

Martin Haloda

MUDr. Tom Philipp, Ph.D., MBA je lékař, manažer a politik, který dlouhodobě propojuje každodenní realitu nemocničního provozu s tvorbou zdravotní politiky a řízením velkých veřejných institucí. Jako přednosta kliniky ve Fakultní Thomayerově nemocnici, předseda správní rady VZP a poslanec Parlamentu ČR se věnuje stabilitě a dostupnosti zdravotní péče, včetně její digitální a kybernetické odolnosti. V rozhovoru se zaměřujeme na aktuální stav kyberbezpečnosti českých nemocnic, dopady nového zákona o kybernetické bezpečnosti ve zdravotnictví, otázku financování bezpečnostních opatření, smysluplné využití umělé inteligence v klinickém a provozním prostředí nemocnic a další.



Darkweb OSINT: mezi mýty a realitou zpravodajské praxe



strana

16

Ondřej Šlechta

Darkweb představuje legitimní zdroj zpravodajských informací v rámci OSINT, který umožňuje organizacím detekovat úniky dat, kompromitované přihlašovací údaje nebo stopy o aktivitách akterů kybernetických hrozeb. Zároveň se jedná o problematický zdroj informací, především s ohledem na vysokou volatilitu obsahu, úmyslnou obfuskaci lokací skrytých služeb a nestálost zdrojových dat. Přestože ale darkweb tvoří relativně malou internet, jeho systematický průzkum se stal nedílnou součástí holistického přístupu k řízení kybernetických rizik.

Výroční analýza používání odposlechů, data retention, rušení sítí a jak s tím ladí chat control



strana

26

Jaromír Novák

Článek pojednává o analýze použití odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí podle trestního řádu a rušení provozu elektronických komunikací Policií České republiky. Tato analýza, kterou zpracovává Policejní prezidium České republiky na základě ustanovení § 98 odst. 3 zákona o Policii, slouží ke kontrole využívání těchto invazivních prostředků a odhalení případných nedostatků. Článek se věnuje využití těchto instrumentů a ochraně proti možnému zneužití.

Nová éra parsování logů: Když logy ve vašem SIEM konečně začnou dávat smysl



strana

9

Yehor Safonov

Kybernetická bezpečnost začíná u viditelnosti. A ta dnes musí být hlubší než kdy dřív. Směrnice NIS2 a nový zákon č. 264/2025 staví logy do středu pozornosti. Článek odhaluje, proč se i drahý SIEM bez kvalitního parsování snadno mění v „garážovou“ investici vyžadující nekonečné ladění. Společně se podíváme pod hladinu „ledovce“ správy SIEM řešení a na to, jak může integrace AI změnit pravidla hry. Bez cloudu, s podporou klíčových SIEM systémů. Méně ručního ladění, nižší náklady, rychlejší detekce. Přečtěte si, jak nechat logy konečně dávat smysl.

Řízení rizik umělé inteligence v kontextu informační bezpečnosti



strana

21

Jiří Diepolt

Tento příspěvek se zabývá problematikou řízení rizik umělé inteligence v kontextu informační bezpečnosti. Analyzuje současné trendy od zneužití generativní AI pro phishingové útoky přes adversariální útoky na AI modely až po zranitelnosti velkých jazykových modelů. Představuje klíčové taxonomie rizik a mapuje hlavní mezinárodní standardy (NIST AI RMF, ISO/IEC 42001:2023, EU AI Act). Významnou část tvoří analýza aktuálního stavu v českém prostředí, která odhaluje kritickou mezeru mezi rychlou adopcí AI (87% organizací) a vyspělostí governance (21% integruje AI rizika do systému řízení). Průzkum identifikuje školení jako nejdůležitější organizační opatření (59% respondentů) a potvrzuje, že organizace s aktivní podporou vedení vykazují o 28% vyšší připravenost.

OBSAH

Články označené prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

Digitální omnibus: právní úprava a praktické dopady



strana

30

Barbora Vlachová, Aneta Kranerová

Článek se zabývá problematikou zjednodušení evropské digitální legislativy prostřednictvím iniciativy digitální omnibus. Nový balíček právních novelizací a dílčích derogací, který Evropská komise předložila v listopadu 2025, obsahuje řadu cílených změn zaměřených na snížení regulatorního břemene při zachování vysoké úrovně ochrany. Mezi navrhované nástroje zjednodušení patří zavedení jednotného vstupního bodu pro hlášení kybernetických incidentů, flexibilnější přístup k regulaci AI a integraci pravidel ochrany soukromí v elektronických komunikacích pod jednotný rámec GDPR.

Nový zákon o kybernetické bezpečnosti v praxi: samoidentifikace, GAP analýza a best practices



strana

46

Martin Haloda

Článek popisuje praktické dopady zákona č. 264/2025 Sb., o kybernetické bezpečnosti na organizace v ČR. Nastihuje, jak lze – provést dopadovou analýzu (sebeidentifikaci), kdy vzniká povinnost ohlásit službu a projít registrací regulované služby u NÚKIB a jaké sankce hrozí při neohlášení. Dále prezentuje rozdíl mezi režimem nižších a vyšších povinností a proč je v praxi dobrým startem GAP analýza (ideálně sladěná s ISO/IEC 27001), aby organizace k řešení kybernetické bezpečnosti přistupovala systémově a byla schopna compliance i úroveň kybernetické bezpečnosti prokázat.

Likvidace nosičů dat a jejich obsahu



strana

35

Vladimír Smejkal

Článek se zabývá bezpečnou likvidací dat a datových nosičů jako řízeným bezpečnostním procesem, u kterého je zásadní nejen správná volba metody (smazání, hlubší sanitizace, nebo fyzická destrukce), ale i prokazatelnost a auditní stopa. Vysvětluje, proč moderní technologie (SSD, virtualizace, cloud) komplikují spolehlivé odstranění dat, shrnuje doporučení podle NIST (Clear/Purge/Destroy) včetně crypto erase a upozorňuje na rizika špatné správy klíčů. Zohledňuje také právní rámec (nový zákon o kybernetické bezpečnosti a vyhlášky NÚKIB), popisuje typická technická a procesní selhání (zálohy, snapshoty, chain-of-custody) a nabízí praktický rozhodovací postup i tipy pro OSVČ a malé firmy.

RUBRIKY

Recenze knihy

51

Metamorfosa 2025: Svatomartinská husa

52

Metamorfosa 2025: Zabijačka anebo workshop

54

Normy a publikace

56

Právní rubrika

57

Management summary

60

Tiráž

62

„Je dlouhodobě neudržitelné stavět plnění nZoKB/NIS2 jen na jednorázových dotacích...“

...rozhovor s Tomem Philippem najdete na str. 6.