Nedostatek zdrojů řeší bezpečnost jako služba

Až 95 procent informatiků ve vedoucích funkcích očekává nárůst kybernetických hrozeb v následujících třech letech. Ale jen 65 procent organizací podle informací společnosti Gartner zaměstnává specialistu na kybernetickou bezpečnost. Část z nich si služby vysoce kvalifikovaného odborníka nemůže dovolit, část jej nedokáže najít na trhu práce.

Text/ **Lukáš Kříž, David Zajíc**

Nedostatek expertů na kybernetickou bezpečnost představuje pro mnoho organizací problém, který nedokážou rychle vyřešit. Do zvýšení ochrany svého technologického prostředí ovšem mohou v podstatě okamžitě zapojit zdroje třetích stran, a to nejen lidské. Namísto relativně pomalého a nákladného budování interních bezpečnostních řešení zvolí cestu rychlých a kvalitativně i kvantitativně přizpůsobitelných výsledků. Ty organizaci poskytne koncept označovaný zkratkou SECaaS – Security as a Service neboli bezpečnost jako služba.

„Hlavním důvodem pro externí zajišťování služeb kybernetické bezpečnosti je, že zákazník nemá adekvátní počet dostatečně zkušených pracovníků, kteří by se o rychle se vyvíjející bezpečnostní technologie starali," říká Martin Frühauf, bezpečnostní expert společnosti S&T CZ. Myšlenku nedostatečných personálních kapacit rozvíjí Miroslav Dvořák, technický ředitel společnost Eset software: „Bezpečnost jako služba organizacím nabízí možnost nikoliv nahradit, ale spíše doplnit interní IT týmy o bezpečnostní experty, na které by jinak neměly finanční prostředky či jejich služeb potřebují využít jen nárazově."

Model cloud computingu vnesl do světa výpočetních technologií několik myšlenek, které se v rámci oboru úspěšně šíří dále. Na místo investic nastoupil pronájem, podpora se stala samozřejmou součástí předplatného, smluvní vztahy začaly s dosud neobvyk-

Karel Galuška,
T-Mobile

> **Z praxe vnímám, že pojem bezpečnost jako služba je používán v několika významech. Předně je používán pro cloudová bezpečnostní řešení jako antimalware či SIEM. Dále pak pro prostý outsourcing některých bezpečnostních činností u zákazníka externím poskytovatelem.**

lou samozřejmostí pokrývat také flexibilní změny objemu odebíraných zdrojů. Organizace si v tomto režimu mohou pořídit jednu aplikaci nebo celou infrastrukturu. Proč by kybernetická bezpečnost měla stát stranou.

Bezpečnost jako služba

Koncept SECaaS má v podstatě podobu outsourcované služby. Její poskytovatel zajišťuje a spravuje jednu nebo více oblastí kybernetické bezpečnosti. Termín v praxi nabývá dvou základních modifikací. „Z praxe vnímám, že pojem bezpečnost jako služba je používán v několika významech. Předně je používán pro cloudová bezpečnostní řešení jako antimalware či SIEM. Dále pak pro prostý outsourcing některých bezpečnostních činností u zákazníka externím poskytovatelem," upřesňuje Karel Galuška, vedoucí týmu bezpečnosti a business konzultací ve společnosti T-Mobile.

Většina zdrojů model SECaaS popisuje jako dodávku a správu určitého bezpečnostního řešení prostřednictvím internetu. Typicky může jít o antiviry, firewally, o nástroje pro monitorování provozu v síti a o mnoho dalších produktů. Jejich funkcionality jsou poskytovány vzdáleně, z cloudových prostředí. Často se obejdou bez instalace softwarových klientů na koncová zařízení.

Administrátorům v podnicích díky modelu bezpečnost jako služba opadá starost o takto dodávané produkty a funkcionality. Jejich chod a správu zajišťují poskytovatelé. Ti ovšem nenabídnou širší vhled do bezpečnostní situace odběratele a nebudou mu asistovat v případě komplexnějších problémů, jež přesahují jimi zajišťovanou oblast. ›

9,5 %

Podle analytiků Gartneru trh řízených bezpečnostních služeb vloni celosvětově navýšil svůj obrat o 9,5 procenta na 10,3 miliardy dolarů.

anketa

Bezpečnost v cloudu

Jaké jsou hlavní výhody bezpečnostních řešení poskytovaných v modelu cloudových služeb?

