TEMATICKÝ MAGAZÍN VYDAVATELSTVÍ ECONOMIA A.S.

Samostatně neprodejné
09 | 2022

ICT REVUE

ERP systémy

Do zpracování dat z ERP systémů rychle pronikají algoritmy umělé inteligence.

Kyberbezpečnost

Digitalizace výroby a připojení strojů k internetu zvyšuje riziko kyberútoku.

Jak zkrotit cloud

Jednou z hrozeb spojených s využíváním cloudu jsou náklady na cloudové služby.

ATS TELCOM

www.atstelcom.cz

Kryptografická ochrana informací

Hlasové sítě a sjednocená komunikace

Systém komunikační a informační bezpečnosti, služby SOC, CSIRT

Kybernetická bezpečnost

LAN/MAN/WAN infrastruktura

Měření rychlosti

Bezpečnostní certifikace NBÚ ČR a NATO na stupeň „TAJNÉ“

ATS-TELCOM PRAHA nabízí:

- **Specialisty** zabývající se koexistencí a integrací nových řešení, která jsou založena na IP technologiích, do existujícího prostředí zákazníka;
- **Alcatel-Lucent Enterprise Rainbow** – náhrada stacionární telefonie – cloudová služba jednotných komunikačních služeb (UC) – chatování, telefonování, audio a video konference včetně mobility v prostředí státní správy;
- **ISIT software CZ** – komplexní nástroj pro řízení rizik a procesů spojených s kybernetickou bezpečností a ochranou osobních údajů, včetně tvorby a udržování bezpečnostní dokumentace v souladu s národní legislativou a standardy;
- **TruCAM II LTI 20/20** – nejnovější generace ručního kompaktního laserového měřiče rychlosti certifikovaného pro použití v ČR.

Alcatel·Lucent Enterprise

ISIT CZ SOFTWARE cybersecurity

LASER TECH

Sídlo firmy: ATS-TELCOM PRAHA a. s., Nad elektrárnou 1526/45, 106 00 Praha 10 – Michle,
IČ: 61860409, DIČ: CZ61860409, tel.: +420 283 003 111
Kancelář Praha: Milíčova 14, Praha 3, 130 00 • **Kancelář Brno:** Vídeňská 122, Brno, 619 00

EDITORIAL

Martin Knížek
editor speciálních projektů

Vážené čtenářky, vážení čtenáři,
kyberútočníci se chovají podobně jako v přírodě supi a hyeny, říká v rozhovoru v tomto vydání ICT revue Tomáš Krejčí, náměstek ředitele NÚKIB. Když je nějaká krize, přiláká to jejich pozornost. Stejně jako v přírodě přiláká pozornost supů a hyen souboj velkých zvířat. Ukázalo se to během covidu a ukazuje se to i v současné krizi spojené s napadením Ukrajiny Ruskem.

Podle průzkumu společnosti Trend Micro mezi velkými průmyslovými firmami v USA, Německu a Japonsku v posledních 12 měsících pocítilo dopady kybernetického útoku 89 procent z nich. Průmyslové a výrobní podniky se stávají stále lákavějším cílem útočníků v kyberprostoru. A útočníci k tomu často mají takřka ideální podmínky. Rychle postupující digitalizace průmyslu nutí firmy jednat rychle, pokud chtějí získat náskok před ostatními nebo alespoň udržet vlastní konkurenceschopnost. A digitalizovat prostředí, které je technologicky velice různorodé a v němž se životnost strojů počítá v desítkách let, s sebou mnohdy v oblasti bezpečnosti přináší kompromisy, jež se mohou později vymstít.

Kyberútočníci navíc dokážou postupovat velmi rychle a neustále vyvíjejí nové techniky a způsoby, jak se do firemních sítí dostat a co největší část jich ovládnout. Výrobní firmy naopak zpravidla postupují mnohem pomaleji a v digitálním prostředí se teprve rozkoukávají.

Podle nedávného doporučení společnosti Rockwell Automation by se proto firmy měly zaměřit na zvýšení odolnosti svých IT systémů prostřednictvím několika základních kroků. Klíčové je vyčlenit dostatek zdrojů. Pokud není bezpečnost zásadní pro nejvyšší management, nebude mít prioritu ani u zaměstnanců. S tím souvisí i odpovědnost – každý musí vnímat kyberbezpečnost jako součást své práce, nejde o problém IT oddělení. Velmi důležitá je také viditelnost a schopnost detekce problému v jeho počátku. Jakmile se hrozba projeví, je už příliš pozdě. V neposlední řadě jde o konzistenci – bezpečnost není jednorázovou událostí, vyžaduje konzistenci jak při odhodlání, tak při realizaci a začlenění do struktury fungování organizace.

MAGAZÍN ICT REVUE – PŘÍLOHA HOSPODÁŘSKÝCH NOVIN, 14. 9. 2022. Ředitel speciálních projektů Aleš Mohout • Art director Jan Vyhnánek • Vedoucí speciálního obsahu Jan Záluský (jan.zalusky@economia.cz) • Editor Martin Knížek (martin.knizek@economia.cz) • Layout Jan Stejskal • Grafika vizuální studio mediálního domu Economia • Adresa redakce Pernerova 673/47, 186 00 Praha 8 • Tisk Walstead Moraviapress s.r.o., Břeclav • Samostatně neprodejné • http://www.hn.cz

OBSAH

Online připojením výroby se firmy otevírají útokům

Chtít od firemního ajťáka, aby se staral o kyberbezpečnost ve výrobě, je podobné jako chtít od zubaře, aby pacientovi operoval srdce. Informační technologie ve výrobě (Operational Technology, OT) mají vlastní specifikace, kterými se zásadně liší od firemního IT.

Životnost obráběcích strojů se často počítá v desítkách let. To je z pohledu informačních technologií věčnost. Tomu bohužel odpovídá i úroveň zabezpečení starších strojů a jejich rozhraní proti kybernetickým hrozbám.

Dopady kybernetického útoku pocítilo v uplynulých dvanácti měsících 89 procent velkých firem. Přitom více než polovina musela zastavit či omezit výrobu na čtyři či více dnů. Vyplývá to z průzkumu společnosti Trend Micro, který proběhl na jaře letošního roku mezi 900 společnostmi z oblasti průmyslové výroby, zpracování ropy a plynu a výroby elektřiny. Týkal se velkých firem s počtem pracovníků nad jeden tisíc lidí v USA, Německu a Japonsku. Průměrná škoda činila 2,8 milionu dolarů a přes 40 procent oslovených firem zaznamenalo v daném období šest až deset pokusů o napadení.

text: Jitka Kvartková, foto: Shutterstock

Mantrou ve výrobním procesu, především v případě kritické infrastruktury, je schopnost udržet výrobu v chodu i ve ztížených či omezených podmínkách. Kybernetická odolnost si žádá dostatečné kapacity podnik ochránit, bránit se kyberútoku a být schopen se z něj rychle zotavit s minimálním dopadem na zákazníka. „K tomu podnik potřebuje zapojit velký počet účastníků zaměřených na různé oblasti. Spadá sem vše od znalosti systémů přes porozumění tomu, jak obnovit výrobu, včetně dostatečných zdrojů nebo způsobu rozhodování během kyberútoku," říká Ondrej Kováč, solution engineer ve společnosti Exclusive Networks Czechia, zabývající se kybernetickou bezpečností pro digitální infrastrukturu.

„Je zcela zásadní, jak si nastavíte priority pro postup během útoku – zda upřednostníte udržení chodu výroby na úkor sběru důkazů. Je to velmi komplexní činnost a hodně záleží také na odvětví a typu služby, kterou podnik poskytuje," doplňuje Kováč.

Odolnost na prvním místě

Zatímco ve firemním IT je v otázkách kybernetické bezpečnosti na prvním místě důvěryhodnost a předcházení úniku citlivých dat (Confidentiality), následovány integritou (Integrity), a teprve na třetí místo se řadí dostupnost (Availability), v průmyslové výrobě se triáda uplatňuje v opačném pořadí.

„Důvěryhodnost je pro zákazníky důležitá. Avšak pokud podnik nezajistí chod výrobních linek a pokud jeho vlastní systémy spolu nekomunikují efektivně, selhává ve své misi. A tomuto pořadí je potřeba věnovat pozornost už při návrhu celého systému," konstatuje Kováč.

Udržet výrobu v chodu je klíčové hlavně v případě kritické infrastruktury, kde může jít o záchranu lidských životů. Zatímco výrobní podnik utrpí v případě odstávky ztrátu příjmů, u veřejných služeb, jako jsou dodávky elektřiny, tepla či pitné vody, ovlivňuje výpadek schopnost obyvatel přežít. Tyto systémy jsou běžně budovány tak, aby v případě živelní katastrofy nastoupily záložní zdroje – zatímco však bouřka nebo povodeň poškodí vždy jen část systému, hacker cíleně útočí tak, aby vyřadil z provozu celý systém včetně záloh.

„Většina veřejných služeb dnes daleko překračuje požadovanou odolnost. Některé energetické společnosti ji mají nastavenou na 99,99998 procenta spolehlivosti. To znamená, že ročně je tolerován výpadek v délce 3 sekundy," konstatuje Ondrej Kováč.

Český versus zahraniční vlastník

Kromě typu výroby se podle oslovených odborníků pohled na kyberbezpečnost ve výrobě citelně liší také podle původu vlastníka firmy. Zatímco ryze české výrobní podniky řeší otázky bezpečnosti převážně jen do té míry, aby byl zajištěn celodenní provoz po sedm dní v týdnu, pobočky zahraničních společností musí vyhovět přísným interním předpisům. Otázka však je, nakolik dochází k naplnění těchto požadavků v realitě a do jaké míry pouze na papíře. Jedním z důvodů je nedostatek odborného personálu, který buď nemá dostatečné znalosti, anebo má tak širokou agendu, že mu na bezpečnost nezbývá čas. V praxi to pak vypadá tak, že podnikoví ajťáci se často učí bezpečnost za pochodu, bohužel často přímo ve válečné zóně.

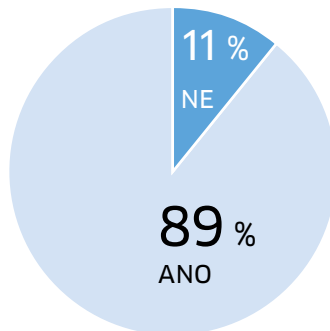
„Výrobní IT má jiné parametry než klasické firemní IT, rozdíly jsou především v komunikačních protokolech," říká Stanislav Simandl, výkonný ředitel MyCom Solutions, zaměřující se na IT outsourcing a kybernetickou bezpečnost. Zatímco pro kancelářský software pravidelně vycházejí aktualizace a bezpečnostní záplaty, producenti výrobních strojů aktualizace ani záplaty běžně neposkytují. „I zavedené firmy mají pokročilou techniku napojenou na počítače třeba z roku 2000, protože stroj nelze k novějšímu počítači připojit. Znamenalo by to výměnu celého stroje, velmi často výměnu celé výrobní linky, což je obrovská komplikace. Dvacet let staré stroje však nejsou na současnou ochranu vůbec uzpůsobeny," vysvětluje Simandl.

