OTEVÍRAT FIRMÁM OČI

KULATÝ STŮL

O kybernetické bezpečnosti napříč celým řetězcem

S hosty našeho Kulatého stolu, kterými tentokrát byli Jan Dobrý (Anect), Karel Klumpner (Comguard), Martin Lohnert (Soitron), Vladimír Mlynárčik (Clico) a Filip Navrátil (Eset), jsme probrali otázky kybernetické bezpečnosti z pohledu partnerů, distributorů a vendorů. Řec byla o aktuálním dění na poli hrozeb, přístupu zákazníků, potenciálu nových obchodních modelů i o odkazu pandemie.

„Do letošního roku jsme asi všichni šli s očekáváním, že už bude lepší pandemická situace," zahajuje diskuzi **Jan Dobrý**, head of security department ve společnosti Anect. „To se bohužel nenaplnilo, lidé stále pracují z domova, nechodí do kanceláří a všechno probíhá on-line. Řeklo by se, že rok je dostatečná doba na to, aby se všichni přizpůsobili, ale není tomu tak. Firmy možná nečekaly, že to bude trvat tak dlouho, ale některé reagují až teď, například tím, že spouštějí e-shopy. To vše s sebou samozřejmě nese různé bezpečnostní výzvy."

„Souhlasím, home office a další formy digitalizace spojené s pandemií jsou jednoznačným trendem této doby a mají za následek velký růst poptávky po cloudových službách," přikyvuje **Karel Klumpner**, obchodní ředitel Comguardu. „Druhým globálním trendem pak je, že v tichosti vypukla regulérní kybernetická válka, která se projevuje cílenými útoky na renomované IT vendory. Namátkou zmíním Bitlocker, SolarWinds, FireEye, Stormshield, Microsoft… a mohl bych pokračovat."

„V oblasti bezpečnosti bohužel hraje zásadní roli stále stejný trend – je dlouhodobě podceňovaná a zanedbávaná," říká **Martin Lohnert**, ředitel bezpečnostního operačního centra Void SOC společnosti Soitron. „U příliš mnoha organizací, se kterými jsme se setkali, bylo zabezpečení ve špatném stavu a nemělo dostatečnou prioritu. Na druhou stranu, během posledního roku se všeobecný přístup k security začal mírně zlepšovat vlivem toho, o čem mluvili kolegové přede mnou. Firmy velmi rychle přešly do on-linu, což se neobešlo bez incidentů, a přinejmenším některým zákazníkům to otevřelo oči a začali vnímat security jako důležité téma."

„Já se mohu jen podepsat pod to, co říkal Martin," navazuje **Vladimír Mlynárčik**, country manager společnosti Clico pro ČR a SR. „Bezpečnost byla v posledních letech velmi podceňované téma a pandemie to z mého pohledu otočila. Dnes se dá se zákazníky hovořit o tématech, o kterých by se nám před dvěma lety ani nesnilo. Neříkám, že z toho je okamžitá monetizace, ale už to, že se ta témata otevírají, je velmi pozitivní."

„Pánové už to trochu nakousli, ale pandemie odkryla v plné nahotě, kdo byl připraven a dokázal se přesunout na digitální platformy, a kdo ne," dodává **Filip Navrátil**, obchodní ředitel českého Esetu. „My jsme si na tohle téma udělali průzkum a zjistili jsme, že české firmy nebyly nachystané na první vlnu, což se ještě dá pochopit, ale řada z nich pak nebyla připravena ani tu na druhou vlnu na podzim, což už se úplně obhájit nedá. Ta nepřipravenost se bohužel projevovala i neznalostí naprosto elementárních zásad, jako je třeba vzdálené připojení přes VPN, což pak mívalo fatální důsledky. Některé kauzy byly medializované, spousta dalších nebyla, ale celkově to ukazuje, jaký mají české firmy přístup k bezpečnosti a jaké zdroje, ať už lidské, technické nebo finanční, jsou jí ochotné věnovat."

Aktuální hrozby

„Pokud to shrnu, útočníci dnes používají staré osvědčené techniky naroubované na aktuální témata, například falešné phishingové e-maily s výsledky testu na koronavirus, registrací na očkování a podobně," říká **Filip Navrátil** (Eset). „To je jedna velká kategorie, tou druhou jsou pak skutečně cílené a sofistikované útoky, o kterých mluvil pan Klumpner. Oblíbenou metodou zůstává ransomware a v poslední době pak zaznamenáváme také zvýšenou oblibu malwaru pro těžbu kryptoměn, protože cena bitcoinu letí nahoru a těžení je pro útočníky čím dál lukrativnější. V blízké budoucnosti bude ještě zajímavé sledovat, do jaké míry se objeví malware zacílený na novou procesorovou architekturu M1 od Applu."

