TRENDY PRO POSKYTOVATELE ŘÍZENÝCH SLUŽEB V ROCE 2025

Stále více podniků se obrací na poskytovatele řízených IT služeb (MSP), ať z důvodu chybějícího IT personálu, vysokých nákladů na vlastní IT, či rostoucí komplexnosti IT prostředí a potřeby její ochrany.

Když se podíváme na budoucnost MSP v roce 2025, bude tato specializovaná skupina IT a technických profesionálů pravděpodobně čelit klíčovému období. A to zejména z pohledu rostoucího využívání IT v podnikovém sektoru.

Rychlá digitální transformace a stále složitější očekávání zákazníků budou představovat výzvy i příležitosti. Vzhledem k tomu, že se organizace a firmy potýkají s přísnými standardy kybernetické bezpečnosti spolu s rozvojem IoT a cloudových služeb, musí MSP čelit potřebám zůstat konkurenceschopní ve světě, kde je adaptabilita na nové příležitosti zásadní pro přilákání a udržení zákazníků.

Za klíčové trendy, které budou v roce 2025 utvářet odvětví MSP, lze považovat následující:

Automatizace řízená AI je nový standard

Automatizace řízená umělou inteligencí se stala základním prvkem moderních postupů v oblasti kybernetické bezpečnosti a nastavila průmyslový standard pro prevenci vyvíjejících se hrozeb. AI se používá pro prediktivní údržbu, patch management, hodnocení zranitelnosti a phishingové simulace, automatizuje zpracování dotazů prostřednictvím přednastavených odpovědí, chatbotů a automatických akcí. Je stále více využívána i k monitorování podezřelého chování, a automatizaci reakcí na kybernetické hrozby a prevenci škodlivých akcí.

Implementace principu nulové důvěry (Zero Trust)

Model Zero Trust (nulové důvěry) se začíná prosazovat jako klíčový přístup k za-

FOTO: Acronis, Myr

bezpečení sítí a zásadně mění způsob, jakým organizace řídí přístup uživatelů a chrání zdroje IT. Tradiční modely zabezpečení založené na ochraně perimetru již nestačí k řešení komplexních hrozeb moderních digitálních prostředí a MSP potřebují integrovat principy Zero Trust do svých služeb, aby umožnily robustní a škálovatelná řešení splňující potřeby klientů a regulační požadavky vyžadované předpisy.

Přechod na multicloudová prostředí

Vzhledem k tomu, že zavádění multicloudů je na vzestupu, očekává se, že i v roce 2025 poroste, a většina MSP bude muset spravovat více cloudových prostředí, aby optimalizovala náklady a výkon. Jak se tyto strategie stávají nezbytnými pro moderní IT infrastrukturu, MSP podporují multicloud jako součást svých portfolií služeb a příští rok se již tato podpora stane nezbytností jako kritická součást IT infrastruktury.

Využití integrovaných platforem kybernetické bezpečnosti

Integrované platformy kybernetické bezpečnosti jsou základní součástí moderních strategií, které odrážejí posun v přístupu podniků k bezpečnostní problematice. Spíš než jako samostatná řešení je nyní kybernetická bezpečnost propojena s kontinuitou podnikání a správou koncových bodů. Tento komplexní přístup zajišťuje, že se organizace mohou efektivně bránit hrozbám a udržovat odolnost proti narušením. MSP musí proto nabízet komplexní, integrovaná bezpečnostní řešení, aby fungovali jako klíčový partner při podpoře dlouhodobé odolnosti klientů a kybernetické bezpečnosti na úrovni aktuálních hrozeb.

Ochrana IoT zařízení se stává nezbytností

Kromě standardních koncových bodů musí poskytovatelé MSP počítat se zařízeními internetu věcí (IoT). Technologie IoT zvyšují provozní efektivitu a umožňují inovativní řešení, jsou ale také cílem útočníků, protože je lze využít jako body průniku. Od MSP to vyžaduje implementovat opatření a protokoly pro správu IoT a zabezpečit, aby byla zajištěna ochrana napříč všemi připojenými zařízeními.

