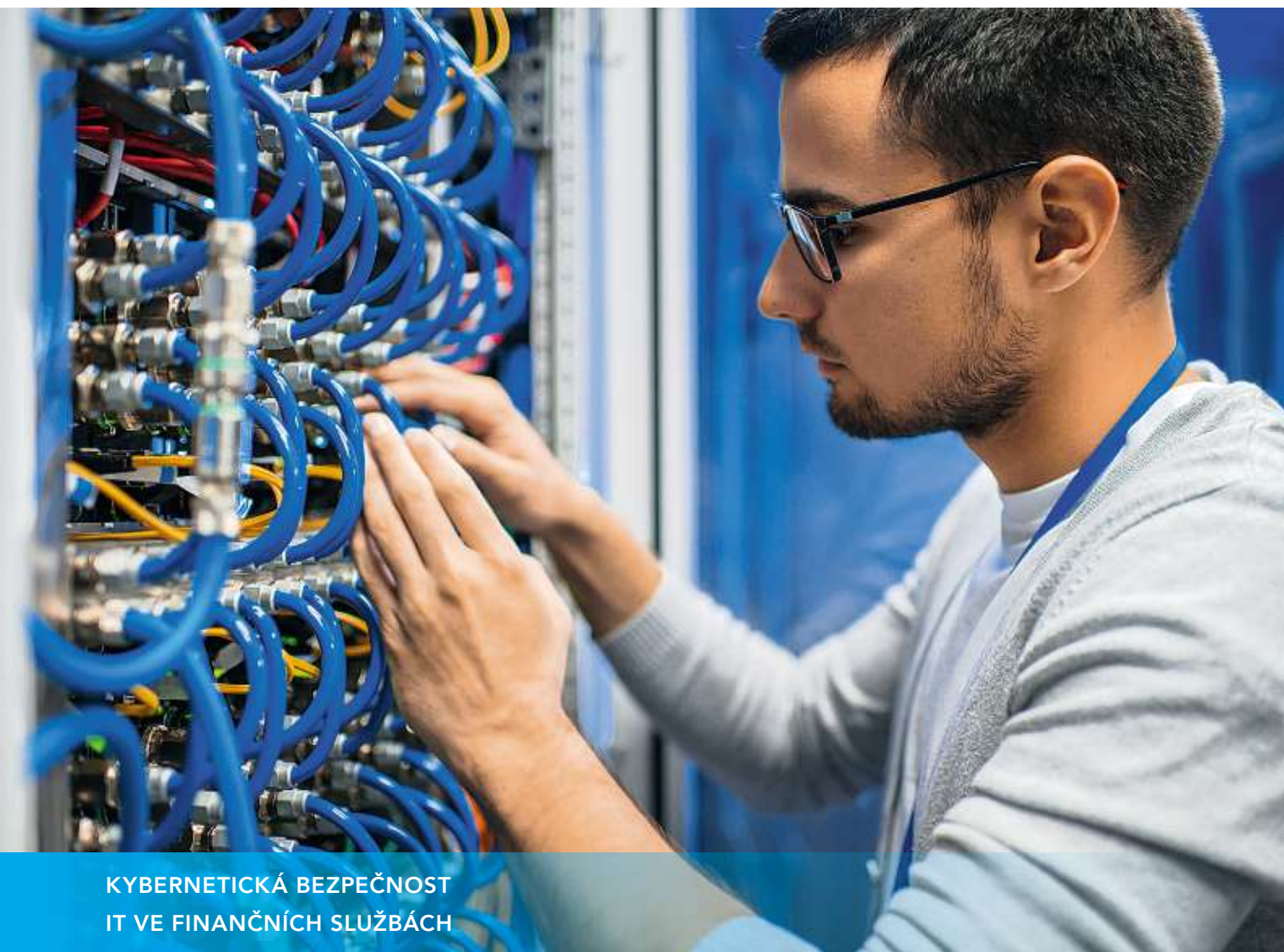


CLOUD VS. DATOVÁ CENTRA? ŽÁDNÝ SOUBOJ, SPÍŠE POKLIDNÁ SYMBIÓZA



KYBERNETICKÁ BEZPEČNOST
IT VE FINANČNÍCH SLUŽBÁCH



DYNAMIC THREAT DEFENSE

CLOUDOVÝ SANDBOX, KTERÝ DETEKUJE NOVÉ A DOSUD NEZNÁMÉ HROZBY.

ESET Dynamic Threat Defense je další
vrstva ochrany, která doplňuje standardní
bezpečnostní produkty ESET.

- ✓ Vyšší úspěšnost detekce
- ✓ Plnohodnotný sandbox
- ✓ Inteligentní cloudová technologie
- ✓ Jednoduchá aktivace a používání
- ✓ Funkční i mimo firemní síť



04

04 COVER STORY

VÝHODY A ÚSKALÍ DNES JIŽ NENÍ TŘEBA PŘEDSTAVOVAT. CLOUDOVÝ MODEL SE ALE VYVÍJÍ A NA ZMĚNY REAGUJÍ DODAVATELÉ I UŽIVATELÉ.

10 DATOVÁ CENTRA

GLOBALNÍ CLOUDOVÉ SLUŽBY ZDÁNĚLIVĚ PŮSOBÍ JAKO HROZBA PRO BYZNYS LOKÁLNÍCH PROVOZOVATELŮ DATOVÝCH CENTER. JEJICH ZKUŠENOSTI ALE UKAZUJÍ, ŽE TOMU TAK NENÍ.

14 ROZHOVOR

POKROČILÁ BEZPEČNOSTÍ ŘEŠENÍ VYŽADUJÍ ODBORNOU SPRÁVU, ŘÍKÁ SLAVOMÍR MAJCHRÁK, OBCHODNÍ ŘEDITEL FIRMY WESTCON-COMSTOR.

18 TECHNOLOGIE

FIRMY SI PORADILY S PŘECHODEM NA PRÁCI Z DOMOVA A SPOLUPRÁCI NA DÁLKU. SOUČASNĚ SE MUSÍ POTÝKAT S NOVÝMI BEZPEČNOSTNÍMI RIZIKY.



MARTIN KNÍŽEK
vedoucí vydání

VEŘEJNÝ CLOUD, NEBO DATOVÉ CENTRUM? ANEB OBOJÍ?

Poptávka po cloudových službách každoročně výrazně roste a doby, kdy cloud ve firmách vzbuzoval obavy o bezpečnost dat, jsou již spíše minulostí. Zájem o cloudové služby je poháněn jednak aktuální pandemií a potřebou rychlého přechodu na vzdálený přístup k datům a aplikacím, jednak snadným přístupem k pokročilým technologiím, jež veřejné cloudy za dostupnou cenu nabízejí. Jako nezbytnou součást své infrastruktury vnímá cloud už velká část firem.

Popularita cloudových služeb ale nijak neubírá na poptávce po službách datových center. Cloud computing z datových center část klientely odvedl, ale jinou skupinu s jinými požadavky zase přivedl. S rostoucí poptávkou po cloudových službách roste také počet firem, které je nabízejí, jak připomíná obchodní ředitel Českých Radiokomunikací Miloš Mastník. A i tyto firmy potřebují spolehlivá datová centra.

Dalším trendem ovlivňujícím poptávku po službách datacenter je hybridní cloudová architektura. Ta přináší výhodu díky kombinaci vyšší kontroly citlivých dat, která mohou být umístěna na privátních serverech v datacentrech, a možností veřejných cloudových služeb.

Se vzrůstající potřebou vzdáleného přístupu úzce souvisí i téma kybernetické bezpečnosti. Cílením na často zranitelnější domácí prostředí se útočníci dostávají blíže i k podnikovým sítím.

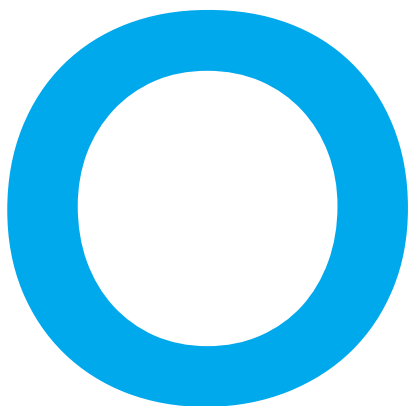


16

Cloud se stává přirozenou součástí firemní infrastruktury

Text | Lukáš Kříž

Foto | Shutterstock



dobí pionýrských projektů cloud computingu skončilo. Jeho výhody a úskalí již není třeba představovat. Cloudový model se ale neustále vyvíjí a na většinu změn musí reagovat dodavatelé i uživatelé.

Cloud computing přestal být módním trendem, stal se samozřejmou součástí moderního technologického světa. Evropa v jeho implementaci mírně zaostává za Spojenými státy. Ne vždy jde ale o projev konzervativního přístupu. V EU panují rozdílné podmínky, které mají dopad i na praktický rozvoj cloudových služeb. Jde například o roli národních států, nesčetné kulturní a jazykové rozdíly, odlišnou technologickou a infrastrukturní vyspělost, politické ambice v technologické oblasti nebo o poměrně komplikovaný regulační rámec.

CLOUD V TUZEMSKU

Podle aktuální predikce společnosti IDC letos tuzemské výdaje na veřejné cloudové služby meziročně vzrostou bezmála o čtvrtinu. Vloni činily téměř jedenáct miliard korun. Model on-premise, v němž

→ ZABEZPEČENÍ VELKÝCH DATOVÝCH CENTER JE NA ŠPIČKOVÉ ÚROVNI, VYUŽÍVÁ NEJMODERNĚJŠÍCH TECHNOLOGIÍ, SLUŽEB ŠPIČKOVÝCH OD BORNÍKŮ A INVESTIC, KTERÝM JEDNOTLIVÍ UŽIVATELÉ MOHOU JE STĚŽÍ KONKUROVAT.



23 %

O tolik má podle předpovědí analytiků společnosti IDC v letošním roce vzrůst spotřeba veřejných cloudových služeb. Růst investic do interních implementací se letos naproti tomu má pohybovat okolo sedmi procent.

jsou informační a komunikační technologie provozovány obvykle interně a na vlastní infrastrukturu, má však v tuzemsku, alespoň z hlediska objemu výdajů, stále navrch. Růst investic do interních implementací se však podle analytiků pohybuje v jednotkách procent (7 % pro rok 2021), zatímco spotřeba veřejných cloudových služeb roste dvouciferně (23 %).

„Cloud se částečně stal prioritní volbou. Není sice vhodný úplně pro všechno, ale pro drtivou většinu modelů užití vhodný je,“ říká Vladimír Kroa, Associate Vice President ve společnosti IDC. Podle jejich průzkumů řadí podnikoví uživatelé mezi hlavní výhody snižování kapitálových výdajů, flexibilní platby ➤



NEJRYCHLEJI ROSTE ODBĚR SLUŽEB VEŘEJNÉHO CLOUDU V TUZEMSKÉM ZDRAVOTNICTVÍ, VEŘEJNÉ SPRÁVĚ, PRŮMYSLU, OBCHODU A FINANČNÍCH SLUŽBÁCH.

► za využití a jednoduchost a rychlost nasazení. Organizace, které nemají dostatek interních odborníků, často volí nabídky řízených cloudových služeb.