„My jako distributor nejsme v první linii, takže předesílám, že většinu informací mám od našich partnerů, nicméně podle všeho v posledních obdobích skutečně častěji dochází k rozsáhlým ransomwarovým útokům," přidává se **Vladimír Mlynárčik** (Clico). „Naši inženýři nedávno asistovali u několika závažných incidentů v Česku a na Slovensku včetně případu velkého průmyslového zákazníka, který měl na tři týdny úplně odstavenou výrobu a tři tisíce zaměstnanců musely zůstat doma. To jen pro ilustraci, jak masivní škody může způsobit neopatrné kliknutí."

„My jsme před několika lety využili právě to, že se u nás sbíhají informace od partnerů, a spustili jsme monitorovací službu ThreatGuard, která sleduje dění na poli zranitelností a hrozeb zaměřených pouze na infrastrukturu firem," navazuje **Karel Klumpner** (Comguard). „Na základě našich poznatků a dat z TreatGuardu pravidelně vydáváme žebříček deseti nejzávažnějších hrozeb a já tu jen telegraficky přečtu ten nejnovější. Sestupně jsou to: SolarWinds, zranitelnost v Microsoft Windows Netlogon Remote Protocolu, kritická chyba v Microsoft DNS Serveru, získání systémových práv pomocí produktů SAP, kritická zranitelnost v produktech VMwaru, vzdálené spuštění kódu a krádež dat z Apache Tomcatu, zranitelnost v Zoomu, zranitelnost v ManageEngine Desktop Centralu, vícenásobná zranitelnost v Cisco Datacenter Network Manageru a možnost eskalace práv v zařízeních s Androidem. Do publikace této naší diskuze se tento žebříček bezesporu změní, nicméně je to pořád hezká ilustrace toho, jak pestré jsou problémy, kterým musejí bezpečnostní týmy umět čelit."

„U našich zákazníků se v posledních měsících nedělo nic, na co bychom nebyli zvyklí," tvrdí **Martin Lohnert** (Soitron). „V drtivé většině případů šlo o takové ty běžné útoky, které všichni dobře známe a víme, jak se před nimi chránit, ať už jde o různé phishingy, nebezpečné plug-iny do prohlížečů a podobně. Nicméně Vlado před chvílí zmínil průmysl, což je velmi zajímavá oblast, neboť se zde stírá hranice mezi digitální a fyzickou bezpečností. Jinými slovy, napadení výrobních technologií může teoreticky vést ke škodám na majetku, zraněním nebo přímo úmrtím, takže si tyto systémy zaslouží obzvlášť pečlivou ochranu. Problém je, že často nemají doslova žádnou. V Soitronu dlouhodobě monitorujeme počet průmyslových systémů, které jsou přístupné z internetu. V ideálním případě by jich mělo být přesně nula, ve skutečnosti se ale nacházíme na historicky nejvyšších číslech, konkrétně 1 425 v Česku a 469 na Slovensku. To jsou skoro dva tisíce výrobních systémů, do kterých může v podstatě kdokoliv získat anonymní přístup. Pokud hovoříme o trendech, průmyslový segment by si bezesporu zasloužil více pozornosti."

„Pan Lohnert má naprostou pravdu v tom, že průmysl, případně jakékoliv další odvětví, kde se používají SCADA systémy, si zaslouží podstatně větší péči," navazuje **Jan Dobrý** (Anect). „Obecným problémem bývá, že průmyslové firmy často razí zásadu na nic nesahat, dokud to funguje, takže výrobní stroje mnohdy běží na nějaké zastaralé variantě embedded Windows, která už dávno není podporovaná. To by samo o sobě nevadilo, pokud by se dbalo na segmentaci sítí, ale to se zpravidla neděje. Vzpomínám si třeba na jeden případ, kdy měl zákazník v rámci jedné sítě zapojenou celou výrobní linku plus padesát počítačů v kancelářích bez jakéhokoliv oddělení. SCADA systémy se navíc nepoužívají pouze v továrnách, jsou to třeba i čidla ve vodárnách, zařízení v elektrárnách a podobně. To už je velké lákadlo, a až přestanou fungovat tyto sítě, bude to teprve problém."

Přístup organizací

„Když se na chvíli vrátíme k ransomwaru, měla by zaznít jedna důležitá věc," říká **Filip Navrátil** (Eset). „Ransomware není celý útok, ale pouze jeho poslední krok, který přijde ve chvíli, kdy s vámi je útočník hotový, to znamená, že úspěšně pronikl do sítě, nakradl si, co chtěl, a možná vám tam zanechal i něco na památku. Často se bohužel stává, že firma řeší pouze zašifrovaná data a nepřemýšlí, jak se útočník dostal do sítě, kdy se tam dostal a co všechno tam napáchal. Zálohovací řešení jsou skvělá věc, ale pokud nevíte, jak dlouho útok probíhal, tak nevíte, ke kterému datu vlastně máte data obnovit, a riskujete, že je obnovíte i se spícím malwarem, který vám je za týden zašifruje znovu. Tohle je téma, o kterém by se také mělo hovořit častěji."