Miroslav Dvořák, technický ředitel, Eset software
Také menší společnosti, které nemají většinou odpovídající znalosti v podobě vysoce kvalifikovaných odborníků, si mohou touto formou pořídit zabezpečení ve standardu běžném pro velké společnosti, navíc za přijatelné peníze.

Pavel Minařík, CTO, Flowmon Networks
Odpadají investice, platí se pouze za využívání služby. Zákazník nemusí budovat vlastní infrastrukturu. Oproti tomu stojí omezené možnosti customizace (přizpůsobení), tedy jednoznačně jsou tyto služby vhodné spíše pro menší zákazníky.

Stanislav Smolár, security business manager, Soitron
Cloudová bezpečnostní řešení nejsou výhodná pro každého zákazníka a pro každý typ bezpečnostního řešení. Když zákazník používá Office 365, je vhodné například řešení typu CASBAS (cloud access security broker) na management přístupu k souborům a aplikacím a bezpečnou autentizaci uživatelů.

Michal Hebeda, sales engineer, Sophos
Bezpečnostní řešení poskytované jako cloudová služba má nespornou výhodu v zajištění vysoké dostupnosti a dostatečného výpočetního výkonu poskytovatelem takovéto služby. Tím odpadá zákazníkovi celá řada dodatečných problémů, jako je licenční zajištění podkladových systémů, vysoká dostupnost a výpočetní výkon dimenzovaný na to nejvyšší možné zatížení. Zároveň jsou cloudové bezpečnostní služby dostupné pro jakýkoliv stroj odkudkoliv.

Martin Frühauf, bezpečnostní expert, S&T CZ
Pro zákazníka znamená kvalitně poskytovaná služba v oblasti kybernetické bezpečnosti prokazatelné splnění auditních, legislativních a bezpečnostních požadavků. Zároveň s tím mu odpadá problém s počtem a zkušenostmi jednotlivých pracovníků, kteří jsou nedostatkovým zbožím a je nutné investovat peníze do jejich průběžného vzdělávání.

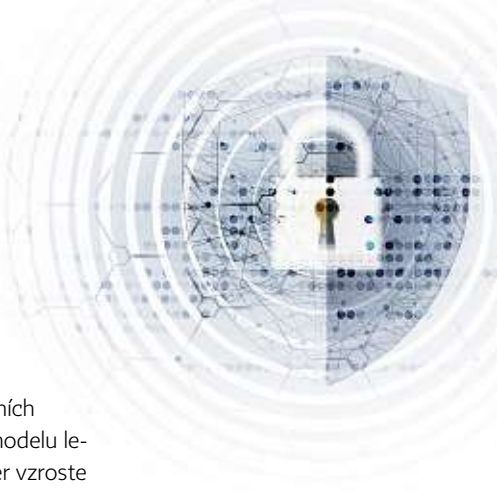
Karel Galuška, vedoucí týmu bezpečnosti a business konzultací, T-Mobile
Primární výhodu vidím v efektivitě služeb dané sdílením prostředků, možnosti vždy čerpat jen potřebné zdroje a rychle škálovat jak ve smyslu navýšení, tak snížení potřebné kapacity. Zákazníkům se tak otevírá možnost využívat špičkové technologie bez pořizovacích nákladů a zbavení se starostí s údržbou těchto technologií. Tradičně obezřetní manažeři kybernetické bezpečnosti postupně objevují výhodu tohoto modelu. Zvláště viditelné je to u bezpečnostních technologií, které ještě nejsou vnímány jako klíčové, ale přitom jsou velmi nákladné jak na pořízení, tak na provoz. ■

Vystupují jen jako dodavatelé, správci a případně i konzultanti konkrétních technologií.

