ROZHOVOR: **ERIK LEO**, COUNTRY MANAGER SPOLOČNOSTI ZEBRA SYSTEMS PRE SLOVENSKO

KYBERNETICKÁ BEZPEČNOSŤ
NIE JE MOŽNOSŤ, ALE NEVYHNUTNOSŤ

O plánoch a zámeroch spoločnosti ZEBRA SYSTEMS dodávajúcej špičkový bezpečnostný softvér a komplexné riešenia sme sa porozprávali s **Erikom Leom**, novým Country Managerom spoločnosti pre Slovensko.

NXT S akými cieľmi a zámermi ste nastúpil na pozíciu Country Managera spoločnosti ZEBRA SYSTEMS pre Slovensko a ako plánujete využiť svoje bohaté skúsenosti v oblasti bezpečnostného softvéru?

Erik Leo: Na pozícii Country Managera pre Slovensko sa starám o distribučný predaj a obchodný rozvoj všetkých značiek distribuovaných spoločnosťou ZEBRA SYSTEMS na Slovensku. Ako hlavný cieľ som si stanovil rozšíriť povedomie o kybernetických riešeniach, ktoré ponúkame, a keďže som v iných firmách pracoval viac ako 10 rokov pre rôzne zahraničné trhy (Nemecko, Rakúsko, Švajčiarsko, Anglicko), rád by som priniesol našim partnerom najnovšie trendy v oblasti kybernetickej bezpečnosti.

NXT O aké produkty a služby ZEBRA SYSTEMS je na Slovensku najväčší záujem?

Erik Leo: Na Slovensku prostredníctvom našich partnerov dodávame kompletné portfólio, t. j. riešenia Acronis, GFI Software, N-able, Cloudflare, AST a Company (Un)Hacked. Okrem predaja poskytujeme našim zákazníkom aj špičkovú podporu a školenia. Spomínané riešenia sa navzájom dopĺňajú, takže naši partneri vedia vytvoriť komplexné kybernetické riešenia. Žiadané sú napríklad kybernetické audity, lebo mnohé firmy často nemajú prehľad o aktuálnom stave zabezpečenia. Ďalšia dôležitá oblasť je školenie v oblasti kybernetickej bezpečnosti, ktoré je v mnohých organizáciách veľmi podceňované, a my ponúkame moderné a atraktívne riešenie školenia vo virtuálnej realite.

NXT Je povedomie o kybernetickej bezpečnosti vo firmách dostatočné? Aké sú trendy v tejto oblasti?

Erik Leo: Máme celkom dobrý prehľad o tom, čo sa deje najmä v segmente malých a stredných podnikov (SMB), pretože mnohí používatelia našich technológií sú z tohto segmentu. Podľa nedávneho prieskumu spoločnosti GFI Software je len 31 % malých a stredných podnikov dobre pripravených na potenciálny kybernetický útok. Malé a stredné podniky sú totiž minimálne rovnako náchylné stať sa obeťou útokov ako veľké spoločnosti, a to práve z dôvodu ich slabej obrany.

Väčšina SMB spoločností má dnes nanajvýš jedného experta na kybernetickú bezpečnosť a mnohé dokonca nemajú žiadneho. Pritom väčšina útokov na tieto spoločnosti využíva značný počet zraniteľností obsiahnutých v neaktualizovaných systémoch a aplikáciách. Preto sa k nim ľahko dostane malvér, phishingové e-maily, ransomvér, útoky DDoS alebo útoky typu man-in-the-middle.

Pre malé a stredné podniky už kybernetická bezpečnosť nie je možnosť, ale nevyhnutnosť. Zaužívaná predstava, že „sme príliš malí na to, aby nás niekto napadol“, je len ilúziou. Preto vidíme zreteľný nárast záujmu o outsourcing IT bezpečnosti profesionálnym poskytovateľom MSP, pričom mnohé malé a stredné podniky už využívajú aspoň niektoré služby MSP, čím eliminujú nedostatok alebo absenciu vlastných IT expertov.

NXT Aké nedostatky a riziká dokáže odhaliť bezpečnostný audit? Aké nástroje na audit ponúka ZEBRA SYSTEMS?

Erik Leo: Ako som naznačil, čoraz viac organizácií požaduje audit kybernetickej bezpečnosti. Podľa niektorých štatistík viac ako polovica malých a stredných podnikov je alebo bola terčom nejakého kybernetického útoku, pričom až tri štvrtiny škodlivého softvéru zostávajú neodhalené prostredníctvom nástrojov založených na signatúrach, ktoré používajú.

Audit kybernetickej bezpečnosti je jedno z proaktívnych opatrení na zníženie rizika týchto útokov. Audit by mal identifikovať oblasti kybernetickej bezpečnosti, ktoré by mali byť pokryté, ako aj posúdiť konkrétne riziká a zaviesť primerané opatrenia.

