

Rozhovor: Marek Ebert

Miroslav Uříčář

strana

6

Předseda Rady Českého telekomunikačního úřadu absolvoval Vysokou školu dopravy a spojů v Žilině (dnes Žilinská univerzita), obor provoz a ekonomika spojů. Postupně se podílel na přijetí řady regulačních a prospěšných opatření a na přípravě souvisejících legislativních návrhů. V dubnu roku 2020 byl vládou jmenován do funkce člena Rady ČTÚ. V rozhovoru se ho ptáme, jak nahlíží na možnosti samoregulace místo regulačních zásahů v některých oblastech, jak vnímá vývoj tohoto úřadu v posledních letech a další.



Koncept zón a konduktů pro zabezpečení provozních technologií (OT) – část I.

Ilja David, Roman Jašek



strana

16

Článek pojednává o konceptu bezpečnostních zón a konduktů, jenž je základem hloubkové obrany provozních technologií (tzv. Operational Technologies - OT). Tento koncept je důležitý pro ochranu kritické infrastruktury a průmyslových podniků, neboť umožňuje navrhnout bezpečnou a zároveň efektivní segmentaci systémů organizace. Je-li užitý společně s modelem PERA, umožňuje zároveň segmentovat systémy na základě bezpečnostního a zároveň funkčního profilu. V článku je popsán koncept zón a konduktů, definice zóny i konduktu a pojednáno o vztahu konceptu zón a spojení a modelu PERA.

Rozhovor: Erik Feldman

Martin Haloda

strana

27

Předseda představenstva VDT Technology a.s. se specializuje na systémy a řešení pro vnitřní bezpečnost. Má zkušenosti s projekty pro Policii ČR, Generální ředitelství cel, Letiště Praha, Ministerstvo obrany, Ministerstvo vnitra a Ministerstvo spravedlnosti. V rozhovoru se ho ptáme, jaký je rozdíl oproti minulému kamerovému systému ve Fakultní nemocnici v Ostravě, zda systém dokáže rozpoznat, když má někdo zbraň a další.



Mezinárodněprávní úprava elektronických důkazních prostředků – část I.

Veronika Hloušková



strana

12

Článek se zabývá mezinárodní právní úpravou elektronických důkazních prostředků. Pozornost je věnována zejména nově přijaté úpravě v rámci Evropské unie. Unijní úprava v souvislosti se sjednocením a zefektivněním zajišťování a jiným nakládáním s elektronickými důkazy v rámci trestního řízení přijala několik právních instrumentů. Článek se věnuje evropskému vyšetřovacímu příkazu, evropskému vydávacímu příkazu a evropskému uchovávacímu příkazu. V závěru pak kriticky hodnotí nově přijatou legislativu.

Fault-tolerant a kyberneticky bezpečný řídicí systém založený na blockchainu

Otto Havle, Jakub Kozák, Věra Šmídová, Jakub Vodsedálek



strana

21

Článek se zabývá principy průmyslového řídicího systému, který využívá technologii blockchainu, aby získal odolnost proti selhání a vysokou kybernetickou bezpečnost. Uvádí možné oblasti použití takového řídicího systému.

Sít' nelže

Matěj Pavelka



strana

31

Existuje podceňovaný zdroj pravdy, na který se můžete spolehnout, když jsou ostatní zdroje bezpečnostních a forenzních dat ohroženy (nebo jsou příliš nákladné). Různé aspekty ilustruje bezpečnostní incident, který začal na úrovni ISP a nakonec skončil v OT síti SME. Projdeme si jednotlivé kroky v řetězci útoku a zjistíme, jaké stopy zůstaly po jednotlivých krocích v síťových protokolech, jaký další kontext bylo možné získat ze síťové vrstvy, s jakou mírou jistoty jej bylo možné odhalit a jak je možné některé kroky zmírnit nebo jim dokonce zcela zabránit. Článek stanoví, že bezpečnost malých a středních podniků je často podceňována, a nabízí možnou spolupráci s poskytovateli internetových služeb.

DSM 1 | 2024

DSM

Obsah

OBSAH

Elektronické důkazy v trestním řízení – právní nástroje využívané k jejich získávání – část I.

Veronika Hloušková



strana

37

Článek analyzuje procesní nástroje, které jsou orgánům činným v trestním řízení svěřeny na základě zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a jež jsou současnou praxí užívány v souvislosti s dokazováním elektronickými důkazními prostředky. Hlavním cílem článku je zhodnocení, zda je současná právní úprava dostačující k účinnému zajištění elektronických důkazů a zároveň chrání ústavně garantovaná práva osob, aniž by docházelo k nepřiměřenému zásahu do těchto práv. Rozebráno je zajišťování elektronických důkazů z e-mailových schránek a sociálních sítí.

Rozhovor: Sylvain Leblanc

Martin Haloda

strana

48

Profesor počítačového inženýrství na Royal Military College of Canada (RMC), kde také působí jako ředitel oddělení kybernetické bezpečnosti a hlavní vyšetřovatel v Laboratoři počítačové bezpečnosti (CSL). Zabývá se výzkumem v oblasti počítačové bezpečnosti a provozu počítačových sítí, přičemž hlavní úsilí věnuje kybernetické bezpečnosti vozidlových systémů, obraně proti špiónážním a podvodným operacím v počítačových sítích, vyhodnocování zranitelnosti a zabezpečení a vzdělávání v oblasti kybernetické bezpečnosti. V rozhovoru se ho ptáme, jaké činnosti je třeba provést pro zajištění spolehlivého provozu vojenských systémů v oblasti kybernetické bezpečnosti, na jaké hlavní oblasti kybernetické bezpečnosti se zaměřuje a další.



Infostealer malware

Daniel Hejda



strana

40

V našem průzkumu světa kybernetických stínů odhalíme zákulisí infostealer malware, skrytého digitálního zloděje. Prozkoumáme, jak tento škodlivý software proniká do vašeho soukromí a jaké informace si z vašich digitálních trezorů odnáší. Dále se ponoříme do temných vod černého trhu, kde se prodávají ukradená data, a odhalíme, jak se tyto informace stávají zbožím. Zjistíme, jak se tento malware šíří a rozmnožuje, a nakonec vám poskytneme návod, jak se proti této neustále se vyvíjející hrozbě bránit. Připravte se objevit, jak se chránit před infostealer malware, neviditelným nepřitelem ve vašem počítači.

RUBRIKY

Virová stránka

50

Normy a publikace

52

Má mozek ještě šanci?

53

Blízké perspektivy kyberneticky bezpečné letecké dopravy

56

Právní rubrika

58

Management summary

60

Tiráž

62

„Na světě neexistují dva lidé, kteří by měli identickou chuť... pokud systém definuje zájmovou problematickou osobu, tak at' si na sebe oblékne cokoli, chuť jí vždycky prozradí.“

...rozhovor s Erikem Feldmanem najdete na str. 27.