

## Rozhovor: Adéla Klečková

strana

6

Daniela Seigová

Adéla Klečková se zaměřuje na konflikty v kybernetickém prostoru a na kybernetický aktivismus. Vystudovala „summa cum laude“ Fakultu válečných studií na King's College London. Vedla výzkumné projekty týkající se kybernetických a informačních operací pro mezinárodní organizace a instituce, jako jsou Evropský parlament či Severoatlantická aliance. V rozhovoru se jí ptáme na internetové trolly a elfy, projekty, dezinformace a další.



## Jak na bezpečnost pomocí ChatGPT - část II.



strana

16

David Pecl, Matej Kačic

V druhém díle seriálu o ChatGPT se zaměříme na možnosti využití této umělé inteligence v oblasti red i blue team bezpečnosti. Podíváme se také na novinky na poli dynamicky se vyvíjející umělé inteligence.

## Rozhovor: Ondřej Kapr

strana

28

Daniela Seigová

Ondřej Kapr působí u Policie ČR více jak 16 let. Je v radě odboru hospodářské kriminality - Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR, kde se mimo jiné zabývají metodikou a koordinací tzv. ostatní kriminality páchané v kybernetickém prostoru, kam spadají například podvody páchané v online prostředí, mravnost, či problematika dětské a závadové pornografie. Pplk. Kapr je součástí skupiny, která se zabývá problematikou podvodů páchaných v kybernetickém prostoru. V rozhovoru se jej ptáme například na dopadení „pedokrále Plyšáčka“, Benešovskou nemocnici, mezinárodní spolupráci a další.



## Nařízení EU o digitálních službách: možné právní nebezpečí - část II.



strana

11

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.

## Phishingator - Praktické vzdělávání uživatelů - část I.



strana

22

Jan Kolouch, Aleš Padrta, Martin Šebela

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.

## Kdo nebo co je DORA? Snaha EU o zvýšení úrovně kyberbezpečnosti finančního sektoru



strana

31

Ondřej Linhart, Petr Šimsa

Článek přibližuje čtenářům obsah nového Nařízení o digitální provozní odolnosti (DORA), které se vztahuje na finanční subjekty a poskytovatele ICT služeb působících v EU. Autoři zároveň hodnotí náročnost implementace požadavků nařízení a nastiňují možnosti využití synergií s již implementovaným systémem řízení bezpečnosti informací dle mezinárodního standardu ISO/IEC 27001.



## Trestní odpovědnost za jednání robotů využívajících AI



strana  
36

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.

## Kovergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti



strana  
45

Ilja David, Roman Jašek

Článek se zabývá řešením kybernetické bezpečnosti provozních technologií (OT). Rámcově popisuje průmyslová odvětví, ve kterých se tyto technologie používají a popisuje hlavní skupiny OT systémů. V článku jsou dále popsány vybrané příklady kybernetických incidentů v OT prostředí a popsány důvody, proč je OT kybernetickou bezpečnost důležité řešit. V závěru jsou popsány výzvy, kterým obor OT kybernetické bezpečnosti čelí a bezpečnostní frameworky, kterými se OT kybernetická bezpečnost úspěšně řeší.

## Deepfakes: Bezpečnostní výzva pro naše uši



strana  
41

Anton Firc, Kamil Malinka, Petr Hanáček

Deepfakes jsou mezi námi již několik let, během kterých urazily dlouhou cestu od buzzwordu a nevinné zábavy až po reálnou hrozbu. V poslední době narůstá počet hlášení o incidentech, kdy byly použity hlasové deepfakes. Tyto útoky cílí jak na lidi, tak systémy. Článek reaguje na tento nový fenomén a diskutuje bezpečnostní dopady využívání této technologie a výzvy, které je potřeba zdolat pro zmírnění dopadů těchto nových hrozeb.

## Recenze knihy: Kybernetická kriminalita

strana  
50

Tomáš Sokol

## PRÁVNÍ RUBRIKA

Virová stránka

52

Normy a publikace

54

Konference IS2

55

Metamorfosa: Nutné kroky k bezpečnému zdravotnictví

57

Právní rubrika

58

Management summary

60

Tiráž

62

**„Nárůst v používání vishingu v tzv. podvodech založených na reakci mezi I. čtvrtletím 2021 a I. čtvrtletím 2022 byl téměř o 550 %.“**

...celý článek Deepfakes najdete na str. 41.