranu osobních údajů. Dále se věnují propojení mezi vojenskými a civilními zdravotnickými strukturami, aby byla zajištěna kontinuita péče o chráněné osoby v krizových situacích, včetně návržení modelu přenosu zdravotních dat chráněných osob. Současně budou prezentovány dílčí výsledky výzkumu zaměřeného na ochranu chráněných osob ve zdravotnických zařízeních. Právě výzkumem byla identifikována významná rozdílnost mezi českými a zahraničními zdravotnickými zařízeními v přístupu k ochraně citlivých dat, zejména v oblasti, kontrolních mechanismů a zabezpečeného přenosu dat. Zkušenosti ze zahraničí v kontextu současného bezpečnostního dění poukazují na nutnost posílení bezpečnostních strategií ve zdravotnických zařízeních.

## Dopady přísné transpozice prepojení podnikov smernice NIS2 na Slovensku



strana

12

Hieu T. Nguyen, Juraj Ondrejka

Slovenská transpozícia smernice NIS2 namiesto harmonizácie priniesla paradox: podniky, ktoré by v iných členských štátoch EÚ ostali mimo regulácie, sa na Slovensku stávajú povinne regulovanými subjektmi len na základe prísneho a formálneho výkladu veľkosti a prepojenia podnikov. Článok odhaľuje, ako sa slovenský prístup líši od flexibilnejšej právnej úpravy v iných členských štátoch a aké dôsledky to môže mať pre regulované podniky. Skutočne ide o zvýšenie kybernetickej bezpečnosti – alebo o zbytočné zaťaženie podnikov?

## Role AI v oblasti DevOps a ITSM - závěr – část III.



strana

24

Vladimír Kufner

Tento článek je poslední v sérii tří článků a shrnuje celkové trendy v nasazení AI s ohledem na konkrétní potřeby DevOps. Rekapituluje poslední trendy v oblasti AI i DevOps, uvádí statistiky a predikuje budoucí rozvoj této oblasti.

## Výzvy OSINT v byznysu a průmyslu – část II.



strana

31

Adam Pavelka, Jan Rada

Článek se zabývá výzvami, které doprovázejí implementaci a využívání OSINT (Open Source Intelligence) v komerčním prostředí. Zaměřuje se na právní mantinely, etická dilemata spojená se sběrem a interpretací veřejných dat, a na technické překážky jako je kvalita dat, neúplnost zdrojů nebo slepá důvěra ve vizualizace. Zvláštní pozornost je věnována omezením tzv. all-in-one OSINT nástrojů a potřebě řešení na míru. Článek dále rozebírá praktické iluze úplnosti a věrohodnosti dat a upozorňuje na budoucí hrozby spojené s generativní umělou inteligencí a dezinformacemi. Nabízí kritický, ale konstruktivní pohled na roli OSINT v rozhodovacích procesech a zdůrazňuje význam odpovědného přístupu k veřejným informacím.

DSM 2 | 2025

DSM

Obsah

# OBSAH

Články označené prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

## Úskalí a hrozby autentizace



strana

37

Jan Dušátko

Autentizace – ověření, že uživatel je skutečně tím, za koho se vydává – je dnes poslední obranou proti krádežím identit, ztrátám dat a přímým finančním škodám. Článek odhaluje slabá místa běžných přihlašovacích mechanismů, ukazuje reálné útoky založené na sociálním inženýrství i technických zranitelnostech a vysvětluje, proč je nutné nasazovat moderní vícefaktorové a bezheslové metody spolu s dobře nastavenými procesy.

## AI Security



strana

47

Jan Kleindienst, Jakub Krchák, Jan Macek

Článek obsahuje tři klíčové oblasti, které dnes ovlivňují práci s umělou inteligencí v praxi: evropské nařízení AI Act, mezinárodní bezpečnostní rámce (GDPR, ISO, NIST) a konkrétní využití AI v kyberbezpečnosti.

## Projekt #SafebyRaiffeisen a spoluvytváření Evropského kybernetického štítu z pohledu RBCZ



strana

43

Gabriela Obešlová, Matouš Vamberský

Kyberbezpečnost má v dnešní době silnou váhu. Únik dat, hrozba kvantových počítačů ani kyberšpionáž nejsou bohužel ojedinělými případy. Inovativní projekt #SafebyRaiffeisen má proto posílit kybernetickou bezpečnost a připravit banku na případné budoucí hrozby. Raiffeisenbank by díky projektu měla být více odolná a připravená na potenciální útoky. Navíc ochrání data klientů a investuje do technologií, které zamezí hrozbám vyplývajícím z nových trendů, včetně kvantových počítačů.

## Rozhovor: Helio Sant'Ana

strana

52

Martin Haloda

Lídr v oblasti kybernetické bezpečnosti s více než 15 lety mezinárodních zkušeností ve vládním, vojenském i soukromém sektoru. V současnosti působí jako manažer CSIRT a reakce na incidenty, dohlíží na globální bezpečnostní operace. V rozhovoru se ho ptáme, co považuje za největší výzvu pro CSIRT týmy, jaké praktické kroky doporučuje společně, které chtějí začít s integrací threat intelligence do svých bezpečnostních týmů a další.



# RUBRIKY

Konference IS2: Digitální Optimismus

56

Síň slávy Cybersecurity 2025

58

Normy a publikace

59

Management summary

60

Recenze knihy: Dračí algoritmus

62

Tiráž

63

**„Kyberprostor není národní disciplína...  
obrana je vždy kolektivní úsilí...“**

...rozhovor s Davidem Mussingtonem najdete na str. 6.