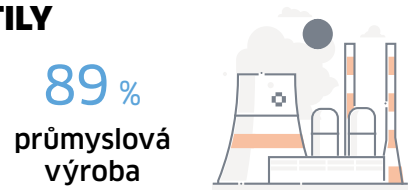
Výrobní sféra se snaží rizikům předcházet různými způsoby, nejúčinnější je pečlivý dohled nad komunikací mezi stroji a jejich maximální izolace. Důsledně se sleduje dění na síti před každým konkrétním strojem.

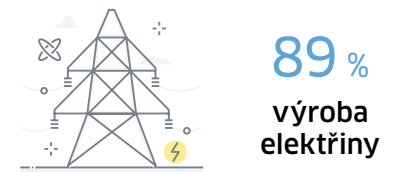
PODÍL FIREM, KTERÉ POCÍTILY NÁSLEDKY KYBERÚTOKU

(v období březen 2021 – březen 2022)

průměr: 89 %

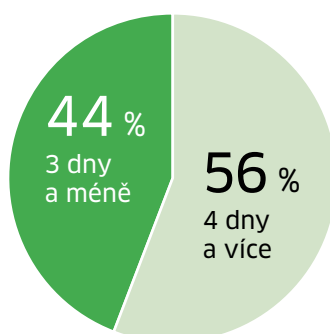


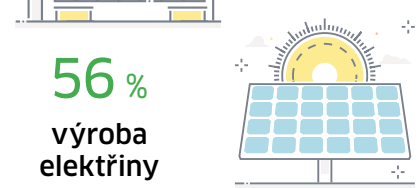




ODSTAVENÍ SYSTÉMŮ NA ČTYŘI A VÍCE DNŮ

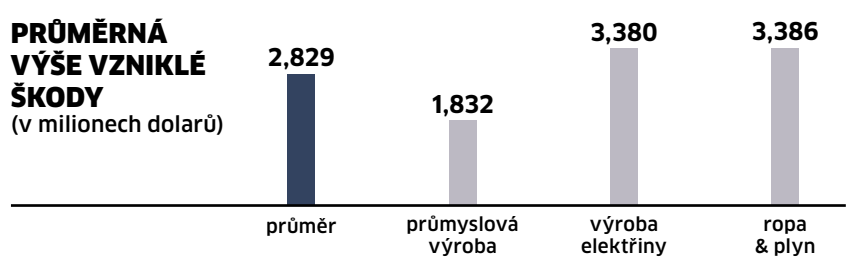
průměr: 56 %





PRŮMĚRNÁ VÝŠE VZNIKLÉ ŠKODY

(v milionech dolarů)



Zahrnuti pouze respondenti, kteří byli útoku vystaveni (tzn. 829 z celkově dotazovaných 900 firem)

Zdroj: Trend Micro Inc., The State of Industrial Cybersecurity, květen 2022

Bezpečnost řešte už při návrhu nové linky

„Při výběru nového stroje by měl požadavek na vysokou bezpečnost tvořit jedno z klíčových kritérií pro konečnou volbu dodavatele. Jednoduchým vodítkem je třeba skutečnost, zda stroj dokáže navazovat spojení se serverem výrobce a sám si stahovat konfigurace a aktualizace. Výrobní stroj by rozhodně neměl být serverem, neboť ten bude v budoucnu obtížné aktualizovat," upozorňuje Stanislav Simandl.

Dobře navržený projekt dopředu ukáže, zda je potřeba linku nastavit jinak, anebo se podívat po jiném výrobci. Dva dodavatelé mohou být schopni dodat stroj sice po technické stránce stejný, avšak z hlediska bezpečnosti se od sebe mohou výrazně lišit.

„Pokud se během údržby linky nemění architektura, začne postupně degradovat a s tím je třeba počítat. Je nutné neustále sledovat dění, jakmile se vyvine nový druh útoku, okamžitě ověřit, zda je proti němu architektura imunní," komentuje Simandl. Zároveň upozorňuje na situace, kdy stroj prochází servisní údržbou a připojí se k němu externí pracovník ze svého zařízení. Po jeho odhlášení je třeba zkontrolovat, zda tento krok neměl dopad na kyberbezpečnost, a eventuálně provést nezbytná bezpečnostní opatření. Čas od času se také vyplatí provést penetrační testy a nechat se otestovat externí firmou, která může odhalit závady, které interní pracovník v rámci provozní slepoty přehlédl.

Outsourcing, nebo vlastní zdroje?

„Setkali jsme se s případem, kdy podnikový ajťák po dvacet let poskytoval bezvadný servis a těšil se neomezené důvěře svých nadřízených. Bohužel došlo k napadení a následně se ukázalo, že i dlouholetý a spolehlivý zaměstnanec může občas něco opomenout anebo nezareaguje včas na nový druh útoku," sdílí zkušenost Simandl. „Zajímavým momentem pro nás bylo přiznání ředitele tohoto podniku, že kdybychom ho s nabídkou externí služby oslovili před útokem, spolupráci by odmítl."

Z opačného úhlu pohledu se na situaci dívá Michal Cimburek, manažer IT v Possehl Electronics Czech Republic, společnosti podnikající v oblasti komplexních aplikací vstřikování plastů: „Jako firma s mezinárodní působností a velkou základnou zákazníků po celém světě klademe vysoký důraz na ochranu proti kybernetickým útokům. Externí odborníci nám předložili nezávislý pohled na stav našeho zabezpečení a následně s námi formou pravidelných konzultací pracovali na vylepšení všech slabých článků. Včetně dodání produktů podporujících ještě vyšší kybernetickou bezpečnost."

K zapojením třetí strany a přenechání starostí na bedrech odborníků se přiklání také Tomáš Hřebejk, ICT manažer tiskárny Svoboda Press, specializující se na tisk časopisů a katalogů: „Jsme si dobře vědomi toho, že každý vydařený útok nás může stát dny i týdny úplného zastavení našich činností. I přestože máme vlastní IT oddělení, rozhodli jsme se navázat spolupráci s externím specialistou. Toto spojení nám přineslo komplexní pohled a přístup – a také klid a možnost soustředit se na polygrafické služby, klíčovou činnost našeho podnikání."

Rizikový dodavatelský řetězec

Dalším článkem, na který odborníci doporučují se podívat hodně zblízka, je dodavatelský řetězec. Podle Ondreje Kováče z Exclusive Networks

Ve výrobě využívající starší stroje je nejúčinnější obranou pečlivý dohled nad komunikací mezi stroji, jejich maximální izolace, jednosměrky v komunikaci a důsledné sledování dění na síti před každým konkrétním strojem.

Czechia roste v poslední době počet útoků, které přišly právě skrze dodavatelské firmy. „S rostoucím počtem dodavatelů roste i toto riziko. Řešením je standardizace jako nezbytná podmínka toho, aby konkrétní firma mohla být zařazena na seznam spolupracujících partnerů. A také pravidelný monitoring dodavatelů," uvádí Kováč.

Oborem, který v tomto směru pokročil zřejmě nejdále, je automobilový průmysl. Standard TISAX (Trusted Information Security Assesment eXchange) z roku 2017 požaduje od výrobců i dodavatelů automotive segmentu splnění náročných kritérií v oblasti kyberbezpečnosti. A to nejen u výrobců součástek nebo náhradních dílů,

ale u všech dodavatelů obecně, tedy například také u dodavatelů finančních, marketingových, právních či jiných služeb.

Krizové scénáře

Schopnost reagovat na kyberútok a vyjít ze situace s co nejmenšími ztrátami závisí vedle pokročilých technologií a vysoce kvalifikovaného personálu také na dobře vypracovaném krizovém plánu. Ten jednoznačně vzniká v dobách míru a je jasným a srozumitelným návodem, jak postupovat v případě napadení. Stanovuje priority, zda se firma bude snažit udržet výrobu a zajistit alespoň omezený chod, anebo upřednostní sběr důkazů. Uvádí jména klíčových účastníků, ať už interních nebo externích spolupracovníků, a jejich specifické role v daném okamžiku. Formuluje, kdo je klíčový dodavatel a kdo „jen" dodavatel. Pojmenovává kritéria, kdy vyhlásit stav katastrofy a spustit nouzový proces a také kdy ho ukončit.

Zájem firem o vypracování krizového plánu roste spolu se zájmem o zaškolení klíčových pracovníků, kteří by se v případě útoku podíleli na řešení situace. „Máme zákazníky, kteří neřeší pouze vzdělávání, ale přechází k tréninkům managementu prostřednictvím služby Table Top.

> S rostoucím počtem dodavatelů roste i riziko útoku prostřednictvím některého z nich. Řešením je standardizace a také pravidelný monitoring dodavatelů.

Během ní simulujeme různé situace rizikových scénářů, které mohou nastat během kybernetického útoku. Tento trénink sleduje, zda plán reakce na kybernetické incidenty funguje a pomohl by eliminovat nebo zmenšit dopad na organizaci," uvádí Dominik Klus, konzultant společnosti S&T CZ, která dodává IT řešení do komerční i veřejné sféry.

Kterým směrem se vydat

Průmyslové podniky se díky Průmyslu 4.0 a připojení do veřejné internetové sítě stále více otevírají útokům. To klade extrémně vysoké nároky na celý design a nastavení výroby tak, aby dokázala poskytovat základní službu i během krize a předcházela sociálním, finančním, psychickým či jiným ztrátám.

„V tuto chvíli považuji za naprosto zásadní striktně aplikovat metodiku 3S a 3R. Zkratky pocházejí z angličtiny a 3S znamená zjednodušení, standardizaci a bezpečnost. Za 3R se skrývá odolný, redundantní a spolehlivý systém. Tento přístup pomůže vyvážit investice nejen do kyberbezpečnosti, ale i do všech dalších oblastí. Kyberbezpečnost musí být neoddělitelnou součástí každé investice, do které se výrobní podnik pustí," uzavírá Ondrej Kováč.

Špatně nastavené procesy stojí firmy až třetinu ročních příjmů

Efektivita procesů je základem úspěchu každé firmy. Mnoho organizací však nedokáže své interní procesy nastavit správně, čímž v konečném důsledku přichází až o 30 procent svých příjmů. Jedním z dostupných nástrojů, které dokážou firemní procesy úspěšně zkrotit, je DMS (Document Management System) eDoCat české společnosti Onlio. Ten slouží pro centrální správu elektronických dokumentů, řízení a automatizaci jejich oběhu po firmě pomocí workflow.

Toto řešení, postavené na opensource platformě **Alfresco CE**, umožňuje kromě klasifikace dokumentů pomocí metadat také práci se šablonami, jemné řízení přístupových oprávnění, fulltextové vyhledávání anebo integrovat strojové vytěžování dat z digitalizovaných dokumentů. Zavedením a správnou aplikací tedy dokáže systém zabránit chybám, které ovlivňují chod celé firmy, neboť podniky často chybují v nastavování procesů v oblasti obchodní i výrobní. A zejména výrobní řetězec je v podstatě velmi křehký organismus náchylný ke značným ztrátám. *„Často však sledujeme také ztráty způsobené neefektivitou podpůrných procesů, třeba kvůli slabým nástrojům na sdílení a oběh dokumentů. Problémem také bývá nedostatečná automatizace a robotizace práce v oblasti účetních dokumentů či distribuce interních dokumentů, například směrnic,"* říká Pavel Nykl, obchodní ředitel společnosti Onlio. I proto je důležité si před vlastním zavedením DMS nechat zpracovat detailní analýzu, která dokáže odhalit konkrétní chyby, a navrhnout řešení vedoucí k optimalizaci procesů. Ty mohou být totiž zavedené roky a mnohdy se již ani neví, k čemu přesně slouží. Analýza by zároveň měla umět firmě definovat úskalí zavedení DMS a najít vhodná řešení.

