

Rozhovor: Brent McConnell

Martin Haloda

Brent McConnell je zkušený bezpečnostní expert s více než 35 lety praxe v oblasti kybernetické bezpečnosti, ochrany kritické infrastruktury, compliance, exportní kontroly a mezinárodní bezpečnostní politiky. Působil ve vedoucích funkcích v americké agentuře CISA, vedl mezinárodní operace a podílel se na strategické spolupráci s partnery v NATO, Evropské unii i dalších regionech. V rozhovoru se mimo jiné ptáme, proč je kritickou infrastrukturu vhodné chápat jako provozní substrát moderní společnosti, jak agentická AI mění tempo útoků, proč je nutné navrhovat systémy pro degradovaný provoz, kde leží hranice mezi užitečnou automatizací a nebezpečnou ztrátou kontroly a další.



strana
6

APT útoky a možnosti jejich mitigace – II. část

Michal Matějka, Jan Kolouch, Zdeněk Jícha

Článek se zabývá pokročilými perzistentními hrozbami z pohledu řízení rizik, auditu a praktické obrany organizací spravujících kritická aktiva. Popisuje využití threat intelligence, monitoringu a rámce MITRE ATT&CK při odhalování APT aktivit a představuje vícevrstvou obranu založenou na řízení přístupů, segmentaci, ochraně dat, detekci a krizové připravenosti. Ukazuje, že APT útokům nelze zcela zabránit, jejich pravděpodobnost a dopady však lze výrazně omezit.



strana
18

Stav algoritmických auditov sociálních médií: Výsledky, výzvy a přísliby

Jakub Šimko, Ivan Srba

Článek se venuje algoritmickému auditování sociálních médií jako perspektivnímu nástroji na odhalování rizik spojených s fungováním doporučacích systémů. Na příkladech troch výzkumných studií platformy TikTok přibližuje, ako algoritmy personalizujú polarizujúci obsah, do akej miery môžu profilovať maloletých pri zobrazovaní reklamy a prečo je reprodukovanie výsledkov podobných auditov také náročné. Autori zároveň poukazujú na potrebu vnímať odporúčacie systémy ako bezpečnostne kritickú súčasť informačného prostredia a presadzujú modelovo riadené a kontinuálne auditovanie ako cestu k transparentnejším, bezpečnejším a dôveryhodnejším digitálnym platformám.



strana
32

Privacy engineering pri vývoji AI systémov a AI agentov

Lenka Gondová

Článok analyzuje, prečo v ére AI už nestačí riešiť ochranu súkromia prostredníctvom dokumentácie a následného auditu, ale je nevyhnutné ju zabudovať priamo do architektúry systému. Vysvetľuje historické „informačné vákuum“ v čase nástupu GDPR, mapuje vývoj technických štandardov a predstavuje tri vrstvy rizík v AI – systém, model a agent. Podrobne rozpracúva evolúciu Privacy-Enhancing Technologies od dátovej úrovne až po architektonické riešenia a ukazuje, ako nové normy a rámce (ISO, NIST, OWASP, AEPD) premieňajú právne princípy na konkrétne inžinierske opatrenia. Záver zdôrazňuje, že ochrana súkromia nie je brzdou inovácie, ale podmienkou dôveryhodnej a dlhodobo udržateľnej AI, ktorá je implementovaná v súlade s legislatívou.



strana
12

LLM jako nástroj ovlivňování

Petra Vokálová

Velké jazykové modely nepřinášejí pouze výhody v podobě rychlejší práce a tvorby textů, ale také riziko prosazování konkrétních názorů, předsudků či agend. Článek se zaměřuje na to, jak se do modelů dostávají informace ovlivňující jejich chování i vytvářený obsah. Dále popisuje vliv ochranných mechanismů (guardrails) a dopady technologického vývoje AI na šíření dezinformací.



strana
27

Jak organizovaný zločin využívá automatizaci, umělou inteligenci a rafinované postupy ke krádeži vašich peněz a praní výnosů

Martin Reháč

Finanční kriminalita se v důsledku digitalizace, automatizace a rychlého nástupu umělé inteligence mění v globální, profesionálně organizované odvětví. Článek vysvětluje, jak zločinecké skupiny využívají automatizované finanční služby, specializované dodavatelské řetězce, padělané dokumenty, účty vedené na bílé koně a nástroje generativní AI. Na konkrétních příkladech ukazuje, proč se podvody stále snáze škálují, jak funguje jejich černý trh a jaké nové nároky tato situace klade na finanční instituce, poskytovatele digitálních služeb i orgány činné v trestním řízení.



strana
37

OBSAH

Články označené prošly odborným recenzním řízením.
Články označené firemním logem jsou komerčními prezentacemi.

Strategická rekonfigurace globálních technologických dodavatelských řetězců - I. část

Radovan Vacek

Článek ukazuje, že konvenční narativ evropské technologické slabosti míří vedle. EU disponuje globálně významnými průmyslovými a technologickými aktivy, její hlavní problém však nespočívá v tom, co má, ale v tom, jak jsou strukturovány její závislosti. Matice regionální soběstačnosti ukazuje, že žádný region na světě – ani USA, ani Čína – není v roce 2026 plně soběstačný. Článek proto posouvá diskusi od snahy o autarkii ke koncepci Minimální životaschopné suverenity.



strana
41

Zákonnost blokování IP adres a ochrana elektronických podatelen

Jaromír Novák

V tomto díle je vysvětleno, kdy mohou elektronické podatelny veřejné správy zákonně blokovat rizikové IP adresy. Zdůrazňuje nutnost objektivního bezpečnostního důvodu, transparentního upozornění na nedoručení a řádného doložení postupu.



strana
50

Rozhovor: Jan Willemson

Martin Haloda

Jan Willemson je estonský informatik a seniorní výzkumník společnosti Cybernetica, který se dlouhodobě zabývá elektronickými volbami, digitální identitou a dalšími oblastmi e-governmentu. Je autorem více než 80 odborných publikací a patří mezi výrazné odborníky na bezpečnost internetového hlasování. V rozhovoru se mimo jiné ptáme, proč mohou být elektronické volby při správném návrhu bezpečnější než hlasování na papíře, jakou roli hraje silná digitální identita, kryptografie a transparentnost, jak Estonsko řeší nátlak na voliče a co by měla vybudovat země, která chce internetové volby zavést.



strana
45

Co nového přinesl MITRE Fight Fraud Framework (F3) pro výuku kybernetické bezpečnosti

Jaroslav Dočkal

Článek představuje MITRE Fight Fraud Framework (F3), který rozšiřuje pohled na kybernetické útoky o fáze vedoucí k finančnímu podvodu a ztrátě. Zaměřuje se také na jeho využití v souvislosti s DORA, NIS2, ISO 27001 a ve výuce kybernetické bezpečnosti.



strana
52

„Autonomní odolnost neznamená dát systému volnou ruku. Znamená získat rychlost, ale zachovat kontrolu...“

...rozhovor s Brentem McConnellem najdete na str. 6.