„Souhlasím, navíc je to téma, které má širší souvislosti," navazuje **Jan Dobrý** (Anect). „Nejde ani tak o kvantitu či kvalitu nástrojů, které máte nasazené, ale o přístup zaměstnanců, a teď nemyslím běžné uživatele, nýbrž administrátory. Pokud nastane situace, že se vám útočník celé týdny, nebo dokonce měsíce bez povšimnutí pohybuje v síti, je to fatální selhání administrátora a většinou za tím stojí laxní přístup, to znamená slabá, případně defaultní hesla, absence dvoufaktorové autentizace a další prohřešky proti pravidlům, jejichž dodržování by mělo být naprostou samozřejmostí. Zašifrování dat a výzva k zaplacení už je skutečně jen taková třešnička na závěr."

„Pánové mají pravdu, a rád bych poukázal na to, jak obrovský prostor se zde nabízí partnerům pro trpělivou osvětu," přidává se **Vladimír Mlynárčik** (Clico). „A podtrhuji slovo trpělivou, protože na jednu stranu ano, každý kybernetický útok může firmě potenciálně způsobit nevyčíslitelné škody, ale na druhou stranu bychom se měli snažit lidsky pochopit, proč k zanedbávání bezpečnosti vůbec dochází. Zaprvé to bývá tím, že zaměstnanci mají nespočet jiných povinností, zadruhé pak tím, že samotná organizace neklade na bezpečnost dostatečný důraz. Před několika lety jsme společně s jedním partnerem dodali řešení pro aplikační firewall na slovenský vládní úřad. Minulý rok se tam dělaly nějaké upgrady a při té příležitosti se zjistilo, že ten firewall celou dobu fungoval v režimu any-to-any, jinými slovy byl otevřený dokořán. V první chvíli se o vás pokoušejí mdloby a říkáte si, jak se to proboha mohlo stát, ale pak vám dojde, že tam nemají žádné dedikované bezpečnostní oddělení, pouze běžné IT oddělení, které má na starosti úplně všechno a je pod neustálým tlakem. A když jsme pod tlakem, děláme chyby. Proto říkám, že je tu obrovský prostor pro partnery, aby trpělivě šířili osvětu a dělali kontroly a analýzy."

„S otázkou lidských zdrojů se setkáváme velmi často," přitakává **Martin Lohnert** (Soitron). „Není to jediná příčina toho neutěšeného stavu, ve kterém

Jan Dobrý
head of security department, Anect

„Bývá me mile překvapeni, když potkáme zákazníka, který má o security nějaké povědomí a dá se s ním hovořit o službách a řešeních na vrcholku bezpečnostní pyramidy. Stále ovšem narážíme na firmy, které potřebují pomoci s úplnými základy."

Karel Klumpner
obchodní ředitel, Comguard

„Někdy mají firmy osvícené vedení, ale demotivované zaměstnance. Jinde se zase vedení střídá jako na běžícím páse a standardy se tam udržují jen díky lidem z provozu. Partner musí být v tomto ohledu chytrý a posuzovat každého zákazníka individuálně."

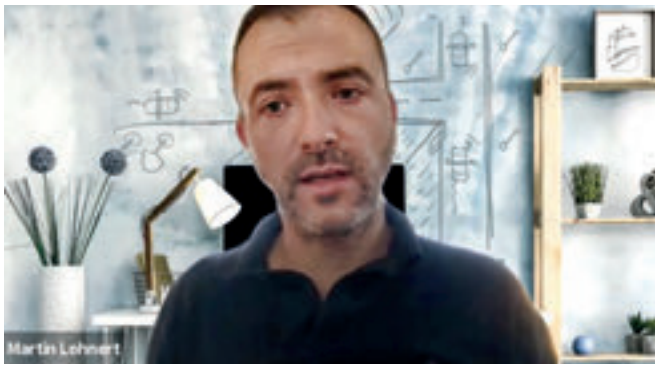
se nacházíme, ale má na něm výrazný podíl. Ovšem i když má zákazník implementované bezpečnostní řešení, což bohužel stále nebývá běžné, a dokonce má i dedikovaného zaměstnance, který se o to řešení stará, což už vůbec nebývá běžné, na tohoto člověka denně vyskočí desítky až stovky poplachů, upozornění a událostí, na které by měl nějak reagovat. Jenže den má pouze 24 hodin, ten člověk někdy potřebuje spát, občas také onemocní nebo chce jet na dovolenou. Proto jsem spíše pesimista, co se týče budoucnosti, protože zaprvé vidím, kolik firem ani dnes žádné bezpečnostní řešení nepoužívá, a zadruhé mě děsí, jaké obrovské množství práce a hlavně kvalifikovaných lidí by bylo zapotřebí, abychom se plošně dostali na nějaký uspokojivý standard."

