

Rozhovor: Jan Beroun

Martin Haloda

Generálporučík Jan Beroun je zkušený bezpečnostní a zpravodajský profesionál s bohatou kariérou v oblasti vymáhání práva, zpravodajství a obrany. V současné době působí jako bezpečnostní ředitel Řízení letového provozu a je poradcem Po-
radce pro národní bezpečnost České republiky. V letech 2014 až 2024 vedl Vojenské zpravodajství ČR. V rozhovoru se mimo jiné ptáme, kde management kritické infra-
struktury nejčastěji podceňuje bezpečnostní rizika, jaké bezpečnostní metriky se používají na jeho úrovni řízení, jak poznat, že organizace buduje skutečnou odolnost, a ne pouze formálně plní požadavky.



strana
7

Normy a regulácie v oblasti umelej inteligencie: výzvy a perspektívy v súvislosti s AI Actom

Lenka Gondová

AI Act je účinný, no harmonizované technické normy, ktoré majú konkretizovať jeho požiadavky, majú výrazné oneskorenie. Standardizačný proces v CEN/CENELEC/ETSI a ISO/IEC sa ukázal ako nezluči-
teľný s legislatívnym harmonogramom a viaceré kľúčové normy sa očakávajú až v rokoch 2026–2027. Tento časový nesúlad vytvára informačnú neistotu a riziko nejednotného výkladu povinností. Článok
vysvetľuje príčiny sklzu, reakciu normalizačných orgánov a poukazuje na existujúce normy a rámce, ktoré môžu organizácie využiť ako dočasnú oporu pri nastavovaní AI governance a riadení rizík.



strana
15

Skončí v ČR povinné uchovávaní provozních a lokalizačních údajů?

Miroslav Uříčář

Článek se zabývá nedávným rozsudkem Nejvyššího soudu ve věci provozních a lokalizačních údajů elektronických komunikací. V kontextu české i evropské judikatury k Data Retention shrnuje hlavní otázky, které toto rozhodnutí vyvolává.



strana
30

Chat Control

Michal Ketner, Mikuláš Peksa

Autoři analyzují legislativní návrh Evropské unie známý jako Chat Control, jeho vnitřní strukturu a vývoj v rámci řádného legislativního postupu. Zaměřuje se na zásadní rozdíly mezi pozicemi Evropské komise, Evropského parlamentu a Rady Evropské unie, zejména pokud jde o rozsah de-
tekčních povinností, ochranu soukromé komunikace a postavení end-to-end šifrování. Text zároveň hodnotí aktuální stav trialogických jednání a naznačuje možné scénáře dalšího vývoje regulace.



strana
10

Základní povinnosti plynoucí z nového zákona o kybernetické bezpečnosti

Klára Humpolíková, Martin Švéda

Příspěvek přináší přehled základních povinností, které organizacím ukládá nový zákon o kyberne-
tické bezpečnosti. Vysvětluje, jak posoudit, zda se na konkrétní organizaci zákon vztahuje, a dále se věnuje klíčovým povinnostem, zejména zavádění bezpečnostních opatření a oznamování kyber-
netických bezpečnostních incidentů.



strana
19

Rozhovor: Daniel Hejda a Michal Hanus

Martin Haloda

Michal Hanus a Daniel Hejda v rozhovoru propojují dva pohledy na kybernetická rizi-
ka: kvantifikaci a praktické testování odolnosti. Michal Hanus se dlouhodobě věnuje řízení kybernetických rizik a propagaci kvantitativních metod. Daniel Hejda působí jako etický hacker a specialista na simulované útoky. Mimo jiné se v rozhovoru ptá-
me, jak zabezpečujete porovnatelnost rizik mezi sebou, jak velké riziko představuje situace, kdy organizace bere výsledek pentestu bez širšího kontextu hrozeb, kritic-
kých aktiv a reálných dopadů, a jak by měl vypadat výstup z pentestu nebo TLPT pro technický tým, risk management i vedení firmy.



strana
24

DSM 1 | 2026

DSM

Obsah

OBSAH

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

Kybernetická bezpečnost v éře umělé inteligence

Peter Chrenko

Téma článku se věnuje proměně kybernetické bezpečnosti v prostředí systémů využívajících umělou inteligenci, v němž tradiční přístupy založené na pravidlech a statických kontrolách přestávají být do-
stačující. Ukazuje, že AI systémy je třeba řídit jako dynamické socio-technické celky v průběhu celého jejich životního cyklu, a zasazuje tento posun do kontextu rámce NIST AI RMF, normy ISO/IEC 42001 a praktických dopadů AI Act na bezpečnost, governance a řízení rizik v organizacích.



strana
35

Z rozhodovací praxe

Jaromír Novák

Článek pojednává o nedávném rozhodnutí nizozemského soudu týkající se zakázání technologie firem Huawei a ZTE v kritické části sítě nizozemského operátora.

strana
48

APT útoky a možnosti jejich mitigace – I. část

Jan Kolouch, Michal Matějka, Zdeněk Jícha

Autoři se zabývají problematikou Advanced Persistent Threat (APT) útoků jako jedné z nejzávažněj-
ších forem současných kybernetických hrozeb. Cílem je analyzovat a popsat charakteristické rysy APT útoků, jejich životní cyklus a používané techniky, stejně jako přístupy k jejich detekci a mitigaci. APT útoky jsou specifické svou vysokou mírou sofistikovanosti, dlouhodobým působením a cíleným zaměřením na konkrétní významné organizace či infrastruktury, přičemž útočníci využívají pokročilé metody k udržení perzistence a minimalizaci pravděpodobnosti odhalení. Článek uvádí i konkrétní příklady APT útoků na české instituce a zdůrazňuje specifika a potřebná opatření pro organizace.



strana
41

Unijní regulace dodavatelských řetězců v oblasti ICT

Patrik Walas

Článek stručně představuje novou unijní regulaci dodavatelských řetězců v oblasti ICT v návrhu na-
řízení CSA2, která přináší zcela nový pohled na regulaci netechnických rizik v oblasti ICT. Tento nový přístup ovšem vyvolává hned několik kontroverzí, což autor propojuje s praktickými znalostmi v ob-
lasti sítí elektronických komunikací.



strana
50

RUBRIKY

Rizika WebView architektury	53
Normy a publikace	56
Právní rubrika	57
Management summary	60
Tiráž	62

„System máme stavěný pro zásah,
ne na zvládnutí dlouhodobé krize...“

...rozhovor s Janem Berounem najdete na str. 7.