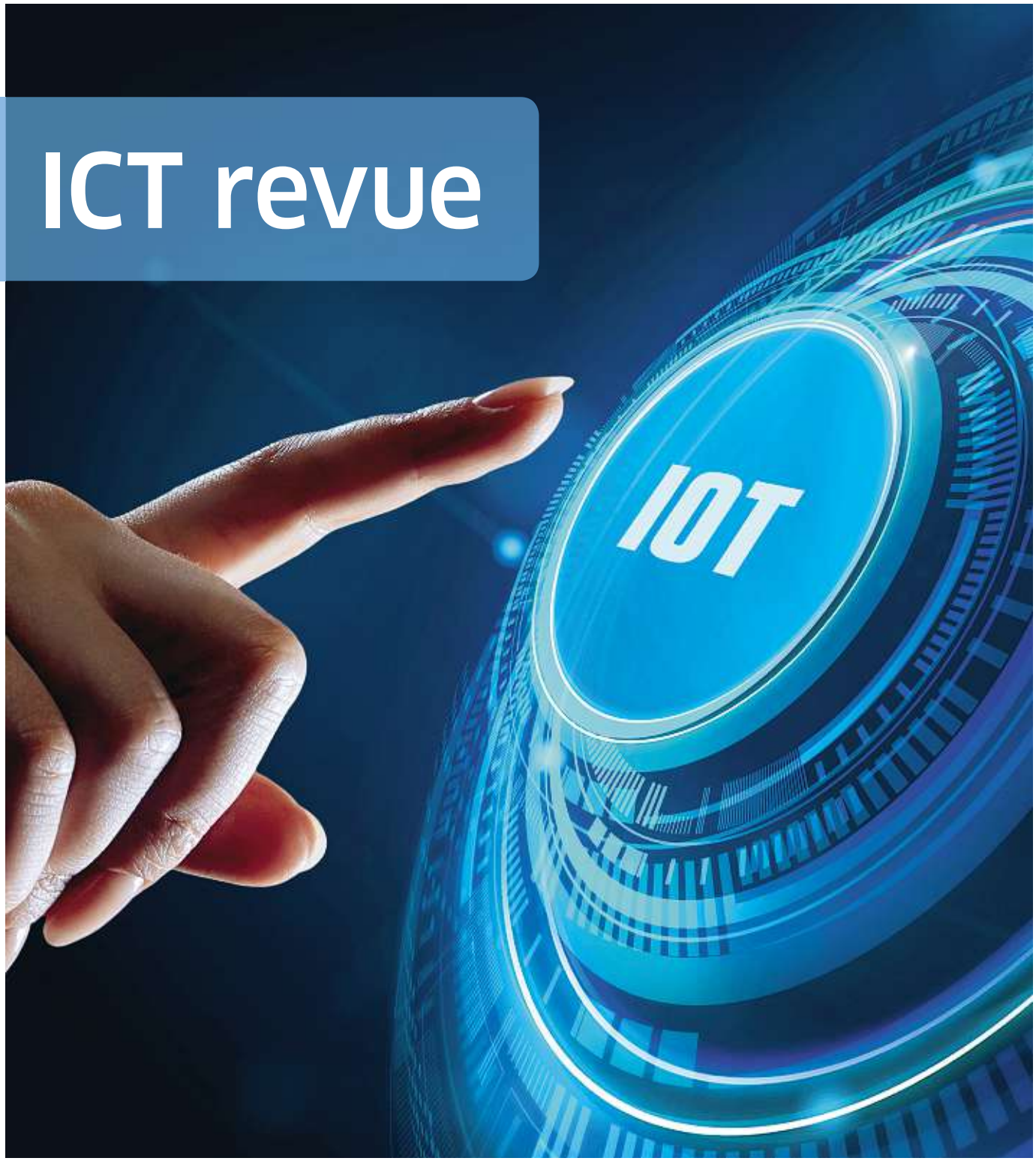
TEMATICKÝ MAGAZÍN VYDAVATELSTVÍ ECONOMIA, A.S.

Samostatně neprodejné
09|2021

ICT revue



Internet věcí

IoT otvírá dveře inovativním přístupům a službám, je ale také bezpečnostním rizikem.

Rozhovor

Firmy požadují stále kratší dobu obnovy dat, říká Martin Štětka, manažer Veeam Software.

Edge computing

Posouvání výpočtů k okrajům sítě umožní zvládnout obří objemy dat z internetu věcí.

#TEAMWORK

veracomp

EXCLUSIVE NETWORKS

An Exclusive Networks Company

Radim Kozel
Business Unit Manager
Fortinet, Veracomp s.r.o.

Bulharské přísloví:

„ZAVOLÁŠ-LI VLKA, POZVEŠ CELOU SMEČKU.“

PŘIDEJ SE DO NAŠÍ SMEČKY A POJĎ LOVIT V RAJÓNU KYBERNETICKÉ BEZPEČNOSTI!

CHCI LOVIT!

hr@veracomp.cz
www.veracomp.cz/kariera

EK013787

EDITORIAL

Martin Knížek
editor speciálních projektů

Vážené čtenářky, vážení čtenáři,

internet věcí, tedy miliardy nejrůznějších zařízení, senzorů, spínačů, kamer a bůhvíčeho všeho připojených do internetu, chrlí denně obrovské množství dat, s jejichž zpracováním a ukládáním si firmy mnohdy nevědí rady, ale také představuje významné bezpečnostní riziko. Do sítě jsou připojena často velmi levná zařízení, s jejichž zabezpečením si v mnoha případech nikdo hlavu nelámal, nebo alespoň ne příliš. Pokud k takovým zařízením při jejich nasazení správci nepřistupují s nejvyšší obezřetností, mohou se stát snadným vstupem do firemní či domácí sítě. Jaké zásady dodržovat při výběru a nasazení IoT zařízení, poradí odborníci v úvodním článku Lukáše Kříže.

Trendy v oblasti ukládání a zálohování dat představí v rozhovoru Martin Štětka, regionální manažer zodpovědný za obchodní aktivity společnosti Veeam Software ve střední a východní Evropě. Také v souvislosti s IoT a jeho integrací do firemních sítí zmiňuje potřebu správné strategie ukládání a zálohování dat, která by i z důvodu snadné škálovatelnosti měla zahrnovat veřejné cloudy. S enormním nárůstem datových toků ze zařízení internetu věcí mohou ale pomoci i technologie, jako je Edge Computing.

Ten posouvá výpočty a ukládání dat k okrajům sítě, blíže ke zdroji dat a místu jejich využití ve fyzickém světě. To snižuje nároky na přenos dat do datových center a zrychluje jejich zpracování, ale kromě vyšších nákladů přináší i některá rizika.

O aktuálních hrozbách v oblasti kybernetické bezpečnosti a způsobech, jak jim čelit, se pak více dozvíte v článku Radka Kubeše. Největším rizikem v této oblasti zůstává pro firmy i nadále ransomware.

Inspirativní čtení!

MAGAZÍN ICT REVUE – PŘÍLOHA HOSPODÁŘSKÝCH NOVIN A TÝDENÍKU EKONOM, 8. 9. 2021 • 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 Martin Impseil • Adresa redakce Pernerova 673/47, 186 00 Praha 8 • Tisk Moraviapress • Samostatně neprodejné • http://www.hn.cz

OBSAH

Internet věcí má problém s bezpečností

Internet věcí otvírá dveře inovativním přístupům a službám ve všech odvětvích. Současně ale pro své uživatele a provozovatele představuje nové bezpečnostní riziko. Zdá se, že tempo zavádění internetu věcí (IoT) značně převyšuje úsilí, jež dodavatelé i jejich zákazníci věnují otázce souvisejícího zabezpečení.

> Podle průzkumu bezpečnostních expertů společnosti Palo Alto Networks může být 57 procent zařízení IoT zranitelných vůči útokům střední nebo vysoké závažnosti.

Na konci roku 2020 odhadovali analytici společnosti Gartner, že je celosvětově v provozu 5,8 miliardy koncových zařízení internetu věcí. Nejvíce jich nachází uplatnění v energetice (1,37 miliardy) a v oblasti fyzické bezpečnosti (1,09 miliardy). Nejrychleji ale přibývají v automatizaci budov, automobilovém průmyslu a ve zdravotnictví. Meziročně jejich počet vzrostl o více než pětinu. V průměrné organizaci se koncové body IoT podílely na celkové množině zařízení připojených ke komunikační síti necelou jednou třetinou.

Stav bezpečnosti rozmáhajícího se světa internetu věcí dokreslují analytici týmu Unit 42 společnosti Palo Alto Networks. Podle jejich zjištění probíhá 98 procent veškeré komunikace internetu věcí bez šifrování. Osobní anebo důvěrná data uživatelů se bez této elementární ochrany stávají mnohem přístupnější. Navíc téměř tři pětiny koncových zařízení IoT obsahují

text: Lukáš Kříž, foto: Shutterstock

střední až vysoce závažné zranitelnosti. Mezi nejpostiženější kategorie se v této souvislosti řadí medicínská zobrazovací technika (51 %), bezpečnostní kamery (33 %), monitorovací systémy pacientů (26 %) anebo tiskárny (24 %).

Kybernetičtí útočníci cílí na instance internetu věcí v podstatě celým arzenálem technik. V souhrnném přehledu firmy Palo Alto Networks ze známějších typů chybí snad jen útoky DoS a DDoS (distributed denial of service). Dvacet šest procent škodlivých aktivit se zaměřuje na chování uživatelů, 33 procent operuje s malwarem a 41 procent sází na exploity, jež využívají zranitelnosti zařízení a systémů.

„Podle průzkumu, který provedli bezpečnostní experti z našeho oddělení Unit 42, může být 57 procent zařízení IoT zranitelných vůči útokům střední nebo vysoké závažnosti," říká Miloš Hrnčár, viceprezident společnosti Palo Alto Networks pro východní Evropu.