Druhá modifikace modelu SECaaS patří více do tradičního světa informačních technologií a přístupů k zajištění jejich provozu. Poskytovatel řízených bezpečnostních služeb typicky přebírá doposud interně zajišťovanou správu příslušných řešení od zákazníka. Jde tedy o tradiční, třebaže úzce specializovaný, outsourcing. Obvykle bývají jeho poskytovatelé označováni zkratkou MSSP – Managed Security Service Provider neboli poskytovatel řízených bezpečnostních služeb.

Dle definice společnosti Gartner se tyto podniky primárně zabývají monitorováním zabezpečení a správou bezpečnostních zařízení u zákazníka. Pro zefektivnění vlastního provozu často zřizují specializovaná operační centra. V nich soustřeďují specialisty na různé technologie nebo problematiky, kteří obsluhují více zákazníků. Mohou z nich část funkcionalit také poskytovat. Operační centra zajišťují rovněž řešení případných bezpečnostních incidentů. „Speciální případ bezpečnosti jako služby představují tzv. SOC – Security Operation Center. Tato centra konsolidují bezpečnostní řešení. Zákazníci využívají jejich služeb a do jisté míry předávají odpovědnost za bezpečnost infrastruktury na třetí stranu," upřesňuje Pavel Minařík ze společnosti Flowmon Networks.

Obě pojetí si podle názoru oslovených expertů v zásadě nekonkurují. V praktickém nasazení je lze úspěšně kombinovat. „Oba typy služeb mají své specifické zákazníky, a příliš si tedy nekonkurují. Cloudová bezpečnostní řešení volí zákazníci, kteří chtějí outsourcovat provoz samotných bezpečnostních technologií nebo se jejich IT infrastruktura vyskytuje již převážně v cloudo-



vém prostředí, avšak bezpečnostní procesy realizované pomocí těchto technologií chtějí provádět vlastními silami. Služby řízené bezpečnosti naopak zajišťují celý bezpečnostní proces a výrazně tak přesouvají odpovědnost na samotného dodavatele. Technické i organizační rozhraní mezi zákazníkem a poskytovatelem je pak pro oba typy služeb na zcela jiné úrovni," vysvětluje Karel Galuška ze společnosti T-Mobile.

„Po technologické stránce není mezi MSSP a cloudovými službami žádný podstatný rozdíl. Rozdíl je v doprovodných službách. Obecně se u poskytovatelů cloudových služeb setkáváme s omezenou podporou a dostat se k relevantnímu pracovníkovi, který pomůže v dané situaci, je mnohdy téměř nemožné. MSSP mají výhodu, jsou zákazníkovi blíž a umí lépe řešit jeho potřeby. Alespoň tak by to mělo být a to je hlavní přidanou hodnotou MSSP. Na druhou stranu je třeba počítat s vyšší cenou služeb," dodává Pavel Minařík, CTO společnosti Flowmon Networks.

Tržní výhledy

„Obecně se dá říci, že řešení IT bezpečnosti nebo celé oblasti IT formou služby poptávají a využívají společnosti, které se chtějí soustředit především na vlastní předmět činnosti. V případě cloudových řešení pak vidím zájem spíše u společností, které provozují IT ve vlastní režii," komentuje současný stav trhu Miroslav Dvořák ze společnosti Eset software.

Obrat globálního trhu bezpečnostních služeb poskytovaných v cloudovém modelu letos podle predikce společnosti Gartner vzroste o 17 procent na 6,86 miliardy dolarů. Zhruba o jednu miliardu dolarů má segment, jenž při mírném zjednodušení lze označit zkratkou SECaaS, každoročně posilovat i v následujících dvou letech. Svým tempem růstu překonává výkonnost celého trhu informační bezpečnosti. Jeho obrat má letos dosáhnout hodnoty 114 miliard dolarů. Meziročně vzroste o 12,4 procenta. Příští rok ale podle predikcí analytiků tempo vývoje trhu informační bezpečnosti zpomalí na 8,7 procenta.

