FÓRUM

www.cacio.cz

ČESKÁ ASOCIACE MANAŽERŮ INFORMAČNÍCH TECHNOLOGIÍ

Cacio

ČASOPIS PŘEDSTAVUJE VÝBĚR ČINNOSTÍ ASOCIACE CACIO V OBDOBÍ 9.2020 AŽ 12.2021

Vážené čtenářky, vážení čtenáři,

žijeme v době, kterou jsem si neuměl reálně představit. Pandemie covidu, růst cen energií i útok na Ukrajinu prověřily naše morální vlastnosti, prověřily připravenost informatik na rychlou změnu, ukázaly možnosti informatiky efektivně pomáhat a řešit nečekané úkoly. Každý z nás si odnesl řadu cenných zkušeností, o které jsme se snažili na akcích CACIO podělit a inspirovat se jimi. Nyní držíte v ruce časopis, který velice stručně rekapituluje činnosti CACIO v období 9.2020 až 12.2021. Akce byly trochu jiné, než v jiných letech, naučili jsme se organizovat on-line semináře, pořádáme hybridní semináře a jiné aktivity, které umožňují vzdálené zapojení účastníků, což vidím jako veliký klad, který přináší možnost efektivní komunikace s účastníky mimo Prahu. Jako další velký klad vidím otevřenost diskutujících, které si velice vážím.

Přeji Vám příjemné čtení a těším se na setkání na akcích CACIO.

Miroslav Hübner
Předseda CACIO

Telegrafická roční zpráva řídicího výboru Cacio

Rok 2021 se zařadil mezi covidové roky. Podařilo se zorganizovat soutěž IT projekt roku, včetně slavnostního předání cen na koncertu v Michnově paláci. Zorganizovali jsme tři hybridní semináře a tři on-line semináře a podíleli se na 7 odborných setkáních, konferencích či seminářích, kde jsme se věnovali praktickým aspektům řízení vnitropodnikové informatiky.

Ke konci roku 2021 jsme měli 172 členů.

Řídící výbor CACIO pracoval ve složení:

- *Ing. Miroslav Hübner, MBA, Předseda CACIO*
- *Ing. Miloslav Marčan, Místopředseda CACIO*
- *Ing. Jiří Polák, CSc, Výkonný ředitel CACIO*
- *Ing. Rostislav Jirkal, Výkonný ředitel CACIO*
- *Ing. Dušan Chlapek, Ph.D. , člen řídícího výboru CACIO*
- *Ing. Hana Staňková, Člen řídícího výboru CACIO*
- *Ing. Petr Pokorný, Člen řídícího výboru CACIO*
- *Ing. Josef Lukeš, Člen řídícího výboru CACIO*
- *Ing. Jan Heisler, Člen řídícího výboru CACIO*
- *Jan Vojtěch Binder, Člen řídícího výboru CACIO*
- *Ing. Pavel Mánek, Člen řídícího výboru CACIO*
- *Ing. Vít Suchánek, Člen řídícího výboru CACIO*
- *Ing. Josef Fantík, Člen řídícího výboru CACIO*
- *Jitka Koudová, Tajemník CACIO*
- *Veronika Melicharová, Tajemník CACIO*

Pokud bychom měli shrnout dané období, lze konstatovat, že došlo k naplnění cílů asociace, což je pomoc při sdílení informací a budování odborné komunity.

Zlatí partneři CACIO

Zapálený idealista s velkými vizemi, a ještě větším srdcem

Odchod Jiřího Poláka zasáhl mnohé. Troufnu si říct, že jen málo osobností ve významných pozicích Jiřího Poláka neznalo. Jiří v jedné ze svých rolí, ať už jako expert, uznávaná autorita, učitel nebo mentor ovlivnil několik generací. Jiřího profesní přesah od poradenství, přes telekomunikaci a energetiku, vzdělávání a v neposlední řadě i založení dvou významných tradicí na poli vážné hudby ukazuje příběh člověka, který bez okázalých gest dokázal uvádět v život nemožné. Ve širším středoevropském kontextu, který člověku Jiřího formátu patřil, je příhodné použití výrazu „mensch". Osobnost, která je hodna obdivu a následování s ohledem na vznešenost charakteru.

Vizionář, člověk, který měnil svět k lepšímu

Izraelská tradice hovoří o konceptu „tikun olam" neboli o napravování světa. Každý z nás může svými činy přispět k tomu, aby se svět stal lepším místem k žití. Jiří za svůj život měnil a změnil k lepšímu hned několik světů. Měl energii a nadšení jak pro velké systémové změny, tak smysl pro pomáhání jednotlivým lidským osudům. Pomohl vždy a mnohým. Skromně, bez velké pozornosti či nároků na odměnu. Transformoval velké nadnárodní společnosti, pomáhal zlepšovat státní správu a přispěl k rozvoji občanské společnosti v tom nejlepším slova smyslu.

Vedení naší asociace CACIO Jiří věnoval více než 20 let svého života. Založením Nadačního fondu Věčná naděje a Institutu terezínských skladatelů naplnil svoje poslání péče o odkaz obětí holokaustu. Přečtěme si knihu o osudu jeho otce, Erika Poláka, jehož memoáry vyšly jak v knižní podobě, tak v podobě audioknihy pod názvem Tři kapitoly.
https://vecnanadeje.org/audiokniha/

Nezapomeneme!

Pod heslem Nezapomeneme! si každoročně připomínáme hrůzy holokaustu a vzpomínáme na 6 000 000 židovských obětí. Podle židovské tradice člověk umírá dvakrát. První smrtí je odchod z fyzického světa, k druhému úmrtí dochází, pokud na člověka zapomeneme.
My všichni, které Jiří Polák svými činy ovlivnil, pojďme na Jiřího vzpomenout tím, že budeme dále šířit odkaz institucí, které založil. Zajímejme se o práci Institutu terezínských skladatelů. Podporujme dále Nadační fond Věčná naděje a navštěvujme povznášející koncerty. Právě nadčasová a všeobecně srozumitelná hudba může být mostem mezi námi a odkazem Jiřího. A naučme se milovat a užívat život tak, jak to Jiří do posledních chvil dokázal a aby se na něj vzpomínalo, jak by si přál.

Rozhovor s prof. Miroslavem Bártou

Miroslava Bárty, předního českého egyptologa, se ptal Jiří Polák, výkonný ředitel CACIO.

Energie a její cena jsou významným faktorem, jak sám píšete. Co k tomu mohou přinést nove zdroje energii? (poznámka: Provozní náklady na jednu MWh z Temelína jsou v řádu jednotek euro, jinak se jedna MWh obchoduje kolem 1500 Kč.) Kde hledat odpověď na nové levné zdroje energie?

Kdo má odpověď, ten zná budoucnost… Já ji nemám. Ale myslím si, že v budoucnosti bude naprosto zásadní energie získávaná ze slunce a především její uchovávání, stejně jako jaderná energie. Vítr je v tuto chvíli krajně nespolehlivý a jen v letošním roce naši energetici zahraňovali Německo před blackoutem nejméně čtyřikrát.

Výstava o energiích byla a je velmi dobrá. Nezapomnělo se při jejím koncipováni na obrovskou energii lidských mozků, které dokáží téměř energeticky nemožné, tj. z kila cukru přinést vynález, který nahradí tuny cukru. Jaká je role vědy a vynálezu ve vývoji civilizace?

Naprosto zásadní. Od okamžiku inovace knihtisku Gutenbergem se obrovsky zrychlil pohyb a sdílení informací. Najednou začaly být myšlenky a nové vynálezy mnohem rychleji mnohem dostupnější. Od zhruba roku 1500 můžeme sledovat díky tomu obrovský boom prakticky ve všech vědních oborech – matematice, fyzice, chemii, medicíně i přírodních a technických vědách.

S tím souvisí ještě jedna otázka, nechybí nám tedy ve výčtu energií energie lidského intelektu? (Nechci psát mozku, možná by se hodilo "mozků".) Jde o kumulativní energii, jejíž uchování a zásadní rozvoj přineslo až používání písma (a knihtisku). Jak do vývoje a kolapsu civilizací zasahuje existence psaných dokumentů?

Naprosto zásadně. Písmo a texty jsou jedním z parametrů, na jejímž základě definujeme civilizaci jako takovou. Písemný záznam je nositelem obsahu dané civilizace. Kolaps jako takový se vyznačuje zásadním a skokovým poklesem ve smyslu dostupné energie, což vede k tomu, že se jí nedostává na to, aby si civilizace udržela dosažený stav svého vědění, technologií a podobně.

Jak by se mohla a měla měřit kumulativní energie (zapsaného) lidského poznání?

Tak toto netuším. Možná bychom mohli zkusit vložit rovnítko mezi dodnes vytvořeným množstvím informací. Dodnes bylo na světě vytvořeno až stovky zettabytů dat. A teď jde o to, kolik energie bylo třeba na jejich produkci vynaložit. Ale je dost možné, že ten výpočet nebude dávat smysl.

Jedno promile lidi na světě vlastni 90% bohatství, jak ho měříme v OECD. A jejich bohatství se za posledních 30 let zdvojnásobilo. Zřejmě tedy veškerá legislativa zemí OECD jim hodně pomáhá, aby bohatli stále lépe a radostněji. Je to trend, který ohrožuje budoucnost civilizace? Nebo má pozitivní vliv na budoucnost naší civilizace. Existují v historii obdobné situace?

Nikdy v historii lidstva nepanovala takováto disproporce. A je to samozřejmě „hra" s nulovým součtem, pokud někdo bohatne, někdo jiný chudne. Nemyslím, že nás čekají dobré konce.

Prof. Mgr. Miroslav Bárta, PhD.

Největší světové korporace mají po statisících zaměstnanců po celém světě. Jejich finanční prostředky jim umožňuji koupit si, s trošičkou nadsázky, kdekoliv cokoliv a kohokoliv. Jejich chovaní se dá přirovnat k chamtivosti otců zakladatelů kapitalismu. Jaký význam mají korporace při urychlovaní (nebo zpomalováni) kolapsu naší civilizace?

Obecně nevidím na korporacích nic špatného ani dobrého. Jsou to organismy, které hromadí lidský kapitál a energii, aby mohly realizovat své cíle. Začíná to právě u nich. Ty mohou být dobré nebo špatné, mohou se proměňovat. A mohou se lišit i cesty, které si ta nebo ona korporace vybírá. Ještě bych asi podotkl, že měnit svět vyžaduje velkou energii a obrovskou dávku leadershipu ve spojení se silou ho prosazovat. Velké cíle prostě vyžadují akumulaci vlivu i síly.

Jaký byl smysl egyptských civilizaci? A jak byste ho poměřil se smyslem českých dějin, nebo - evropských dějin - když by se Vám naše kotlina zdála moc malá?

Každá civilizace svůj smysl vytváří a definuje svým bytím. Staří Egypťané vnímali Egypt jako svět, kterému vládne panovník – bůh, který zajišťuje komunikaci s bohy a tím řád světa. Panovník měl povinnost starat se o blaho – živobytí svého lidu a tím udržoval společenskou smlouvu. Dokud na to měl energii, vše běželo. Když došla, nastal kolaps. Ve staroegyptských dějinách nejméně čtyřikrát.

Před časem jsme chvíli diskutovali na téma leadershipu (zejména ve firmách a korporacích). Koho považujete za dobré vůdce ve starověkém Egypte a koho v dnešní Evropě?

Ve starém Egyptě to mohl například být velice dobře zakladatel Staré říše panovník Džoser (žil ve 27. stol. př. Kr.) nebo panovník Nyuserre ve 24. stol. př. Kr. V moderní Evropě například Winston Churchill, Charles de Gaulle nebo Václav Havel.

V zemích OECD (a dalších výkonných ekonomikách) není pravidlem pro velkou většinu jejich obyvatel dřít 10 hodin denně šest dní v týdnu a brát za to méně, než je hranice chudoby. Jinak řečeno v mnoha zemích žije pod hranicí chudoby málo obyvatel – ti ostatní mají např. kde bydlet, koupelny, televize, počítače, topení/klimatizaci, postel, dost jídla; a ještě mají volný čas, aspoň tak 30 hodin týdně. Existovala již v minulosti nějaká taková civilizace? Existují modely budoucího chování jednotlivců a skupin v takovémto prostředí?

Myslím, že efektivita výrobních procesů i masivní nástup AI povede k tomu, že lidé budou muset pracovat stále méně a méně, aby uspokojili své základní životní potřeby, a to povede k novým výzvám ve smyslu fungování států v budoucnosti.

