


OBSAH

Články označené  prošly odborným recenzním řízením.

Články označené firemním logem jsou komerčními prezentacemi.

Daniel Rous

Michal Wojnar, Daniela Seigová

Rozhovor s Danielem Rousem – bezpečnostním ředitelem Skupiny ČEZ. Za DSM jsme se ptali na možnost blackoutu v ČR, zkušenosti z praxe ve zpravodajských službách, zabezpečení dodavatelského řetězce po kauzách SolarWinds a Hafnium a bezpečnostní opatření spojená s dostavbou Dukovan a mnoho dalšího.



strana
8

Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443

Ilja David, Luděk Lukáš

Článek se zabývá řešením kybernetické bezpečnosti dle norem IEC 62443, rámcově popisuje kategorie technických i organizačních bezpečnostních požadavků a jednotlivých úrovní bezpečnosti. Dále podrobně analyzuje, jakým způsobem jsou v této normě řešena kompenzační opatření, možné důvody jejich zavedení a je zde navržen soubor možných kompenzačních opatření. Kompenzační opatření lze poté aplikovat v rámci komplexního systému řízení kybernetické bezpečnosti.



strana
16

Hodnocení zranitelnosti – část II.

Lubomír Almer, David Pecl

Návrh nové metody pro hodnocení zranitelnosti, který eliminuje nedostatky Common Vulnerability Scoring Systému a OWASP Risk Rating. Tato metoda využívá jednotlivé silné stránky těchto nejpoužívanějších metod a zároveň minimalizuje jejich slabé stránky. Utváří tak komplexní metodu pro efektivní a přesné hodnocení zranitelnosti, které je vztažené přímo na hodnocené prostředí.



strana
28

Průzkum: Bezpečné zdravotnictví v ČR 2020 – část II.

Karolína Kubínová, Michal Wojnar

Společnost PricewaterhouseCoopers zkoumala ve spolupráci s TATE International úroveň kyberbezpečnosti v českém zdravotnickém sektoru. Průzkum se zaměřil například na vývoj technologií ve zdravotnictví v příštích letech, jejich zabezpečení a vliv pandemie na zdravotnictví. Součástí průzkumu byly mimo jiné také otázky týkající se investic v sektoru, subjektivního vnímání citlivosti určitých typů informací nebo otázky zaměřené na identitu jednotlivých aktérů hrozeb. Tento dvoudílný seriál přináší druhou část přehledu nejzajímavějších výsledků, které průzkum nabízí.



strana
11

Dramatický nárůst zájmu o provozní a lokalizační údaje

Miroslav Uříčář

Povinné plošné uchování provozních a lokalizačních údajů (Data Retention) a jejich využívání oprávněnými orgány bylo v posledních letech předmětem mnoha soudních rozhodnutí. Společně vyhlášené rozsudky Soudního dvora EU ze 6. října 2020 jsou zatím nejnovější v této řadě. Soudní dvůr v nich opětovně deklaroval zákaz plošného uchování provozních a lokalizačních údajů, současně vymezil výjimky z tohoto zákazu a stanovil podmínky pro jejich aplikaci, vždy se musí jednat o výjimečné a časově omezené situace. V právním řádu ČR však naopak čím dál víc přibývá orgánů oprávněných vyžádat si provozní a lokalizační údaje. K dosavadním orgánům nedávno přibyl Úřad pro ochranu osobních údajů, nyní by měly následovat Úřad pro ochranu hospodářské soutěže a Státní hygienická služba. Autor má silné pochybnosti o souladu těchto návrhů s jednoznačnými závěry Soudního dvora.



strana
23

Identity Management aneb Centralizovaná správa identit v IT systémech

Lukáš Cirkva

Článek o Identity Managementu pojednává o tom, co je a co není IdM, kdy je vhodné jej zvolit a s čím konkrétně vám může pomoci. Dozvíte se informace od automatizace procesů IdM až po jeho výhody v souvislosti s bezpečností, centralizací i evidencí. Dále získáte informace ohledně IdM a správy konkrétních účtů. Z článku zjistíte, jak vybrat vhodný IdM, na co si při jeho výběru dát pozor a které otázky byste měli dodavateli klást. Dozvíte se také, jak probíhá jeho migrace, čeho se týká a které jsou její dva základní přístupy.



strana
35



Jakub Čegan, Daniel Tovarňák

Článek se věnuje open source platformě pro kyberbezpečnostní vzdělávání vytvořené Masarykovou univerzitou při řešení projektů Bezpečnostního výzkumu Ministerstva vnitra. V první části se popisuje genezi vzniku platformy, důvody pro rozhodnutí poskytnout ji jako otevřené řešení a její současné využití. Druhá část přináší vhléd do technologie platformy a zejména se zaměřuje na technický popis přípravy a realizace kyberbezpečnostních školení.

Síň slávy Cybersecurity

Představení ocenění a krátký rozhovor s Jaroslavem Šmidem.

ITIL 4 – Základní koncepty a fakta – část II.



Vladimír Kufner

Článek pokračuje v představování základních faktů o ITIL 4 započatým v 1. dílu. Konkrétně představuje pět základních komponent systému hodnoty služeb SVS. Začíná sedmi tzv. Návodnými principy (doporučované metody přístupu při implementaci). Dále diskutuje oblast Governance (návaznost na ISO 38500) a vysvětluje co je to Hodnotový řetězec služby SVC se šesti jeho klíčovými aktivitami. Poslední dvěmi probíranými částmi SVS je oblast tzv. Praktik a Kontinuálního zlepšování.

„V budoucnu je proto podle mého názoru třeba věnovat maximální úsilí vzdělávání lidí tak, aby si každé dítě už od základní školy uvědomovalo, že osobní údaje jsou jeho vlastnictvím stejně jako pastelky, mobil nebo v budoucnu dům, a podle toho se ke svým i cizím osobním údajům chovalo.“

...Rozhovor s Danielem Rousem najdete na str. 8.

RUBRIKY

Virová stránka	54
Normy a publikace	56
Metamorfosa: Zabijačka anebo workshop	57
Právní rubrika	58
Management summary	60
Tiráž	62