„Pánové mají naprostou pravdu a já přemýšlím, co k tomu dodat," usmívá se **Karel Klumpner** (Comguard). „Snad jenom to, že pokud přesvědčíte ty nahoře, vznikne tím prostor pro vzdělání těch dole – tolik k osvětě a na koho s ní primárně cílit. Co se týče přehlcení informacemi, jež vyskakují na zaměstnance ze všech systémů, které jim prodáváme, tak si to samozřejmě uvědomujeme. Možným řešením jsou služby, jako je třeba náš ThreatGuard, které tyto informace analyzují a filtrují, aby se k uživateli dostalo jen to skutečně důležité. Ostatně na tomhle principu už funguje celá škála řešení, jako jsou SIEM, vulnerability management, incident response management a podobné. Myslím si, že automatizace může přinejmenším zčásti vyřešit nedostatek kvalifikovaných lidí."

„Mně se moc líbí vaše poznámka o přesvědčování těch nahoře," reaguje **Filip Navrátil** (Eset). „Často se mluví o edukaci zaměstnanců, což je samo o sobě dobrá myšlenka, jenže podle našich průzkumů se v oblasti bezpečnosti školí pouze ve třetině firem a často navíc až v reakci na nějaký incident. Přesvědčení managementu mi proto přijde jako efektivnější cesta, zejména když vedení firem, a nejen těch malých, často stále vnímají bezpečnost jako nějaké nutné zlo, což se pak odráží na objemu prostředků, které jsou na ni uvolňovány. Navíc se obávám, že mnoho firem má pocit, že si jejich IT oddělení zvládne poradit úplně se vším, což už ale v dnešní době při počtu a složitosti různých systémů není možné. Souhlasím, že partneři by měli hrát edukativní roli, ale jejich hlavní úlohou by mělo být dodávání bezpečnostních řešení a jejich následná správa. V ideálním světě by to vypadalo tak, že si firemní IT ředitelé přiznají, že potřebují pomoc zvenčí, a partneři budou dělat všechno pro to, aby jim tu pomoc dokázali poskytnout. Protože upřímně, dodat řešení zvládne skoro každý, ale spravovat ho, být schopný zákazníkovi poradit a ukázat mu, co dělá špatně, to už vyžaduje snahu. A myslím, že kolegové budou souhlasit, že klienti přesně tohle potřebují."

„Naprosto souhlasím," přikyvuje **Jan Dobrý** (Anect). „Přesně to, co jste popsal, u zákazníků děláme, vzletně to nazýváme security analýzou, ale často musíme začít úplně základním zmapováním klientova prostředí a analýzou rizik, protože to nikdo předtím neudělal. Typickým příkladem je start-up, kterému rychle vyroste byznys, nabere nové zaměstnance, ale po bezpečnostní stránce se zasekne úplně na začátku, takže tam přijdete a okamžitě vidíte desítky problémů. U takového zákazníka si musíte promluvit s IT ředitelem a nasměrovat ho, ukázat mu věci, jež musí vyřešit okamžitě, a nachystat mu roadmapu pro vyřešení těch méně akutních záležitostí, se kterou pak může jít za vedením, protože může trvat dlouhé měsíce, dokonce i několik let, než se daná firma dostane z hlediska bezpečnosti do nějakého přijatelného stavu. Bývá me i mile překvapeni, a to když potkáme zákazníka, který má nějaké povědomí a dá se s ním hovořit o službách a řešeních na vrcholku bezpečnostní pyramidy. Stále přitom narážíme na firmy, které potřebují pomoci s úplnými základy."

„Naše zkušenost s povědomím zákazníků je velmi podobná tomu, co říkal pan Dobrý, a stejně tak souhlasím s tím, že občas najdete někoho, kdo vás překvapí," přidává se **Martin Lohnert** (Soitron). „Dokonce bych řekl, že stačí, když se ve firmě najde alespoň jeden člověk, který si uvědomí význam bezpečnosti a vezme si to téma za své a začne ho stavět do popředí. Čím výše stojí v hierarchii, tím samozřejmě lépe, ale obecně platí, že přítomnost takového člověka ve firmě může udělat obrovský



Martin Lohnert
ředitel centra Void SOC, Soitron

„Nedokážu si představit jinou cestu poskytování bezpečnosti než přes služby, outsourcing a technologie. Kdybychom chtěli dosáhnout uspokojivého zabezpečení firem postaru, potřebovali bychom tisíce specializovaných odborníků, kteří jednoduše neexistují."