Sluneční králové

Každoročně pořádáme pro partnery a kamarády CACIO setkání, na kterém hodnotíme aktivity spolku, jeho cíle a připravujeme plán na další období. Poslední setkání proběhlo 17. 6. 2021 a podařilo se jej doplnit návštěvou výstavy Sluneční králové, na které nás osobně provázel profesor Bárta.

Výstava Sluneční králové byla výjimečným mezinárodním projektem, který dokumentoval největší archeologické objevy českých egyptologů spjaté s výzkumem egyptského Abúsíru, starověkého královského pohřebiště sousedícího na severu s Gízou a na jihu se Sakkárou.

Jako sluneční králové jsou v egyptských dějinách označováni panovníci 5. staroegyptské dynastie (asi 2435–2306 př. n. l.), kteří jsou neodmyslitelně spjati s lokalitou Abúsír, kde v průběhu jejich vlády vyrostlo královské pohřebiště se třemi pyramidami. Bohatou reliéfní výzdobu, vybavení, ale i běžný chod těchto pyramidových komplexů jsme mohli prozkoumat díky vystaveným předmětům, ale i za pomoci audiovizuálních materiálů. Výstava nepředstavuje pouze osudy vládců starověké země na Nilu. Podívali jsme se i do příslovečného stínu pyramid – nekrálovského Abúsíru.

Z tohoto jedinečného zážitku jsme vám připravili alespoň krátkou fotografickou reportáž.

Soutěž IT projekt roku

CACIO (Česká asociace manažerů informačních technologií) každoročně organizuje soutěž IT projekt roku, jejímž cílem je ocenit nejlepší projekty vývoje, zavedení informačních technologií, pečovat o jejich mediální prezentaci a tím trvale zvyšovat prestiž, kvalitu a přínosy IT projektů.

Účast v soutěži je umožněna jednotlivcům, podnikům, institucím, korporacím, spolkům a sdružením či jakýmkoliv jiným subjektům včetně organizací státní správy a samosprávy bez omezení místem podnikání, majetkovým vlastnictvím či lokalizací jednotky.

Projekt do soutěže přihlašuje zástupce zadavatele projektu nebo uživatele výsledků projektu, který může být současně autorem části či celého projektu.

Soutěž je stanovena jako mezinárodní s tím, že uživatel nebo dodavatel projektu (nebo jeho organizační část) se musí nacházet na území ČR.

Telegrafické informace z posledních dvou velmi úspěšných ročníku jsou v následujících řádcích.

Dovolte nám stručnou rekapitulaci posledních dvou ukončených ročníků soutěže.

IT projekt roku 2019 – 17.ročník

17. ročník soutěže se zařadil opět mezi velice úspěšné, hodnotící komise musela vybrat vítěze z devatenácti velice kvalitních projektů.

Finálové projekty:

- Projekt **„Služba sdílených vozidel pro zaměstnance ŠKODA Click“**, zadavatel: ŠKODA AUTO, a. s., dodavatel: Ústav pro nanomateriály, pokročilé technologie a inovace, Technická univerzita v Liberci
- Projekt **„Chytrý svoz odpadů“**, zadavatel: Hlavní město Praha - odbor životního prostředí – odd. odpadů + městské části Praha 1, 3, 5, 6, 7, 8, 9, 10, 16 a 18., dodavatel: MHMP/ Operátor ICT, a. s.
- Projekt **„Numbro - Profesionální správa kontaktů pro firmy a celé týmy“**, zadavatel: Numbro, s. r. o., dodavatel: elevup, s. r. o.
- Projekt **„Chatovací nástroj na kariérních stránkách kdejinde.cz“,** zadavatel: ČEZ, a. s., dodavatel: Blindspot Solutions, s. r. o.
- Projekt **„Datová platforma hlavního města Prahy - Golemio“,** zadavatel: MHMP/OICT pro MHMP, městské části, příspěvkové a zřízené organizace MHMP a MČ, OpenData pro širokou veřejnost, dodavatel: MHMP/Operátor ICT, a. s.

Vítězné projekty 17. ročníku soutěže IT projekt roku:

- Projekt „**Rozvoj krajského digitálního uložiště PACS snímků“**, zadavatel: Krajský úřad Zlínského kraje, dodavatel: OR-CZ, spol., s. r. o.
- Projekt **„Včasné detekce napadení lesních porostů lýkožroutem smrkovým (Ips typographus) pomocí bezpilotních leteckých prostředků“**, zadavatel: Česká zemědělská univerzita v Praze, dodavatel: HSI, spol. s r. o.
- Projekt „**Bezpečnost informačních systémů nemocnice**“, zadavatel: Psychiatrická nemocnice v Opavě, dodavatel: AUTOCONT, a. s.

Specializovaná ocenění:

- Cenu ČIMIB za přínos v oblasti kybernetické bezpečnosti získal projekt **„Rozvoj krajského digitálního uložiště PACS snímků“** zadavatel: Psychiatrická nemocnice v Opavě, dodavatel: AUTOCONT, a. s.
- Cenu ITSMF za přínos v oblasti řízení služeb informačních a komunikačních technologií získal projekt **„Nový ITIL pro podporu města Ostravy“**, zadavatel: OVANET, a. s., dodavatel: ALVAO, s. r. o.

Čestnou cenu předsedy CACIO získaly:

- Projekt **„Vytvoření, provoz a rozvoj portálu BusinessInfo.cz“**, zadavatel: Česká agentura na podporu obchodu CzechTrade (realizátor), Ministerstvo průmyslu a obchodu (gestor), dodavatel: Barclet, a. s.
- Projekt **„Numbro - Profesionální správa kontaktů pro firmy a celé týmy“**, zadavatel: Numbro, s. r. o., dodavatel: elevup, s. r. o.

IT projekt roku 2020 – 18.ročník

18. ročník soutěže probíhal od 9.2020 do 9.2021 a zúčastnilo se ho dvacet dva velice kvalitních projektů.

Finálové projekty:

- Projekt **„Junior centrum excelence pro kybernetickou bezpečnost a ICT při SŠ Čichnova Brno“**, uživatel: Střední škola informatiky, poštovnictví a finančnictví Brno, dodavatel: Comimpex, spol. s r. o.
- Projekt **„Škola v pyžamu“**, uživatel: veřejná aplikace pro základní školy, zástupce - ZŠ Svážná Brno, dodavatel: Capsa.cz
- Projekt **„Program podpory malých podniků postižených celosvětovým šířením onemocnění COVID-19 působeného virem SARS-CoV-2“**, zadavatel: Ministerstvo průmyslu a obchodu, dodavatel: Unicorn Systems, a. s.
- Projekt **„Implementace Digital Integration HUB s cílem digitalizovat firemní procesy, produkty a prodejní kaná-**

FÓRUM

ly bez změny „legacy“ systémů“, zadavatel: W.A.G. Payment Solutions, a. s., dodavatel: GSW Development, s. r. o.

- Projekt **„Dramox“**, zadavatel: Dramox, s. r. o., dodavatel: elevUP, s. r. o.
- Projekt **„Moje VZP“**, zadavatel a dodavatel: VZP ČR

Vítězné projekty 18. ročníku soutěže IT projekt roku:

- Projekt **„Elektronická neschopenka“**, zadavatel: Česká správa sociálního zabezpečení, dodavatelé: Asseco Central Europe, a. s., KOMIX, s. r. o.
- Projekt **„Aplikace pro plánování optimální nakládky kontejnerů“**, zadavatel: Škoda Auto, a. s., dodavatel: Blindspot Solutions, s. r. o.

Čestnou cenu předsedy CACIO získaly:

- Projekt **„Junior centrum excelence pro kybernetickou bezpečnost a ICT při SŠ Čichnova Brno“**, uživatel: Střední škola informatiky, poštovnictví a finančnictví Brno, dodavatel: Comimpex, spol. s r. o.
- Projekt **„Škola v pyžamu“**, uživatel: veřejná aplikace pro základní školy, zástupce - ZŠ Svážná Brno, dodavatel: Capsa.cz

Specializovaná ocenění:

- Cenu ČIMIB za přínos v oblasti kybernetické bezpečnosti získal projekt **„Junior centrum excelence pro kybernetickou bezpečnost a ICT při SŠ Čichnova Brno“**, uživatel: Střední škola informatiky, poštovnictví a finančnictví Brno, dodavatel: Comimpex, spol. s r. o.
- Cenu ITSMF za přínos v oblasti řízení služeb informačních a komunikačních technologií získal projekt „**Implementace Digital Integration HUB s cílem digitalizovat firemní procesy, produkty a prodejní kanály bez změny „legacy“ systémů“**, zadavatel: W.A.G. Payment Solutions, a. s., dodavatel: GSW Development, s. r. o.
- Cenu CNZ za přínos v oblasti dlouhodobého uchování informací získal projekt **„Digitalizace Krajského úřadu Pardubického kraje, elektronické schvalování a digitalizace oběhu účetních dokladů“**, uživatel: Pardubický kraj, dodavatel: GORDIC, spol. s r. o. (GORDIC Distributor KMS).

Komise soutěže

Velký dík za úspěšnost soutěže patří hodnotitelské komisi, která jednotlivé projekty hodnotí dle kritérií:

I. Cíle projektu, s kterými byl projekt zahajován a jak tyto cíle byly naplněny.
II. Základní parametry projektu (Rozsah, rozpočet a harmonogram).
III. Originalita, zajímavý nápad, netradiční řešení.
IV. Poučení, která projekt a jeho řízení přinesl.

V 17. a 18. ročníku soutěže komise pracovala ve složení:

- *prof. Ing. Zdeněk Molnár, CSc (předseda komise), ČVÚT*
- *Ing. Dušan Chlapek, Ph.D. (místopředseda komise), FIS VŠE*
- *Ing. Jiří Dohnal, ICZ, a. s.*
- *Ing. Jan Heisler, CNZ, o. s.*
- *Ing. Petr Hofman, Škoda Auto, vítěz 16. ročníku*
- *Ing. Ivette Korandová, itSMF*
- *Ing. Petr Koucký, SÚKL, vítěz 16. ročníku*
- *Ing. Jiří Lagner, HSI*
- *Ing. Pavel Mánek, Magistrát HMP*
- *Ing. Petr Plecháček, Ernst & Young*
- *Ing. Jaroslav Straka, CSc, Asseco Central Europe, a. s.*
- *Ing. Vít Suchánek, CACIO*
- *Ing. Aleš Špidla, ČIMIB*
- *Ing. Petr Trojan, ČKD Blansko, vítěz 15. ročníku*
- *Ing. David Šetina, NAKIT (porotce v 17.ročníku)*
- *Ing. Václav Špáňa, KPC Group (porotce v 18.ročníku)*
- *Stanislav Taťoun, Severomoravské vodovody a kanalizace Ostrava, a. s. (porotce v 18.ročníku)*

IT projekt roku 2021

Zdenka Molnára, předsedy hodnotící komise, se ptal Dušan Chlapek, proděkan FIS VŠE a člen vedení CACIO.

Co k tomu říci?

Je to už 19. ročník, to je úctyhodné číslo a těším se (a doufám, že se toho dožiji), na jubilejní 20 ročník, kterým bych rád zakončil svoje dvacetileté působení v roli předsedy Odborné hodnotitelské komise. Devatenáctý ročník byl zahájen vyhlášením soutěže v září 2021 a bude ukončen vyhlášením vítězů soutěže v dubnu 2022. Mezi tím proběhne již zavedená a osvědčená procedura hodnocení přihlášek dle stanovených kritérií a následně tajná volba vítězů.

Jaké je poslání a cíle soutěže?

Posláním soutěže je především přispívat ke zvyšování efektů a kvality projektů ICT a vytvářet žádoucí vzory řešení v této oblasti pro podnikání i veřejnou správu. To je také formálně zaručeno definovanými cíli soutěže, jako možnost přihlásit projekt bez omezení velikostí organizací (neorientovat se pouze na velké organizace), a bez ohledu na aplikační oblasti s oslovením širokého spektra dodavatelů, řešitelů včetně vedoucích pracovníků, aby byly na kladných příkladech ukázány přínosy a síla ICT.

Jak jsou projekty hodnoceny?

Projekty jsou hodnoceny jednak podle toho, jak splňují jednak **formální kritéria** jako jsou základní parametry projektu (rozsah, rozpočet a harmonogram), jaké byly cíle projektu a jak byly tyto cíle naplněny. Rozhodující pro můj přístup k projektům jsou ale **neformální kritéria** jako je originalita, zajímavý nápad, netradiční řešení a hlavně poučení, která z projektu a jeho řízení vyplývají nejen pro IT komunitu, ale i pro laickou veřejnost.