Hlavní produktovou kategorii v segmentu bezpečnostních služeb poskytovaných z cloudu představují řešení pro správu přístupů a identit. Na celkovém obratu segmentu se podílejí téměř dvěma pětinami. Po desetině shodně generují e-mailové a webové bezpečnostní brány. Jednociferné podíly drží bezpečnostní testování apli- ›

sloupek

Michal Hebeda,
sales engineer, Sophos

Cloudová správa bezpečnostních produktů – strašák, nebo hrdina?

Již od počátku vývoje bezpečnostních IT produktů bylo nutno řešit jejich správu. Zpočátku byl každý jednotlivý produkt řízen zcela samostatně a administrátor musel nastavovat zabezpečení na každém počítači. Velkým skokem bylo uvedení a zavedení centrální správy. Řada procesů byla zjednodušena, bylo možno nastavit současně stovky klientských počítačů.

Řešení s jednou centrální administrací bylo velmi výhodné v situaci, kdy všechny spravované počítače jsou v jedné lokální síti. Avšak doba se mění a v současnosti je nemalá část uživatelů připojena odkudkoliv a někdy celé týdny mimo mateřskou lokální síť. Přesto je vyžadováno být nepřetržitě v kontaktu s centrální konzolí kvůli stahování nových politik či virových definic nebo reportování stavu.

Z výše uvedených důvodů bylo nutno vytvářet VPN propojení a otevírat administrační porty z internetu směrem do lokální sítě.

Nejeden výrobce přišel s myšlenkou řízení produktů pomocí cloudové administrace na svých serverech. Tyto servery jsou přístupné odkudkoliv z internetu, obvykle na standardních portech s garantovanou vysokou dostupností, již bychom těžko zajišťovali u sebe. Uživateli tak odpadá starost se zajištěním dostatečně výkonných serverů, internetové konektivity a celkově údržby svých serverů.

Pokud výrobce nabízí více různých produktů, je cloudová správa tou správnou možností, jak tyto produkty spravovat z jednoho místa, bez nutnosti násobných administračních konzolí. Dokonce jsou takoví výrobci, již naučili své produkty mezi sebou takto navzájem komunikovat.

A jaká jsou úskalí cloudové správy? V první řadě jde o zabezpečení přístupu. Dobrý výrobce nabízí vysokou úroveň zabezpečení vlastního datacentra a také vícefaktorové ověřování pro přístup. ■

kací, funkcionality SIEM a vzdálená detekce zranitelností. Téměř čtvrtina obratu trhu ale připadá na řešení zařazená do kategorie Ostatní. Nejrychleji se podle analytiků společnosti Gartner rozvíjejí dílčí segmenty malwarových sandboxů, šifrování dat, správy zabezpečení koncových stanic, zpravodajství týkající se hrozeb a webové aplikační firewally. Ke všem řešením a službám v předchozím výčtu se samozřejmě pojí přívlastek cloudový.

„Přístup zákazníků se v posledních letech silně mění a i některé tradiční vertikály, jako například státní správa, již začínají cloudové bezpečnostní služby využívat. Zpočátku byl vidět příklon ke cloudové bezpečnosti ve formě služby hlavně u menších zákazníků, kteří neměli dost možností pro budování potřebné infrastruktury, nicméně nyní vidíme opravdu velkou poptávku po cloudových bezpečnostních službách od zákazníků všech velikostí i vertikál," prezentuje tržní potenciál bezpečnosti jako služby Michal Hebeda, sales engineer ve společnosti Sophos.

Zájemci ze všech oblastí průmyslu

Na zájmu o bezpečnost jako službu mezi oslovenými specialisty nepanuje jednoznačná shoda. Podle Stanislava Smolára, security business managera ve společnosti Soitron, patří k nejčastějším odběratelům bezpečnosti ve formě služby firmy z energetického sektoru. „Bezpečnost není jejich hlavní byznys, a proto hledají možnosti, jak tento problém řešit efektivně," dodává. Martin Frühauf ze společnosti S&T CZ specifikuje současnou uživatelskou základnu šířeji: „Z našeho pohledu jsou nejčastějšími odběrateli bezpečnosti ve formě služby zákazníci z finančního sektoru, následovaní provozovateli kritické informační infrastruktury a významných informačních systémů. Stále více požadavků se objevuje z oblasti průmyslu a výroby."

