MAGAZÍN ICT REVUE

11
20

ROZVOJ CHYTRÝCH MĚST UMOŽŇUJÍ A SOUČASNĚ POHÁNÍ DIGITÁLNÍ TECHNOLOGIE

KYBERNETICKÁ BEZPEČNOST
FIREMNÍ TISK

KOMERČNÍ PŘÍLOHA HOSPODÁŘSKÝCH NOVIN A TÝDENÍKU EKONOM

interiAIR

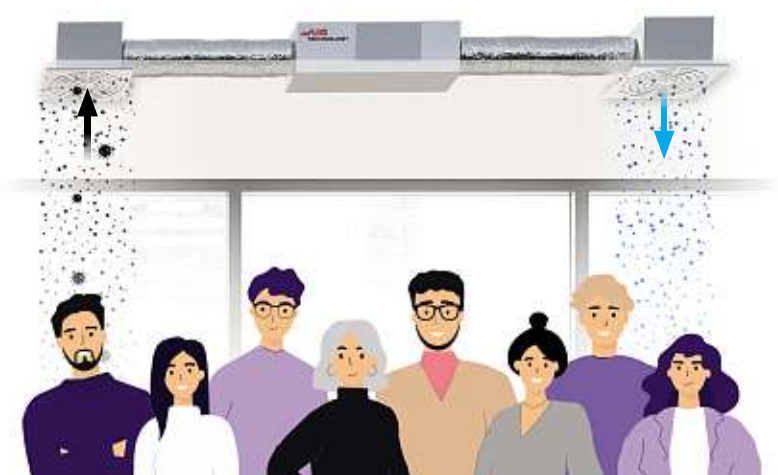
Zůstaňte na **zdravém vzduchu**

A DOST!
BÝT VĚČNĚ DOMA NÁS UŽ DUSÍ.

Chceme chodit mezi své kolegy a znovu vídat své zákazníky.
Existuje přece lepší řešení než vylidněné pracoviště.
Řešení chytřejší, pohodlnější a dlouhodobě efektivní:
Zajistit pracoviště filtrační jednotkou, která důsledně
zachytává mikročástice pronikající do plic vč. těch, které jsou < 0,3 µm.

Pojďme nákazám jednou pro vždy předcházet – ne je co čtvrt roku obcházet!

interiair.cz | airtechnology.cz



AIR TECHNOLOGY

Jednotka INTERIAIR od společnosti AirTechnology zajistí zdravotně nezávadné ovzduší bez jemného prachu, virů a mikroorganismů. Pod ochranou inteligentního i-HEPA filtru třídy H13 s účinností minimálně 99,95 %, pod dohledem senzoru monitorujícího obsazenost prostoru.

EK012976

Magazín vydavatelství Economia • samostatně neprodejný • **Datum vydání** • 4. 11. 2020
Redakce komerčních příloh • Pernerova 673/47, 186 00 Praha 8 • komercni.prilohy@economia.cz
Ředitel speciálních projektů • Aleš Mohout • **Vedoucí speciálního obsahu** • Jan Záluský
Vedoucí vydání • Martin Knížek, martin.knizek@economia.cz • **Layout** • Jolana Petrlíková
Manažeři inzerce • Jan Sapožnikov, tel.: 777 239 336 • Marie Bočková, tel.: 724 763 328
Foto na titulní straně • Shutterstock

MARTIN KNÍŽEK
vedoucí vydání

JEN TECHNOLOGIE Z MĚST CHYTRÁ NEUDĚLAJÍ

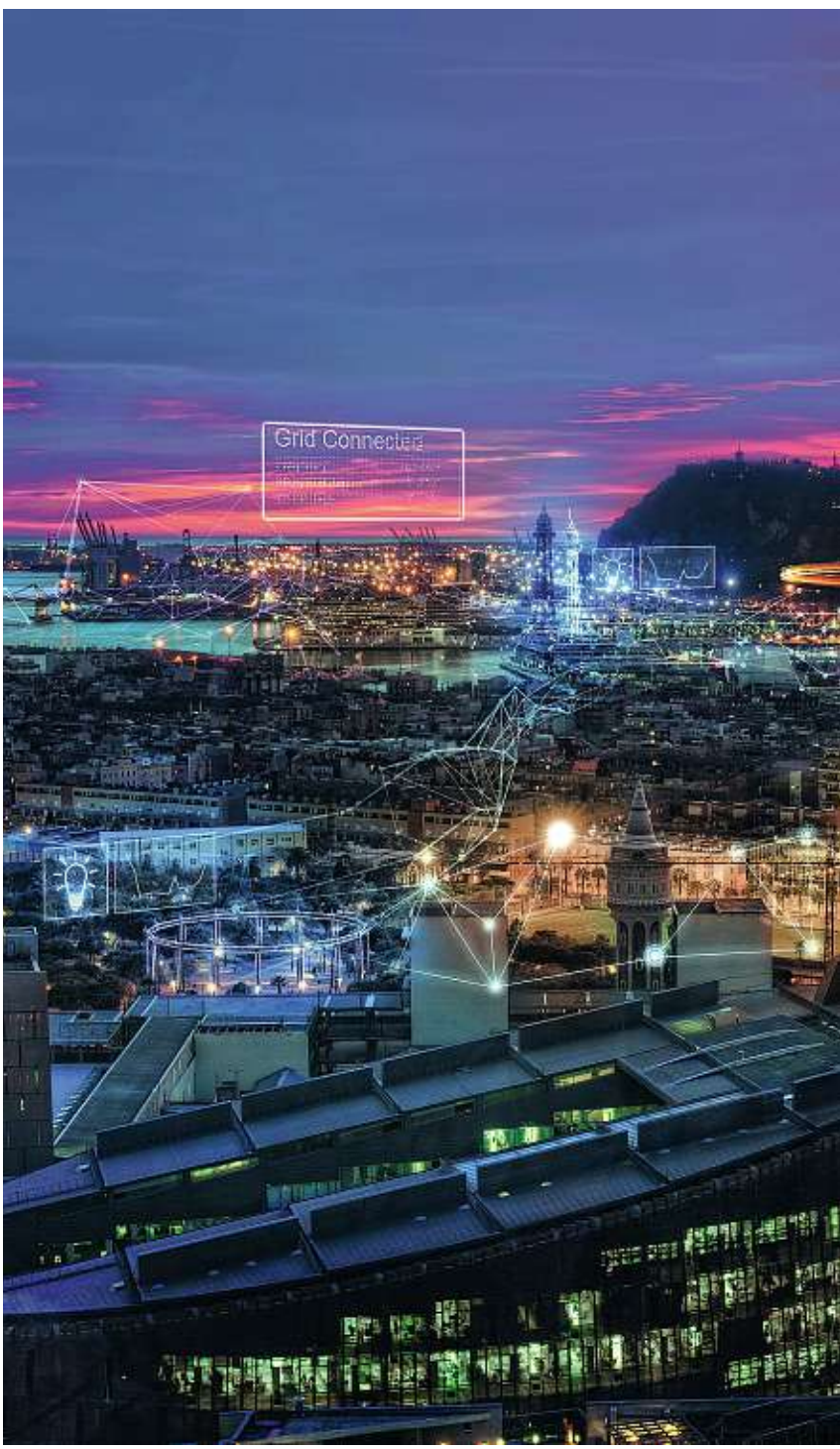
Koncept smart city rozvíjejí již řadu let i česká města a obce a od poněkud sporných projektů typu chytrých laviček s USB nabíjením či wi-fi se pomalu posouvají k takovým, které jejich obyvatelům skutečně usnadňují život. Jde například o řešení související s digitalizací veřejné správy, díky kterým mohou občané mnoho úředních úkonů zvládnout on-line, projekty usnadňující parkování, veřejnou dopravu, placení za městské služby nebo ty, které šetří životní prostředí a přinášejí úsporu energie či jiných zdrojů.

Takové úspěšné projekty postupně otevírají cestu k prohlubování spolupráce firem a městských samospráv a rozvoji nových služeb na budované digitální infrastruktuře. Chytré město vznikne tehdy, pokud se v této fázi jednotlivé projekty propojí do smysluplných celků, jež sledují celkovou strategii a koncepci chytrého města a přispívají k naplňování jednotlivých jeho atributů, jako je například bezpečnost, udržitelnost, zdraví či atraktivita pro obyvatele.

V této fázi se většina českých měst usilujících o smartifikaci zatím nenachází. Sledovat dlouhodobou koncepci v podmínkách relativně krátkých funkčních období veřejné správy vyžaduje dosažení základní shody na strategii napříč politickým spektrem. A té se často nedaří dosáhnout ani na úrovni městských samospráv. Cestu k chytrým městům tedy sice dláždí moderní technologie, ale vzniknout mohou jen tam, kde existuje vůle se dohodnout.