Nejrychleji roste odběr služeb veřejného cloudu v tuzemském zdravotnictví, veřejné správě, průmyslu, obchodu a finančních službách. Ve všech uvedených odvětvích podle informací společnosti IDC překračuje meziroční nárůst výdajů 20procentní hranici.

„Cloudový model se aktuálně stává rovnocennou volbou ve srovnání s on-premise prostředím. V Red Hatu zaznamenáváme zvýšený zájem o řízené služby,” říká Zdenka van der Zwan, Channel manažerka pro ČR a SR ve společnosti Red Hat, a dodává: „Potvrzuje se, že cloud vnímá většina podniků i poskytovatelů jako nezbytnou součást své infrastruktury.”

Opatrnější hodnocení situace na lokálním trhu podává Vratislav Břenek, Global Partners Business Manager ve společnosti VMware. Podle něho cloudový model prozatím není prioritní volbou podniků. „Věřím, že se tak stane v průběhu několika příštích let. Dopady na tuzemský IT průmysl tato změna myšlení mít bude a nemusí být nutně negativní. Jsem optimista a věřím, že cloud s sebou přinese nakonec vyšší efektivitu a vyšší odbornost lidí pracujících v IT, ať už na straně dodavatelů, nebo na straně zákazníků,” myslí si Břenek.

V tuzemském odběru veřejných cloudových služeb v roce 2019 převládal model software jako služba (74,2 %), následovala infrastruktura jako služba (14,1 %) a platforma jako služba (11,7 %). Meziročně vzrostly výdaje na veřejné cloudové služby téměř o 29 procent. Dvouciferné tempo růstu si podle predikce společnosti IDC udrží minimálně do roku 2024. Zhruba jednou desetinou se na celkových cloudových výdajích podílí privátní varianta. Její růst dosahuje ve srovnání s veřejnou přibližně polovičního tempa.

Poměrně optimisticky komentuje aktuální vývoj na tuzemském trhu cloudových služeb Eduard Bartko, manažer divize Cloud Marketing ve společnosti Microsoft Česká republika a Slovensko: „Trh postupně rozeznává výhody cloudových služeb, schopnost

jejich integrace s místní infrastrukturou, jakožto i nové možnosti, které jsou dostupné často primárně právě prostřednictvím cloudu. Cloud se tak často stává první volbou při zavádění významných inovací, jako jsou například řešení postavená na prvcích umělé inteligence, řešení pokročilého zpracování dat s integrovanými prvky strojového učení, IoT řešení či řešení v oblasti bezpečnosti.”

CLOUDOVÉ TRENDY

V následujících letech nahradí více než 40 procent podniků na celém světě své zastaralé provozní modely cloudovými. Podle predikce analytiků společnosti IDC firmy od této změny očekávají zejména nárůst či zvýšení úrovně spolupráce a agility. Výsledkem mají být pochopitelně lepší obchodní výsledky.

„Poskytovatelé cloudových služeb reagují na situaci na trhu, kdy v nejistých časech, ve kterých se nacházíme, uživatelé ve zvýšené míře migrují do cloudových prostředí,” komentuje nové trendy Vladimír Kroa ze společnosti IDC. „Nejde však o jednoznačný přechod do veřejného cloudu. Uživatelé migrují na hybridní architektury, které mohou zahrnovat cloud veřejný, privátní či multicloud. Takové prostředí však klade velké nároky na správu, proto poskytovatelé investují do softwarových nástrojů, které jim umožní zajistit konzistentní správu a výkon napříč různými platformami.”

Cloudové predikce společnosti IDC letos hovoří také o zvyšující se potřebě přenositelných řešení v kategorii software jako služba (SaaS). Roste tlak na poskytovatele služeb, kteří budou nuceni zásadně změnit architekturu svých systémů. Podniky chtějí řešení SaaS umisťovat a provozovat v cloudech dle své vlastní volby.

„Na inovace a trendy v oblasti cloud computingu můžeme nahlížet z několika úhlů. Z pohledu zákazníků je zde stále zřetelný tlak na rychlejší vývoj a dodávky nových vlastností při současném snižování provozních nákladů. To je situace, ve které se nacházíme dlouhodobě. Novým trendem je pak podpora takzvaného hybridního cloudového modelu, kdy je možné některé cloudové služby provozovat v on-premise prostředí,” doplňuje trendový přehled Zdenka van der Zwan ze společnosti Red Hat.

Podle letošních predikcí společnosti IDC pro oblast cloud computingu se v následujících letech organizace zaměří na modernizaci aplikací a datovou integraci napříč cloudovými silami. Pětina podniků pro řešení těchto výzev využije propojené cloudové architektury. Modernizace aplikací a jejich transformace v nativní cloudové se stane tématem pro polovinu stávajících uživatelů z řad podniků.

Věřím,

že obava z bezpečnostních rizik v cloudu se zmírňuje, úplně ale nemizí. Neustále z trhu vnímáme obavy z bezpečnosti v cloudu.

VRATISLAV BŘENEK,
GLOBAL PARTNERS BUSINESS MANAGER
VE SPOLEČNOSTI VMWARE



„V současnosti vidím na trhu, konkrétně u poskytovatelů cloudových služeb, kteří svá prostředí staví na našich technologiích, několik trendů,“ říká Vratislav Břenek ze společnosti VMware. „Prvním z nich jsou jednoznačně kontejnery (standardizované a přenositelné balíčky aplikací, pozn. red.). Druhý trend je prodávat svým klientům i to, co jsem se naučil při stavbě svého vlastního cloudu. Zejména při modernizaci aplikací se stává, že oddělení infrastruktury mluví jinou řečí než oddělení vývoje. Tento problém už má cloud provider vyřešen a disponuje prakticky zaměřeným překladovým slovníkem. Trendem se tedy stává nejen prodej cloudu jako takového, ale také využívání vlastních zkušeností v oblasti konzultační.“

Už v letošním roce alokují podniky až 20 procent z nových výdajů na veřejné cloudové služby do oborově přizpůsobených řešení, která vyhovují specifickým požadavkům daného byznysu. Podle analytiků čeká odvětvovou specializaci bouřlivý rozvoj. „U naší cloudové platformy Azure probíhá rozvoj v desítkách oblastí. Příkladem jsou integrované nabídky cloudových řešení optimalizované pro specifická odvětví. Jde například o nedávno oznámené oborové cloudy pro finanční instituce, výrobní odvětví či pro neziskové organizace,“ říká Eduard Bartko z Microsoftu.

NÁKLADY CLOUDU

„Dnes jsou už ekonomické vlastnosti cloud computingu považovány za nespornou výhodu,“ hovoří o nákladových benefitech veřejného cloud computingu Eduard Bartko z Microsoftu a pokračuje: „Vý-

hody OPEX modelu (předvídatelných provozních nákladů, pozn. red.) v porovnání s modelem postaveným na kapitálových výdajích či možnost přesného škálování jsou těmi nejvíce oceňovanými. Zákazníkům nabízíme i další ekonomická zvýhodnění, jako je například možnost úspor při přenosu již zakoupených licencí vybraných řešení do prostředí Azure.“

Velmi podobný pohled na ekonomiku veřejného cloud computingu přináší také Vladimír Kroa ze společnosti IDC: „Zkušenosti s cloud computingem ukazují, že snižuje kapitálové náklady spojené zejména s nákupem infrastruktury, jelikož ze svého principu umožňuje platbu dle aktuální spotřeby. Znamená to, že se dokáže elasticky přizpůsobit požadavkům na výpočetní výkon, je tudíž ideální pro prostředí s kolísavými, sezonními požadavky či pro krátkodobé účely. Na druhou stranu nasazení hybridních prostředí či multicloudů zvyšuje nároky na správu a integraci, což se musí promítnout do ceny.“

INZERCE

EK013586

**VISION ERP
SOFTWARE
PRO ZDRAVÉ
PODNIKÁNÍ**

VÝROBA – OBCHOD – SLUŽBY



vision
www.vision.cz

JAK SE CLOUDOVÉ VLNĚ PŘIZPŮSOBILY TUZEMSKÉ PODNIKY?



ZDENKA VAN DER ZWAN, CHANNEL MANAŽERKA PRO ČR A SR, RED HAT

V Česku vnímáme stále větší adopci cloudového prostředí. Nevidíme žádné výrazné zaočastování v jednotlivých oborech. Od služeb přes e-commerce až po finanční domy, u kterých jsme se v minulosti mohli setkávat s bariérou pocitu nedostatečné bezpečnosti, a samozřejmě průmysl. Cloud, cloudové technologie a nástroje již dnes v Česku používá většina firem. Stále přibývá také organizací, které mají na cloudu založenu celou podnikovou infrastrukturu, nejen dílčí oblasti, jako například řešení záloh nebo e-mailovou komunikaci.



VRATISLAV BŘENEK, GLOBAL PARTNERS BUSINESS MANAGER, VMWARE

Osobně bych spíše mluvil o „přlivu“ než o „vlně“. Prozatím u nás nevidíme velké využití multicloud řešení, což je dáno především velikostí našich firem a trhu. Mnoho podniků však hovoří o cloudové strategii, popřípadě už na ní pracuje s výhledem do příštích let. Cloud však není možné vnímat jako „místo“, ale jako „způsob“ doručování IT. Pokud se na to díváme touto optikou, tak je adopce podstatně větší. Pozitivní trend lze vidět mimo jiné ve finančním sektoru. Stále však přetrvávají představy a mýty, proč se cloudu bránit.



EDUARD BARTKO, MANAŽER DIVIZE CLOUD MARKETING, MICROSOFT ČR A SLOVENSKO

Firmy a organizace si stále více uvědomují výhody a možnosti, které jim cloudové technologie přinášejí. Naše cloudové služby nacházejí uplatnění napříč všemi odvětvími. Nárůst zájmu pozorujeme jak v odvětvích a organizacích, kterým cloudové služby umožňují lépe naplňovat očekávání jejich IT oddělení, tak i v organizacích, jež v IT hledají přidanou hodnotu – byznysovou nebo zdroj významné inovace.



VLADIMÍR KROA, ASSOCIATE VICE PRESIDENT, IDC

Nějakou formu cloudu dnes konzumuje více méně každá společnost. Pro velké podniky může být ekonomičtější budovat si hybridní cloudy s tím, že základní infrastrukturu si zajistí samy a z veřejného cloudu využívají jen prostředky nad rámec běžné potřeby. Jde například o pokročilejší služby platforma jako služba. V neposlední řadě do veřejného cloudu nasazují aplikace, které se používají globálně.

► Podle zjištění analytiků si organizace uvědomují problém plýtvání v oblasti pořizovaných veřejných cloudových služeb. V průměru jde o 15 procent jejich výdajů. Právě z tohoto důvodu chtějí v nejbližších letech zavést nástroje pro řízení cloudových nákladů a snížit jejich prostřednictvím plýtvání na polovinu.