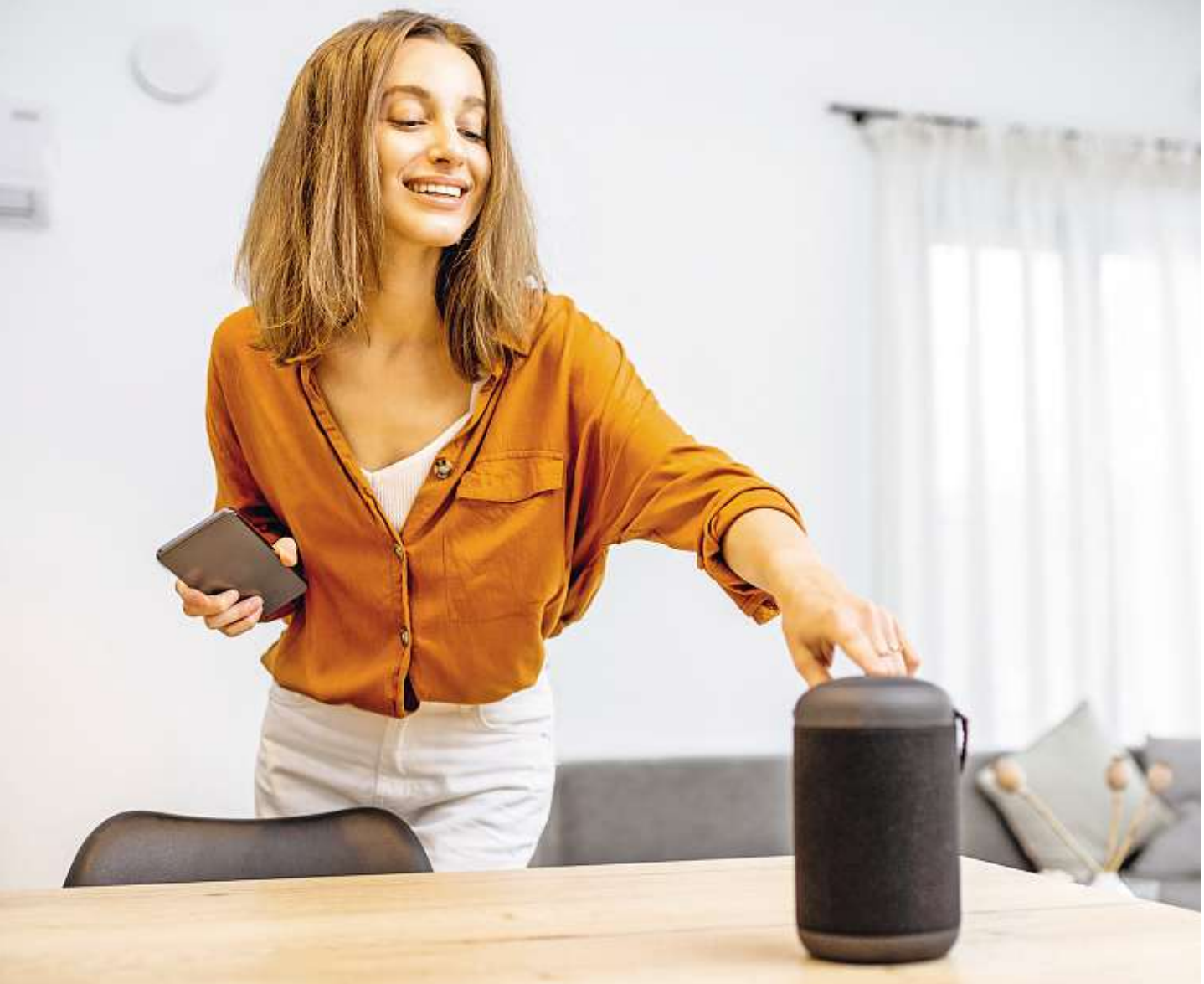
Hlavní rizika

„V současné době je celosvětově nově aktivováno každý den přibližně milion zařízení IoT. Už jen samo rozšíření určité platformy tedy představuje významné riziko. Kvalifikovaný útočník má velmi silnou motivaci se na ni zaměřit a samozřejmě tato situace s sebou nese také vyšší riziko zranitelností," říká Ondřej Šťáhlavský, ředitel společnosti Fortinet pro region střední a východní Evropy, a doplňuje: „Na straně druhé jsou velkým rizikem i sami uživatelé, kteří mohou klást bezpečnost internetu věcí na nižší úroveň a vystavit tak útočníkovi vstupenku k přístupu do sítě a potažmo k důležitým datům nebo funkcím."

Zařízení internetu věcí rychle přibývají také ve firmách s postupující automatizací výroby.

Zkušenost z praxe zohledňuje při identifikaci hlavních rizik Miloš Hrnčár ze společnosti Palo Alto Networks: „Hlavní riziko spočívá v tom, že u mnoha zařízení internetu věcí je bezpečnost často řešena až dodatečně, místo aby byla zahrnuta do jejich počátečního návrhu." Zařízení IoT mohou fungovat jako vstupní body do sítě organizace, takže je důležité, aby jejich zabezpečení bral každý podnik vážně.

„Zařízení internetu věcí jsou obecně více zranitelná a zároveň neumožňují jejich provozovatelům bezpečnost vylepšit kvůli poměrně nízké spravovatelnosti a upravitelnosti operačních systémů či firmwarů," říká k problematice



hlavních bezpečnostních rizik internetu věcí Lubomír Galatík, business unit manager HPE Aruba ve společnosti Hewlett Packard Enterprise. „Ve vaší síti se pak nacházejí zařízení, která se dají jen velmi těžko bezpečnostně zhodnotit a přijmout dostatečná opatření." Jediné, co následně zbývá, je maximálně je izolovat od všeho ostatního, na což nemusí být správci IT dostatečně připraveni.

„Jedním z hlavních rizik je, že některá zařízení internetu věcí bývají dostupná z internetu. Útočníci toho mohou využít k průniku do firemní sítě. Jak se zvyšují počty a prohlubuje využití zařízení IoT ve firmách, roste i náročnost udržet všechna tato zařízení pod kontrolou. Ideálním řešením bývá implementace principu nulové důvěry (žádné zařízení, které žádá o přístup do firemní sítě, není považované za důvěryhodné a je při každém takovém pokusu kontrolováno – pozn. red.)," rozšiřuje paletu klíčových rizik Miroslav Kořen, generální ředitel společnosti Kaspersky pro region střední a východní Evropy. To potvrzuje i Ondřej Šťáhlavský ze společnosti Fortinet: „I v případě IoT je důležité implementovat v co největší možné míře bezpečnostní přístup zvaný zero trust, který říká, že nemůžeme věřit nikomu a ničemu a musíme se podle toho k těmto zařízením chovat."

Bezpečnost v kybernetickém prostoru samozřejmě utváří řada faktorů, z nichž jen část tvoří samotné technologie či technika v podobě aplikací a zařízení. V případě internetu věcí tomu nebude jinak. Zdá se ale, že technika a programové vybavení zařízení internetu věcí hrají v jeho bezpečnosti prioritní roli. „Každý rok se k internetu připojí miliardy nových zařízení IoT a dohlédnout na všechna slabá místa a kybernetická rizika bude poměrně náročný úkol. Klíčové je přitom získání přehledu – nemůžete zabezpečit to, co nevidíte," dodává Miloš Hrnčár ze společnosti Palo Alto Networks.

Rizika v ekosystému IoT

Nejviditelnější součást implementací internetu věcí tvoří jeho fyzická zařízení. A právě jejich různorodost, obvykle vysoký počet výrobců i platforem, vzbuzují řadu obav. „Výrobci zařízení internetu věcí hrají jednu z klíčových rolí v bezpečnostním ekosystému," říká Ondřej Šťáhlavský ze společnosti Fortinet a dodává: „Bezpečnost by měla být povinnou a nedílnou součástí už samotného návrhu dané technolo-

Zajímavým příkladem bezpečnostního rizika mohou být virtuální asistenti ovládaní hlasem. Jejich mikrofon bývá trvale zapnutý a zařízení je připojeno k internetu.

> Jedním z hlavních rizik je, že některá zařízení internetu věcí bývají dostupná z internetu.

gie. To se ale v praxi bohužel dost často neděje. Dalším rizikem jsou pak sami uživatelé, ať už jednotlivci, nebo firmy, kteří ne vždy kladou IoT zařízení z hlediska zabezpečení na úroveň klasických či tradičních prostředků informačních technologií a přehlížejí i jejich vzájemnou propojenost."

Analogický pohled na roli výrobců zařízení internetu věcí předkládá i Miloš Hrnčár ze společnosti Palo Alto Networks: „Výrobci, designérské týmy a vývojáři by měli kybernetickou bezpečnost zvažovat a řešit již od počáteční fáze návrhu. To umožňuje odhalit bezpečnostní problémy a předcházet jim co nejdříve již v procesu návrhu."

Různorodá úroveň zabezpečení či péče o ni se zpravidla odvíjí od pořizovací ceny. Hodnota zařízení internetu věcí se pohybuje v širokém rozmezí od několika málo korun až po desítky milionů. „V propojeném světě může být senzor za desetikoruny připojen k síti za desítky miliard. Nemůžeme očekávat stejné investice do bezpečnostních opatření, když se hodnota prostředků IoT tak výrazně liší. Navíc tyto malé a levné senzory jednoduše nemají dostatečnou kapacitu pro vestavěné zabezpečení," doplňuje Miloš Hrnčár. „Většina dodavatelů na trhu IoT v současnosti prochází velmi dynamickým obdobím, a tak se zkrátka na bezpečnost samotných produktů nelze plně spoléhat," dodává k tématu ekosystému IoT Lubomír Galatík ze společnosti Hewlett Packard Enterprise. „Klíčovou roli hrají správci sítí a kybernetické bezpečnosti dané společnosti. Ti musí nasadit efektivní a modernizované přístupy k zabezpečení a mikrosegmentaci řešení internetu věcí."