Technologie nabízejí chytrým městům nové příležitosti

Text | **Lukáš Kříž**
Foto | **Siemens, Operátor ICT**



Rozvoj chytrých měst, který umožňují a současně pohání digitální technologie, bývá považován za jeden z vrcholných úspěchů veřejné správy v 21. století. Životy obyvatel se postupně v mnoha ohledech stávají jednodušími, více naplňujícími a bezpečnějšími.

Změnu do každodenního života měst přinášejí nové služby, jež by nemohly vzniknout bez asistence dříve nedostupných digitálních technologií. I přes řadu dílčích úspěchů transformační úsilí se značkou smart cities teprve začalo. Nikdo však nepochybuje o tom, že bude pokračovat. Neustále roste počet obyvatel měst, zvyšují se nároky na jejich zásobování, k citlivým tématům patří environmentální udržitelnost, novým výzvám čelí instituce samospráv a jimi poskytované služby.

Koncept chytrých měst pro zdárnou implementaci vyžaduje mnohem více než jen samotné technologie a s nimi spojené inovace. Oboroví konzultanti i analytici se shodují na tom, že kritickou disciplínu a podmínku jeho dalšího rozvoje představují vztahy mezi hlavními aktéry. Jsou jimi na jedné straně veřejné autority a na druhé soukromoprávní subjekty. První strana definuje cíle, určuje cestu k jejich dosažení a zadává tvorbu relevantních řešení. Druhá tato za-

2,5 bilionu

dolarů představuje finanční objem, jehož by podle analytiků společnosti Grand View Research do pěti let mohl dosáhnout globální trh řešení a služeb pro chytrá města. Otázkou zůstává, jak tento výhled ovlivní probíhající pandemie a její důsledky.

dání konzultuje a následně realizuje. Společného jmenovatele představují obyvatelé měst, v jejichž zájmu by se celé úsilí mělo odehrávat.

„Vždy jsou zde tři entity, samospráva, občané a firmy, mezi kterými musí fungovat rovnováha. Lidé chtějí dobře žít. Pokud se jim žije dobře, budou spokojeni s vedením města, proto se město snaží vytvářet podmínky jak pro žití, tak pro podnikání, aby firmy zase mohly nabízet své služby a podporovat místní ekonomiku. Technologie pro chytrá města pak podporují vznik takovéto rovnováhy," říká Pavel Křižanovský, technický ředitel tuzemského zastoupení společnosti Cisco.

Na význam netechnologických aspektů chytrých měst upozorňuje také Jan Alexa, manažer výzkumu ve společnosti IDC: „Můžete mít tu nejlepší smart city aplikaci v zemi, ale když o ni obyvatelé města nevědí nebo jí nevěří, je k ničemu. Chytrá města jsou spojována především s technologiemi, ale úspěch nebo neúspěch vždy stojí na lidech."

TŘÍVRSTVÉ KONTINUUM

Vztahy mezi dvěma hlavními zúčastněnými stranami, tedy městskými institucemi a dodavateli, se podle konzultantů společnosti PwC vyvíjejí v rámci třívrstvého modelu či kontinua. Své pozorování pokládají za globální trend, jenž v různých zemích, městech i kategoriích služeb probíhá odlišným tempem. Všechny tři vrstvy navíc mohou koexistovat, přičemž každou doprovázejí jiné charakteristiky a důsledky.

V rámci první vrstvy vztahového kontinua vznikají dílčí projekty, jež pokrývají konkrétně vymezené potřeby města. Jde například o zavedení systému pro správu parkování, o implementaci úsporného a autonomního osvětlení LED nebo o vznik mobilních aplikací s relativně jednoduchým účelem, jakým je například ohlašování výmolů ve vozovce. Veškeré vztahy upravují smluvní ujednání, která pokrývají jeden konkrétní projekt, jednu specifickou potřebu.

„Aby se město nebo obec staly chytrými, nestačí jen nainstalovat inteligentní osvětlení nebo lavičku. Nemělo by jít o nasazování jednotlivých konkrétních řešení, ale o komplexní přístup, který řeší řadu potřeb města. Společným jmenovatelem chytrého ▸

KTERÉ TECHNOLOGIE CHYTRÝCH MĚST JSOU POUŽITELNÉ A DOSAŽITELNÉ I PRO MENŠÍ OBCE?

JAN ALEXA, MANAŽER VÝZKUMU, IDC

I menší města mohou v principu dosáhnout skoro na všechna řešení. Mohou spojit síly se sousedy a společně pořídit a implementovat dražší technologie. Menší města by se měla zaměřit především na technologicky standardizovaná řešení, která nevyžadují velké přizpůsobení. Jakákoliv řešení na míru stojí vždy více peněz a v případě menších měst nebudou pravděpodobně tolik nákladově efektivní.

VÁCLAV KOUDELE, ARCHITEKT STRATEGICKÝCH ŘEŠENÍ PRO VEŘEJNÝ SEKTOR, MICROSOFT

Zcela jistě jde o všechny senzory hlídající různé parametry, jako například kvalitu ovzduší a podobně. Dále pak o nástroje podporující turistický ruch v menších městech. Rovněž řešení chytrých budov jsou dobře využitelná i v menších obcích. Opomenout nesmíme ani oblast odpadového hospodářství a nasazení senzorů do kontejnerů, které přispěje k efektivnějšímu plánování svozu odpadu.

DAVID KOPPITZ, NÁMĚSTEK PRO ŘÍZENÍ SEKCE REGIONÁLNÍHO ROZVOJE, MMR ČR

Důležité je samozřejmě zabezpečit správné fungování samotného úřadu ještě předtím, než se začnou technologicky rozvíjet další oblasti. Nad rámec úřadu za nás dávají smysl technologická řešení, která přispívají například ke zvýšení kvality prostředí ve školách, pocitu bezpečí občanů či energetické bezpečnosti a soběstačnosti obce jako celku. V neposlední řadě si musíme uvědomit, že není možné vybavit všechny obce veškerou veřejnou infrastrukturou a veškerými veřejnými službami, proto je důležité vytvářet prostor pro sdílení služeb mezi obcemi, podporovat digitalizaci a mobilitu.

PETR KREJČÍŘ, ŘEDITEL ÚSEKU SMART INFRASTRUCTURE REGIONAL SOLUTIONS, SIEMENS

V první řadě by obec měla mít svou koncepci a na její realizaci dlouhodobě pracovat. V rámci „smartifikace" pak lze začít například s chytrým osvětlením nebo parkováním. Pokud je v dané lokalitě vhodná budova, instalace systému pokročilého hospodaření s energiemi umožní uživateli monitorovat využití energií a řídit jejich spotřebu s cílem snížit plýtvání.

PAVEL KŘIŽANOVSKÝ, TECHNICKÝ ŘEDITEL, CISCO

Za posledních pět let se dostupnost chytrých řešení rozšířila natolik, že v řadě případů je mohou využít i menší obce. Ty těžko dosáhnou na nějaká robustní řešení, na druhou stranu je ale ani nemusí potřebovat. Mnohdy si vystačí s různými senzory, datovou sítí, wi-fi a jednoduchou infrastrukturou a aplikací, v níž budou data zpracovávat, vyhodnocovat a dělat na základě nich rozhodnutí. Jako datovou platformu lze již často využívat cloudové služby, které jsou čím dál tím dostupnější a mají výhodu rychlého nasazení.

- města pak jsou atributy zdraví, doprava, bezpečí, úspora energií, dostupnost, udržitelnost a atraktivita. Platí přitom, že všechny tyto vlastnosti se v chytrém městě navzájem prolínají," dodává Petr Krejčíř, ředitel úseku Smart Infrastructure Regional Solutions ve společnosti Siemens.

Úspěšné dílčí implementace otevírají cestu soukromým subjektům k hlubší spolupráci. Na jejím počátku obvykle stojí návrhy a doporučení dodavatelů pro další inovace a služby. Faktor zúročení úspěchů z prvních projektů chytrého města přibližuje také Pavel Křižanovský ze společnosti Cisco: „Hlavními motivy vedení měst pro realizaci smart city projektů jsou úspory a zavádění nových služeb pro občany. Jakmile se jim ale podaří vybudovat smysluplný projekt a vidí, jaké má dopady – jednodušší řízení, přehled nad danou oblastí a podobně –, často se do dalších projektů pouští kvůli rozšíření těchto pozitivních efektů i na další městské agendy."