Jaké je složení Odborné hodnotitelské komise?

Komise má obyčejně kolem 16 členů a její složení je velmi pestré, v komisi jsou zastoupeni odborníci z různých oblastí ICT, a to jak dodavatelů, tak uživatelů a také akademické obce. Jsou v ní představitelé významných dodavatelů informačních systémů, poradenských organizací, veřejné správy a také zástupci speciálních organizací, jako jsou „Český institut manažerů informační bezpečnosti“,

Profesor Zdeněk Molnár s žezlem, jako symbolem soutěže, při předávání ocenění 17.ročníku soutěže IT projekt roku

Dušan Chlapek při předávání ocenění 18.ročníku soutěže IT projekt roku

společnosti „Co po nás zbude“ a globální organizace itSMF, která sdružuje organizace zapojující se do řízení ICT. Nově je letos členem komise i zástupce Klubu finančních ředitelů. To složení je opravdu reprezentativní a pro mne je to velká pocta, že mohu s takovými lidmi komunikovat a pracovat.

Existuje etický kodex porotce?

Ano, existuje celkem 7 zásad: (1) **férovost**, kdy každý nominovaný porotce jedná sám za sebe, a to bez ohledu na to, v jaké organizaci pracuje a jaké pracovně hájí zájmy, (2) **zodpovědnost,** pokud má porotce vztah k některému z přihlášených projektů, je jeho povinností oznámit tuto skutečnost předsedovi poroty a tento projekt nehodnotit, (3) **disciplína**, kdy každý porotce si je vědom velmi krátkého časového období, které má pro zpracování a celkové vyhodnocení všech projektů, a tedy musí důsledně dodržovat dané termíny hodnocení.(4) **loajálnost**, podle které musí každý porotce vystupovat na veřejnosti tak, aby svým chováním a postojem zvyšoval kredit soutěže a společnosti CACIO, (5) **týmovost**, kdy každý dodržuje schválená pravidla a akceptuje hodnocení ostatních porotců. (6) **zachování mlčenlivosti**, kdy každý porotce zachovává mlčenlivost o výsledku hodnocení až do vyhlášení výsledků soutěže a v neposlední řadě, (7) **profesionalita**, kdy každý porotce svým hodnocením potvrzuje svoji erudici a znalosti v oblasti ICT.

Jak ovlivnil COVID soutěž a IT projekt roku?

I přes pandemické období se 18. ročník soutěže zařadil mezi velice úspěšné ročníky soutěže a hodnotící komise musela vybrat vítěze z dvaceti dvou velice kvalitních projektů. Za zmínku stojí, že celý ročník prvně proběhl elektronicky, a proto bych rád poděkoval všem soutěžícím i členům komise, že to perfektně zvládli.

Co Vám osobně dala za ty roky soutěž IT projekt roku?

Já nebudu mluvit o tom, co mi dala soutěž po odborné stránce, ale o tom, co mi dala po stránce lidské. Především je to úžasné pracovat dlouhodobě s lidmi, myslím tím porotce, kteří jsou otevření, spolehliví, přátelští a současně i spravedlivě kritičtí. Z prezentacích finalistů na mě emotivně působilo, s jakým entusiasmem prezentovali svoje projekty a jak velmi často obětavě s maximálním nasazením na nich pracovali. Právě ten entusiasmus a obětavost lidí, kteří na projektech pracovali, a to jak tvůrců, tak uživatelů, často ovlivňuje mé hodnocení projektů.

Superpočítače aneb kde cloud ani distribuované výpočty nestačí

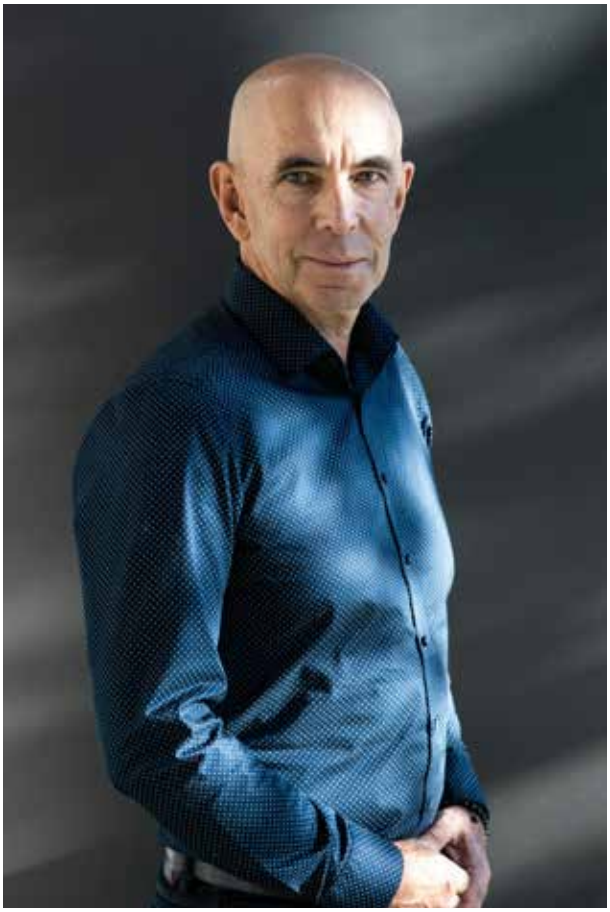
Zhruba před třemi dekádami začaly vznikat první velké projekty zabývající se distribuovanými výpočetními systémy. Poté na ně navázala architektura client server a s adopcí internetu přišel fenomén cloudu, který vytvořil obecné přesvědčení, že je univerzálním řešením pro všechny typy výpočetních zátěží. Záhy se ale ukázalo, že pokud potřebujete provádět složité modelování komplexních procesů, analýzu velkých dat v reálném čase, simulaci následků přírodních katastrof nebo funkčních programů pro umělou inteligenci, tak cloud nebo distribuované systémy nedosahují potřebného výkonu nebo propustnosti.

Zároveň náklady na vývoj High Performance Computing (HPC) systémů v poměru k relativně malým prodejním objemům byly obrovské, takže během posledních let došlo k dramatické konsolidaci dodavatelů v oblasti supercomputingu. Nicméně v týmu připravujícím globální strategie firmy Hewlett Packard Enterprise (HPE) panovalo jasné přesvědčení, že po počáteční euforii okolo cloudu dojde k vystřízlivění, a poté k výraznému nárůstu prodeje HPC systémů. A to se ukázalo jako pravdivé. Nárůst prodeje byl způsoben nástupem trendů jako je IoT, Big Data a AI a s nimi spojenou potřebou procesovat obrovské objemy vznikajících dat ve velmi krátkém čase. Dalším fenoménem je analýza dat vznikajících v rámci sociálních sítí, ať už motivována národními zájmy (bezpečnost státu, "velký bratr"), nebo analýzou dat a tvorbou AI procesů za účelem monetizace cílené reklamy. Prvním krokem v realizaci naší globální strategie byla akvizice firmy SGI v roce 2016, následované akvizicí firmy Cray v roce 2019. Obě akvizice nám umožnily nejen získat špičkové technologie a zvýšit "economy of scale" díky nárůstu zákazníků, ale také rozšířit náš expertní tým o špičkové pracovníky obou firem. Po konsolidaci HPC technologií firem HPE, SGI a Cray vzniklo nové HPC portfolio, které nám umožnilo stát se největším dodavatelem těchto technologií v globálním měřítku.

Současné trendy v oblasti HPC se točí okolo potřeby flexibility do dnešní doby velmi specializovaných superpočítačů, tak aby je v budoucnu bylo možné využívat ve všech třech typických výpočetních zátěžích:

1. Tradiční využití na modelování a simulaci výrobních nebo přírodních procesů (robotizace, vývoj nových léků…)
2. Analýza velkých dat (autonomní řízení, letecká doprava, výrobní procesy…)
3. Podpora pro rozvoj umělé inteligence (AI) včetně jejích podskupin jako je Deep Learning (DI) nebo Machine Learning (ML) a jejich využití v celém spektru aplikací přes různá odvětví včetně státní správy.

To vyžaduje vyřešit řadu technologických výzev. Jedna z nich je efektivní chlazení, kdy HPE používá technologii Direct Liquid Cooling (DLC) umožňující dosáhnout hustoty přes 100 kW na 1 stojan. Další z nich je technologie speciálních datových úložišť umožňující super rychlé paralelní datové přenosy do jednotlivých procesorových jednotek. Klíčový je také škálovatelný management, který řídí efektivní paralelní zpracování jednotlivých úloh. A je tu ještě celá řada dalších technologických vychytávek, které nejsou běžně používané v klasických počítačových centrech. V rámci České republiky HPE získalo prvenství jak v dodávce největšího podnikového superpočítače pro výpočetní centrum Škoda Auto, tak i projekt dodávky národní superpočítačové infrastruktury pro Vysokou školu báňskou - Technickou universitu



Jan Kameníček, generální ředitel Hewlett Packard Enterprise Česká republika

Ostrava. Námi dodaný superpočítač Karolína je největší a nejmodernější superpočítač v rámci České republiky a svým výkonem se vejde do top 20 v Evropě a do první stovky celosvětově. A náš HPC tým pracuje na řadě nových zákaznických projektů nejen v České republice, ale v celém regionu střední a východní Evropy, takže se těším na nové technologicky unikátní zakázky i v roce 2022. High Performace Computing je zcela jistě budoucnost IT světa.

Jan Kameníček

Hewlett Packard Enterprise

Koncert s předáním cen vítězných projektů soutěže IT projekt roku

Pandemie zasáhla do života nás všech, do soutěže IT projekt roku se promítla změnou času i formy slavnostního předání ocenění. Z března se stalo září, místo společenského večera jsme zvolili koncert vážné hudby a udělali jsme dobře. Akce se realizovaly, atmosféra byla výborná, předávání důstojné a na atmosféru pandemie, která byla občas znát zpětně jenom v dobrém vzpomínáme.

Na základě těchto dobrých zkušeností jsme se rozhodli koncerty včlenit jako pravidelnou aktivitu spolku CACIO, jako poděkování účastníkům soutěže, porotcům a všem, kteří pomáhají s průběhem soutěže IT a chodem CACIO.

Z těchto setkání přinášíme pár fotografických vzpomínek.

Koncert s předáním cen vítězům 17.ročníku soutěže IT projekt roku

15.9 2020

Součástí programu bylo představení historie Lichtenštejnského paláce

Vyhlášení výsledků 17.ročníku soutěže IT projekt roku proběhlo důstojně

Pan Prof Spurný uvedl Kapralova Quartet, který zahrál:

- *Josef Suk - Meditace na chorál Sv. Václave*
- *Joseph Haydn - Smyčcový kvartet op.76 č. 2*
- *Antonín Dvořák - Smyčcový kvartet op.96 "Americký"*

Koncert s předáním cen vítězům 18.ročníku soutěže IT projekt roku

8.9 2021

Součástí programu bylo představení historie Michnova paláce

Pan Prof. Luboš Spurný uvedl Graffovo kvarteto, které nám zahraje tří komorní skladby:

- *Gideon Klein: Fantazie a Fuga pro smyčcové kvarteto (1942–1943)*
- *Antonín Dvořák: Smyčcový kvintet Es dur, op. 97*
- *Miloš Štědroň: Suita pro smyčcové kvarteto „Tajné touhy lovce“*

Vyhlášení výsledků 18.ročníku soutěže IT projekt roku proběhlo ve velice příjemné atmosféře

Zamyšlení nad pravidly pro tvorbu hesel

Přihlašování do různých informačních systémů málo co charakterizuje tolik, jako přihlašovací jméno a heslo, které všichni používáme každý den, v podstatě od našeho prvního seznámení s informačními technologiemi. Za tu dobu bylo po nás požadováno splnění nemalého množství požadavků na vlastnosti hesel, tyto požadavky se navíc v čase proměňovaly. Některé smysl dávají, jiné už méně – například vynucování použití speciálního znaku v 15znakovém náhodně generovaném hesle.

Proto bychom rádi v rámci tohoto textu nejčastější požadavky prošli a zkusili se zamyslet, zdali v současné době ještě dávají smysl, anebo se jedná o již překonané relikty dob dávno minulých.