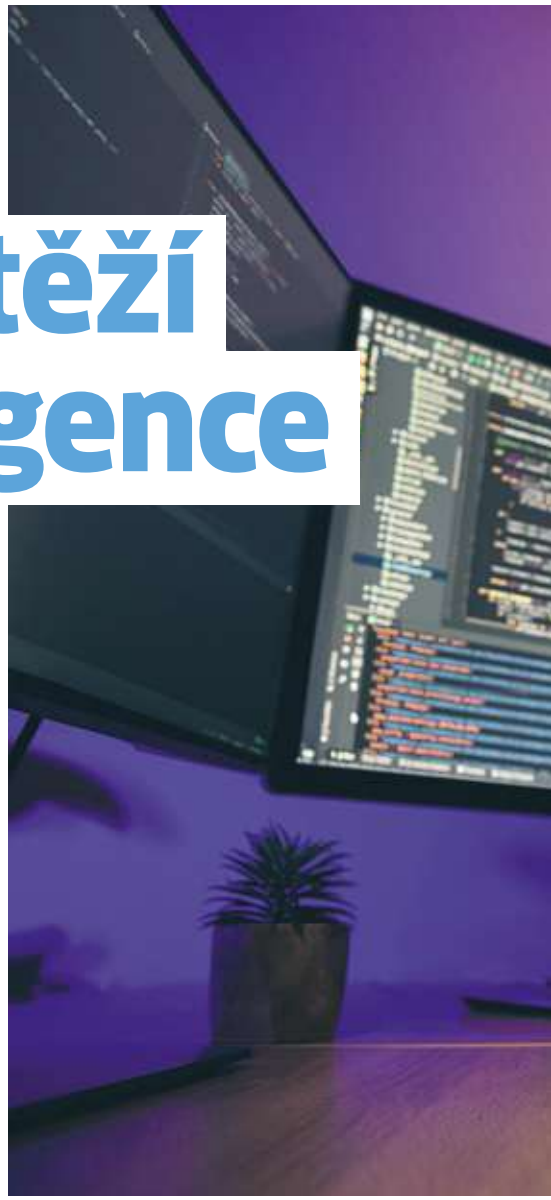
eDoCat DMS pracuje jako komplexní nástroj

Celý systém je dostupný jak v cloudu v podobě SaaS, tedy v modelu „software jako služba", nebo v on premise variantě, kdy si jej firma instaluje na své vlastní servery. Pokud si firma zvolí silně zabezpečenou cloudovou variantu, mají uživatelé možnost ke všem dokumentům přistupovat prakticky odkudkoliv, a to bez dalších investic do firemní IT infrastruktury. Což znamená, že mohou také daleko pružněji reagovat a v případě potíží je ihned začít řešit. Ovšem je důležité podotknout, že je třeba rozlišovat mezi nástroji pro týmovou spolupráci a DMS. Například finanční ředitel potřebuje dokumenty sice sdílet, ale zároveň nepotřebuje, aby si je mohl kdokoli libovolně upravovat, narozdíl například od obchodníků, kteří často vyvíjí své nabídky v mnoha variantách ve vícečlenném týmu. Také by nikdo jistě nespoléhal na to, že zaměstnanci zvládnou dokonale a trvale dodržovat oběh dokumentů ve firmě a dobrovolně evidovat jednotlivé kroky. *„To znamená, že firma potřebuje nástroj, který lidem usnadní práci, ale také stanoví pevné mantinely a pravidla. Devízou DMS systémů ve srovnání s cloudovými úložišti typu Google Drive či Microsoft One Drive je právě jejich schopnost vynutit si na uživatelích dodržování firemních pravidel,"* pokračuje Pavel Nykl.

eDoCat DMS je součástí firemního intranetu. Jinými slovy, uživatelé se mohou pod jedním "loginem" pohybovat jak v intranetu, tak právě i v DMS. *„Jedná se tedy o jedno místo, v němž zaměstnanci mohou najít veškeré informace a dokumenty ke své práci. Tím, že jsou tyto dvě aplikace propojené, také mohou uživatelé sledovat své nevyřízené úkoly v rámci **DMS systému eDoCat** přímo v intranetu. Ihned po přihlášení tak zjistí, zda není třeba seznámit se s nějakým novým dokumentem v rámci řízení oběhu firemních dokumentů anebo nějaký dokument schválit,"* pokračuje dále s tím, že toto spojení také zjednodušuje procesy spojené například se zaškolováním nových zaměstnanců, protože mají opět veškeré potřebné informace na jednom místě.

eDoCat DMS se také zaměřuje na robotizaci procesů, takzvané RPA. Díky robotům lze automaticky spouštět požadované akce na základě událostí, k nimž v systému dochází, ale také na základě hodnocení metadat u konkrétních dokumentů. Podle Pavla Nykla tak běžní uživatelé nemusejí díky robotům ztrácet čas při odbavování rutinních a manuálních úkonů. „Také ale pracujeme na strojovém učení a AI pro naše roboty, což má za cíl využít znalosti historie zpracování dokumentů tak, aby se usnadnila práce uživatelů i snížila chybovost zpracování." A v neposlední řadě je třeba zmínit, že **eDoCat DMS** je možné integrovat pomocí rozhraní API i s ostatními firemními informačními systémy, například účetními – od Pohody až po SAP, ERP systémy, nástroji pro elektronické podepisování, dlouhodobé důvěryhodné uložení dokumentů v souladu s eIDAS a podobně

Data z ERP systémů vytěží umělá inteligence



Chytré algoritmy pomáhají například předpovídat budoucí trendy na trhu nebo z dat připravují informace jako podklady pro kvalifikovaná manažerská rozhodnutí.

S

Současné ERP systémy využívají řadu technologických novinek a prorůstají stále novými oblastmi. Nabízejí například propojení s e-shopy pro rychlé a automatizované obchodování, sběr dat ze zařízení internetu věcí a jejich zpracování umělou inteligencí nebo vysoký stupeň automatizace podnikových procesů. Navíc procházejí nepřetržitým vývojem, takže je dnes samozřejmé provozovat ERP systém v cloudu, jeho funkce jsou dostupné z jakéhokoli – typicky mobilního – zařízení a nemůže chybět ani robustní datová analýza, která poskytuje nové pohledy na fungování podniku a samozřejmě i cenné podklady pro manažerská rozhodnutí.

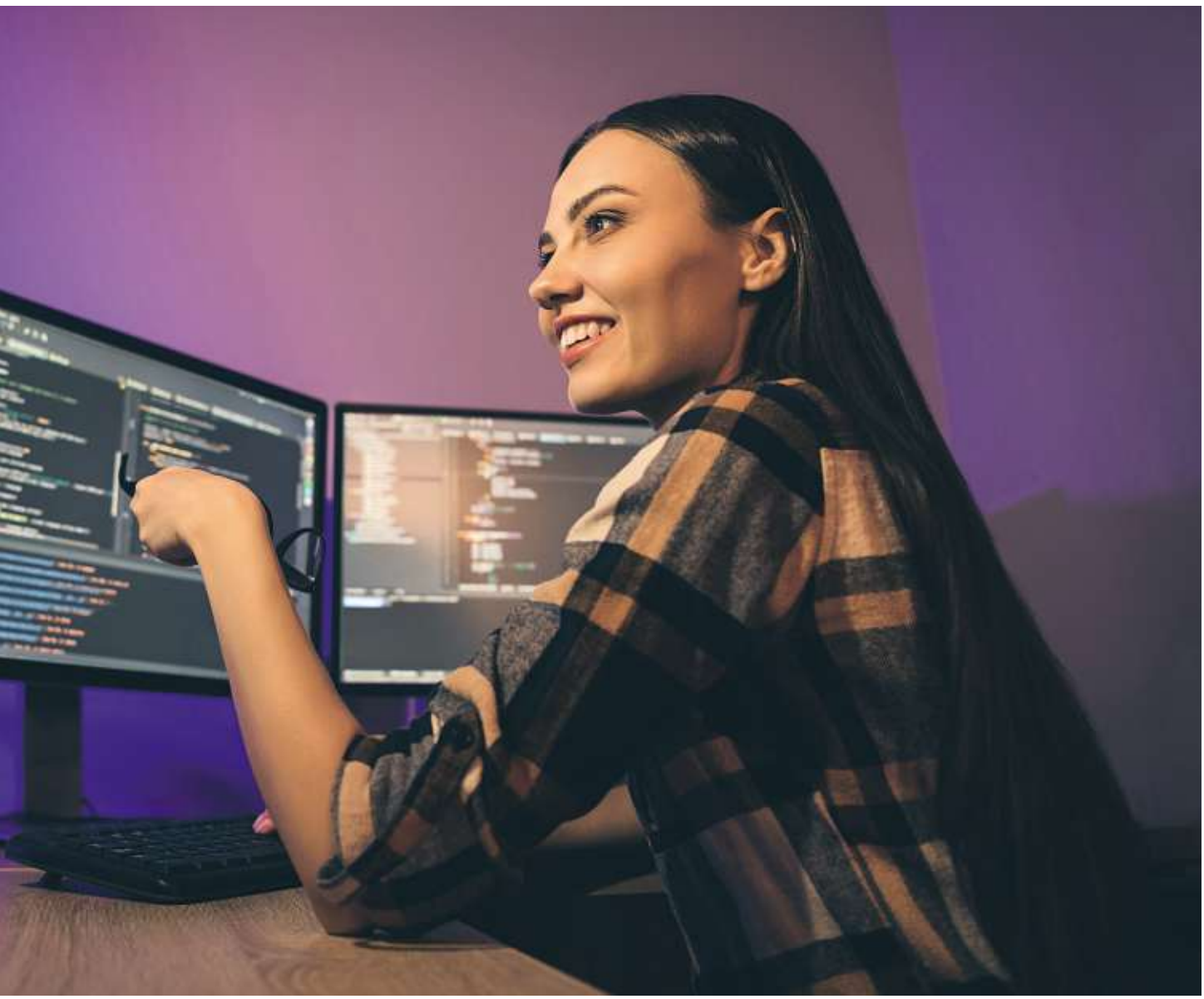
Pro každého něco

Dalším zajímavým trendem je headless architektura, tedy rozdělení ERP systému na back-end, reprezentující byznysovou logiku ERP, a front-end, tedy reprezentaci informací a funkcí směrem k uživatelům. Smysl takové architektury ERP systému spočívá v tom, že různí uživatelé ERP systému potřebují pro svoji práci odlišné informace a funkce. Headless ERP tak každému uživateli poskytne jedinečné prostředí v závislosti na jeho roli v rámci organizace.