Vertikalizace a školení

Konkurence mezi MSP se zintenzivňuje. Před covidovou pandemií většina MSP primárně obsluhovala klienty lokálně, v rámci místní oblasti. Během ní a po covidové éře však i nejmenší MSP začali nabízet služby vzdáleným zákazníkům, a to i mezinárodně. Rozšířený dosah spojený s nárůstem práce na dálku znamená, že MSP musí pro zachování konkurenceschopnosti odlišit své nabídky. Odrazilo se to mj. v silnějším zaměření na průmyslová odvětví založeném na compliance požadavcích a specializovaném softwaru. S tím, jak se nároky na dodržování předpisů stávají složitějšími, MSP často potřebují více specialistů na podporu více odvětví a musí si vybrat konkrétní vertikály, kde mohou nabídnout nejlepší hodnotu. Dosažení lepší konkurenceschopnosti vyžaduje i investice do průběžného školení a rozvoje dovedností, a zajistit, aby zaměstnanci a technici IT byli dobře vybaveni k poskytování specializovaných služeb pro různá průmyslová odvětví a regiony.

CO JE MSP A POJEM ŘÍZENÝCH SLUŽEB?

Řízené služby (Managed services) poskytují nástroje, personál a ověřené odborné znalosti pro komplexní přístup ke správě firemních IT potřeb. Nebo společně řízené IT (Co-managed IT services), kdy poskytovatel řízených služeb (MSP – Managed Services Provider) spolupracuje s interním IT týmem firmy, aby zlepšil správu a podporu její IT infrastruktury.

MSP představují pokročilejší přístup, zaměřený primárně na správu a podporu infrastruktury a provozu IT (včetně údržby, monitorování, kybernetické bezpečnosti apod.) na základě předplatného, pojímaný spíše jako forma dlouhodobého partnerství.

Podpora vzdálené pracovní síly

Posun ke vzdáleným pracovním prostředím a práci pouze na dálku se v podnikové sféře stává standardem. MSP a firemní IT profesionálové musí přizpůsobit své strategie, nástroje i metodiky, aby mohli tento vývoj účinně podpořit a zároveň vyvažovat pohodlí a produktivitu s kybernetickou bezpečností a regulačními požadavky.

„Vše jako služba“

Koncept „Vše jako služba“ (XaaS) se rychle prosazuje v různých sektorech a zásadně mění způsob, jakým podniky využívají technologie a služby. Tento model přesahuje nákup tradičního softwaru a infrastruktury a zahrnuje řadu služeb včetně ukládání dat, kybernetické bezpečnosti, zálohování, aplikací a poradenství. To vyžaduje v tomto ohledu přizpůsobit nabídku předplatného, aby odpovídalo reálné poptávce.

Klíčový význam prediktivní analýzy

Prediktivní analytika je rostoucí trend a očekává se, že v roce 2025 se stane kritickou součástí, protože je zapotřebí využít obrovské množství dat. Díky AI a pokrokům v technologii sběru dat mohou nyní firmy analyzovat historická data v reálném čase a předpovídat budoucí trendy, chování i výsledky. Tento posun zásadně mění rozhodovací procesy napříč různými průmyslovými odvětvími. Stejně důležitou se ale stává ochrana dat používaných při zpracování AI, protože kybernetičtí útočníci mohou manipulovat rozhodnutí řízená AI úpravou dat, na něž se AI spoléhá.

Rostoucí význam energetické účinnosti

Stále důležitější je dostupnost elektrické energie pro datová centra provozující komplexní pracovní zátěž AI, protože energetická účinnost přímo ovlivňuje schopnost provádět složité výpočetní úkoly. Více klientů tak začne hledat řešení pro úsporu energie a pro MSP je to příležitost nabídnout služby, které pomohou zlepšit spotřebu energie v datových centrech optimalizací pracovního zatížení a konzultacemi o udržitelných postupech při řízení provozních nákladů i dopadu na životní prostředí. ■

Štěpán Bínek
Manažer prodeje cloudových řešení Acronis v ZEBRA SYSTEMS