Heslo musí mít minimálně x znaků

Tento požadavek byl platný v minulosti, a je platný i nyní. Pouze se mění konkrétní hodnota určující minimální délku hesla. Zatímco před 10-15 lety bylo plošně požadováno minimálně 8 znaků, nyní vyhláška o kybernetické bezpečnosti předepisuje minimálně 12/17 znaků (dle typů uživatele). Správně by sice systém neměl kontrolovat délku hesla, ale jeho entropii (náhodnost), běžný uživatel však mnohem lépe pochopí jednoduchý požadavek na délku než abstraktní požadavek na entropii.
Požadavek na minimální délku hesla by však nikdy neměl být absolutní, ale měl by zohledňovat další parametry, jako je citlivost systému (přímá úměra), požadovanou frekvenci změny hesla (nepřímá úměra), i existenci opatření omezujících zkoušení hesla.

Heslo nesmí obsahovat jméno, příjmení, jména dětí, partnerů, datum narození, nejčastější slova apod.

Ani s tímto požadavkem není možné nesouhlasit. Heslo by mělo být tak obtížně uhodnutelné, aby útočník byl nucen použít útok hrubou silou, který je možné detekovat. Použití výše uvedených textových řetězců jako části hesla jeho neuhodnutelnost bohužel nezvyšuje.

Heslo se musí skládat z jednoho velkého písmena, jednoho malého písmena, číslice a speciálního znaku

Toto je první požadavek, který prošel revizí, kterou však dosud ne všichni zaregistrovali. Původním cílem bylo zvýšit entropii hesla tím, že uživateli nebude umožněno zadat heslo, které se skládá pouze z malých písmen. Bohužel praxe ukázala, že většina uživatelů tento požadavek splnila tím, že použila první velké písmeno, a nakonec hesla doplnila číslo doplněné tečkou nebo jiným podobným znakem. Tím se paradoxně složitost hádání snížila, neboť útočník víceméně věděl, že z 8znakového hesla je první znak velké písmeno, prostředních 5 znaků malá písmena, následuje číslo a speciální znak.
Na toto reagoval v roce 2016 NIST, který ve svém standardu NIST 800-63 B zrušil požadavek na složení hesla, i vyhláška o kybernetické bezpečnosti, která požaduje umožnit použití malých a velkých písmen, číslic a speciálních znaků, nikoliv však vyžadovat jejich použití.

Heslo je nutné měnit po 3 měsících

Stejně jako požadavek na složení hesla prošel i tento požadavek revizí vynucenou střetem s přístupem uživatelů. Uživatelé zvolili heslo s číslem na konci, které postupně zvyšovali, případně heslo zcela změnili, ale pak si ho poznamenali někam na dobře viditelné místo, protože díky častým změnám nebylo možné si heslo pamatovat.
Výše zmíněný standard NIST 800-63 B na tuto skutečnost opět reagoval požadavkem neomezovat dobu platnosti hesla bez jasného důvodu (jako je například podezření na jeho zneužití). Vyhláška o kybernetické bezpečnosti tak daleko zatím nejde, ale omezuje platnost hesla na poměrně pohodlných 18 měsíců, což je už dostatečná doba na to, aby si heslo uživatel zapamatoval.

Jedno heslo nesmí být použito ve více IS

Tento požadavek byl platný v minulosti, a je platný i nyní. Vždy je nutné předpokládat, že služba bude napadena a databáze hesel bude odcizena (což se už v minulosti stalo i větším službám jako LinkedIn). V závislosti na kvalitě způsobu ukládání hesla, kterou bohužel většinou neznáme, může potom útočník získat jak naše přihlašovací jméno (většinou email), tak i heslo, a pro útočníka není nic jednoduššího, než tuto kombinaci vyzkoušet i v jiných službách.

Všechna hesla jsou nebezpečná a musí být nahrazena 2FA

Jako většina absolutních tvrzení, je i toto tvrzení nesprávné. Heslo je nejlevnější, nejrozšířenější a nejvíce akceptovaný způsob autentizace. Proto je možné předpokládat, že pro nekritické systémy či služby bude (kvalitní) heslo používáno i nadále, neboť negativa 2FA (dvoufaktorové autentizace) převáží její přínos, tedy zvýšenou úroveň bezpečnosti.
Je tedy nutné odlišovat systémy, kde je 2FA nutností – bankovní systémy, národní identita, přístup do společnosti přes VPN, nebo i hlavní e-mailový účet, a systémy, kde opravdu není potřeba – veřejná fóra diskutující, z pohledu uživatele, ne citlivá témata (zahrádkářství, stavebnice, atd.), e-shop, ze kterého objednávám na dobírku.

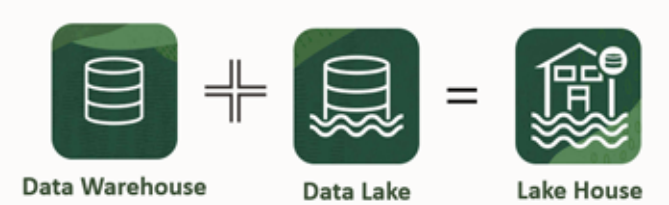
Jak jsme si výše ukázali, ne všechny požadavky na hesla dávají v současné době smysl a je nutné je stanovovat v kontextu prostředí, kde jsou hesla použita. Toho by si měli být vědomi zejména tvůrci a správci aplikací, neboť přílišné požadavky kladené na běžné uživatele mohou vést, jak jsme výše ukázali, ke snížení bezpečnosti nebo k falešnému pocitu bezpečnosti.

Data Lake House - řešení pro práci s daty a informacemi pro agilní firmu

V tomto článku představíme koncepty „Data Mesh“ a „Data Lake House“ – popisující principy řízení a návrhu architektury pro práci s daty a informacemi v moderních organizacích řízených agilním způsobem.

Úvod

Termín „Data Lake House“ vznikl v angličtině jako kombinace dvou jiných termínů: „Data Warehouse“ (česky se používá pojem datový sklad) a „Data Lake“. Oba dva koncepty pro správu, uložení a analýzu dat již nějakou dobu existují a řešení na jejich principech jsou implementována v mnoha organizacích. Oba dva tyto koncepty mají jedno společné: v obou případech se jedná o centralizovaná řešení, která mají na jedné straně zdrojové systémy a různé způsoby získávání dat z těchto systémů a a straně druhé jsou nejrůznější výstupy (od statických reportů po pískoviště pro datové vědce). Uprostřed je (většinou velmi velké) datové úložiště – ať již se jedná o relační databázi nebo např. o objektové úložiště na principu Hadoop clusteru.
Ve všech případech narážíme na organizační a technologická omezení těchto řešení.



Koncept Data Mesh

Koncept Data Mesh představuje způsob, jak přistoupit k řízení správy dat a informací distribuovaným způsobem a odstranit tak organizační omezení a limity monolitických architektur. Tento koncept jako první představil Martin Fowler ve svém článku „How to Move Beyond a Monolithic Data Lake to a Distributed Data Mesh“.
Koncept vychází z principů návrhu mikroslužeb a hovoříme o tzv. „Domain Driven Design“ (DDD). V zásadě se jedná o rozdělení obrovské monolitické architektury na jednotlivé domény. Doména je definovaná jako oblast IT architektury, která řeší konkrétní business úlohu. Doména v sobě obsahuje všechna pravidla a procesy nutné pro zpracování příslušné úlohy. Jsou jasně definované vstupy a výstupy do/z takovéto domény. Doména je maximálně autonomní a žádná jiná závislost na okolním světě (kromě definovaných vstupů a výstupů) neexistuje.

Koncept Data Lake House

Jak z konceptu Data Mesh a z principů DDD vyplývá, každá doména je co nejvíce soběstačná a tato soběstačnost je i na úrovni IT infrastruktury. Tj, v každé doméně může být trochu jiné řešení, které bude naplňovat požadavky na příslušnou doménu. Typicky například, pokud bude vyžadováno dávkové zpracování, bude k dispozici příslušný ETL nástroj, pokud bude vyžadováno zpracování toku událostí (např. IoT), bude k dispozici příslušná streaming platforma.
V zásadě se datová platforma dělí na tři části:

- Společná infrastruktura pro celou platformu
- Produktová vrstva
- Vrstva řízení.

IT architektura, která umožňuje nasazení maximálního možného množství jednotlivých elementů informační architektury se nazývá Data Lake House. V Data Lake House mohou vedle sebe existovat dávkové i real time zpracování dat, může tam být úložiště relační databáze vedle objektového úložiště. Klíčová je společná infrastruktura a společná vrstva řízení. Data Lake House se tak spojuje výhody Data Lake (které spočívají v rychlém a levném uložení velkého množství dat) se strukturovaným přístupem relačních databází.
Celý logický Data Mesh koncept bude v příslušné organizaci realizován několika navzájem propojenými Data Lake House, přičemž v každé doméně bude Lake House implementován/konfigurován podle potřeby příslušné domény.

Jakub Illner, Viktor Němec

ORACLE

Cyklus setkání „Praktické aspekty řízení informatiky“

Organizace odborných seminářů a konferencí je hlavním cílem aktivit asociace CACIO. Snažíme se vytvořit odbornou komunitu, ve které se zaměřujeme na aktuální témata a inspirující příklady a v následných diskusích hledáme inspiraci a podklady pro náš odborný přehled.

Seminář na téma: „IT opatření v době korony, aneb která opatření se nám povedla a kterých se příště raději vyhneme“ ONLINE

3. 11. 2020

Zaměřili jsme se na aktuální téma, jak se vyrovnat a efektivně podporovat problematiku vzdálené práce. Hlavní témata byla:

- Práce z domova okem právníka
- V čem nás poučila situace kolem COVID-19.

Seminář na téma: „Ohlédnutí za Gartner IT Symposiem 2020“ ONLINE

25. 11. 2020

Nastává éra modulárního, komponovaného byznysu. Přizpůsobivý, odolnější obchodní model, postavený modulárně na principech komponovaného byznysu je podle analytiků tím, na co by se podniky měly systematicky zaměřit. Seminář byl rozdělen do následných bloků:

- CIO agenda (výběr)
- Top tech trendy (výběr)
- Top předpovědi (výběr)
- Composable business (úvod / výběr).

Seminář na téma: „BYOD: problematika licencí a GDPR také s ohledem na home office“ ONLINE

9. 12. 2020

Nosné téma se z jiného pohledu vrátilo k tematice dopadů pandemie, konkrétně:

- Licence na vlastních zařízeních zaměstnanců, také při Home Office
- Kdo má jaká práva k softwaru; proprietární a Copyleftové licence aneb jak je to s využitím open source softwaru
- BYOD & Ochrana osobních údajů & Home office
- Identifikace rizik na poli ochrany osobních údajů při výkonu práce na vlastních zařízeních zaměstnanců – zejm. při práci z domova - a možnosti jejich mitigace
- NÚKIB: pohled na kyberbezpečnost při Home Office, zejména s ohledem na otázky kolem elektronické pošty ve státní správě; jak s BYOD?

Seminář na téma: „Kybernetická bezpečnost 2021“ ONLINE

11. 3. 2021

Online provoz s sebou přináší i nové požadavky na kybernetickou bezpečnost, která zatím často nebyla řešena s vážností, jež jí přísluší a dokud se nic nestalo, tak jsme naráželi na neochotu kybernetickou bezpečnost řešit a financovat. Proto jsme vybrali zajímavé případové studie a významné projekty v oblasti kybernetické bezpečnosti:

- Aktuální trendy a vize v oblasti kybernetické ochrany
- Případová studie – řešení incidentu ransomware / Phobos C
- Případová studie – SolarWinds – co se stalo? A jak tomu předejít?
- Zvýšení bezpečnosti a efektivity v Psych. nemocnici Opava – inspirace úspěšným projektem
- IT Security Solution Tech Data s využitím Palo Alto Networks a dalších vendorů
- Význam implementace SIEM v prostředí IT systémů nemocnic
- Computer Emergency Response Team v Izraeli – a jak je to u nás?
- Jak aktivně zvýšit v roce 2021 ve Vaší organizaci odolnost proti kybernetickým útokům.

Seminář na téma: „Agilní řízení v praxi“ ONLINE

27. 4. 2021

Seminář se zaměřil na představení zkušeností a diskusi použití agilních přístupů v praxi. V průběhu semináře byl představen přehled nejnovějších přístupů k agilnímu řízení. Následně jsme prezentovali zkušenosti dvou významných subjektů s používáním těchto přístupů. V prvním případě se jednalo o společnost Vodafone, v druhém o Ministerstvo průmyslu a obchodu. Mohli jsme tak porovnat přístupy v soukromé společnosti i v prostředí veřejné správy. Na závěr semináře proběhla velmi zajímavá panelová diskuse s vystupujícími.