Stále více ERP systémů dnes také umožňuje přizpůsobení a vytváření nových funkcí či reportů bez nutnosti programování. Low-code či no-code přístup poskytuje technicky trochu zdatnějším uživatelům možnost zvolit si datové zdroje a způsob zpracování i prezentace dat a vytvářet si tak nové funkce, které potřebují ke své práci. To znamená, že není nutné zadávat tvorbu nových funkcí vývojářům a čekat na ně týdny či měsíce. Díky větší flexibilitě ERP systémů podporujících low-code/no-code vytváření nových funkcí lze snadněji zajistit jejich přizpůsobení

> “ Snahou dodavatelů je co největší zkrácení doby nasazení nových ERP funkcionalit u zákazníků.

text: Radek Kubeš, foto: Shutterstock



oborovým standardům i nejnovějším požadavkům na funkčnost a také získat konkurenční výhodu.

Jedním z důležitých trendů vývoje ERP systémů je nepochybně také podpora automatizace podnikových procesů. Díky automatizaci odpadá velké množství manuální práce při zadávání a zpracování dat. Zaměstnanci, kteří ji vykonávali, se díky tomu mohou věnovat náročnějším a důležitějším úkolům. Automatizace v ERP systému umožňuje procesy celkově zjednodušit, což zároveň vede ke zvýšení produktivity a efektivity podniku. „V poslední době je vidět jednoznačný trend otevření ERP systémů pro připojení externích specializovaných aplikací a zavádění robotické automatizace procesů napříč jednotlivými systémy. Softwarový robot v ERP systému tak umí nahradit člověka, vykonávat přidělenou práci bezchybně, výrazně rychleji, a navíc s nižšími náklady," potvrzuje trend automatizace David Kazda, Business Systems Director ve společnosti Algotech.

Také ERP systémy dnes umožňují přizpůsobení a vytváření nových funkcí či reportů bez nutnosti programování. Low-code či no-code přístup umožňuje uživatelům vytvářet si nové funkce, které potřebují ke své práci.

Rychlejší implementace i noví zákazníci

Obecný trend digitalizace znamená i zavádění ERP systémů v podnicích, které se zatím bez podobného řešení obešly a nahrazovaly jej například různými dílčími aplikacemi. Ukazuje se také, že když už se podnik pro zavedení ERP rozhodne, hledá především flexibilní řešení s možností rychlé implementace. „Na trhu dnes vnímám snahu dodavatelů o co největší zkrácení doby nasazení nových ERP funkcionalit u zákazníků. A to ve dvou rovinách – jednak hledají cesty a nástroje, které umožní zkrátit dobu implementace ERP řešení, jednak poskytují nástroje, které umožní rychle aktualizovat používané řešení o nově vyvinuté funkcionality

ze strany výrobce," říká Milan Tesař, obchodní ředitel společnosti InfoConsulting. Při porovnávání ERP systémů je tedy důležité nejen to, jaké funkcionality dokáže ERP řešení poskytnout nyní, ale také jaké jsou možnosti jeho rozvoje do budoucna, stejně jako složitost adopce těchto změn a jejich nasazení do produkčního prostředí z pohledu zákazníka.

Podobnou zkušenost s novými implementacemi ERP systémů u zákazníků potvrzuje také Michal Říha, Head of Customer Advisory CZ & SK ve společnosti SAP ČR: „Sledujeme trend, kdy řada menších firem a start-upů hledá vyhovující ERP systém. Hlavním kritériem je rychlost nasazení a vyspělost ERP včetně pokročilých analytických funkcí, tak aby byly společnosti připraveny rychle reagovat na změny v byznysu a predikovat trendy vývoje. V posledních letech bylo doménou ERP hlavně řízení procesů a komplexnost informací pro optimalizaci chodu firmy, nyní se společnosti přiklánějí k využití analytických nástrojů k modelování a nastavování trendů a jejich rychlého uvádění do praxe."

Když skladník naskenuje zásobu, kterou chce zaskladnit, ERP systém je schopen zjistit, zda a kde je položka případně potřeba a přesměrovat manipulaci žádaným směrem.

V poslední době se také objevují unikátní způsoby nasazení, které jsou spojené s agilní metodikou. Některé společnosti jsou schopné nasadit ERP systémy v horizontu tří až čtyř měsíců, což snižuje náklady spojené s délkou implementace a přináší další výhody. Velkou měrou tomu přispívá právě příklon k ERP v cloudu, kde odpadá řada zdlouhavých činností, díky kterým pak vlastní nasazení trvá měsíce namísto let.

Pružnější plánování

Zásadní změnou ve světě ERP je také výrazné zpřesnění řízení podnikových procesů. Zatímco dříve probíhalo řízení a plánování s denním termínováním, nyní má stále větší množství podniků požadavek na řízení online v reálném čase. „Za tímto vývojem požadavků našich zákazníků není jenom změna ve funkcionalitě ERP systému, ale i praktické využívání nových technologií pro komunikaci se systémy třetích stran

a partnerů. Pokud například přijde od zákazníka zakázka, nečeká se na reakci uživatele, ale ERP systém ji ihned vyhodnocuje a posouvá k zaplánování a expedici," vysvětluje Vladimír Bartoš, ředitel pro strategii společnosti Minerva Česká republika.

Plánování výroby již standardně využívá pokročilé metody jako APS (advanced planning and scheduling) a potřebuje znát okamžité zásoby, jejich umístění a hlavně aktuální rozpracovanost. To vyžaduje, aby ERP systém přímo řídil a evidoval výrobu nebo aby online komunikoval s výrobním informačním systémem MES (Manufacturing Execution System) a stroji. „Podobně řídíme i skladníky. Pokud skladník naskenuje zásobu, kterou chce zaskladnit, ERP systém je schopen zjistit, zda a kde je případně potřeba, a přesměrovat manipulaci žádaným směrem," dodává Vladimír Bartoš. Obchodování se zrychluje a online řízení umožňuje vynechat zbytečné aktivity. To přináší rychlejší reakce na výpadky ve zdrojích i na potřeby zákazníků a vyšší efektivitu.

ERP v cloudu podporuje využití umělé inteligence

Využívání umělé inteligence a automatického strojového učení je v posledních letech stále častější, především díky možnosti využití výpočetního výkonu ERP systémů v cloudu a rychlosti provádění složitých algoritmů umělé inteligence. „ERP systémy obsahují mnoho dat, která lze pomocí umělé inteligence proměnit na cenné informace. Také je zde stále velký potenciál pro zapojení umělé inteligence při vytěžení informací z již existujících dat. Už dnes zákazníci používají sofistikované systémy, které odhalí podezřelé transakce v systému, upozorní na odchylky chování uživatelů nebo pomohou s předpovědí trendů prodeje," uvádí David Kazda ze společnosti Algotech.

Vyspělé ERP systémy mají technologie umělé inteligence a strojového učení už nativně zabudované. S jejich využitím se dá snížit náročnost práce s ERP systémem, řadu operací je možné svěřit umělé inteligenci, která podle naučených vzorců dokáže řešit řadu operací zcela samostatně. Některé procesy tak lze provádět automaticky, bez nutné obsluhy lidskými zdroji. „Z mého pohledu je umělá inteligence jedním z klíčových prvků inovací ERP řešení. Umožňuje vytěžit informace z toho obrovského množství dat, které ERP systémy typicky obsahují, a na jejich základě poskytnout lepší podklady pro řízení firmy," doplňuje Milan Tesař ze společnosti InfoConsulting.

> “ Už dnes zákazníci používají sofistikované systémy, které odhalí podezřelé transakce v systému, upozorní na odchylky chování uživatelů nebo pomohou s předpovědí trendů prodeje.

Pomůže ERP v současné krizi?
Především výrobní podniky se v současné době potýkají s řadou závažných problémů – ať už jde o výpadky v dodavatelských řetězcích, nebo rostoucí ceny energií a dalších vstupů. Může se do řešení nějak zapojit i ERP systém? Podle Michala Říhy ze SAP ČR bezpochyby ano: „Vhodné ERP řešení, které disponuje skutečně komplexními informacemi a vyspělými analytickými nástroji umožňuje podnikům reagovat na aktuální problémy a podle toho přizpůsobovat svoje chování. Čas a flexibilní možnost změn v podnicích v tomto případě hrají obrovskou roli."

Například rostoucí ceny vstupních materiálů lze mírnit efektivním poptávkovým řízením a vyhledáváním nových dodavatelů. Pokud to nepomůže, ERP systém umí rychle a přesně překalkulovat náklady na výrobky včetně započítání příslušných vícenákladů. Ceny energií lze nasmlouvat tak, aby byly výrazně levnější do mezní hodnoty spotřeby, domluvené s dodavatelem. „Plánování výroby umí započítat čerpání energií jako sekundární omezující zdroj a plánovač tak má možnost vyhlazovat plán s cílem nepřekročit domluvenou mez. Pokud ceny energií rostou, ERP umí simulovat náklady na výrobek včetně těchto změn," popisuje možnosti podnikových

> ERP systém umožní vytěžit maximum z toho, co je k dispozici, a minimalizovat dopady výpadků ze strany dodavatelů.

systémů Vladimír Bartoš ze společnosti Minerva Česká republika.

Narušené dodavatelské řetězce znamenají výpadky v dodávkách materiálu. Nákupčí musí aktivně prověřovat dodávky a do ERP systému aktualizovat plánované termíny příjmu materiálů. Plánování pak rozvrhuje výrobu nejen s ohledem na omezené kapacity pracovišť, ale i se zohledněním plánované dostupnosti materiálu. Pořadí operací se mění automaticky dle priorit zakázek ve snaze najít nejlepší cesty. I přes všechny těžkosti se pak může podařit naplnit slíbené termíny dodávek zákazníkům, nebo alespoň včas určit reálné termíny a férově informovat zákazníky o zpožděních. „V okamžiku, kdy na trhu není potřebný materiál či polotovar, s tím sebelepší ERP řešení nic nenadělá. Na druhou stranu ERP systém umožní vytěžit maximum z toho, co je k dispozici, a minimalizovat dopady výpadků ze strany dodavatelů. Algoritmy plánování potřeby materiálu jasně říkají, co a kdy bude třeba, nákupní proces je jasně řízený a správná data jasně napovídají nákupčímu, jakým směrem má vést vyjednávání. Systém umožní identifikovat dopady neuskutečněných dodávek na výrobu a její přeplánování tak, aby byly minimalizovány dopady vůči zákazníkům," dodává Milan Tesař ze společnosti InfoConsulting.

text: Radek Kubeš, foto: Billigence

Budoucnost jsou data v cloudu

Bez pokročilé datové analýzy firmy v současném světě u zákazníků neuspějí. Michael Kapr se svou společností Billigence pomáhá dalším firmám tuto oblast zvládnout.

Se zkušenostmi z práce v několika nadnárodních korporacích založil Michael Kapr společně se svou manželkou téměř před 16 lety firmu Billigence. Dnes má firma pobočky v Praze, Londýně, Frankfurtu, Varšavě, Sydney, Singapuru a San Diegu a svým klientům z celého světa poskytuje odborné znalosti a služby v oblasti datové analýzy, budování datových skladů a podpory manažerského rozhodování.