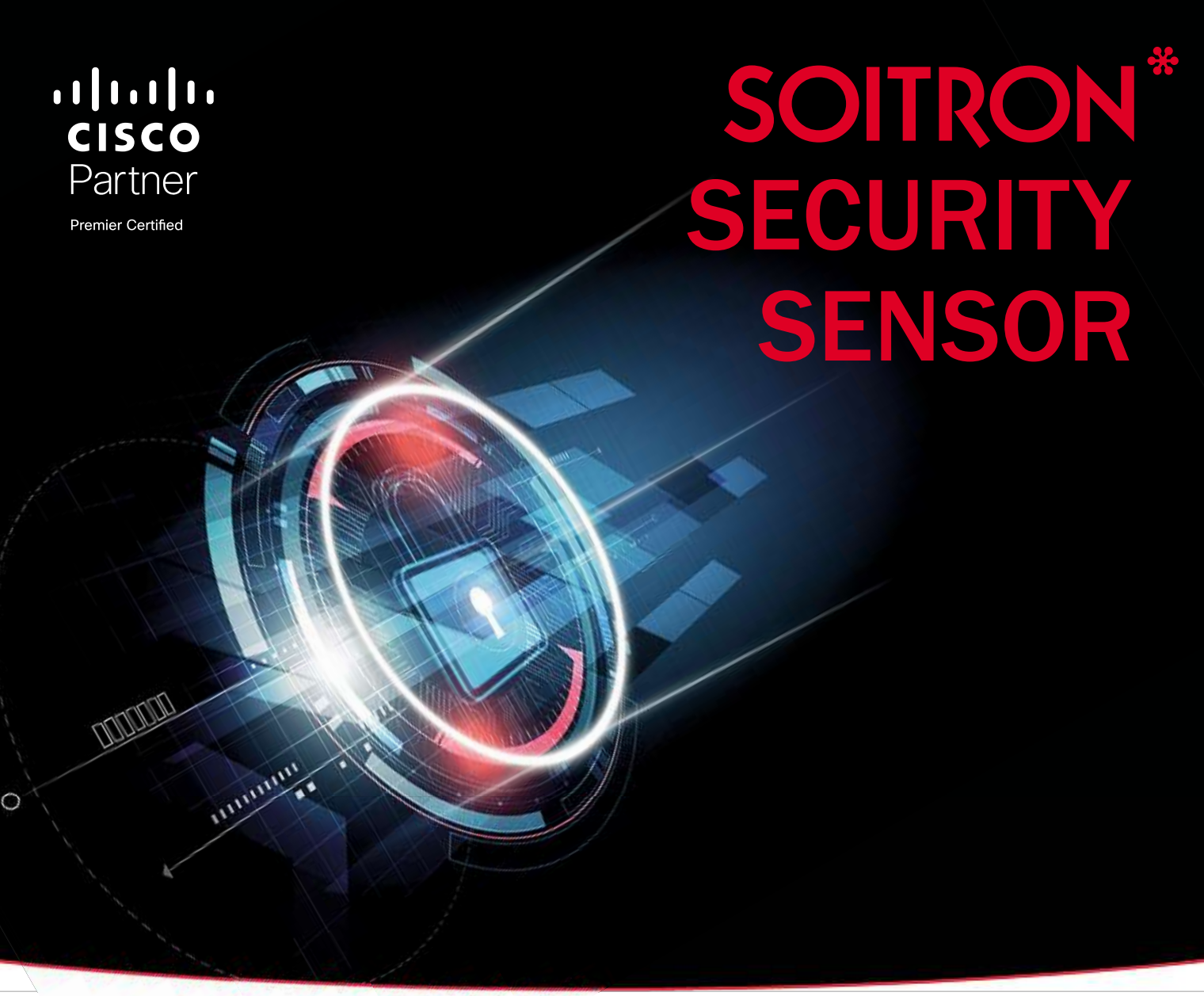
Růst trhu SECaaS pohání především poptávka generovaná podniky kategorie SMB. Podle analytiků pro ně cloudové médium představuje přirozený prostředek pro naplnění jejich potřeb. „Podnik by měl uvažovat o outsourcingu vždy v případě, když nemá dostatečné vlastní zdroje. Díky optimalizaci lidských a technických zdrojů v rámci poskytování bezpečnosti jako služby umí být řešení cenově výhodné i pro malé a střední podniky," doplňuje Stanislav Smolár ze společnosti Soitron. Díky službám poskytovaným z cloudu získávají i menší podniky přístup k jinak nedostupným řešením a funkcionalitám. Analytici společnosti Gartner navíc očekávají, že do dvou let bude polovina bezpečnostních produktů poskytována ve formě cloudových služeb.