Bezpečný přístup k IoT

Problematiku bezpečnosti internetu věcí samozřejmě nelze zužovat pouze na jeho koncová zařízení. „Důležité je nejen zabezpečení zařízení, když sjede z výrobní linky, ale také rizika a zabezpečení IoT v reálném nasazení. Zaměření pouze na bezpečnost zařízení nebere v úvahu další oblasti, jako je způsob konfigurace, síť a další zařízení, ke kterým je připojeno, nebo podnik, ve kterém se používá," vysvětluje Miloš Hrnčár ze společnosti Palo Alto Networks. Firmy by podle něho měly zajistit školení svých zaměstnanců, aby následně mohly podnikat kroky k prevenci nebo minimalizaci bezpečnostních rizik.

Kromě ochrany před hackerskými útoky je v případě IoT zapotřebí dbát také na ochranu fyzickou. „Pokud se některá zařízení nacházejí

5,8

miliardy koncových zařízení internetu věcí bylo podle odhadu analytiků společnosti Gartner na sklonku loňského roku celosvětově v provozu. Nejvíce jich nachází uplatnění v energetice (1,37 miliardy) a v oblasti fyzické bezpečnosti (1,09 miliardy). Nejrychleji ale přibývají v automatizaci budov, automobilovém průmyslu a ve zdravotnictví. Meziročně jejich počet vzrostl o více než pětinu.

delší dobu v odlehlejší lokalitě a nejsou řádně zabezpečena, existuje riziko, že s nimi může někdo neoprávněně manipulovat," upozorňuje Miroslav Kořen ze společnosti Kaspersky.

Jak vybírat IoT pro osobní potřebu

Internet věcí má v praxi svou spotřebitelskou a průmyslovou či podnikovou podobu. Lze předpokládat, že první svět více spoléhá na výchozí nastavení, druhý se s pouhým příslibem bezpečnosti nespokojí. „Jedním z hlavních kritérií výběru služeb a zařízení IoT pro osobní potřebu by měla být reputace a historie výrobce daného zařízení. Produkt koupený od oficiálního prodejce a renomovaného výrobce na tom bude s bezpečností rozhodně lépe než zařízení bezejmenného výrobce z asijského on-line obchodu," říká Ondřej Šťáhlavský ze společnosti Fortinet a dodává: „Pokud uživateli záleží na soukromí a bezpečnosti, měl by zároveň zvážit i investici do zařízení, které mu celý jeho IoT ekosystém ochrání komplexně. A to platí zejména v případě, kdy jsou do sítě zapojena nejen osobní, ale i firemní zařízení, ať už v rámci samotného podniku, či při dnes hojně využívané práci z domova."

Také další oslovení experti se shodují, že výběr zařízení by měl být podřízen kreditu, stabilitě a dlouhodobé perspektivě daného výrobce a jeho konkrétního řešení. „Důležité je si vybrat dodavatele, kteří v dané oblasti působí dlouhodobě. Pak je šance, že zákazníkem zakoupený produkt bude mít alespoň nějaký výhled na vývoj hardwaru, ale hlavně aktualizaci firmwaru," říká Lubomír Galatík ze společnosti Hewlett Packard Enterprise.

V oblasti řešení internetu věcí pro domácnosti je dnes většina produktů řízena či monitorována z cloudu, což má nepochybně své výhody, ale je to samozřejmě zároveň velké lákadlo pro hackery. „Doporučil bych vybírat si řešení těch silných a velkých firem, které své produkty a cloudové služby dokážou maximálně dobře zabezpečit a u nichž je hrozba hackerským útokem tak velké reputační riziko, že udělají maximum, aby se mu vyhnuly. Dále bych se také poohlížel po řešeních, která jsou schopna fungovat i bez dostupnosti cloudové služby jako takové. Poslední, co chcete, je nemoci si v noci rozsvítit jen kvůli nedostupnosti cloudu," dodává Galatík.

> Pokud uživateli záleží na soukromí a bezpečnosti, měl by zároveň zvážit i investici do zařízení, které mu celý jeho IoT ekosystém ochrání komplexně.

ANKETA

V čem se liší bezpečný přístup k IoT v podání podniků a jednotlivců?

Miroslav Kořen
generální ředitel pro region střední a východní Evropy, Kaspersky

Ondřej Šťáhlavský
ředitel pro region střední a východní Evropy, Fortinet

Lubomír Galatík,
Business Unit Manager HPE Aruba, Hewlett Packard Enterprise

Většina běžných domácích uživatelů zařízení internetu věcí pouze využívá jejich moderní výhody a na bezpečnost ani nepomyslí. Zajímavým příkladem mohou být virtuální asistenti ovládaní hlasem. Jejich mikrofon bývá trvale zapnutý a zařízení je připojeno k internetu. Podniky naopak čím dál více kladou důraz na bezpečnost internetu věcí a obecně disponují lepším zabezpečením svého IT díky vyšším rozpočtům, zavádění norem či regulací.

Snahy o zabezpečení IoT motivují hrozby finanční ztráty, ztráty soukromí, dobrého jména a v některých případech i hrozby ohrožení lidského života a zdraví. A podle míry tohoto rizika jsou alokovány v domácnostech a organizacích i příslušné bezpečnostní zdroje, tedy zejména čas, finance či vědomosti. Je přitom zřejmé, že hlavní rozdíl mezi jednotlivci a firmami je obecně právě ve znalostech a finančních možnostech. Nicméně i s minimem úsilí lze bezpečnost dané technologie výrazně zvýšit a případného útočníka odradit a demotivovat. Může jít o pouhé pravidelné softwarové aktualizace zařízení IoT či užívání silných hesel. Útočník totiž vždy bude mít k dispozici velké množství snadnějších cílů, kterým dá následně přednost.

U jednotlivců bych neočekával příliš vysoké schopnosti a technické prostředky potřebné k omezení bezpečnostních rizik plynoucích z praktického nasazení a využití internetu věcí. U firem bych to ale považoval za klíčovou kompetenci, zejména pokud jsou na IoT provozně závislé. S nedostatkem času, kompetence či zdrojů se můžeme potkat i v podnikovém prostředí, ale u jednotlivců se pohybujeme na úplně jiných úrovních těchto ukazatelů.

Hledáním dokumentů mohou zaměstnanci strávit minutu, ale také několik hodin

Řešení a služby společnosti Iron Mountain pro digitalizaci a správu dokumentů pomáhají firmám i organizacím snižovat náklady na ukládání digitálních dat i papírových dokumentů, dodržovat předpisy regulující nakládání s daty, řídit rizika a využívat hodnotu existujících informací.

Foto: HN – Lukáš Bíba

Na bezpečnost a zpracování informací se společnost Iron Mountain soustřeďuje již 70 let. Dnes má tato firma více než 140 tisíc zákazníků ve 39 zemích světa – včetně Česka. Na trendy v oblasti digitalizace a digitální transformace jsme se zeptali Přemysla Nikrmajera, jednatele společnosti.

Blíží se doba, kdy se firmy definitivně zbaví papírových dokumentů?
Postupně se na tuto cestu jako společnost vydáváme, ale podle mého názoru to bude ještě několik let trvat. Covid samozřejmě digitální transformaci výrazným způsobem urychlil a upozornil vedení firem, že tuto oblast není možné zanedbávat či podceňovat – jak z pohledu efektivity, tak i samotné provozuschopnosti firmy při práci z domova. Velkým katalyzátorem bude také Národní plán obnovy, spolufinancovaný EU, který podpoří i digitální transformaci státní správy a malých i středních firem.

Nahrává větší míře digitalizace také česká legislativa?
Můžeme říci, že česká legislativa nijak nezaostává za tou evropskou. Od roku 2016 jsme museli implementovat evropské nařízení EIDAS, díky čemuž vznikl Zákon o službách vytvářejících důvěru pro elektronické transakce (297/2016 Sb.). Ten zaručuje, že existuje ekvivalent vlastnoručního podpisu v elektronickém prostředí a že státní správa, samospráva či soudy nemohou dokument odmítnout pouze proto, že je v elektronické podobě.

Na druhou stranu, výše uvedená legislativa řeší primárně elektronickou komunikaci mezi subjekty státní správy a mezi státní správou a třetími stranami (občan či firma) a nijak příliš elektronickou komunikaci mezi firmami navzájem.

Ve kterých oblastech pokročila digitalizace nejdále?
Z pohledu managementu dokumentů ve firmách lze říci, že jako jedny z prvních přišly na řadu účetní dokumenty – konkrétně faktury, které řada firem digitalizuje již několik let, ať už interně či kompletním outsourcingem včetně následné úschovy dokumentů. Nový trendem v této oblasti jsou fakturační portály, kde dodavatelé zadávají faktury již v elektronické podobě a často vyplňují také různá indexová pole. Především korporace tak přenáší náklady digitalizace na své dodavatele a faktury následně automatizovaně zpracovávají. Malé a střední podniky tyto činnosti často stále ještě realizují vlastními silami, ačkoliv by díky outsourcingu či automatizaci mohly ušetřit.