Jaké hlavní problémy dnes vaši zákazníci při práci s daty řeší?
Jde především o nepřetržitý nárůst množství dat, který je výsledkem rozsáhlé digitální transformace, a obecně rychlý přechod do digitálního prostředí kvůli pandemii. Tato data je nutné nejen někam ukládat, ale především zpracovat a získat z nich důležité pohledy na fungování firem a jejich zákazníky. Tomu ale brání absence potřebných nástrojů a také všeobecný nedostatek analytiků a datových vědců, kteří umějí z dat dostat to, co každá firma potřebuje – přehled a podklad pro kvalifikovaná rozhodnutí.

Datová analýza dávno nespočívá v generování reportů, které v podstatě popisují minulý stav. Firmy se potřebují dívat do budoucnosti, protože konkurence je stále ostřejší, byznys rychlejší a zákazníci náročnější. Manažeři a obchodníci potřebují vědět, jestli mají jejich rozhodnutí a aktivity správný směr, a potřebují rozumět svým zákazníkům – o co mají zájem a jak jim prodávat. Proto musí neustále vyhodnocovat efektivitu kampaní, reakce zákazníků i vývoj trhu a správně odhadovat trendy.

Mají vaši klienti obecně dobrou představu, co mohou ze svých dat získat?
První typ našich klientů přesně ví, jaká data je nutné zpracovávat a jaké pohledy na ně chtějí získat. Pro nás to znamená zvolit vhodný nástroj, nastavit jeho byznysovou logiku a připravit základní pohledy na data. Další si pak uživatelé snadno vytvářejí sami. Druhá skupina našich zákazníků také s daty nějak pracuje, ale nezískává z nich očekávanou přidanou hodnotu. V tomto případě musíme navrhnout změny ve způsobu nakládání s daty, vyzkoušet nové postupy a pohledy a často i zajistit, aby se k výstupům z datové analýzy dostali všichni, kdo je potřebují.

Michael Kapr, zakladatel a CTO Billigence Group, pochází z Česka, ale už více než 25 let žije v Austrálii. Do Sydney se přesunul s firmou KPMG na projekt velké implementace řešení SAP a už tam zůstal. Z IT přešel do oboru analýzy dat, ve které viděl budoucnost.

> “ Data je nutné nejen někam ukládat, ale především zpracovat a získat z nich důležité pohledy na fungování firem a jejich zákazníky.

Preferují vaši klienti ukládání a zpracování dat lokálně, nebo v cloudu?
Jednoznačně dominují cloudová řešení, a to hned z několika důvodů. Tím prvním je neomezená škálovatelnost zdrojů na ukládání a výpočetní zpracování dat. Dále je to obrovská pružnost při nakládání s daty, která není nutné pro jejich zpracování kamkoli přenášet či kopírovat. Data zůstávají na jediném místě a můžeme nad nimi vystavět libovolný počet data warehousů pro různé účely. Pak je zde samozřejmě možnost přístupu k datům a reportům odkudkoli a snadná možnost sdílení dat s partnery či zákazníky. To je v lokálním prostředí – s přijatelnými náklady – prakticky neřešitelné.

A nejsou právě náklady důvodem, proč řada firem stále spoléhá na vlastní datové centrum?
Rozhodně ne. Sám jsem během let prošel pozicemi, kde jsem měl na starosti byznys systémy podniků z různých zemí světa. A tak moc dobře vím, jak obrovské množství času a peněz jsme museli věnovat samotné přípravě na vybudování potřebné IT infrastruktury a pak i její správě, údržbě a rozšiřování. Ale co je nejhorší – ani vzdáleně se takto nepřiblížíte flexibilitě cloudu, kdy pro spuštění nového datového skladu, služby nebo databáze pro testování stačí doslova několik kliknutí. A pokud jde o provozní náklady, pomocí technologií jako Snowflake je lze výrazně ušetřit. Tato cloudová technologie totiž umožňuje oddělit ukládání surových dat, které je velmi levné, od jejich zpracování. Při čerpání výpočetní kapacity pak našim klientům pomůžeme s rozhodnutím, které analýzy je nutné provádět rychle, a tedy za vyšší cenu, a které reporty lze nechat levně vygenerovat třeba přes noc.

Na technologii Snowflake hodně spoléháte, jaké jsou její další výhody?
Kromě zmíněného řízení nákladů je to možnost provozovat Snowflake na Microsoft Azure, AWS i Google Cloud a také velmi rychlé nasazení i snadná ovladatelnost. To mimochodem pomáhá řešit i nedostatek kvalifikovaných datových vědců a analytiků.

Můžete představit některou z vašich referencí?
Z poslední doby mohu uvést nadnárodní pojišťovnu, s velmi drahou infrastrukturou a rozsáhlým analytickým týmem. Aby zůstala konkurenceschopná, musela začít rychle zavádět nové, digitální produkty a také poskytovat výrazně lepší datový servis svým partnerům – penzijním fondům. Komplikace, se kterými se pojišťovna potýkala několik let, se nám podařilo vyřešit během týdnů. Potřebná data jsme migrovali do cloudu, nastavili principy výměny dat a podpořili vytváření nových produktů. Také máme zákazníky v bankovnictví od velkých institucí po start-upy, které začínají rovnou s cloudem a zdatně konkurují zavedeným firmám. Zajímavým příkladem našeho zákazníka je také sportovní asociace, která využívá datové cloudové technologie pro ohodnocení výkonnosti atletů, tvorbu tréninkových plánů i pro komunikaci mezi trenéry, atlety a pořadateli mezinárodních soutěží i olympiád.

Nahlásit bezpečnostní incident je vždy výhodnější

text: Radek Kubeš, foto: HN – Tomáš Škoda

Největší slabinou je lidský faktor. Systém může být nastaven sebelíp, ale člověk prostě může z mnoha příčin udělat chybu a ty zabezpečené dveře nechtěně otevřít, říká v rozhovoru Tomáš Krejčí, náměstek ředitele pro řízení sekce Národního centra kybernetické bezpečnosti (NCKB) Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Oběť si často sama stáhne malware a hacker dostane přístup v podstatě naservírovaný. Jednou z priorit NÚKIB je proto i vzdělávání v oblasti kybernetické bezpečnosti. „V kritické chvíli může správná reakce naskočit jen tehdy, když je zažitá. Lidé si musí uvědomit, že internet není bezpečné prostředí, že musí být obezřetní," vysvětluje Tomáš Krejčí, který se většinu svého působení na úřadu zabýval implementací zákona o kybernetické bezpečnosti a kontrolou plnění povinností, které z něj vyplývají.

Jak váš úřad při zajišťování kybernetické bezpečnosti Česka postupuje a co konkrétně řeší?
Hodně obecně řečeno má NÚKIB mimo jiné za úkol pomocí nástrojů, které mu dal zákon č. 181/2014 Sb., o kybernetické bezpečnosti, určit důležité subjekty pro chod státu, které jsou závislé na informačních a komunikačních systémech, a těm pomocí vyhlášky stanovit, co mají udělat pro to, aby byla zajištěna jejich kybernetická bezpečnost. Dále se například věnuje osvětě v kybernetické bezpečnosti, pořádá cvičení v této oblasti, monitoruje hrozby v kyberprostoru, provádí penetrační testování důležitých systémů, skeny zranitelností, ale například i dozoruje, zda subjekty plní povinnosti plynoucí ze zákona. A tyto kroky, které ale nejsou absolutním výčtem toho, co vše úřad dělá, slouží ke zvýšení kybernetické bezpečnosti v Česku.

Jaké specialisty pro plnění těchto úkolů potřebujete a jak je náročné je získat?
Kyberbezpečnost je vlastně multioborová disciplína. Potřebujeme mnoho šikovných lidí, od právníků přes specialisty na IT s dobrými technickými znalostmi až po odborníky na kryptografii. Takové lidi je ale obtížné najít. Proto se snažíme vytipovat vhodné kandidáty třeba už i na vysokých školách. Obecně se snažíme k sobě přitáhnout schopné lidi – buď s už dostatečnými znalostmi, nebo s potenciálem, který můžeme rozvíjet. Nabídnout jim můžeme zajímavou práci, různorodé projekty, spolupráci se zahraničím a to, že získají jedinečné zkušenosti v oboru, který má budoucnost.

Jaké máte zkušenosti s hlášením kyberbezpečnostních incidentů napadenými firmami? Převažuje snaha incidenty tajit, nebo podniky bez problému plní svoje povinnosti? Co firmám, které incidenty nehlásí, hrozí?
Zákon o kybernetické bezpečnosti se v tuto chvíli týká jen velmi omezené skupiny společností v Česku – v podstatě pod něj spadají jen subjekty důležité pro chod státu. A právě pouze

Tomáš Krejčí

náměstek ředitele pro řízení sekce Národního centra kybernetické bezpečnosti NÚKIB

Je absolventem oborů manažerská informatika a informační management na VUT v Brně.

V Národním úřadu pro kybernetickou a informační bezpečnost pracuje od jeho vzniku. Odborně se velkou část působení na NÚKIB zaměřoval na problematiku implementace zákona o kybernetické bezpečnosti a kontrolu plnění povinností, které z něj vyplývají.

Od července tohoto roku je náměstkem ředitele NÚKIB a řídí sekci Národního centra kybernetické bezpečnosti.

> V kritické chvíli může správná reakce naskočit jen tehdy, když je zažitá.

u nich může NÚKIB vymáhat plnění povinností, jako je třeba právě hlášení kybernetických bezpečnostních incidentů. Společnosti k tomu přistupují různě. Někdo hlásí poctivě všechno, někdo skoro nic – my to zjistíme při kontrolách a pak hrozí provinilci pokuta.

Nahlásit incident je rozhodně výhodnější. Zaprvé to automaticky neznamená nějakou naši kontrolu a zadruhé můžeme v případě potřeby zasaženému velmi účinně pomoci – třeba i vyslat na místo náš tým rychlé reakce, jako se to stalo v minulosti například při útoku na jednu fakultní nemocnici, o kterém média informovala.

Kolik hlášení v průměru měsíčně obdržíte a jak jsou incidenty závažné?

NÚKIB přijímá hlášení desítek incidentů měsíčně. Závažnost se samozřejmě liší a pohybujeme se v rozmezí od těch méně závažných až po velmi závažné incidenty ohrožující například dostupnost služeb. Na našem webu naleznete veřejný měsíční report Kybernetické incidenty pohledem NÚKIB, kde je možné se dozvědět víc o řešených incidentech.

Kontrolujete zpětně, zdali napadené podniky zavedly preventivní opatření?

Obecně pravidelně kontrolujeme, jak námi regulované subjekty plní bezpečnostní opatření daná zákonem a vyhláškou. Máme na to dokonce speciální odbor. A zároveň samozřejmě taky můžeme prověřovat, jak tyto subjekty implementují různá varování nebo ochranná opatření, která vydáváme podle aktuální situace tak, jak nám ukládá zákon o kybernetické bezpečnosti.

Jaký máte prostor pro řešení nahlášených kybernetických incidentů?