Trh řízených bezpečnostních služeb vloni celosvětově navýšil svůj obrat o 9,5 procenta na 10,3 mil. dolarů. Podle analytiků Gartneru se na něm vedle zavedených hráčů úspěšně etabluje řada nových poskytovatelů. Tomuto trendu odpovídá i skladba výdajů na informační bezpečnost. Téměř čtvrtina pořizovaných bezpečnostních řešení, případně funkcionalit, se k zákazníkům dostává právě prostřednictvím řízených služeb.

Oboroví analytici se v definici segmentu řízených bezpečnostních služeb liší. Různé zdroje je kvantifikují v intervalu 10 až 50 mil. dolarů. Rozdílnost mají obvykle na svědomí bezpečnostní řešení poskytovaná z cloudu, tj. převažující pojetí bezpečnosti jako služby. ■

cisco Partner
Premier Certified

SOITRON SECURITY SENSOR



OTESTUJE BEZPEČNOST VAŠÍ FIREMNÍ INFRASTRUKTURY.

- Analýza IT sítě
- Odborné poradenství
- Přehled hrozeb

www.soitron.com

EK011742

Integrace se širokým záběrem

Společnost Soitron působí v sedmi zemích po celé Evropě jako systémový integrátor v oblasti síťové infrastruktury, datových center a hlasových řešení. Slávka Šikurová, obchodní ředitelka pro český a slovenský trh, právě tyto oblasti označuje jako dlouholetý core business společnosti.

Text/ **Aleš Procházka**

Můžete společnost Soitron krátce představit? Čím se zabýváte?
Společnost Soitron je středoevropským integrátorem, který působí na IT trhu více než 27 let. Svým klientům nabízí produkty a služby v oblasti robotizace a automatizace procesů, internetu věcí (IoT), IT infrastruktury, komunikačních a cloudových řešení, IT bezpečnosti, služeb, outsourcingu, IT poradenství a aplikací.

Soitron Česká republika je členem skupiny Soitron Group, ve které pracuje přes 800 mezinárodních odborníků a sdružuje profesionální týmy na Slovensku, v České republice, Rumunsku, Turecku, Bulharsku, Polsku a Velké Británii.

Která řešení a služby tvoří váš core byznys?
Jsme systémový integrátor v oblasti síťové infrastruktury, datových center a hlasových řešení – toto je náš dlouholetý core business.

Ale i tyto oblasti se neobejdou bez automatizačních a analytických nástrojů, o které jsme naše kompetence před několika lety rozšířili a díky nim jsme dnes schopni velmi pružně reagovat na změny, jež v této oblasti nastávají. Obzvláště tím, že nástroje sami vyvíjíme a rozvíjíme na základě zkušeností z nasazených projektů.

Automatizace v komunikačních řešeních pomocí botů je díky tomu dnes naším denním tématem, taktéž analytika a interpretace dat, které dnes díky IoT řešením vznikají v nepřeberném množství. A díky našim dovednostem v oblasti outsorcingu a servisním službám jsme schopni všechna tato řešení klientům doručit, jak formou služby, tak jako řešení s požadovanou úrovní podpory.

Naším cílem je být vždy na technologické špici, inspirovat naše klienty k inovacím a rozvíjet nové projekty, které posléze přejdou do IT trendů.

