TD SYNNEX

Exkluzivní rozhovor s novou generální ředitelkou CISCO ČR

Už nejsme jen lídři networkingu, máme také hattrick v bezpečnosti

Zuzana Švecová je od začátku září generální ředitelkou CISCO ČR. A jak je v jednom ohni, moc rozhovorů ještě dát nestihla. O to více si považujeme toho, že si našla hodinu na povídání pro portál TD SYNNEX. Ještě než se otevřou dveře výtahu v pátém patře pankrácké budovy Parkview, kde české CISCO sídlí, říkáme si: Snad to nebude příliš opatrné, plné oficiálních frází. Ale pak nás nová žena v čele české pobočky špičkové IT korporace odzbrojí úsměvem a bezprostředností. V průběhu rozhovoru pak jasnými názory, odžitými zkušenostmi, nepředstíraným vztahem ke značce a tahem na bránu. Po hodině perfektně rozumíme, proč právě ona dostala důvěru vést CISCO do turbulentních let, kdy se dlouholetý lídr v networkingu chce stát absolutní špičkou také v celé oblasti IT infrastruktury, zpracování dat, umělé inteligence nebo kyberbezpečnosti.

Od časů, kdy byly nejviditelnějším symbolem CISCO pevné linky na stolech kanceláří, už uplynul nějaký čas. Co je CISCO dnes?

Prošli jsme si různými etapami. Od roku 1984, kdy jsme byli založeni, jsme uvedli na trh ledasco. Například první router, který umožnil dvěma počítačům mezi sebou komunikovat, což byl jeden ze základních předpokladů pro budoucí rozšíření internetu. Pak tyto slavné IP telefony, bezpečnostní brány, switche, wi-fi. Posledních patnáct let je klíčovým hybatelem veškerých našich produktů a řešení bezpečnost. Jsme bezpečnostní firma spojená s networkingem. Naše zařízení zastřešují datovou komunikaci mezi jednotlivými počítači, servery, datovými centry a cloudy, takže je logické stavět na nich také zabezpečení. Pustit se do toho bylo správné rozhodnutí, protože dnes je bezpečnost kritérium číslo jedna, aby firmy mohly pracovat se svými daty, komunikovat s uživateli i zákazníky a bez obav se věnovat svému podnikání. Bereme na sebe odpovědnost za výstavbu sítě, definování pravidel pro uživatele, pro jednotlivá zařízení a celkový dohled nad toky dat.

Dříve se produkty prodávaly jako „kusy“, dnes se v zásadě celý vendorský svět snaží své služby prodat v rámci „as a service“ s těžko odlišitelnou hranicí software, hardware a lidské péče či servisu. Jak to máte vy?

Trend v celém odvětví je nepopiratelný. Dnes je alfou a omegou inovací software. Ten podporuje veškeré změny, které ve firmách či institucích probíhají. U nás to není jinak. Uzavřeli jsme historicky první rok, kdy většinu našeho obratu tvoří software, což je výrazný posun oproti původně „hardwarové“ společnosti. Zároveň si ale uvědomujeme, že musíme zůstat srozumitelní všem typům zákazníků. Proto jsme například pro oblast bezpečnosti vytvořili jednotlivé balíčky produktů pro ochranu koncových zařízení a uživatelů, které je možné pořídit jednotlivě. Jsou však připraveny tak, že ve chvíli, kdy byste uvažovali o koupi dvou, už se vám vyplatí komplexní bezpečnostní sada, která obsahuje sedm produktů. Na trhu musíme konkurovat nejen kvalitou produktů nebo služeb, ale také cenou, zákaznickou péčí a srozumitelností.

Co v oblasti kyberbezpečnosti dnes nabízíte?

Vzali jsme si sedm oblastí a pro každou z nich máme konkrétní řešení. Hlavně ale vytváříme platformu, tedy prostředí, ve kterém nejrůznější nástroje pomáhají automatizovat, zjednodušovat, definovat dohled, bezpečně využívat AI a data. Především však reagujeme na společenské změny, na které technologie reagují.

Můžete být konkrétnější?

Dříve se řešila bezpečnost koncového uživatele a jeho jednotlivého počítače, ale dnes už nežijeme tak jednoduše. Když uživatel přichází do kontaktu se sítí, využívá nejen firemní notebook, ale také telefon. Ten je jeho vlastní, který využívá i mimo pracovní sféru. Potřebuje se dostat k firemním aplikacím, které jsou ve firemním datovém centru a on do něj přistupuje. Proto, když dnes řeším ochranu uživatele, musíme řešit řadu navazujících věcí a dělat to komplexně. Je to tedy komplex různých bezpečnostních řešení a je lepší je využít v jedné platformě a mít naplánované všechny scénáře a akce.
I proto, že málokdo má v praxi čas si vybírat, kterou nuanci toho celého systému potřebuje pro ten který konkrétní případ. Náš byznys model jde dvěma směry.
Software znamená inovaci. A platformizace umožňuje ochranu.