Druhá vrstva využívá digitální infrastrukturu vybudovanou v první etapě. Spolupráce mezi městem a dodavateli se rozšiřuje i mimo kritické či klíčové požadavky a služby. Obě strany z provozu podobných řešení profitují. Za příklad uveďme univerzální systém plateb za veřejné služby, které pokryjí i hromadnou dopravu. Prohloubení spolupráce s sebou ovšem nese jistá úskalí, která mohou vyústit ve stagnaci, monopolizaci nebo jednostrannou ekonomickou nevýhodnost. Služby poskytované na principech spolupráce veřejného a soukromého sektoru (PPP: Public-Private Partnership) podle konzultantů PwC vyžadují zvýšenou pozornost v oblasti smluvních dohod a ujednání.

Třetí vrstva vztahů se teprve začíná formovat. Charakterizuje ji budování digitálního ekosystému

chytrého města, na jehož základě vznikají zcela nové služby, produkty i subjekty, které mají potenciál generovat příjmy poskytovatelům a samosprávě. Třetí vrstva skrývá v podstatě neomezenou paletu příležitostí, které je třeba identifikovat, koordinovat a řídit.

„Smart znamená využívat digitální konektivitu mezi systémy a daty a v reálném čase reagovat na potřeby obyvatel. Kromě parciálních řešení jde o služby pro celou komunitu. Nezapomínejme také, že by chytré město mělo snižovat byrokracii, propojovat jednotlivé městské instituce a usnadnit tak obyvatelům jejich denní kontakt s městem a občanskou společností," shrnuje Petr Krejčíř ze společnosti Siemens.

TECHNOLOGICKÝ VÝHLED

Globální trh řešení a služeb pro chytrá města prochází bouřlivým vývojem. Letos podle analytiků společnosti Grand View Research dosáhne obratu jednoho bilionu dolarů, do pěti let by mohlo jít až o 2,5násobek. Otázkou samozřejmě je, jak tento výhled ovlivní probíhající pandemie onemocnění covid-19 a její důsledky. Ale i bez ohledu na ni rozvoj chytrých měst v praxi dle konzultantů společnosti

Smart

znamená využívat digitální konektivitu mezi systémy a daty a v reálném čase reagovat na potřeby obyvatel. Kromě parciálních řešení jde o služby pro celou komunitu.

PETR KREJČÍŘ,
ŘEDITEL ÚSEKU SMART INFRASTRUCTURE REGIONAL SOLUTIONS, SIEMENS

PwC determinuje šestice ekonomických a technologických faktorů. V souhrnu představují vzájemně podmíněné výzvy a příležitosti, kterým je třeba se věnovat, pokud možno komplexně.

Již zmíněný model PPP umožňuje samosprávám překlenout vysokou finanční nákladnost mnoha, řekněme celoplošných, technologických řešení. Jeho vedlejší efekty se ale projevují i v technologických faktorech. Soukromé subjekty mohou městům například poodhalit potenciál rozvíjejících se technologií. Mezi ně pat- ▸

↑ JEDNÍM Z DÍLČÍCH PROJEKTŮ Z OBLASTI SMART CITY, KTERÉ SE ZKOUŠELY V PRAZE, JSOU KOMPRESNÍ KOŠE BIGBELLY. JSOU NAPÁJENÉ SOLÁRNÍMI PANELY A POSKYTUJÍ ON-LINE INFORMACE O SVÉM NAPLNĚNÍ.

ří distribuovaná databáze blockchain, infrastruktura pro elektrická vozidla, internet věcí a další. Zapojit jej lze i do rozsáhlých projektů, k nimž patří zajištění internetové konektivity v rámci celé sídelní oblasti.

Dostupnou a dostatečně dimenzovanou konektivitu pokládá za klíčový předpoklad vzniku a rozvoje chytrých měst David Koppitz, náměstek pro řízení Sekce regionálního rozvoje na ministerstvu pro místní rozvoj: „Vysokorychlostní připojení k internetu je naprosto nezbytné nejen pro zavádění chytrých řešení, ale i pro samotné fungování ekonomiky, rozvoj malého a středního podnikání a kvalitní život obyvatel. Vysokorychlostní internet musí být přitom cenově dostupný, což zajistí pouze dostatečná konkurence."

S postupující vyspělostí a pokročilostí chytrých měst se do popředí zájmu dostávají témata ochrany dat a jejich využití. Zajištění kybernetické bezpečnosti představuje klíčový parametr důvěry mezi samosprávou, jejími dodavateli a obyvatelstvem. Data nesmí být také použita pro jiné než zcela transparentní a schválené účely. Tento bod se týká především různých analytických řešení a vytěžování obsahu, tedy disciplín, které skýtají nemalý potenciál pro další využití. „Základní datovou architekturu a platformu smart city by mělo mít rozmyšleno každé město již dnes. V budoucnu se tyto základní iniciativy mohou přerodit v digitální dvojče – holistický digitální model fungujícího města," dodává Jan Alexa ze společnosti IDC.

V nejbližší budoucnosti se iniciativy chytrých měst podle konzultantů společnosti PwC zaměří na témata inteligentních křižovatek, aplikace umělé inteligence do stávajících systémů, posílení konceptu chytrých přenosových sítí, zvýšení bezpečnostní úrovně a ochrany soukromí, rozvoj ekologických projektů a na rostoucí využití akumulovaných dat. Inovační vlna neopomene ani využití otevřených dat s cílem zvýšit zapojení komunit a rozvoj možností propojených vozidel. Stranou zájmu nezůstane rovněž podpora výstavby chytrých komerčních budov nebo aplikace všesměrové komunikace mezi všemi zapojenými stranami.

Reflexi projektových priorit tuzemských obcí přidává Václav Koudele, architekt strategických řešení pro veřejný sektor ve společnosti Microsoft: „Česká města dnes nejčastěji sahají po nástrojích pro řízení spotřeby energií či po systémech pomáhajících zlepšit fungování městské hromadné dopravy a dopravy obecně. Samostatnou oblastí je pak odpadové hospodářství, kdy je s pomocí senzorů možné efektivně plánovat svoz odpadu. Kontejnery se osadí čidlem, které dokáže detekovat, zda už je kontejner plný, a tudíž potřebuje vyvézt. Další oblastí je pak měření oxidu uhličitého ve školách či jiných budovách, které vás upozorní na to, kdy je třeba větrat. A v neposlední řadě bych zmínil i oblast chytré turistiky."

VÝZVY A PROBLÉMY BUDOVÁNÍ CHYTRÝCH MĚST

Městské technologické iniciativy stále patří mezi průkopnické počiny. Jejich strůjci se sice mohou inspirovat v inovačních projektech komerčních subjektů, ty však nelze kvůli rozdílnosti prostředí, podmínek a možných dopadů přeceňovat. Budovatelé chytrých měst čelí výzvám a problémům, které se v podnikovém sektoru nikdy neobjeví a nejspíše ani neprojeví. Jde zejména o sociální důsledky a politické konsekvence realizace různých projektů a o specifické ekonomické vztahy.

Výčet běžných překážek rozvoje chytrých měst v tuzemsku uvádí David Koppitz z ministerstva pro místní rozvoj: „Bariér, které se snažíme překonávat, je řada. Z hlediska technologického pokroku je jedním z problémů například neexistence norem pro řízení IT služeb ve městech. IT je nástroj pro vytvoření služby. Ten musí být kvalitní, efektivní, aktualizovatelný, škálovatelný, ekonomicky výhodný a schopný inovace. Obce také často kupují digitální řešení, která jsou ovšem vázána na software dodavatele, jenž může obci zvýšit cenu svých služeb. Při zavádění chytrých systémů a služeb jsou preferována taková řešení, která umožní změnu dodavatele bez velkých nákladů. Je nutné vlastnit data a mít jistotu, že při změně dodavatele nedojde k jejich ztrátě – buď tím, že předchozí dodavatel je odmítne předat, nebo je předá v takovém formátu, že je není možné využít."