Výrazným trendem posledních let je koncept cloudu. Jaká je podle vašich zkušeností adopce takových řešení mezi českými či slovenskými firmami?
Nejsme typickým cloudovým poskytovatelem služeb. Naší výhodou v rámci cloudových služeb je nestranný pohled na využití cloudů různých poskytovatelů a optimální kombinace těchto služeb. Nedílnou součástí je zejména stanovení vhodnosti použití cloudu nebo takzvaného hybridního režimu – cloudu a on-premise řešení.

Rozdíl mezi českým a slovenským trhem v oblasti absorbce cloudových služeb není nijak dramatický – což už nelze konstatovat ve vztahu k západní Evropě. Náš trh je značně konzervativní (ale to neznamená, že i tady nejsou černé labutě) a přijímání těchto novinek je značně pomalejší. O důvodech můžeme jen spekulovat, ale minimálně jeden se opakuje v podstatě všude – neochota předat své kritické systémy/data do prostředí, které IT správci nemají pod kontrolou. Proto v poslední době řešíme velké množství scénářů realizace datových center, která jsou založena na hybridních architekturách, kdy jsou kombinované výhody cloudové architektury s on-premise řešením.

Naše kompetence, jak v architektuře a migraci do cloudových řešení s kombinací s dlouhodobými zkušenostmi v designu, tak v implementaci a provozování on-premis řešení, nám umožňují najít pro klienta ten nejvhodnější model. A mnohdy se opravdu ukazuje, že i z ekonomického hlediska je tato cesta nejvýhodnější, v čem nám také hodně pomohly hyperkonvergované platformy.

Dá se říct, v kterých odvětvích průmyslu jeví firmy o cloud největší zájem?
Naše řešení a služby jsou prioritně postaveny na potřebách zákazníka. Tedy nelze jednoznačně říct, kde jsou cloudové služby vhodné a kde ne. Vždy záleží na návrhu architektury řešení, které plyne ze znalosti každého jednotlivého zákazníka. A tímto jsme pro zákazníka transparentní partner, protože neprotlačujeme jediné řešení, ale kombinaci několika možností, které plně respektují požadavky na IT zákazníka.

Nemyslím si, že jsou nějaká odvětví, kde to jde lépe a kde hůř. Extrémně záleží na architektuře stávajících aplikací a úrovni „standardizace“ IT prostředí klienta. Obchodní řetězce, výrobní podniky, bankovní sektor dnes běžně využívají cloudové služby, a to mnohdy i pro core aplikace. Dnes většina seriózních poskytovatelů cloudových služeb disponuje veškerými certifikáty spojenými s bezpečností, ochranou dat, dostupností služeb, že ani v této oblasti nejsou nějaká zásadní omezení.

Je ale zcela evidentní, kde se cloudovému prostředí daří nejvíce, jsou to projekty budované na zelené louce (a tím myšleno i uvnitř již zaběhlých firem), kde rychlost a dynamičnost cloudového prostředí je pro tyto projekty přímo ideálním prostředím.

Firmám, které s cloudem váhají, poskytujete „simulační“ službu Soitron Cloud Testing (Soitron CT)? Co jí sledujete?
Tyto služby mají pomoci klientům odpovědět na otázky, které si mnohdy klienti ani sami neuvědomují anebo netuší, že si je musí položit.

Na základě našich zkušeností a ověřeného postupu klientovi nastíníme, na co by se měl zaměřit. Necháme ho nasimulovat často opomíjené migrační scénáře, uděláme simulaci požadovaných výkonů v cloudovém prostředí, případně otestujeme aplikace, které při analýze identifikujeme jako problematické. Takže každý klient, který si nedokázal na nastíněné otázky sám sobě odpovědět před testingem, tuto službu následně rád využije.

Důležitým výstupem je mimo jiné i zvolení správného cloudového poskytovatele. Což může být jedním z požadovaných ukazatelů zákazníka.

Máte svá datová centra?
Vlastní datová centra neprovozujeme, pro naše klienty vždy vybíráme nejvhodnější datové centrum z nabídky na trhu. Čemuž odpovídá i výše zmíněná služba Soitron CT.

V nabídce máte celou řadu vlastními odborníky navržených služeb. Jednou z nich je například řešení pro analýzu a dohled na síti. Pro koho je tato služba určena?
Soitron Security Senzor je řešení, které klientovi pomáhá získat reálný pohled na bezpečnostní situaci v rámci jeho infrastruktury.

