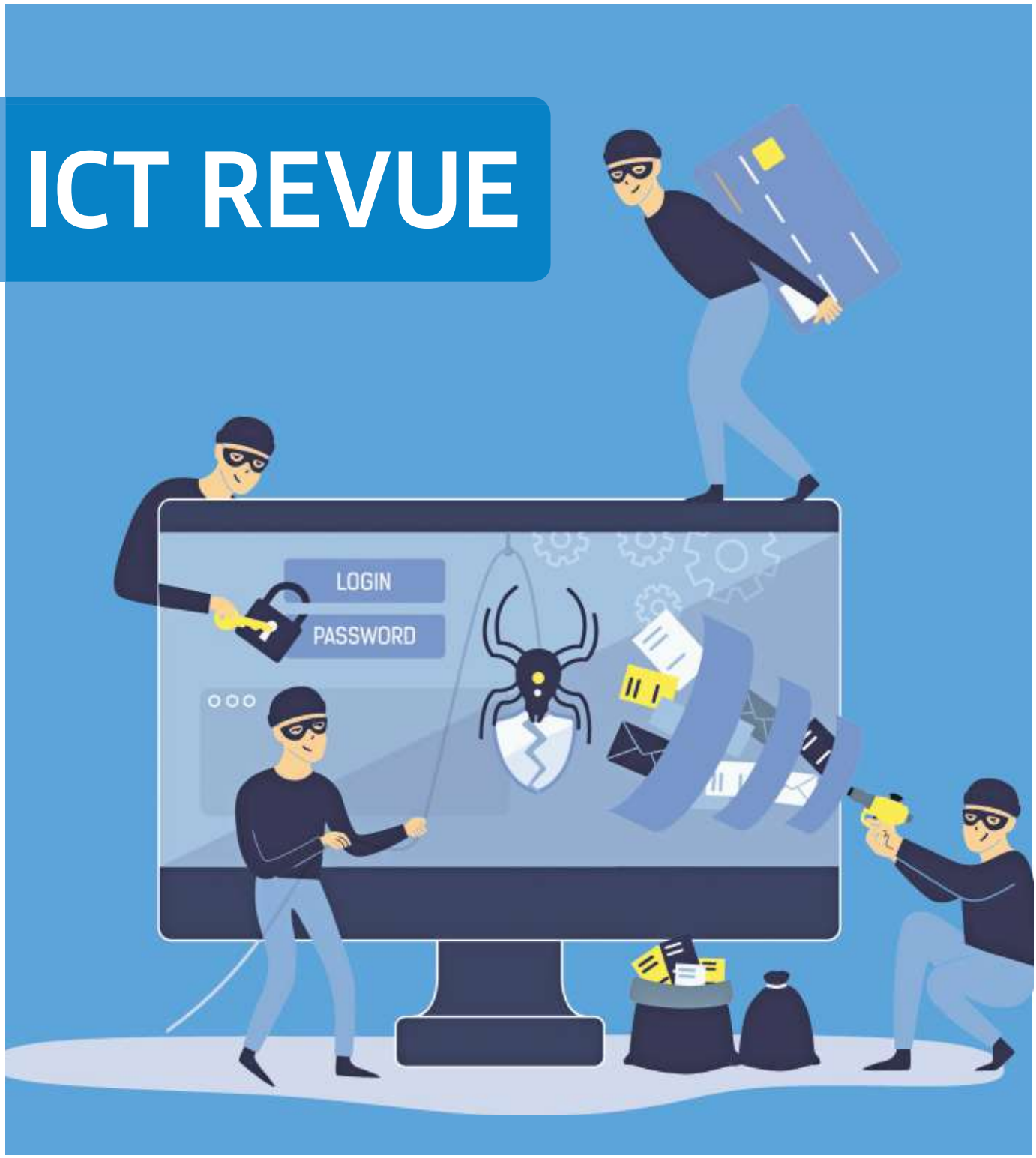
TEMATICKÝ MAGAZÍN VYDAVATELSTVÍ ECONOMIA A.S.

Samostatně neprodejné
4 | 2022

ICT REVUE



Kyberbezpečnost

Ransomware ohrožuje i partnery a zákazníky napadených firem.

ERP systémy

Podnikové informační systémy se mění v otevřené integrační platformy.

Low code / no code

Chcete nové aplikace? S moderními nástroji na jejich modelování si je vyvinete sami.

EDITORIAL

Martin Knížek
editor speciálních projektů

Vážené čtenářky, vážení čtenáři,

podle nedávného rozsáhlého průzkumu společnosti Salesforce mezi 23 tisíci pracovníky v 19 zemích si většina současných i budoucích zaměstnanců myslí, že jim chybí odpovídající dovednosti, které by je připravily na digitální budoucnost. V indexu připravenosti na digitální dovednosti získali pracovníci v 19 zemích průměrně 33 bodů ze 100 možných v oblastech, jako je připravenost, přístup ke vzdělávání, úroveň dovedností či účast na školeních. Obecně se předpokládá, že vyspělé země a mladší generace se cítí být lépe připraveny na digitální dovednosti, které vyžadují dnešní pracovní pozice. Zjištění společnosti Salesforce však tyto předpoklady zpochybňují.

V průzkumu se pouze 31 procent respondentů z generace Z – první skutečně digitálně nativní generace – označilo za „velmi dobře vybavené" pro práci v digitální oblasti. A pouhých 18 procent si myslí, že má pokročilé digitální dovednosti v oblasti kybernetické bezpečnosti.

Není proto ani moc překvapivé, že nejsnazší cesta kyberútočníků do firemních sítí vede právě přes nedostatečně poučené uživatele. Angela Gunnová, výzkumnice kyberbezpečnostních hrozeb ve společnosti Sophos, v rozhovoru říká, že pro útočníky je levnější vyvinout přesvědčivý sociálně inženýrský útok než najít nové technické taktiky nebo překonat bezpečnostní obranu firemních sítí.

Podobným způsobem byla vedena i série nedávných útoků skupiny Lapsus$ na největší světové technologické firmy. Během několika týdnů skupina ukradla a zveřejnila interní data Samsungu, Ubisoftu, Microsoftu nebo třeba Nvidie. Jejich taktika využívala jak e-mailové phishingové kampaně, tak například inzeráty nabízející desítky tisíc dolarů za přístup do interních sítí.

Kromě krádeží dat a vydírání firem pomocí hrozby jejich zveřejnění se útočníci stále častěji uchylují i k vydírání zákazníků a obchodních partnerů napadených společností, čímž zvyšují tlak na zaplacení výkupného.

MAGAZÍN ICT REVUE – PŘÍLOHA HOSPODÁŘSKÝCH NOVIN, 13. 4. 2022 a MAGAZÍNU EKONOM, 14. 4. 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

text: Lukáš Kříž
foto: Shutterstock

Systémy ERP se mění v otevřené integrační platformy

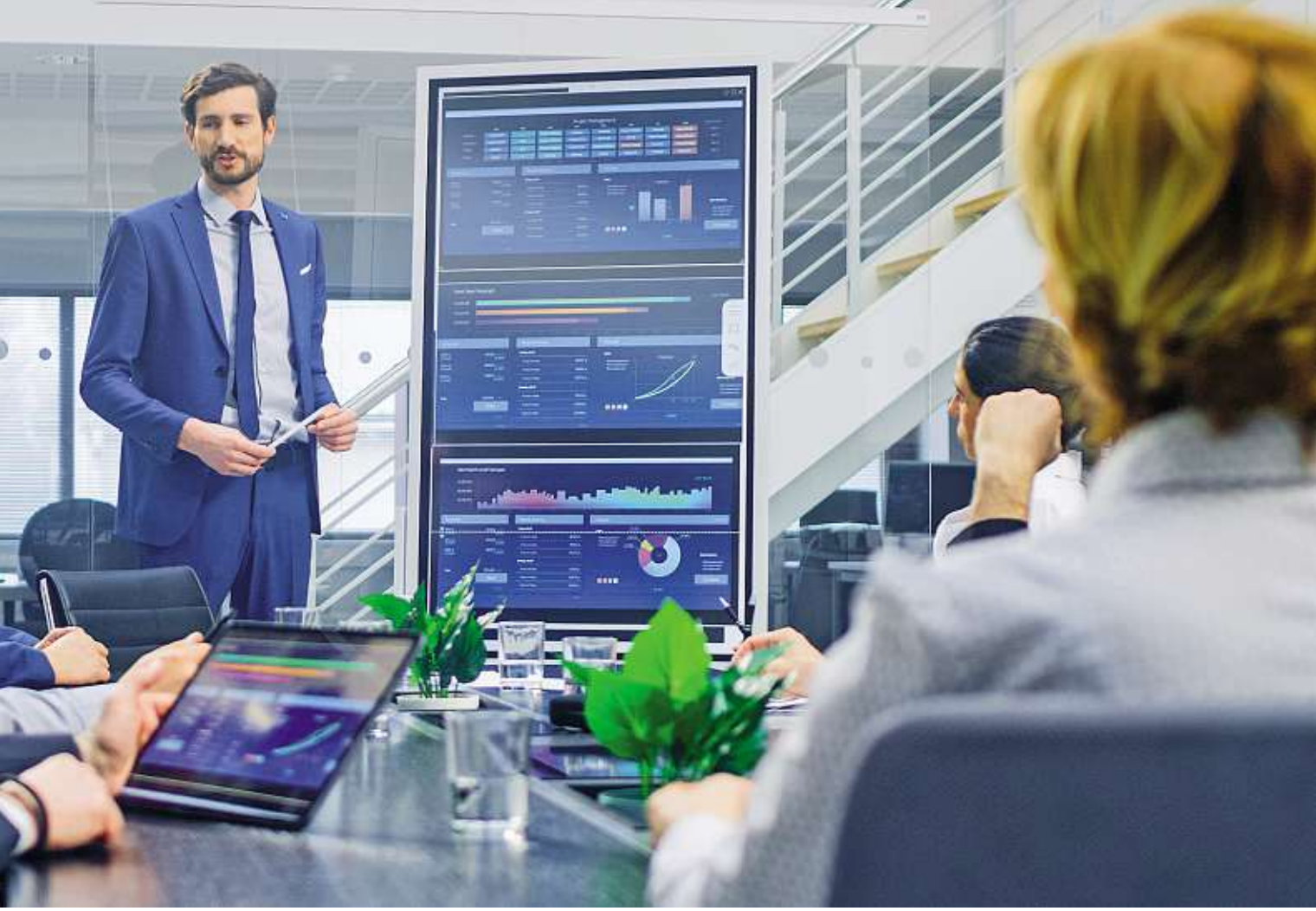
Firemní investice do informačních technologií v loňském roce díky ekonomickému oživení a sílícímu optimismu rostly. Důvěra v budoucí vývoj ale nebyla jediným jevem, který doprovázel očekávání spojovaná s koncem pandemie. Specialisté společnosti Panorama Consulting ve své zprávě ERP Report 2022 uvádějí, že zájemci o nové systémy pro řízení podnikových zdrojů neboli ERP zdůvodňovali motivy jejich pořízení především efektivitou, mobilitou a zdokonalením procesů. Přímo či nepřímo reagovali na dva nové aspekty byznysu, jež zviditelnilo pandemické období.

Organizace musí do budoucna počítat s hrozbou rozsáhlých narušení dodavatelských řetězců a s vynucenou absencí zaměstnanců na pracovištích. Zatímco první zkušenost zjevně přetrvá a zvýší četnost svého výskytu i kvůli probíhajícímu válečnému konfliktu na Ukrajině, druhá mnoha podnikům otevřela cestu k praktickému ověření alternativních či hybridních pracovních modelů. Dnes od nich odvíjejí potenciální úspory plynoucí z redukcí kancelářských prostor, a navíc dosahují větších úspěchů a efektů při slaďování profesních a osobních životů zaměstnanců.

Výběr softwaru a změny v zavádění

V současném vysoce konkurenčním prostředí nezbývá organizacím nic jiného než postupně nahrazovat své zastaralé podnikové systémy moderními. Podle konzultantů společnosti Panorama Consulting totiž roste potřeba efektivního a rychlého zpracování dat. Bez analytického vhledu do vývoje provozu a hospodaření podniku lze jen obtížně zlepšovat zákaznickou zkušenost nebo optimalizovat procesy v dodavatelském řetězci. Konkurence navíc analogické operace provádí v reálném čase a nad velmi rozsáhlými soubory dat. To jsou vlastnosti a schopnosti, jež starým aplikacím z oblasti ERP obvykle chybí.

Rozhodnutí o pořízení nového informačního systému by mělo zohledňovat cíle a potřeby organizace v pěti- až desetiletém horizontu. Následně dojde na výběr vhodných aplikací. Doba, kdy podniky volily řešení jednoho dodavatele, už skončila. Většina jich, jak dokládá zpráva ERP Report 2022, kombinuje produkty více výrobců. Aplikují přístup označovaný termínem best-of-breed, tedy nejlepší produkt v dané kategorii či daného typu. Vedle specializovaných



Bez analytického vhledu do vývoje provozu a hospodaření podniku lze jen obtížně zlepšovat zákaznickou zkušenost nebo optimalizovat procesy v dodavatelském řetězci.

Do světa podnikových informačních systémů vstupuje trend různorodosti. Proniká do všech jeho dimenzí, ale v principu má jedinou oběť. Tou jsou zastaralé systémy pro řízení podnikových zdrojů, jež v současném prostředí obstojí už jen výjimečně.

samostatných programů a služeb využívají částečně nebo plně integrované.

„Výběr dodavatele ERP je úzce spjatý s tím, jak podnik uchopí digitální transformaci. Některé přistupují k digitalizaci jako k jakési skládačce a vybírají si jednotlivé stavební kameny izolovaně. Jiné naopak vybírají mezi ERP, jež co nejvíce pokryjí jejich klíčové procesy," říká Ivo Procházka, senior local sales representative ve společnosti Ness Czech.

Klíč pro optimální volbu řešení a jejich dodavatelů představují prioritní funkční oblasti. Potřeby podniku, který do popředí staví provoz a správu dodavatelského řetězce, budou výrazně odlišné od potřeb firmy s preferencí rozvoje zákaznické zkušenosti. „Dávno pryč jsou časy, kdy firmy přicházely s požadavkem: ‚Máme dané procesy, nasaďte na ně ERP.' Dnes zákazníci spolu s implementací očekávají nejen pokrytí firemních procesů, ale také přidanou hodnotu ve formě informací, které posunou jejich byznys dál. Očekávají doplnění know-how z daného oboru, chtějí zkušeného implementačního partnera," rozvíjí téma výběru dodavatele Tomáš Smutný, generální ředitel společnosti QI Group.