Vladimír Mlynárčik
country manager CZ/SK, Clico

„Pandemie nestvořila žádný z trendů, o kterých se dnes hovoří, pouze je urychlila a přenesla do popředí zájmu. Pojďme je s ní proto tolik nespojovat a berme je jako validní obchodní a technologické otázky, které budou velmi důležité i poté, co pandemie opadne."

rozdíl. Na zavedení základních pravidel přece nepotřebujete žádný astronomický budget, spousta informací je dostupná on-line a zdarma, stačí jen, když se o to někdo začne zajímat, vezme to do rukou a začne to prosazovat. To je dobrý začátek."

Karel Klumpner (Comguard), dodává: „Pánové mají naprostou pravdu a samozřejmě je ideální, když se takto osvícený člověk najde v nejvyšším vedení. Nicméně pokud máte demotivované nebo špatně placené zaměstnance, tak se vám na nějaké zásady bezpečnosti stejně vykašlou, tam je to marné. Pak máte také společnosti, kde se vedení střídá jako na běžícím páse, a naopak se vyplatí udržovat dobré vztahy s lidmi z provozu, protože oni jsou ti, kdo se tam zuby nehty snaží udržet nějaké standardy. Zkrátka musíme být šikovní a posuzovat jednotlivé zákazníky individuálně."

„Já jen doplním krátkou anekdotu," říká **Martin Lohnert** (Soitron). „Byl to rozhovor s majitelem středně velké průmyslové firmy, který prohlásil, cituji: ‚Kybernetická bezpečnost? O tom jsem ještě nikdy neuvažoval.' A teď si představte, že se ho někdo, ať už to budou jeho podřízení, nebo externí partner, snaží přesvědčit o tom, že je nutné investovat peníze a dělat ve firmě nějaké změny."

„Ale není to pro něj vlastně krásně osvobozující?" směje se **Filip Navrátil** (Eset). „Já jsem teď nedávno měl možnost mluvit s kolegou z velké globální společnosti se stovkami tisíc klientů. Ta firma provozuje vlastní SoC, její IT oddělení je větší než lecjaká firma tady na našem trhu, ale přesto jsou smířeni s tím, že venku existují hackerské skupiny, kterým by neodolali, a že jim to maximálně mohou udělat co nejtěžší. No a na opačném konci spektra je ten průmyslník, který o nějaké bezpečnosti v životě neuvažoval a určitě má z těch dvou klidnější spánek. Alespoň dokud se něco nestane. Přesně takovým musíme otevírat oči. Oni si vůbec neuvědomují, na jak tenkém ledě bruslí."

„Jenže takového majitele přesvědčíte jen velmi těžko," navazuje **Jan Dobrý** (Anect). „Jestli v životě nepřemýšlel o bezpečnosti a jeho firma zatím nečelila žádnému útoku, tak své podřízené odbude s tím, že doteď přece všechno fungovalo, tak proč po něm chtějí peníze na nějaké zbytečnosti. O něco vyšší šance je, když mu dáte zmíněnou bezpečnostní analýzu z pozice externího partnera. I tak to bude ale řada majitelů pořád vnímat tak, že se z nich snažíte vytáhnout pouze peníze za nic. Zkrátka je potřeba mít správné lidi na správném místě."

„Pánové, v tom případě je asi čas na oblíbené téma, kolik velkých kybernetických útoků ještě potřebujeme na to, aby podobní lidé prozřeli," nadhazuje **Martin Lohnert** (Soitron).

„My jsme v loňském roce několik velkých útoků řešili a můj dojem je bohužel takový, že to nikoho příliš nevystrašilo," odpovídá **Vladimír Mlynárčik** (Clico). „Pomáhali jsme například řešit následky útoku na fakultní nemocnici v Brně a mluvili jsme o tom při jednání se dvěma velkými nemocnicemi na Slovensku. Oni si nás pozorně vyslechli, v principu souhlasili, že máme pravdu… a to bylo všechno. Slovenský partner mě pravidelně informuje, jestli se něco změnilo, a ty nemocnice nedělají vůbec nic. Občas slýchám názory, abychom zákazníky strašili napřímo, udělali na ně malý útok a něco jim shodili, ale tak to nefunguje. Co podle mého názoru naopak funguje, je ukázat klientovi věci, které se v jeho síti dějí dnes a denně, aniž o tom ví. Každý druhý vendor vám dnes zdarma nabídne nějaký nástroj na monitorování sítí, který pak můžete nasadit u zákazníka a říct mu: ‚Podívej, tady se ti do sítě připojili boti z Kazachstánu, tady další odněkud z Ameriky. Víš, co tam dělají? Chceš je tam?' Takto mu můžete pomalu a trpělivě otevírat oči, dokud nepochopí, že je exponovaný."