Názorný komentář k nákladové stránce veřejného cloud computingu přidává Vratislav Břenek ze společnosti VMware: „Pokud hovoříme o veřejných cloudech, tak praktické pozorování ukazuje, že ne vždy je taková služba levnější. Situace se ale mění, když začneme oceňovat všechny vstupy. Například to, že bych sice mohl vybudovat datové centrum levněji se svými lidmi, pokud bych je ale měl k dispozici, pokud bych je uměl správně vést a pokud by měli správnou sadu znalostí a zkušeností. Kolik času bych potřeboval, aby se všechny výše uvedené věci staly? A jaká je cena za to, že uvedu svůj produkt na trh později? Takže obecně si myslím, že často neumíme skutečné náklady dobře spočítat.“

BEZPEČNOST V CLOUDU

Otázka bezpečnosti veřejných cloudových služeb prošla v očích uživatelů velkou evolucí. Od potenciálně nebezpečného neznáma se postupně přesunula mezi prověřené jistoty. Podle predikcí analytiků společnosti IDC ale stále nemá cloud vyhráno ve všech oblastech. Pokud organizace zvažují přesun citlivých osobních dat do cloudových služeb, vyžadují detailní a striktní záruky bezpečnosti, a to i na velmi podrobné úrovni.

„Neustále z trhu vnímáme obavy z bezpečnosti v cloudu,“ říká Vratislav Břenek ze společnosti VMware. „Naším posláním je pomáhat zákazníkům v digitální transformaci tak, aby mohli provozovat jakoukoliv aplikaci, v jakémkoliv cloudu, na jakémkoliv zařízení, a to všechno nativně zabezpečeným způsobem. V praxi to znamená, že není nutné mít jen správné produkty, ale také správný návrh celého řešení. Věřím, že obava z bezpečnostních rizik v cloudu se zmírňuje, úplně ale nemizí.“

Pochybnosti o bezpečnosti cloudových řešení vrací Vladimír Kroa ze společnosti IDC: „O nižším či nedostatečném zabezpečení cloudových služeb panovala mylná představa od počátků jejich poskytování. Zabezpečení velkých datových center je na špičkové úrovni, využívá nejmodernějších technologií, služeb špičkových odborníků a investic, kterým jednotliví uživatelé mohou je stěží konkurovat. To však neznamená, že cloud computing je bez výzev a že implementace jsou bezproblémové. V bezpečnosti zůstává otázkou suverenity citlivých dat, dodržování nařízení GDPR nebo geografické umístění dat.“



ALEŠ HOK,
OBCHODNÍ
ŘEDITEL
ZEBRA SYSTEMS

K DATŮM KDYKOLIV, ODKUDKOLIV A HLAVNĚ BEZPEČNĚ

Na svých prezentacích a webinářích mohu využívat stále více příkladů českých firem a organizací, které přišly o svá data a dostaly se do nepříjemných provozních problémů. Rostoucí závislost na digitální infrastruktuře, práce na dálku a vynalézavost kybernetických útočníků přispívají k tomu, že následky nedostupnosti dat jsou čím dál fatálnější. To může vést k výpadkům znamenajícím v krajním případě i ukončení činnosti podniku.

Například ministerstvu průmyslu a obchodu vyhořel v lednu server se systémem pro žádosti o státní podporu v rámci programů Covid a nefungoval 24 hodin. V březnu hackeři zastavili provoz pražských poliklinik tím, že zablokovali přístup do databází laboratoří a k e-mailům.

Stále více procesů závisí na dostupnosti dat – bez nich dnes nedodáte službu, nevyrobíte požadovaný produkt a v lepší restauraci ani neuvaříte oběd. Proto se většina organizací dnes již neptá, jak ochránit svá data, ale spíše jak zajistit jejich maximální dostupnost v zájmu nepřerušované kontinuity vlastního byznysu.

Základním doporučením je zálohovací pravidlo 3-2-1, tedy tři kopie dat na dvou různých médiích a alespoň jedna fyzicky mimo firmu. Většina společností se dnes již nebojí umisťovat kopii svých kritických dat do cloudu s aktivním zabezpečením, protože ví, že tam budou ve 100% bezpečí, ať se stane cokoli – požár, nešikovnost uživatelů či kybernetický útok. Jedinou nevýhodou je rychlost obnovy – podle rychlosti připojení může stahování dat z cloudu trvat i hodiny. Většina firem několikahodinový výpadek asi překoná, ale například firmy z automobilového průmyslu, e-shopy nebo nemocnice si nemohou dovolit ani to. Pro ně existuje řešení Disaster Recovery, které nahradí výpadek systémů během několika sekund až minut.

Procesy, které nezávisí na dostupnosti dat, je naprosté minimum a akceptovatelná doba výpadku se zkracuje. O to více je třeba věnovat pozornost kybernetické ochraně kritických IT systémů. ■

INZERCE

PODCAST RANNÍ BRÍFINK HN

Vše, co potřebujete vědět, než ráno otevřete e-mail.
Byznys, politika, zahraničí.

K poslechu na podcastových aplikacích:



Jaroslav Mašek

Jana Klímová

Petr Honzejek

Martin Ehl

Ondřej Houska



Datová centra kvetou ve stínu cloud computingu

Text | Radek Kubeš

Foto | Shutterstock



eřejné cloudové služby poskytované z globální sítě datových center zdánlivě působí jako hrozba pro lokální byznys provozovatelů komerčních datových center. Jejich zkušenosti ale ukazují, že tomu tak není.

Už více než deset let masivně roste popularita cloudových služeb. Mnozí poskytovatelé podnikového softwaru omezují své nabídky řešení pro model on-premise a lákají uživatele do multitenantních systémů (tedy sdílených více zákazníky) umístěných v hyperškálovatelných datových centrech. Jaké dopady má cloudová vlna na provozovatele komerčních datových center?

„Situace a struktura zákazníků se skutečně změnily. Dříve obvyklý postup, kdy zákazník začal nejdříve na službách datových center a pak je rozšířil o cloud nebo do něj migroval, už není typický. Není výjimkou, že zákazník fázi datového centra přeskóčí a jde rovnou do cloudu,“ popisuje Miloš Mastník, obchodní ředitel společnosti České Radiokomunikace. Není to ale vždy pravidlem. Podle Mastníka je řada firem, které si chtějí provozovat virtualizační platformu plně nebo částečně samy. Takové firmy pak chtějí primárně spolehlivé datové centrum. „Samozřej-



mě s růstem poptávky po cloudových službách roste také počet firem, které je nabízejí. A ty potřebují pro své prostředí také spolehlivé datové centrum. Takže z pohledu datového centra jde o obměnu struktury zákazníků,“ vysvětluje Mastník.

Je zjevné, že cloud computing z datových center část klientely odvedl, ale jinou skupinu s jinými požadavky zase přivedl. „Naše datacentrum poskytuje jak tradiční kolokační služby, tak i cloudové služby, takže z hle-

Cloud

computing z datových center část klientely odvedl, ale jinou skupinu s jinými požadavky zase přivedl.

diska datacentra k odlivu služeb nedochází. Řekněme spíše, že se mění skladba hardwaru ve prospěch cloudu. Klasické služby jako housing nebo dedikované servery zpomalily svůj růst, cloudové služby rostou rychlejším tempem," říká Erich Syrovátka, ředitel společnosti Internet CZ. Větší zákazníci podle něho nejčastěji využívají hybridní infrastrukturu, kdy ve většině případů svůj core business nechávají na fyzické infrastruktuře a cloud využívají zejména pro zálohování, vývoj nových projektů a aplikace využívané zaměstnanci přistupujícími z různých míst.

Do značné míry symbiotický vztah služeb datových center a cloud computingu potvrzuje také Tomáš Křešťák, ředitel pro fixní produkty

jako je virtualizace infrastruktury mobilní přístupové sítě, nebo jsou důsledkem požadavků na minimalizaci latence u implementací internetu věcí.

„V průběhu minulého roku se v souvislosti s dopady pandemie covidu-19 zvýšil tlak na zabezpečení a navýšení kapacit infrastruktury datových center k obslužení nárůstu poptávky po službách. V současnosti budou poskytovatelé mnohem více pomáhat zákazníkům s optimálním rozložením a nastavením konkrétní aplikační zátěže mezi cloudová a in-house řešení. Právě řízení a správa hybridního cloudu, respektive multicloudu, patří mezi prioritní a aktuální témata," dodává Pavel Roland, Research Director ve společnosti IDC.

TRENDY DATOVÝCH CENTER A JEJICH SLUŽEB

„V obecné rovině sledujeme požadavek na budování modernizovaných datových center, to znamená automatizovaných, škálovatelných, softwarově definovaných a podporujících multicloudová prostředí," říká Libor Dvořák, Senior Research Analyst ve společnosti IDC. Registruje rovněž zvýšenou poptávku koncových zákazníků o řešení typu infrastruktura jako služba u lokálních provozovatelů datových center. „Nejčastějším argumentem pro využití jejich služeb je rychlá a přímá komunikace s člověkem, který problém vyřeší a mluví česky. Jde o benefit, který překonává i nižší ceny globálních poskytovatelů hyperškálovatelných datových center," říká Dvořák.

Zmiňovanou problematiku hybridních cloudů považuje za jeden z hlavních oborových trendů i Michal Koláček, manažer služeb digitální infrastruktury ve společnosti T-Mobile: „Současné dění v datacentrech ovlivňuje přesun firem k hybridní cloudové architektuře. Hybridní přístup přináší výhody vyšší kontroly citlivých dat na privátních serverech umístěných v datacentrech a expanzivního potenciálu veřejných cloudů."

Podle Miloše Mastníka z Českých Radiokomunikací v poslední době kromě fyzické a provozní bezpečnosti významně roste důraz na provozní efektivitu datových center. „Myslím, že tento aspekt začne stále více převažovat. Mezi našimi nejžádanějšími službami v poslední době jsou privátní datové sály. Jde nejen o bezpečnost, ale právě i o efektivitu. Zákaz-



ve společnosti O2: „Nevidíme, že by byl rozmach cloudů spojen s odlivem klientů, naopak. Často si klienti svoje vlastní cloudové aplikace dávají do komerčních datových center, takže se spíše jedná o změnu požadavků." Z pohledu telekomunikačního operátora jde podle něho o kombinaci dvou přístupů – centralizovanou část obsluhovanou z hyperškálovatelných datových center a paralelně fungující koncepty edge neboli okrajových datových center. Tento přístup využívají řešení,

MÁ ČESKO DOSTATEČNÉ KAPACITY DATOVÝCH CENTER, NEBO JE PROSTOR K NAVYŠOVÁNÍ?



DAVID LINTIMER, OBCHODNÍ ŘEDITEL, VSHOSTING

V posledních letech vzniklo díky dotacím EU mnoho nových datacenter na různých místech republiky. Často ale nebyla postavena na základě reálné poptávky na trhu. Mnoho z nich je stále nezaplněných, a to z důvodu malé poptávky i dostatečných kapacit ostatních datacenter. Svou roli hraje i nedostatek kvalifikovaného personálu.



TOMÁŠ KŘEŠŤÁK, ŘEDITEL PRO FIXNÍ PRODUKTY, O2

Myslím si, že v současné době je volných prostor dostatek. Ale jde o dlouhodobý byznys s dlouhou návratností, takže pokud se díváme na případnou výstavbu nebo obnovu datového centra, tak je to s horizontem užívání na příštích 20 a více let. Předpokládáme, že potřeba lokálních datových center v budoucnu poroste.



ERICH SYROVÁTKA, ŘEDITEL, INTERNET CZ

Přesná data nemáme, nicméně myslíme si, že je v Česku dostatek kapacit pro obsluhu požadavků. Na základě nastupujících trendů ale i my plánujeme expanzi a rozšíření kapacit jak pro služby datacentra, tak případně pro cloudové služby. Podle dostupných informací zvažuje výstavbu dalších datacenter i globální konkurence, zejména z důvodů splnění požadavků na uložení dat na území Česka.