Co je vůbec největší kyberbezpečnostní nedostatek dnešních firem?

Nejspíš budu trochu kontroverzní, ale řeknu to tak, jak situaci cítím. Mnoho organizací podceňuje riziko do chvíle, než se problém stane u nich. Nabízí se příměr s konfliktem na Ukrajině. Neustále jsme podceňovali výdaje na obranu a ve chvíli, kdy se válka objeví u sousedů, se rázem probudíme a začneme všechno horečnatě dohánět. Proto je velice důležitá legislativa typu NIS2, která pomáhá, aby se z trendu stal standard. My sami jsme v tom zapojeni ve dvou ohledech. Úzce spolupracujeme s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), který logicky v posledních měsících rychle roste. A za druhé, jsme aktivní v rámci iniciativy NIS2READY, jež sdružuje firmy, které proaktivně připravují firmy na to, aby se propojila legislativa s realitou.

S tím ale souvisí, odkud kyberbezpečnostní policy začít. Přece jen, firma má obvykle mnoho různých řešení a často neví, co jsou priority…

Klíčovým zdrojem rizika pro firmy je stále uživatel. Právě on je největší bezpečnostní hrozbou. Hackeři a útočníci prahnou po jeho identitě a pokouší se do systému dostat skrze ni. Je to přece jen jednodušší než se tam prokousávat skrze všechna další bezpečnostní opatření. Ochrana identity je proto priorita číslo jedna. Vedle toho narůstá ransomware, ale i skryté plíživé útoky na bezpečnostní architekturu. Často se dlouhé měsíce nebo i několik let pohybuje ve vašem systému cizí element, který čeká na příležitosti, aby vám vzal data. Výsledky bývají často fatální a vedou často až k úplné paralýze firem. My máme velkou konkurenční výhodu v centru Cisco Talos, které sídlí v Krakově a neustále vyhodnocuje globální útoky a chrání všechna Cisco řešení. Pro představu, denně jich je 800 miliard. Talos je také hlavním centrem, které pomáhá kyberbezpečnosti na Ukrajině.

Lze takovou informaci zveřejnit?

Ano, jsme na naši podporu Ukrajině hrdí. My logicky, protože máme tento konflikt kousek za hranicemi. Ale je to priorita i pro naše globální vedení. Náš CEO Chuck Robbins tu byl letos v červenci, a právě o toto téma se zajímal přednostně.

Na trhu je velký nedostatek IT security specialistů. I to může být úzké místo celého systému, protože technologie potřebují lidi s know-how a znalé potenciálních rizik i aktuálních řešení?

Úzkou spolupráci s NÚKIB už jsem zmiňovala. Ale děláme toho v České republice opravdu hodně. Máme vlastní program Networking Academy, jehož součástí je také kyberbezpečnost a dnes je o ni dokonce větší zájem než o tradiční networking. Snažíme se edukovat na vysokých, ale často i středních školách, protože tam zároveň hledáme také mozky, které to posunou dál. Letos jsem se zúčastnila projektu Kyber cena roku, kde se oceňují zajímavé bezpečnostní projekty nebo individuální odborníci v oboru, kteří školí trh, státní správu i veřejnost. Významnou roli v tom hrají právě střední školy, které mají vlastní školicí kurzy pro bezpečnost. Hodně nám také pomáhá, že v Praze na Karlově náměstí máme vlastní R&D centrum. Sto padesát špičkových vývojářů, kteří dělají na globálních řešeních a mají mimořádnou expertízu v oblasti bezpečnosti nebo umělé inteligence. To nám může pomoci i obchodně, protože máme vlastní odborníky, kteří mohou proškolit trh v češtině. Dlouhodobě máme Tech Club webináře, kde celé téma „polidšťujeme“ pro širší veřejnost. Hodně se snažíme, aby to nebyla jen suchá prezentace, ale aby to byla i zábava s praktickými ukázkami.

Jak se v produktové road mapě projeví akvizice Splunku?

Bezesporu výrazně. Získali jsme k sobě dlouhodobého lídra SIEM a zároveň datovou platformu, jejíž principy můžeme integrovat do všech částí našeho portfolia. Do networkingu, security, dohledu nad celou sítí i částmi IT. Bezprostředně po akvizici jsme spojili vývojové týmy a ty jedou na plné obrátky.

Na co dalšího se od Cisco těšit v příštích měsících?