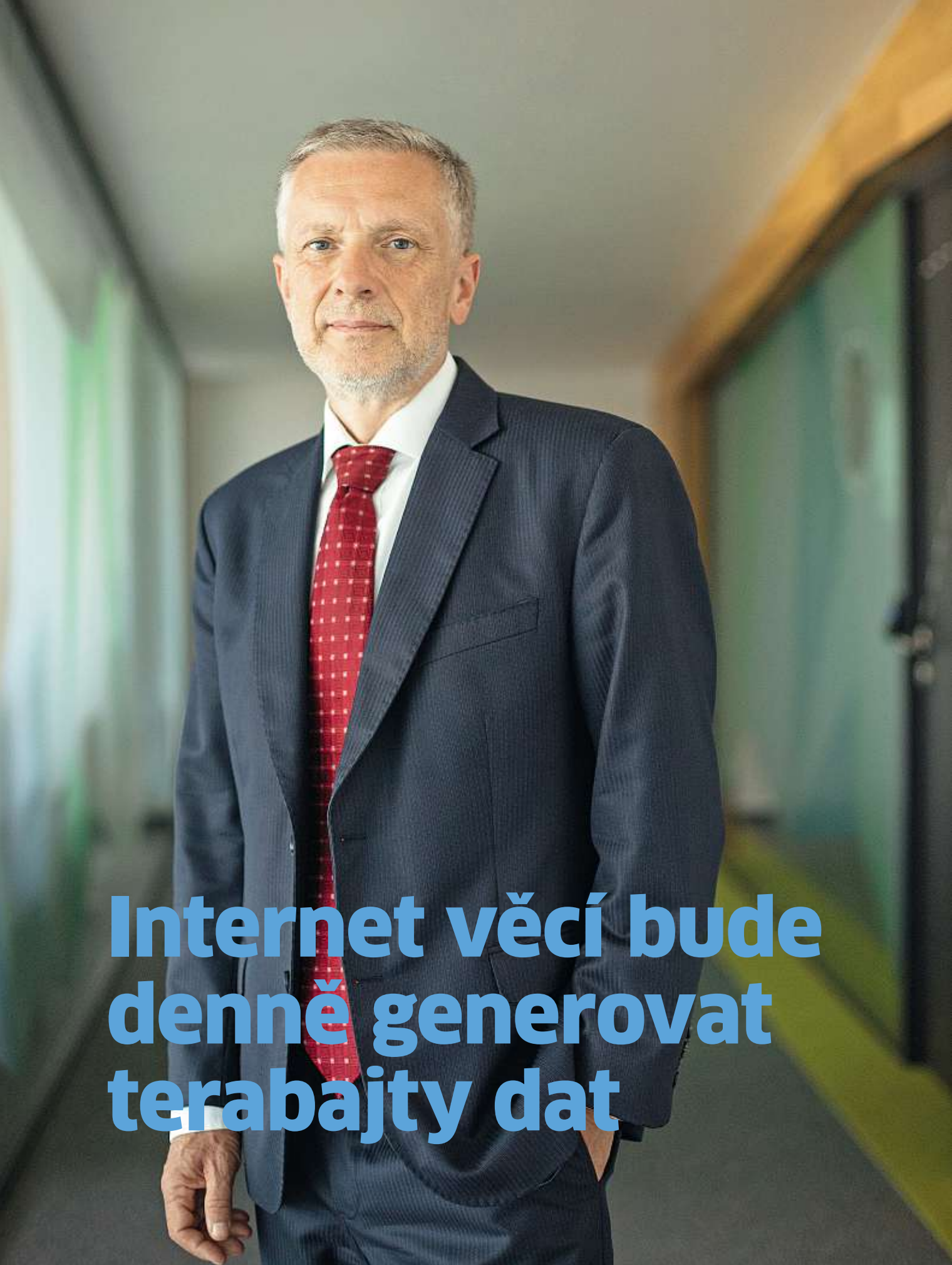
Které rutinní úkoly pomáhá digitalizace automatizovat?
Digitalizace či digitální transformace řeší nejen automatizaci rutinních úkolů. Její hlavní přidanou hodnotou je snadná dohledatelnost a přístupnost dokumentů, včetně snadného sdílení či vyhledávání podle obsahu nebo možnost filtrování většího objemu dokumentů podle různých kritérií. Aplikace umělé inteligence pak přidanou hodnotu dokumentů v digitální podobě výrazným způsobem povyšují a umožňují jejich automatizovanou klasifikaci, analýzu či vizualizaci, ale také sledování různých vzorců při odhalování podvodného jednání a podobně.

O jaká řešení digitalizace mají české podniky v současné době největší zájem?
V souvislosti s covidovou pandemií sledujeme nárůst zájmu klientů o služby digitální podatelny pro nově vznikající dokumenty, tedy přesměrování veškerých fyzických dokumentů na třetí stranu, která dokumenty přijme, zdigitalizuje, prostřednictvím elektronického úložiště či aplikací pro workflow rozdistribuuje mezi koncové uživatele a následně ve fyzické podobě dokumenty uloží až do doby jejich skartace. Z důvodu zajištění kontinuity procesů při práci z domova firmy také velmi často zpětně digitalizují své fyzické archivy různé dokumentace.

Kromě toho roste zájem o elektronickou úschovu dokumentů, ideálně s využitím cloudových řešení, a s tím spojená časová razítka a elektronické podpisy. Firmy velice často preferují komplexní řešení služeb managementu životního cyklu dokumentů ve fyzické, ale zároveň také v elektronické podobě.

Jakou návratnost investic do digitalizace a souvisejících služeb mohou firmy očekávat?
Pokud klient porovnává pouze náklady na uložení historické dokumentace ve fyzické či elektronické podobě, vyplatí se digitalizovat pouze dokumenty s dlouhou dobou uložení (například 40 a více let) z důvodu prvotních nákladů na skenování a vytěžení dokumentů. Pokud však klienti zvažují přínosy digitální transformace v širším měřítku, tedy z pohledu dohledatelnosti či přístupnosti a sdílení dokumentů, možnosti vyhledávání, automatizace manuálních činností, menší chybovosti, sledování přednastavených procesů a jejich efektivity, možnosti analýzy dat a tvorby přidané hodnoty, uvidí návratnost investic ve zcela jiném světle. Například hledáním dokumentů mohou zaměstnanci strávit minutu, ale také několik hodin týdně. Jinými slovy, návratnost investice lze spočítat v momentě, kdy dokážete kvantifikovat přidanou hodnotu všech výše zmíněných složek.

Více o digitalizaci a správě dokumentů na www.ironmountain.cz.



Internet věcí bude denně generovat terabajty dat

text: Radek Kubeš, foto: HN – Matej Slávik

Závislost firem na datech dramaticky snižuje požadovanou dobu obnovy dat, říká **Martin Štětka**, regionální manažer zodpovědný za obchodní aktivity společnosti Veeam Software v regionu CEE.

V důsledku masivního přechodu na práci z domova firmy v oblasti ukládání a zálohování dat stále častěji využívají cloudové, hybridní nebo multicloudové strategie. Závislost firem na datech také dramaticky snižuje požadovanou dobu obnovy dat, jejichž objem navíc neustále exponenciálně narůstá, říká v rozhovoru Martin Štětka, regionální manažer zodpovědný za obchodní aktivity společnosti Veeam Software ve střední a východní Evropě. Terabajty dat ze zařízení internetu věcí pomůže podle něho zkrotit komplexní a správně nastavená strategie správy dat a moderní technologie jako edge computing, umožňující zpracování dat přímo v koncových zařízeních.

Zálohování je velmi důležitou součástí ochrany dat, jak pomáhá proti aktuálním kybernetickým hrozbám – především ransomwaru?

Zálohování mimo hlavní lokalitu, off-line zálohování a robustní možnosti obnovy po havárii mohou podnikům pomoci obnovit data, která útočníci zašifrovali. Vzhledem k tomu, že rizika a možnosti ransomwaru jsou různorodé, potřebují podniky plán prevence, který zvýší odolnost jejich IT. Z hlediska síťové architektury je nejlepším způsobem boje proti ransomwaru mikrosegmentace. Znamená to rozdělení sítě na samostatné oblasti, na jejichž hranicích probíhá bezpečnostní kontrola a přísné monitorování datového provozu. Tak zůstanou útočníci uzamčeni v příslušném segmentu, což zabrání rozšíření jejich aktivit do okolního prostředí. Chránit síť před útoky prostřednictvím odcizených přístupových údajů a uživatelských účtů pak pomáhá princip nulové důvěry, v jehož rámci jsou přesně definována přístupová práva. Každý uživatel tedy vidí ze sítě pouze to, co má povoleno vidět – zbytek zůstává neviditelný.

Kromě toho doporučujeme pravidlo 3-2-1-1-0, což je rozšířená varianta zálohování typu 3-2-1, kdy jsou data uchovávána ve třech kopiích (produktivní data a dvě kopie). Kopie by měly být na dvou různých typech médií, přičemž jedna z nich by měla být uložena mimo podnikovou síť. V souvislosti s ransomwarem jsme pravidlo 3-2-1 doplnili o jedničku a nulu. Jedna z těchto kopií by měla být neměnná, a tedy chráněná proti ransomwaru nebo útokům zevnitř. Toho lze dosáhnout například využitím funkce S3 Object-Lock poskytovatelů cloudových služeb nebo také zálohováním, které je outsourcováno poskytovateli služeb prostřednictvím služby Cloud Connect s aktivovanou ochranou proti zneužití vnitřních informací. Dobrou ochranu samozřejmě poskytují i tradiční pásky, pokud jsou pravidelně vyměňovány. Nula znamená doslova „nulovou“ chybovost při obnově díky průběžně prováděným a automatizovaným testům obnovy a antivirovým kontrolám záloh.

Jak se změnily potřeby firem v oblasti zálohování dat a kam se budou dále vyvíjet?

Pandemie zanechala stopy v mnoha oblastech souvisejících s IT. V důsledku masivního přechodu do režimu práce z domova firmy stále častěji využívají cloudové, hybridní nebo multicloudové strategie, aby zajistily kontinuitu svého podnikání a měly svá data neustále k dispozici a chráněná. To ale přináší i potřebu rozšířit stávající ochrany také na platformy pro spolupráci, jako je Microsoft Teams, nové koncové body i data v cloudu. Dobré je, že existuje potřebná technologie a její implementace není žádná raketová věda.

Enormní závislost podniků na datech také způsobuje, že se dramaticky snižuje požadovaná doba obnovy dat. To znamená mít nejen ověřené kopie dat, která lze obnovit během několika minut, ale dokonce i nepřetržitou ochranu dat, kdy je potenciální ztráta dat omezena na minuty a obnova kritických úloh trvá několik sekund.

Objem všech typů dat celosvětově exponenciálně roste. V podnikovém prostředí vidíme

> “ Enormní závislost podniků na datech způsobuje, že se dramaticky snižuje požadovaná doba obnovy dat.

Martin Štětka
regionální manažer,
Veeam Software

Ve společnosti Veeam Software pracuje více než deset let a zaměřuje se zejména na zavádění inovativních technologií správy dat do praxe v podnikovém prostředí. Je zodpovědný za obchodní aktivity firmy ve střední a východní Evropě. V Česku je Veeam Software nejen největším dodavatelem řešení na zálohování a ochranu dat, ale ve výzkumném a vývojovém centru, které se nachází v Praze a je největším R&D centrem společnosti, vyvíjí softwarové produkty pro zákazníky po celém světě.

masivní nárůst zejména u dat ze standardních podnikových systémů, nestrukturovaných dat z internetového provozu a stále rychleji rostoucí data z internetu věcí (IoT). A také je třeba zmínit kontejnerizaci a Kubernetes (automatickou koordinaci virtualizace na úrovni operačního systému – pozn. red.) – technologie, které nabírají na síle a podle předpovědí způsobí v IT stejnou revoluci jako před mnoha lety virtualizace.

