Prečo malé firmy stále podceňujú kyberbezpečnosť

27.7.2026 - | Podnikajte.sk

Malé a stredné firmy ochranu často odkladajú pre nedostatok ľudí, času či rozpočtu. Pri kyberútoku však rozhoduje, ako rýchlo ho odhalia a začnú reagovať.

Kybernetický útok sa nemusí začať dramaticky ako vo filmoch. Niekedy stačí infikovaná príloha, dôveryhodne vyzerajúci odkaz alebo slabé heslo. Navonok sa pritom nemusí diať nič nezvyčajné.

Práve nenápadnosť dáva útočníkom čas. Hrozba môže zostať v systéme bez povšimnutia celé týždne či mesiace. Keď sa incident naplno prejaví, už nemusí ísť iba o problém s počítačom. Firma sa nemusí dostať k objednávkam, fakturácii či e-mailom a útočník môže získať prístup k zmluvám, cenovým podmienkam alebo údajom o zákazníkoch. Aj krátky výpadok či únik citlivých informácií tak môže ohroziť tržby a poškodiť obchodné vzťahy aj dôveru klientov.

Prečo malé firmy ochranu odkladajú

Menšie firmy často **nemajú vlastného špecialistu na kybernetickú bezpečnosť**. O technické prostredie sa stará interný IT pracovník alebo externý dodávateľ, ktorý popri bezpečnosti rieši aj zariadenia, softvér a každodenné problémy zamestnancov.

Ďalšou bariérou je presvedčenie, že **malá firma nie je pre útočníkov zaujímavá**. Automatizované útoky však vo veľkom vyhľadávajú slabé heslá, neaktualizované systémy či nezabezpečené zariadenia. Veľkosť podniku preto sama osebe nepredstavuje ochranu.

Firmy odrádzajú aj **náklady a zložitosť**. Vybudovanie vlastného bezpečnostného dohľadového centra si vyžaduje technológie, nastavené procesy, nepretržitý monitoring a kvalifikovaných ľudí. Odborníkov na kybernetickú bezpečnosť je pritom na trhu nedostatok.

Pri útoku rozhoduje rýchlosť

Čím skôr firma podozrivú aktivitu zachytí, tým väčšiu má šancu obmedziť škody a zabrániť tomu, aby sa incident rozšíril do ďalších častí infraštruktúry.

Samotné upozornenie však ešte nemusí prezradiť, aký vážny problém firma rieši. Bezpečnostné udalosti treba vyhodnocovať v súvislostiach, odlíšiť falošný poplach od reálnej hrozby a zvoliť správny spôsob reakcie. To si vyžaduje nielen technológiu, ale aj skúsených odborníkov.

Dohľad aj bez vlastného bezpečnostného centra

Jednou z možností, ako môžu firmy získať nepretržitý dohľad bez budovania vlastného centra, je manažovaná služba **Dynamic SOC**.

Dynamic SOC, teda Security Operations Center, spája špičkové technológie a automatizovanú reakciu s nepretržitým dohľadom bezpečnostných analytikov. Bezpečnostné udalosti tak nesleduje iba systém, ale aj skúsení odborníci, ktorí ich vyhodnocujú v súvislostiach a v prípade incidentu pomáhajú firme okamžite reagovať. Služba monitoruje zariadenia, servery a ďalšie časti firemnej

infraštruktúry. Ak zachytí podozrivú aktivitu, môže napríklad izolovať napadnuté zariadenie od siete, ukončiť škodlivý proces alebo presunúť súbor do karantény.

Službu na slovenský trh prináša Orange Business. Ide o prémiové riešenie kybernetickej bezpečnosti vyvinuté expertmi z Orange Cyberdefense. Odbornej verejnosti bola prvýkrát predstavená na Orange konferencii, ktorá sa venovala aj pripravenosti firiem na nové technologické a bezpečnostné výzvy.

Dynamic SOC je dostupný firmám už **od 20 zariadení**. Cena začína od **6 eur na zariadenie** mesačne, bez skrytých poplatkov a bez cien založených na objeme spracovaných logov.

„Kybernetická bezpečnosť sa dnes stáva súčasťou základnej pripravenosti firmy. Nejde len o IT problém, ale o schopnosť chrániť prevádzku, dáta, reputáciu aj dôveru zákazníkov. Dynamic SOC prináša firmám prístup k expertíze a nepretržitému dohľadu, ktorý im pomáha zvládať bezpečnostné riziká bez toho, aby museli budovať vlastné dohľadové centrum," hovorí Hana Kvartová, Chief Commercial B2B Officer spoločnosti Orange Slovensko.

Dve úrovne ochrany podľa potrieb firmy

EDR, teda Endpoint Detection & Response, sa zameriava na ochranu koncových zariadení, ako sú pracovné stanice a servery. Pomáha odhaľovať podozrivú aktivitu, reagovať na incidenty a uchovávať technické údaje potrebné na spätnú analýzu.

XDR, teda Extended Detection & Response, rozširuje ochranu nad rámec koncových zariadení. Analyzuje logy zo sieťových zariadení, kritických serverov alebo SaaS služieb a poskytuje širší pohľad na dianie v digitálnej infraštruktúre firmy.

Všetko dôležité po ruke

Firmy majú bezpečnostné udalosti dostupné v jednej konzole a v mobilnej aplikácii MySecurity. Vidia aktuálny stav incidentov aj prijaté opatrenia a v prípade potreby sa môžu spojiť s analytikmi.

Kybernetická bezpečnosť tak nemusí byť pre malé a stredné firmy nedostupná, drahá ani príliš zložitá. Riziko je reálne a aj jediný nešťastný klik môže ochromiť prevádzku, spôsobiť finančné straty a poškodiť dôveru zákazníkov. Ochranu preto netreba začať riešiť až vo chvíli, keď už útok prebieha.

Viac informácií o riešení Dynamic SOC nájdete na webstránke orange.sk/biznis.

https://www.podnikajte.sk/technologie/preco-male-firmy-stale-podcenuju-kyberbezpecnost