

Rozhovor: Lukáš Klučka

Martin Haloda

Lukáš Klučka je 1. náměstkem ministra vnitra a od roku 2026 také vládním zmocněncem pro digitalizaci a strategickou bezpečnost. Ve státní správě se dlouhodobě pohybuje na pomezí digitalizace, bezpečnosti a řízení strategických projektů; působil na Ministerstvu vnitra i Ministerstvu obrany a zkušenosti získal také v poradenském prostředí. V rozhovoru se věnujeme tomu, jak budovat odolný a bezpečný digitální stát, proč digitalizace veřejné správy postupuje pomaleji, než by měla, a jak lépe řídit odpovědnost, rizika a priority jednotlivých projektů. Ptáme se také na riziko závislosti státu na jednom dodavateli AI nebo cloudu, připravenost Česka na evropskou peněženku digitální identity EUDIW, ochranu soukromí a metadat, přeshraniční interoperabilitu či odolnost digitálních služeb při kybernetických útocích a výpadech. Rozhovor se dotýká i možnosti využití digitální identity ve zdravotnictví a principu, podle něhož má občan sdílet pouze ty údaje, které jsou pro konkrétní službu skutečně nezbytné.



strana
6

Jak EU Action Plan mění pravidla hry v kybernetické bezpečnosti

Jaroslav Dočkal

Článek se zabývá dopady nového evropského Akčního plánu pro kybernetickou bezpečnost a umělou inteligenci na řízení bezpečnosti organizací. Zaměřuje se zejména na proměnu bezpečnostní architektury v prostředí autonomních AI agentů, limity tradičních nástrojů typu SIEM, význam guardrails, SOAR a auditovatelnosti a na nové požadavky kladené na SOC, AI governance a správu zranitelnosti. Text současně zasazuje tyto změny do širšího kontextu evropské technologické suverenity a propojení regulací NIS2, DORA, AI Act a Cyber Resilience Act. Závěrem uvádí konkrétní kroky, které mohou organizace začít zavádět již nyní při bezpečném nasazování AI do provozu a kybernetické obrany.

strana
16

eDoklady ve volební místnosti

Šárka Horneková

Článek shrnuje stav eDokladů k září 2026, bezpečnostní model digitálního stejnopisu, dvě technické cesty ověření, zabezpečení strany ověřovatele a opatření přijatá po veřejném zátěžovém testu eDokladů ze 13. srpna 2026. Závěrečná část se věnuje návaznosti na evropskou peněženku digitální identity.

strana
10

APT útoky a možnosti jejich mitigace – III. část

Zdeněk Jícha, Michal Matějka, Jan Kolouch

Článek se zabývá kybernetickými hrozbami ve zdravotnictví se zaměřením na APT a sofistikované ransomwarové útoky. Vymezuje zdravotnická data podle GDPR, stručně porovnává evropský přístup s rámci HIPAA, ISO/IEC 27799 a HL7 FHIR a analyzuje hlavní aktéry, vektory útoku a vybrané incidenty ve zdravotnických zařízeních. Pozornost věnuje také provozním a klinickým dopadům útoků, ochraně dostupnosti a integrity zdravotnických informačních systémů a jejich významu pro kontinuální péči a bezpečnost pacientů. Závěrem zasazuje problematiku do kontextu českého legislativního rámce kybernetické bezpečnosti a odolnosti kritické infrastruktury.

strana
23

Rozhovor: Rain Ottis

Martin Haloda

Major Rain Ottis patří k výrazným osobnostem estonské kybernetické obrany a dlouhodobě působí v Estonské obranné lize, akademické sféře i oblasti národní kybernetické bezpečnosti. V rozhovoru se mimo jiné ptáme, jak funguje estonský model dobrovolné kybernetické obrany, kde mohou dobrovolníci státu v krizi přinést největší hodnotu, jaké jsou limity tohoto přístupu a jakou roli v něm hrají důvěra, spolupráce se soukromým sektorem a nástup umělé inteligence.



strana
34

DSM 3 | 2026

DSM Obsah

OBSAH

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

Strategická rekonfigurace globálních technologických dodavatelských řetězců – II. část

Radovan Vacek

Druhý díl třídílné série ukazuje, že rozdíl mezi evropským a americkým podnikovým IT nespočívá jen v kvalitě technologií, ale také v odlišném modelu provozu a odpovědnosti. Článek porovnává evropské alternativy v oblasti cloudu, kancelářského softwaru, správy identit a procesorových architektur a vysvětluje jejich význam pro technologickou suverenitu. Současně upozorňuje na limity evropských řešení a převádí téma do praktické roviny prostřednictvím smluvního checklistu a 24měsíční roadmapy pro diverzifikaci dodavatelů a posílení odolnosti.

strana
38

Odolnost namísto absolutní bezpečnosti: praktický pohled na principy regulace kybernetické bezpečnosti

Klára Humpolíková, Martin Švéda

Regulace kybernetické bezpečnosti v České republice je představena jako nástroj pro budování odolnosti. Text se zaměřuje na klíčové principy právního rámce a jejich praktický dopad na zavádění a provádění bezpečnostních opatření.

strana
51

Určení stanoveného rozsahu podle § 12 zákona o kybernetické bezpečnosti v kontextu telekomunikačního sektoru

Michal Krejčík, Michaela Holíková, Jan Tomíšek

Článek vysvětluje, jak podle nového zákona o kybernetické bezpečnosti správně určit stanovený rozsah v telekomunikačním sektoru. Zaměřuje se na primární a podpůrná aktiva, fakturační a podpůrné systémy i hranice odpovědnosti mezi operátory při propojení sítí a roamingu. Upozorňuje také na rizika příliš širokého vymezení rozsahu a na potřebu soustředit ochranu na aktiva skutečně nezbytná pro poskytování regulovaných služeb.

strana
45

RUBRIKY

Normy a publikace

Metamorfosa 2026: Voda a život

Konference IS2: Není čas váhat

Management summary

Tiráž

55

56

58

61

63

„Člověk musí mít důvěru, že digitální identita není nástrojem sledování...”

...rozhovor s Lukášem Klučkou najdete na str. 6.