Zpráva ERP Report 2022 naznačuje, že častý přístup organizací k výběru počítá s implementací řešení od některého velkého dodavatele. Následně jej rozšiřují o další moduly stejné provenience nebo o nástroje a doplňky třetích stran. „Z pohledu majority lze konstatovat, že stále dominuje ortodoxní přístup v podobě univerzálního komplexního ERP. Ale situace se mění a jsou vertikály, kde již dominují řešení specializovaná, složená z více heterogenních subsystémů," říká k tématu výběru dodavatele Lukáš Ontl, vedoucí oddělení inovací a rozvoje produktů ve společ-

nosti Asseco Solutions. „Osobně si myslím, že doba komplexních univerzálních řešení již svůj boom zažila a v této oblasti nás čeká významná transformace. Tím neříkám, že tato ERP řešení již nebudou mít tržní potenciál, ale věřím, že se bude postupně snižovat ve prospěch heterogenních řešení pracujících na jednotné datové, či spíše integrační platformě."

Přístup tuzemských průmyslových podniků přibližuje také Vladimír Bartoš, ředitel pro strategii ve společnosti Minerva Česká republika: „Čím hlouběji se české výrobní podniky v digitalizaci pouštějí, tím méně jsou použitelní univerzální dodavatelé systémů ERP. Naši zákazníci dnes hledají nejen dodavatele informačního systému, ale i partnera, který jim řekne, jak změnit podnikové procesy, aby byly co nejefektivnější, a pak jim změnu pomůže zrealizovat."

Převaha cloudového modelu

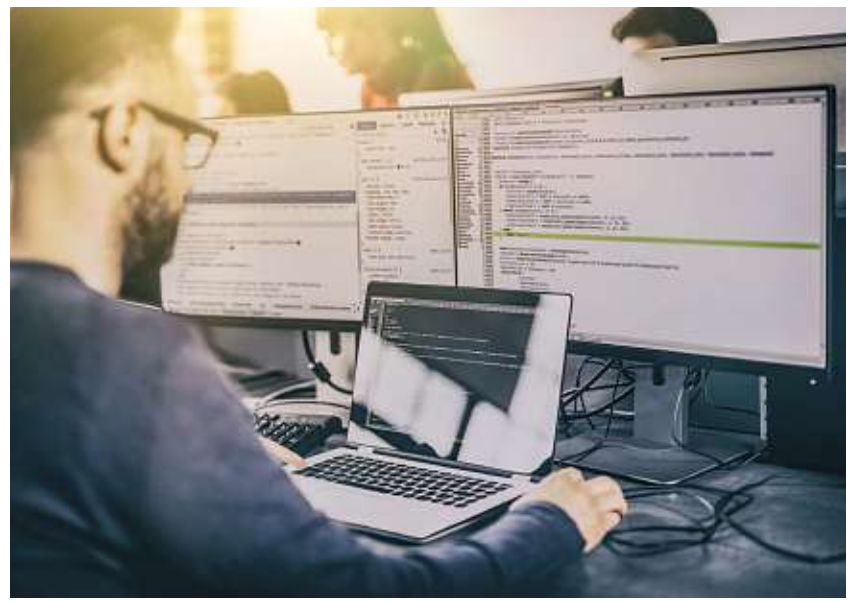
K poměrně zajímavým zjištěním letošního ročníku studie společnosti Panorama Consulting patří relativní neatraktivnost čistě cloudových podnikových systémů. V dotazovaném vzorku je sice do svého aplikačního mixu zařadilo 65 procent respondentů, zbývajících 35 procent ale upřednostnilo model on-premises. Cloudové aplikace mají za sebou bezmála 20 let vývoje, prokázaly své kvality a zejména nabízejí vysoký integrační komfort. Konzultanty společnosti Panorama Software výsledek rovněž překvapil. Důraz kladený na zpracování dat v reálném čase vede podniky k přirozenému nasazení a využití cloudových technologií.

Proč se organizace vyhýbají cloudovým systémům? Více než třetina z těch, které tak loni učinily, se odvolává na riziko bezpečnostního selhání. Zhruba 16 procent se obává ztráty dat nebo problémů s konektivitou. Necelých pět procent dotazovaných organizací nemá o cloudových řešeních dostatek informací. Přibližně desetina volí on-premises kvůli nákladům a šest procent kvůli obavám z problematické integrace. Poslední uvedená položka se ale v praxi nejspíše týká jen napojení na zastaralé systémy.

„ERP systém provozujeme v modelu on-premises. Prioritně jsme se rozhodli pro toto řešení na základě strategického rozhodnutí vedení společnosti. Chceme mít všechny důležité interní aplikace s firemními daty ‚doma'," objasňuje preferenci aplikací provozovaných na interním hardwaru Jan Havlík, vedoucí procesního oddělení ve společnosti Fermat CZ.

V rámci cloudové taxonomie zavedli konzultanti společnosti Panorama Consulting specifickou klasifikaci. Za cloudové řešení považují aplikace hostované, poskytované třetí stranou nebo odebírané v režimu software jako služba (SaaS). A poslední uvedená varianta patří k nejpopulárnějším. Mezi podniky, jež zvolily cloudové řešení podnikového informačního systému, ji preferovalo bezmála 64 procent.

Model SaaS s sebou nese řadu pozitiv, ale není ani bez negativ. „Vnímám dvě základní výhody cloudového modelu," říká Milan Tesař ze společnosti InfoConsulting Czech. „V případě renomovaných dodavatelů bude cloudový provoz vždy bezpečnější, protože investice těchto poskytovatelů do bezpečnosti jsou zcela neporovnatelné s tím, co dokáže investovat standardní podnik. Druhý aspekt souvisí se změnou pohledu na IT v podniku. Obvykle nemá smysl zaměstnávat lidi, kteří se zabývají technickými aspekty provozu ERP řešení. Daleko větší smysl má mít lidi s přesahem do byznysu, kteří dokážou ERP řešení operativně konfigurovat a nastavovat v souladu s tím, co podnik aktuálně potřebuje."



Přizpůsobování systémů na úrovni kódu ale má svou cenu a nelze jej doporučit pro každý podnik a situaci. Prioritně by organizace měly vytěžit maximum z konfigurace a personalizace.

> Doba, kdy podniky volily řešení jednoho dodavatele, už skončila.

Digitální transformace

Pojem digitální transformace zastřešuje různorodé projekty, které se typicky věnují modernizaci provozovaných informačních technologií, optimalizaci aktivit v digitálním prostoru nebo tvorbě nových digitálních obchodních modelů. Tvůrci zprávy ERP Report 2022 se respondentů dotazovali i na souvislost jejich loňské implementace systému ERP a digitálního směřování. Identifikují tak nejen roli této kategorie softwaru v organizaci, ale do jisté míry i její pozici v transformačním trendu.

Bezmála třetina respondentů zařadila implementaci ERP mezi projekty digitální transformace. Více než čtvrtina se spokojila s méně ambiciózní či honosnou kategorií, v níž technologie zdokonalují byznys. Zhruba dvě pětiny dotazovaných firem se spokojily s prostým konstatováním, že šlo jen a pouze o implementaci systému ERP. „Příslušné projekty organizace často prezentují jako součást digitální transformace. Reálně se však povětšinou jedná o obnovu podnikového informačního systému. Aby mohly být takové projekty plnohodnotnou součástí digitální transformace, musí podniky k modernizaci přistupovat holisticky a komplexně, s cílem postupně zdigitalizovat a zautomatizovat všechny podnikové

procesy. Ne všechny se totiž odehrávají v ERP," dodává Ivo Procházka ze společnosti Ness Czech.

Digitální transformace obvykle zahrnuje detailní rozbor zákaznických potřeb a očekávání, stejně jako zásadní rekonfiguraci podnikových procesů. S implementací ERP se pojí méně rozsáhlé a významné změny v organizaci. „Úvaha o ERP by měla být součástí digitalizační strategie, protože ERP je obvykle považováno za jednotnou datovou základnu v rámci podniku, kolem které lze budovat další specializované digitalizační iniciativy. Moderní ERP může být tím, co tyto oddělené iniciativy propojí do funkčního celku napříč celou společností," dodává Milan Tesař, obchodní ředitel InfoConsulting Czech.

Žádaná přizpůsobení

Podnikové informační systémy obvykle nevyhovují plně zavedeným procesům v organizaci. Část specifických požadavků lze řešit konfigurací a personalizací, část požadovaných úprav si ale vyžádá mírné či výrazné přizpůsobení aplikace, za hranicí její standardní funkcionality.

O tom, že přizpůsobení stále patří mezi běžné aktivity implementačních projektů ERP, svědčí i výsledky průzkumu a zprávy ERP Report 2022. Téměř polovina respondentů uvedla, že jejich systém prošel mírným přizpůsobením. Skoro 16 procent dotazovaných indikovalo výrazné zásahy. Jen necelá čtyři procenta systémů byla nasazena do provozu okamžitě po instalaci, a to i bez konfigurace a personalizace.

Vysvětlení vysokého rozšíření přizpůsobení systémů ERP je dvojí. Některé organizace provozují natolik unikátní procesy, že je konfekční informační systém nedokáže postihnout. Jiné si zase přizpůsobením zajišťují konkurenční výhodu. V praxi to znamená, že obě skupiny dělají věci jinak než jejich okolí.

„ERP systém jsme si museli při upgradu v některých ohledech přizpůsobit programovými úpravami. Šlo ale o podstatně menší úpravy než v roce 2012 při první implementaci. Nyní jsme systém přizpůsobovali především kvůli zjednodušování a automatizaci práce," přibližuje vlastní zkušenost Jan Havlík ze společnosti Fermat CZ.

> “ Digitální transformace obvykle zahrnuje detailní rozbor zákaznických potřeb a očekávání, stejně jako zásadní rekonfiguraci podnikových procesů. S implementací ERP se pojí méně rozsáhlé a významné změny v organizaci.

Přizpůsobování systémů na úrovni kódu však má svou cenu a nelze jej doporučit pro každý podnik a situaci. Prioritně by organizace měly vytěžit maximum z konfigurace a personalizace. Je navíc otázka, jak k tématu přizpůsobení systému a ke zveřejněným hodnotám přistupovat v případě převažujících cloudových aplikací. „Je zcela běžné, že systémy nabízejí nějaký rozsah pokrytí funkčnostmi, ale zákazník očekává ještě toto a tamto. Proč ne, ale vše má své plusy i minusy," říká Tomáš Smutný ze společnosti QI Group a dodává: „Mezi nevýhody z pohledu implementátora patří složitá údržba zakázkových úprav. Zákazníka takové řešení stojí víc peněz. Je ale jasné, že základ systému ERP nemůže nabídnout vše, a tudíž se bez zakázkových úprav nikdo ani v budoucnu neobejde."

Nasazení nového informačního systému do provozu může proběhnout v různých variantách. Pětina organizací průzkumu ERP Report 2022 zaváděla nová řešení po modulech, 12 procent po lokalitách a osm procent po útvarech. Přes 16 procent respondentů zrealizovalo operaci zvanou velký třesk. V jejím rámci přešla na nový systém celá organizace najednou. Dvě pětiny dotazovaných aplikovaly kombinovaný neboli hybridní přístup, jenž ve vyšším detailu reflektuje potřeby a možnosti organizace.

„Po základní implementaci nového systému v závěru roku 2020 následovalo v roce 2021 jeho další rozšiřování o workflow, příprava na implementaci modulu Nájmy, Správa pohledávek a podobně," říká Michal Kubišta, finanční manažer společnosti Cimex Invest, a dodává: „Přizpůsobování softwaru běží v oboustranném směru neustále od doby implementace. Jde o customizaci softwaru, jakož i rozvíjení a doplňování dalších modulů do ERP tak, jak jsme schopni standardizovat interní podnikové procesy v oblastech řízení pohledávek, řízení majetku, řízení oběhu dokumentů a dalších."

Výsledky a splněná očekávání

Plánovaný rozpočet splnilo 59 procent projektů, jež autoři zprávy ERP Report 2022 loni zkoumali. Meziročně jejich podíl vzrostl o 19 procentních bodů. Téměř desetina projektů navíc ani nedosáhla plánované úrovně rozpočtu. Zhruba třetina jej mírně překročila a necelá desetina výrazně. Za vyššími náklady nejčastěji stály organizační problémy, neočekávaná potřeba dalších technologií nebo komplikace se zaváděním dat.

Časové harmonogramy implementačních projektů loni v podstatě kopírovaly ty finanční. Přibližně polovina jich skončila přesně na čas, desetina dokonce dříve. Necelá třetina nabrala

Digitální transformace obvykle zahrnuje detailní rozbor zákaznických potřeb a očekávání, stejně jako zásadní rekonfiguraci podnikových procesů.

malé zpoždění a zhruba osm procent výraznější. Za zdržením nejčastěji stály technické problémy, obtíže s daty a organizační zádrhele.

„Každý projekt je tak trochu sázka do loterie. Klíčové atributy, které případná rizika minimalizují, jsou jednoznačně schopnost uživatele definovat své požadavky a následné profesionální vedení implementačního projektu zástupci obou stran. Samozřejmě že pochybení může nastat i na straně dodavatele. Takové případy mohou mít sice dopad do harmonogramu projektu, ale nikoliv do jeho rozpočtu," říká Lukáš Ontl ze společnosti Asseco Solutions.

Více než čtyři pětiny zkoumaných loňských projektů implementace ERP dosáhly očekávání

> Nejčastější příčinou skluzů v termínech jsou nepřipravená a nevyčištěná data.

v oblasti návratnosti investic. Dařilo se jim plnit předem nastavené laťky například v oblasti optimalizace skladových zásob, souladu s předpisy, interakce s dodavateli, standardizace nebo získávání a zpracovávání dat v reálném čase.

„Objektivně řečeno, nejčastější příčinou skluzů v termínech jsou nepřipravená a nevyčištěná data ze strany klienta," komentuje téma neplnění rozpočtů a harmonogramů Vladimír Bartoš ze společnosti Minerva Česká republika. Příčinou zdražení projektu také bývá žádost klienta, aby část služeb, které původně chtěl realizovat svými lidmi, provedl dodavatel. „Často také naši klienti rozšíří původní zadání projektu a s tím je pochopitelně spojeno navýšení nákladů," dodává Bartoš.

ANKETA

Jaká témata na trhu ERP systémů nejvíce rezonují? Jaké funkce jsou klíčové?

Vladimír Bartoš,
ředitel pro strategii společnosti Minerva ČR

Dodavatelé automobilového průmyslu vyžadují funkce rozvrhy a odvolávky spolu s EDI komunikací pro společné plánování dodávek se zákazníky a dodavateli. Všechny české výrobní firmy požadují pokročilé plánování výroby a řízení výroby spojené s digitalizací.