Služba je určena všem klientům bez rozdílu velikosti či zaměření. Umožňuje pomocí velmi hloubkové analýzy a aktivního skenování prostředí klienta získat přehled o možných bezpečnostních rizicích, kterým je společnost vystavena. Klient obdrží velmi podrobný report o stavu s doporučením, jak které riziko eliminovat.

Naše zkušenost říká, že všude, kde jsme Soitron Security Senzor použili, tak jsme identifikovali rizika na různých úrovních.

V čem se Security Senzor odlišuje např. od bezpečnostního systému SIEM, jehož implementaci také nabízíte?
SIEM je management nástroj, který slouží primárně ke korelaci informací ze všech systémů v rámci společnosti, k jejich vyhodnocování a interpretaci. Nejedná se o aktivní nástroj, který podrobuje prostředí aktivnímu testování.

Velkým tématem je dnes digitalizace a automatizace, automatizace firemních procesů. Ve kterých oborech s tím svým zákazníkům pomáháte?
Automatizace procesů je nejen velkým tématem, ale je i prostorem pro zákazníky provést optimalizaci procesů a získat úsporu jak v čase, tak možná i v personální oblasti. Z naší zkušenosti se toto týká nejen interních procesů, ale i externích procesů našich zákazníků, a to především v oblastech výroby, bankovnictví a pojišťovnictví.

Vezme-li například zmíněnou oblast finančních služeb. Co všechno lze automatizovat?
Ve finančních službách lze optimalizovat zejména vyřízení všech požadavků klientů finančních subjektů. Zde lze poměrně velkou část komunikace automatizovat a optimalizovat. Ale nenechme se mýlit, že největším přínosem pro finanční subjekty je pouze optimalizace „externích" procesů, lze optimalizovat i vnitřní a kontrolní procesy. Těchto optimalizačních změn může být celá řada a mohou přinést nemalé úspory a vyšší efektivitu a výkon.

Další oblastí související s digitalizací je internet věcí, také těmito technologiemi se zabýváte. Máte již konkrétní projekt založený na IoT řešeních?
Ano, máme a ne jeden. Jde o projekty z oblasti facility a výroby. V těchto odvětvích posouváme IoT vnímání, které si mnohdy představujeme jen jako sběr veličin. My ale jdeme dále a vnášíme do řešení nejen analytické prvky, nýbrž v neposlední řadě také prvky automatické predikce. Zákazníci takto získávají s naším řešením kompletní nástroje na řízení svých nákladů, a to nejen jako spotřebu energií, ale i řízení nákladů jako vstupů do jejich produktů. Tedy provázáním nákladových položek s výrobkem. Toto je náš největší benefit.

Na začátku jste zmínila, že Soitron zaměstnává 800 lidí. Je obecně známým faktem, že na trhu chybí IT odborníci všeho druhu. Jaké profese jsou neproblematičtější?
Největší problém je s lidmi na pozici architektů – takoví, kteří mají zkušenosti skrz více oblastí a dokážou vidět širší souvislosti, navrhovat řešení, která zasahují do více technologických oblastí – a to platí jak pro infrastrukturní, tak aplikační projekty. Dlouhodobým problémem jsou také lidé, kteří mají schopnosti být opravdovými konzultanty – umět komunikovat s klientem, vést dialog, směrovat myšlenky týmu (jak interního, tak i na straně klienta) – této schopnosti lze člověka, který má odborné dovednosti, naučit. ■

Foto: Eva Kořínková

Slávka Šikurová (40),

má více než 15leté zkušenosti na různých vedoucích pozicích v oblasti IT, v retailu či službách.

Do Soitronu nastoupila v roce 2016 na pozici ředitelky divize pro IT infrastrukturu a softwarové aplikace. Aktuálně zastává post obchodní ředitelky pro český a slovenský trh a zároveň je jednatelkou softwarové firmy Millennium.

Slávka Šikurová vystudovala Management na Univerzitě Komenského v Bratislavě a na Australian International College získala certifikát v oblasti informačních technologií.