Jaké funkce potřebují firmy pro ukládání a zpracování dat ze zařízení internetu věcí?
V mnoha situacích je jedinou schůdnou cestou k vytvoření rozsáhlých IoT řešení hyperškálovatelný veřejný cloud. Realita je taková, že řešení využívající tisíce a tisíce zařízení IoT bude v reálném čase generovat tolik dat, že rychle vyčerpá komunikační linky a úložné zdroje tradičního datového centra. Veřejné cloudy naproti tomu nabízejí škálovatelnost, která tuto změnu a narůstající provoz dokáže pojmout. Tím, že součástí řešení IoT bude od samého počátku i cloud, se firmy vyhnou složitým problémům, které by později mohly ohrozit jejich infrastrukturu a zařízení.

Kromě toho existuje ještě jedna překážka, kterou je třeba překonat. Mnoho výrobních linek nebo systémů nelze zcela nahradit zařízeními IoT. V některých případech zde i nadále běží stará zařízení a stroje s protokoly SCADA (Supervisory Control and Data Acquisition), které jsou zastaralé a musí být stále integrovány jako starší hardware. Právě ty se však mohou stát vstupní branou pro útoky, jako je ransomware, protože tyto stroje nebyly nikdy určeny k připojení do internetu nebo cloudu. Jejich data dříve putovala jen v rámci omezeného produkčního prostředí, ale nyní jsou směrována do různých systémů prostřednictvím cloudových nebo multicloudových prostředí, a dokonce i do dalších lokalit. I tato data se denně hromadí a musí být zahrnuta do strategie zálohování.

Má-li být internet věcí rozšířen ve velkém měřítku, navíc v kombinaci s edge computingem a sítí 5G, musí být cloudové prostředí i správa dat řešeny od samého počátku. Příliš často se při plánování zanedbává účinné řešení zálohování a obnovy dat, přestože by si všichni měli uvědomovat, že ne všechny hrozby lze odvrátit.

Jak velký nárůst tohoto typu dat v blízké budoucnosti očekáváte?
Zařízení internetu věcí se stále více integrují do všech procesů podniku nebo výroby – ať už jde o stroje obecně, autonomní vozidla, chytré budovy, mobilní zařízení nebo zdravotnické systémy. Kde dříve jezdil jen vysokozdvižný vozík, může brzy síť IoT zařízení tvořit systém, který denně generuje několik terabajtů dat. A firma může mít desítky takových systémů. Celkově se tvoří téměř nezvládnutelné množství dat, které již vyžaduje složitý kompromis mezi inteligentními zařízeními a nežádoucími problémy se sítí a úložištěm kvůli požadavkům na ukládání dat, šířku pásma a výpočetní výkon.

> “
> Příliš často se při plánování zanedbává účinné řešení zálohování a obnovy dat.

Souvisí zpracování dat ze zařízení internetu věcí s aktuálním trendem edge computingu?
Samozřejmě, je zde přímá souvislost. Edge computing je koncept nasazení IT, které pomáhá maximalizovat dostupnost aplikací a dat blíže k uživateli nebo v rámci internetu věcí. Zajišťuje, že výpočetní kapacita je využívána přímo v koncových zařízeních, kde probíhá jak sběr dat, tak jejich vyhodnocení, případně i ukládání, které je zpravidla náročné na datový tok. Zpracování dat přímo v zařízeních IoT, tedy na „okraji sítě“, má řadu výhod, od úspor na přenosových kapacitách a nižšího zatížení serverů přes zrychlení procesů až po rychlejší dostupnost aktuálních výsledků v místě pořízení dat. Tato decentralizace výpočetních sil zvyšuje nejen efektivitu provozu, ale snižuje i případná rizika a dopady bezpečnostních incidentů.

Jak mohou firmy ušetřit na ukládání neustále rostoucího množství dat z internetu věcí?
Nejen v případě dat z IoT, ale obecně v oblasti ukládání dat lze optimalizovat náklady vhodnou kombinací úložišť. Pro data z IoT je vhodná kombinace cloudu a datacentrových, respektive edge technologií. Ukládání archivních dat na primární úložiště je zbytečně drahé a i ukládání aktivních dat do archivní vrstvy objektového úložiště se může prodražit. Klíčová je tedy klasifikace IoT dat z pohledu jejich obchodní hodnoty v průběhu jejich životního cyklu.

Jak se u dat z internetu věcí řeší obvyklý rozpor mezi rychlou dostupností dat, potřebnou kapacitou a souvisejícími náklady?
Ambicí pro nasazení IoT je umožnit analyzovat dostupná data tak, abychom mohli přijímat správná rozhodnutí v reálném čase a dodat našemu podnikání vyšší hodnotu nebo získat konkurenční výhodu. Tomu by měla odpovídat i naše ochota investovat. Praxe ale naopak ukazuje, že IoT přináší podnikům výrazné úspory, které kompenzují náklady vynaložené na jeho implementaci. Konkrétně můžeme zmínit, že náklady spojené se zavedením IoT vyrovnají vyšší efektivita provozu, zkrácení prostojů či včasná eliminace problémů ve výrobě, zlepšení správy skladů, nižší náklady na personál v provozu, ale například i úspory v oblasti spotřeby energií. V neposlední řadě lze zmínit i vyšší bezpečnost.

Jak mohou firmy poznat optimální poměr mezi využíváním lokálních a cloudových úložišť?
Stejně jako u každého jiného rozhodování je i zde klíčem důsledná analýza. Je potřeba detailně analyzovat data a jejich nákladové parametry. Musíme zvážit, s jakými daty pracujeme, kam je primárně ukládáme, kde a na jak dlouho je můžeme uchovávat a jak dlouho danou kopii dat potřebujeme mít k dispozici. A ani zde nesmíme zapomínat na bezpečnostní rizika a musíme zvážit způsob ochrany proti případným útokům v té které lokalitě.

text: Lukáš Kříž, foto: Shutterstock

Edge computing zrychluje data, ale přináší i rizika

Edge computing představuje nové paradigma, ve kterém jsou výpočty a data umístěny na okrajích sítě, co nejblíže ke zdroji a místu využití dat ve fyzickém světě. Uplatnění nachází především v hraničních či okrajových prostředích, což definovalo i jeho název.

Minimálně teoreticky se edge computing začal rozvíjet před několika lety a v dosavadní praxi je nejčastěji vnímán jako doplněk cloud computingu anebo jako řešení některých jeho nedostatků. V minimalistickém pojetí může konceptu edge computingu vyhovět i jedno jediné zařízení, které interně sebere, zpracuje a vyhodnotí určitá data. O svém stavu nebo nestandardních vstupech informuje prostřednictvím sítě nadřízenou instanci.

Výše popsaný model naznačuje dvojí tvář edge computingu. Někteří odborníci doporučují, aby se jeho pojetí rozdělilo právě na zařízení a konektivitu, hovoří o edge devices a edge cloud. Druhý uvedený termín samozřejmě nepokrývá jen komunikační linky, ale i navazující systémy, jimž jsou informace určeny.

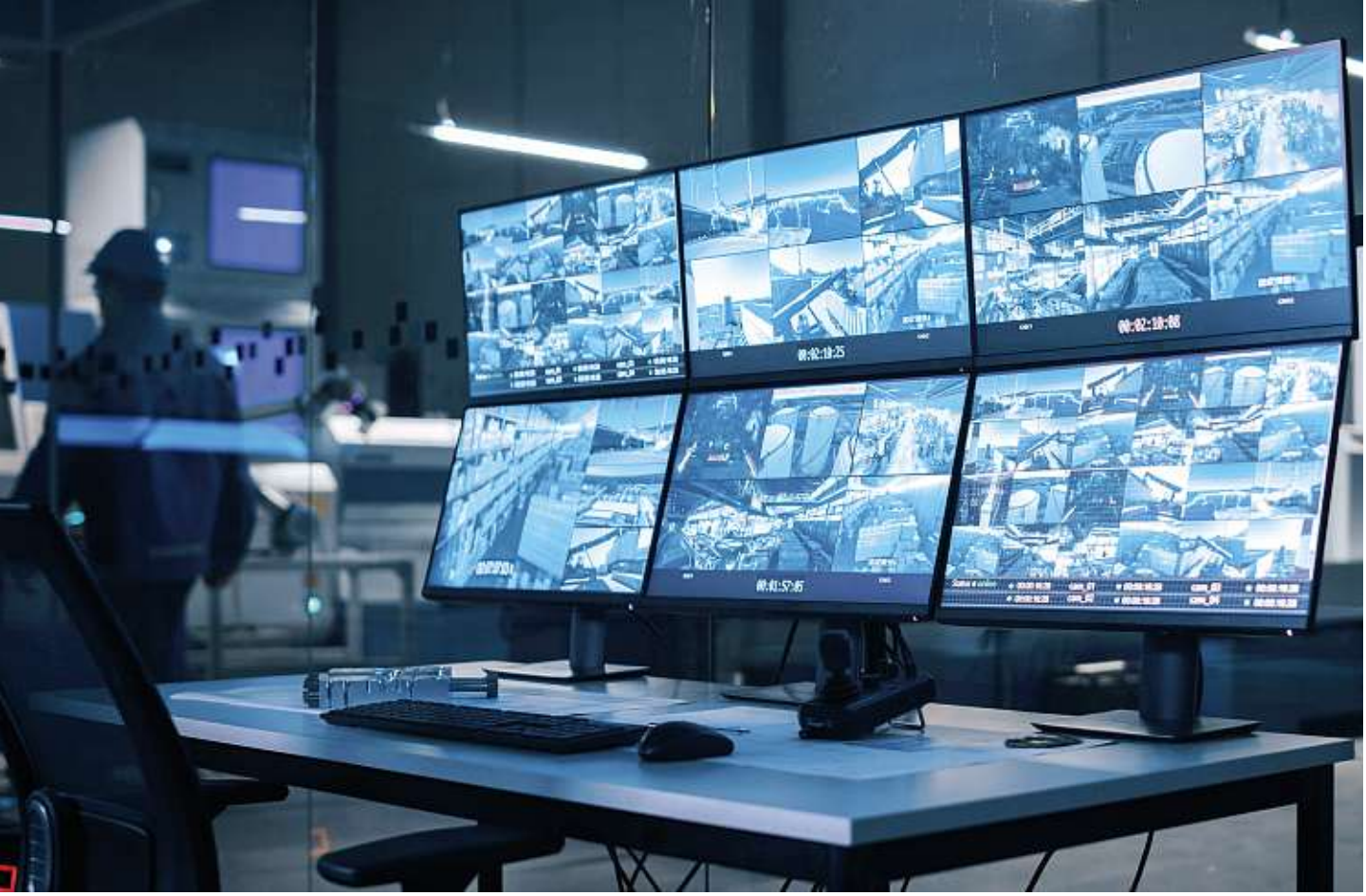
Edge computing v současnosti představuje atraktivní koncept, což potvrzují i slova Jana Hakena, business development managera pro globální výpočty a sítě ve společnosti Dell Technologies: „Největší zájem projevuje průmysl. V něm většina zákazníků cítí z nových technologií velký potenciál pro zvýšení své konkurenceschopnosti. Zde jde edge computing ruku v ruce s rozvojem sítí 5G. Velký zájem se objevuje i ve veřejném sektoru, v němž nabízí nemalý potenciál v různých aplikacích pro ochranu obyvatel."