Lukáš Ontl,
vedoucí oddělení inovací a rozvoje produktů společnosti Asseco Solutions

Popisovat konkrétní funkcionality je složité. Výrobní firma má jiné nežli obchodní a potravináři jiné než strojaři. Ale pokud bych to trochu zobecnil, tak bezesporu rezonují témata jako business intelligence, automatizace rutinních operací, datová integrace a uživatelsky přívětivé prostředí.

Milan Tesař,
obchodní ředitel společnosti InfoConsulting Czech

Výrobci ERP adoptují nové technologie a přenáší je do smysluplné aplikace ve svých řešeních. Kladou důraz na automatizaci procesů, uplatnění strojového učení či na usnadnění propojenosti s vnějším světem, zejména s jinými informačními systémy nebo fyzickými zařízeními.

Na druhé straně, ERP by mělo mít vždy povahu strategického projektu a při výběru by měl zákazník nahlížet na to, jak dokáže systém podpořit jeho strategické cíle, jakými může být například rozšíření na další trhy, změna obchodního modelu, podpora udržitelné ekonomiky apod.

Ivo Procházka,
senior local sales representative společnosti Ness Czech

Zjednodušit současné prostředí, které je komplikované, v kterém se vyskytuje mnoho aplikací třetích stran, mnoho tabulek v Microsoft Excelu a mnoho manuálních předávek a intervencí. Komplexita podnikového prostředí firmy výrazně zatěžuje a neumožňuje se rychle a správně rozhodnout.

Tomáš Smutný,
generální ředitel společnosti QI Group

Nejvíce rezonujícími tématy z mého pohledu jsou digitalizace personální i mzdové agendy, napojení ERP na stroje a e-shopy nebo plánování výroby.

Dostupnost a lepší plánování

Role podnikových informačních systémů roste až do té míry, že bez jejich dostupnosti se firma zastavuje.

V současnosti nejen u výrobních firem stále více rezonuje dostupnost z jakéhokoliv místa, a proto i ERP QAD Adaptive využívá technologie, které jej zpřístupňují kdykoliv, kdekoliv a na čemkoliv. Firmy s dobře implementovanými či cloudovými ERP systémy měly v průběhu pandemie najednou obrovskou konkurenční výhodu. Zaměstnanci v karanténách se dokázali ze dne na den přesunout domů, připojit se do ERP a pracovat s aktuálními údaji. Nyní nastává další nová situace, se kterou se budou muset firmy vypořádat.

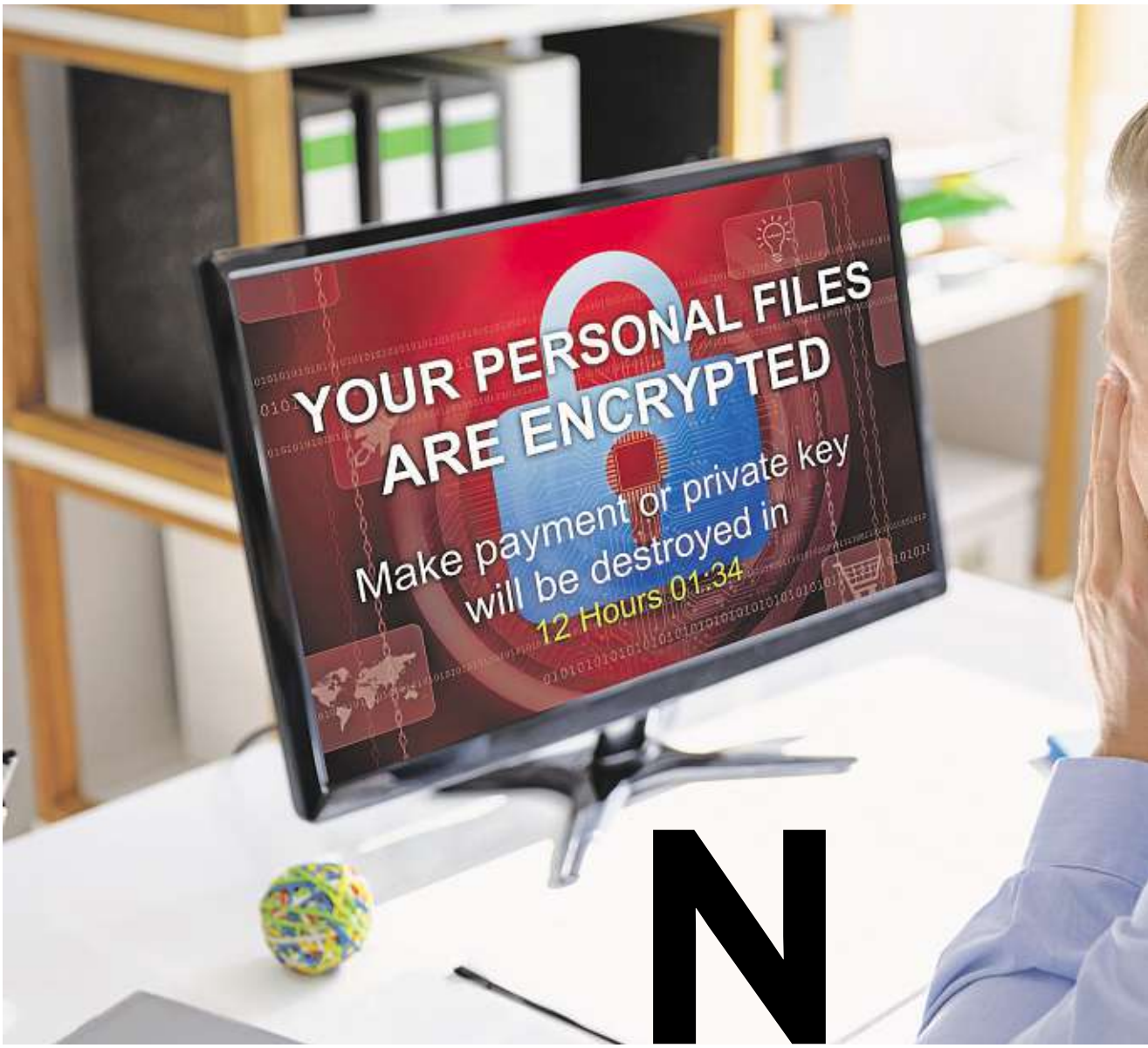
V oblasti funkcionality ERP systémů stoupá poptávka po přesnějším plánování výroby a nákupu, včetně optimalizace a rychlého přeplánování v případě nečekaných změn. Pomáháme rozvrhovat statisíce operací na různá pracoviště podle jejich specifik. Máme zákazníky, kteří vyčíslili přínosy na miliony korun ročně. V souvislosti s pandemií se zvýšil zájem o internetový prodejní a nákupní portál, který je integrovaný přímo v QAD Adaptive. Umožňuje samoobslužné a rychlejší obchodování. Dále rostou nároky na podporu rozhodování, které využijí všichni běžní uživatelé ERP. Tím vzrostla i potřeba analýzy klíčových uživatelů až na detailní transakce.

> V oblasti funkcionality ERP systémů stoupá poptávka po přesnějším plánování výroby a nákupu.

Minerva slaví letos třicet let od svého založení a právě díky dlouholetým zkušenostem s IT projekty ve výrobních společnostech se stala specialistou v oboru. Nerealizujeme pouze zadané dodávky, ale působíme na projektech i v roli poradce pro návrh efektivních podnikových procesů v daném odvětví, nasazení správných technologií a podpory konkurenceschopnosti konkrétního zákazníka.

Digitalizaci nově podporujeme také díky řešení pro digitální obchod od americké společnosti WebJaguar, nejlepšího poskytovatele řešení pro digitální služby. Společnost WebJaguar se stala součástí partnerské společnosti QAD a Minerva začne nabízet její produkty v našem regionu. Řešení Digital Commerce společnosti WebJaguar posiluje schopnosti kompletní správy zákazníků, což umožňuje vícekanálovou strategii prodeje. Jde o modulární a vysoce konfigurovatelné řešení a umožňuje zákazníkům snadno a rychle poskytovat personalizované webové nakupování, které je integrováno s ERP.

EK014152



Kyberzločinci: Zaplaťte vy i vaši zákazníci

a první pohled by se mohlo zdát, že dodavatelé bezpečnostních IT řešení s působností po celém světě zaznamenali v uplynulém roce celkem příznivý trend. Došlo totiž k mírnému poklesu kybernetických útoků prostřednictvím škodlivého softwaru (malwaru) v podobě virů, trojských koní a další „havěti“. Optimismus ale určitě není namístě, protože pohled na delší časovou osu ukazuje, že se v podstatě jen vracíme do „normálu“ po obrovském nárůstu množství malwarových útoků, zaznamenaných po lockdownech a rychlém přechodu na práci na dálku v souvislosti s koronavirovou pandemií.

Útočníkům se tím otevřela zcela mimořádná příležitost napadnout obrovské množství nových zařízení, která se začala vzdáleně připojovat do podnikových sítí. Samozřejmě tomu nahrávala i skutečnost, že rychlý přechod na práci z domu v mnoha firmách neposkytoval dostateč-

text: Radek Kubeš, foto: Shutterstock

Počet obětí vyděračského softwaru neustále roste. Přinejmenším o nějaká data přišlo vlivem ransomwarových útoků už 68 procent východoevropských organizací.

Na čele žebříčku kybernetických hrozeb se drží ransomware, ale to neznamená, že by se techniky kyberzločinců dále nevyvíjely. Stále častěji také dochází k trojímu vydírání, kdy se kromě požadavku na výkupné za dešifrování a nezveřejnění dat primární oběti ransomwaru obracejí kyberútočníci také na její zákazníky a partnery.

> V uplynulém roce zaznamenaly ransomwarové útoky více než dvě třetiny východoevropských organizací. Po těchto útocích se nepodařilo obnovit v průměru 32 procent ztracených dat.

ný prostor na pečlivé zabezpečení všech zařízení a vstupních bodů podnikových sítí. V průběhu loňského roku se situace zklidnila, firmy ošetřily největší mezery v zajištění vzdáleného přístupu ke svým aplikacím a datům a nasadily zabezpečení koncových zařízení.

Přípravy na válku

Velké obavy z hlediska kyberbezpečnosti ale v současnosti vyvolává i rusko-ukrajinský konflikt. Už v loňském roce Microsoft uváděl, že až 58 procent kybernetických útoků tolerovaných (spíše ale přímo podporovaných) vládami národních států pochází z Ruské federace. Data z bezpečnostního systému Turris Sentinel, který v reálném čase sleduje úroveň kybernetických hrozeb a za kterým stojí sdružení CZ.NIC, správce české národní domény, odhalují, že kyberútočníci z Ruska už 36 hodin před zahájením invaze na Ukrajinu výrazně zvýšili svoji aktivitu ve vyhledávání snadno napadnutelných internetových cílů na Ukrajině.

„Podrobnou kontrolou našeho bezpečnostního systému jsme zjistili přibližně desetinásobný nárůst cíleného monitorování snadno napadnutelných internetových cílů. Zmíněná aktivita proběhla krátkodobě v úterý 22. února krátce po poledni a pocházela výhradně z ruských IP adres," říká Petr Palán, šéf projektu Turris. „Tato aktivita spočívá ve velmi intenzivním vyhledávání jakékoliv služby dostupné z internetu, kterou by bylo možné napadnout. Během přibližně dvou hodin zachytila asi čtvrtina našich routerů, které sdílejí data se systémem Turris Sentinel, tyto snahy pocházející z Ruska. Z našeho pohledu nešlo přímo o útoky, ale o hledání míst napadnutelných následným útokem."

Na napadení stovek ukrajinských zařízení virem HermeticWiper těsně před vpádem ruských pozemních jednotek upozornila také společnost Eset. „První vzorky jsme zachytili ve středu 23. února v 16:52 místního času. Z analýzy malwaru vyplynulo, že vznikl již 28. prosince 2021, z čehož lze vyvodit, že útok byl připravován poslední dva měsíce," popisuje Michal Cebák, bezpečnostní analytik společnosti Eset. Úkolem malwaru HermeticWiper je smazat v napadených zařízeních uživatelská data – a tím je prakticky vyřadit z provozu. Před zahájením invaze čelila řada ukrajinských institucí také útokům typu DDoS (cílené zahlcení internetových služeb obrovským množstvím požadavků).

Současná situace se nutně promítá i do požadavků českých firem v oblasti kybernetické bezpečnosti, jak potvrzuje Kateřina Hůtová, manažerka systému řízení bezpečnosti informací ve společnosti SoftwareONE Czech Republic: „V souvislosti s aktuální situací vnímáme u našich zákazníků především zvýšenou poptávku po školeních a vyhotovení plánů pro udržení kontinuity činností organizace a obnovu po havárii. Společnosti chtějí být připraveny a schopny rychle reagovat na potenciální hrozby. Dlouhodobě s tím souvisí také stále větší vy-

Zálohu dat je v případě ransomwarového útoku, který se nepodaří odrazit nebo zastavit, nutné vnímat až jako poslední linii obrany. Aby byla účinná, doporučují odborníci rozšíření klasického modelu zálohování, spoléhajícího se na tři kopie dat na dvou úložných médiích s jednou kopií uloženou na geograficky vzdáleném místě, o další dva prvky (ilustrační foto).

užití cloudových služeb, což zvyšuje mobilitu zaměstnanců a možnost pracovat odkudkoliv.“ Podle Kateřiny Hůtové je současným trendem IT bezpečnosti také úspěšná prevence a detekce útoků a zálohování informací důležitých pro chod společnosti pro případ nutnosti přesunu společnosti či práce do jiné lokality.

Jedno vydírání už nestačí

Pokud bychom situaci kolem malwaru označili za „stabilizovanou“, vývoj kolem ransomwarových útoků jde neustále k horšímu. Například společnost SonicWall uvádí, že v loňském roce její bezpečnostní zařízení, umístěná u klientů po celém světě, zaznamenala 623 milionů ransomwarových útoků. To představuje nárůst o 105 procent oproti roku 2020, a dokonce trojnásobné zvýšení počtu útoků oproti roku 2019. Společnost Veeam ve své studii Data Protection Trends Report 2022 uvádí, že v uplynulém roce zaznamenaly ransomwarové útoky více než dvě třetiny (69 procent) východoevropských organizací (mezi které Veeam počítá i české podniky) a že se po těchto útocích nepodařilo obnovit v průměru 32 procent ztracených dat. Přinejmenším o nějaká data přišlo vlivem ransomwarových útoků 68 procent východoevropských organizací.