Upřímně řečeno – kapacity sice máme, ale v současné době jsou omezené. NÚKIB není stále dobudovaný a sehnat dostatečný počet odborníků není jednoduché, o tom už jsme mluvili. Kdyby se sešlo víc závažných incidentů v jeden moment, museli bychom si určit priority, kam pošleme naše týmy rychlé reakce a kde to může chvíli počkat. Ale to je podobné třeba i u lékařské záchranné služby. Nikdo nemá neomezené možnosti.

Jak se vyvíjejí rizika kyberbezpečnosti a množství a závažnost incidentů v souvislosti s aktuálními událostmi, jako je pandemie a nyní válka na Ukrajině?

Kybersvět je zrcadlem toho reálného, takže to samozřejmě má zásadní vliv. Kdykoli nastane nějaká krizová situace, ať už jde o válku, povodně, pandemii nebo cokoli podobného, přiláká to pozornost útočníků, podobně jako v přírodě souboj velkých zvířat přiláká pozornost supů a hyen. Ti se vždycky snaží zneužít zmatku, protože vědí, že právě v takovou chvíli je nejvyšší šance, že někdo třeba i pod vlivem emocí udělá chybu. Například otevře zavirovanou přílohu e-mailu a podobně. My se snažíme to předvídat, být rychlejší a přimět všechny povinné subjekty k preventivním krokům.

Spolupracujete se zahraničními úřady podobného typu, jako je NÚKIB? Jaké máte z této spolupráce zkušenosti?

Samozřejmě, spolupráce s ostatními partnery je klíčová a vnímáme ji do budoucna jako jednu z hlavních součástí naší strategie kybernetické bezpečnosti. Máme na to i speciální vyslance – cyber attaché, kteří pracují v zahraničí. V kybersvětě jsou totiž informace tím nejcennějším a jejich výměna se spojenci je pak velkým přínosem. Sdílet zkušenosti s incidenty nebo varování před podezřelou aktivitou patří mezi základní stavební články štítu, kterým Česko chráníme.

Co může NÚKIB dělat pro zvýšení šance na postih kyberzločinců?

Úřad se zaměřuje na ochranu systémů důležitých pro fungování státu, nikoli na vyšetřování trestné činnosti poté, co se stala, nebo na trestání viníků. Boj s kyberzločinem a vyšetřování trestné činnosti je v gesci orgánů činných v trestním řízení, především policie. A my s nimi v případě potřeby samozřejmě spolupracujeme.

Kde vidíte největší slabiny v kybernetické bezpečnosti v českých firmách a organizacích? Máte nějaké mezinárodní srovnání?

Největší slabinou je lidský faktor. Systém může být nastaven sebelíp, ale člověk prostě může z mnoha příčin udělat chybu a ty zabezpečené dveře nechtěně otevřít. Oběť si sama stáhne malware a hacker nemusí ani tolik využít svoje znalosti, aby dostal přístup v podstatě naservírovaný. Jednou z priorit NÚKIB je proto i vzdělávání v oblasti kybernetické bezpečnosti. Snažíme se třeba zvrátit mylný názor, že kyberbezpečnost je věcí pouze IT oddělení. Tak to není a zodpovědnost má každý, od řadového zaměstnance až po nejvyšší úrovně topmanagementu – ten navíc musí zajistit adekvátní zdroje a podmínky.

Na co by se měly české firmy a organizace zaměřit, jaká rizika jsou v současné době nejvíce aktuální?

Je to právě zmíněné vzdělávání – je potřeba školit, školit a školit. Zní to otřepaně a nudně, ale opakování je matka moudrosti a v kritické chvíli může správná reakce naskočit jen tehdy, když je zažitá. Lidé si musí uvědomit, že internet není bezpečné prostředí, že musí být obezřetní. Musí mít na paměti, že všechna nařízení a omezení mají smysl a nikdo je nevydává jen proto, aby jiným znepříjemnil život. Štěstí prostě přeje připraveným. Kdo chce být aktivní, může sledovat naše webové stránky a taky využít školení, která jsou zdarma dostupná na našem webu www.osveta.nukib.cz.

Dopadne směrnice o kybernetické bezpečnosti NIS 2 i na vás? Poraďte se s odborníky ze společnosti VISITECH a.s.

Směrnice NIS 2 („o síťové a informační bezpečnosti"), mezi jejíž hlavní cíle patří sjednocení strategií států EU v boji proti kybernetickým hrozbám a zvýšení kybernetické bezpečnosti, by měla vstoupit v platnost v r. 2024. Následovat bude období pro zavádění do legislativ jednotlivých států. Nové požadavky jsou však natolik zásadní, že byste neměli otálet s přípravami, se kterými vám rádi pomohou také specialisté ze společnosti VISITECH a.s.

Na koho se NIS 2 vztahuje?

Mezi organizace, které budou muset zpřísněná pravidla dodržovat, patří např. instituce z oblasti energetiky, dopravy, bankovnictví, zdravotnictví, potravinářství, petrochemie nebo odpadového hospodářství. Dále jsou zahrnuti i poskytovatelé digitálních a informačních služeb, provozovatelé datových center, subjekty veřejné správy či pošta. V ČR je to celkem přibližně 6 000 subjektů.

Povinnosti a sankce

Firmy a instituce budou muset přijmout nezbytná technická a organizační opatření ke zvýšení své síťové a informační bezpečnosti. Jde např. o analýzu rizik, odolnost vnitřní sítě a informačních systémů, šifrování, prevenci a řešení incidentů, krizové řízení atd. Dalším z požadavků je zabezpečení dodavatelského řetězce. Směrnice zároveň zavede přímou odpovědnost statutárních orgánů firem.

Prohřešky lze pokutovat částkou dosahující až 10 000 000 eur nebo dvou procent z celkového celosvětového obratu dosaženého v předchozím roce.

K obavám není důvod!

Služba SOC365 poskytovaná společností VISITECH a.s. vyřeší bezpečnost za vás. Spolehnout se můžete na prevenci, detekci a ošetření hrozeb v reálném čase i na ochranu před narušením dat a dalšími kybernetickými incidenty. Služba garantuje kvalifikovanou aktivní reakci na útoky v režimu 24 × 7 i podklady sladěné s aktuální legislativou.

Dáváme zákazníkům úplnou volnost. Neplatí za služby, které nevyužijí

Písecký start-up The Cloud Provider poskytuje komplexní služby v oblasti ICT. V současné době firma investuje desítky milionů korun do obnovy technického řešení a připravuje pro své zákazníky nové služby.

Nejvýznamnějším produktem firmy je vlastní cloudová platforma postavená s využitím otevřených technologií OpenStack a Kubernetes. Samozřejmou součástí všech nabízených produktů je nepřetržitá technická podpora. „Chceme našim stávajícím, ale i potenciálním zákazníkům nabídnout to nejlepší, co na současném IT trhu mohou dostat. Naplňujeme tak hlavní motto firmy, které zní: Posouváme vaše IT na vyšší úroveň," vysvětluje Lukáš Kučera, ředitel společnosti The Cloud Provider.

V čem přesně posouváte IT svých zákazníků na vyšší úroveň?
Náš tým má mnohaleté zkušenosti z oblasti fyzické i virtuální infrastruktury. Klíčoví členové našeho týmu navrhli a dodnes provozují datové centrum v Písku. To bylo již v roce 2014 připraveno na provozování cloudových služeb, které v tu dobu v Česku ještě nebyly tak rozšířené jako dnes. Kolegové sbírali zkušenosti téměř po celém světě a tyto zkušenosti se posléze promítly nejen do samotné architektury a fungování datového centra, ale i do všech produktů, které dnes nabízíme.

Díky těmto zkušenostem a znalostem jsme dnes schopni zákazníkům nabídnout širokou škálu různých řešení, ať již s využitím fyzické infrastruktury, virtuální infrastruktury nebo jejich kombinace. Uvědomujeme si, že každý má jiné potřeby, které jen těžko beze zbytku uspokojí jedno univerzální řešení. Proto k zákazníkům přistupujeme individuálně a snažíme se nabídnout to nejlepší pro každého.

V čem spočívají individuální potřeby a požadavky zákazníků?
Většina zákazníků se dnes nechce o nic starat a chce po dodavateli kompletní řešení na míru, bez výpadků, bez starostí a řekněme s optimálními, spíše minimálními náklady. To jsme si vzali k srdci a zákazníkům nabízíme nejen výše zmíněné produkty, ale zajišťujeme i kompletní technickou podporu v režimu 24/7/365 v českém a anglickém jazyce. Kolegové dokážou díky svým znalostem a zkušenostem pomoci zákazníkům s IT strategiemi, s optimalizací nákladů na provoz IT infrastruktury a podobně. Navíc díky řadě partnerství dokážeme zákazníkům nabídnout i privátní cloudové řešení.

> U většiny globální konkurence je nutné volit z předem definovaných parametrů služeb, zatímco my se dokážeme dokonale přizpůsobit zákazníkovým potřebám.

Více informací naleznete na webu The Cloud Provider (odkaz v QR kódu).

Provoz datového centra musí být v dnešní situaci rostoucích cen energií poměrně náročný. Jak se s touto situací vypořádáváte?
Ano, i naší společnosti se významně dotkl zejména nárůst cen elektrické energie. My ale nevyužíváme datové centrum jako většina konkurence pouze pro housing serverů. Provozujeme v něm zmíněné cloudové služby a nové nadstavbové služby, jako je Dashpoint, která představuje automatizovanou platformu pro monitoring, sběr, vizualizaci a reporting dat na klíč, či Kubepoint, což je plně automatizovaná platforma pro snadnou produkci Kubernetes clusterů, tedy specifická služba pro vývojáře softwaru. Díky virtualizaci v rámci datového centra znásobujeme jeho celkový výkon a dokážeme tím veškeré provozní náklady lépe „rozložit".

Náš rozhovor vzniká v období prázdnin, dovolených. Máte i ve vaší firmě volněji?
Naopak. Období letošního léta využíváme ke kompletní obnově našeho technického řešení, a to jak fyzického, tak virtuálního. Chceme oslovit nové trhy, zlepšit služby stávajícím zákazníkům a rozšířit portfolio našich služeb. Investujeme desítky milionů korun, abychom našim stávajícím, ale i potenciálním zákazníkům mohli nabídnout to nejlepší, co na současném IT trhu mohou dostat.

Můžete to blíže specifikovat?
Pořizujeme nové servery, úložiště, síťovou a virtualizační platformu, na které provozujeme cloudové a další nadstavbové služby. Nové technické řešení bude rychlejší, bezpečnější, dostupnější a obecně výkonnější a pro nás efektivnější z hlediska provozních nákladů. Je to obrovská investice, ale velmi dobře víme, že pokud bychom ji nezrealizovali, do budoucna bychom neudrželi krok s konkurencí. Dovolím si tvrdit, že díky této investici budeme alespoň na nějaký čas před ní. Novinkou bude také nový, přehlednější ovládací systém námi poskytovaného cloudu, který významně zjednoduší práci a uspoří čas našim zákazníkům.