Audit nevyrieši jeden produkt alebo nástroj, je to predovšetkým proces, ktorý si vyžaduje čas, úsilie zodpovedných pracovníkov a dôsledné vykonávanie potrebných opatrení. Konkrétne bezpečnostné nástroje, ako napríklad GFI LanGuard, však môžu poskytnúť cenné informácie, ako napríklad identifikáciu hrozieb, inventarizáciu zariadení, systémov a softvéru alebo úroveň zabezpečenia, čo celý proces veľmi zefektívni.

NXT Najslabším miestom, čo sa týka zabezpečenia v mnohých firmách, je ľudský faktor. Čo by sa malo zlepšiť v oblasti vzdelávania zamestnancov?

Erik Leo: Kybernetické útoky sú v súčasnosti dobre organizovaným odvetvím, ktoré útočí na najslabší článok kybernetickej bezpečnosti – firemného používateľa. Podľa spoločnosti Cox BLUE je 48 % úspešných kybernetických útokov v malých a stredných organizáciách spôsobených ľudským faktorom. Preto je dôležité nenudiť zamestnancov štandardnou prezentáciou, ale skôr ich atraktívnym spôsobom motivovať, aby získali povedomie o kybernetických hrozbách a snažili sa vyhnúť rizikovému správaniu.

Nedávno sme sa stali distribútorom riešenia Company (Un)Hacked, ktoré umožňuje zamestnancom naučiť sa špecifické triky, ktoré hackeri používajú, aby sa dostali k citlivým informáciám, pričom počas školenia prechádzajú rôznymi na seba nadväzujúcimi scenármi. Jedinečnosť tohto projektu spočíva v tom, že školenie vo virtuálnej realite je skôr dramatická udalosť než tradičná nudná prezentácia. Počas školenia zamestnanci preberajú úlohu hackera, ktorý vykonáva vybrané úlohy špecificky zamerané na kancelárske a firemné prostredie, a vďaka tomu sa stávajú odolnejšími proti skutočným kybernetickým útokom, čo v konečnom dôsledku posilňuje celkovú bezpečnosť spoločnosti.

NXT Čoraz populárnejšou formou realizácie zabezpečenia, hlavne vo firmách, ktoré nemajú vlastných IT špecialistov, sú manažované IT služby. Aké sú výhody MSP?

Erik Leo: Spoločnosti si často nemôžu dovoliť správcov IT, ktorí by boli schopní pokryť ich potreby v oblasti IT, alebo jednoducho nie sú na trhu. To je však len jeden z dôvodov, prečo prejsť na služby MSP. Ďalšími sú rastúci strach z kybernetických útokov, nepríjemné skúsenosti s výpadkami alebo nepredvídateľné náklady na vlastníctvo IT.

Keď organizácie prejdú na model služieb MSP, presne vedia, koľko budú platiť mesačne alebo ročne. Navyše ich údaje budú bezpečnejšie ako vo vlastných systémoch, pretože poskytovatelia MSP si môžu dovoliť lepšie zabezpečenie. A napokon sa nebudú musieť starať o údržbu, modernizáciu alebo licencovanie svojej IT infraštruktúry, pretože to všetko je už zahrnuté v cene služby. A dopyt rastie – nedávna správa spoločnosti N-able uvádza, že 97 % poskytovateľov MSP očakáva, že príjmy zo služieb MSP v najbližších rokoch porastú.

NXT Pre každého dodávateľa IT produktov a služieb je kľúčový partnerský ekosystém. Aká je aktuálna situácia a čo v tejto oblasti plánujete zlepšiť? Aké podujatia pre zákazníkov a partnerov pripravujete?

Erik Leo: Na Slovensku máme silnú partnerskú základňu, ktorú sa snažíme po cely rok informovať o novinkách v našich riešeniach, a to vrátane rôznych podujatí, webových seminárov a konferencií. Minulý rok sme napríklad zorganizovali roadshow v Bratislave a potom sme sa stretli s partnermi v Košiciach a Banskej Bystrici. Tento rok chceme rozšíriť portfólio podujatí aj do ďalších regiónov, napríklad do Žiliny, Popradu a Nitry. Tento rok sa 26. septembra vraciame do Bratislavy s našou Zebra Cyber Roadshow 2024, kde sa účastníci dozvedia najnovšie trendy v oblasti kybernetickej bezpečnosti.

Okrem toho vykonávame aj množstvo marketingových aktivít vrátane webových seminárov, technických školení, prieskumu trhu a udeľovania cien za najlepší predaj. Neustále sa snažíme informovať našich partnerov a poskytovať im čo najlepšie podmienky na dosahovanie stále lepších výsledkov. Pretože náš úspech závisí predovšetkým od ich úspechu a spokojnosti ich zákazníkov.

Ďakujeme za rozhovor.

■