ČESKÉ FIRMY MAJÍ TECHNOLOGICKÝ DLUH,

POMÁHÁME JIM ZVLÁDNOUT HROZBY A VYUŽÍT EFEKTIVNĚ CLOUDOVÉ SLUŽBY

Marek Chmel stojí v čele nového týmu, který v rámci Konica Minolta IT Solutions Czech zavádí u firem cloudové služby a řeší problematiku kyberbezpečnosti. Zeptali jsme se ho, jak jsou na tom v této oblasti české firmy, a zjistili jsme, že zavádění umělé inteligence s sebou nese i určitá úskalí.

Marek Chmel
Cloud & Security Consulting

Foto: Natalie Havelková

Jaké jsou hlavní oblasti, na které se soustředí váš tým v rámci společnosti Konica Minolta IT Solutions Czech?

Náš tým je kompletně nově postavený a je zaměřený především na cloudové služby a bezpečnost. Primárně se specializujeme na cloudové služby od společnosti Microsoft, ale není to nezbytně nutná podmínka. Jsme schopni pracovat i se softwarem od jiných poskytovatelů.

V čem je vaše největší výhoda?

Jsme na trhu, kde všichni hráči cloudové služby znají a věnují se jim. My se od nich odlišujeme v tom, že máme dlouhodobé a velmi hluboké znalosti výrobních systémů, systémů pro řízení financí a ERP systémů. Historicky jsme se na tuto oblast soustředili, takže víme, jak fungují procesy ve velkých firmách. Máme díky tomu také náskok při adopčních a implementačních scénářích. Když realizujeme transformaci stávajících systémů do moderního cloudového prostředí, tak se tyto znalosti a zkušenosti velmi hodí.

Ze zkušenosti vašich projektů - kde vidíte největší slabinu v českých firmách, co se IT oblasti týče?

V mnoha společnostech vidíme především poměrně velký technologický dluh. Digitální transformace je výbornou příležitostí, jak firmy mohou tento dluh odstranit a posunout se mílovými kroky dopředu. Není to jen samotné zvednutí softwaru na novější verze, ale hlavně komplexní transformace všech procesů a jejich přizpůsobení novým možnostem digitálních nástrojů. Díváme se na možné oblasti digitalizace v organizacích tak, aby se daly jejich agendy co nejvíce elektronizovat a automatizovat. Nové možnosti samozřejmě nabízí také umělá inteligence a i na tomto poli jsme schopní pomoci.

Ale zpět k vaší otázce. Co se týče slabin, tak určitě nejslabším článkem v oblasti bezpečnosti je neproškolený zaměstnanec. Na zaměstnance cílí velké množství kybernetických útoků. Nejčastější variantou je phishing jako forma sociálního inženýrství.

Jak přesně fungují?

Útoky mohou mít různé podoby od necíleného masového útoku, který zasahuje obrovské množství uživatelů, až po tzv. sphear-phishing, což je naopak velmi cílený útok na konkrétní zaměstnance. Většinou jde o vrcholové managery, CxO společností apod. Takovému konkrétnímu útoku předchází OSINT analýza, kdy si útočníci shánějí o těchto lidech co nejvíce informací, než na ně zaútočí.

Vy jste schopni v této oblasti firmám pomoci?

My pomáháme firmám s primární obranou v podobě proškolení zaměstnanců, aby se zvýšila jejich odolnost proti těmto formám kyberútoků. Používáme službu Microsoft 365, na který se náš tým specializuje. Využíváme i celou řadu dalších bezpečnostních nástrojů od Microsoftu, jako je Defender nebo Sentinel. Náš tým realizuje kompletní nasazení a konfiguraci těchto systémů a zařízení u klienta. Nabízíme i další podporu zákazníkům, tak aby uměli s těmito systémy pracovat, a pomáháme jim při jejich správě.

O Microsoftu a jeho bezpečnostních programech se dříve pochybovalo, jak je to dnes?