Globálně se počet ransomwarových útoků nejen rychle zvyšuje, ale současně zaznamenáváme i dva trendy, kterými se kyberzločinci vydávají. Tím prvním je zásadní snížení nezbytné vstupní úrovně znalostí pro provedení útoku. S pomocí nástrojů označovaných jako Ransomware as a Service (RaaS) může ransomwarové útoky provádět téměř kdokoliv. Stačí, když si formou služby pořídí příslušné nástroje, ke kterým jejich tvůrci poskytují dokonce i technickou podporu – tak jako to známe u běžného softwaru nebo cloudových služeb. Je nepochybné, že i kvůli RaaS a praktické nepostižitelnosti útočníků bude ransomwarových útoků jen přibývat.

Druhým, a snad ještě nepříznivějším trendem je dvojí, či dokonce trojí vydírání. Nový způsob vydírání spočívá v tom, že si kyberzločinci během ransomwarových útoků podniková data ještě před jejich zašifrováním zkopírují. Následně svým obětem vyhrožují, že ukradená data obsahující citlivé osobní informace nebo obchodní tajemství firmy publikují na internetu. Tím samozřejmě zvyšují tlak na své oběti, aby zaplatily výkupné. Mimochodem, společnost PurpleSec uvádí, že průměrné výkupné v roce 2021 meziročně vzrostlo o 82 procent na 570 tisíc dolarů.

Ale to ještě bohužel není konec špatných zpráv. Stále častěji dochází k trojímu vydírání, kdy se kromě požadavku na výkupné za dešifrování a nezveřejnění dat primární oběti ransomwaru obracejí kyberútočníci také na její zákazníky a obchodní partnery, které by mohlo zveřejnění odcizených dat rovněž poškodit. Opět jde o zvýšení tlaku na oběti, aby zaplatily výkupné, v tomto případě navíc s devastujícími následky na pověst a partnerské vztahy napadené firmy.

Konec proplácení výkupného

Vypadá to, že se zatím nedaří proti ransomwaru najít účinnou zbraň. Jen v loňském roce byly z celosvětově známých firem ransomwarem úspěšně napadeny například společnosti Accenture, Nvidia, Swissport, Puma, MediaMarkt a mnoho dalších. Trpělivost s kyberútočníky dochází už i pojišťovnám a vládám. Takže například pojišťovna AXA ve Francii oznámila, že nově uzavřené pojistné smlouvy na kybernetická rizika nebudou pokrývat výkupné zaplacené ransomwarovým útočníkům. O všeobecném zákazu proplácet náklady na výkupné z pojištění firem uvažuje nizozemská vláda. Omezení finančních zdrojů na zaplacení výkupného ale samo o sobě problém s ransomwarem nevyřeší.

I společnosti z oblasti kybernetické bezpečnosti a ochrany dat si uvědomují, že asi nebude možné absolutně zabránit proniknutí ransomwaru do podnikových sítí. Na počátku takových útoků totiž stojí zpravidla velmi promyšlená strategie, využívající sociální inženýrství a cílené útoky na uživatele, kteří nechtěně otevřou ransomwaru dveře do podnikové infrastruktury IT. Proto je nutné zaměřit se kromě detekce škodlivého softwaru a odvrácení útoků také na zmírnění následků a rychlou obnovu po úspěšném ran-

somwarovém útoku. Společnost Venafi přitom uvádí, že dvojité nebo trojité vydírání je dnes součástí až 83 procent úspěšných ransomwarových útoků. To znamená, že pro nápravu po takových útocích bohužel už nestačí obnovit data ze zálohy, protože vydírání bude hrozit i nadále.

Přidejte offline zálohu a šifrování

Firmy často sázejí na zálohy dat jako na spolehlivý nástroj pro rychlé obnovení provozu po ransomwarovém útoku. V praxi to ale tak jednoduché zase není – a nejde jen o výše zmíněnou třetinu dat, která se podnikům v průměru nepodaří obnovit. Veeam totiž ve své studii dále uvádí, že až 15 procent dat východoevropských organizací není zálohováno vůbec. A navíc ani existence zálohy ještě neznamená, že se podaří obnovit všechna data – a také v přiměřeném čase. Plných 85 procent východoevropských organizací podle společnosti Veeam trpí disproporcí mezi tím, jakou rychlost návratu k produktivitě očekávají a jaké ve skutečnosti dosahují.

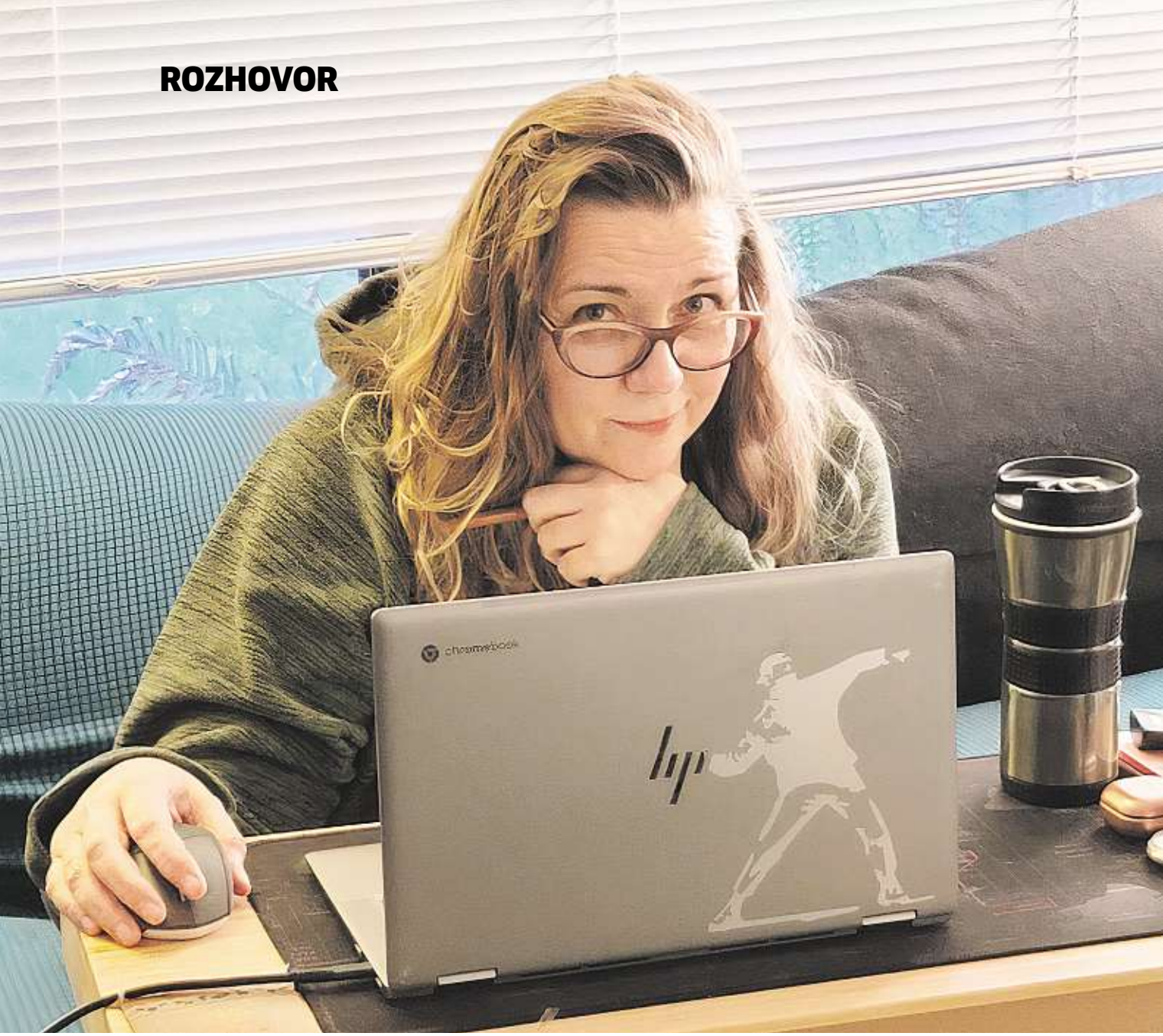
Zálohu dat je v případě ransomwarového útoku, který se nepodaří odrazit nebo zastavit, nutné vnímat až jako poslední linii obrany. Aby byla účinná, doporučuje Veeam rozšíření klasického modelu zálohování, spoléhajícího se na tři kopie dat na dvou úložných médiích s jednou kopií ulo-

> “
> Plných 85 procent východoevropských organizací podle společnosti Veeam trpí disproporcí mezi tím, jakou rychlost návratu k produktivitě očekávají a jaké ve skutečnosti dosahují.

ženou na geograficky vzdáleném místě, o další dva prvky. Model 3-2-1-1-0 přidává jednu offline kopii (tedy zálohu nepřístupnou z podnikové sítě, kterou nemůže ransomware napadnout) a nulovou chybovost při obnově dat ze zálohy (dosažitelnou především opakovaným testováním různých scénářů obnovy dat).

Zálohování ale samozřejmě nemůže posílit ochranu proti vícenásobnému vydírání. Účinným nástrojem je zde nasazení šifrování v maximální možné míře, stejně jako posílení ochrany přístupu k citlivým datům. Mezi účinná opatření patří především striktní kontrola přístupu uživatelů k datům, včetně omezení přístupových oprávnění jen na nezbytně nutnou míru a nasazení dvoufaktorového ověřování přístupu. Na vzestupu je také přístup k síti na principu nulové důvěry (zero trust network access), kdy jsou oprávnění jednotlivých uživatelů a jejich zařízení redukována na nezbytné minimum a současně je jejich přístup do podnikové sítě a ke zdrojům neustále ověřován.

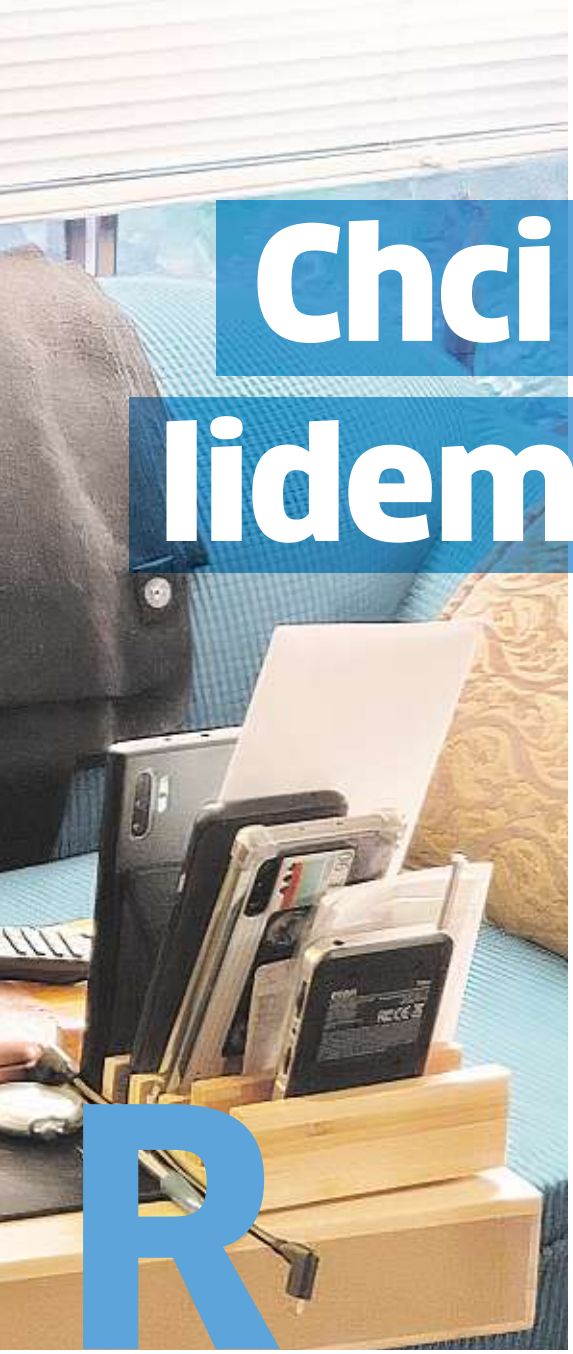
Jakkoli nemůžeme vědět, jaký vývoj kybernetických útoků nás v budoucnosti čeká, kombinace existujících nástrojů na detekci, zastavení a nápravu kyberútoků dává více než slušnou šanci útočníkům odolat – nebo alespoň minimalizovat škody.



Po kariéře oceňované technologické novinářky, autorky a televizní moderátorky se **Angela Gunnová** rozhodla vyzkoušet život na druhé straně reportérského zápisníku. Stala se výzkumnicí kyberbezpečnostních hrozeb ve společnosti Sophos, kde se specializuje na reakci na incidenty a ochranu osobních údajů – dvě oblasti, které jí umožňují, jak sama říká, „živit se řešením hádanek“.

text: Radek Kubeš, foto: archiv Angely Gunnové

Chci pomáhat lidem, aby byli silnější



Roky naléhavé a dramatické práce při řešení incidentů přivedly Angelu Gunnovou k otázce, jak řešit problémy kybernetické bezpečnosti dříve, než k nějakému incidentu dojde. Od toho už byl jen krůček k jejímu současnému výzkumu v oblasti navrhování atraktivních a účinných bezpečnostních školení pro netechnické lidi.

V posledních letech se zvýšil počet útoků ransomwaru. Změnilo se to v uplynulých týdnech v souvislosti s geopolitickou situací?
Skutečný ransomware, tedy situace, kdy útočník, který se dostane do systému, zašifruje v něm uložená data a požaduje po oběti peníze za jejich dešifrování, se v posledních týdnech zdaleka nevyskytuje tak často jako běžné podvody, zejména ty, kdy se zločinci snaží podvést lidi s dobrými úmysly, aby „přispěli“ na falešné charitativní organizace. To je bohužel běžný vzorec chování útočníků po přírodních katastrofách nebo jiných hrozných událostech, které zločinci zneužívají.

Jaké typy útoků tedy nyní převažují?
Všichni se přirozeně obávají možnosti větších kybernetických útoků a objevily se i zprávy o bezpečnostních incidentech s velkým dopadem, jako byl výpadek Viasatu nebo nešifrovaná válečná komunikace Rusů, která byla zachycena a manipulována. Je však překvapivé, k jak velkému množství nesofistikovaných útoků nebo pokusů o podvody z příležitosti dochází – ať už jde o prosté krádeže a podvody, nebo útoky typu DDoS (distribuované odepření služby), které zahlcují provoz na konkrétních cílových webových stránkách.