Jedním z hlavních oznámení, které jsme už udělali, je Cisco HyperShield. Ten přichází s úplně novou architekturou distribuovaného firewallingu na bázi AI, jež zapadá do všech částí sítě od uživatele až do datového centra. S pomocí AI jsou tam mechanismy, které dokážou identifikovat hrozby na všech možných úrovních. Protože, co je vlastně firewall? Centrální místo, přes které jde veškerý provoz v síti. Ale firewall v podobě jednoho centrální bodu jednak může zpomalovat celý provoz, jednak už neodpovídá dnešní složitější komplexnější komunikaci mezi uživateli, datovým centrem a cloudem a zároveň nestačí odchytávat všechno. Proto musí dojít ke změně architektury.
Mimořádně pyšná jsem také na náš „securitní hattrick“.

Securitní hattrick?

Je to velký majstrštyk našich vývojářů. Ve Forrester Reportu jsme jediní, kdo má ve třech kvadrantech vedoucí postavení v oblasti bezpečnosti. Jsme lídři v segmentaci sítě, tradičním firewallingu i OT bezpečnosti. Tedy specifické bezpečnosti v oblasti výrobního prostředí či jiném prostředí, které se netýká tradičních kanceláří.

V čem je vlastně v řetězci důležitá role IT distributora?

Role kvalitního distributora je nenahraditelná, protože zná nejlepší cesty na trh. I přesto, že Cisco má v České republice opravdu velký tým lidí, stále jsou naše kapacity omezené na to, kolik zákazníků máme. Bez distributorů není možné škálovat. Proto je pro nás distributor první partner v celém řetězci, a až na něj navazují partnerské firmy. Máme v ČR 264 dedikovaných partnerských firem, jsou větší a menší; a nemáme šanci je všechny obsloužit interně na denní bázi. Pro mě je distributor konkrétní člověk nebo firma, kterou partneři znají, mají s ní silný vztah, mají komu zavolat, komu se ozvat. Zároveň mají špičkové znalosti, které dokážou distribuovat na trh. Extrémně se mi líbí například projekt „sekuritní triáda“, který jsme rozjeli s TD SYNNEX. A konečně, distributor je pro mě reputační bod. Je vizitkou pro naše partnery. On rozhoduje, jak bude reference nebo obchodní případ vypadat.

Jak se vám spolupracuje s TD SYNNEX?

S českým týmem se mi spolupracuje výborně. Za poslední roky se ten tým zněkolikanásobil a to je příkladem toho, že je spolupráce úspěšná a zároveň se kompetence rozšiřují. Je tam kombinace hladu po byznysu, expertízy a dostatečného počtu lidí, kteří dokážou obsluhovat stále víc zákazníků a partnerů.

Na závěr mi dovolte ještě dvě osobnější otázky. Jaké je být v čele takto velké firmy?

Jsem ve firmě 11 let a už nějaký čas se pohybuju v řídících funkcích. Ale dokud si skutečně nesednete do křesla generálního ředitele, nejste schopni ten kolotoč zažít. Určitě nebudu říkat, že se nudím. Ale vycházím ze síly týmu. A ten je veliký, jsou to profesionálové a hodně inteligentní lidé. To, že já zastávám nějakou funkci, je jen malá část našeho celkové snažení. Ale společně děláme na věcech a řešeních, je to radost. A to je pro mě i důvod, proč jsem ochotná to celé podstupovat. Značka je pro mě také nekonečným zdrojem inspirace, protože se neustále mění řešení a vidím za námi výsledky, kdy firmy nebo instituce přijdou s tím, že díky nám skutečně zautomatizovaly, zefektivnily, zabezpečily svoje prostředí. Samozřejmě, musím svoji roli vyvažovat také se svojí rodinou, která vždy bude mojí prioritou. Ale věděla jsem do čeho jdu a že tomu musím věnovat kus sebe, a velkou porci času a energie.

A úplně poslední: Vzpomenete si na vůbec první den ve firmě a ten pocit, když jste do Cisco přicházela?

Vzpomínám si, že jsem si šla před nástupem do práce koupit boty s podpatky v domnění, že se to v práci sluší a patří. A kolega Martin Doležel se mě zeptal: „Co to máš na těch nohách?“ Od té doby jsem podpatky nenosila, protože interní IT prostředí je hodně uvolněné. Spíš je potřebuji až teď. Přišla jsem z ekonomického světa do týmu mladých lidí, a hned od začátku začala intenzivní vlna školení. Na začátku jsem se párkrát sama sebe ptala, jestli to je svět, který chci vzít za svůj. Ale ten rytmus a nepřetržitá inovace je skvělá, každý měsíc musíte něco změnit a něco nového se naučit. A stále tu platí, že pokud máte hlad a odhodlání, můžete tu zažít zajímavé pracovní výzvy. Jako je teď ta má.

Máte zájem o více informací k Cisco produktům a řešením?
Kontaktujte náš TD SYNNEX Cisco tým: cisco.cz@tdsynnex.com