Nekoncepční přístup považuje za významný problém tuzemského rozvoje chytrých měst Václav Koudele ze společnosti Microsoft: „Držet se jednotné strategie napříč volebními obdobími není jednoduché. Obvykle po volbách přichází nová politická garnitura, která má svou strategii. Je proto dobré, aby dlouhodobá strategie pro chytré město byla průběžně schvalována i s opozicí." ▪

KDYKOLIV, ODKUDKOLIV A HLAVNĚ BEZPEČNĚ

MARTIN KRŠŇÁK,
BUSINESS DEVELOPMENT DIRECTOR,
ASSECO SOLUTIONS

Bezpečný vzdálený přístup k ERP systému snad nikdy nebyl důležitější než letos. S nárůstem počtu lidí pracujících z domova vzrostl i počet kybernetických útoků. Ty například v dubnu ochromily řadu českých nemocnic, ale jejich cílem byly i nejrůznější firmy a jejich ERP systémy. Naši bezpečnostní experti zaznamenali útoky zejména na RDP (Remote Desktop Protocol), který se používá pro přístup ke vzdálené ploše. Rekordmanem byla firma s 35 tisíci pokusů o útok na RDP za jediný den.

Přístup ke vzdálené ploše má přitom řadu výhod. Ta klíčová spočívá v tom, že se spotřebovává výpočetní výkon serveru či hostujícího počítače ve firmě, a nikoliv zařízení, z něhož se připojujete. To slouží jen jako jakýsi prohlížeč obrazových dat ze serveru a nástroj pro sběr dat z klávesnice a myši či dotykového displeje. Díky tomu, že vše se odehrává výlučně na serveru, můžete s libovolnou aplikací pracovat z libovolného zařízení s libovolným operačním systémem.

Většina elektronické pošty, firemní komunikace, firemních portálů, e-shopů a obecně náročných webových aplikací dnes funguje v cloudu. Ten je zejména u malých a středních firem považován za mnohem bezpečnější než vlastní firemní servery. V přísně zabezpečených datových centrech lze provozovat takřka libovolné aplikace. To platí i o některých podnikových informačních systémech – ERP, například o těch, které provozuje společnost Asseco Solutions na vlastní specializované cloudové platformě Erport.

V takových případech dodavatel zajišťuje dodatečné zabezpečení vzdáleného přístupu. Základem je šifrování veškeré komunikace, ale klienti si mohou omezit vzdálený přístup jen z konkrétního rozsahu IP adres, využít přístup výlučně prostřednictvím VPN nebo nasadit multifaktorovou autentifikaci uživatelů, která v podstatě znemožní neautorizovaný přístup do systému. Přes to vše by firmy měly dbát i na maximální zabezpečení koncových zařízení. ▪

ON-LINE IDENTIFIKACE KLÍČEM DO NOVÉHO SVĚTA FINANCÍ

PAVEL HORÁK,
MANAŽER OBCHODNÍ JEDNOTKY IDGUARD,
UNICORN SYSTEMS

Žijeme v éře dynamicky se rozvíjející e-commerce, která nám umožňuje pořizovat si širokou paletu zboží a služeb z pohodlí domova. Už to není jen elektronika, oděvy nebo potraviny, ale ve stále větší míře i finanční služby. Technologie pronikají do světa peněz a nejrůznější start-upy a inovátoři nutí měnit přístup i značně konzervativní instituce, jakými jsou banky či pojišťovny.

Společný jmenovatel je jasný: služby zvyšující komfort, poskytované na dálku – on-line. Ať už jde o platby, peněžní účty, půjčky, spoření či pojištění, člověk má stále širší možnosti – jen vzít do ruky mobil nebo sednout k počítači. Ve světě financí ovšem více než kde jinde vyvstává potřeba zákazníka identifikovat a jeho totožnost ověřit. Nejen proto, že jde zpravidla o dlouhodobější obchodní vztah a významnější finanční hodnoty, ale i proto, že poskytovatelé finančních služeb z velké většiny podléhají paragrafům proti praní špinavých peněz.

Současné technologie s využitím biometrie kontrolu totožnosti on-line umožňují. Je dobré zvolit řešení, které nabízí jednoduché, ale zároveň bezpečné a důvěryhodné ověření. Získaná data z identifikace lze pak bezprostředně porovnávat s databázemi odcizených dokladů, insolvenčními rejstříky a dalšími externími zdroji. Požadavek na fyzické ověření lze vyřešit využitím takzvané převzaté identity – v české praxi k tomu účelu může posloužit chystané BankID.

Vedle alternativ, které jsou náročné na instalaci a provozní náklady, jsou dnes na trhu i řešení poskytovaná formou on-line služby. Jejich zavedení je rychlé, protože k připojení stačí jedna URL adresa, zatímco na druhé je vzápětí k dispozici výsledek se získanými daty, včetně potvrzení identity zákazníka. Takovou službu mohou využít společnosti všech druhů a velikostí. Zatímco provoz je nenáročný, přínosy jsou značné. ▪

Nejúspěšnější jsou stále plošné útoky malwaru

Text | Radek Kubeš
Foto | HN – Lukáš Bíba

Největší ohrožení firemní IT infrastruktury dnes představuje zero-day malware, na který v danou chvíli není vydána bezpečnostní aktualizace softwaru. Dalším zdrojem problémů je masový přechod zaměstnanců na práci z domova. S ochranou před aktuálními hrozbami pomůže využití strojového učení, umělé inteligence a dalších pokročilých technologií v bezpečnostních řešeních, říká v rozhovoru Martin Frühauf, bezpečnostní expert společnosti S&T CZ.

Trendem v oblasti kybernetické bezpečnosti jsou dnes řízené služby. Můžete tento typ služeb blíže popsat?
Poskytovatelé řízených bezpečnostních služeb (MSSP, Managed Security Services Providers), respektive poskytovatelé řízených služeb (MSP, Managed Services Providers), kteří se specializují na oblast IT bezpečnosti, pomáhají z pozice externích členů IT týmů organizacím zajišťovat kontinuitu podnikání a řešit případná technologická rizika. Jejich služby využívají zpravidla firmy, které nemají interní zdroje na to, aby si tuto oblast kvalitně pokryly.

Hlavní předností tohoto modelu je, že firma získává profesionální službu nebo řešení, aniž by musela investovat do vlastních technologií či expertů, nehledě na to, že na trhu dnes takto vysoce erudovaní bezpečnostní experti de facto nejsou k mání. Řízené služby jsou v současnosti tím nejefektivnějším způsobem, jak IT bezpečnost zajistit, a to zejména pro organizace, které nedisponují potřebnými rozpočty nebo oblasti bezpečnosti dostatečně nerozumí. Jediný pracovník IT bezpečnosti, kterého má průměrná organizace často k dispozici, není schopen pojmout všechny klíčové oblasti, natož je zodpovědně zabezpečit.

V čem se řízené služby v bezpečnosti liší od konceptu bezpečnost jako služba (Security as a Service)?
Řízené služby jsou komplexnější a jejich poskytovatel zákazníka „vede za ruku". Také se v nich spojuje více oblastí dohromady – od osvědčených postupů přes zákon o kybernetické bezpečnosti, certifikace ISO, interní pravidla až po technická opatření. Celkově jde o dlouhodobější spolupráci a znalost zákazníka. U SaaS už se jedná o poskytování konkrétní služby nebo služeb, které přímo cílí na určité problémy, jako je například bezpečnostní dohled, správa zranitelností a podobně.

Myslím si,

že v několika následujících letech bude využití umělé inteligence a strojového učení v kyberbezpečnosti běžnou praxí.

S jakými kybernetickými hrozbami se v současné době české firmy nejvíce potýkají?

Nejzávažnějším typem kybernetické hrozby se zásadním dopadem na fungování organizace je zero-day malware. Tedy škodlivý software, který ještě není detailně popsán, přesněji řečeno na něj zatím neexistuje účinná obrana typu aktualizace softwaru nebo konkrétní aktualizace bezpečnostního softwaru. Společnost pak musí spoléhat na svoji úroveň IT bezpečnosti jako celku, vhodně doplněnou o moderní bezpečnostní nástroje, které zásadně pomáhají při detekci zero-day hrozeb.

Největší zásah si stále připisují plošné útoky malwaru, které jsou vzhledem k neuspokojivé úrovni IT bezpečnosti v Česku úspěšné. Důvodem je zejména nedostatečná ochrana organizací, jejichž zastaralé IT bezpečnostní řešení mnohdy není schopno detekovat hrozby a reagovat na ně včas. Příkladem jsou subjekty v oblasti zdravotnictví nebo průmyslové výroby, které nejsou technicky ani procesně připravené a bojují s nedostatkem IT personálu či bezpečnostních expertů a které zpravidla zjistí útok až v momentě, kdy jim přestanou fungovat systémy. V českém prostředí vidíme i případy cílených útoků, ale je jich málo.

Došlo v tomto směru k nějaké změně vlivem koronavirové pandemie?

