

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **103** ze dne **8.4.2025**

Jen třetina malých a středních firem dokáže komplexně řešit ochranu dat

Vývoj kybernetických hrozeb vede k tomu, že zabezpečení vlastní firemní sítě v podobě VPN, firewallu a antivirových řešení už nemůže stačit. A to nejenom díky narůstající mobilitě dat, ke kterým uživatelé přistupují z firemních, soukromých i veřejných zařízení, ale i možnostem práce na dálku, kdy data mohou být uložena prakticky kdekoli, od on-premise řešení až po cloud. Zejména pro menší firmy je proto velmi obtížné zajistit komplexní ochranu svých dat.

Vyplývá to z analýzy společnosti ComSource, která uvádí, že pouze 30 % malých a středních podniků se v rámci zabezpečení svého IT zaměřuje na ochranu dat a dokáže ji řešit komplexně.

K současným trendům bezpečnostních mechanismů patří vícefaktorová autentizace, automatizace bezpečnostních opatření, synchronizovaná ochrana koncových bodů nebo detekce potenciálně slabých míst. V ochraně podnikové informační architektury je však klíčové zaměřit se na to základní – ochranu samotných dat.

"Data jsou opravdu to nejcennější, co firma má. U ochrany dat je proto třeba zaměřit se na komplexnost celého procesu – tedy od samotného zaznamenávání a uložení dat, přes jejich přenos, až po ošetření chybných konfigurací souvisejících nástrojů a odhalení anomálií ve zpracování. V praxi to například znamená data zálohovat, maskovat, šifrovat, čistit v okamžiku jejich příjmu i dalšího zpracování, ověřovat důvěryhodnost instalačních balíčků nebo eliminovat nebezpečné kódy a URL adresy. Setkáváme se s tím, že firmy mají například dobře zvládnutou oblast šifrování, naopak velmi problematická bývá správa uživatelských identit, kdy zdaleka ne všichni zaměstnanci mají přístup jen k tomu, co skutečně potřebují. Na komplexní ochranu dat ale firmy zpravidla nemají dostatek kapacity," říká Jaroslav Cihelka, spolumajitel společnosti ComSource a expert na kybernetickou bezpečnost.

Z pohledu prevence ochrany dat před kybernetickými útoky se musí firmy umět připravit na to, že se útočníci dokážou nepozorovaně infiltrovat do firemní IT infrastruktury a mohou vyčkávat měsíce, ale i rok, aby zasáhli co nejefektivněji. Důležité je pak poznat, v jakém rozsahu se útočníkům podařilo zakotvit ve firemní síti a najít cesty, kterými se do ní dostali.

"Samotné zastavení útoku nestačí. K ochraně dat slouží neustálé hloubkové audity a monitoring síťového provozu, aby bylo možné orientovat se v běžném chování datového obsahu. Dojde-li ke kybernetickému útoku, pomohou nám tyto procesy odvodit abnormality v době útoku, ale i po něm. Čím dříve se jakékoli odchylky v rámci analýzy datového obsahu odhalí, tím lépe. Přestože datově orientovaná bezpečnost ve spojení s dalšími bezpečnostními mechanismy dokáže účinně vyřešit většinu aktuálních hrozeb, nelze nikdy dosáhnout 100% ochrany. Pro případ kybernetického útoku by tak firmy měly mít připravenou i analýzu rizik, která určuje ochranu klíčových systémů a business aplikací pro zajištění kontinuity jejich podnikání. Musí si i stanovit rizika, která jsou z ekonomického pohledu schopny u případných ztrát akceptovat," uzavírá Jaroslav Cihelka.

Zdroj: AVcentrum ČR