V čem spatřujete hlavní výhody nového řešení pro zákazníky?
Obchodně spatřuji velký potenciál v možnosti oslovit nové cílové trhy, například oblast telekomunikací a návazných oborů. Budeme například jediná firma v Česku, jež nabízí NVMe disky, které jsou až šestkrát rychlejší než klasické SSD disky, navíc připojené 100gigabitovými sítěmi. Máme k dispozici různé výkonové řady procesorů postavené na 3. generaci Intel Xeon a AMD EPYC, takže uspokojíme jednoduše každého. Obecně bych to shrnul tak, že každému zákazníkovi nabídneme právě takové řešení, které potřebuje. Nebude zbytečně platit za vstupy, které nepotřebuje či nevyužije.

Lukáš Kučera vede společnost The Cloud Provider od jejího založení v červenci 2020. Má za sebou dlouholeté zkušenosti s řízením portfolia investiční skupiny z oblasti IT či real estate. Pomáhá řídit a současně rozvíjet nové start-upy z oblasti IT. Vystudoval ekonomický obor na Jihočeské univerzitě, začínal jako středoškolský, posléze jako vysokoškolský pedagog.

A co postavení vůči světovým hráčům? Může malá česká firma konkurovat světovým řešením?
Rozhodně. A to nejen samotným technickým řešením našich služeb, ale zejména kompletní podporou v režimu 24/7/365, která je poskytována z Česka, ale především individuálním přístupem, který u globálních poskytovatelů nikdy nezískáte. U většiny globální konkurence je nutné volit z předem definovaných parametrů služeb, zatímco my se dokážeme dokonale přizpůsobit zákazníkovým potřebám. Každé řešení u nás je vlastně privátním řešením. A díky tomu, že využíváme otevřené technologie, „nezamykáme“ naše zákazníky a dáváme jim naprostou volnost. U nás mají zákazníci svůj provoz mnohem více pod kontrolou, nastavují si kompletní síťové prostředí i datové spojení mezi servery. A to, že data jsou uložená v datovém centru v Písku, které splňuje standardy Tier III, už je jen třešničkou na dortu.

Jak zkrotit výdaje na cloud?

text: Radek Kubeš, foto: Google, Shutterstock

Náklady na cloudové služby je třeba pravidelně kontrolovat (na snímku datové centrum společnosti Google v Mayes County v Oklahomě).

Kromě nesporných výhod mají cloudové služby také nemalá rizika. Jedna z hlavních hrozeb je spojená se správným řízením nákladů na cloud, které se snadno mohou vymknout kontrole.

Hlavní zaklínadlo poskytovatelů cloudových služeb zní velmi lákavě: „Platte jen za to, co doopravdy spotřebujete." Má to ale háček – jak zjistit a pravidelně kontrolovat, co (které služby a v jakém objemu) vlastně potřebujeme, kdo cloudové zdroje spotřebovává a s jakým rozpočtem na následující období musíme počítat? Problém s měřením nákladů na cloudové služby a jejich vykazováním oproti obchodním jednotkám, oddělením nebo konkrétním projektům je stále aktuálnější, především proto, že i využívání cloudu je v českých podnicích stále intenzivnější.

Nejnovější studie Journey to the Cloud společnosti SAP, vycházející z průzkumu agentury Kantar, uvádí, že alespoň jedno řešení založené na cloudu využívá v Česku hned 77 procent firem. Zpravidla navíc ve firmách najdeme hned několik různých cloudových řešení a služeb. „České podniky si velice dobře uvědomují, že budoucnost spočívá v přechodu z klasických serveroven na systémy, které jim dokážou poskytnout potřebnou flexibilitu a efektivitu. V následujícím roce plánuje více než polovina z nich implementovat alespoň jeden systém běžící v cloudu," říká Hana Součková, generální ředitelka SAP ČR. Podle studie české podniky v nadcházejícím roce investují do cloudových služeb v průměru 30 procent svých rozpočtů na IT. To je poměrně hodně peněz, které jistě stojí za to si pečlivě ohlídat.

Náklady mimo kontrolu

Růst nákladů firem na cloudové služby potvrzuje také globální studie State of the Cloud Report 2022 společnosti Flexera. Firmy podle ní v následujícím roce utratí za cloudové služby o 29 procent více než za poslední rok. Grand View Re-

Výhodu zjednodušení správy vlastní IT infrastruktury může při přechodu do cloudu snadno brzy převážit cena cloudových služeb. Jednoduchost jejich spouštění může v organizacích vést až ke ztrátě kontroly nad jejich využíváním.

search přitom odhaduje globální trh cloud computingu za rok 2021 téměř na 369 miliard dolarů.

Flexera ale také uvádí, že firmy v průměru o 13 procent překračují svoje naplánované rozpočty na cloudové služby a co hůř, téměř třetinu (32 procent) nákladů na cloud považují za zbytečně utracené. Není se potom čemu divit, že podle zmíněného průzkumu uvádí 59 procent dotazovaných podniků jako hlavní cíl v rozvoji využívání cloudových služeb nikoli migraci dalších úloh do cloudu (to jako jeden z hlavních cílů uvádí 57 procent organizací), ale optimalizaci svých současných nákladů na cloud.

Snadno otevřené kohoutky

Ukazuje se, že podniky nemají dostatečný přehled a kontrolu nad podstatnou částí svých nákladů na cloudové služby (a tedy IT obecně). Jednou z příčin tohoto stavu je přitom velmi pravděpodobně i lehkost, s jakou lze aktivovat stále nové a další cloudové zdroje. „To, co je nepochybně jednou ze skvělých vlastností cloudu, když potřebujeme rychle navýšit dostupné zdroje a kapacitu pro spouštění nebo testování nových aplikací, služeb či projektů, je zároveň velkou hrozbou, pokud nemáme přehled o tom, kde zůstaly otevřené kohoutky – tedy zbytečně běžící cloudové služby," říká Vladimíra Desková, PyraCloud Engagement Lead ve společnosti SoftwareONE, která se podílí na optimalizaci využívání cloudových služeb a softwarových licencí pomocí nástroje PyraCloud.

Dalším rizikem snadného spouštění cloudových služeb, ke kterému stačí platební karta a pár kliknutí myší, je i vznik „stínového IT". To spočívá v pořizování nových předplatných cloudových služeb zcela mimo kontrolu IT oddělení a často i za podstatně méně výhodných podmínek než při nákupu standardní cestou – prostě jen na základě okamžité iniciativy některého z oddělení, posvěcené vedoucím, který disponuje menším rozpočtem na provozní náklady. Kromě toho, že se tímto způsobem dále zvyšují náklady podniku na IT (i když na úkor jiného rozpočtu), to znamená, že se mimo kontrolu oddělení IT dostávají i (potenciálně citlivá) firemní data. Jak se tedy vrátit k využívání cloudu v souladu s myšlenkou platit jen za ty zdroje, které skutečně potřebujeme a využijeme?

Kontrola nad čerpáním cloudu

Jakkoli mohou světy cloudových služeb a klasického, licencovaného podnikového softwaru působit vzdáleně, principy, jak dostat pod kontrolu náklady na cloud i software, jsou do značné míry podobné. „Především je nutné dostat do jednoho prostředí přehled o všech předplatných cloudových službách – včetně nároků a závazků, které s nimi souvisejí. A to samé platí o softwarových licencích, licenčních podmínkách a nárocích. My jsme za tímto účelem vyvinuli platformu PyraCloud, která poskytuje kompletní přehled nad cloudovým i softwarovým portfoliem organizace," vysvětluje Vladimíra Desková ze SoftwareONE.

Jak takový přehled o cloudovém portfoliu může vypadat? Organizaci by měl poskytovat především kontrolu nad čerpáním typických cloudových služeb, jako jsou Microsoft Azure, Amazon Web Services (AWS) nebo Google Cloud Platform, s jednotným reportingem. Důležitý je také přehled dostupných rozpočtů na cloud (konkrétní cloudové služby) a jejich čerpání v reálném čase – s rozkladem na jednotlivá nákladová střediska. A konečně, nastavení indikátorů a upozornění zajistí včasné varování před přečerpáním stanovených rozpočtů. „Důležitou součástí monitoringu cloudových služeb jsou rovněž nástroje na plánování a predikci spotřeby cloudových zdrojů stejně jako identifikaci možných úspor nákladů a také roz-

poznání rizik souvisejících se zabezpečením, výkonem a dostupností konkrétní služby, jako je třeba Microsoft Azure," dodává Vladimíra Desková. Právě předvídání trendů spotřeby cloudových zdrojů odhaluje potenciál k optimalizaci a poskytuje další pohledy, využitelné při vyjednávání o podmínkách nových smluv na cloudové služby.

Strategie je základ

Nasazení nástroje na řízení spotřeby a sledování nákladů na cloudové služby je ale pouze jedním z kroků na cestě k efektivnímu využívání cloudu v rámci celé organizace. Současně je nutné nepodcenit i další fáze optimálního přechodu z klasického softwaru, provozovaného ve vlastním datovém centru, ke cloudovým službám. Celkem jde o řadu postupných kroků, které začínají už samotnou strategií přechodu na cloudové služby. Organizace se musí rozhodnout, jaké aplikace a služby budou migrovány do cloudu, v jakém pořadí a co je vlastně cílem tohoto přechodu. Ze strategie vzejdou požadavky na konkrétní cloudové služby společně s plánem, jak je bude organizace nakupovat.

Po pořízení předplatných cloudových služeb musí následovat nasazení nástrojů na zjišťování strukturování a řízení cloudových prostředků. Pokud se organizace chce vyhnout plýtvání, jde o naprosto klíčový krok, který je podmínkou pro efektivní využívání cloudových služeb. Dále je nutné přiřadit cloudové zdroje konkrétním organizačním jednotkám, aby bylo možné interně rozdělovat náklady na konkrétní pobočky, oddělení či projekty. Tyto organizační jednotky pak musejí mít přiděleny rozpočty na cloudové služby, jejichž čerpání bude sledováno prostřednictvím nastavených indikátorů a upozornění na spotřebu cloudových zdrojů. „Teprve když projdeme touto cestou, můžeme se pustit do analýzy výdajů na cloud a jejich optimalizace. To vyžaduje i definici parametrů reportů, na jejichž základě může podnik sledovat, predikovat a optimalizovat výdaje na cloudové služby," uzavírá Vladimíra Desková ze SoftwareONE.

Schopnost sledovat a řídit veškerý softwarový majetek a cloudové zdroje na jednom místě je klíčem k efektivnímu řízení životního cyklu softwaru (Software Lifecycle Management). Organizace přitom potřebují řídit životní cyklus softwaru a cloudových zdrojů od okamžiku jejich nákupu až po jejich vyřazení z používání. Získání takového přehledu a kontroly pomůže firmám optimalizovat náklady na software a cloudové služby.

> Důležitou součástí monitoringu cloudových služeb jsou rovněž nástroje na plánování a predikci spotřeby cloudových zdrojů.

EK014490

Digitalizace dokumentů firmám šetří čas i peníze. Jak funguje v praxi?

Velké množství dokumentů, které zaměstnanci zpracovávají ručně, je možné snadno digitalizovat. Automatizovat můžeme všechny kroky zpracování – od převzetí dokumentů, roztřídění, vytěžení dat, kontrolu dat až po nahrání dat do interních systémů.