Seminář na téma: „Otázky Home Office z psychologického a neurologického pohledu“ ONLINE

8. 6. 2021

COVID změnil svět, změnil naše okolí a změnil nás. Jedna velká změna, kterou vidíme okolo nás, je plošné rozšíření možnosti práce z domova. Ponechali jsme stranou technické možnosti a podívali se na psychologické dopady takovéto práce.
Přenášky se velice povedly, ještě lepší byla společná diskuse, kde se probíralo co dělat, abychom se z toho nezbláznili.


Seminář na téma „Open source“ HYBRIDNÍ FORMA

20. 7. 2021

Při rozvoji informatiky jsme často postaveni před dilema, kdy zvolit standardní robustní řešení a kdy hledat alternativu, ať již z důvodů nákladů, rychlosti řešení či jiného. Z tohoto důvodu jsme jako téma semináře opět zvolili problematiku open source, kde jsme na konkrétních projektech diskutovali otázku proč jsme si zvolili open sorce a zda to byla správná volba.



FÓRUM na téma „Informatika v době průšvihové“ HYBRIDNÍ FORMA

21. 9. 2021

Svět okolo nás se mění, na informatiku je kladen velký tlak z pohledu rozsahu služeb, bezpečnosti i adaptace nových technologií. Zároveň zažíváme dobu, ve které se střídají klimatické anomálie, dopady pandemie, či jiné průšvihy. Diskutovali jsme spolu jak budovat moderní IT, jak využít jejich potenciál a zajistit jeho maximálně efektivní provoz. Hlavní diskusní příspěvky byly:

- Pandemie COVID-19 – zkušenosti s vývojem a provozem nástrojů chytré karantény
- Jak se vyrovnat s kybernetickým útokem
- Datové centrum pod přímým zásahem tornáda v Čechách
- Co vše se vyskytuje v temné části webu.



FÓRUM na téma „ Jak efektivně řídit IT“ ONLINE

25. 11. 2021

Nastala éra digitální revoluce, ve které se radikálně mění technologické možnosti, obchodní podmínky, a hlavně chování populace okolo nás. Jak reagovat na takovéto změny, či jak přežít? Tyto otázky si celá řada z nás klade a hledá odpovědi. Bohužel, ale neexistuje univerzální rada, jak správně řídit informatiku, neboť každá organizace, tým či obchodní příležitosti jsou jiné. Existuje řada metodických pravidel a doporučení, nicméně nejvíce se vždy naučíme příkladem druhých. Proto jsme zvolili velice inspirující témata:

- Ohlédnutí za Barcelonou – konference Gartner Barcelona 11/2021
- Zásadní Hlavní trendy na trhu práce v datech
- Implementace Digital Integration HUB s cílem digitalizovat firemní procesy, produkty a prodejní kanály bez změny „legacy“ systémů
- Elektronická neschopenka – eNeschopenka
- Digitální transformace PRE na časové ose, aneb kam jsme došli po 3 letech
- Transformace IT v postcovidové - digitální době.


Dobré heslo

Vzdělávejme své uživatele, protože pracují a používají přístupová hesla i do našich systémů, vysvětlujme jim, co je nebezpečné chování v prostředí internetu a čeho se mají vyvarovat. Přínos bude nejen pro nás, ale i pro ně.

Jak udělat dobré heslo, tady je dobrá rada drahá 😊.

Nechci se opakovat, ale klíčem k dobrému heslu je jeho délka. Co si budeme povídat, je to všechno o matematice a samozřejmě i o důvtipnosti útočníka. Hned udělám malou odbočku – víte jaká technika samoobslužné obnovy hesla je považována za nejhorší? Je to kontrolní otázka (tak často kdysi používaná u různých webmailů). Proč tomu tak je? Jednak, protože všichni používali svého času stejnou (první volba zpravidla byla – jméno matky za svobodna), jednak je uživatelé sami zapomínali a jednak je útočníci dokázali poměrně snadno luštit.

Takže v první řadě by nemělo naše heslo nijak s námi spojeno, nemělo by to být uhodnutelné slovo, kterému případně dáme nápovědu na sociálních sítích. Když už jsem zmínil resetovací otázku, ono je to dost podobné i s hesly. Sice máme (nebo jsme jako bezpečáci měli) složité politiky hesel nutící uživatele k malému a velkému písmenu, číslici a divokému znaku, ale na druhou stranu si ta hesla uživatelé nepamatují. Pokud vygenerujeme nějaké složité náhodné heslo, je velmi pravděpodobné, že uživatel si ho nezapamatuje (což znamená, že si ho někde bude zapisovat) a na druhou stranu (pokud není heslo dostatečně dlouhé) dokážou je stroje celkem rychle luštit. Mimochodem, víte o tom, že zpravidla velké písmeno dáváme jako první znak hesla a číslici jako poslední – je to přirozenost vyplývající z toho, jak jsme se učili ve škole psát, a kyberzločinci to ví také.

Pokud uděláme pseudonáhodné heslo tvořené sekvencí znaků klávesnice jako jsou „qwert“ nebo „qazwsx“ určitě tím nástroje na lámání hesel neoklameme, a navíc to znamená, že jsme se za 75 let moc neposunuli. Stejnou chybu totiž dělali během 2. světové války němečtí šifranti při vytváření denních šifrovacích klíčů, což mj. přispělo k prolomení Enigmy.

Pojďme tedy k matematice a délce klíče – odhadovaná doba prolomení heslo „qscrgn“ 7 milisekund (podle https://howsecureismypassword.net/), heslo má 6 znaků, a to opravdu není v dnešní době pro počítače žádný oříšek. Zkusím tedy prodloužit délku na 12 znaků a neudělám to nijak chytře, prostě jen zopakuji sekvenci na „qscrgnqscrgn“. Dostáváme výsledek 3 týdny, to už sice útočníkovi trochu otráví život, ale pokud o to bude stát, tak ty tři týdny vydrží počkat. Zkusíme to tedy ještě protáhnout na 18 znaků a dáme „qscrgnqscrgnqscrgn“. Výsledek je 23 miliónů let! Když půjdeme po časové ose zpět, tak před 23 milióny let teprve začínala na Zemi éra savců. Samozřejmě testovací program pracuje s výkonem jednoho běžného PC, takže při zapojení více a silnějších strojů se dostáváme na řádově nižší čísla, nicméně pokud budeme u hesla uvažovat o 15 znacích, věřte tomu, že bude ještě dlouhou dobu (nevím, jak daleko jsou s kvantovými počítači 😊) bezpečné.

A jak dosáhnou dlouhého hesla a přitom zapamatovatelného?

Použijte frázi, větu… Fráze, věta, která má nějaký smysl se dá snáze zapamatovat, a přitom naplní všechny požadavky na bezpečnost. Mimochodem, původně, kdysi se v „dřevních“ dobách počítačů používalo výraz „Passphrase“ a nikoliv „Password“.

Nespoléhejte na to, že se Vaši uživatelé dokážou vždy sami ubránit, chystejte je na to, trénujte je na to. Bohužel se dá čekat, že ten útok jednou přijde.

Pokud nevíte, kde je největší nebezpečí, co byste měli udělat hned a co počká, jaký bezpečnostní systém je vhodný pro vás s ohledem na váš business a velikost, klidně se obraťte na AUTOCONT. Rádi Vám poradíme a jak se říká za zeptání, nic nedáte 😊 AUTOCONT ví jak.

AUTOCONT

Upozornění: Tento článek používá cookies, ale žádné neukládá…

V září 2021 byla schválena novela zákona o elektronických komunikacích, která s platností od 1. ledna 2022 přináší novou povinnost pro provozovatele webů ukládat cookies pouze s aktivním souhlasem návštěvníků. Vlastně to celé začalo nenápadně už mnohem dříve. Tu a tam se na nějakém webu objevilo upozornění na práci s cookies. Ale v poslední době přes tyto lišty už ani skoro není vidět samotná webová stránka.

Za vším stojí poměrně stará směrnice EU 2002/58/ES, článek 5, bod 3 z 12. července 2002. Tato směrnice byla později novelizována pomocí další směrnice 2009/136/ES. Je úkolem členských států tyto pokyny implementovat do národní legislativy. Poslední aktualizace v českém právu nabývá účinnosti právě od 1. 1. 2022.
Technická podstata cookies je vlastně banální a na první pohled nepředstavuje žádné riziko. Jednoduše server nabízející příslušnou webovou stránku si do vašeho zařízení uloží malé množství dat, a to je při příští návštěvě odesláno zpět serveru. Je to myšlenka z 90. let od firmy Netscape, autora jednoho z prvních prohlížečů. Cookies se běžně využívala k rozlišování jednotlivých uživatelů, resp. jejich preferencí a předvoleb.
Celkem praktický mechanismus začal být využíván k cílení reklamy, ve spojení se sociálními sítěmi a giganty jako Google nebo Facebook a za pomoci bezbřehé exhibice některých uživatelů lze pomocí cookies dnes často identifikovat konkrétní osoby. Administrativa Evropské unie pak vytáhla do boje za ochranu uživatele právě v podobě nařízení a směrnic a sankcí za jejich porušování. Bohulibý úmysl – transparentnost a ochrana uživatele – se však v praktické implementaci stává, nikoli poprvé, trochu absurdním divadlem. Vzpomeňme například na opatření přikazující dodavateli operačního systému dát možnost svobodně vybrat internetový prohlížeč. A nyní nám webové stránky zase zaplňují nejrůznější ovládací lišty pro nastavení cookies. Na druhou stranu si dnes už můžete nainstalovat rozšíření prohlížeče, které za vás lišty ovládá, aniž by Vás s tím obtěžovalo. Kde je pak vědomý souhlas uživatele?
Otevřel se i další trh, několik firem se pustilo do nového businessu a prodávají nebo ještě lépe pronajímají provozovatelům webů nástroje na řízení cookies, aby poskytovatelům obsahu zajistili soulad s legislativou.
Pikantérií je pak už jen rozhodnutí soudu v německém Wiesbadenu z 1. 12. 2021, který reaguje na skutečnost, že nástroje – pluginy pro outsourcing řešení cookies, které jsou provozovány nebo využívají služeb společností se sídlem mimo EU (typicky v USA), jsou de facto v rozporu s legislativou, protože nelze garantovat, že data o uživatelích neopustí EU.
Obecně je samozřejmě velmi těžké hledat rovnováhu mezi svobodou a regulací. Ačkoli v naší kultuře stavíme právě svobodu mezi nejvyšší hodnoty, nezřídka v dobré víře vytváříme složitou spleť pravidel, norem, pokut, dotací a dalších opatření a protiopatření, které poškozují nejen svobodu podnikání a tím i kreativitu a pokrok, ale přirozenou opatrnost a pozornost uživatelů. Přílišnou snahou úřadů o ochranu lidí je tak paradoxně děláme ještě zranitelnějšími.

Jak tedy na cookies?

Z pohledu provozovatele webu - jednou tu máme legislativu, která je prací volených zástupců, tak ji je třeba dodržovat. Postihy mohou být velmi přísné, a proto není radno nic podceňovat. Každý web musí dát uživateli jasně možnost vyjádřit vůli, zda a jaké sledovací kódy lze používat. Uživatel musí mít právo kdykoli své rozhodnutí změnit. Pokud se nám jeho rozhodnutí nelíbí, nesmíme mu zablokovat přístup k webu a všechno je třeba udělat v rámci EU, aby neunikla ani data o preferencích nastavení ukládání dat.
Z pohledu uživatele - je to asi jednodušší, musíme si uvědomit, co děláme a že digitální svět má nekonečnou paměť. Už jsme přijali fakt, že telefonní hovor včetně obsahu reálně není až tak soukromá věc, jak by se mohlo zdát. Stejně tak každé „kliknutí“ na internetu je uloženo a zpracováno. Ostatně, i kdyby nebylo cookies, naše zařízení si při komunikaci se serverem vyměňuje spoustu technických informací počínaje IP adresou, rozlišením, typem prohlížeče nebo operačního systému atp. Celkem přesně je možné identifikovat uživatele pomocí dané kombinace technických parametrů bez využití cookies. I ti, kteří na mobilu pečlivě odebírají aplikacím oprávnění (a kolik nás takových skutečně je?) nejsou zcela neviditelní. Jsou aplikace, které například zjišťují, jaká zařízení stejných technických parametrů mají v daný čas stejně nabitou baterii, a tak identifikují, že se s největší pravděpodobností jedná o téhož uživatele, kterého se pak dál snaží identifikovat nebo alespoň profilovat. Protože mj. právo zjistit stav nabití baterie v procentech až na 5 desetinných míst nebo přesný čas je aplikacím běžně přístupný.

A co to vše přinese?