MILOŠ MASTNÍK, OBCHODNÍ ŘEDITEL, ČESKÉ RADIOKOMUNIKACE

V posledních letech v Česku přibýlo několik nových datových center nebo došlo k jejich rozšíření. Pro lokální zákazníky s požadavky v desítkách racků to bude na několik let stačit. Stále častěji se ale objevují poptávky ze zahraničí, u nichž nejsou výjimkou stovky racků. Bude nutné vybudovat kapacity nové. Řada současných center nebude schopna dosáhnout požadované efektivity bez modernizací.



MICHAL KOLÁČEK, MANAŽER SLUŽEB DIGITÁLNÍ INFRASTRUKTURY, T-MOBILE

Na území Česka jsou v provozu desítky datových center, což může působit dojmem tržní saturace. Nicméně pouze některá budou schopná dlouhodobě naplňovat požadavky na bezpečnost a efektivitu provozu. Budoucnost datacenter bude dále ovlivňovat poptávka po vyšším energetickém výkonu serverových instalací. Optimálních provozních parametrů bude možné dosáhnout implementací moderních technologií převážně v oblasti chlazení či záložních energetických zdrojů, a vznikne tak prostor pro výstavbu nových moderních datových sálů.

► ník si sám určuje provozní podmínky pro své technologie a může tam přímo pozitivně ovlivnit i své provozní náklady, které mohou být u větších řešení v desítkách tisíc korun měsíčně," vysvětluje Mastník.

Velký důraz na celkovou efektivitu v zabírané ploše a v oblasti spotřeby elektrické energie zdůrazňuje také Tomáš Křešťák z O2. „Výsledkem je koncentrace obrovského výkonu na menší zastavěné ploše, kterou je třeba efektivně napájet, popřípadě chladit," dodává.

OSUD PODNIKOVÝCH SERVEROVEN

Oslovení odborníci se v názoru na roli, postavení a význam tradičních podnikových datových center rozdělili přibližně do tří proudů. Zástupci jednoho je považují za zastaralá, druhého za více či méně trpěná a třetího za v mnoha případech stále opodstatněnou možnost či volbu.

„Éra vlastních serveroven skončila už asi před pěti lety. V dnešní době jde o přežití, minimálně mezi e-commerce a IT společnostmi. Tendence hostovat in-house zatím úplně nevymizela, může dávat smysl například u vlastních ICT systémů, ale jde spíše o rariť. U nových klientů se s tím, že by k nám přecházeli z vlastní serverovny, už několik let nesetkáváme," říká David Lintimer ze společnosti vshosting.

Na postupné snižování významu podnikových datových center upozorňuje také Miloš Mastník z Českých Radiokomunikací. Počet firem, které stále trvají na vlastní infrastruktuře, se podle něho prokazatelně snižuje. Spíše než o jednotlivé firmy jde o celé obory. „Příkladem mohou být banky. Diskuse o přesunutí IT do komerčního datového centra byla před deseti lety téměř nemyslitelná. V současnosti už tam většina bank je. S růstem náročnosti na informační systémy a se stále větším důrazem na on-line dostupnost roste logicky náročnost na provoz datových center. Zákazníci tak dříve nebo později dojdou do bodu, kdy se to vlastními silami nevyplatí," uvádí Mastník.

Současná pandemická situace a s ní spojené požadavky například na práci z domova odhalují slabá místa podnikových serveroven. „Limitem in-house řešení je právě omezená škálovatelnost výpočetního výkonu v denních špičkách, dostupnost kvalitních služeb konektivity a často chybějící geografická redundance (nadbytek zdrojů pro případ výpadku, pozn. red.)," dodává Michal Koláček z T-Mobilu.

Do značné míry opačný pohled na budoucnost podnikových datových center a serveroven však předkládá Pavel Roland z IDC: „I přes rostoucí popularitu cloudu a aktuální růst poptávky po cloudových službách hyperskálovatelných datových center je stále z našich průzkumů vidět, že vlastní infrastruktura

ra či datová centra mají klíčové a nenahraditelné postavení mezi organizacemi pro určité typy aplikační zátěže. A pravděpodobně se to nezmění ani do budoucna. Veškeré typy aplikační zátěže lze dnes obsloužit v prostředí veřejného cloudu, nicméně bude záležet na strategii každé organizace, které typy úloh se rozhodne držet ve vlastním datovém centru a které zmigruje do veřejného cloudu.“

ENERGETICKÉ ZDROJE A NÁROKY

Cloudový boom rapidně zvýšil počet, výkonnost a také energetické nároky datových center. Jejich provozovatelé se nezdíka chlubí většími či menšími úspěchy, kterých v environmentální oblasti dosáhly. Jak si vedou tuzemští hráči?

„Energie je v oboru datacenter obrovským tématem – jen naše datacentrum jí spotřebuje asi jako malé sídliště. Bohužel podle našich kalkulací v současné době na první pohled ekologické varianty typu využití odpadního tepla pro vytápění nedávají ekonomický, ale ani ekologický smysl. Ve výsledku by se totiž na podobné řešení spotřebovalo ještě více energie,“ říká David Lintimer ze společnosti vshosting. Za lepší cestu považuje například zvyšování efektivity chlazení či technologický pokrok ve výkonu serverů, které umožní snížit celkovou spotřebu energie.

Příklad využití moderních technologií pro energeticky efektivnější provoz datového centra uvádí Michal Koláček ze společnosti T-Mobile:

PROVOZOVATELÉ VELKÝCH DATOVÝCH CENTER DBAJÍ NA SNÍŽENÍ UHLÍKOVÉ STOPY A K TOMU VYUŽÍVAJÍ OBNOVITELNÉ ZDROJE ENERGIE. MOHOU TOTIŽ ARGUMENTOVAT, ŽE JI TÍM VLASTNĚ SNIŽUJÍ SVÝM KLIENTŮM.

„Pro chlazení v jednom z našich datacenter využíváme nepřímý freecooling se skrápěním výměníku pomocí dešťové vody. Tu zachytáváme na ploše osmi tisíc metrů čtverečních a je uchovávána v podzemní nádrži o objemu 1600 metrů krychlových.“

Měli by provozovatelé datových center řešit obnovitelné zdroje energie? „To je určitě správná otázka a odpověď je jednoznačně ano. Provozovatelé velkých datových center dbají na snížení uhlíkové stopy a k tomu využívají obnovitelné zdroje energie, jako například sluneční, vodní, větrnou či geotermální. Mohou totiž argumentovat, že tím vlastně snižují uhlíkovou stopu svým klientům,“ shrnuje marketingové přínosy Pavel Roland ze společnosti IDC.

INZERCE

EK013462-1



Efektivnější ekonomický chod firmy. Díky řešení ERP QAD Cloud.

Výhody pro vaši firmu:

Ekonomická transparentnost:

přehledný systém měsíčních splátek. Žádné neplánované nárazové výdaje, žádné skryté náklady.

Lidské zdroje:

o cloudové řešení se u nás stará několik vzájemně zastupitelných správců. Ušetříte tak náklady na vlastní specialisty.

Pružnost:

Informační systém využíváte neomezeně dle svých potřeb a platíte jen to, co jste reálně využili.

Před pandemií jsme si mysleli, jak zabezpečení velký

Text | Radek Kubeš
Foto | archiv Westcon



Větším organizacím se stále více vyplácí svěřit kybernetické zabezpečení kvalitnímu externímu dodavateli, protože pokročilá bezpečnostní řešení vyžadují odbornou správu a dohled, myslí si Slavomír Majchrák, obchodní ředitel společnosti Westcon-Comstor pro region střední a východní Evropy, celosvětového distributora informačních technologií a poskytovatele souvisejících služeb. Jako jeden z důsledků přechodu na práci z domova vidí i zásadní rozšíření množství používaných aplikací a služeb při výrazně menším přehledu o zařízeních, která se připojují k firemní síti a pracují s podnikovými daty.

Jak se českým firmám z bezpečnostního hlediska podařilo vypořádat se s obrovským nárůstem zaměstnanců pracujících z domu?

Firmy a jejich IT oddělení, ať už interní nebo externí, se musely či ještě musí vypořádat s řadou zásadních otázek z oblasti procesů a zejména bezpečnosti. V případě, že pracovník používá stolní počítač, přesuneme ho celý, nebo se může pracovník připojit ze svého vlastního zařízení? Povolíme zaměstnancům používat vlastní hardware? Jaký máme mechanismus ověřování a autorizace vzdáleného přístupu a jaké jsou bezpečnostní parametry používaných zařízení? Mohou uživatelé přistupovat

do podnikových systémů přes webové rozhraní nebo přes VPN či sdílenou plochu?

Lépe zvládly situaci organizace, které ještě před pandemií a masivním přechodem uživatelů do režimu vzdálené práce přesunuly svoji infrastrukturu do cloudu. Nemusely tak řešit zvýšení přístupu systémů ve vlastním datovém centru a zvyšovat související bezpečnostní opatření.

V souvislosti se vzdáleným přístupem se zmiňuje i přístup s nulovou důvěrou (zero trust access). Můžete vysvětlit, o co jde?



je rozsah našeho



Základem přístupu zero trust je ničemu nedůvěřovat a vše ověřovat. Tento princip lze aplikovat na přístup k internetu, k datům i aplikacím, ale je zde několik důležitých požadavků. V první řadě je důležité zanalýzovat, kde všude máme uložená data, zda ve vlastním, nebo externím datovém centru, jaké je geografické rozdělení a podobně a jaká máme data z pohledu jejich identifikace a klasifikace, tedy zda jde o osobní údaje, duševní vlastnictví či jiná citlivá data. Kdy a kým byla data pořízena, kde jsou uložena a s kým a jakým způsobem je lze sdílet.

Dalším důležitým krokem je definice uživatelů. Základem pro zajištění maximální bezpečnosti je, že jakýkoliv přístup k datům bude ověřený.

Proto potřebujeme ověřovací autoritu, která ověří a poskytne identitu uživatele, jeho zařízení i samotný kontext přístupu ke zdrojům.

Také musíme definovat, k čemu má mít daný uživatel přístup. Jednotný přístup k datům a aplikacím by měl být založený na minimálním oprávnění, které je navrženo pouze k vykonání dané úlohy. Bezpečnější je uživatelům postupně rozšiřovat práva přístupu k datům a aplikacím než naopak, protože každá aplikace nebo její rozhraní jsou branou k citlivým datům. ►

► **Je s rostoucím množstvím útoků a složitostí bezpečnostních řešení stále ještě v silách menších a středně velkých firem spravovat zabezpečení vlastními silami?**

Na toto není jednoznačná odpověď. Schopnost zajistit dostatečnou bezpečnost se mimo jiné odvíjí i od oblasti, v které daná organizace působí. V dnešní době je náročné držet krok s neustále se měnícími požadavky a bezpečnostními trendy, a to zejména pro organizace, jejichž hlavní činnost nijak s bezpečností nebo technologiemi obecně nesouvisí. Pro malou firmu je to pak přímo nemožné, pokud tedy s nadsázkou nemají v týmu IT hackera, jehož koníčkem je bezpečnost.