Čím dříve v procesu začne organizace pracovat se strukturovanými digitálními daty, tím méně časově náročný a chybový je každý další krok. Ruční zpracování dokumentů přirozeně trvá déle, navíc hrozí riziko zanesení lidských chyb. Například při zpracování dokumentů nezbytných pro schválení bankovního úvěru, jako je potvrzení o příjmu či bankovní výpisy, je efektivnější získat vstupní data v digitální podobě přímo od žadatelovy banky než vyžadovat papírové dokumenty.

Ale například i mzdová oddělení firem se denně potýkají s velkým množstvím dokumentů pro ruční zpracování. Díky naší aplikaci Daňovka mohou zaměstnanci jednoduše a online vyplnit Žádost o Roční zúčtování daně či Prohlášení poplatníka daně z příjmu fyzických osob. Daňovka je provede každým krokem vyplnění, zajistí validaci vyplňovaných informací a ve spojení s plně digitální komunikací šetří čas zaměstnanců i mzdových účetních a pomáhá udržovat pořádek v dokumentech.

Co ale dělat, pokud je digitalizace dat hned na vstupu příliš složitá na implementaci nebo není finančně rentabilní? V takovém případě přicházejí na řadu nástroje, které umí zajistit digitalizaci dat z dokumentů přijatých v různých formátech (obrázky, PDF aj.) a vytěžit jejich obsah do struktury, se kterou již mohou pracovat další interní systémy (např. xml).

Ve finančním sektoru například náš moderní nástroj DocumentAnts dokáže automaticky rozpoznat a vytěžovat informace z rozvah, výsledovek či daňových přiznání. Zatímco zaměstnanci by kontrola a přepsání dat z výkazu do interního systému trvaly i desítky minut, chytří mravenci sami najdou potřebné informace a vše zpracují za zlomek času. Navíc je možné naučit naše mravence vytěžovat téměř jakýkoliv typ dokumentu, takže mohou najít využití i v mnoha jiných odvětvích.

Ing. Václav Trnka,
Product Manager ve společnosti StringData

stringdata

Váš strategický partner pro digitalizaci | www.stringdata.cz

EK014540

O kybernetické bezpečnosti se hodně mluví, ale reálné kroky chybí

Není třeba znovu objevovat kolo, dobrá praxe a standardy existují.

Jak hodnotíte úroveň ochrany v rámci nakládání s citlivými daty ve veřejné správě?
O nutnosti řešit cyber security se hodně mluví, ale reálné kroky často chybí. K potřebným investicím do technologií a lidí se přistupuje často až potom, co je organizace reálně zasažena, protože „nám se to přece nemůže stát." Přičemž není třeba znovu objevovat kolo, dobrá praxe a standardy existují. Pro oblast kybernetické bezpečnosti platí tzv. „Zákon o kybernetické bezpečnosti", který myšlenkově vychází z rodiny ISO 27000. Důležité je rovněž i vzdělávání uživatelů. Už jen cvičné phishingové kampaně mohou naučit uživatele rozeznávat podvržené maily a správně reagovat.

Na kterou oblast zabezpečení se zapomíná?
Narušení firemní infrastruktury útočníkem často vede k úniku citlivých dat nebo narušení procesů. To může znamenat nejen finanční ztrátu, ale i poškození reputace a v krajních případech může dojít i na odpovědnost statutárního orgánu. Běžná bezpečnostní opatření dnes staví na zajištění perimetru prostřednictvím firewallů a ochrany koncových bodů. Nicméně mezi perimetrem a koncovými body se nachází rozsáhlá firemní infrastruktura, které je věnováno jen málo pozornosti a to je problém. Na celou řadu systémů totiž nelze nainstalovat ochranu koncových bodů. Ve skutečnosti tak zjistíte, že chráníte sotva polovinu zařízení. Řešením je monitorování a analýza síťového provozu s cílem detekovat bezpečnostní incidenty a anomálie.
V této oblasti se s naší vlajkovou lodí – řešením Progress Flowmon – pohybujeme již více než 15 let. Z původně akademického projektu a startupu jsme se vypracovali na jednoho z mála globálních hráčů v oblasti NPMD (Network Performance Monitoring & Diagnostics) a NDR (Network Detection & Response).

Pavel Minařík,
VP Technology, Progress.

A co ransomware?
Ten vás vždy dostane do nepříjemné situace. Zejména, pokud jej odhalíte příliš pozdě. Typický útok, jehož cílem je zašifrovat data, trvá dny až týdny. Jakmile dojde k zašifrování dat, je už pozdě. Je proto potřeba zaujmout realistický přístup a změnit paradigma z „budeme chránit a předcházet" na „musíme rovněž detekovat a reagovat". Zde se naplno ukazují výhody našeho řešení Progress Flowmon. Nespoléhá jen na signatury nebo reputační databáze, ale v reálném čase vyhodnocuje chování všech zařízení na síti včetně šifrovaného provozu. Díky tomu dokáže ransomware odhalit včas a zabránit rozsáhlým škodám, jak potvrzuje celá řada našich zákazníků.

GIRITON

Domluvme si schůzku a ukázku systému:

+420 728 543 275 | **info@giriton.com**

Docházkový systém

Chtějte od svého docházkového systému **maximum**.

www.giriton.com

Moderní docházkový systém

Evidence docházky, služebek, homeofficů, přesčasů, hlídání zůstatků dovolených, stravenek, noční, práce o víkendu, ve svátek, osoby na pracovišti, příplatky na míru...

Žádosti

Podávání a schvalování žádostí (o dovolenou i další aktivity) z píchaček, mobilní appky i z webu, včetně dodržení nastavených limitů...

Plány směn

Plánování směn, registrace na směny a ohlídání limitů osob přihlášených na směny. Dodržení legislativy (povinné odpočinky atp.), žádosti o změny směny...

Čas na projektech

Vykazování práce na projektech a zakázkách, výpočet nákladovosti projektů, úprava hodinové odměny dle projektu...

Tiskové sestavy a exporty

Desítky tiskových sestav, které lze ukládat i do excelu, exporty do mzdových systémů, exporty na míru a REST API.

Plánované úlohy, notifikace

Hlídání přítomnosti na pracovišti, notifikace o 300 hod u DPP, konci zkušební doby, konci prac. smlouvy, automatické notifikace o neočekávaných událostech.

Docházka GIRITON je moderní řešení s jednoduchým ovládáním, snadným napojením na ERP, CRM, mzdy atd. Zakládáme si na rychlé technické podpoře na telefonu, emailu i vzdálené ploše a systém konfigurujeme klientovi přímo na míru. Kromě docházky, přesčasů, stravenek, služebních cest nebo třeba vykazování času na jednotlivých projektech podporujeme i další pokročilé agendy.

+420 728 543 275 | **info@giriton.com** | **www.giriton.com**

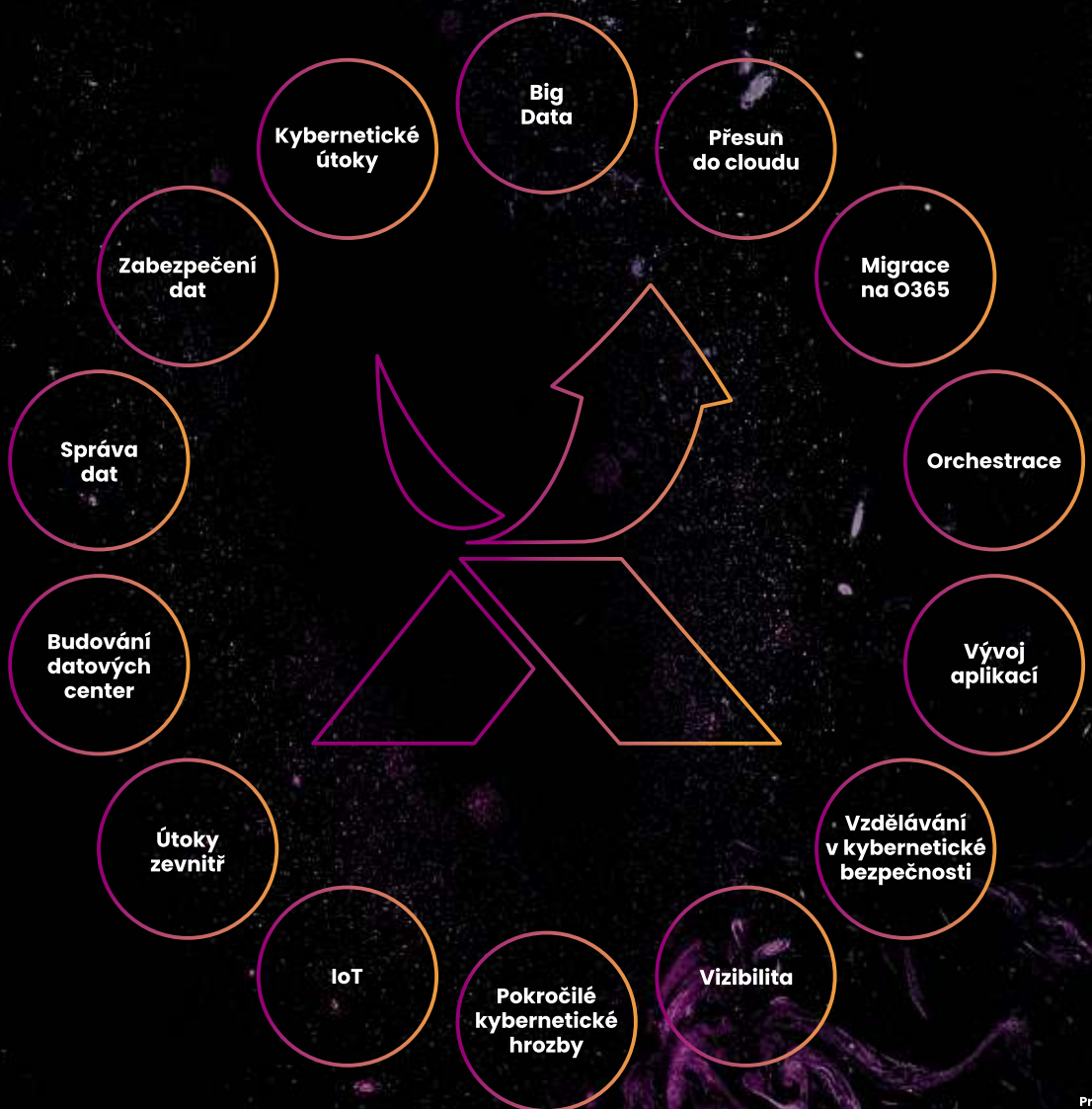
EK014497

Váš globální specialista na kybernetickou bezpečnost pro digitální infrastrukturu

Exclusive Networks Czechia

Naše vize plně důvěryhodného digitálního světa je poháněna nejlepším technologickým portfoliem ve své třídě.

Nabízíme produkty pro všechny businessové výzvy dnešních dní:



Prozkoumejte naše produktové portfolio

EXCLUSIVE NETWORKS

Exclusive Networks Czechia s.r.o. | Šafaříkova 201/17 | 120 00 Praha
IČ: 28321561 | DIČ: CZ28321561 | Tel: +420 724 647 785 | E-mail: info@exclusive-networks.cz
www.exclusive-networks.cz

EK014274