Bezpečnostní nástroje od Microsoftu dnes patří určitě k tomu lepšímu, co je na trhu k dispozici. Netvrdím, že je to nejlepší a nejdokonalejší produkt, ale určitě je pryč doba, kdy měly tyto nástroje nepříliš dobrou pověst. Před patnácti lety to bylo možná oprávněné, ale dnes je Microsoft úplně jinde. Bezpečnost je pro Microsoft obrovsky důležitým pilířem a sama firma říká, že do ní investuje nemalé částky peněz. Security byznys berou nesmírně vážně a neustále rozšiřují a zlepšují své produkty. Síla je v jejich propojení v jedné platformě s kancelářskými a podnikovými aplikacemi a také infrastrukturou.

Jak probíhá vaše spolupráce s firmami konkrétně, co uděláte jako první?

To je individuální podle každého zákazníka. Vždy se snažíme nejprve vše analyzovat. Cílem je pochopit, s jakým problémem zákazník přichází. Podíváme se, jaké máme možnosti, jaké jsou nástroje a rozpočet. Poté si vše odsouhlasíme a můžeme nasadit jednotlivé týmy, které na řešení společně se zákazníkem pracují. Nejčastěji pracujeme s balíkem Microsoft 365, ve kterém je schovaná i týmová komunikace, spolupráce, bezpečnost. Jsme schopni vyvinout nový software nebo změnit systémové procesy, pomoci migrovat stávající prostředí do cloudu a zvednout úroveň zabezpečení. A připravit vše tak, abychom mohli nasadit i nástroje umělé inteligence.

Jakou roli hraje v těchto procesech využití umělé inteligence?

Dnes každý mluví o umělé inteligenci, generativní umělé inteligenci a různých AI asistentech, Copilotech. Ale málokdo se na začátku zamýšlí nad tím, že je potřeba si nejprve udělat pořádek ve vlastní bezpečnosti. Můžete se lehce dostat do situace, kdy umělá inteligence vidí v podstatě kamkoliv a může také výsledky dodávat komukoliv, kdo má třeba špatně nastavené oprávnění. Tedy by třeba některé informace - osobní, finanční nebo projektové - mít neměl. To jsou pak takové situace, kdy zaměstnanci se zeptají na plat svých kolegů a umělá inteligence bez skurpulí odpovídá. Takže i systémy umělé inteligence musí být vhodně nastaveny a zabezpečeny. Ne vždy je nasazení umělé inteligence vhodné bez rozmyslu, nejedná se o univerzální řešení na všechno.

Nabízíte firmám i školení?

Nejsme sice školicí centrum a není to náš primární úkol, ale v případě transformačního projektu provádíme i zaškolení a pomáháme s adopcí. Bez toho by to ani nešlo, nelze nainstalovat nový software, upravit všechny procesy a pak prostě odejít. Musí následovat cílené seznámení uživatelů, aby vše mohli - a chtěli - sami používat. Máme pro tyto účely i náš vlastní software.

Můžete ukázat nějaké konkrétní případy, kdy jste firmám pomohli?

Měli jsme firmu z oblasti finančního sektoru, které jsme pomohli transformovat jejich procesy a převést obrovské množství papírové agendy do digitální podoby. Tím jsme jim pomohli ušetřit čas a zmenšit prostor pro chyby. Také jsme jim výrazně zjednodušili schvalovací a komunikační procesy. V jiné velké výrobní společnosti jsme zase realizovali migraci jejich obrovského datového centra do cloudu. Nebyla to jen migrace služeb, ale i automatizace a optimalizace. Šlo o celkovou změnu IT backgroundu, aby odpovídal moderním standardům. I tam jsme myslím splnili zadání na výbornou a firma byla velmi spokojená.

Jaké vize máte se svým týmem do budoucna?

Chceme se stát respektovaným partnerem a posílit jméno Konica Minolta v oblasti cloudu a bezpečnosti. Dostat se mezi zavedené velké hráče. Celkově pak společně s ostatními firmami chceme pomoci tomu, aby české firmy byly odolnější vůči kyberútokům. To by měl být cíl nás všech. Ostatní firmy v tomto nebereme jako konkurenty, ale spíše jako partnery.