Už jsem se setkal s názory, že nejrůznější regulace a represe transparentnost nepřinesou a že celá řada firem stejně už má nejrůznější data o uživatelích. Například antivirový program Vám proskenuje kompletně celý počítač s tím, že hledá viry, ale vzpomeňme na aféru dceřiné firmy Avastu, která obchodovala s daty zákazníků. Jsou však i tací, kteří naopak tvrdí, že by srovnalo příležitosti a zvýšilo transparentnost, pokud by existovala možnost volného přístupu řekněme burzy takových údajů. Těžko říct, zda se něčeho takového dočkáme. Pokrok nelze zastavit a snaha potlačit využívání cookies nahrává vlastně jen starým tištěným novinám nebo rádiím, která nemohou svoji reklamu tak snadno cílit. Výsledkem může být i oslabení financování online médií, a naopak další posílení mnohdy institucionálně sponzorovaných dezinformačních webů.

Závěrem

Provozování i těch nejjednodušších IT služeb jako třeba www stránky (pro akciové společnosti dnes povinné), ačkoli technicky jednoduché, může být netriviální, pokud se mají splnit všechny legislativní požadavky. I na oblast IT začaly doléhat mnohé regulatorní povinnosti. A tak lidem odpovědným za IT nezbývá nic jiného než krom technologických a bezpečnostních novinek bedlivě sledovat i legislativní povinnosti a implementovat všechny směrnice do spravovaných systémů.

Internet (opět) v plamenech

Kvůli kritické zranitelnosti téměř všudypřítomné logovací knihovny přinesl předvánoční čas snad všechno, jen ne předvánoční klid.

Knihovna Log4j, kterou používá drtivá většina významných softwarových produktů a řešení postavených na programovacím jazyku Java, se ukázala být časovanou bombou pro všechny firmy, které takový software používají. Důvodem je zranitelnost typu „Remote Code Execution“ (vzdálené spuštění kódu), která byla vyhodnocena jako kritická a nese si na škále 0 – 10 hodnotu 10, tedy nejvyšší. Hodnocení 10 znamená, že útočník pomocí jednoduchého útoku bez jakékoliv interakce s uživatelem plně kompromituje nejen zranitelný cíl, ale i související prostředky.

Útok je jednoduché provést, ale pochopení samotné zranitelnosti a hlavně jejích dopadů je však mnohem náročnější. Problém totiž leží v knihovně, která pracuje s logy aplikace. To znamená, že žádná naše aplikace, kterou provozujeme v internetu, nemusí být přímo zranitelná, ale útočníci mohou přesto kompromitovat naše interní prostředí. Jak je to možné? Představme si scénář, kdy každý přístup uživatele na naše internetové stránky je zalogován – toto je běžné nastavení a každý, kdo provozuje nějaký web, tyto logy má. Dále si představme, že tyto logy jsou dále zpracovávány nějakou monitorovací technologií, např. nám logy jdou do centrálního systému (např. SIEM). Tato technologie je naprogramována v jazyce Java a pro práci s logy používá inkriminovanou knihovnu Log4j. Dále, náš SIEM (nebo cokoliv jiného) je umístěn v důvěryhodné zóně naší interní sítě – těžko někdo vystaví SIEM do internetu. Avšak díky tomu, že je zranitelná knihovna právě v našem SIEMu, do kterého doputuje log z externí webové aplikace, zranitelnost se projeví až na SIEMu v interní síti. V ten okamžik dochází ke kompromitaci SIEMu, což je zdroj v důvěryhodné zóně, odkud může útočník dále a zřejmě poměrně snadno útočit na další cíle, například doménový řadič. A právě zde je záludnost celého problému, protože tradiční pojetí bezpečnosti, kdy si firmy extrémně hlídají svůj externí perimetr a interní síť považují za důvěryhodnou a bezpečnou, zde kompletně padá. Externí perimetr se začíná silně rozplývat, protože tato zranitelnost může být zneužita například přes výše uvedený scénář, ale i jinými způsoby - třeba prostřednictvím automatizovaného zpracování e-mailů či SMS.

Jaké mohou být dopady?

Vzhledem ke kritičnosti zranitelnosti i fatální. Nejenže útočník může snadno překonat náš velmi střežený a draze budovaný perimetr, ale hlavně získá kontrolu nad velmi cennými zdroji v našem interním prostředí. Díky tomu může získat citlivé informace, jako jsou například logy, nebo může převzít kontrolu nad serverem v interní síti a pokračovat v dalších útocích. Běžnou praxí je, že internímu prostředí plně důvěřujeme. Důsledkem je, že klademe velmi malé překážky útočníkovi, který již v interním prostředí je. Výsledkem pak může být poměrná rychlá kompromitace celého interního prostředí kvůli převzetí kontroly nad doménovým řadičem a tím pádem všech zdrojů napojených na interní doménu. V takový okamžik si můžeme být téměř jisti, že naše sensitivní data poplují k útočníkovi, aby je prodal na dark webu, a současně horkotěžko obnovujeme naše prostředí z útoku ransomware. Jiný a možná ještě horší scénář je takový, že naše prostředí bylo kompromitováno v první vlně oportunistických útoků. Útočník, který takto získal přístup do našeho prostředí, pak tento přístup prodá na dark webu. Kupci mohou být jak skupiny živící se ransomware, tak ale i skupiny útočníků, které mají mnohem nebezpečnější agendu. Jako příklad můžeme uvést útoky Black Energy a NotPetya, které několikrát vyřadily ukrajinskou přenosovou soustavu, útok na Demokratickou stranu při kandidatuře Hillary Clintonové na americkou prezidentku, či SolarWinds, kdy útočníci kompromitovali obrovské množství významných firem i státních úřadů po celém světě.

Jak se bránit této zákeřné zranitelnosti?

Bohužel neexistuje žádné jednoduché řešení. I když tvrzení: „aktualizujte knihovnu Log4j na poslední verzi“ tak může znít, ruku na srdce, kdo ví, kde všude tuto knihovnu máme? Účinné řešení je tak ještě komplikovanější než pochopení samotného nebezpečí

Pokud se vaše organizace dosud tímto problémem nezabývala a přesto víte, že tuto všudypřítomnou Java knihovnu budete ve svém prostředí mít zřejmě také, musíte nad rámec úvah o tom, jak zranitelnost co nejrychleji vyřešit, přidat i úvahy o tom, jak zjistit, jestli vaše firma nebyla již kompromitována. A to je ještě o řád složitější cvičení než to, které jsem popsal výše.

Základní doporučení je začít od zjištění, jestli je vaše firma zranitelná (i přesto, že víte, že knihovnu máte). Na to je nejlepší provést penetrační test. Pokud vám vyjde dobře, tedy že zranitelní nejste, můžete v klidu hledat knihovnu a postupně patchovat. Proč neskončit tím, že nejste zranitelní, tak patchovat nepotřebujete? Protože penetrační test nikdy 100 % negarantuje, že našel všechny zranitelnosti. Současně, výsledky penetračního testu jsou platné k daným podmínkám a času. Tudíž, můžete v krátké době spustit nový systém, který podmínky změní, a můžete se stát zranitelnými. V případě, kdy vám penetrační test řekne, že zranitelní jste, je nutné si připustit, že jste opravdu byli kompromitovaní. Pak je potřeba si říci, za jakých podmínek je možné zranitelnost zneužít, posoudit, zda-li jsou to podmínky reálné a podle toho navrhnout další postup. Ten by měl být takový, že hledáte projevy kompromitace. Základním předpokladem je existence logů a schopnost je vyhodnocovat. Tím, že ke kompromitaci dochází pomocí spuštění Java kódu přímo v paměti, je úloha najít kompromitovaný stroj opět velmi složitá. Je tedy nutné hledat spíše průvodní jevy kompromitace, jako jsou excesivní datové toky na nezvyklá místa v internetu, neobvyklá datová spojení, komunikace se sítí TOR, či neobvyklé vytížení zdrojů. Samozřejmě lze hledat i „obvyklé podezřelé“, jako je přítomnost CobaltStrike klienta či pofidérní příkazy PowerShellu.

Co říci závěrem?

Snad jen to, co je patrné z celého textu – tuto situaci nelze brát na lehkou váhu. Dá se totiž předpokládat, že bez příslušných opatření může být každá významná firma či organizace prostřednictvím této zranitelnosti za nějakých podmínek napadena.

Top strategické technologické trendy Gartneru pro rok 2022

Z průzkumů Gartneru mezi CEO organizací jasně vyplynuly tři klíčové priority pro rok 2022: růst, digitalizace a efektivita. CIO mohou tyto priority podpořit pomocí technologií se silovým multiplikačním potenciálem napomáhajícím růstu a technologiemi podporujícími potřebné digitální změny – to vše by mělo vycházet ze stabilních a odolných technologických základů, které umožňují podniku efektivní rozvoj a růst bez neustávajících dodatečných investic.

Analytici Gartneru proto sestavili přehled nejdůležitějších strategických technologických trendů tak, aby tyto priority odrážel – podobně jako v předchozích letech uspořádali klíčové technologické trendy do tří skupin:

- **Budování důvěry** kombinuje trendy, jež umožňují postavit odolné a efektivní IT základy.
- **Formování změn**: Podstatou digitalizace je proměnit podnik tak, aby vytvářel více přidané hodnoty s pomocí technologií, jinými slovy hledat nové tvůrčí způsoby jejich využití.
- **Akcelerace růstu** pochopitelně staví na efektivních IT základech a tvůrčím komponovaném přístupu, díky nimž je možné vymýšlet nové způsoby tvorby přidané hodnoty (či vylepšovat ty existující) v existujícím či nových obchodních ekosystémech.

Top strategické technologické trendy Gartneru pro rok 2022

Vybrané trendy popisujeme dále:

#7 Datová osnova (Data Fabric) představuje pružnou, odolnou integraci dat napříč platformami a byznys uživateli tak, aby byla data dostupná, kdekoliv je třeba. Má ale též vestavěné analytické funkce umožňující zjistit či vyhodnotit, jaká data jsou kde používána. Skutečná hodnota datové osnovy spočívá v její schopnosti doporučovat další, odlišná a kvalitnější data – odpadá tedy práce s hledáním či vytěžováním dat. Tím lze snížit pracnost v oblasti správy dat až o 70 % a výrazně rychleji dosahovat cíle.

#6 Kyberbezpečnostní síť či pletivo (Cybersecurity Mesh). Pro sdílení dat je pochopitelně důležitá důvěra – a ve chvíli, kdy se připojujete kamkoliv, mohou být kdekoliv také klíčová aktiva a uživatelé, tradiční bezpečnostní perimetr tak postupně pozbývá smyslu a data je třeba zabezpečit pomocí nové technologie kyberbezpečnostní sítě či pletiva (Cybersecurity Mesh). Jde o přístup spojující různé bezpečnostní služby tak, aby bylo možné rychle a spolehlivě ověřit identitu, kontext a soulad s pravidly. Jde vlastně o celopodnikový framework komponované důvěry poskytující distribuovanou bezpečnost bez ohledu na místo.

Datová osnova

#5 Výpočetně posílená ochrana soukromí (Privacy-Enhancing Computation). Integrace a zabezpečení statických dat dnes již nestačí. Tvorba přidané hodnoty je stále častěji vázána na zpracování dat – v cloudu, pro analytické účely nebo AI modelování. To mnohdy znamená nutnost sdílet je napříč partnerskými ekosystémy – pochopitelně způsobem, který dbá na ochranu soukromí jednotlivců. Výpočetně posílená ochrana soukromí nabízí nové příležitosti, jak zpeněžit informace napříč vaším ekosystémem při současné ochraně soukromí, jde přitom o klíčovou schopnost – analytici odhadují, že do roku 2025 ji nasadí 60 % organizací.

#4 Komponované aplikace (Composable Applications). Základním stavebním kamenem komponovaných aplikací jsou tzv. PBC (Packaged Business Capabilities, tedy balíčky byznys funkcí), jde o softwarově definované byznys objekty, které mohou reprezentovat například pacienta, digitální dvojče nebo úvěrový rating. PBC utvářejí znovu použitelné moduly, z nichž fúzní týmy mohou samy sestavovat či rychle vytvářet komponované aplikace integrované do datové osnovy (Data Fabric) a vybavené UI nadstavbou. Možná se vám vybavily SOA či mikroslužby, ale lépe je o PBC uvažovat jako o atomech a o komponovaných aplikacích coby molekulách vytvářených z nich fúzními týmy chemické sloučeniny.

Dalšími strategickými technologickými trendy pro rok 2022 (a další léta) jsou:

#3 Rozhodovací inteligence (Decision Intelligence): praktický návod, jak (složením PBC obsahujících byznys vhled, analytiku a inteligenci, a jejich integrací do datové osnovy) zlepšit rozhodování pomocí modelování rozhodovacího procesu.