Vliv pandemie lze pozorovat ve dvou rovinách. Jednou je zvýšený zájem lidí o téma covidu-19, a proto útočníci toto téma využívají ve svých kampaních, které se tváří, že přinášejí nové informace o pandemii a případných opatřeních. Jde o malware, který má poměrně vysokou úspěšnost, podobně jako v minulosti například e-maily s podvrženými fakturami. Nicméně tato situace není nijak nová, útočníci budou vždy využívat témata, o která se společnost zajímá.

Druhou oblastí jsou pak rizika spojená s masovým přechodem zaměstnanců na práci z domova. Z pohledu IT bezpečnosti to pro mnohé organizace znamená nový úhel pohledu na možná rizika – lidé pracují mimo prostředí firmy, připojují se z vlastních zařízení a domácích sítí, které často nedisponují potřebnými bezpečnostními prvky a nad kterými nemá správce podnikového IT žádnou kontrolu. Je nutné se tedy nově vypořádat s fungováním a koloběhem firemních dokumentů a know-how v prostředí s výrazně větším rizikem ztráty či odcizení. ▸

MARTIN FRÜHAUF

VE SPOLEČNOSTI S&T CZ VEDE DIVIZI SECURITY, JEJÍŽ SOUČÁSTÍ JE I SECURITY OPERATIONS CENTRUM. JAKO EXPERT NA OBLAST KYBERBEZPEČNOSTI DISPONUJE ŘADOU BEZPEČNOSTNÍCH CERTIFIKACÍ A JEHO SPECIALIZACÍ JSOU NÁVRHY, IMPLEMENTACE A SPRÁVA SYSTÉMŮ PRO SBĚR A VYHODNOCOVÁNÍ AKTIVIT V PODNIKOVÝCH IT PROSTŘEDÍCH, ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ, ANALÝZY PODNIKOVÝCH INFORMAČNÍCH SYSTÉMŮ A SYSTÉMY PRO DETEKCI A PREVENCI PRŮNIKU. V MINULOSTI SE PODÍLEL NA REALIZACÍCH ŘEŠENÍ BEZPEČNOSTNÍHO DOHLEDU PRO VÝZNAMNÉ A KRITICKÉ INFORMAČNÍ SYSTÉMY A NAPLNĚNÍ POŽADAVKŮ ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI U ORGANIZACÍ JAKO NAKIT, ČNB, ČESKÁ SPOŘITELNA, ČESKÁ EXPORTNÍ BANKA A ŘADY ČESKÝCH MINISTERSTEV.

Jak mohou podniky současný masivní přechod na práci z domova ošetřit?

Pro organizace, které dosud neměly žádné zkušenosti s prací zaměstnanců mimo prostředí firmy a které si často ani nejsou vědomy rizik s tím spojených, může přechod na současný režim znamenat velké ohrožení. Primárním cílem je zajistit kontinuitu provozu, ideálně by měla mít každá organizace plán pro zachování kontinuity činnosti dříve, než taková situace nastane. Součástí plánu je samozřejmě i záruka bezpečnosti provozu, do které spadá především minimálně dvoufaktorová autentizace přístupů zejména do cloudových služeb a vzdáleného přístupu k interním systémům, zajištění pravidelných aktualizací softwarových nástrojů a centrální instalace ověřených on-line nástrojů pro spolupráci a schůzky zaměstnanců.

Dostala se v českých firmách bezpečnost do popředí zájmu, nebo jde o zanedbávanou či podfinancovanou oblast?

Přístup k IT bezpečnosti se často liší podle oblasti podnikání. Ve finančním nebo energetickém sektoru je úroveň bezpečnosti velmi vysoká, ale například ve zdravotnictví jsou značné rezervy. Příčin může být hned několik: na dodržování povinností vyplývajících ze zákona o kybernetické bezpečnosti nemají zdravotnická zařízení dostatečné zdroje a historicky se spíš než do IT a zabezpečení investuje do zdravotnického vybavení. Obecně soukromý sektor má schopnost rychle reagovat na případné bezpečnostní hrozby, naopak u státních institucí je úroveň zabezpečení tradičně nižší, zde je to otázka nejen rozpočtů, ale i kompetencí a schopnosti reagovat na změny.

I v soukromém sektoru jsou ale oblasti, kde se bezpečnosti nevěnuje příliš velká pozornost. Jde například o průmyslovou výrobu, kde případný bezpečnostní incident zpravidla způsobí velké škody, ale kde jsou také schopni problémy vyřešit v řádu dní a ztráty dále neprohlubovat. Naopak ve zdravotnictví je situace odlišná, jak ukazují i poslední útoky na nemocnice, kde téměř ve všech případech musí s ohledem na rozsah útoku s řešením pomoci i kraje či NÚKIB. Kdyby se stala obdobná událost v soukromé společnosti, s největší pravděpodobností by zkrachovala. Nemocnice mají, a nyní v souvislosti s pandemií o to víc, mnoho problematických oblastí, které vyžadují jejich pozornost, IT bezpečnost je pouze jednou z nich.

Čím se zabývá vaše centrum kybernetické bezpečnosti?

Bezpečnostní kompetenční centrum S&T CZ (SOC, Security Operation Centre) provozujeme od června 2018 a možností jeho pronájmu jako služby nabízíme firmám flexibilitu a nákladovou efektivitu při zajišťování kybernetické bezpečnosti. „Pronájmem" mám na mysli škálu odborných činností, které si u nás mohou zákazníci objednat jako službu na míru. Mezi ně patří zejména průběžný nepřetržitý monitoring a analýza kybernetické bezpečnosti v dané organizaci a analýza aktivit v sítích, na koncových bodech, serverech, v aplikacích, databázích a dalších systémech organizace, díky které zajišťujeme včasnou detekci a reakci na případné bezpečnostní události. Odhalujeme, analyzujeme a reagujeme včas na bezpečnostní incidenty, což nám umožňuje kombinace špičkových technologických řešení, prověřeného souboru procesů a vysoké úrovně certifikovaných bezpečnostních expertů. Podle zvolené úrovně služby přebíráme zodpovědnost za bezpečnost organizace v příslušné míře.

Můžete uvést příklady odvrácení závažných kybernetických útoků?

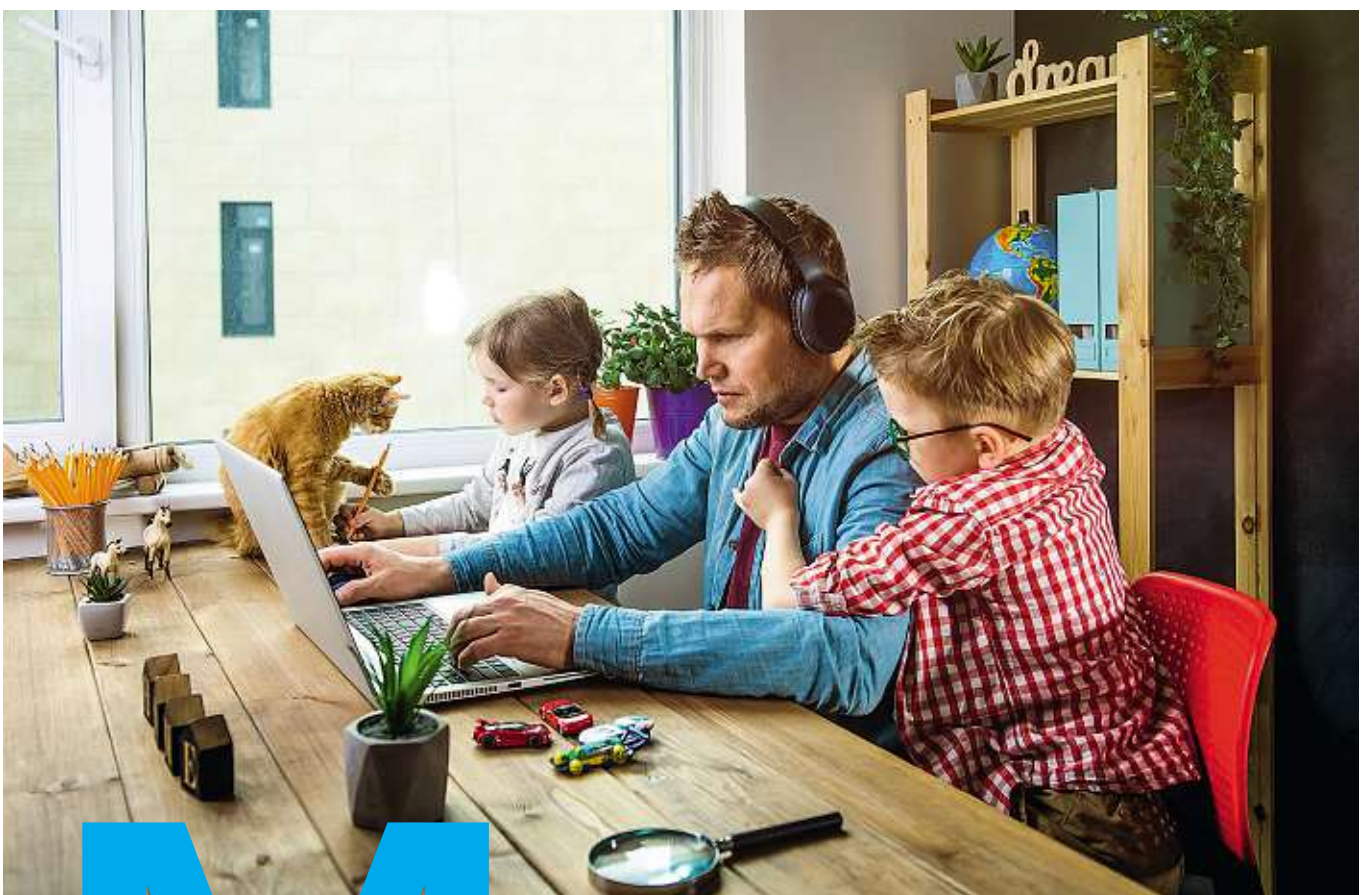
Nemohu uvádět konkrétní příklady, ale obecně mohu potvrdit, že se nám daří detekovat velké množství pokusů například o zneužití privilegovaných přístupů ze strany interních zaměstnanců u našich zákazníků. Pokročilé technologie a procesy nám umožňují detekovat i většinu průniků zvenku. Naši bezpečnostní experti jsou schopni na základě behaviorální analýzy odhalit anomálie v prostředí zákazníka a následně určit rozsah útoku a všechny systémy, které jsou nebo by mohly být zasaženy. A to v reálném čase, takže vytvoří prostor pro adekvátní reakci.