Komplexní zabezpečení je pro firmu významnou investicí, jak funguje a jak se osvědčil model „bezpečnost jako služba“?

Hlavní myšlenka tohoto modelu je, že není nutné outsourcovat celé IT, ale jen v daném okamžiku potřebnou část. Poskytování bezpečnosti jako služby (SECaaS) je efektivní. Třetí strana může spravovat konkrétní část infrastruktury a procesů bez toho, aby zasahovala do ostatních systémů. Interní IT oddělení se věnuje standardním úkonům, jako je například aktualizace softwaru a technická podpora uživatelů, zatímco SECaaS tým řeší závažnější bezpečnostní otázky.

Pro malé a střední podniky je mnohem náročnější udržet potřebné znalosti bezpečnostního týmu, pokud vůbec nějaký existuje, a model SECaaS dává možnost mít IT bezpečnost na úrovni velkých technologických společností. Je třeba také zmínit, že náklady na tyto služby jsou zpravidla výrazně příznivější než v případě zajištění bezpečnosti vlastními silami.

Existuje obrovské množství dodavatelů bezpečnostních řešení hardwarových i softwarových – stejně jako souvisejících služeb. Očekáváte v roce 2021 nějakou konsolidaci trhu?

Všichni si jistě pamatujeme na dobu před pandemií, kdy jsme si mysleli, že rozsah našeho zabezpečení je velký. Ale nyní, když zaměstnanci pracují vzdáleně, do každodenního pracovního procesu zavádíme nové aplikace pro video a spolupráci a zároveň máme menší dohled nad zařízeními a přístupy do sítě, všichni toužíme po zdánlivě vzduchotěsné bezpečnosti z roku 2019.

Firmy konsolidují náklady na bezpečnostní řešení, a to jak hardwarové, tak softwarové, což bude mít dopad na výrobce. Ti v reakci konsolidují svá produkto-
vá portfolia a služby, aby tak lépe reagovali na aktuální situaci a vytěžili z ní maximum. Obecně vidíme zvy-



SLAVOMÍR MAJCHRÁK

JE OBCHODNÍM ŘEDITELEM PRO REGION STŘEDNÍ A VÝCHODNÍ EVROPY SPOLEČNOSTI WESTCON-COMSTOR, CELOSVĚTOVÉHO DISTRIBUTORA INFORMAČNÍCH TECHNOLOGIÍ A POSKYTOVATELE SOUVISEJÍCÍCH SLUŽEB. DLOUHODOBĚ SE ZAMĚŘUJE NA OBLAST TECHNOLOGIÍ PRO SJEDNOCENOU KOMUNIKACI A SPOLUPRÁCI V PODNIKOVÉM PROSTŘEDÍ, V POSLEDNÍCH LETECH S DŮRAZEM ZEJMÉNA NA PROBLEMATIKU KYBERBEZPEČNOSTI.

šování efektivity při současném snižování výdajů, přičemž optimální řešení je možné najít ve spolupráci s klíčovými dodavateli. Více stávajících řešení je možné nahradit jediným – modernějším a efektivnějším.

Která oblast zabezpečení je v českých firmách a organizacích trvale podfinancovaná?

Obecně můžeme říct, že pandemie a mediálně hojně komunikované zprávy o útocích například na nemocnice postavily mnohé firmy do pozoru. Zvyšující se míra digitalizace a vzdálený přístup k citlivým datům přinášejí mnohem vyšší rizika útoku nebo zneužití dat a firmy si to uvědomují. Úměrně tomu musí zvýšit i rozpočty nejen na IT obecně, ale i na oblast kybernetického zabezpečení. A zde je důležité zmínit, že spolu s posilováním systémového zabezpečení je potřeba i pravidelná edukace uživatelů, zvláště nyní, v době, kdy většina zaměstnanců pracuje vzdáleně. A právě tato oblast bývá velmi často podfinancovaná.

Jsou české firmy na kybernetické hrozby připraveny nejen technologicky, ale také personálně?

PRO MALÉ A STŘEDNÍ PODNIKY JE NÁROČNÉ UDRŽET POTŘEBNÉ ZNALOSTI BEZPEČNOSTNÍHO TÝMU, POKUD VŮBEC NĚJAKÝ EXISTUJE. MODEL BEZPEČNOSTI JAKO SLUŽBY DÁVÁ MOŽNOST MÍT KYBERNETICKÉ ZABEZPEČENÍ NA ÚROVNI VELKÝCH TECHNOLOGICKÝCH SPOLEČNOSTÍ.

Z technologického hlediska mají organizace dobré předpoklady aktuální bezpečnostní rizika zvládnout, už i proto, že jim to velmi ulehčuje možnost využití různých důležitých funkcí formou cloudových služeb nebo využití modelu SECaaS. Personálně už to bude náročnější, protože odborníků na bezpečnost je na trhu nedostatek. Nabízí se tak možnost začít ve větší míře využívat odborných stážistů z řad studentů IT oboru zaměřených na kybernetickou bezpečnost. Je to oboustranně výhodné, firma získává začínajícího odborníka, kterého si může zaučit, a student získává cennou zkušenost z reálného provozu. Velkým úskalím a podmínkou pro úspěšný boj s kyberzločinci je už zmíněná vzdělanost zaměstnanců, kteří jsou nejslabším článkem zabezpečení. Organi-

zace nesmí vzdělávání uživatelů podceňovat, protože jde o velmi důležitý prvek celé mozaiky kybernetického zabezpečení.

Jaké typy kybernetických útoků budou firmy v roce 2021 nejvíce ohrožovat?

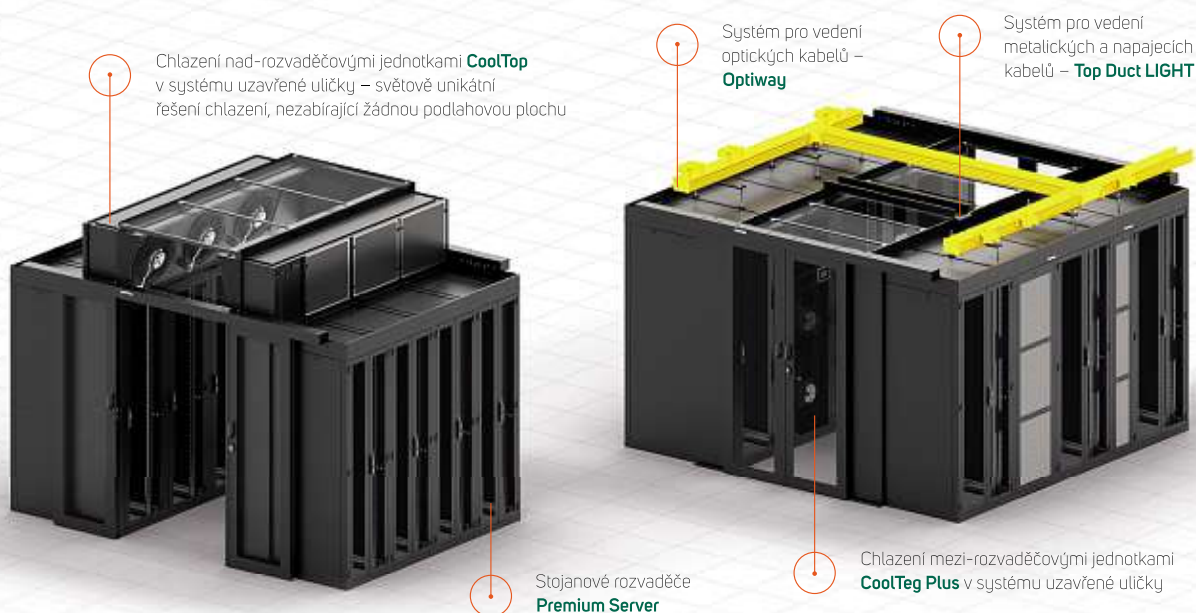
Letos vidíme velké množství typů útoků, které se buď nově objevily v důsledku pandemie, nebo se kvůli ní zhoršily. Kromě standardních útoků typu DDoS nebo útoků na poskytovatele cloudů lze jako největší bezpečnostní hrozby roku 2021 uvést průniky do podnikové sítě nebo zneužití dat prostřednictvím zařízení mimo podnikovou síť a uživatelů pracujících vzdáleně, phishing související s tématem pandemie nebo narušení cloudů kvůli rychlé a nepromyšlené migraci dat do cloudů s cílem zajistit okamžitý přístup zaměstnancům pracujícím z domova. Kyberútočníci také stále více nacházejí slabiny v procesech obchodních operací, které skýtají potenciál finančního zisku. Pozorováním systému najdou zločinci slabé vazby v procesech – například když organizace používá automatizovaný nástroj na fakturaci, který by mohl být sám o sobě zranitelný.

INZERCE

CONTEG – přední výrobce řešení pro datová centra

CONTEG

[WWW.conteg.cz](http://www.conteg.cz)