Jak velkou hrozbu představují trendy jako Ransomware as a Service nebo Cybercrime as a Service? Hovoříme o sofistikovaných útocích, nebo jde spíše o jednoduché nástroje v rukou amatérů?
Úroveň technických dovedností potřebných k používání těchto nástrojů a služeb je nízká, a o to jde – takovou službu může používat kdokoli. Problémem je, že i nekvalifikovaný útok může uspět, pokud cíl nereaguje na včasné náznaky takového útoku. Útočníci s nízkou kvalifikací mohou být neznalí, ale nejsou hloupí. Pokud si oběť nevšimne příznaků útoku a nechá ho nějakou dobu pokračovat, útočník se může na úkor oběti zdokonalovat ve svých dovednostech nebo může upozornit nějakého jiného útočníka, který ví, co dělá, a může oběti výrazně ztížit život.

Jak se v průběhu času vyvíjí podíl investic do kybernetické bezpečnosti na celkovém rozpočtu IT?
Určitě roste, protože si příslušní manažeři uvědomují zásadní důležitost kybernetické bezpeč-

> “ Je překvapivé, k jak velkému množství nesofistikovaných útoků nebo pokusů o podvody z příležitosti dochází.

Angela Gunnová

výzkumnice kyberbezpečnostních hrozeb ve společnosti Sophos

Specializuje se na reakci na incidenty a ochranu osobních údajů.

Před nástupem do společnosti Sophos pracovala téměř dvě desetiletí jako technologická novinářka, autorka či televizní moderátorka se zaměřením na kyberbezpečnost, vývoj softwaru a ochranu soukromí a osobních dat. Je autorkou několika knih a řady technologických publikací.

Mnoho zkušeností získala také v největších společnostech v oboru, jako jsou Microsoft, HPE a BAE Systems.

Vystudovala filozofii na Occidental College a je „certified information systems security professional" a „certified information privacy professional". Žije v Seattlu a těší se, jak se po pandemii vrátí ke svému oblíbenému cestování.

nosti. Jak covid, tak četné incidenty v oblasti kybernetické bezpečnosti v posledních několika letech zanechaly hluboký dojem. Investice do bezpečnosti rostly jistě i předtím, ale události posledních několika let vyvolaly skutečnou potřebu, aby kybernetická bezpečnost tvořila větší část rozpočtů na IT. A společnostem nyní nestačí pouze budovat „pevnost", ale musí být silné a zároveň odolné vůči aktuálnímu vývoji hrozeb. A to je společné úsilí. Je třeba, aby oddělení IT implementovalo bezpečnostní záplaty, konfigurace a další kvalitní kontrolní mechanismy. Potřebujete zabezpečení, abyste vytvořili vhodné zásady a postupy, a samozřejmě je nutné sledovat prostředí. Mnoho podniků si uvědomuje, že potřebují navázat chytrá partnerství s externími bezpečnostními odborníky, a to jak kvůli odborným znalostem, tak kvůli perspektivě.

Odhadujete na základě současné situace, že podniky a organizace budou investovat ještě více?

Všechny průzkumy, které jsem měla možnost vidět, ukazují, že ano, že je to jasný směr. A ohledně „současné situace" nezapomeňte na důležitou, ale možná nudnou věc, kterou je ochrana osobních údajů. Bezpečnost a soukromí patří k sobě a zákazníci právem očekávají obojí.

Odvětví kybernetické bezpečnosti se neustále vyvíjí a rozvětvuje. Je vůbec v možnostech podnikových týmů IT zvládnout celou problematiku?

Tradiční oddělení IT si každým dnem stále více uvědomují důležitost a složitost kybernetické bezpečnosti. Požadavek, aby oddělení IT řešilo všechny potenciální problémy kybernetické bezpečnosti, ale představuje riziko jeho zahlcení, protože má už tak důležitou a složitou práci. Najímání pracovníků v oblasti kyberbezpečnosti je však obtížné. Člověk, který je zběhlý v jedné oblasti bezpečnosti, může mít v jiné jen základní dovednosti. Bezpečnostní odborníci s hlubokými a aktuálními znalostmi všech významných aspektů kybernetické bezpečnosti jsou neuvěřitelně vzácní a jejich udržení v interním týmu je velmi nákladné, protože nemusí mít důvod využívat své specializované znalosti každý den. Vzestup řízených služeb – tedy zabezpečení jako služby – je skvělým a rozumným protipólem jak rostoucích nákladů, tak neustálého vývoje hrozeb.

Bude více společností využívat zabezpečení jako službu?

Tímto směrem se vývoj určitě ubírá. Je to praktický způsob, jak ve špičkové kvalitě uspokojit potřeby podniku a zároveň nechat záležitosti jako specializované odborné znalosti a monitorování hrozeb s nízkými náklady mimo podnik. Když se zákazníci spolehnou například na službu Sophos Managed Threat Response, získají výhody chytrého a důkladného bezpečnostního týmu, který se nezabývá ničím jiným než řešením hrozeb a dalších bezpečnostních problémů, bez dopadu na personální náklady firmy. Hlídáme bezpečnostní perimetr, aby se naši zákazníci mohli věnovat své vlastní práci, a sdělujeme jim, co vidíme a proč. Přirovnávám to k situaci, kdy máte rodinného lékaře nebo právníka na smlouvu – nepotřebujete specialisty každou hodinu pracovního dne, ale když je potřebujete, chcete ty nejlepší.

Jaká jsou úskalí outsourcingu kybernetické bezpečnosti?

Klíčová je komunikace. Na začátku vztahu je třeba si ujasnit, kdo bude za co zodpovědný, jaká doba odezvy se očekává, co je a co není v kompetenci poskytovatele služeb. Toto musí být zkrátka všem zúčastněným jasné a měly by existovat záložní plány pro případ, že původní plán nefunguje nebo že někdo nezvedá telefon. A je bohužel velmi snadné, aby se tento vztah mezi klientem a poskytovatelem služeb narušil. Pokud například klient provede velké změny v IT a nezapojí do nich poskytovatele bezpečnostních služeb, může to v případě krize vést ke ztrátě času a zbytečnému úsilí.

Pojišťovny chtějí přestat hradit výkupné za pojištěné společnosti napadené ransomwarem. Pomůže to zastavit finanční toky směrem ke kyberzločincům?

Jistě to změní rizika pro pojištěné podniky. Pokud se pojišťovny rozhodnou, že již nebudou krýt požadavky na výkupné nebo sníží úroveň krytí, bude muset většina podniků vyčlenit zdroje na pokrytí tohoto rizika. Myslím, že většina podniků by raději vynaložila své peníze na další posílení své obrany a možností obnovy, než aby si odkládala velký balík peněz pro zločince. Takže se možná dočkáme toho, že podniky budou více odolávat požadavkům na výkupné a zaměří se na obranu. A co víc, podniky se možná začnou zcela bránit placení. Ostatně, placení výkupného jen podporuje další útoky – a upřímně řečeno, oběti ne vždy dostanou svá data zpět nebo jsou dále vydírány, i když zaplatí.

Existuje nějaká šance, že budou kybernetičtí útočníci častěji stíháni? Třeba díky lepšímu sledování finančních toků?

Můžeme v to doufat, ale jak mezinárodní právo, tak vnitrostátní zákony mají co dohánět, než se činnost kyberzločinců stane skutečně rizikovou. Stíhání je náročné také proto, že útočníci se často nacházejí v zemích, které nemusí mít zájem při jejich stíhání a zatýkání pomáhat.

Za jak velkou hrozbu považujete různé „deepfake" technologie v oblasti hlasu a videa?

Rozhodně se jedná o rostoucí hrozbu, protože naše lidské mozky nedokážou tyto podvrhy dobře rozpoznat. V případě deepfaků žádáte lidské bytosti, aby neuvěřitelně sofistikovaně posuzovaly, zda je řečník skutečně člověk, kterého

znají, když se zároveň snaží analyzovat obsah jeho sdělení. Naše mozky na to nejsou stavěné, takže mám jisté obavy. Například deepfake prezidenta Zelenského, který údajně nabádá Ukrajince, aby se vzdali boje, nebyl nijak zvlášť dobře provedeným deepfake videem a většina lidí, kteří ho viděli, pravděpodobně vycítila, že jde o obraz vytvořený počítačem. Obávám se však, že se dočkáme dalších a lepších podvrhů. Dobrou zprávou je, že technologie, které je umožňují dobře provést, jsou prozatím stále drahé a komplikované. Boom deepfakeů proto ještě nepřišel. Zatím.

Jak se proti nim bránit?

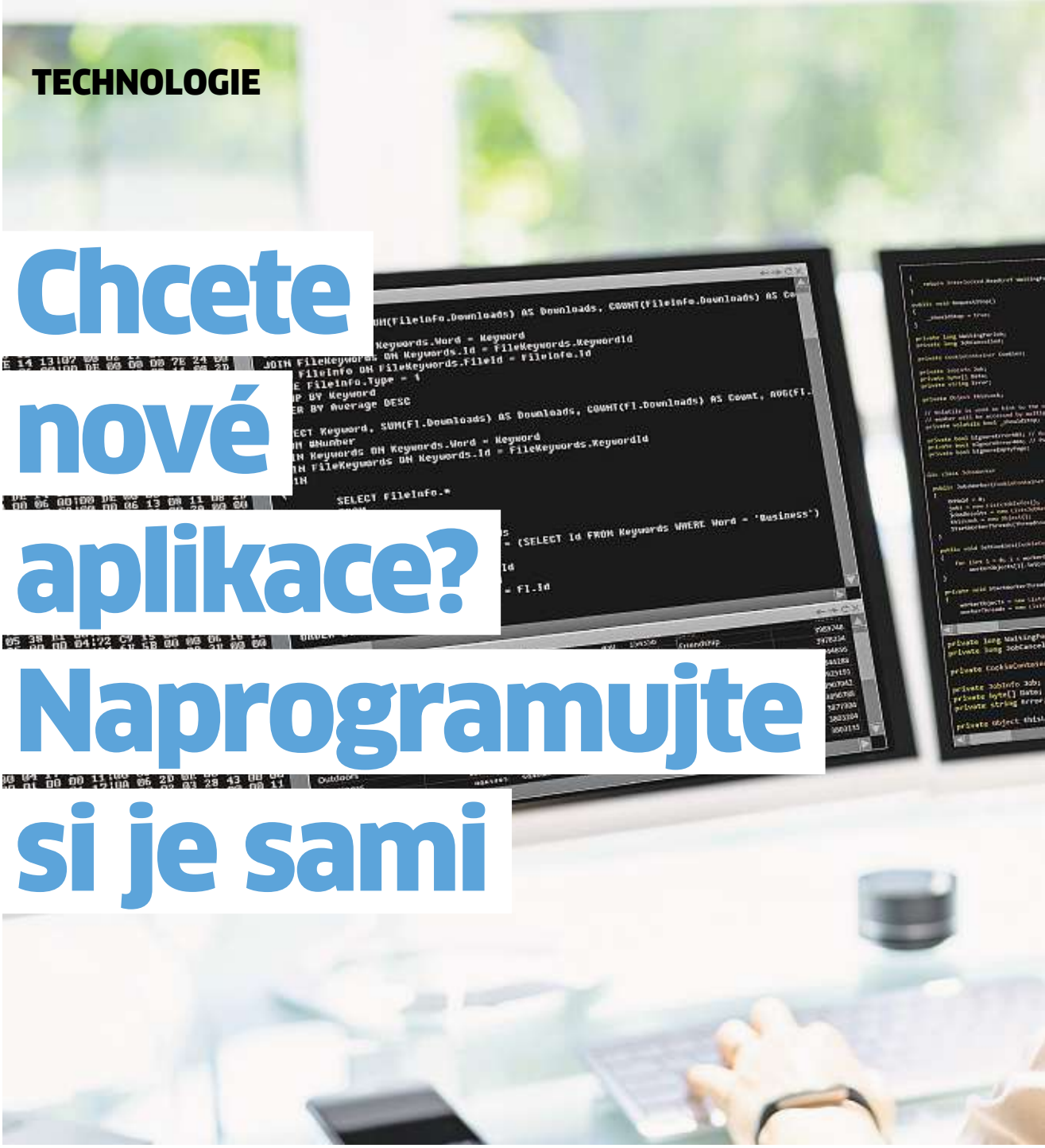
Viděla jsem několik zajímavých „menších" technologií, jako jsou plug-iny do internetových prohlížečů, které byly vytvořeny s cílem pomoci uživatelům identifikovat „fotografie" vytvořené jedním z populárních generátorů deepfake portrétů. Prozatím jsou ale nejlepší obranou proti deepfakeům osvědčené způsoby ochrany proti jiným druhům podvrhů: Je zdroj těchto informací všeobecně respektovaným zdrojem jiných zpráv? Potvrzuje tuto informaci více respektovaných zpravodajských zdrojů? Dalo by se očekávat, že mluvčí, který informaci poskytuje, by opravdu řekl to, co říká? Kdo má prospěch z toho, co se říká? Jakou reakci se snaží vyvolat a proč? A pokud ve vás informace vyvolává pocit, že nemáte čas si toto tvrzení potvrdit – i to je podezřelé. Ukvapené rozhodování je přítelem těch, kdo se snaží manipulovat vaším strachem, nejistotou a pochybnostmi. Snažte se odolat.

> Útočníci zjišťují, že je levnější vyvinout přesvědčivý sociálně inženýrský útok než najít nové technické taktiky nebo překonat bezpečnostní obranu.

Jaké jsou hlavní trendy kybernetické bezpečnosti pro rok 2022?

Jedním z trendů je nepochybně vývoj ransomwaru, což souvisí s tím, na co se ptáte, tedy s bojem proti deepfakeům a velmi sofistikovaným útokům. Lidé jsou bohužel stále zranitelní vůči starším formám podvodů. Útočníci zjišťují, že je levnější vyvinout přesvědčivý sociálně inženýrský útok než najít nové technické taktiky nebo překonat bezpečnostní obranu. Útočné kampaně jako BazarLoader a Lapsus$ nespočívají v technickém kouzlení, ale v oklamání lidí, aby odhalili své přihlašovací údaje. Běžně se říká, že slabinou kybernetické bezpečnosti jsou lidé, ale já věřím, že mohou být naopak silným místem. Mým cílem pro rok 2022 je pracovat na způsobech, jak lidem pomoci, aby byli v tomto ohledu silnější.

Chcete nové aplikace? Naprogramujte si je sami



Podniky už nebaví čekat na vývoj každé nové aplikace celou věčnost. S moderními nástroji na modelování aplikací mohou vzít situaci do svých rukou. Low-code platformy pro tvorbu aplikací nabízejí uživatelsky přívětivé prostředí, prostým poskládáním stavebních bloků lze postavit zcela nové aplikace nebo různé nástavby nad stávajícími podnikovými řešeními.

