TLAČOVÁ SPRÁVA č. 02/2025
20. MAREC 2025

Kritický nedostatok kybernetických analytikov ohrozuje firmy – odborníci radia malým a stredným podnikom, ako sa chrániť proti kybernetickým útokom

Firmy na Slovensku aj v zahraničí čelia rastúcim kybernetickým hrozbám, no počet špecialistov v oblasti IT bezpečnosti, naopak, nerastie. Odborníci na kybernetickú bezpečnosť aj HR manažéri upozorňujú na nedostatok kyberšpecialistov. Mária Krahulecová z Qubit Conference® radí, ako majú malé a stredné podniky zabezpečiť svoju prevádzku, keď svojich kybernetických špecialistov postrádajú.

Bratislava, 20.3.2025

Podľa údajov portálu Profesia.sk bol v roku 2024 zaznamenaný pokles pracovných ponúk na pozíciu špecialistu IT bezpečnosti na 1550, čo je výrazne menej ako v roku 2023 (1900) a ešte prudší prepad oproti roku 2022 (2800). Záujem uchádzačov je podpriemerný – na jednu ponuku reagovalo vlani len 8 kandidátov, rok predtým dokonca iba 5.

Odborníci varujú, že podniky bez kybernetických špecialistov si musia osvojiť preventívne opatrenia, aby minimalizovali kybernetické riziká.

Ako sa firmy môžu chrániť?

Nedostatok kybernetických analytikov na trhu práce núti firmy prebrať zodpovednosť za svoju bezpečnosť do vlastných rúk. Aj bez interného tímu expertov môžu podniky výrazne znížiť svoje riziká správnou kombináciou technických opatrení, školení a pravidelného testovania bezpečnosti.

Mária Krahulecová, organizátorka konferencií o kybernetickej bezpečnosti Qubit Conference® upozorňuje, že kybernetická bezpečnosť nie je jednorazová úloha, ale kontinuálny proces: „Podniky by mali implementovať viacúrovňové zabezpečenie vrátane firewallov, antivírusového softvéru, šifrovania dát a pravidelnej aktualizácie systémov. Dôležitou súčasťou ochrany je aj vzdelávanie

zamestnancov v oblasti kybernetických hrozieb, by vedeli rozpoznať phishingové útoky a iné podvodné praktiky.“ Okrem toho zdôrazňuje, že podniky by nemali zabúdať na preverovanie bezpečnosti svojich dodávateľov a partnerov. Zdôrazňuje, že často sa zabúda práve na fakt, že slabým článkom bezpečnosti môžu byť tretie strany, ktoré nemajú dostatočne zabezpečené systémy.

Bezpečnostné audity, testovanie systémov a školenia zamestnancov by mali firmy vykonávať minimálne raz za štvrťrok. Softvérové aktualizácie a kontroly hrozieb by však mali prebiehať priebežne. Kým veľké podniky disponujú robustnejšími IT infraštruktúrami a čelia väčšiemu množstvu útokov, preto investujú do špecializovaných bezpečnostných tímov, malé firmy môžu tento hendikep kompenzovať využívaním cloudových bezpečnostných služieb a dodržiavaním osvedčených postupov.

Bezpečnosť dát nadovšetko: Zapamätajte si toto zlaté pravidlo

Malé a stredné podniky sa často stretávajú s obmedzenými finančnými a personálnymi zdrojmi, čo sťažuje implementáciu komplexných bezpečnostných opatrení. „Problémom je aj nedostatočná digitálna gramotnosť zamestnancov a nesprávne nastavené procesy reakcie na bezpečnostné incidenty,“ upozorňuje M. Krahulecová.

Bezpečnostný analytik a člen odbornej komisie z Qubit Conference® Boris Mutina pripomína dôležitosť funkčného a obnoviteľného zálohovania: „Praktizovanie zlatého pravidla zálohovania **3-2-1-1-0** je dnes viac ako aktuálne – minimálne tri kópie dát, na dvoch rôznych druhoch médií, s minimálne jednou kópiou na inej lokácii, jednou kópiou offline a s nulovými chybami v zálohách.“ Tento systém zabezpečuje, že podniky môžu svoje dáta obnoviť aj v prípade rozsiahleho kybernetického útoku alebo technickej poruchy ako tomu bolo napríklad v prípade katastrálneho portálu Úradu geodézie, kartografie a katastra SR.

Ste malá firma? Top pravidlá, ako sa vyhnúť kybernetickému útoku

„Ignorovanie kybernetickej bezpečnosti môže viesť k značným finančným stratám, poškodeniu reputácie či dokonca právnym následkom. Naopak, dôkladná ochrana posilňuje dôveru zákazníkov a obchodných partnerov, znižuje riziko výpadkov a zvyšuje celkovú odolnosť firmy,“ dodáva Krahulecová.

Ako sa firmy môžu efektívne chrániť dodržiavaním základných princípov kybernetickej bezpečnosti:

- Silné heslá a dvojfaktorová autentifikácia
- Pravidelné zálohovanie dát
- Aktualizácie softvéru a systémov
- Firewall a antivírusová ochrana
- Školenia zamestnancov o kybernetických hrozbách
- Pravidelné bezpečnostné audity
- Plán reakcie na kybernetický incident