Dodáváme

IT rozvaděče
Chlazení

Monitoring a zabezpečení
Napájecí systémy

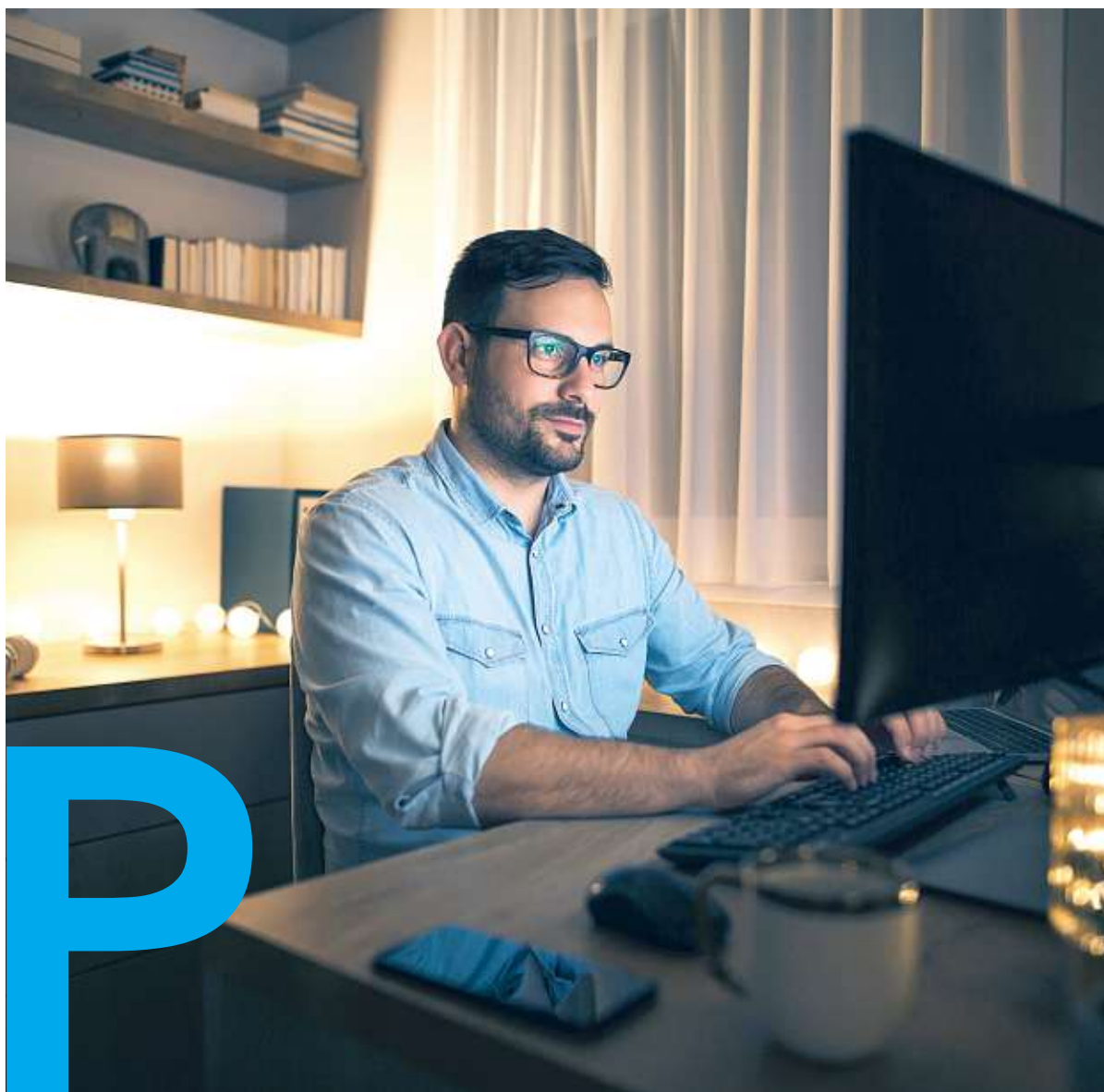
Požárně ochranné systémy
Příslušenství

EK013597

Přechod na home office odhalil bezpečnostní rizika

Text | Radek Kubeš

Foto | Shutterstock



o roce od propuknutí koronavirové pandemie vidíme, že si firmy rychle poradily s přechodem na práci z domova a nasazením nástrojů na spolupráci na dálku. Současně se musí potýkat s novými bezpečnostními riziky.

Uplynulý rok byl z pohledu kybernetického zabezpečení podnikových sítí a dat zlomový. Přechod velké části lidí na práci z domova znamenal obrovskou změnu v zabezpečení a hackeři toho neváhali využít. Cílením na často zranitelnější domácí pro-

38 %

Společnost Veeam Software v průzkumu zjistila, že až 38 procent zazálohovaných dat není možné v případě potřeby obnovit. Firmy často sice nasadí řešení na zabezpečení své IT infrastruktury, koncových zařízení a dat, ale dál už pravidelně neprověřují jeho funkčnost a spolehlivost.

středí se totiž útočníci dostávají blíže i k podnikovým sítím. Co se naopak příliš nezměnilo, jsou metody, které kyberlozinci využívají – stále se spoléhají především na sociální inženýrství a phishing a mezi typy hrozeb kraluje ransomware, tedy škodlivý software, který zašifruje data v napadeném počítači nebo serveru a útočník následně požaduje výkupné za jejich opětovné zpřístupnění. Například data laboratoří FortiGuard, dodavatele bezpečnostních řešení Fortinet, ukazují v druhém pololetí roku 2020 sedminásobný nárůst celkové aktivity v oblasti ransomwaru oproti první polovině roku. Útočníci pochopitelně zneužívali i zájem lidí o témata spojená s covidem-19, takže není velkým překvapením, že bylo v roce 2020 zaznamenáno přibližně 16 milionů kampaní cílených právě na covid téma. Útoky využívaly především podvodné internetové stránky, mobilní aplikace se škodlivým kódem a phishingové e-maily.

Čím dál častější jsou také útoky na cloudové služby, které začalo mnoho firem a organizací používat na vzdálenou komunikaci a spolupráci. „V souvislosti se stále intenzivnějším využíváním cloudových řeše-

ní získává na popularitě cloud jacking, kdy se útočník za pomoci různých metod snaží získat přístup ke cloudovým účtům uživatele. Obecně jsou útoky čím dál více cílené a velmi roste množství útoků zaměřených na kritickou infrastrukturu, zdravotní zařízení a průmyslové provozy, které jsou tradičně hůře chráněné, a tak i velmi zranitelné,” komentuje trendy kybernetických útoků Ondřej Štáhlavský, senior regional director CEE společnosti Fortinet. ➤

INZERCE

Onlio se rozděluje

Divize APS se stane samostatnou společností

Přední poskytovatel konzultačních služeb a softwarových řešení pro podnikání se chystá více soustředit na rozvoj robotizace a umělé inteligence, expanze do zahraničí, ale současně také přiblížení se specifickým potřebám klientů. Proto míří nově vzniklá společnost do Atlassian cloudu a clusterovaných řešení.

Zásadní okamžik

Pro značnou část firem využívajících produkty Atlassian přichází zlomový moment – migrace do cloudu. Divize APS je dlouhodobě „#1“ v licenčním businessu na CZ&SK trhu v segmentu řešení Atlassian. Nyní tedy jako společnost Onlio APS, a.s., vyrazí po vlastní ose. Tým má před sebou zásadní výzvu

v podobě ukončení platformy Server ze strany výrobce Atlassian a přechod mnoha firem na cloudové řešení.

Specializované služby Onlio APS

Díky ukončení platformy Server ze strany výrobce Atlassian se velká část Enterprise zákazníků využívajících toto řešení vydá cestou clusterovaných řešení Atlassian DataCenter, včetně podpory integrace do dalších systémů zákazníka. Pro značnou část firem může být DataCenter vhodnější. Proto Onlio APS buduje tým specializující se na tento druh řešení a nabídne těmto náročným klientům nejen špičkový konzultační servis, ale také pomoc s výběrem vhodných licencí s ohledem na výkon a cenu řešení.

Tým Onlio APS byl schopen jako jeden z mála na CZ&SK trhu obhájit nejnáročnější certifikaci Platinum Solution Partner. Pokud aktuálně řešíte téma migrace produktů Atlassian, je tým Onlio APS tím nejlepším partnerem.



Pavel Nykl
Obchodní ředitel

 **onlio aps**

Onlio APS, a.s.
Gen Office Gallery
U Garáže 1611/1
170 00 Praha 7
Tel.: 222 744 755
onlioaps.com





← KRITICKÝM MÍSTEM ZABEZPEČENÍ JSOU TAKÉ SAMOTNÍ ZAMĚSTNANCI, KTERÍ MNOHDY TVOŘÍ PRVNÍ LINII OBRANY PŘED KYBERNETICKÝM ÚTOKEM.

ČASTOU CHYBOU JE OPOMÍJENÍ INSTALACE BEZPEČNOSTNÍCH ZÁPLAT POUŽÍVANÉHO SOFTWARE A ODKLÁDÁNÍ JEHO AKTUALIZACÍ.

► PRO BEZPEČNOU PRÁCI Z DOMOVA NESTAČÍ JEN ANTIVIR

Při rychlém přechodu na práci z domova bylo pro firemní IT prioritou zajistit základní funkčnosti samotného vzdáleného připojení, což se ve většině společností podařilo vyřešit. Postupně se ale ukázalo, že stávající strategie, kdy se bezpečnost soustředí na ochranu na úrovni firemní sítě, přestává stačit a je nutné zajistit zabezpečení i všech koncových zařízení bez ohledu na to, kde se fyzicky nacházejí. Nutnost změn v zabezpečení podnikových sítí potvrzuje i Martin Bratičák, regional director CEE společnosti Zyxel: „Je nesporné, že práce z domova se stala novou normou a bude výrazně ovlivňovat naši budoucnost. Pro organizace bude životně důležité zajistit za všech okolností bezpečné připojení svých vzdálených zaměstnanců. Samozřejmě platí, že organizace musí i nadále chránit svou firemní síť a vzhledem k rostoucímu počtu uživatelů připojících se z domova ji zabezpečit ještě důkladněji než doposud.“

Zabezpečení přechodu na práci z domova či obecně mimo kancelář ale neznamená jen zajistit bezpečné připojení do firemní sítě. Často nedostatečně zabezpečená jsou mobilní zařízení používaná pro práci, která pak představují velké riziko možného úniku dat nebo neautorizovaného přístupu do firemní sítě a systémů. Firmy přitom pořád ve velké míře spoléhají na klasický antivirus, který však na ochranu před současnými kybernetickými hrozbami nestačí. „Adekvátní ochranu proti aktuálním hrozbám nabídnou pouze bezpečnostní řešení nové generace v kombinaci s pokročilou ochranou proti ransomwaru a technologiemi umělé inteligence a hlubokého učení,“ vysvětluje Patrick Müller, regionální manažer pro východní Evropu ve společnosti Sophos. Další častou chybou je opomíjení instalace bezpečnostních záplat používaného softwaru a odkládání jeho aktualizací. Ve většině podniků nejsou nastavena pravidla, takže není určeno, kdo je zodpovědný za proces aktualizací, co má být aktualizováno, kdy a jakým způsobem. Tento problém přitom mohou řešit specializované nástroje na patch management.

Kritickým místem zabezpečení jsou také samotní zaměstnanci, kteří mnohdy tvoří první linii obrany před kybernetickým útokem. „Uživatele bych označil za vůbec nejslabší článek zabezpečení. Firmy často neinvestují dostatečné prostředky do vzdělávání svých zaměstnanců, neprovádějí phishingové a pe- ►

Co přivedlo globálního lídra ATOS do virtuálního datového centra?



+20%
VÝKONNOST

+100%
RYCHLOST

-50%
NÁKLADY

Atos je globálním lídrem digitální transformace s více než sto tisíci zaměstnanci v sedmdesáti zemích světa. Nespolehlivost fyzické infrastruktury vedla jeho český vývojářský tým do virtuálního datového centra předního českého poskytovatele The Cloud Provider (TCPPro). Proč Atos tohoto kroku nelituje?

Atos se zaměřuje na infrastrukturu, cloudová řešení, implementaci SAP, systémové integrace a kybernetické služby. Spolehlivé fungování IT infrastruktury je pro jeho tým klíčové. Během probíhajících projektů ale začal Atos pociťovat nevyhovující zázemí vlastní infrastruktury, kterou bylo potřeba vyměnit. Společnost Atos poptala i virtuální datové centrum a tým TCPPro ji přesvědčil, že to je to správné řešení jejich problémů. Atos tak technicky stabilizoval vývojové prostředí, vytvořil procesy řízení a snížil náklady na IT infrastrukturu.

Výzva

Atos narazil na několik problémů. Jedním bylo fyzické vybavení. Nešlo jen o nevyhovující hardware, ale také o problémy s výpadky elektrické energie, nestabilitu prostředí a nespolehlivé zálohování. Navíc bylo náročné správně nastavit procesy a zodpovědnosti za správu. Při správě vlastní infrastruktury společnost narážela na to, že lze jen těžko měřit náklady. Novou strategií bylo vyřešit problém virtualizací v externím datovém centru.

Atos zvažoval několik parametrů, které bylo potřeba v optimálním řešení najít: stabilitu prostředí, flexibilitu při

vytváření infrastruktury, jasně definované náklady za jasně definovaný výběr služeb, reakční dobu v případě servisních požadavků a udržitelný finanční model.