Evropská data o rozšíření edge computingu v průmyslu představuje Jan Burian, analytik společnosti IDC pro oblast průmyslu: „V loňském průzkumu mezi evropskými výrobními firmami uvedlo 55 procent respondentů, že edge computing v provozní oblasti nevyužívají a ani to nemají v blízké budoucnosti v plánu. Bezmála pětina dotázaných podniků jej sice v současnosti nevyužívá, ale do dvou let s ním začnou pracovat. A 16 procent respondentů již edge computing pro aplikace ve svém provozu nasadilo."

Nejednotnost pojetí

Nad obsahem a významem termínu edge computing zatím nepanuje jednoznačná shoda. Pojetí ze světa telekomunikačního byznysu přibližuje Jiří Rynt, key account manager ve společnosti Ericsson: „Na poli telekomunikačním často používáme pojmy mobile edge computing a multi-access edge computing. Jde o posunutí výpočetních zdrojů a úložišť dat blíž ke konečnému

> V současné době je edge computing chápán jako umístění výpočetního výkonu, zejména serverů, mimo datové centrum.



uživateli, v tomto případě tedy buď v rámci sítí operátorů, nebo například v továrních budovách a zařízeních firem, v domácnostech a dopravních prostředcích od vlaků a letadel po soukromé vozy."

„Pojem edge computing bude jistě ještě vyzrávat," říká Jan Haken ze společnosti Dell Technologies a dodává: „V současné době je chápán jako umístění výpočetního výkonu, zejména serverů, mimo datové centrum. Servery se objevují přímo ve výrobních halách, na ulicích, ve speciálních vozidlech."

Benefity edge computingu

„Z průzkumu společnosti IDC vyplývá, že mezi hlavní důvody pro zavádění edge computingu v evropském průmyslu patří zvyšování spolehlivosti a odolnosti IT systému, možnost využívat analytické modely přímo v místě vzniku dat, zajištění IT bezpečnosti a minimalizace latence při přenosu dat v rámci industriální sítě," potvrzuje hlavní benefity Jan Burian ze společnosti IDC.

Hlavní přínosy edge computingu, které dnes dodavatelé a jejich zákazníci vnímají, přibližuje Jan Haken ze společnosti Dell Technologies: „Největší výhody nabízí aplikacím, jež potřebují výkon a zpracovávají velké množství dat, u nichž nás zajímají jen výsledky. Jednoduchým příkladem je rozpoznávání osob s využitím umělé inteligence. Nezajímají nás hodiny kamerového záznamu, ale jen fotografie osob vstupujících například do skladu a to, zda mají oprávnění ke vstupu. Dochází k velké redukci dat u zdroje, šetří se kapacita internetové linky a vzhledem k rychlosti odpovědí je možné použít výsledky k řízení dalších aplikací."

Typickým příkladem využití edge computingu je rozpoznávání osob s využitím umělé inteligence. Nezajímají nás hodiny kamerového záznamu, ale jen fotografie osob vstupujících například do skladu a to, zda mají oprávnění ke vstupu.

Edge cloud

nepokrývá jen komunikační linky, ale i navazující systémy, jimž jsou informace určeny.

Výčet mnoha benefitů edge computingu představuje Ivo Němeček, ředitel projektové divize ve společnosti Simac Technik: „Přináší výhody v případech, když potřebujeme zlepšit doby odezvy vzdálené aplikace, rozprostřít výpočetní výkon a zrychlit tak zpracování dat, snížit nároky na přenosové pásmo, zkrátit vzdálenost stanice napájené z baterie od nejbližšího uzlu, zmenšit tak potřebu vysílacího výkonu a prodloužit tím životnost baterie, zjednodušit zpracování dat na koncové stanici, prodloužit životnost baterie snížením výkonu potřebného pro zpracování dat, zvýšit odolnost řešení a v neposlední řadě posílit jeho bezpečnost."

Příležitosti pro byznys

Edge computing nachází uplatnění v mnoha oborech, které ovšem podle Jana Hakena ze společnosti Dell Technologies nejčastěji sdílí jeden společný aspekt: „V současné době je největší přínos v aplikacích využívajících zpracování obrazu. V praxi jde například o kontrolu kvality, zefektivnění výroby, bezpečnost, Smart Cities, analýzu chování zákazníků v obchodech, autonomní vozidla a mnohé další."

Potenciál edge computingu je ale podle Jaroslava Novotného, IT architekta ve společnosti Oracle, mnohem širší: „Obecně jej lze efektivně nasadit všude tam, kde vzniká velké množství dat mimo páteřní datová centra. Typicky jde o projekty internetu věcí, zdravotnická zařízení, výrobní závody, systémy CCTV a podobně. A v je-

jich případě nelze hovořit o výhodě, ale spíše o nutnosti. Edge computing umožňuje masové zpracování dat co nejblíže ke zdrojům a násobně snižuje nároky na konektivitu a výkon centrálního datového centra."

„V rámci konkrétních příkladů v prostředí českých firem vidím velký potenciál zejména v aplikacích spojených s prediktivní údržbou, monitoringem podmínek, prediktivní kvalitou, vzdáleným sledováním strojů a sledováním nebo vyhodnocováním odchylek ve výrobě," doplňuje Jan Burian ze společnosti IDC.

„Možnosti edge computingu je nutné vidět v širším kontextu, kdy tento koncept dovolí vzniknout mnoha novým případům užití, například řešením založeným na internetu věcí nebo také privátních 5G sítích," říká Jiří Rynt ze společnost Ericsson a dodává: „Předpokládáme, že za rok či dva začnou mobilní operátoři ve svých celostátních sítích uplatňovat network slicing (provoz virtualizovaných a nezávislých logických sítí na stejné fyzické síťové infrastruktuře – pozn. red.), což umožní mnohem pokročilejší propojení veřejných sítí s firemními řešeními."

Kdy se edge computingu vyhnout

Koncept edge computingu ale nedoprovázejí jen pozitiva. Hodí se pro řadu poměrně specifických situací, což naznačuje už jen jeho definiční mnohotvárnost, ale musí v nich svým provozovatelům dávat ekonomický smysl. „Vždy je třeba zvážit, jestli se investice do edge computingu v konkrétním případě vyplatí. Tedy zda není levnější a efektivnější postavit dané řešení centralizovaně," říká Jiří Rynt ze společnosti Ericsson.

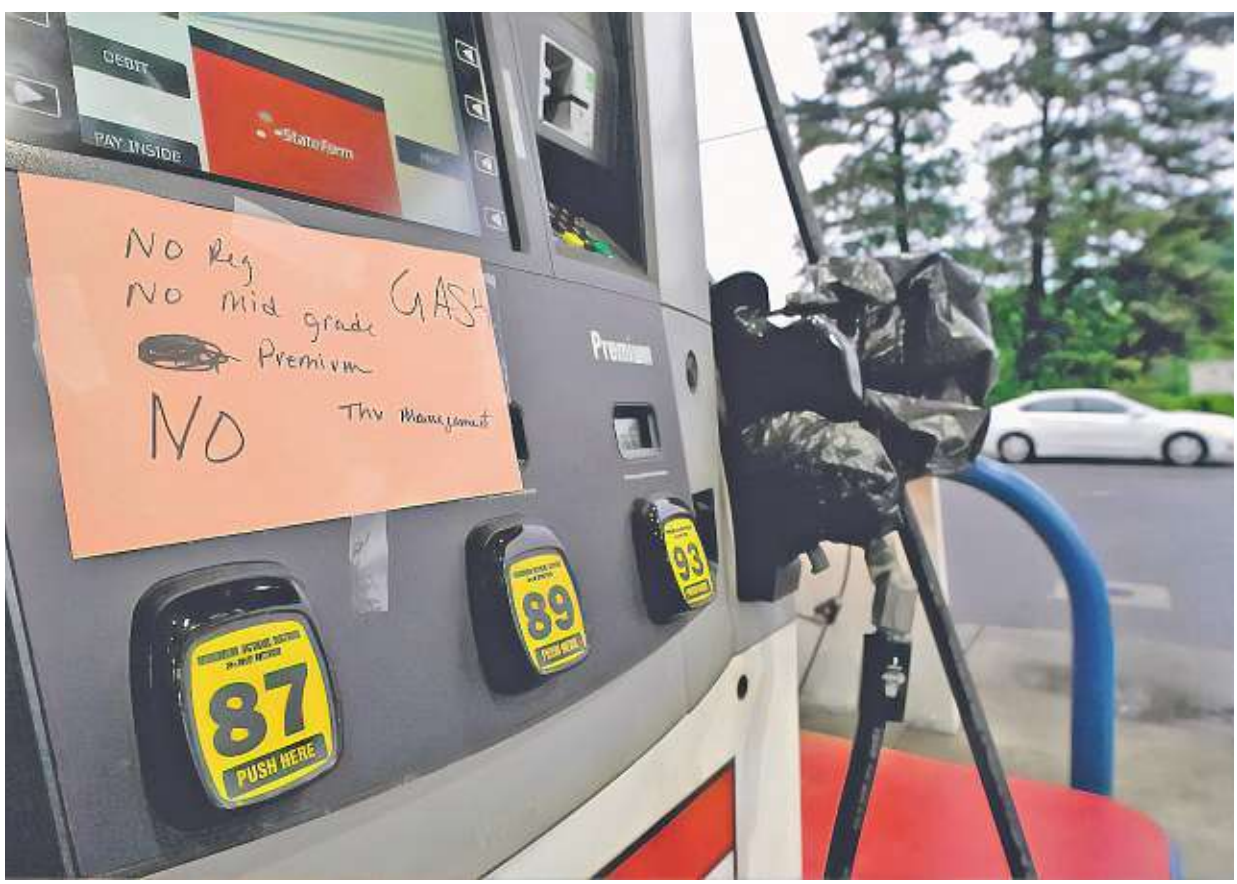
Ekonomické aspekty zohledňuje i Jaroslav Novotný z firmy Oracle: „Všude tam, kde lze pomocí komunikace na nějaký centralizovaný systém poskytnout uživateli nebo cílovému systému požadovanou IT funkcionalitu v odpovídající kvalitě, zejména z pohledu latence, nebude nasazení konceptu edge computingu ekonomicky výhodné."