Jaký je váš výhled kyberbezpečnostní situace a jaké technologie budou v boji proti kyberútočníkům hrát rozhodující roli?

Bude pokračovat nárůst zero-day hrozeb, což podpoří další rozvoj pokročilých inteligentních technologií jako strojového učení a umělé inteligence a jejich implementaci do bezpečnostních řešení. Ta budou schopná se samostatně učit v prostředí zákazníka a upozorňovat na anomálie. Pozornost se pak bude věnovat co nejvyšší automatizaci procesů, přičemž cílem bude využívat lidských zdrojů už ke konkrétním klíčovým úkonům na základě již do určité míry zanalyzovaných dat právě pokročilými technologiemi. O využití umělé inteligence a strojového učení v oblasti kyberbezpečnosti hovoříme řadu let a už dnes vidíme jejich reálná nasazení. Domnívám se, že v několika následujících letech bude využití těchto technologií běžnou praxí.

Kyberútočníci zneužívají pandemii koronaviru a práci z domova

Text | Radek Kubeš
Foto | Shutterstock



Mnoho firem muselo narychlo řešit přesun svých pracovníků na home office, tedy mimo zabezpečený perimetr podnikové sítě, do domácího prostředí, kde jsou zařízení zaměstnanců podstatně méně chráněná.

Nejnovější studie společnosti Kaspersky, z července tohoto roku, provedená v Česku a dalších třiceti zemích po celém světě, ukázala, že mezi současná největší rizika v IT bezpečnosti patří phishingové útoky na firmy a jejich pobočky. V souvislosti s pandemií čínského koronaviru navíc musela řada organizací urychlit svoji digitální transformaci, čímž u nich stoupla závislost na IT systémech. Kyberzločinci po celém světě nezahálí a každým dnem vylepšují, inovují a vyvíjí nástroje a systémy tak, aby se vyhnuli detekci, a mohli tak útočit na internetové uživatele a těžit z globální pandemie.

Mění se také taktika útoků kyberzločinců, především těch, kteří využívají ransomware, tedy vyděrač- ▸

ský malware. V minulosti platilo, že útočníci použili ransomware k zašifrování dat, aby pak mohli napadenou firmu vydírat a dostat zaplaceno za poskytnutí klíče, kterým by bylo možné zašifrovaná data odemknout a znovu zpřístupnit. To se nyní změnilo, jak popisuje Maroš Barabas, head of product management společnosti AEC: „Firmy se přizpůsobily, s touto hrozbou počítají a začaly více zálohovat. Zareagovali ale také útočníci a jejich nová taktika spočívá v tom, že dnes data skutečně kradou. Zejména klientská data, ale samozřejmě také smlouvy, interní ceníky, know-how, zkrátka všechno, co je nějak citlivé, či dokonce kompromitující."

Ukradená data se následně prodávají na černém trhu, kde si je pořizují další kyberzločinci, kteří vědí, jak je zneužít, například k vydírání anebo k dalším útokům. O svá data se může přihlásit i okradená firma a za bitcoiny si je odkoupit zpět. „Bizarní na tom je, že si útočníci pronajímají call centra s operátory, kteří vás provedou celým procesem včetně důkazu, že daty disponují, a po zaplacení je i někdy vrátí," dodává Maroš Barabas.

HOME OFFICE JAKO NOVÉ RIZIKO

Hromadný přechod kancelářských pracovníků do režimu práce z domu s sebou přináší i větší rizika. Pro firmy je mnohem náročnější ochránit zařízení svých zaměstnanců pracujících mimo firemní síť, a navíc do hry vstupují i další členové rodiny, typicky děti, které si na pracovním počítači rodičů pustí nějakou hru nebo sledují videa. A právě tito další lidé, kteří nebývají v informační bezpečnosti zběhlí, mohou zařízení velice snadno infikovat. Zaměstnavatel se přitom ani nemusí dozvědět, že je zařízení kompromitované, a útočníci se takové situaci velmi rychle přizpůsobili.

„Aktuálně vidíme velký problém v různých pokusech o prolomení RDP (Remote Desktop Protocol), což je technologie, kterou firmy využívají pro vzdálený přístup k firemním sítím. Ve druhém čtvrtletí tohoto roku jsme zaznamenali nárůst o 30 procent. Na vině je masivní přesun pracovníků do domácího prostředí. Například v červnu jsme detekovali po celém světě průměrně 104 tisíc pokusů o prolomení unikátních zařízení denně, přičemž v Česku šlo o stovky takových útoků denně. Jakmile se útočníci do sítě dostanou, velmi často využijí ransomware k zašifrování dat," vysvětluje Václav Zubr, bezpečnostní expert společnosti Eset.

Veškerá slabá místa náchylná ke kyberútokům proto musí být pokryta. Pokud se zaměstnanci připojují ke korporátním zdrojům na dálku, je nezbytné, aby k tomu používali pouze spolehlivou VPN, která zajistí bezpečné spojení s firemní infrastrukturou. Tím ochrání korporátní data před vnějšími vlivy. Zaměstnanci by také měli používat výhradně pracovní e-mail, což například usnadní zjištění pokusů o vydávání se za zaměstnance, pokud k tomu kyberzločinci použijí účet na jiné doméně. E-mailové servery musí být chráněny technologiemi, které jsou schopny detekovat pokusy o změnu odesílatele zprávy. Kromě zabezpečení před škodlivým softwarem by měly být pracovní notebooky a telefony vybaveny programem schopným na dálku vymazat veškeré korporátní informace. Dále by měl zaměstnavatel zajistit oddělené ukládání osobních a korporátních dat, zavést omezení na instalace aplikací a zároveň automaticky aktualizovat software a operační systém. Mezi další IT firemní pravidla by mělo patřit používání silných hesel, vícefaktorové autentikace a automatického zamykání obrazovky.

DĚTI SI NĚKDY NA PRACOVNÍM POČÍTAČI RODIČŮ PUSTÍ NĚJAKOU HRU NEBO SLEDUJÍ VIDEA. A PROTOŽE NEBÝVAJÍ V INFORMAČNÍ BEZPEČNOSTI ZBĚHLÉ, MOHOU ZAŘÍZENÍ VELICE SNADNO INFIKOVAT.

„Nejdůležitější však je, aby firmy své zaměstnance předem poučily o základních pravidlech práce na dálku, on-line bezpečnosti a ujistily se, že jsou zaměstnanci srozuměni s jejich zodpovědností za udržování korporátních dat v bezpečí," dodává Miroslav Kořen, generální ředitel společnosti Kaspersky pro východní Evropu. Důležitější než kdy dříve je také nasazení kvalitního EDR systému (Endpoint Detection and Response), který zaznamenává a vyhodnocuje veškeré změny na koncových zařízeních s cílem detekovat podezřelé aktivity, které nemusí přímo souviset jen s malwarem.

