

Rozhovor: Pavel Východský

Martin Haloda

Ing. Pavel Východský, Ph.D., byl k 1. květnu 2022 zvolen do funkce člena představenstva Letiště Praha, a. s., se zodpovědností za oblast korporátních služeb. Jeho současná pozice v oblasti korporátních služeb na Letišti Václava Havla Praha (LVHP) s sebou nese odpovědnost za oblast financí, informačních technologií, lidských zdrojů, kybernetické bezpečnosti, interního auditu, compliance a řízení rizik. V rozhovoru se ho ptáme, jaké digitální technologie dnes nejvíce ovlivňují fungování letiště, jakým způsobem letiště chrání klíčové IT systémy a další.



strana
6

Zajištění bezpečnosti chráněných osob a ochrana jejich osobních údajů ve virtuálním prostředí zdravotnického zařízení – část II.

Lukáš Miklas, Jan Kolouch

Druhá část článku se zaměřuje na aplikaci bezpečnostních opatření pro ochranu osobních údajů chráněných osob v digitálním prostředí zdravotnických zařízení. Autoři analyzují analogickou aplikaci právních norem z oblasti fyzické bezpečnosti a ochrany osobních údajů na kybernetické hrozby. Zabývají se implementací specifických technologií, jako jsou šifrování, vícefaktorová autentizace a systémy dynamického řízení přístupu, které zabezpečují data uvnitř i mezi zdravotnickými zařízeními. Využívají mezinárodních zkušeností a doporučení, aby ilustrovali efektivitu těchto opatření v reálných podmínkách.



strana
15

ZeroTrust security model sa vždy šíje na mieru, pričom úspech je v postoji jednotlivca – část III.

Tomáš Masný

Chcete zabezpečiť svoj biznis na najvyššej úrovni? Prechod na model Zero Trust je nevyhnutný krok pre moderné firmy. Získajte komplexný pohľad na to, ako posunúť svoju kybernetickú bezpečnosť na nový level. Zbavte sa závislosti na tradičných perimetrových riešeniach a chráňte svoje dáta nezávisle na ich umiestnení. Zistíte, ako minimalizovať riziko útokov a zvýšiť odolnosť vašej organizácie pomocou konceptu Just-in-Time prístupu a ďalších moderných bezpečnostných mechanizmov.



strana
29

Výzvy implementace DORA

Martin Fleischmann

Téma textu je věnováno hlavním výzvám, které provází a budou provázet implementaci nařízení DORA v regulovaných institucích, upozornění na některé změny v požadavcích kladených na instituce i v nástrojích používaných orgány dohledu. Článek se v této souvislosti dotýká nesporných přínosů, ale i potenciálních úskalí nové regulace. Podstatným předpokladem ke zvládnutí výzev spojených s implementací DORA je připravenost ke změně přístupu k zajištění kybernetické bezpečnosti napříč organizací, vedením společností počínaje. Součástí příspěvku je i zasazení DORA do kontextu dalších souvisejících evropských legislativních iniciativ zejména ve vztahu ke směrnici Network and Information Security 2 (NIS2).



strana
11

Role AI v oblasti DevOps a ITSM – jak implementovat AI v DevOps? – část II.

Vladimír Kufner

V této části série článků o AI se věnujeme, jak ji optimálně implementovat. Je jasné, že neexistuje nějaký přesný a určitě úspěšný návod a komplexita tématu neumožňuje jít do nějaké větší úrovně detailů, takže si probereme roli a klíčové funkce AI (resp. ML) v procesu DevOps, představíme si obecné návodné principy, kterých bychom se při implementaci AI do DevOps měli držet. Probereme i negativní faktory jako jsou nevýhody nasazení AI, identifikované výzvy a rizika.



strana
22

Důvěryhodné služby, eIDAS2 a Národní blockchainový registr NABRE

Otto Havle, Jakub Kozák, Věra Šmídová, Jakub Vodsedalek

Autoři se zabývají postavením blockchainu v rámci důvěryhodných služeb definovaných nařízením EU 2024/1183 známým jako eIDAS2. Toto nařízení je průlomem, který pokládá legislativní základy k využití blockchainu mimo kryptoměny, do běžné průmyslové a obchodní praxe. Článek seznamuje s důvěryhodnými službami a technologiemi, současným stavem implementace eIDAS2.



strana
34

DSM 1 | 2025

DSM Obsah

OBSAH

Články označené prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

CSIRT.CZ – 15 let ve sdružení CZ.NIC

Pavel Bašta

Pozornost je věnována vývoji národního bezpečnostního týmu CSIRT.CZ a jeho služeb v reakci na měnící se kybernetické hrozby. Na konkrétních incidentech ukazuje, jak se proces řešení bezpečnostních událostí vyvíjel od reaktivního přístupu až po proaktivní opatření a vznik nových preventivních služeb. Případ sofistikovaného útoku Red October pak dokládá, že i české instituce se mohou stát cílem vyspělých kybernetických útoků a proč je nutné neustále inovovat bezpečnostní postupy.



strana
41

Národní kryptografické prostředky

Jiří Truxa

Národní kryptografické prostředky hrají klíčovou roli v ochraně citlivých informací v době rostoucích kybernetických hrozeb a technologického pokroku. Nejde jen o kryptografii samotnou, ale i o širší kontext jejich využití v globalizovaném světě, kde dominují cloud computing, umělá inteligence a kvantové počítače. Jaká je jejich budoucnost a proč je důležité, aby si státy udržely kontrolu nad vlastními bezpečnostními technologiemi?



strana
51

Tzv. data retention v českém právním řádu

Jaromír Novák

Článek shrnuje vývoj právní úpravy data retention v českém právním řádu, včetně posledních změn vyvolaných překotně schváleným konsolidačním balíčkem.



strana
47

RUBRIKY

Normy a publikace	55
Ohlédnutí za IS2 2024	56
Právní rubrika	58
Management summary	60
Tiráž	62

„Ideální kombinace využít AI jako podporu, ale kontrolu ponechat člověku...“

...rozhovor s Pavlem Východským najdete na str. 6.