Na bezpečnostní hledisko odkazuje Jan Haken ze společnosti Dell Technologies: „Spolu s rozvojem edge computingu je nutné vnímat veškerá rizika s ním spojená. Konkrétně jde o fyzickou bezpečnost, možnost narušení sítě, citlivost zpracovávaných dat nebo rychlé procesní změny. Tyto aspekty by měly být promyšleny a rizika odstraněna před začátkem všech projektů edge computingu."

Zcela pragmatický postoj k otázce, kdy se vyhnout edge computingu, zaujímá Ivo Němeček ze společnosti Simac Technik: „Když všechno funguje, jak má, i bez edge vrstvy."

> Potenciál vidím zejména v aplikacích spojených s prediktivní údržbou, monitoringem podmínek, prediktivní kvalitou, vzdáleným sledováním strojů a sledováním nebo vyhodnocováním odchylek ve výrobě.

Na automatizaci sází už i kyberzločinci



Největším rizikem v oblasti kybernetické bezpečnosti zůstává pro firmy i nadále ransomware. Díky automatizaci mohou vyděračské útoky provádět i méně zkušení kyberzločinci.

Kvůli nedávnému útoku na společnost Colonial Pipeline, provozovatele obří palivové sítě v USA, došlo k zastavení zásobování 12 tisíc čerpacích stanic benzinem a naftou a vyhlášení stavu nouze v 17 amerických státech.

text: Radek Kubeš, foto: ČTK, Shutterstock

Vyřadit z provozu velký podnik, nemocnici nebo třeba provozovatele kriticky důležité infrastruktury vyžaduje méně úsilí, než by se mohlo zdát. Aktuální příklady úspěšných kybernetických útoků přitom najdeme nejen v Česku (brněnská či benešovská nemocnice, OKD a další), ale i jinde po světě. Kvůli nedávnému útoku na společnost Colonial Pipeline, provozovatele obří palivové sítě v USA, došlo k zastavení zásobování 12 tisíc čerpacích stanic benzinem a naftou a vyhlášení stavu nouze v 17 amerických státech. Ransomware, vypuštěný pravděpodobně hackerskou skupinou DarkSide, přitom neútočil na samotný potrubní systém, namísto toho zasáhl účetní systémy provozovatele, který bez nich nemohl evidovat distribuci paliva. Požadované výkupné ve výši kolem 90 milionů korun zaplatila společnost Colonial Pipeline během pár hodin, ale výpadek přesto trval několik dní.

Podniky z oblasti energetiky a ropného či plynového průmyslu jsou pro kyberzločince velmi lákavé. Jak ukazuje celosvětový průzkum The State of Ransomware 2021 společnosti Sophos, požadavek na zaplacení výkupného v uplynulém roce splnilo 43 procent napadených organizací z tohoto sektoru. Experti to přisuzují faktu, že tyto firmy provozují obvykle velké množství starší infrastruktury, kterou nelze snadno obnovit. Hned druhou nejvyšší úroveň zaplacení výkupného vykazují organizace státní a veřejné správy (42 procent). Ale i když oběť zaplatí, šance na získání všech dat zpět jsou velmi malé. Podle zmíněné studie organizace, které zaplatily výkupné, získaly zpět v průměru jen 65 procent zašifrovaných souborů. Skoro třetina (29 procent) respondentů uvedla, že se jim podařilo obnovit 50 procent nebo méně souborů, a pouze 8 procent společností získalo zpět všechna svá data. Průměrná výše zaplaceného výkupného přitom činila v přepočtu přes 3,5 milionu korun. Zaplacení výkupného představuje ale jen část nákladů na nápravu po útoku. Průměrné náklady na odstranění dopadů ransomwarového útoku (včetně nákladů na odstávku, čas pracovníků či ztráty zisku) činily v přepočtu skoro 39 milionů, což je mimochodem více než dvojnásobek oproti údaji z roku 2020.

Nové triky kyberzločinců

Prostředí kybernetických hrozeb a taktika útočníků se samozřejmě neustále vyvíjí. Sophos zjistil, že sice klesá podíl ransomwarových útoků, při kterých se kyberzločincům podaří zašifrovat data napadené organizace, ale zároveň se meziročně více než zdvojnásobil podíl útoků, kdy je oběť vydírána nikoli na základě zašifrování, ale kvůli odcizení citlivých podnikových dat a hrozbě jejich zveřejnění. Bylo by přitom naivní se domnívat, že útočník po zaplacení výkupného získaná data zlikviduje. Naopak se vyskytují případy, kdy kyberzločinci vydírají také klienty napadené organizace. To je případ i jedné finské kliniky, která sice za odcizená data výkupné zaplatila, ale zločinci se poté obrátili s dalšími finančními požadavky přímo na pacienty, jejichž zdravotní záznamy získali.

The State of Ransomware 2021

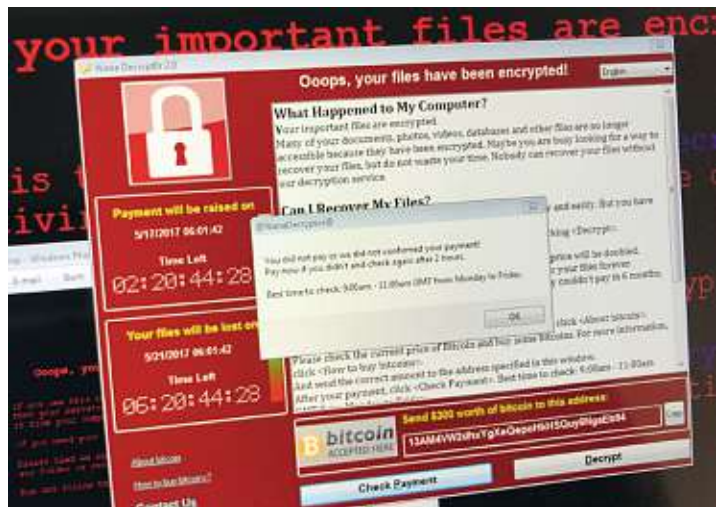
Podle celosvětového průzkumu společnosti Sophos splnilo v uplynulém roce požadavek na zaplacení výkupného 43 procent napadených organizací z oblasti energetiky a ropného průmyslu. Druhou nejvyšší úroveň úspěšnosti vydírání vykázaly organizace státní a veřejné správy, kde výkupné zaplatilo 42 procent napadených.

> Bylo by naivní se domnívat, že útočník po zaplacení výkupného získaná data zlikviduje.

Vedle ransomwarových útoků, které jsou navíc často automatizované, což otvírá prostor pro méně zkušené útočníky, sledujeme také nárůst vysoce sofistikovaných útoků. Kyberzločinci totiž zjistili, že zaměřit se na konkrétní zajímavou oběť a věnovat jí značnou péči se vyplatí více než široce útočit na velké množství cílů bez většího zisku. „Takový útok ale nelze provést automatizovaně pouze za pomoci malwaru. Proto se útočníci přetransformovali ve skupiny tvořené lidmi rozdílných rolí. Důležité je nejen programování, ale i dobrá znalost týkající se administrace sítí nebo nástrojů využívaných penetračními testery. Penetrační průniky spolu s nákupem již zavedeného backdooru jsou také často vektor útoku, jak se tyto skupiny do sítí svých obětí dostávají. Nezřídka k tomu dochází za pomoci zneužití softwarové zranitelnosti, což je sám o sobě další trend této doby," vysvětluje Václav Zubr, Pre-Sales Engineer společnosti ESET. Problém je, že takové útoky mohou proběhnout kompletně bez použití škodlivého kódu, takže klasické antiviry nemají co detekovat.

Charakteristickým rysem, který v současnosti postihuje oba tábory stejnou měrou, je nedostatek personálu. I útočníci proto stále více využívají moderních technologií, jako je automatizace. „Moderní hrozby jsou schopny zcela autonomně ovládnout infrastrukturu v řádu desítek minut, přičemž útočník má za úkol pouze posoudit hodnotu cíle. Zda jde o strategický cíl, jako je banka nebo vládní instituce, nebo jen o subjekt, kterému stáhne a zašifruje data pro další případné použití, typicky pro vydírání nebo získání informací o obchodních partnerech či know-how. Takové chování není možné odhalit jinak než s využitím technik umělé inteligence nebo analýzou chování," uvádí Petr Zubrický, bezpečnostní expert ve společnosti S&T CZ. Na straně obránců proto roste význam využívání technik založených na umělé inteligenci, jako jsou pokročilé IDS (intrusion detection system) a IPS (intrusion prevention systems) na detekci a prevenci útoků, ale i kontroly chování uživatelů nebo administrátora za účelem detekce abnormálního chování.