#2 Distribuovaný podnik (Distributed Enterprise): firma či organizace s velkým počtem na dálku pracujících zaměstnanců. To ovlivní další rozvoj a růst byznysu (e-commerce, geolokační služby, hybridní zdravotní péče, využívání dronů, hybridní vzdělávání, eventy apod.).

#1 Totální zážitek (Total Experience): model, v němž jsou všechny aspekty zákaznického zážitku (a také zážitku zaměstnaneckého) vzájemně propojeny a řízeny – počínaje onboardingem přes podporu či doporučování dalších kroků až po retenci, a to jak v komerční, tak i veřejné sféře.

Lukáš Erben
KPC-Group, zastoupení Gartner pro ČR, SR a Rumunsko.

Pardubický kraj získal Cenu CNZ v rámci soutěže IT projekt roku

V 18. ročníku soutěže IT projekt roku CACIO vybírala hodnotící komise vítěze z dvaceti dvou přihlášených velice kvalitních projektů. V důsledku pandemických opatření byly výsledky vyhlášeny elektronickou formou. I tentokrát byla udělena cena CNZ za mimořádný přínos pro oblast digitální kontinuity, důvěryhodnosti a dlouhodobého ukládání digitálních dokumentů. Laureátem se stal Pardubický kraj za svůj projekt Digitalizace krajského úřadu, realizovaný společností GORDIC.

Projekt přinesl zefektivnění práce jednotlivých odborů s využitím digitalizace celé řady agend, elektronického podepisování a schvalování v aplikaci Elektronická podpisová kniha. Ta je využita i při schvalovacích procesech v ekonomických agendách s vazbou na finanční kontrolu. Schvalovací procesy i elektronická finanční kontrola jsou striktně definovány. Tím je zabezpečeno, že pracovníci nevynechají žádný z požadovaných kroků dle zákona nebo Interní směrnice a nelze provést úhradu bez schválení určenou osobou.

Pro veřejnost se kraj rozhodl poskytovat digitální služby prostřednictvím Portálu občana, který slouží ke sběru elektronických žádostí o dotace i pro úplná elektronická podání s využitím kvalifikovaných systémů elektronické identifikace. Od papírových dokumentů se zcela oprostila i agenda usnesení. Podklady jsou vytvářeny digitálně, elektronicky je zajištěna i jejich distribuce.

Projekt, jehož realizace započala ještě před nástupem pandemie COVID-19, tak přispěl k udržení funkčnosti úřadu i jím zajišťovaných služeb pro veřejnost. Portál občana Pardubického kraje se tak stal místem, kde bude kraj v budoucnu nabízet své digitální služby dle zákona č. 12/2020 Sb.

Patnáctá – a přitom první

V polovině října loňského roku proběhla již patnáctá konference CNZ, tentokrát pod názvem „Digitalizace není náhrada papíru elektronickým dokumentem“. Byť šlo již o patnáctou konferenci, kterou spolek pořádal, byla první, která se díky pandemickým omezením musela přesunout do virtuálního prostředí. Fakticky to tedy byla premiéra jak pro některé z přednášejících, tak žel i pro účastníky, zvyklé na osobní setkání v prostorách Národního archivu na Chodovci.

Změna prostředí však dle všeho atraktivnost konference nijak nesnížila. První blok, věnovaný dopadům povinností, uložených původcům zákonem č. 261/2021 Sb., sledovalo na Teams a YouTube kanálu CNZ přes pět set diváků. Obdobné to bylo i v dalších dnech, kdy se střídala témata reagující nejen na nové povinnosti uložené veřejné správě, ale i práva jejích klientů. Se značným zájmem se setkal blok, věnovaný elektronizaci agendy soudních znalců, zejména část věnovaná Elektronickému znaleckému podpisu a metodice jeho použití. Nechyběla ani tradiční diskuse, tentokrát zaměřená na cíle elektronizace výkonu agend veřejné správy a nejčastější chyby, spojené s tvorbou a vyřizováním digitálních dokumentů. Záznamy z jednotlivých dnů jsou na YouTube kanálu CNZ https://www.youtube.com/channel/UCFvoOCgTpqevVfw3L-CaZ8WQ stále přístupné a těší nás, že počty shlédnutí rostou. Zajímavé byly i odpovědi bezmála sedmdesáti účastníků, kteří následně vyplnili anketní formulář. Mírná většina (přesně 55,2 %) v něm mimo jiné uvedla, že On-Line formát jim vyhovuje více než klasická podoba konference. Nicméně pokud to situace dovolí, rádi se letos alespoň s některými účastníky sejdeme opět na tradičním místě. Osobní setkání spojené s výměnou zkušeností jsou totiž nenahraditelná.

Co po nás zbude

Doba datové komunikace a její bezpečnost „teorie versus praxe“

Očekává se, že v roce 2025 bude 80 % veškerých B2B obchodních interakcí mezi dodavateli a kupujícími uskutečněno pomocí digitálních kanálů. Pro zabezpečení dat byla vždy důležitou součástí i bezpečná komunikace.

Z historie lze uvést kódovací nástroj ENIGMA, který umožňoval 3.28 x 10^{114} počet kombinací, praxe byla ovšem jiná a ve skutečnosti se nevyužívaly všechny možnosti v nastavení, a tak v běžném provozu samotný počet kombinací poklesl na 1.07 x 10^{23}.

JaredOwen Animation

Kybernetická bezpečnost je obor, který přináší enormní počet nových informací a technologií pro vyšší zabezpečení společností. Jde o nikdy nekončící proces, který musí reagovat na nové vnější hrozby a zároveň splňovat nové legislativní požadavky na lokální i globální úrovni. Pracovníci bezpečnosti jsou vždy o krok pozadu oproti útočníkům a vyvíjejí maximální snahu tento náskok minimalizovat.

Společnosti jsou pod neustále rostoucím množstvím útoků. Důkazy o tom, že se jednalo o úspěšné útoky, jsme mohli zaznamenat u státních institucí, výrobních podniků nebo nemocnic, kde docházelo k částečnému i úplnému zastavení provozu.

Pokud se na kybernetický prostor podíváme z jiného úhlu pohledu, můžeme tento celek rozdělit na více oblastí jako jsou Technologické řešení, Řešení kybernetické bezpečnosti a Řešení na snížení rizika. Zákazníci využívající tuto perspektivu nalézají výrazně efektivnější řešení, které splňují jejich individuální potřeby a včas reagují na nová rizika.

Několik příkladů z praxe

Prvním je zákazník spadající pod Zákon o kybernetické bezpečnosti, a tudíž se silným důrazem na on-prem řešení. Má velmi silný technologický tým, využívá on prem SIEM (Systém pro správu bezpečnostních informací a událostí) řešení a buduje interní SOC tým. Je nucen provozovat několik aplikací v cloudu a řeší, jak nejefektivněji vyřešit bezpečnostní dohled i nad těmito aplikacemi.

Druhým příkladem je zákazník, který je zároveň velkým MSSP se silným týmem a know-how, ale vše provozuje na On-prem řešení. Nově přechází do O365 a potřebuje vyřešit bezpečnost a dohled nového cloudového prostředí.

Třetím příkladem je mezinárodní zákazník, poskytující obchodní služby po celém světě. Kybernetickou bezpečnost má kompletně zajištěnou externí společností (SOCaS). Má dlouhodobou zkušenost s vlastním provozem aplikací a infrastruktury v cloudu. Potřebuje vyhovět novým legislativním požadavkům v rámci EU (NIS 1.0 a NIS 2.0) a v případě kybernetického útoku prokázat co, kde a jak nastalo.

Řešení

Společným řešitelem bylo velice efektivní a rychlé SIEM řešení Microsoft Sentinel, které u prvních 2 příkladů běží v Hybridním módu.

Výsledkem třetího příkladu je provoz pouze jediného cloudového SIEMu, který si zákazník nově implementoval a svému externímu dodavateli SOC služby toto řešení poskytnul.

Lze tedy konstatovat, že vytvořené řešení je vhodné pro většinu typů zákazníků, jelikož umožňuje jednoduše a efektivně vybudovat i zcela nový dohledový a bezpečnostní systém.

Za implementaci Hybridního SIEM řešení pro T-Mobile Czech Republic & Slovak Telekom jsme obdrželi od společnosti Microsoft ocenění Projekt roku 2021 v kategorii „Secure Remote work“.

Závěr

Závěrem lze říct, že každá situace má řešení. Je však nezbytné opakovaně provádět revizi a zároveň používat nejnovější dostupné nástroje pro zvýšení zabezpečení celého prostředí. Nicméně stále platí pravidlo používat selský rozum, a hlavně se nepo…, jak říkával náš slavný hokejista a trenér Ivan Hlinka, neboli se nebát a řešit vše racionálně a profesionálně.

David Řepa
Crayon Czech Republic and Slovakia, s. r. o.

Systémy chytrého měření elektřiny nastupují. Jak fungují a co od nich očekáváme

Nové přístupy v oblasti řízení distribučních energetických sítí jsou z velké části založeny na automatizovaném sběru a zpracování velkého množství dat o spotřebě v reálném čase a na možnosti vzdáleného řízení spotřeby či výroby. Systémy inteligentního měření – tzv. smart metering umožňuji zavádět pokročilé postupy řízení soustavy se zapojením decentralizovaných obnovitelných zdrojů i regulace koncové spotřeby a jsou proto součástí plánů řešení klimatických změn prostřednictvím efektivního využívání energií.

Systémy AMM v Evropě a u nás

V rámci balíčku legislativních nařízení Evropské komise vydaného v roce 2016 pod názvem *Čistá energie* pro všechny Evropany je navrženo nové uspořádání evropského trhu s elektřinou, které počítá s uplatněním nových technologií a konceptů jako je akumulace, decentralizované obnovitelné zdroje a využívání flexibility spotřeby. Předpokládá se, že plošné zavedení systémů automatického měření a související infrastruktury neboli AMM (automated meter management) pomůže zákazníkům díky okamžitým informacím o spotřebě elektřiny optimalizovat náklady na elektřinu, umožní zavádění dynamických obchodních tarifů reagujících na aktuální cenu a umožní agregaci flexibility jako nového nástroje využitelného pro řízení energetické soustavy.

I když jsou systémy inteligentního měření dostupné na trhu již delší dobu, k jejich masivnímu rozšiřování dochází až v posledních několika letech. V západní Evropě jsou v současnosti dokončovány plošné rollouty nasazení AMM, a to i přes to, že se dosud zcela nenaplnily kalkulované přínosy v oblasti energetických úspor nebo snižování provozních nákladů. V průběhu posledních let se nicméně i díky těmto projektům podařilo vyřešit řadu výzev spjatých s AMM týkajících se spolehlivosti datových přenosů, kybernetické bezpečnosti nebo ochrany osobních údajů.

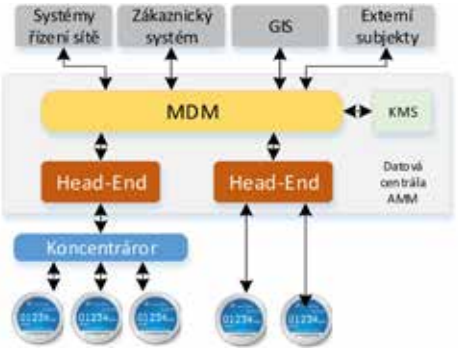
V České republice je rámec zavádění systémů inteligentního měření stanoven Národním akčním plánem pro chytré sítě. Dle schváleného harmonogramu se předpokládá zahájení roulloutu AMM od roku 2024, v polovině roku 2027 by měla být dokončena 1. etapa nasazení pro zákazníky s roční spotřebou nad 6 MWh.

Architektura AMM

Architektura AMM řešení obsahuje několik hlavních navzájem integrovaných komponent. Základní vrstvu zajišťují vlastní inteligentní měřiče, které komunikují s nadřazeným systémem buď přímo nebo prostřednictvím datových koncentrátorů. Pro komunikaci jsou využívány technologie přenosu pomocí mobilní sítě, pevného datového připojení nebo komunikace po elektrické síti.

Jádrem celého systému je datová centrála, která obsahuje následující základní komponenty

- Head End Systém (HES) zahrnující funkce, které umožňují komunikaci s měřidly
- Meter data management (MDM), který podporuje proces instalace a provozu inteligentních měřičů a slouží ke správě energetických dat
- Key management systém (KMS) – řešení pro správu digitálních certifikátů pro zajištění bezpečné komunikace s měřicími zařízeními.