„Co se týče velkých útoků, které by přesvědčily firmy k investicím do bezpečnosti, s dovolením budu citovat Aleše Špidlu, který prohlásil, že zatím je to pořád příliš malý průšvih. Akorát tehdy použil trochu jadrnější výraz," směje se **Karel Klumpner** (Comguard). „Ale abychom nebyli pouze pesimističtí, mám pocit, že firmy, které už prozřely, v poslední době přemýšlejí o bezpečnosti hlouběji a systematičtěji než dříve. Ty, které zatím neprozřely, musíme dál donekonečna přesvědčovat."

„Útoky nám podle mě samy o sobě nepomohou, nicméně se budou dít dál, takže budeme připisovat nová data a jména na

Filip Navrátil
obchodní ředitel, Eset

„V ideálním světě by to vypadalo tak, že si IT ředitelé přiznají, že potřebují pomoc zvenčí, a partneři budou dělat všechno pro to, aby jim tu pomoc dokázali poskytnout. Dodat řešení zvládne skoro každý, ale spravovat ho a poskytovat konzultace, to už vyžaduje snahu."

seznamy napadených firem," uzavírá **Jan Dobrý** (Anect). „Pokud něco fungovat může, tak je to hledat ve firmách osvícené lidi, o kterých mluvil pan Lohnert, a z pozice partnera jim co nejvíce pomáhat. Model, kde je firma ochotná naslouchat partnerovi a partner je schopný poradit firmě, je podle mě základem dobře fungujícího zabezpečení."

Cloud, služby a MSP

„Obchodní modely postavené na službách jsou podle nás jednoznačnou budoucností," otevírá nové téma **Filip Navrátil** (Eset). „Adopce na českém trhu ještě není taková, jako na západ od nás, ale dříve nebo později se to stane mainstreamem, což jako vendor podporujeme, protože model služeb je podle nás prospěšný pro všechny zúčastněné. Jedním z důvodů, proč adopce zatím pokulhává, je poměrně složitý proces přechodu na nový model, ani ne tak na straně zákazníků jako spíše u partnerů. Jakmile ovšem budou mít ten přechod za sebou, bude pro ně podstatně jednodušší poskytovat zákazníkům vlastní přidanou hodnotu, zatímco klienti budou moci čerpat služby přesně podle své potřeby, bez nutnosti budovat a spravovat vlastní infrastrukturu a samotné řešení. To je podle mě neoddiskutovatelně lepší uspořádání než u tradičního modelu."

„Adopce nových technologií a trendů na našich trzích je přibližně o čtyři nebo pět let pozadu oproti Západu, ale tyto modely sem určitě přijdou, a pokud na to připravíte své partnery a investory, budete za hrdinu," směje se **Vladimír Mlynárčik** (Clico). „Teď budu sice hovořit pouze na příkladu vendorů z našeho portfolia, nicméně jsem přesvědčený, že ten trend je obecný. Zaprvé se do popředí zájmu dostává cloud security, tedy zabezpečení dat, aplikací a platforem, které zákazník ukládá nebo provozuje v cloudu, zadruhé jsme dosáhli enormního úspěchu s nabídkou EDR platformy jednoho z našich vendorů formou řízené služby. Znovu zdůrazňuji, že to vidím pouze z pohledu úzké výseče našich vendorů, nicméně pokud se hovoří o růstu cloudu a MPS modelů, říkám, že u nás se to děje také."

„A u nás také," navazuje s úsměvem **Karel Klumpner** (Comguard). „Ty trendy jsou velmi zřetelné, a jestli se mohu pochlubit, koncem loňského roku jsme ve spolupráci s partnerem a vendorem realizovali unikátní projekt, který zastřešuje security pro zákazníkovo cloudové a on-premise prostředí s jednotnou bezpečnostní politikou, je v tom zahrnuto EDR, sandboxing a další pokročilé technologie, pokrývá to šest tisíc uživatelů, a navíc jsme to celé zvládli integrovat za měsíc a půl, na což jsem obzvlášť hrdý. Zmiňuji to ale i proto, že jde o práci s hybridním prostředím, což je velké téma v podnikovém IT obecně a mělo by to být tématem i pro nás."

„Berte mě prosím s rezervou, protože jsem v tomhle ohledu velmi zaujatý, ale nedokážu si představit jinou cestu poskytování bezpečnosti než přes služby, outsourcing a sofistikované technologie," pokračuje **Martin Lohnert** (Soitron). „Kdybychom

PROGNÓZA

Dědictví pandemie a výhled pro letošní rok

„Pandemie přinesla extrémně rychlé nasazování nových technologií, které neprošlo standardními procesy, čímž vznikla celá škála bezpečnostních rizik," říká **Martin Lohnert** (Soitron). „V té době to bylo pochopitelné a řada firem to zřejmě brala jako provizorní řešení, dokud se nevrátí do běžného režimu, jenže ta situace trvá už více než rok a z dočasného provizoria se de facto stala nová norma. Proto je nejvyšší čas to začít konsolidovat."