Pandemie covidu-19 urychlila digitální transformaci ve firmách o tři až čtyři roky a až o sedm let oproti původním předpokladům poskočil podíl digitálních nebo digitálními technologiemi podporovaných produktů v portfoliích podniků. Alespoň to tedy uvádí průzkum společnosti McKinsey, provedený mezi manažery firem po celém světě. Co ale pandemie v žádném případě neurychlila, je „přísun“ nových vývojářů. Právě naopak – nutnost zrychlit digitalizaci vysála z trhu prakticky všechny dostupné vývojové kapacity. A v nejbližších letech jistě nebude situace jiná, protože digitalizace a rozvoj digitálních služeb, na které si během pandemie zákazníci zvykli, budou pokračovat i dále.

text: Radek Kubeš, foto: Shutterstock

Pro podniky to znamená pokračování přetahované o vývojáře i delší čekání na vyvinutí aplikací externími dodavateli a všechna rizika s tím spojená – především zaostávání za náskokem konkurence a očekáváním zákazníků. Existuje ale jiné řešení?

Vývoj aplikací bez programování

V oblasti IT jsme často svědky toho, jak původně velmi složitá technologie projde evolucí, na jejímž konci je její daleko širší zpřístupnění uživatelům bez expertních znalostí. A nejinak je to s vývojem podnikových aplikací. V poslední době totiž přibývají nástroje a celé platformy, které umožňují vytváření podnikových aplikací i bez znalostí programovacích jazyků a vývojářských postupů. Hovoříme o model driven přístupu, respektive low-code způsobu vývoje podnikových aplikací.

K rychlému vývoji aplikací (rapid development), které podniky nutně potřebují pro pokračování své digitální transformace, už nejsou nutné znalosti vývojáře. Namísto toho je vytvářejí modeláři, kteří mají jasnou představu, jaké má mít aplikace funkce a jak má vypadat, ale obejdou se bez znalosti programování. „Zatímco vychovat dobrého vývojáře zabere roky, na vyškolení modeláře v práci s low-code platformou pro rapid development podnikových aplikací stačí několik týdnů. Modelář potřebuje znalosti na rozhraní IT analytika a byznysového přístupu, aby mohl vytvářet jednoúčelové aplikace napojené na databáze a další řešení, jež se už v rámci podniku používají," vysvětluje Petr Majer, obchodní ředitel společnosti Metada, která vyvíjí podnikovou low-code platformu Metada Platform.

K rychlému vývoji aplikací už nejsou nutné znalosti vývojáře. Namísto toho je vytvářejí modeláři, kteří mají jasnou představu, jaké má mít aplikace funkce a jak má vypadat, ale obejdou se bez znalosti programování.

Zjednodušeně řečeno představují low-code platformy uživatelsky přívětivé prostředí, v rámci kterého lze prostým poskládáním stavebních bloků (například databází, datových zdrojů, vzorců pro zpracování dat či formulářů) postavit zcela nové aplikace nebo různé nástavby nad stávajícími podnikovými řešeními. Tvorba aplikací na low-code platformách je velmi rychlá. To podporuje flexibilitu při digitalizaci a zavádění nových služeb pro zákazníky nebo aplikací, které ušetří zaměstnancům podniků spoustu času. V rámci platformy je navíc rovnou otestována funkčnost modelované aplikace, která pak může rovnou zamířit do provozu. I díky tomu low-code vývoj aplikací v současné době intenzivně využívají například banky a pojišťovny, které potřebují rychle uvádět nové produkty pro své klienty, aniž by bylo nutné je složitě vyvíjet nebo zasahovat do core systémů. Zároveň mají kompletní vývoj pod kontrolou, což je důležité především z hlediska bezpečnosti.

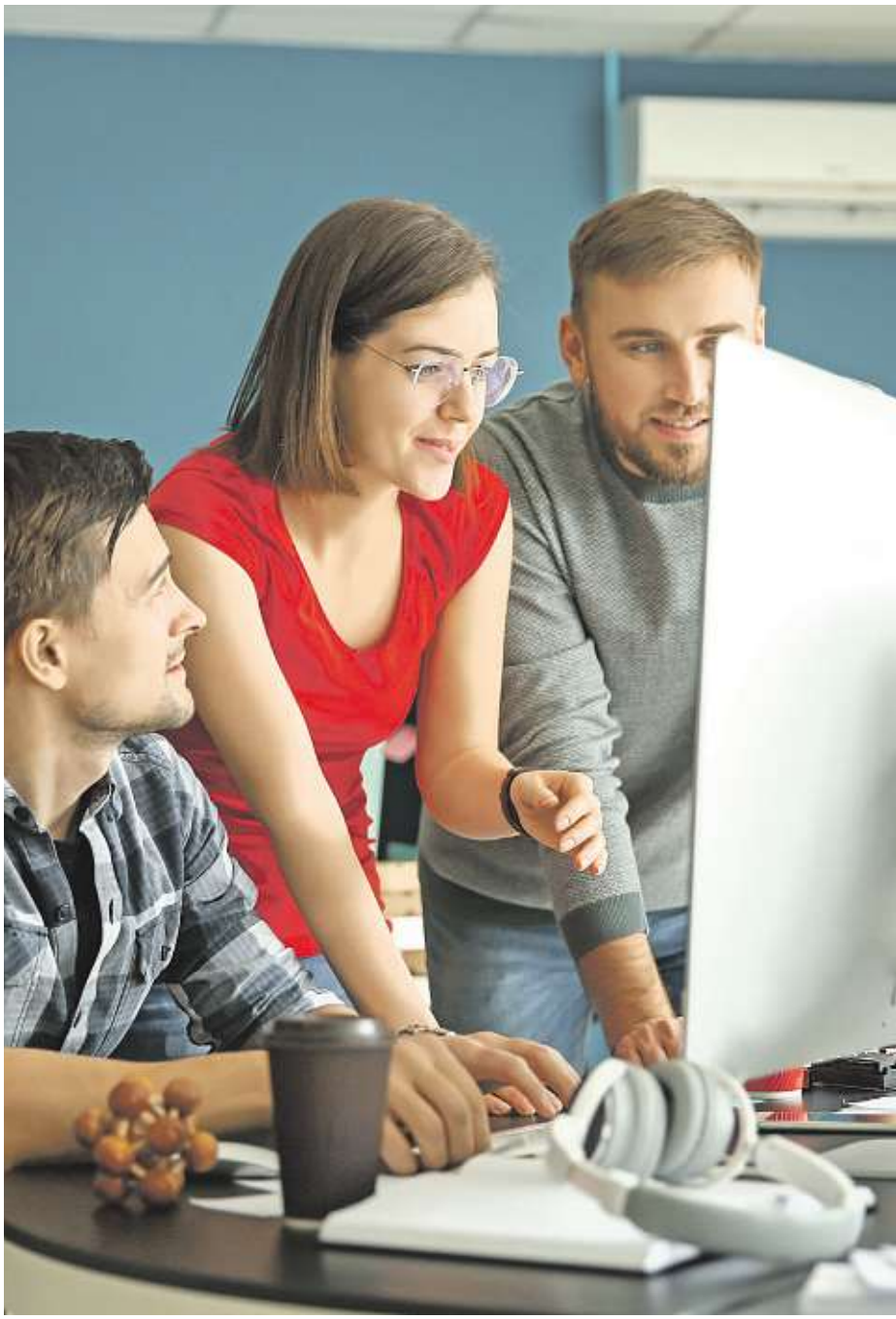
České banky využívají low-code vývoj aplikací například pro digitální procesy spojené s investičními produkty, hypotékami nebo stavebním spořením. „V souladu s naší digitální strategií vždy usilujeme o využití pokročilých technologií. Při implementaci nového produktu v podobě kompletně online refinancování spotřebitelských úvěrů Refixo jsme od začátku věděli, že chceme low-code/no-code řešení. Vedla nás k tomu zkušenost, že implementace změn je v takovém případě dramaticky rychlejší a jednodušší. To v konečném důsledku znamená kvalitnější a v neposlední řadě levnější řešení," říká Ondřej Makovec, head of retail loans v Expobank CZ. „Platforma, kterou jsme si vybrali, předčila naše očekávání založené na předchozích zkušenostech. Dává nám obrovskou pružnost jak v řízení procesů a obchodních pravidel, tak v jednoduchosti připojování datových zdrojů nebo v úpravách uživatelského rozhraní. Podobných výsledků bychom jinak dosáhli jen s mnohem větším týmem a za mnohem delší dobu," dodává Makovec.

S low-code vývojem aplikací experimentuje například také společnost Red Hat, především v integračním řešení Red Hat Fuse. „Low-code platformy vnímám jako pravidelně se opakující trend, který se snaží přinést výrazné zjednodušení do tvorby softwaru. Obecně však lze říci, že i když low-code platformy na první pohled výrazně zjednodušují vývoj, jejich slabinou je z našeho pohledu náročnější úprava a další rozvoj tímto způsobem vytvořených aplikací a integrací. To, co mohu v klasickém přístupu opravit změnou několika řádků kódu, se může v low-code přístupu ukázat jako velmi náročná úprava. Ale platí to i opačně," říká David Bečvařík, technology lead pro Česko a Slovensko ve společnosti Red Hat.

Aplikace nezávislé na tvůrci

Je ale opravdu možné vyvinout celé aplikace bez programování? „Modelář aplikací by kromě znalosti práce s low-code platformou měl mít schopnost strukturovaného přemýšlení o aplikaci, která musí poskytovat konkrétní výstupy. O vše ostatní se postará low-code platforma, která prostřednictvím API dalších systémů získá potřebná data, zpracuje je požadovaným způsobem a prezentuje je ve zvolené podobě. A právě front-endu (prezentační vrstva softwaru, pozn. red.) modelované aplikace (pokud tedy nějaký potřebuje) se týká jediná potřeba kódování, kdy je nutné připravit kaskádové styly CSS pro popis způsobu zobrazení elementů v uživatelském rozhraní. Další už ale opět zajistí low-code platforma, která například přizpůsobí front-end aplikace různým koncovým zařízením – nejčastěji obrazovkám počítačů a smartphonů," popisuje low-code vývoj aplikací Petr Majer ze společnosti Metada. Pokud by snad možnosti low-code platformy a napojení na datové zdroje a podnikové systémy nebyly pro danou aplikaci dostačující, je možné do aplikace připojit komponenty vytvořené v libovolném programovacím jazyce. Příkladem může být napojení aplikace na platební bránu, které lze snadno vyřešit právě vložením již existujícího programového kódu.

Low-code tvorba podnikových aplikací navíc řeší i další problém, se kterým se podniky při vývoji na zakázku potýkají. Platformy jako Metada Platform vytvářejí přímo v modelu i dokumentaci, na základě které je možné aplikaci kdykoli později upravit a podle potřeby aktualizovat. V údržbě a úpravách jednotlivých komponent aplikace může pokračovat kterýkoli jiný modelář, což takto vyvinutým aplikacím značně prodlužuje životní cyklus a podnikům výrazně šetří náklady. „Na modelování v oblasti integrací vsadila Česká spořitelna již před 20 lety, byli jsme tehdy jedni z průkopníků tohoto přístupu. Současná technologie low-code nám umožňuje nezávisle na dodavateli modelovat integrační služby a kompozitní operace v celé šíři potřebné pro náš IT provoz," dodává k využití low-code technologie Miroslav Lhotský, CoE integration and internal services lead České spořitelny.



Pokud firma nemá vlastní modeláře, může jejich služby poptat u tvůrce low-code platformy či jeho partnerů a postupem času, s vývojem dalších aplikací, si vlastní modeláře nechat vyškolit.

Existuje i možnost přenosu aplikace na jiné technologie nebo low-code platformy, protože čím méně programového kódu aplikace obsahuje, tím lépe je možné ji převádět mezi různými technologiemi. To znamená, že firma není omezena na jediného dodavatele technologií, na kterých již nějaké aplikace vytvořila.

Zrychlení vývoje

Zásadní výhodou modelování aplikací na low-code platformách je především mnohem rychlejší a pružnější reakce na byznysové potřeby podniku oproti tradičnímu vývoji. „Kromě

samotného vývoje se mnoho času ušetří i ve fázi analýzy a modelování aplikace. V podstatě stačí jen souhra mezi zadavatelem, který jasně popíše, co má nová aplikace dělat, a modelářem aplikace, jenž na low-code platformě namodeluje funkční a otestovanou aplikaci. V porovnání s klasickým vývojem, do kterého je nutné zapojit mnoho různých profesí, jde o úsporu v řádu týdnů až měsíců," vypočítává Petr Majer ze společnosti Metada.

S přínosem low-code technologií pro zrychlení vývoje aplikací souhlasí také David Bečvařík z Red Hatu: „Největší benefit low-code přístupu vidím v oblasti prototypování aplikací a tvorby minimálních životaschopných produktů, tedy produktů s nejmenší možnou funkcionalitou, které jsou ale plně použitelné a umožňují rychle získat zpětnou vazbu od zákazníků pro další vývoj. Zde tyto platformy opravdu velmi výrazně pomáhají a umožní rychle a efektivně prozkoumat nové možnosti."

Low-code platformy lze využívat formou cloudové služby nebo jako klasické podnikové řešení, instalované na vlastním aplikačním serveru. Pokud firma nemá vlastní modeláře, může jejich služby poptat u tvůrce low-code platformy či jeho partnerů a postupem času, s vývojem dalších aplikací, si vlastní modeláře nechat vyškolit. „Jsme přesvědčeni, že modeláři budou mít daleko větší smysl pro byznysové potřeby našich zákazníků než členové běžných vývojových týmů. Díky rychlosti vývoje a samodokumentační schopnosti low-code platformy můžeme našim zákazníkům předávat aplikace za velmi krátkou dobu. Navíc díky rychlosti zaškolení nového modeláře se zákazníci o další rozvoj dodaných aplikací již mohou postarat efektivně i vlastními silami," říká Lukáš Pešl, senior consultant ve společnosti Principal engineering.

Aplikace bez programování

Součástí rozhodování o způsobu vývoje podnikových aplikací je samozřejmě i ekonomická stránka. Low-code platformy pro modelování vlastních aplikací jsou zpravidla dostupné na základě ročních licenčních poplatků a jejich pořízení se vyplatí v případě, že se podnik chce vlastní tvorbě aplikací věnovat dlouhodobě nebo když má vysoce specifické potřeby.

„Low-code vývoj aplikací není pro jednotlivé firmy vhodný pro komoditizovaná řešení, jako jsou například účetní, ERP nebo CRM řešení, neuvažujeme-li například o vývoji nového CRM řešení jako produktu, který budeme dále na trhu nabízet. Stejně tak nemá ekonomický smysl pořídit si podnikovou low-code platformu pro vývoj jedné či dvou drobných aplikací. K tomu existují vhodnější nástroje. Pokud ale firma nad svými současnými systémy potřebuje vyvíjet stále nové aplikace a efektivně je rozvíjet, je low-code jasnou a ekonomicky velmi výhodnou volbou," dodává Petr Majer, obchodní ředitel společnosti Metada.

