## Rozhovor: Liina Kamm

strana 7

Martin Haloda

Liina Kamm získala v roce 2015 doktorát z informatiky na univerzitě v Tartu. Je vedoucí výzkumnou pracovnicí a hlavní řešitelkou ve společnosti Cybernetica. Svou profesní kariéru zahájila návrhem softwaru pro Estonskou nadaci pro genom a pro přeshraniční klinické studie. V rozhovoru se jí ptáme na technologie pro zvýšení ochrany soukromí (PET), e-government a další.

## Phishingator – Jak na vlastní cvičný phishing? – část II.

strana 16

Aleš Padrta, Martin Šebela, Jan Kolouch

Podvodné kampaně v poslední době nabírají na intenzitě, ale především dochází k jejich rychlé modifikaci ze strany útočníků. Využívány jsou jak klasické phishingové, vishingové, smishingové útoky, tak především jejich kombinace. Ochranu před podobnými útoky do jisté míry poskytují antivirová, antiphishingová, antispamová a jiná technická řešení, ale úspěšnost těchto technických opatření je různá. Vhodným řešením je kombinace těchto technických opatření a součinné zvyšování digitální odolnosti koncových uživatelů.

## Smí správce daně využívat záznamy z policejních dopravních kamer?

strana 28

Miroslav Uřičař

Text se zaměřuje na systém dopravních kamer na silnicích ČR a analyzuje právní možnosti využití záznamů těchto kamer pro účely odlišné od zajištění bezpečnosti dopravy. Ve světle aktuální judikatury soudů ČR ke konkrétnímu případu, včetně Ústavního soudu ČR, text zkoumá zejména možné využití informací ze záznamů dopravních kamer v daňovém řízení vedeném s provozovatelem vozidla zachyceného kamerovým systémem.

## Nařízení EU o digitálních službách: možné právní nebezpečí – část III.

strana 10

Ivo Telec

Příspěvek podrobně právně rozebírá některá právní rizika, která vyplývají z nařízení EU o digitálních službách (DSA) z roku 2022. Zvláštní kritická pozornost je věnována systémovému riziku, které má nově spočívat v závažném negativním dopadu šířených textů, fotografií a videí na tělesnou a duševní pohodu lidí. Autor dospívá k právnímu závěru o rozporu takového přístupu s mezinárodními smlouvami o lidských právech a s českou Listinou základních práv a svobod.

## Použitie digitálnej forenznej analýzy vo firemnom prostredí

strana 22

Peter Pištek

Digitálna forenzná analýza je bežne používaná vec pri súdnych vyšetrovaniach. Jej použitie je však zaujímavé aj vo firemnom prostredí, kde vie poskytnúť pridanú hodnotu. Je na to potrebné ju však prispôsobiť potrebám firmy, nie vždy sa musí jednať o veľký a robustný proces. Vieme si vystačiť aj z jeho odľahčenou verziou, ak napríklad pátrame po príčine incidentu a podľa potreby vieme pridávať ďalšie „klasické“ forenzné postupy.

## Trestní odpovědnost za jednání robotů využívajících AI – část II.

strana 34

Vladimír Smejkal

Článek se zabývá trestní odpovědností za jednání robotů. Vysvětluje, proč současné připravované předpisy EU týkající se AI tuto oblast nepostihují a upozorňuje na zvyšující se složitost robotických systémů s AI, která znemožňuje snadno či vůbec určit, kdo za protiprávní jednání robota odpovídá.

## Jak bezpečně využívat umělou inteligenci?

strana 40

Miroslav Nečas

Zodpovědné využívání umělé inteligence je jedna z priorit mezinárodních organizací, jako jsou NATO, EU či OECD. Měl jsem příležitost podrobně se tomu tématu věnovat jako předseda skupiny NIAG SG 279. Společně s týmem 60 expertů z 15 různých zemí jsme analyzovali reálné příklady užití AI v NATO a relevantní průmyslové standardy s cílem navrhnout obecný přístup k ověřování souladu AI aplikací s principy zodpovědného užití AI v rámci NATO. Článek prezentuje poznatky NIAG SG 279, které lze aplikovat i v dalších oblastech.

## Zaměření na kybernetickou bezpečnost v EU: Úloha agentury EU pro kybernetickou bezpečnost

strana 45

Juhan Lepassaar

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), která byla zřízena v roce 2004 a původně se nazývala Evropská agentura pro bezpečnost sítí a informací, byla v roce 2019 rozšířena a její mandát se stal trvalým na základě evropského zákona o kybernetické bezpečnosti (CSA).

## Směrem k řešení OT kybernetické bezpečnosti

strana 44

Ilja David, Roman Jašek

Článek se zabývá řešením kybernetické bezpečnosti provozních technologií (OT) a vybranými příklady jejich incidentů i s odůvodněním, proč je musíme řešit a jaké bezpečnostní frameworky zvolit. Dále také rámcově popisuje i průmyslová odvětví, ve kterých se tyto technologie používají a popisuje hlavní skupiny OT systémů.