TLAČOVÁ SPRÁVA č. 04/2024
24. SEPTEMBER 2024

Kybernetická bezpečnosť – kľúč k ochrane v digitálnom svete

S rastúcim počtom kybernetických útokov, ktoré ohrozujú právnické aj fyzické osoby, je dôležité objasniť význam prevencie a dôsledného zabezpečenia digitálnych systémov. Odborníci varujú, že náklady na kybernetickú kriminalitu by mohli do roku 2025 dosiahnuť nepredstaviteľných 10,5 bilióna dolárov ročne, čo podčiarkuje potrebu robustných bezpečnostných stratégií a vzdelávania v oblasti kybernetickej bezpečnosti. Tieto výzvy si vyžadujú nielen technologické investície, ale aj zmenu kultúry vnímania bezpečnosti na všetkých úrovniach – od jednotlivcov cez podniky až po vládne inštitúcie. Október je vyhlásený za Európsky mesiac kybernetickej bezpečnosti.

Bratislava, 24.9.2024

Podľa štatistík Data Breach Investigations Report (2020) má až 71 % všetkých kybernetických útokov motiváciu vo finančnej otázke. Tieto útoky môžu zahŕňať krádež osobných údajov, duševného vlastníctva a dokonca špionáž. „Otázka kybernetickej bezpečnosti sa týka každého, či je to podnikateľ alebo jednotlivec, a zahŕňa ochranu telefónov, počítačov, vytváranie hesiel, spôsoby ukladania a nezdieľania prístupov," vysvetľuje Mária Krahulecová, spoluzakladateľka Qubit Conference®. Je zrejmé, že nedostatok vzdelania v tejto oblasti môže mať vážne dôsledky, najmä pre tých, ktorí nie sú technicky zdatní.

Vedeli ste, že aj GPS dáta sú osobné údaje?

Používatelia na sociálnych sieťach často sami zdieľajú osobné a citlivé údaje, či už ide o dátum narodenia, miesto narodenia, rodinný stav, zamestnanie, vzdelanie alebo svoju polohu. "Takéto informácie môžu byť použité na vytvorenie falošného profilu alebo na sledovanie používateľa," píše na svojom webe Ministerstvo investícií, regionálneho rozvoja a informatizácie. Hrozbami v kybernetickom priestore je vydieranie, kyberšikana, krádež identity, ohováranie, špionáž, phishing (pokus o podvodné získanie informácií) a mnoho ďalších. Ako upozorňuje Ministerstvo informatizácie, regionálneho rozvoja a investícií na svojom webe, napríklad pri krádeži identity útočník môže zneužiť ukradnuté osobné údaje na získanie prístupu k bankovým účtom alebo kreditným kartám.

V digitálnom svete sú osobné a citlivé údaje, ako sú finančné informácie, zdravotné záznamy alebo identifikačné údaje, neustále ohrozené. „Kybernetická bezpečnosť chráni tieto údaje pred krádežou alebo zneužitím. Zabezpečenie systémov pomáha predchádzať útokom. Udržiavanie vysokého štandardu kybernetickej bezpečnosti zvyšuje dôveru zákazníkov, partnerov a verejnosti. Kybernetická bezpečnosť hrá kľúčovú úlohu v ochrane kritickej infraštruktúry, ako sú energetické siete, zdravotnícke systémy a dopravné systémy, pred potenciálnymi hrozbami. Kybernetické hrozby nepoznajú hranice, a preto je dôležité, aby organizácie a krajiny spolupracovali na zabezpečení svojich systémov a výmene informácií. Rôzne techniky a nástroje, ktoré útočníci používajú, si vyžadujú neustálu aktualizáciu a prispôsobenie bezpečnostných stratégií," uviedol Ondrej Kreheľ, špičkový odborník na kybernetickú bezpečnosť, ktorý pôsobí viac ako 20 rokov v New Yorku a spolupracuje s americkou vládou a najväčšími nadnárodnými korporátmi.

AKO ROZPOZNAŤ HROZBY?

Kybernetická bezpečnosť nie je len technická záležitosť, ale aj otázka zodpovednosti. Základným krokom je, aby sa firmy a jednotlivci naučili rozpoznať a reagovať na kybernetické hrozby. Zamestnanci hrajú kľúčovú úlohu v ochrane pred kybernetickými útokmi. „Zamestnanci by mali byť pravidelne školení v oblasti kybernetickej bezpečnosti, aby vedeli rozpoznať phishingové e-maily a iné podvodné techniky," uvádza Ondrej Kreheľ z Qubit Conference®.