„Mnoho firem to na počátku výrazně podcenilo a ještě dnes to dohánějí," přitakává **Jan Dobrý** (Anect). „Teď se postupně smiřujeme s tím, že budeme i nadále fungovat on-line, takže očekávám výraznou akceleraci témat, jako je zabezpečení konektivity a vzdáleného přístupu, zabezpečení aplikací a koncových bodů, nasazování EDR platforem, zkrátka všeho, co souvisí s tou náhlou proměnou obchodních modelů a modelů práce."

„Pojďme letos méně hovořit o pandemii a více o samotných tématech," navrhuje **Vladimír Mlynárčik** (Clico). „Pandemie žádný z těch trendů, o kterých jsme dnes hovořili, nestvořila, ona je pouze urychlila a přenesla do popředí zájmu. Pojďme je s ní proto tolik nespojovat a berme je jako validní obchodní a technologické otázky, které budou velmi důležité i poté, co pandemie opadne. A je na nás, abychom je takto prezentovali klientům, věcně a profesionálně."

„Zkusím doplnit konkrétní trendy, které jsou, případně velmi brzy budou, aktuální," říká **Karel Klumpner** (Comguard). „V první řadě je to zabezpečení cloudu a jednotná bezpečnostní politika pro hybridní prostředí, dále pak svatá trojice SIEM, SOC, SOAR, technologie typu XDR a EDR, správa identit a přístupů PIM/PAM, ochrana DNS, aplikační firewally a nakonec úplná novinka v podobě endpoint configuration security. Těmto kategoriím řešení doporučuji letos věnovat pozornost."

„Pandemie zamíchala pravidly hry na všech úrovních a některé věci se už prostě nevrátí tam, kde byly předtím," soudí **Filip Navrátil** (Eset). „Pokud například firma poslala zaměstnance na home office, už je nikdy nepřinutí, aby zase seděli pět dní v týdnu v kanceláři. Souhlasím s kolegy, že tady za poslední rok vznikla ztráta, kterou firmy musejí dohnat, a to nejen z bezpečnostního hlediska, ale v celkové koncepční rovině. Letos se posuneme od řešení, jestli ty věci vůbec fungují, k tomu, zda jsou správně implementované a plně využíváme jejich potenciál."

chtěli dosáhnout uspokojivého zabezpečení firem postaru, potřebovali bychom na to tisíce, ne-li desetitisíce specializovaných odborníků, kteří jednoduše neexistují. Soitron působí celkem v sedmi zemích a akutní nedostatek specialistů, který známe z našich trhů, panuje úplně všude. Jinými slovy, kdyby se firmy zítra rozhodly nakoupit a provozovat svá vlastní bezpečnostní řešení, nesehnaly by nikoho, kdo by se jim o ně staral, a navíc by to celé bylo strašně neefektivní."

„Se vším souhlasím a obzvlášť bych podtrhl ten poslední bod," říká **Jan Dobrý** (Anect). „Obrovská výhoda řízených služeb je v tom, že je můžete replikovat. Pokud jste dříve vyvíjeli jedno řešení pro jednoho klienta, nyní můžete totéž řešení nabídnout v podstatě libovolnému počtu zákazníků formou služby a všechno spravovat centrálně přes jednu konzoli. Další nespornou výhodou je flexibilita a možnost tu službu škálovat podle toho, jak vaši klienti rostou, například z hlediska potřebného výkonu nebo počtu licencí. Pak je tu již zmíněná příležitost pro poskytování přidané hodnoty, protože zákazník si tu službu sám nenainstaluje, ale hlavně si sám nevyhodnotí, co vlastně potřebuje. V neposlední řadě pak službám pomáhá, že v nich vendoři vidí budoucnost a podporují je."

„Ještě mě napadla jedna věc, která platí vlastně pro nás všechny," dodává **Filip Navrátil** (Eset). „Naším společným úkolem je naučit zákazníky správně počítat TCO, aby se nestávalo, že se podívají na poplatky za službu, srovnají to s pořizovacími náklady on-premise řešení a řeknou, že tu službu nechtějí, protože je moc drahá. Ona tak totiž působí jenom do chvíle, kdy na druhé strašně započítáte méně patrné náklady, jako jsou čas a práce zaměstnanců, provoz a údržba infrastruktury a podobně. Když se to spočítá skutečně poctivě, služba najednou stojí podobně, ne-li dokonce méně než on-premise varianta. A nutno připomenout, že oproti on-premise řešení získá zákazník kromě samotných technologií i kvalifikovanou pracovní sílu a cenné know-how, tedy to, čeho je na trhu obecně málo."