Možná trochu nečekaný problém představují i bezpečnostní kamerové systémy. „Velkým problémem je zanedbaná údržba a aktualizace IP kamerových systémů. I bezpečně instalované kamery se tak s postupem času mohou stát snadným terčem pro hackery. Doporučujeme proto u kamerových systémů vždy jasně nastavit režimová pravidla a naplánovat jak pravidelné funkční zkoušky, tak aktualizace jejich firmwaru," říká Jan Huml, CTO společnosti Securitas. Význam aktuálnosti softwaru kamerových systémů zdůrazňuje také Richard Malíř, sales engineer společnosti Axis Communications v Česku: „Kyberútoků na kamerové systémy přibývá a projevilo se to



Taková obrazovka vítala uživatele počítače s operačním systémem Microsoft Windows, který byl napaden ransomwarem WannaCry. Výsledkem byla zašifrovaná data na pevném disku. Za dešifrování útočníci žádali platbu v bitcoinech.

65 %

Organizace, které zaplatily výkupné, získaly zpět v průměru jen 65 procent zašifrovaných souborů. Skoro třetina (29 procent) respondentů uvedla, že se jim podařilo obnovit 50 procent nebo méně souborů. Pouze 8 procent společností získalo zpět všechna svá data.

ve zvýšené míře i v období koronaviru. Podobně jako u jiných síťových zařízení, i v bezpečnostních kamerách se čas od času objeví zranitelnosti. Klíčové je, jak se chovají jejich výrobci – pokud okamžitě vydají aktualizaci firmwaru se záplatou a poskytují přesné instrukce svým partnerům a zákazníkům, lze předejít velkým škodám."

Nevěřte nikomu

Klasické řešení zabezpečení perimetru je v dnešní době mobilních zařízení a využívání vlastních zařízení zaměstnanci téměř nerealizovatelné. Proto se dnes stále častěji prosazuje princip nulové důvěry (zero trust), definovaný již v roce 2010, který představuje změnu zejména v tom, že žádné zařízení, které žádá o přístup do firemní sítě, není považované za důvěryhodné a je při každém takovém pokusu kontrolováno. „Princip zero trust přináší větší jistotu v oblasti bezpečnosti díky neustále probíhajícím kontrolám a omezení potenciálního útoku s využitím rádoby důvěryhodného externího zařízení. Firmy se také dokážou rychleji adaptovat na probíhající změny, odstraňovat práva odcházejícím zaměstnancům a měnit práva těm, jejichž role se změnily," popisuje Miroslav Kořen, generální ředitel společnosti Kaspersky pro východní Evropu. Zero trust přístup je také odpovědí na otázku, jak z bezpečnostního hlediska správně řešit mobilitu uživatelů. Nezáleží na tom, kde se uživatel nachází, protože při přístupu k informacím je vždy ověřován, například v kontextu místa připojení a hodnoty dokumentu.

Ověřování uživatelů ale samo o sobě představuje zásadní bezpečnostní problém, protože je relativně snadné přesvědčit i zkušené uživatele, aby vyzradili útočníkovi své heslo. I proto je trendem v oblasti dvoufaktorového ověřování „password-less" přístup. „Jde o ověřování na základě klíčů k povolení přihlašovacích údajů uživatele, které jsou vázané na zařízení, se kterým se uživatel přihlašuje a na kterém používá PIN kód nebo biometrickou ochranu. Systém analyzuje kontext přihlášení uživatele – tedy zda se přihlašuje v práci, doma, nebo v zahraničí – a riziko dané operace – zda jde o přístup k běžným dokumentům, nebo například ke správě serveru. Podle toho buď umožní vstup bez zadání hesla, nebo si vyžádá specifickou autentizaci," vysvětluje Petr Zubrický z S&T CZ. Typickým příkladem takové autentizace je zobrazení třech čísel v aplikaci mobilního telefonu, ze kterých uživatel vybere to, které je zobrazeno na monitoru zařízení, se kterým se přihlašuje. Nejen že jde z pohledu uživatele o pohodlnější přístup, protože ve většině případů nezadává žádné heslo, ale tento způsob přihlašování je i mnohem bezpečnější.

> "Moderní hrozby dokážou zcela autonomně ovládnout infrastrukturu v řádu desítek minut, přičemž útočník má za úkol pouze posoudit hodnotu cíle.

Investice do zabezpečení rostou

Podle loňského průzkumu společnosti Kaspersky, která oslovila přes 5000 IT manažerů, vzrostl podíl investic do IT bezpečnosti meziročně zhruba o 12 procent. To znamenalo i nárůst podílu investic do IT bezpečnosti na 26 procent z celkového IT rozpočtu – i přes to, že objem celkových investic velkých společností do IT zaznamenal mírný pokles. „U soukromých společností vidíme tlak managementu na analýzu IT obecně. Tedy zjistit, v jakém stavu síť je, do čeho je třeba investovat a kolik by stálo povýšení zabezpečení o nové technologie nebo kyberbezpečnostní služby. Z tohoto pohledu je také vidět trend ve zvažování případné migrace části infrastruktury do cloudu," uvádí Václav Zubr ze společnosti ESET.

Obecně lze sledovat, že si české firmy začínají uvědomovat, že kybernetická bezpečnost musí být základní součástí jejich prostředí – především kvůli ochraně dat jako jejich nejcennějšího majetku. „Schopnost získávat, ukládat a analyzovat data o zákaznících, jejich chování nebo potřebách je dnes zásadní konkurenční výhodou. Bezpečné prostředí je pak základem pro rozvoj obchodních aktivit a předpoklad k tomu, konkurenční výhodu si udržet. A právě proto firmy navyšují rozpočty a prostředky vynaložené nejen na ochranu před útoky, ale primárně do udržení své konkurenční výhody," dodává Petr Zubrický, bezpečnostní expert ve společnosti S&T CZ.

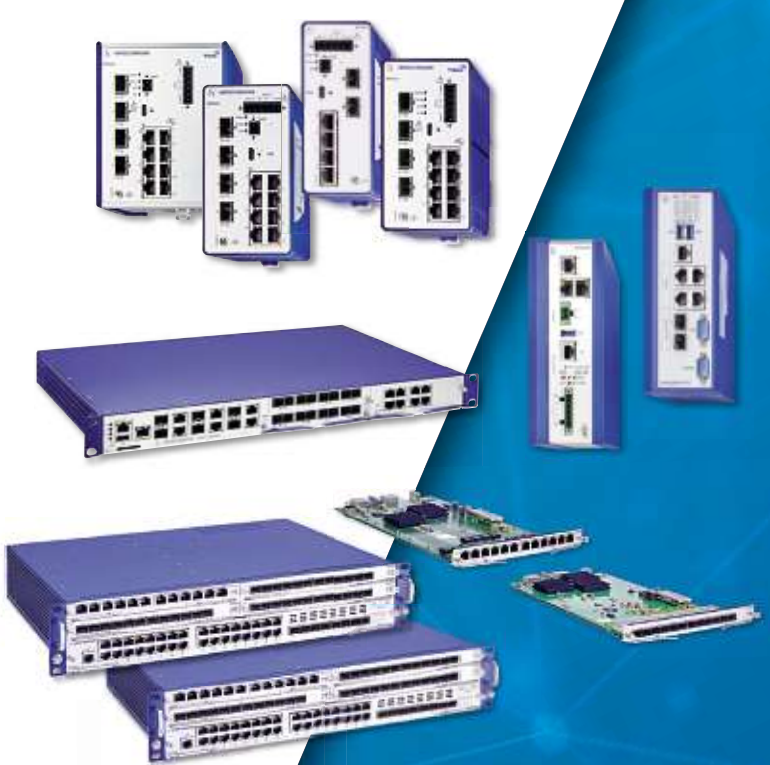
www.colaut.cz | obchod@colaut.cz

Průmysl je v současné době zcela závislý na komunikačních technologiích. Pro spolehlivý chod je zapotřebí bezpečné a robustní prostředí. Společnost COLSYS – AUTOMATIK pro průmyslové podniky zajišťuje kompletní rozsah této oblasti, a to od zmapování aktuálního stavu včetně analýzy rizik, návrhu projekčního řešení až po kompletní konfigurační parametry a dodání celého systému včetně servisu. „Staré technologie nezvládají současné bezpečnostní požadavky, jako je například periodická změna hesla nebo šifrování komunikace. Proto je potřeba najít jiný způsob ochrany," vysvětluje Jiří Kasner ze společnosti COLSYS – AUTOMATIK, která se průmyslové komunikaci věnuje už dvacet let.

PROVOZ PRŮMYSLOVÝCH PODNIKŮ JE ZÁVISLÝ NA BEZPEČNÝCH KOMUNIKAČNÍCH SYSTÉMECH

Podcenění rizik stojí peníze

Spousta firem podceňuje zabezpečení průmyslové komunikace včetně kritické infrastruktury. Často si možná rizika ani neuvědomují. Výpadky a narušení pak ale značně komplikují provoz a stojí nemalé peníze. Je zásadní finanční rozdíl v tom, jestli vám nefunguje hodinu poštovní klient nebo turbína. Nechte zkušené odborníky nahlédnout do vašich průmyslových komunikačních systémů. Analýza rizik a návrhy řešení, které bude kombinovat robustnost ve smyslu záložních systémů a bezpečnost, povedou ke spolehlivému zajištění provozu. Kdo je připraven, není překvapen. Zde to platí dvojnásob.



Podívejte se na náš YouTube kanál COLSYS – AUTOMATIK, a.s.

HIRSCHMANN
A BELDEN BRAND

HiSecOS
Hirschmann™ Security Operating System

COLSYS
AUTOMATIK

PRO FIRMY

EK013491

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

www.eset.cz/firmy