INVESTICE DO ZABEZPEČENÍ JSOU NEZBYTNÉ

S počátkem koronavirové pandemie začalo v prostředí českých firem vznikat více pootevřených dveří pro útočníky. Jde zejména o zmíněné vytváření přístupů k prostředkům firmy pro zaměstnance pracující z domova. Kombinace nedostatku potřebného

30 %

Skoro o třetinu více útoků na vzdálený přístup k firemním sítím pomocí technologie Remote Desktop Protocol zaznamenala ve druhém čtvrtletí společnost Eset. Důvodem zájmu útočníků je masivní přesun pracovníků do domácího prostředí.

času, připravenosti, financí a znalostí byla pravděpodobně důvodem, proč se při nastavování přístupů často dostatečně nemyslí na bezpečnost. Této situace si všimli útočníci a začali toho ve velkém využívat. „Problém firem v Česku je, že ve srovnání s přístupem společností na západ od nás reagují až ex post. Ať už se to týká přímo hrozeb nebo třeba nových aktuálních způsobů ochrany, je adaptace nových přístupů, technologií a principů ze strany firem velmi opožděná. To zpoždění je u nás zhruba tři až pět let oproti západní Evropě, o Spojených státech nemluvě," konstatuje Maroš Barabas z AEC.

Přístup firem často souvisí s tím, zdali již mají zkušenost s vážnějším bezpečnostním incidentem. „Většinou jim chybí nástroje pro vyšetřování incidentů, jakými jsou EDR, XDR (Extended Detection and Response) a síťové BDS (Breach Detection System). Podezřelá aktivita zachycená na koncové stanici končí často jen reinstalací a nikdo příliš nezkoumá, jak se útočník do sítě dostal, kam všude získal přístup, jaké aktivity provedl nebo zda se v síti stále nachází," popisuje typický přístup firem Filip Marvan, Security Engineer společnosti Trend Micro, a dodává: „Velký problém je také v nedostatku kvalifikovaných lidí, kteří mají dostatečné znalosti pro vyšetřování pokročilých útoků. Přesto je většina firem přesvědčena, že bezpečnost zvládnou samy, a jen velmi málo využívají služeb vyškolených specialistů dodavatelů bezpečnostních řešení."

Investice do zabezpečení by měla vycházet z míry rizik, kterou je vedení společnosti ochotné podstoupit. Je třeba identifikovat a kvantifikovat aktiva a následně analyzovat hrozby, jež mohou mít na tato aktiva dopad. Výsledkem by mělo být stanovení odpovídající míry ochrany aktiv informovaným vedením společnosti. Ideálně s výhledem na další roky. Koncová částka nejde jednoduše určit a může být zásadně odlišná i u podobných společností z jednoho oboru. „Neexistuje jednoduché pravidlo, které by určovalo, kolik by měla firma investovat do bezpečnosti. Je třeba vzít v úvahu odvětví, velikost podniku, spoléhání se na technologie i toleranci vůči riziku. Pokud je firma stoprocentně digitální, musí více investovat do ochrany před výpadky. Některé podniky se rozhodnou přijmout větší riziko než jiné, a proto mohou za zabezpečení utratit méně. Určitá úroveň zabezpečení může být stanovena i legislativou," říká Patrick Müller, senior channel account executive společnosti Sophos pro Česko a Slovensko.

Při vyčíslení nákladů spojených s bezpečnostním incidentem je navíc potřeba počítat nejen se ztrátou dat nebo například „výpalným" za jejich rozšifrování, ale i s časem vlastních nebo externích lidí, náklady na obnovení záloh, přerušením provozu, možnými pokutami a v neposlední řadě se ztrátou důvěry. „Z mezinárodních průzkumů vyplývá, že například finanční instituce investují do bezpečnosti zhruba desetinu svého IT rozpočtu. Nicméně podle dalších průzkumů se zdá, že tyto investice nejsou dostatečné. Navíc se situace v IT i kvůli globální pandemii výrazně změnila a musí se změnit i přístup k zabezpečení," uvádí Filip Marvan z Trend Micro.

KLÍČOVÁ ROLE ZAMĚSTNANCŮ

Výzkumy ukazují, že neinformovaní či bezohlední zaměstnanci jsou náchylnější k chybování, což otevírá cestu phishingu a sociálnímu inženýrství. Tito lidé zároveň mívají větší problém s rozpoznáním legitimních aktivit od těch škodlivých. Pokud zaměstnanci skutečně způsobí kyberbezpečnostní ohrožení nebo svým chováním k němu přispějí, často se to navíc pokusí zamaskovat, což následně vede k dalším problémům.

„Základním krokem zabezpečení firemních dat je proškolení zaměstnanců o bezpečném chování v on-line světě. Už jen to, že pracovníci budou věnovat více pozornosti e-mailům, které jim přicházejí, nebudou klikat na podezřelé odkazy a stahovat přílohy, může být v prevenci proti útokům zásadní. Mnoho firem se však na tato školení nezaměřuje nebo je nepovažuje za důležitá. Zejména firmy, které působí mimo technické obory, kde je tato znalost přirozenou, s tím mohou mít problém," uvádí Vítězslav Šantrůček, produktový ředitel společnosti Avast.

Z pohledu útočníka je zaměstnanec samozřejmě jedním z nejjednodušších prostředků, jak se do firmy dostat. Lidé o sobě zveřejňují mnoho informací, které pomáhají zvýšit šanci na úspěch v případě sociálního inženýrství. „Koncoví uživatelé představují riziko, ale jsou také jedním z vašich největších aktiv, pokud jde o včasné odhalení a prevenci útoků proti vaší organizaci. Důležité je vytvořit a podporovat silnou kulturu zabezpečení v rámci firmy. Neexistuje jedno řešení pro všechny, ale dobrým začátkem je zajištění správných lidí, procesů a nástrojů, které zvyšují šance při boji s kyberútočníky," dodává Patrick Müller ze společnosti Sophos.

Tisk se přesouvá z kanceláří domů

Text | Richard Voigts
Foto | Konica Minolta

Pandemie koronaviru se projevila v souvislosti s rozšířením práce z domova i v prodeji tiskáren a spotřebního materiálu. Roste zájem o menší multifunkční zařízení, která se hodí jak do kanceláře, tak pro častější práci doma. Roste také podíl skenování, i když typický poměr naskenovaných a vytištěných stránek zatím výrazně hraje ve prospěch tisku. Digitalizace dokumentů a jejich elektronický oběh je však jednoznačným trendem.

Kdo z pamětníků by si nevzpomněl na revoluci v tisku, která přišla ruku v ruce se sametovou revolucí v roce 1989, kdy přišly do kanceláří malé a spolehlivé rastrové jehličkové tiskárny Epson. Trhu v jehličkovém tisku dnes dominují dva výrobci – Epson a Oki. Jehličkové tiskárny však z pracovních stolů vymizely, protože vydávají zvuk jako u zubaře a pro kvalitnější tisk jsou nepoužitelné. Svoje místo si však našly ve zvláštních provozech, například v pekárnách, protože dokážou tisknout i v prašném prostředí.

Druhů tiskáren a technologií tisku se v průběhu času objevilo více, ale pro kancelářský tisk se dnes používají prakticky pouze laserové a inkoustové tiskárny.

Laserové tiskárny pracují na principu světelného přenosu tiskové předlohy přes světelně citlivý kovový válec s vrstvou polovodiče na povrchu. Existují přitom v zásadě dva druhy laserového tisku – s pohyblivým a nepohyblivým ústrojím. V prvním případě laserový paprsek prochází deflektorem, který v závislosti na přivedeném napětí propouští nebo nepropouští laserový paprsek. Rotující zrcátko přitom rozprostírá paprsek po celé šířce válce. Toner se na válci uchytí jen na osvětlených místech, obtiskne se na papír a je k němu tepelně fixován. V druhém případě je soustava laseru a pohyblivé optiky nahrazena nepohyblivou řadou nebo maticí laserových LED v těsné blízkosti světelně citlivého válce pokrývající celou jeho šířku. Výhodou LED tisku je, že neobsahuje deflektor s pohyblivými díly. Více než 90 procent poruch v IT totiž připadá na pohyblivé díly.

S laserovým tiskem přišla firma Xerox u kopírek a první dostupnou osobní laserovou tiskárnu přivedla na svět firma Hewlett-Packard. Lídry trhu laserového tisku jsou dnes HP, Canon a Konica Minolta. Oki zase vyrábí tiskárny s laserovou LED technologií.