Vztahy v řetězci

„Všichni se vyvíjíme společně – technologie, zákazníci, vendoři, distributoři i my partneři," otevírá nové téma **Martin Lohnert** (Soitron). „Security je natolik komplexní odvětví, že se navzájem potřebujeme a nemůžeme si dovolit nespolupracovat napříč celým řetězcem. Zároveň platí, že tempo a směr naší práce udává trh. Kdybychom si společně s vendory a distributory vymysleli něco, co by zákazníkům nedávalo smysl, tak nás s tím vyženou. Tyto dvě věci, tedy nutnost úzké spolupráce a nutnost naslouchat trhu, v zásadě zaručují, že se celé odvětví pohybuje správným směrem."

„Jako partner jste první na ráně," navazuje s úsměvem **Jan Dobrý** (Anect). „I když s vámi vendor nebo distributor spolupracuje v pre-sales fázi projektu, v konečném důsledku je na vás, abyste zákazníkovi dodali vše, co jste mu slíbili. Vendoři a distributoři si ovšem tuhle skutečnost uvědomují a systém vzájemné spolupráce a podpory je nastavený velmi dobře. Jediné, co by se v ideálním případě mohlo zlepšit, je rychlost reakce, ale to je zkrátka dáno tím, že teď všichni máme hodně práce."

„Já bych to shrnul tak, že jak dobrý je tým, tak dobré jsou výsledky," říká **Karel Klumpner** (Comguard). „Pokud spolupráce na ose vendor–distributor–partner probíhá hladce, je to radost a dokážete společně dělat skvělé věci. Když to ale někde začne skřípat, okamžitě se vám to projeví v číslech. K úspěchu se dostanete kombinací kvalitní technologie, kvalitní spolupráce a také vzájemné důvěry všech zúčastněných, takže plně souhlasím s panem Lohnertem, že pokud chceme kráčet kupředu, tak jedině společně."

„Naprosto souhlasím s kolegy a ke kvalitě spolupráce v rámci řetězce dodám ještě jeden rozměr, a sice že vendoři konečně začali vnímat potřeby jednotlivých trhů," doplňuje **Vladimír Mlynárčik** (Clico). „V channelu působím přes dvacet let, pracoval jsem i u vendora a vzpomínám si, jak se sem přesazovaly strategie z úplně jiných regionů, bez jakéhokoliv ohledu na lokální specifika. To se teď mění, přinejmenším část vendorů se pustila do segmentace trhů a já to vnímám jako obrovské pozitivum. Když totiž jako vendor přijdete s nabídkou, která má hlavu a patu a bere ohledy na velikost lokálních zákazníků, na jejich potřeby, problémy a preference, partneři budou mnohem ochotnější si vás vyslechnout. Další pozitivní trend vidím v rostoucím zájmu partnerů o placené vzdělávání. Pro většinu vendorů v našem portfoliu fungujeme jako školicí středisko a poptávka je až překvapující."

„Ono záleží i na velikosti vendora," navazuje **Jan Dobrý** (Anect). „Menší lokální vendor, který je z našeho regionu, zná českého nebo slovenského zákazníka perfektně. Z toho úhlu pohledu je pak komunikace jednodušší. U obřích globálních hráčů mám pocit, že logicky potřebují více argumentů od více partnerů a dostatečný čas."

„Ona ale existuje i druhá cesta," upozorňuje **Martin Lohnert** (Soitron). „Pokud vendor nemůže nebo nechce uzpůsobovat své produktové portfolio lokálním podmínkám, může alespoň umožnit, aby to za něj udělal někdo jiný, ať už hovoříme o jazykové lokalizaci nebo o přidání nějaké specifické vlastnosti vyplývající, dejme tomu, z místní legislativy. Pokud má vendor pocit, že se mu to nevyplatí, může se toho ujmout někdo z místních hráčů a bude to jeho přidaná hodnota."

„My jsme vendor, který vyrostl na česko-slovenském trhu, takže nevím, co bych dodal," usmívá se **Filip Navrátil** (Eset). „Česko je pro Eset v podstatě domácí trh, naše pobočka tu funguje dvacet let a já to beru jako obrovskou výhodu, protože tu máme své lidi, jsme nablízko všem našim partnerům a oni nám díky tomu zachovávají věrnost. To je totiž věc, která řadě vendorů uniká – když se o partnera staráte, reagujete na jeho podněty a věnujete mu pozornost a pomáháte mu s jeho zákazníky, nemá žádný důvod se poohlížet po jiné značce – za předpokladu, jsou vaše produkty kvalitní, samozřejmě. Naproti tomu partner, který má pocit, že je vendorovi úplně ukradený, při první příležitosti odejde někam za lepším." ●

Připravil Matěj Čuchna

Partnery tohoto kulatého stolu byly společnosti Anect a Eset.