Obrázek 1 Struktura AMM řešení

Datová centrála je integrována s řadou dalších systémů, a to jak v oblasti řízení distribuční sítě, tak podnikovými aplikacemi jako je zákaznický systém, GIS, systém řízení pracovních příkazů apod. Současně komunikuje s externími systémy v rámci trhu s energiemi pro zajištění předávání informací operátorovi trhu, dodavatelům a zákazníkům.

Jakkoli je hlavním úkolem systému AMM zajištění obousměrného přenosu informací mezi centrálním systémem a měřicími zařízeními, předpokládá se jeho využívání i pro další inovativní postupy a řešení, např. při detekci poruch a výpadků, automatizované údržbě topologie sítě, identifikaci technických a netechnických ztrát, monitorování zátěže sítě i její částečné řízení. Řešení rovněž umožní zefektivnit procesy instalace, výměny a odpojování, změny tarifů a případně přímo komunikovat se zákazníkem.

Řešení CGI Sm@rtering

Příkladem existujícího úspěšně komerčně nabízeného AMM systému je řešení společnosti CGI Sm@rtering. Jde o integrovanou platformu zahrnující funkce Head-end, Meter Data Management a modulu zajišťujícím dohledové funkce sítě. Společnost CGI do produktu Sm@rtering v poslední době významně investovala a vyvinula díky tomu moderní řešení, které disponuje řadou funkcionalit, jimiž se odlišuje od platforem dalších dodavatelů. Za zmínku stojí zejména funkce týkající se monitorování a správy distribuční sítě.

Klíčovou vlastností řešení Sm@rtering je jeho otevřenost a široké možnosti integrace - funguje nezávisle na použitých AMM technologiích a umožňuje tak integrovat zařízení různých výrobců.

Obrázek 2 Ukázka uživatelského rozhraní řešení CGI Sm@rtering

Řešení CGI Sm@rtering má již více než 10 letou historii a je využíváno energetickými společnostmi v EU (Portugalsko, Španělsko) a v Kanadě.

CGI

itSMF Czech Republic

itSMF Czech Republic
The IT Service Management Forum

itSMF Czech Republic je česká pobočka mezinárodně působící nezávislé a neziskové organizace itSMF (IT Service Management Forum), založené roku 1991 ve Velké Británii. Účelově se věnuje všem aspektům řízení služeb informačních a komunikačních technologií. Současně je také fórem uživatelů celosvětového standardu pro tuto oblast, kterým je ITIL (Information Technology Infrastructure Library).

Mezinárodně platná pravidla stanovují, že každá národní pobočka musí být zcela nezávislá na dodavatelích ICT i konzultačních společnostech, nesmí prosazovat jednostranné zájmy silných subjektů a musí v ní být zastoupeny všechny zájmové skupiny od dodavatelů a výrobců ICT, přes podnikatelskou sféru a státní správu až po poskytovatele konzultačních služeb a vědecké a výzkumné instituce.

Česká pobočka této organizace itSMF Czech Republic, z. s. existuje od 30. 3. 2006 jako právnická osoba založená dle zákona č. 83/1990 Sb. o sdružování občanů, od 1. 1. 2015 podle nového Občanského zákoníku jako zapsaný spolek.

Jejím úkolem je – jako u všech ostatních poboček ve světě – vytvořit komunikační platformu napříč celým odvětvím informatiky a tím umožnit členům sdílení znalostí a zkušeností z oblasti řízení ICT služeb.

Na základě zkušeností nabytých během více než patnáctiletého působení v České republice jsme rozšířili odborný záběr našeho fóra o další vědomostní rámce/frameworky a s nimi spojené osvědčené postupy/best practices. Zejména jde o DevOps, Agile a Project Management.

Tím umožňuje napomáhat dalšímu rozvoji a rozšiřování nejlepších osvědčených postupů, jakož i zvyšování profesionality odborníků v tomto oboru.

Spolek itSMF Czech Republic, z. s., naplňuje své poslání především:

- provozováním vlastního webového informačního portálu
- aktivní účastí na odborných konferencích a seminářích
- pořádáním pracovních schůzek svých členů, klubových večerů a pravidelné výroční konference
- publikováním informací a novinek z oboru na vlastních webových stránkách a odborných časopisech
- vydáváním „itSM News“, rešeršemi odborné literatury a článků a pořádáním průzkumů
- vytvořením a udržováním seznamu specialistů certifikovaných v oboru ITSM
- vytvořením a prosazováním etického kodexu člena itSMF Czech Republic, z. s.
- udržováním aktuálního seznamu členů a jejich kontaktních údajů a zprostředkováváním kontaktů jak v rámci spolku, tak i v rámci širší odborné veřejnosti
- navazováním spolupráce s ostatními soukromými, veřejně-prospěšnými a státními subjekty, jejichž činnost se jakkoli dotýká oblasti řízení informatiky.

Naše konference

Výroční konferenci pořádá itSMF CR od roku 2007 obvykle ve třetím, případně čtvrtém týdnu ledna. Formát konference se vyvíjel v čase a nikdy nenabyl definitivního, neměnného formátu. Na první pohled se to může jevit jako nevýhoda, nicméně se nám tento přístup osvědčil, protože nám umožnil pružně reagovat počtem a zaměřením programových bloků i počtem přednášek, případně workshopů na žhavá témata konkrétního období.

Až na covidové roky 2021 a 2022 se časový rámec konference ustálil na jednom a půl dni a na 2 až 4 přednáškových sálech. Vzrůstající počet účastníků, pohybující se v posledních letech mezi 250 až 270 posluchačů, je měřítkem spokojenosti s náplní a průběhem konference.

O tom, že letošní konference proběhla opět elektronicky, rozhodl přípravný výbor na konci prosince 2021, kdy již nemohl spoléhat na to, že bude možné zajistit obvyklý formát s osobními kontakty. Dvoudenní konference itSMF 2022 se konala ve dnech 21.-22. ledna 2022. S ohledem na počet příspěvků, jejich kvalitu a atraktivnost témat a akceptovatelný časový rámec, byl zvolen formát „jednoho sálu“ s ukončením v 16:05, resp. 14:30.

Letošní konference byla zaměřena na lidskou stránku Digitální Transformace a pod názvem *Chatbot: člověče, nezlob se* byla rozdělena do následujících tematických bloků:

1. TSM a Lidé
2. Vedení & nové dovednosti v digitálním věku
3. Nikoli digitální ale kulturní transformace
4. Budoucnost IT a technologie.

Klíčovými řečníky byli letos Paul Wilkinson (jeden z top světových odborníků v ITSM) a Kaimar Karu (bývalý ministr zahraničního obchodu a IT v Estonsku). Konference se nevyhnula ani tématu cyber security, nedílné součásti IT služeb, které zmínil Aleš Špidla.

Všichni přednášející souhlasili s tím, aby účastníci měli možnost po skončení konference stáhnout prezentace a obrazový záznam přednášek. Vrcholným bodem konference, byla panelová diskuse, kterou moderoval Petr Koubský.

Panelisty, kteří diskutovali a odpovídali na otázky účastníků konference byli Ondřej Profant (náměstek vicepremiéra pro digitalizaci), Vladimír Dzurilla (ředitel SPCSS a NAKIT), Zdeněk Zajíček (prezident ICT Unie) a Michal Bláha (hlídač státu, propagátor e-gov/chytrého a moderního státu).

Bližší info o Programu 2022 – 16. výroční konference itSMF Czech Republic - můžete najít na https://conference.itsmf.cz/program/.

Pro příští 17. Výroční konferenci 2023 předpokládáme prezenční formu, předběžně jsme se rozhodli pro změnu formátu oproti předchozím prezenčním konferencím, pro jeden sál ve dvou dnech s delší dobou ve čtvrtek. Vycházíme při tom z odezvy účastníků, kteří oceňují nejen kvalitní a velmi užitečné přednášky, ale také možnosti networkingu, tj. navazování osobních kontaktů jak s přednášejícími, tak mezi sebou navzájem. Definitivně se rozhodne nejspíše do konce roku. Budeme se těšit na viděnou za rok!

Plán akcí CACIO v roce 2022

Pro rok 2022 řídící výbor CACIO připravil ve spolupráci s partnery plán aktivit, který Vám zde představujeme. Při přípravách všech aktivit chceme reagovat na aktuální témata, takže může dojít k drobným úpravám či aktualizacím. O všech akcích i změnách budete podrobně informováni na našem webu www.cacio.cz.

Leden

- *Konference ITSMF, Chatbot: "Člověče, nezlob se!" (partnerství)*
- *Ukončení sběru přihlášek do soutěže IT projekt roku*

Únor

- *Seminář – Praktické aspekty řízení informatiky – Aktuální otázky bezpečnosti*
- *Zasedání hodnotitelské komise soutěže IT projekt roku – 1. kolo presentací*

Březen

- *Zasedání hodnotitelské komise soutěže IT projekt roku – 2. kolo presentací*
- *Kulatý stůl - aktuální otázky bezpečnosti*

Duben

- *Seminář – Praktické aspekty řízení informatiky – Řízení projektů a změn*
- *Galavečer CACIO – vyhlášení finalistů a vítězů 19. ročníku soutěže IT projekt roku*

Květen

- *Seminář - Aktuální otázky bezpečnosti*

Červen

- *CACIO fórum – jak technologie mění svět*
- *Výjezdní zasedání řídícího výboru CACIO*

Červenec

- *Seminář – Praktické aspekty řízení informatiky - Open source*

Září

- *Koncert – Poděkování za práci a podporu aktivit CACIO*

Říjen

- *Konference CNZ (partnerství)*
- *Seminář – Praktické aspekty řízení informatiky – Krizové řízení*

Listopad

- *CACIO fórum - Praktické aspekty řízení informatiky – Jak efektivně řídit IT*

Prosinec

- *Vánoční setkání realizačního týmu CACIO*

Poznámka: *V průběhu roku pořádáme také uzavřená jednání energetické sekce a sekce státní správy.*

Těšíme se na spolupráci a tvůrčí setkání.
Řídící výbor CACIO

Nadační fond Věčná naděje

Na základě kladných ohlasů s koncerty, které doplnily aktivity CACIO se ukázalo velice prospěšné doplnit odborná setkání i setkáním společenským. Proto jsme začali v roce 2022 spolupracovat s Nadačním fondem Věčná naděje a těšíme se na společné aktivity.

V roce 2017 **vznikl Nadační fond Věčná naděje** s cílem zachovat a dále rozvíjet unikátní umělecký odkaz středoevropských kulturních hodnot spojených s územím dnešní České republiky, a to především **formou hudebního festivalu.**

Nejen tzv. terezínští skladatelé byli náhle a násilně umlčeni událostmi druhé světové války, také jiní tvůrci české a německé národnosti, židovského i křesťanského vyznání za doby nesvobody v průběhu 20. století trpěli. Hudba je právě jedním z projevů unikátního uměleckého odkazu středoevropských kulturních hodnot spojených s územím dnešní České republiky. Poslání Nadačního fondu Věčná naděje a jeho stejnojmenného festivalu je připomínat historické události, nést jejich odkaz a usilovat především o to, aby nedocházelo k násilí, nenávisti či jiným formám diskriminace z důvodů rasy, etnické či kulturní odlišnosti.

Cílem Nadačního fondu Věčná naděje je vybudovat prestižní festival s důrazem na výjimečnou uměleckou kvalitu. Základ festivalu tvoří opomíjená díla umělců Terezína, autorů jako byli Viktor Ullmann, Gideon Klein, Hans Krása, Pavel Haas, i jiných, která vznikala v podmínkách koncentračních táborů druhé světové války a zůstávají stále nedoceněna. Program je vždy doplněn o díla dalších českých a světových hudebních velikánů a reaguje na aktuální výročí a události.

Posláním festivalu je přiblížit mimořádné interpretační umění co nejširší veřejnosti. Festival je prestižní společenskou událostí založenou na geniu loci a skvělé interpretaci hudebních děl „našich“ festivalových autorů. Festival je určen posluchačům vážné hudby, ale i příznivcům divadla a kabaretu, šansonu i jazzu, všem generacím vnímavého publika.

Duchovním bohatstvím festivalu je myšlenka věčné naděje. Naděje, která překoná útlak, nenávist, nesvobodu, vykořenění a dává prostor kráse, víře a svobodnému životu.

Časopis CACIO Fórum vydává Česká asociace manažerů informačních technologií, Na Cihlářce 30, 150 00 Praha 5, www.cacio.cz, jako svou šestou neperiodickou publikaci, únor 2022 počet stran 24.