Inkoustové tiskárny také využívají dvou základních technologií – teplou a studenou. V termální inkoustové tiskárně pracuje tisková hlava s tepelnými tělísky zahřívajícími inkoust. Při zahřátí vznikne v trysce bubli-

← NÁROKY NA RYCHLOST A KVALITU TISKU A TAKÉ SKENOVÁNÍ A AUTOMATICKÝ OBĚH DOKUMENTŮ V MODERNÍCH KANCELÁŘÍCH NEUSTÁLE ROSTOU.

na, která způsobí vymrštění inkoustové kapky na papír. U běžných kancelářských tiskáren bývá tisková hlava součástí patrony (cartridge) s náplní inkoustu.

Ve „studené" piezoelektrické tiskárně je tisková hlava tvořena komůrkami z destiček piezoelektrických krystalů schopných měnit svůj objem (tvar) vlivem elektrického napětí. Tím se komůrka (za studena) smršťí a vypudí kapku inkoustu, který není tepelně namáhán. U piezoelektrického tisku tisková hlava zpravidla vydrží několik desítek až stovek tisíc stran.

Lídry trhu v inkoustovém kancelářském tisku jsou Epson (piezoelektrický tisk, zcela opustili laserový), samozřejmě HP a Canon; Brother nabízí všechny technologie (v inkoustovém tisku piezoelektrickou).

LASER, NEBO INKOUST?

Výběr optimální technologie záleží na nejčastější tiskové úloze, množství tisku měsíčně, četnosti barevného tisku, formátu tisku a podobně. Záleží i na výrobci zařízení, jakou technologii který model nabídne.

Pořizovací ceny laserových a inkoustových tiskáren začaly splývat už před lety, a to jak u osobních tiskáren, tak u kancelářských. Cena laserového tisku byla od začátku nízká a jeho provoz je tichý a rychlý. Barevný laserový tisk byl donedávna drahý, vytištěné dokumenty jsou však barevně stálé; tisk fotografií nebo letáků na laserovkách není tak kvalitní jako z inkoustovek. Toner pro laserovky nepodléhá stáří – vždyť jsou to „jen" saze, třebaže už synteticky vyráběné.

O nízkou cenu za potištěnou stranu bojovaly také inkoustové tiskárny, až se v některých případech dostaly i pod cenu laserového tisku, zejména díky velkokapacitním náplním. Nevýhodou inkoustových tiskáren je možnost zasychání inkoustu, zejména u piezoelektrických, čímž dojde ke znehodnocení tiskové hlavy. Při vyšších rychlostech inkoustového tisku může docházet ke krabacení papíru vlivem vlhkosti inkoustu.

Laserový tisk má také několik nevýhod. „Těmi hlavními jsou vysoká spotřeba elektrické energie, produkce ozonu, tepla a prachu. Jde o kontaktní technologii, takže se součásti tiskárny, jako je válec, transferový pás a fixace, opotřebovávají dotykem o potiskovaný materiál. I při tisku třeba malého loga se díly dotýkají celé plochy papíru, to často vede ke vzniku pruhů v obraze," vysvětluje Martin Lucký, obchodní specialista Epsonu. Oproti tomu u inkoustové technologie, ať už jde o termální nebo studenou piezo ▸

KLASICKÁ KANCELÁŘ ZÍSKALA JINÝ ROZMĚR, NEJDE O JEDNO DEDIKOVANÉ MÍSTO A ZÁROVEŇ JE ZDE TLAK NA OBĚH DOKUMENTŮ V JINÉ NEŽ PAPÍROVÉ PODOBĚ.

technologii, se papír tiskové hlavy nedotýká a hlava přejíždí pouze přes místa, kde tiskne. „To umožňuje inkoustovým technologiím potiskovat materiály vícevrstvé nebo citlivé na teplo a tlak," dodává Lucký.

Ve většině kanceláří se dnes používají laserové nebo LED tiskárny. Technologie ale podle Marka Sojaka, marketingového manažera HP, nehraje důležitou roli: „Primárně jde o ekonomickou výhodnost a bezproblémovost celého tiskového řešení, to znamená dostupnost zařízení, bezpečnost či správu. Inkoustový nebo laserový tisk vybíráme podle potřeb a požadavků zákazníka, například pro barevné tisky jednoznačně převládá inkoustová technologie."

Podle Petera Halma, ředitele Xeroxu pro Česko a Slovensko, je však laserová tiskárna pro firemní tisk vhodnější vzhledem k nákladům na provoz, delší výtěžnosti toneru a rychlosti tisku. „Zdánlivou nevýhodou jsou vyšší pořizovací náklady. Ale to v době, kdy si tisková zařízení pronajímáte nebo platíte celé tiskové řešení jako službu, nepředstavuje už problém."

TISKÁRNA JEDINĚ SE SKENEREM

Většina chodbových kancelářských tiskáren se dodává jako multifunkční zařízení, tedy tiskárna ve spojení se skenerem. Souvisí to s digitalizací – proč hned tisknout, když lze dokument naskenovat, případně převést text z papíru do digitální formy?

„V kancelářích pozorujeme stále náročnější požadavky na rychlost a kvalitu tisku, dále pak skenování a automatický oběh dokumentů," potvrzuje Michal Peter, obchodní manažer společnosti Brother. „Zaregistrovali jsme také vyšší poptávku po malých kancelářských zařízeních. Kvůli aktuální situaci se dovybavují domácí pracoviště."

V poslední době je podle Václava Dvorského, marketingového manažera firmy Kyocera Document Solutions Czech, největší zájem o barevná multifunkční zařízení formátu A3. „Vychází z potřeb firmy, kde chytrá multifunkce tvoří vstupní bod pro digitalizaci dokumentů a jejich následný oběh ve firmě. Zároveň tato zařízení poskytují vysoký tiskový výkon, mají nízké náklady na tisk a lze je jednoduše začlenit do stávající architektury tiskového prostředí firmy."

↑ PROČ HNED TISKNOUT, KDYŽ LZE DOKUMENT NASKENOVAT, PŘÍPADNĚ PŘEVÉST TEXT Z PAPÍRU DO DIGITÁLNÍ FORMY?

NOVÝ ROZMĚR KANCELÁŘÍ

Pandemie koronaviru se projevila v souvislosti s rozšířením práce z domova i v prodeji tiskáren a spotřebního materiálu do starších modelů. „Největší zájem registrujeme o vstupní profesionální modely barevných multifunkčních zařízení, které se hodí do kanceláře, případně i pro častější práci v domácnosti. Části zákazníků dostačuje práce s černobílými multifunkcemi. Ty v posledních letech v mnoha případech nahradily samostatné tiskárny," popisuje Lenka Niemiecová, marketingová manažerka Oki Systems. „V souvislosti s koronavirem jsme zaznamenali také vyšší zájem o spotřební materiál ke starším modelům. Ukazuje se, že kvalitní tiskárny zákazníkům slouží běžně i sedm a více let. Skenuje se zhruba desetkrát méně, než se tiskne, tedy na jeden sken připadá 10 výtisků, podíl skenování ale roste, proto jsou třeba stále robustnější a spolehlivější skenery. To naznačuje, co dnes obnáší běžný kancelářský provoz. Statistiky říkají, že podíl objemu A3 tisku bývá nižší než tři procenta, takže tvoří ve firmách jen malý zlomek úloh, a to samé platí o skenování ve formátu A3," doplňuje aktuální kancelářské trendy Niemiecová.

„Klasická kancelář získala jiný rozměr, nejde o jedno dedikované místo a zároveň je zde tlak na oběh dokumentů v jiné než papírové podobě. Současná situace tento trend jen urychlila. Díváme-li se na tiskový segment ve střednědobém horizontu, sníží se podíl tisku, ale na významu nabude digitální forma oběhu dokumentů. Zařízení nebo tisková řešení nebudou situována jen v kancelářích, ale půjde o kombinaci s domácími pracovnami," dodává Petr Hnilička, produktový specialista Canonu.

Jsme banánové děti

Kdo je druhá generace Vietnamců,
která se již narodila v Česku?

Proč si říká „banánové děti“
a považuje vůbec Česko za svůj domov?

jsmebananovedeti.cz

Aktuálně.cz

1 Gb/s

o GIGA rychlejší stahování dat

Podnikejte s Gigabit internetem za 399 Kč měsíčně

vodafone.cz/gigabitprofirmy

bicepsdigital.

Rudolf Matějček a Allen Vidras
spolumajitelé Bicepsdigital

vodafone business