Při porovnání jednotlivých nabídek došel Atos k výběru virtuálního datového centra TCPPro díky ochotě týmu vysvětlit a předvést funkčnost řešení a také nabídnout velmi výhodné cenové podmínky.

Řešení

Spolupráce začala jasnou definicí výchozího prostředí včetně plánu na postupné rozšiřování. Prostředky byly za podpory technického týmu zmigrovány, aniž by byly omezeny nebo ohroženy běžící projekty. Hned po migraci se projevíly pozitivní dopady na výkon a dostupnost infrastruktury. Zvýšila se i stabilita vývojového prostředí. Z přechodu také vyplynula revize nutných výrobních prostředků a zdrojů, což vedlo k optimalizaci nákladů.

“Přechod Atosu do virtuálního datového centra bylo dobré rozhodnutí, které otevírá dveře novým možnostem, technologiím a postupům v krátkém čase,” říká Petr Holan, Solution Architect.

Jednou z hlavních výhod je optimalizace infrastruktury jako celku, což zahrnuje zbavení se nepotřebných zdrojů, upravení pravidel pro poskytování služeb a modernizaci platformy. *“VDC se naplno přizpůsobuje našemu procesu vytváření softwaru a umožňuje nám tak pracovat efektivně. Spolu s výbornou podporou a její okamžitou reakční dobou představuje stabilní páteř pro vývoj našich produktů,”* dodává Petr Holan.

Výsledek

Díky změně Atos zrevidoval procesy a zkrátí čas, který bylo nutné vyhrazovat pro definici nových zdrojů a řešení problémů. Zavedení stabilního prostředí a rychlá reakční doba podpory zvýšily efektivitu práce. Případné požadavky jsou vyřešeny vždy svižně.

“Vnímáme také pozitivní dopad na naše zákazníky, kteří těží z větší dynamiky, se kterou můžeme definovat zdroje potřebné k řešení jejich požadavků a tedy efektivněji realizovat jejich projekty,” uzavírá Petr Holan.

- **O 20 % výkonnější infrastruktura, která se pružně přizpůsobuje potřebám**
- **O 100 % rychlejší možnost práce s definicí prostředí a stavbou vlastních zdrojů**
- **O 50 % snížení nákladů na správu vývojového prostředí**

Více informací a další případové studie najdete na našich stránkách
www.tcppro.cz

TCPRO
the cloud provider

► netrační testy a jejich zaměstnanci neumí rozpoznat legitimní e-mail od podvodného,” dodává Patrick Müller. Vzdělávání je tradičně slabé místo v rámci bezpečnostní strategie. V poslední době je sice patrný určitý posun k lepšímu, ale týká se spíše menšího počtu firem, které se bezpečnosti intenzivně věnují. Mnoho společností vzdělávání zaměstnanců v oblasti kyberbezpečnosti neřeší vůbec. „Obvykle bývají školení zaměřená na ochranu informací a kybernetická bezpečnost součástí zaškolení nových zaměstnanců. Další vzdělávání zaměstnanců v těchto oblastech už není tak obvyklé, ale výjimkou jsou společnosti, které mají certifikace zaměřené na tuto oblast, například ISO 27001, kde je vzdělávání nastaveno na pravidelné bázi. V poslední době je oblíbená i forma newsletterů, zaměřených vždy na konkrétní téma jako vytváření hesel, používání mobilních zařízení, phishing a další,” vysvětluje Kateřina Hůtová, information security management system manager společnosti SoftwareONE.

DŮVĚŘUJ, ALE PROVĚŘUJ

Firmy často chybují i v tom, že sice nasadí řešení na zabezpečení své IT infrastruktury, koncových zařízení a dat, ale dál už pravidelně neprověřují jeho funkčnost a spolehlivost. Například pokud jde o zálohování důležitých dat, společnost Veeam Software zjistila v rámci svého průzkumu, kterého se zúčastni-

ly i české podniky, že až 38 procent zazálohovaných dat není možné v případě potřeby obnovit. „Dvě třetiny českých firem se potýkají se zásadním rozpořem v tom, jak často jsou jejich data zálohována a jaké množství dat si mohou dovolit ztratit v případě havárie nebo kybernetického útoku mezi dvěma zálohami,” dodává Martin Štětka, regionální manažer CEE, Veeam Software.

Kromě schopnosti obnovit data ze zálohy by měly firmy prověřovat také spolehlivost svého kybernetického zabezpečení prostřednictvím auditů a penetračních testů. „Pokud společnost ve spěchu při přechodu do on-line prostředí zanedbala otázku bezpečnosti, měla by co nejdříve provést audit zabezpečení svého prostředí, kterým přehledně ukáže, jakým oblastem se věnovat nejdříve a jaká rizika plynou z nečinnosti,” vysvětluje Martin Trněný, cloud security consultant společnosti SoftwareONE. Na českém trhu působí řada organizací poskytujících služby etických hackerů (kteří odhalené chyby nezneužijí, ale informují o nich zadavatele), penetrační testy a simulace bezpečnostních incidentů. „Ročně realizujeme stovky projektů v oblasti penetračních testů. Stále více však našim zákazníkům doporučujeme řešit bezpečnost systémů v jejich celém životním cyklu, tedy nejen pravidelným testováním, které se soustředí na známé zranitelnosti v kódu nebo konfiguraci,” dodává Maroš Barabas ze společnosti AEC. ■



◀ **VZDĚLÁVÁNÍ JE TRADIČNĚ SLABÉ MÍSTO V RÁMCÍ BEZPEČNOSTNÍ STRATEGIE. MNOHO SPOLEČNOSTÍ VZDĚLÁVÁNÍ ZAMĚŠTNANCŮ V OBLASTI KYBERBEZPEČNOSTI NEŘEŠÍ VŮBEC.**

DATOVÉ CENTRUM BEZ STAROSTÍ

Tradiční třívrstvá infrastruktura byla v průběhu let dopilována k dokonalosti, jenže omezení daná jejími principy již nelze obejít. Co když data zase vrátíme zpět do serverů a objednáme tak nutnost použití SAN? Strach z této změny bývá často tou jedinou překážkou pro nasazení hyperkonvergované infrastruktury (HCI). Pokud se přes něj přenesete, otevřou se vám výhody HCI v celé své kráse.

Jednoduché, efektivní a flexibilní řešení

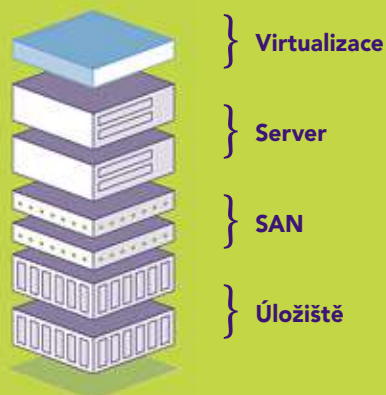
Hyperkonvergovaná infrastruktura je v principu a z pohledu architektury až geniálně jednoduchá. Představte si ji jako skupinu serverů zapojených do LAN. Na rozdíl od klasické třívrstvé architektury mají tyto servery v sobě i disky, tedy úložiště dat. Hardware je tedy triviálně komoditní, a z toho plynou dvě zásadní výhody – nízká cena a snadná dostupnost. To, co dělá z těchto obyčejných serverů vysoce dostupné, odolné, neomezeně škálovatelné, univerzální a efektivní řešení, je softwarová vrstva Nutanix. Díky ní získáte zcela plnohodnotné enterprise řešení.

Univerzálnost hyperkonvergované infrastruktury plyne z naprosté flexibility, s jakou lze cluster budovat a rozšiřovat. Ostatně i giganti, jako je Google či Facebook, využívají hyperkonvergovaná řešení.

Více informací a referenční
instalace ve FN Motol:



www.taktik.cz/DC



Nutanix jako lídr

Softwarová vrstva Nutanix nabízí mimo jiné největší svobodu ohledně volby HW platformy nebo provozovaného hypervizoru. Když se rozhodnete pro integrovaný nativní hypervizor Nutanix, ušetříte za licence VMware nebo Hyper-V. Pokud ale chcete používat jiný hypervizor, nic tomu nebrání. Ať chceme nebo ne, hyperkonvergovaná infrastruktura je budoucnost datových center. A proč vlastně nechtít?



- nízké TCO v porovnání s tradiční infrastrukturou
- vysoká míra automatizace a nízké nároky na správu a lidské zdroje
- zásadní úspora místa v serverovně, nákladů na chlazení i spotřeby elektřiny
- svoboda volby hardwarové platformy i hypervizoru
- univerzální řešení jak z pohledu velikostí, tak provozované zátěže
- robustní řešení s nativní podporou DR scénářů a replikací
- stovky VDI nebo téměř milion IOPS ve 2U appliance
- neomezená škálovatelnost, flexibilita a postupný růst řešení
- komfort a rychlost cloudových služeb pro on-premise nasazení

Bankéře nahradí roboti a umělá inteligence

Text | Radek Kubeš

Foto | Shutterstock

obslouhou klientů bez návštěv na pobočkách si banky během pandemie poradily poměrně dobře. Klienti ale brzy budou chtít na dálku řešit prakticky všechny finanční služby.

Omezení pohybu lidí a uzavření provozoven jasně ukázalo, které obory jsou dobře připravené na obsluhu svých zákazníků na dálku. Excelovaly samozřejmě e-shopy a pandemická situace hrála do karet například i poskytovatelům e-learningu. Špatně si nevedly ani banky, protože jejich klienti jsou už zvyklí na využívání služeb internetového a mobilního bankovníctví. Rozhodně to ale neznamená, že by byly české banky perfektně připraveny na novou dobu, kdy ani velmi konzervativní klienti nezačnou po uvolnění všech pandemických opatření opět chodit na pobočky bank. Více než kdy jindy dnes lidé očekávají, že s nimi bude jejich banka komunikovat plně digitálně, v čase, který jim vyhovuje, a s okamžitou odezvou.

Pro banky to znamená, že musí věnovat daleko větší pozornost digitálním kanálům a možnostem samoobslužného přístupu ke stále většímu okruhu svých služeb. „Koronavirová pandemie významně urychlila digitalizaci bankovníctví. Také ale ukázala, že nestačí jen digitalizovat vybrané, nejčastější činnosti. Banky v současné době musí nabídnout opravdu kompletní digitální obsluhu klientů – od za-

→ LIDÉ OČEKÁVAJÍ, ŽE S NIMI BUDE JEJICH BANKA KOMUNIKOVAT PLNĚ DIGITÁLNĚ, V ČASE, KTERÝ JIM VYHOVUJE, A S OKAMŽITOU ODEZVOU.



ložení účtu přes všechny běžné služby, jako jsou úvěry, hypotéky či pojištění, až po investice,” říká Karel Beran, šéf produktů a inovací ve společnosti BSC, a dodává: „Tento přístup ale vyžaduje i digitalizaci procesů na straně banky – jak pro jejich automatizaci, tak pro zvýšení přesnosti, například při výběru

On-line

Banky v současné době musí nabídnout kompletní digitální obsluhu klientů – od založení účtu přes všechny běžné služby, jako jsou úvěry, hypotéky či pojištění, až po investice.

vhodné nabídky pro klienta nebo při stanovení úvěrového rizika.”

