


Články označené  prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

Rozhovor s Jeffreyem Bardinem

Adam Lamser

Jeffrey Bardin je výkonným ředitelem a zároveň hlavním zpravodajcem ve firmě Treadstone71. Jako předního odborníka jak na zpravodajství, tak i na kyberprostor jsme se ho v tomto díle ptali na cyber threat intelligence, co to vlastně znamená být zpravodajcem v soukromém sektoru a jak vnímá pokroky kybernetické bezpečnosti od jejího zrodu.



strana

7

PKI v systému pro správu kryptografických klíčů – část II.

Jiří Urbanec

V druhé části miniseriálu o PKI zapojeném do systému správy asymetrických klíčů je popsána architektura typického CKMS pro asymetrické klíče, jeho funkční bloky, procesy, požadavky a přehled existujících standardů, na kterých jsou CKMS stavěny. Architektura je popsána z pohledu schopnosti spravovat velké množství různých klíčů a schopnosti rychle a s malým rizikem selhání přecházet mezi službami a dodavateli, a to bez narušení provozu. Článek v závěru shrnuje aktuální výzvy v zapojení konceptu CKMS a dává doporučení pro organizace vyžadující pružnost v řízení asymetrických klíčů.



strana

18

Řízení incidentů v souladu se současnou legislativou – část II.

Jaromír Veber

Článek se zaměřuje na popis toho, jakým způsobem současná legislativa zasahuje do procesu řízení incidentů. Jsou popsány relevantní legislativní požadavky zákonů v oblasti platebních služeb a GDPR a jejich uplatnění při procesu řízení incidentů v praxi. Čtenáři si tak mohou ověřit, zda jejich proces je vhodným způsobem nastaven, nebo jakým způsobem proces přizpůsobit, aby vyhovoval legislativě, která se na ně uplatňuje.



strana

26

Wireless M-Bus: kdo ví, že perete?

Libor Polčák

Tento článek se zabývá odečty spotřebovaných energií pomocí protokolu Wireless M-Bus. Vzhledem k požadavkům vyplývajícím z obecného nařízení o ochraně osobních údajů upozorňuje na rizika použití tohoto protokolu v domácnostech a přináší rady, jaká data přenášet.



strana

13

Uplatnění kultury DevOps v Portálu občana

Jan Vlasák

Autor přibližuje řešení Portálu občana z pohledu způsobu jeho vývoje a provozu, do kterého se promítají současné trendy kultury DevOps. Zároveň popisuje, jakým způsobem je realizována bezpečnost v projektu, který je od samého počátku řízen agilně a kde je vítána každá změna v implementaci softwaru nebo samotné infrastruktury.



strana

23

Testování blockchainových řešení

Jakub Jedlinský, Kryštof Jelínek

Článek se zabývá současným stavem využitelnosti blockchainových řešení. Rozlišuje mezi korporátními DLTs a veřejnými DLTs. Následně prezentuje výsledky uživatelského testování čtyř aplikací na veřejných blockchainech a vyvozuje z nich obecnější poznatky o připravenosti těchto řešení.



strana

32



Tento článek dále rozvíjí téma bezpečnosti v rámci DevOps a navazuje tak na předchozí díl. Vysvětluje koncept kontinuální bezpečnosti (Continuous Security), diskutuje téma vazeb bezpečnosti a infrastruktury v kontextu využití cloud computingu a popisuje nutné změny, jak bezpečnost do DevOps implementovat na úrovni technologií, procesů a firemní kultury. Vysvětluje koncept vůdcovství a angažovanosti vyššího managementu jako klíčového faktoru úspěchu pro SecDevOps. V závěru je ilustrován praktický příklad začlenění některých bezpečnostních metod do životního cyklu DevOps a diskutovány přínosy bezpečnosti pro DevOps a obráceně.

Klamat a mást protivníka: jak získat taktickou výhodu změnou vašeho kybernetického terénu

PR Fidelis Cybersecurity

D I R D I K V

Virová stránka

52

Normy a publikace

54

Metamorfosa: Letní soirée

55

Informace z partnerských společností

56

Právní rubrika

58

Management summary

60

Tiráž

62

Nová komunikační síť pro systém IoE (Internet of Everything) pro Papežskou baziliku a svatý konvent sv. Františka z Assisi



Fabio Garzia

Článek popisuje realizaci projektu nové komunikační sítě v unikátním prostředí, kterým je bazilika sv. Františka v italském Assisi. Pro projekt byly využity nové postupy, jako jsou Internet všeho (IoE), integrovaný multidisciplinární model řízení zabezpečení a bezpečnosti (IMMSSM), genetické algoritmy (GA) a informační digitální model budovy (BIM). Popsané metody jsou obecně použitelné na kterékoliv podobné lokalitě.

Zatímco vývoj a funkce budou už někde na měsíci, bezpečnost se nedostane ani do vedlejší místnosti. Stejný problém, jako jsme řešili před 20 lety.

...Rozhovor s Jeffreyem Bardinem najdete na str. 7.