Petr Smolík
generální ředitel a zakladatel společnosti Metada

Vývoj aplikací pro každého

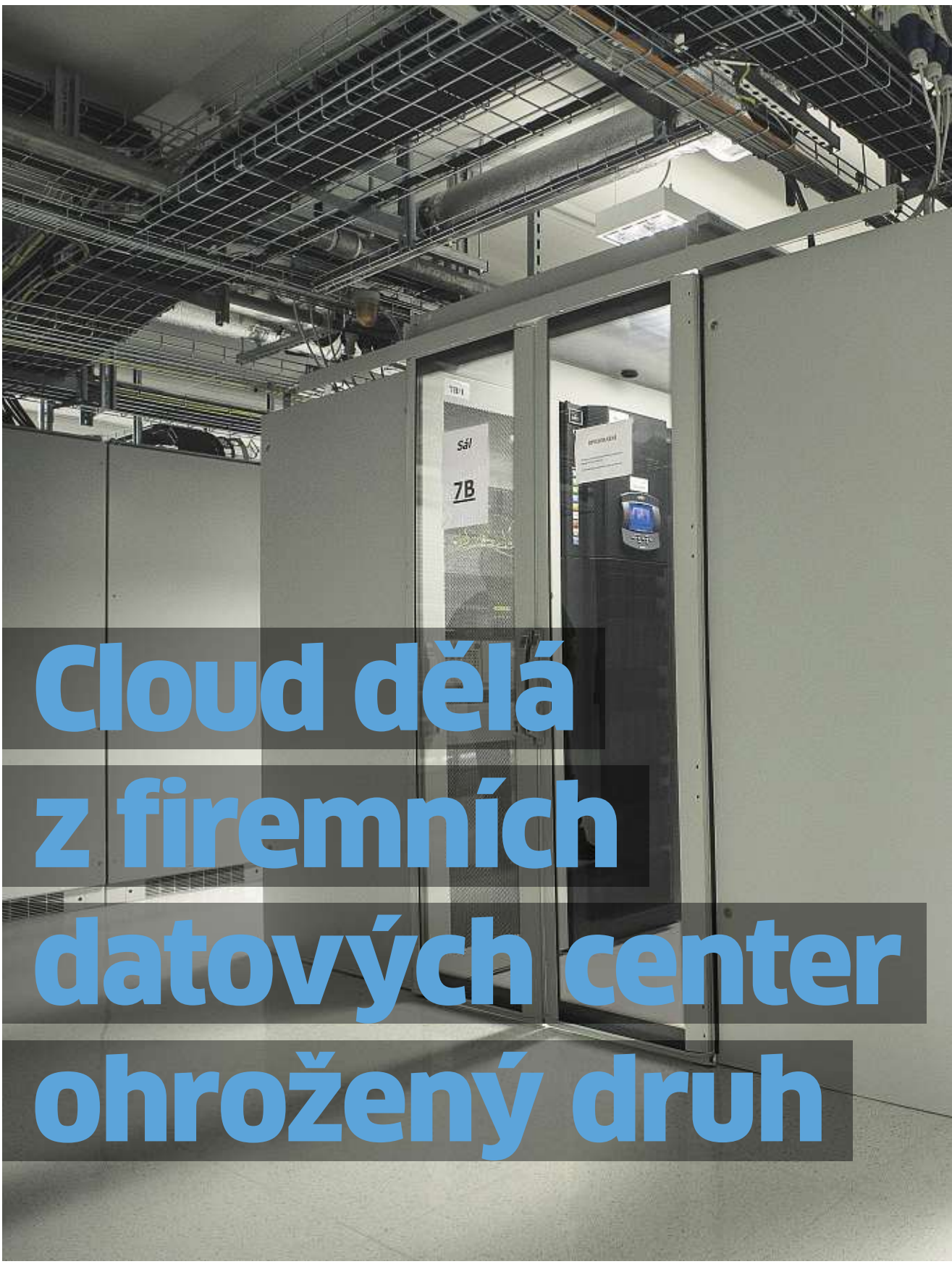
Platforma pro low-code vývoj aplikací musí tvůrcům poskytovat možnost vytvářet přesně to, co potřebují, ale také musí být co nejjednodušší, aby bylo možné pracovat rychle, efektivně a s co největší radostí, říká v rozhovoru Petr Smolík, generální ředitel a zakladatel společnosti Metada.

Jaká byla evoluce low-code platforem?
Napřed se nástroje používaly k vygenerování koster, do kterých se pak doprogramovávala logika aplikací. To zrychlovalo počáteční vývoj, ale protože se pak generovaný kód měnil, aplikace se špatně udržovaly. Další fází bylo generování kódu, který se už následně neměnil. To bylo lepší, ale generátory bylo složité udržovat a aplikace se špatně ladily. Nejpokročilejší fází je interpretace, která umožňuje aplikaci ihned spustit, testovat a ladit.

Na jaké parametry je vhodné se při výběru zaměřit?
Důležité je si napřed ujasnit, jak složité aplikace jsou potřeba a kdo bude low-code platformu reálně používat. Jsou platformy, které umožní laikům rychle sestavit jednoduchou aplikaci z předpřipravených dílů. Pak jsou platformy, které umožňují programátorům vyvíjet aplikace rychleji. Posledním typem jsou profesionální platformy, které umožňují IT analytikům vytvářet celé aplikace bez programování.

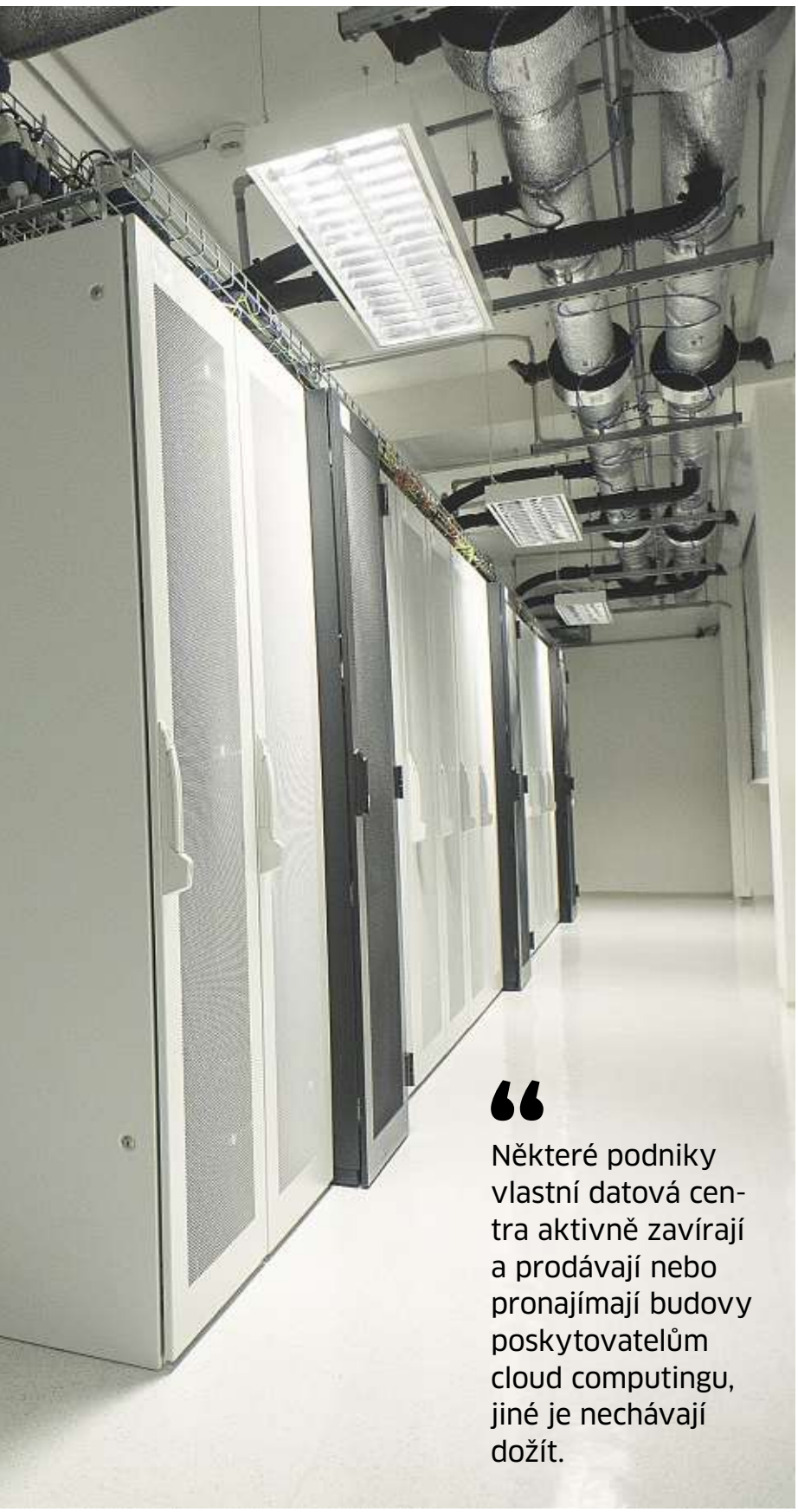
Jaká jsou úskalí low-code vývoje aplikací?
V případě platforem pro laiky může nastat situace, kdy se všechny potřebné díly musí stejně napřed naprogramovat, protože ještě neexistují. V případě platforem pro programátory je problém s nedostatkem programátorů. Profesionální modelovací nástroje zase mají určitou složitost, kterou je potřeba na začátku překonat.

Kde vidíte prostor pro další vývoj low-code platforem?
Účelem platforem je co nejvíce zefektivnit vývoj aplikací a jejich následný rozvoj a údržbu. Platforma musí tvůrcům poskytovat sílu, aby mohli vytvářet přesně to, co potřebují, ale zároveň co největší jednoduchost, aby s nimi bylo možné pracovat rychle, efektivně a s co největší radostí.



Cloud dělá z firemních datových center ohrožený druh

text: Lukáš Kříž, foto: Shutterstock, HN – Honza Mudra



Vlna cloud computingu ovládla svět podnikové informatiky. Její technologie nacházejí uplatnění v širokém spektru oblastí a činností. Mezi výhradním využitím čistě veřejných cloudových služeb a provozem vlastní infrastruktury v modelu on-premises dnes existuje škála hybridních a kombinovaných přístupů.

Veřejné cloudové služby dobývají svět. Pandemická zkušenost do jejich sítí přivedla i mnohé do té doby váhající organizace. V období, kdy osobní interakce omezovala preventivní opatření, v podstatě neexistovala dostupnější technologie. Doslova přes noc dokázaly organizace vytvořit pro své zaměstnance nová digitální pracovní prostředí, v nichž se mohli okamžitě začít vzdáleně realizovat.

Analytici společnosti IDC předpovídají, že také v zemích střední a východní Evropy bude poptávka po veřejných cloudových službách růst. Jejich zvyšující se spotřeba se mimo jiné odrazí v expanzi nových datových center, z nichž budou poskytovatelé obsluhovat region. Situaci samozřejmě může zkomplikovat probíhající válečný konflikt na Ukrajině, jenž primárně postihne právě východní Evropu.

Cloudový příklon

Rostoucí odběr cloudových služeb v regionu EMEA ilustruje také dlouhodobá predikce nasazovaných infrastrukturních platforem dle provozního modelu. Ještě v roce 2016 byly zhruba dvě třetiny nově pořizovaných serverů nasazovány do necloudových implementací. Do roku 2024 jejich zastoupení poklesne pod 50 procent. Zbývající část si podělí cloudové a sdílené implementace výpočetní infrastruktury.

Příklon ke cloud computingu bývá dost možná zveličován marketingem jeho poskytovatelů. Ještě v polovině roku 2020 indikovala výhradní využití cloudových služeb jen dvě procenta evropských organizací. Stejnou exkluzivitu ve vztahu k modelu on-premises vyjádřilo 14 pro-

> “ Některé podniky vlastní datová centra aktivně zavírají a prodávají nebo pronajímají budovy poskytovatelům cloud computingu, jiné je nechávají dožít.

Kromě finančních nákladů patří k omezeným zdrojům i dovednosti a zkušenosti nezbytné pro provozování vlastního datového centra.

cent dotazovaných subjektů. Zbývající organizace operovaly ve smíšeném módu, v němž více či méně preferovaly určitý model. Data společnosti IDC navíc naznačují, že mezi evropskými podniky nepanují zásadní rozdíly ani v závislosti na úrovni jejich digitální vyspělosti.

Pro ilustraci dodejme, že už před dvěma lety osm desetin evropských organizací provozovalo své aplikace ve veřejném nebo privátním cloudovém prostředí. Stejný zdroj ale uvádí, že jen jedna z pěti společností starého kontinentu považuje implementaci cloudových služeb za úspěšnou. Mezi nejčastější důvody neúspěchu řadí bezpečnostní a výkonnostní aspekty, problémy s důvěrou vůči poskytovateli, absenci potřebných kompetencí a narušené vnímání vlastní datové suverenity.

Hypotetický souboj cloud computingu a tradičního IT, či lépe modelu on-premises má jasného vítěze. I v Evropě převládlo modernější pojetí k zajištění výpočetních zdrojů. Mezi výhradním využitím čistě veřejných cloudových služeb a provozem vlastní infrastruktury v modelu on-premises existuje široké spektrum hybridních a kombinovaných přístupů. Patří mezi ně hybridní cloud computing a privátní cloud computing. Model on-premises navíc nad čistým využitím veřejných cloudových služeb vítězí.

Ještě před dvěma lety byla v Evropě zhruba čtvrtina aplikací provozována on-premises, tedy na vlastní infrastruktuře organizace, ve vlastní serverovně, datovém centru nebo v pronajaté části datového centra. V případě veřejných cloudových služeb šlo zhruba o 15 procent. Podle dat společnosti IDC necelá třetina úloh a aplikací fungovala v hybridním modelu, jenž kombinuje modely on-premises a veřejný cloud. Přibližně třetinu evropské podniky poskytovaly z prostředí privátních cloudů.

Příležitost edge computingu

Specifické téma, které víří ve vědomí provozovatelů a uživatelů datových center, představuje edge computing. Tento specifický technologický model překlenuje nedostatky a odstraňuje nevýhody, jež přinesla centralizace cloud computingu. Ne všechna data musí doputovat do ústředních služeb a datových center, v mnoha situacích je efektivnější, tedy rychlejší a levnější, provést úvodní zpracování co nejblíže ke zdroji.