ROBOTICKÝ BANKÉŘ

Do budoucna je jasné, že si banky vystačí s mnohem menším počtem zaměstnanců na pobočkách, ale o to více klientských dotazů a požadavků budou odbavovat prostřednictvím telefonátů, webových chatů a také sociálních sítí. Zkušenosti s nasazením technologie umělé inteligence v podobě robotů zajišťu-



jících textovou nebo hlasovou komunikaci s klienty (tedy chatboty a voiceboty) přitom jasně ukazují, že je možné tímto způsobem odbavit většinu opakujících se dotazů a požadavků zákazníků a výrazně snížit nápor na „lidské“ operátory kontaktních center. S pomocí technologie strojového učení lze navíc

neustále rozšiřovat okruh témat, se kterými si voicebot nebo chatbot poradí, aniž by je musel předávat operátorovi.

Využití umělé inteligence při komunikaci s klienty ale přináší kromě rozšíření komunikačních kanálů a jejich zpřístupnění bez kapacitních a časových omezení i další efekty. Nasazení technologií zvyšujících efektivitu a snižujících náklady pomáhá zvyšovat konkurenceschopnost a řešit problém klesajících výnosů z běžných bankovních služeb, jak potvrzuje i Zdeňka van der Zwan, channel manager CZ & SK ve společnosti Red Hat: „Stejně jako všechny komerční podniky musí i finanční instituce zapracovat na nástrojích pro zvýšení konkurenceschopnosti. Evropská směrnice PSD 2 změnila prostředí poskytování bankovních služeb a zvýšená potřeba mobility přinesla nové vzorce chování a očekávání jednoduché obsluhy ze strany zákazníků. Tyto faktory, společně s historicky nízkými úrokovými sazbami, vystavují banky silnému tlaku na zvýšení efektivitu a zrychlení zavádění inovací.”

UMĚLÁ INTELENCE ODHALÍ PODVODY A NABÍDNE SPRÁVNÉ PRODUKTY

Využití technologií umělé inteligence není pro banky žádnou novinkou. Už delší dobu se strojové učení využívá na analýzu transakcí s cílem včasného odhalení podvodů nebo pro detekci a zastavení kybernetických útoků. Pokročilá technologie může prakticky v reálném čase analyzovat obrovské množství transakcí a zjišťovat anomálie, které mohou souviset s podvody a útoky.

Další oblastí využití umělé inteligence je například i automatizované úvěrové hodnocení klientů, kterým může následně internetové bankovníctví přímo nabízet úvěry v předeschválené výši. Obecně lze na základě analýzy dat, kterých mají banky o svých klientech obrovské množství, nabízet právě takové produkty, o které budou mít klienti opravdu zájem. Banka má přitom možnost do své analýzy zapojit řadu hledisek vypovídajících o aktuální životní situaci klienta a jeho skutečných potřebách. Personalizace ➤

KLÍČOVÉ JE, ABY SI ZÁKAZNÍK Z VYUŽITÍ DIGITALIZOVANÉ SLUŽBY ODNESL PŘINEJMENŠÍM STEJNĚ KVALITNÍ ZÁŽITEK JAKO Z OSOBNÍHO JEDNÁNÍ S BANKÉŘEM.

► na takové úrovni, s přijatelnými náklady, by nebyla bez robustního technologického základu vůbec možná. „Cestou k poskytování vysoce personalizovaných služeb v čistě on-line prostředí je digitalizace a schopnost masivního zpracování dat, typicky s využitím technologií umělé inteligence a strojového učení,“ vysvětluje Karel Beran z BSC, ale zároveň upozorňuje na významné riziko: „V cestě za co nejvyšší úrovní digitalizace je velmi snadné zapomenout na extrémně důležitý faktor přívětivosti a osobního přístupu k zákazníkovi. Přitom je naprosto klíčové, aby si zákazník z využití digitalizované služby odnesl přinejmenším stejně kvalitní zážitek jako z osobního jednání s bankéřem, který zná aktuální situaci klienta a umí vyhodnotit jeho potřeby.“

NOVÉ SLUŽBY PRO KLIENTY

Digitalizace a využití nejnovějších technologií otevírá i prostor pro zavádění nových služeb, které tradičním bankám pomohou získat nové klienty a konkurovat progresivním internetovým bankám, stejně jako internetovým gigantům typu Googlu nebo Facebooku. Jednou z cest je další zvýšení komfortu využívání finančních služeb – například možnost posílat peníze přátelům pomocí jednoduchého výběru příjemce z adresáře kontaktů v mobilním telefonu. Další možností je zpřístupnění jinak poměrně náročných finančních produktů a služeb širšímu okruhu klientů. Může jít například o správu investičního portfolia s pomocí robota, který nejen že bude pracovat nonstop, ale díky lepším algoritmům, vyšší rychlosti, přístupu k datům a absenci emocí pomůže i méně zkušeným investorům dosáhnout lepších výsledků. Do budoucna bude bezpochyby zajímavé také obchodování s kryptoměnami, které představují extrémně rychle rostoucí finanční instrument, jenž je ale bankami, jistě i kvůli chybějící regulaci, zcela opomíjen. Inovativní banky ale mají nyní jedinečnou příležitost pomoci svým klientům pochopit velmi komplikovaný princip kryptoměn a nabídnout jim související služby. Je přitom prakticky jisté, že kryptoměny z finančního trhu nezmizí, ale naopak

→ POMOCÍ CHATBOTŮ A VOICEBOTŮ JE MOŽNÉ ODBAVIT VĚTŠINU OPAKUJÍCÍCH SE DOTAZŮ A POŽADAVKŮ ZÁKAZNÍKŮ A SNÍŽIT TAK NÁPOR NA OPEŘÁTORŮ KONTAKTNÍCH CENTER.



se blížíme okamžiku, kdy vlastní virtuální měnu uvede některá z centrálních bank. Ostatně o zavedení čistě digitální měny neuvažují jen velké internetové společnosti a některé státy, ale také Evropská centrální banka.

Inovativních technologií a na nich postavených služeb se finančnímu sektoru nabízí řada, ale toto tradiční odvětví často dlouho váhá s jejich nasazením. Překážkou jsou často také historické bankovní systémy a způsob řízení rozvojových projektů, jak potvrzuje Zdeňka van der Zwan ze společnosti Red Hat: „Banky o nové technologie zájem rozhodně mají, ale brzdí je jejich současné systémy, stejně jako organizační struktury a procesy řízení. V obou oblastech dochází k řadě změn, ale hlavní obtíž je přejít od stávající situace směrem k požadovanému designu nových služeb. Není také snadné transformovat vývoj aplikací z klasického monolitického přístupu k novým metodám, stejně jako zavádět nové technologie, jako jsou kontejnery a veřejný cloud, které nabourávají deset let zažitě principy architektury.“ ■

Zoo do Cloudu nepatří

Co vzít s sebou do Cloudu, co raději nechat před jeho branami a jak to vůbec zjistit? **Vít Grossmann** radí největším firmám, jak získat ty správné odpovědi a neprodělat na adopci Cloudu kalhoty.



Vít Grossmann

Náročným IT projektům se věnuje více než 20 let. V posledních letech provádí klienty oblastmi Cloud compliance, Cloud strategy, Cloud qualification a Readiness consulting. Během své kariéry pomáhal zákazníkům jako např. Generali, skupině ERSTE včetně České spořitelny, Societe Generale, ČSOB, Kooperativa nebo skupině Raiffeisen Bank International.

Určitě často odpovídáte na otázku: „Co je to Cloud?“ Začneme ale netradičně: Co Cloud není?

Cloud není kouzelné místo, kde zmizí všechny vaše (IT) problémy. To rozhodně ne. Cloud také není *Someone else's computer*, jak nosí na tričku někteří vtipálci, když se šinou vytrhnout server z racku, proklínajíce firmu, že ještě není v Cloudu.

Dobrá – a co tedy Cloud vlastně je?

Podle mě je Cloud způsob, jak dělat IT. Takzvaným „cloudovým chováním“ se učím od těch nejlepších: Cloud poskytovatelé se naučili absolutní efektivitě, automatizaci, škálovatelnosti, robustnosti a dalším „superschopnostem“. Abych navázal na předchozí otázku: Cloud též funguje jako lupa nebo zesilovač potíží mého současného IT.

Lupa? Zesilovač? Mluvíte v Cloud šifrách?

To bych nerad. Zkrátka když nemáte v IT uklizenou, ale máte tam technologickou zoologickou zahrádku, kterou držíte nad vodou ručně, co instalace to unikát, tak jakýkoliv takový nestandard vás v Cloudu stojí peníze.

Na konci dne můžete skončit v režimu 50:50, kdy budete k provozu vašeho IT potřebovat dvě party: starou na zoo a novou na Cloud.

To zní jako horor. Neměli bychom se tedy Cloudu raději vyvarovat?

To by bylo přinejmenším zbabělé! Když se Cloud dobře podchytí, vymyslí a naplánuje, dokáže přinést nemalé benefity. Platí to nejen v oblasti úspor, ale zejména v podpoře vašeho podnikání, škálovatelnosti byznysu, možnosti cokoliv si rychle vyzkoušet, rychle adaptovat, nebo naopak rychle opustit. Cloudové technologie vám taky pomohou „nezastarat“ – přinutí vás inovovat a takzvaně držet prst na tepu doby.

To už zní lépe, ale kde začít?

Startovací pozici určuje vyspělost IT ve vaší organizaci. Někomu tíží historické investice, jiného aplikace či odbornost IT kolegů. Proto jsme zvyklí začínat rychlým přezkumem IT vyspělosti společnosti a určením základních strategických cílů, kterých může v dohledné době 1–3 let dosáhnout. Tvorba takové Cloud strategie se samozřejmě odvíjí od obchodních či existenčních ambicí a potřeb dané organizace.

Kdy bude Cloud strategie úspěšná?

Když se zamyslíte nad spoustou otázek. Kde se nacházím a kam chci? Jak se připravit a zvládnout změnu? Jak to ovlivní mé zaměstnance, zákazníky a partnery? Kde mi to pomůže? Jaké znalosti a schopnosti pro takovou změnu potřebuji? A kde je vzít, když je nemám?

To je hodně otázek.

Ano. Ale za nimi přijdou odpovědi, včetně jasného plánu kudy se vydat, kam investovat čas, peníze a co vám to přinese – mimo jiné kolik ušetříte.

A kolik tedy ušetříme? A jsou na to důkazy?

Úspěšné implementace Cloud strategií nám opakovaně potvrzují, že úspory přicházejí v horizontu 2–3 let pečlivé práce.

Cesta je cíl?

Částečně ano, je to Cloud Journey. Ale v tomto případě se vyplatí nezůstat v její půli. Chce to včas vyplout se správným kapitánem a neztroskotat. Tak přeji všem úspěšnou plavbu po oblacích a žádný útes!



I díky ABRA Software...



Kateřina Svatošová
OK Aviation Group

...létáme dál.

Modernizujeme e-shop a s fakturami pracujeme jenom elektronicky.

↳ **Automatizujte rutinní práci.**



Ondřej Krátký
Liftago

...jezdíme dál.

Optimalizujeme činnost kurýrů – stejné vozy přepravují osoby i zásilky.

↳ **Inovujte procesy i produkty.**



Vladimír Finsterle
Lékárna.cz

...se staráme dál.

Přesná data nám říkají, do jakých produktů a služeb investovat energii.

↳ **Podnikejte na pevných základech.**