Podvodné (phishingové) emaily je možné rozpoznať podľa viacerých znakov. „Jedným z nich je podozrivá emailová adresa odosielateľa, ktorá môže vyzerať podobne ako známe spoločnosti, ale obsahovať malé chyby. Typickým rysom je aj vytváranie pocitu naliehavosti s výzvami na okamžitú akciu, napríklad hrozbou blokácie účtu. Takéto emaily často obsahujú gramatické a pravopisné chyby, čo pôsobí neprofesionálne," hovorí spoluzakladateľka Qubit Conference® Mária Krahulecová. Phishingové správy vás môžu žiadať o osobné údaje, čo legitímne spoločnosti nikdy nerobia. Odkazy v takýchto emailoch vedú na podozrivé webové stránky, ktoré sa dajú overiť podržaním myši nad odkazom bez klikania. „Častým znakom sú aj neočakávané prílohy, ktoré môžu obsahovať škodlivý softvér. Vizualizácie ako logá bývajú falošné a pri bližšom pohľade nekvalitné. Email vás často osloví neosobne, a sú často doručované v nezvyčajných časoch, ako napríklad v noci alebo cez víkendy, a ich formátovanie býva nekonzistentné, s chybnými tlačidlami alebo nefunkčnými odkazmi," vysvetľuje M. Krahulecová.

S rozvojom AI prichádza aj tvorba deep fake videí, ktoré na prvý pohľad vyzerajú ako skutočné. Tieto videá môžu byť zneužité na šírenie dezinformácií a manipuláciu. „Dnes sa stáva rozšíreným spôsobom, že počas konferenčných hovorov sa zapájajú dvojníci, ktorí sú nerozoznateľní od tých reálnych," varuje M. Krahulecová z organizácie, ktorá sa venuje organizovaniu podujatí o kybernetickej bezpečnosti. Tieto technológie môžu viesť k ohrozeniu bezpečnosti, najmä pokiaľ ide o citlivé informácie a interakcie na virtuálnych platformách. „Je nevyhnutné, aby sme sa naučili, ako sa chrániť pred kybernetickými hrozbami. Základné kroky zahŕňajú ochranu proti phishingu, pravidelné zálohovanie systémov, zabezpečenie osobne identifikovateľných informácií a ochranu sietí. Je dôležité, aby organizácie investovali do technológie na prevenciu a detekciu hrozieb, ako aj do školení zamestnancov, aby si boli vedomí rizík a vedeli na ne reagovať," dopĺňa M. Krahulecová.

AKO NA NÁS VPLÝVA DIGITÁLNY STRES

Digitálny stres, ktorý mnohí zažívajú, najmä starší ľudia, je ďalším aspektom, ktorý je potrebné zohľadniť. Mnohí sa cítia preťažení technológiami a vyžadujú si podporu a porozumenie.

„Digitálny stres ovplyvňuje v dnešnej dobe takmer každého z nás, ale v rôznej miere. Pri strese sa nám zvyšuje hladina kortizolu, čo je pri krátkodobom strese prospešné, pretože nám pomáha zvládať záťaž. Digitálny stres má významný vplyv na našu psychiku, ktorý sa môže prejaviť zvýšenou dráždivosťou alebo agresivitou, problémami so spánkom, únavou a vyčerpaním, ťažkosťami s koncentráciou či pamäťou. Pokiaľ dlhodobo pretrváva môže viesť k úzkostiam, vyhoreniu alebo depresiám," upozorňuje klinická psychologička Mgr. Alica Farkašová. Otvorené diskusie, otázky a zdieľanie pocitov sú dôležité pre prekonanie týchto výziev. Je dôležité poskytnúť seniorom a menej zdatným používateľom dostatok informácií a nástrojov, ktoré im pomôžu orientovať sa vo svete digitálnych technológií. Kybernetická bezpečnosť nie je len technická záležitosť, ale aj otázka zodpovednosti, vzdelania a ochoty učiť sa nové veci. Posilnením našich vedomostí a zručností v oblasti kybernetickej bezpečnosti môžeme chrániť seba a našich blízkych pred potenciálnymi hrozbami a zaistiť si tak bezpečnejšiu budúcnosť.

O aktuálnych trendoch a novinkách v oblasti kybernetickej bezpečnosti budú hovoriť experti z bánk, súkromného a štátneho sektora na Qubit Conference® 13.-14.11.2024 v Jasnej.