Mezi lety 2019 a 2020 se využití edge datových center ve světě zdvojnásobilo. Analytici společnosti IDC navíc poukazují na jejich rostoucí potřebu. Vznikají celé sítě edge datových center, které jsou poměrně náročné na správu a údržbu. Zviditelňují rovněž nedostatky strategií v oblasti kybernetické bezpečnosti a dodržování shody s předpisy, které obvykle nepočítají s geograficky rozsáhlými a současně propojenými sítěmi menších datových center.

Příležitost edge computingu využívají především telekomunikační operátoři, kteří v této disciplíně zužitkovávají své zkušenosti s obsluhou geograficky vzdálených míst. Současně do ní mohou zapojit stávající sítě a nově i mobilní sítě páté generace, jež rozvoj edge computingu do značné míry akcelerují.

Perspektivy podnikových datových center

Jak si dnes vedou podniková datová centra, která by s trochou nadsázky mohla být symbolem přežité a opouštěné tradice? „Počet podnikových datových center se díky vzestupu cloud computingu obecně snižuje. Pro podniky je výhodnější průběžně platit za konzumaci infrastruktury než za udržování a rozšiřování vlastních datových

center nebo stavění nových," říká Kamil Gregor, senior analytik společnosti IDC, a dodává: „Musíme mít na paměti, že kromě finančních nákladů patří k omezeným zdrojům i dovednosti a zkušenosti nezbytné pro provozování vlastního datového centra."

Problematická dostupnost zdrojů zjevně přispívá k upouštění od tradičních forem zajištění provozu informačních technologií v podnicích. Co se děje s kdysi běžnými a masově rozšířenými podnikovými datovými centry? „Některé podniky vlastní datová centra aktivně zavírají a prodávají nebo pronajímají budovy poskytovatelům cloud computingu, jiné je nechávají dožít a už nerozšiřují jejich kapacitu," vysvětluje Kamil Gregor ze společnosti IDC. Zároveň podle něho platí, že ústup od podnikových datových center není rovnoměrný a velmi se liší v závislosti na velikosti firmy či odvětví. Rozdíly jsou i mezi různými evropskými zeměmi.

Stále existují obory, v nichž podniky vlastní datová centra z různých důvodů preferují. „Jde o organizace, které vnímají provoz vlastního datového centra jako konkurenční výhodu či nezbytnost. Informační technologie provozují jako fundament své existence. Jsou to například vyhledávací portály, nadnárodní spediční firmy nebo telekomunikační operátoři," objasňuje přístup k vlastním datovým centrům Vojtěch Vojík, obchodní ředitel divize DataSpring ve společnosti Autocont. Jde také o firmy, jež mají svou IT historii a provozují rozsáhlé firemní prostředí, které je mnohdy hodně heterogenní a jehož migrace do prostředí jiného provozovatele není triviální záležitost. Typicky to podle Vojíka mohou být banky nebo instituce státní správy.

> Datové centrum budoucnosti bude modulární a prefabrikované, uložené v racku nebo v kontejneru, případně v jejich sestavách. Nebude vyžadovat významné stavební úpravy.

Hybridní a kombinované modely provozu podnikové informatiky se budou rozvíjet a ze scény nezmizí ani podniková datová centra. „Budoucnost datových center se odehraje na softwarové úrovni. Půjde zejména o možnost propojit vlastní datové centrum s datovým centrem pronajatým nebo datovým centrem globálních poskytovatelů," myslí si Vojtěch Vojík ze společnosti Autocont.

Datové centrum budoucnosti také možná bude modulární a prefabrikované. „Bude v racku nebo v kontejneru, případně v jejich sestavách. Nebude vyžadovat významné stavební úpravy, bude stát třeba pod okny, případně bude moci cestovat za svým pánem," připojuje svou vizi Miloš Macúch, viceprezident pro strategii a rozvoj obchodu ve společnosti Altron.

text: Radek Kubeš, foto: Billigence

S daty musí pracovat všichni

S Data Governance jde především o celkové smýšlení o práci s daty v rámci firmy a způsobu, jak data řídit a starat se o ně.

Pro Data Governance je klíčová podpora managementu, protože se týká všech oddělení ve firmě, říká v rozhovoru Michal Lichter, regionální ředitel společnosti Billigence pro střední a východní Evropu zodpovědný za řízení společnosti a její celkovou strategii v rámci globální struktury Billigence.

Co pro vás představuje pojem Data Governance a proč by měly firmy taková řešení potřebovat?
Data Governance je především celkové smýšlení o práci s daty v rámci firmy a způsobu, jak data řídit a starat se o ně. Proto bych nemluvil přímo o řešení, ale o kompletním nastavení a optimalizaci způsobu, jak jsou data ve firmách získávána, ukládána a dále využívána. Data Governance je o schopnosti data najít a také jim rozumět a důvěřovat. To samozřejmě zahrnuje i kontrolu kvality dat, stejně jako nastavení pravidel pro jejich zpřístupnění a využívání. Pro firmy by Data Governance mělo představovat určitý základ pro další práci s daty a efektivní vytěžování jejich hodnoty.

V praxi ale stále vidíme, jak podniky hromadí data z desítek a stovek datových zdrojů, aniž by s nimi někdo dále pracoval – což ostatně často, kvůli jejich stavu, není ani možné. Také není výjimkou, že novým analytikům nebo vývojářům trvá měsíce až roky, než se v datových zdrojích firmy zorientují. Data Governance zajistí, že v rámci firmy budeme pracovat se stejnými datovými sadami, které bude možné efektivně používat k vývoji nových produktů a služeb, kvalifikovanému rozhodování na základě dat a ve finále samozřejmě i pro získání náskoku před konkurencí.

Jak souvisí Data Governance se zabezpečením podnikových dat?
Zatímco zabezpečení dat před vnějšími riziky, jako jsou kyberútoky či ransomware, je plně v kompetenci podnikového IT, úlohou Data Governance je kontrola a řízení přístupu k datům z pohledu interních uživatelů. S daty ve firmě pracuje každý, a proto v rámci Data Governance data klasifikujeme podle jejich citlivosti a následně řídíme, kdo k nim bude mít přístup a jak s nimi může pracovat. Velkým současným trendem je demokratizace dat, tedy jejich transparentní zpřístupnění pro využití všemi odděleními ve firmě. S regulacemi typu GDPR, stejně jako ještě přísnějšími požadavky v oborech, jako jsou finance, telekomunikace či energetika, ale musíme velmi pečlivě kontrolovat, kde se data nacházejí a kdo k nim má přístup. A právě plnění těchto požadavků je dalším z přínosů Data Governance.

Michal Lichter je regionálním ředitelem společnosti Billigence pro střední a východní Evropu. Má více než osm let zkušeností v consultingu v oblasti datové analytiky, Data Governance a Business Intelligence u zákazníků napříč kontinenty.

> “ Podniky hromadí data z desítek a stovek datových zdrojů, aniž by s nimi někdo dále pracoval.

Jaké konkrétní nástroje na práci s daty Data Governance poskytuje?
Aby bylo možné získat z dat jejich přidanou hodnotu, je nutné, aby všichni pracovali se stejnými daty, rozuměli stejně definicím, například kdo je zákazník, a měli co nejjednodušší přístup k potřebným zdrojům a reportům. Jiný pohled má obchod, finance, výroba, logistika či IT. Proto by se měly nástroje Data Governance do značné míry těmto požadavkům přizpůsobit. To znamená například různé pohledy na datový katalog nebo reporty a datové zdroje. Dále by měly umožňovat vyhledávání a řízení kvality dat, stejně jako obsahovat slovníky byznyspojmů nebo třeba definice KPI. Funkce Data Lineage pak dokáže kompletně ztransparentnit datový tok od vzniku dat po jejich finální využití, aby bylo možné sledovat, jaké souvislosti bude mít konkrétní zásah do datové struktury.

Na co se musí firma před nasazením Data Governance připravit?
Především na to, že nejde o jednorázový „projekt“, který má svůj začátek a konec. Jak už jsem zmínil, jde spíš o způsob smýšlení o podnikových datech, samozřejmě podpořený příslušnými nástroji. Pro Data Governance je klíčová podpora managementu, protože se týká všech oddělení ve firmě. I proto je jeho součástí průběžné vzdělávání zaměstnanců v oblasti datové gramotnosti. Doporučujeme začít posouzením současného stavu práce s daty a na základě rozhovorů s představiteli různých oddělení odhalit slabá místa a problémy. Výsledkem je akční plán, jak se v Data Governance posunout, aby firmě její data přinášela hodnotu. Není nutné pustit se hned do rozsáhlých změn, ale je vhodné začít postupně – s řešením nejpalčivějších problémů.

Obecně se má za to, že s daty umí pracovat především menší a novější firmy. Ale vidíme, že i velké a tradiční instituce, jako je například náš klient Česká spořitelna, mohou pomocí Data Governance a intenzivního rozvoje datové gramotnosti rychle uvádět nové produkty, zlepšovat zákaznický servis a tím si udržovat náskok před konkurencí.

Jak vybrat správné řešení na podporu Data Governance?
V dnešní době existují desítky teoretických konceptů a frameworků, které ale v praxi nefungují. Data Governance by mělo především řešit skutečné byznysové problémy firmy, čemuž by měl odpovídat výběr nástroje. Za více než deset let jsme implementovali různé nástroje a vždy doporučujeme ten, který plně odpovídá potřebám dané firmy. Doporučuji vybrat řešení i podle toho, s jakými datovými zdroji jej potřebujeme propojit – ERP, CRM či třeba BI.

Je škoda platit za službu, kterou nevyužíváte. Z Microsoft 365 jde vymáčknout mnohem víc

Petr Čuda a Orbitech pomáhají firmám modernizovat IT, aby se stalo silným článkem jejich podnikání. Opakovaně přitom zjišťuje, že firmy nevyužívají většinu možností z široce rozšířeného balíku aplikací Microsoft 365 (M365). V rozhovoru radí, jak to změnit.

Jak často se stává, že firmy mají nakoupené licence M365 a nevyužívají je?

Nečekaně často. Některou verzi balíku M365 u nás používá přes 60 % firem a většina za něj platí z velké části zbytečně.

Jak k tomu dojde?

Obvykle firma kdysi nakoupila licence Office kvůli tradičním kancelářským aplikacím jako Word, Excel a Outlook. Když nadešel čas jejich obnovy, zdálo se rozumnější platit za licence formou pronájmu, a mít tak stále aktuální verzi. Častým důvodem byla i potřeba online komunikace přes Teams během pandemie covidu.

Znamená to, že přechod na model pronájmu licencí M365 byla chyba?

To vůbec ne. Jde o to, že v balíku M365 je mnohem víc aplikací a funkcí než jen ty zmíněné. Základní sada obsahuje aplikací asi 25 (nejvyšší verze přes 50) a firmy za ně platí, ale využívají jen některé.

Co můžeme udělat pro to, abychom M365 využívali naplno?

Porovnejte skladbu aplikací, které si v rámci M365 platíte, s vlastními potřebami. K tomu je dobré mít po ruce profesionála, který zná M365 jako své boty, a řekne vám, které problémy vyřešíte a které procesy nastavíte efektivněji s nástroji M365 bez toho, abyste museli kupovat jiné produkty.

Tím profesionálem asi myslíte Orbitech.

Mnoho firem si myslí, že zmigruje a má hotovo. To je ale chyba. My nejprve diskutujeme s IT oddělením i uživateli, co je vlastně trápí a čeho chtějí dosáhnout. Neřešíme cestu, ale cíl. Po vymyšlení koncepce a realizaci migrace, která je vlastně velmi jednoduchá, přichází na řadu takzvaná adopce. Jde vlastně o seznámení uživatelů s tím, jak využívat nových možností. Fáze adopce se všeobecně podceňuje: čím menší je firma, tím je podcenění větší.

Nepřeceňujete ji naopak? Na používaní Teams a Wordu přece není nic těžkého.

Tak to sice vnímá většina společností, ale je třeba si uvědomit, že přechod na M365 je mnohem víc změnou kulturní než technickou. Najednou máte nástroje, které jsou převážně cloudové, čímž se mění styl práce. Na dokumentu pracuje ve stejnou chvíli celý tým současně a nemusí si nic přeposílat. Roste význam spolupráce a automatizace.

Uživatelé zlepšováky jistě ocení. Neznamená ale migrace do M365 více práce pro IT oddělení?

V tom je kouzlo M365 – ajťáci ho berou jako velké zjednodušení. Snadněji ho spravují a odpadají jim starosti se třetími stranami. Při následném provozu prostředí sice ještě objevujeme bolavá místa, jejich „léčba“ ale vede k ještě větší automatizaci a zefektivnění procesů.

Jak konkrétně zákazníkům s adopcí M365 pomáháte?

M365 se jako cloudová služba neustále mění. Na sledování změn přitom nikdo nemá kapacitu. Sami zákazníci nás přivedli k myšlence, že bychom je měli průběžně seznamovat s novinkami a provádět jakousi kontinuální adopci. A tak vznikla naše služba Discover365.

Čili vaši klienti už nepátrají po změnách a nemusí rozpoznávat ty podstatné?

Přesně tak. V M365 dochází k desítkám změn týdně a jejich distribuce je pro běžného smrtelníka naprosto nepřehledná. Proto jsme sestavili tým se zkušenostmi z adopčních projektů, který novinky vyhledává, třídí, sám na sobě testuje a následně je předává zákazníkům – skrze workshopy, newslettery nebo webový portál.

Jak zajistíte, že se firmy s novinkami sžijí a přinesou jim očekávané benefity?

Nestačí, že my rozumíme svým klientům, oni také musí rozumět nám. Proto používáme dva jazyky: „ajťáštinou“ mluvíme o platformních a technických věcech, o zabezpečení a podobně. Běžné uživatele oslovujeme normálním jazykem bez „sprostých“ IT slov a zkratek. Proškolení ambasadoři pak „evangelizují“ zbytek firmy. Máme radost, když nám klienti popisují, jak jim nová funkce či vlastnost zjednodušila každodenní život a jaké „aha momenty“ při tom zažili. Výsledkem služby Discover365 jsou zkrátka firmy, které konečně naplno využívají aplikace a nástroje M365, za něž už platí. V tom vidíme smysl. Vždyť i IT můžete mít rádi, fakt *(smích)*.

CO NAPLÁNUJETE, TO PODPOŘÍME

Korporátní bankovnictví

Ať už vidíte budoucnost kdekoli, náš tým pomůže vaší firmě na každém kroku. I při zásadní změně plánů. Od financování přes exportní poradenství až po moderní online služby pro tuzemský i zahraniční obchod. Důvěřujeme vašim schopnostem, stejně jako věříte vy nám.

Jan, 47 let, CEO,
rekonstrukce továrny

BUDOUCNOST JSTE VY

KB