

STE PODNIKATEĽ? AKO ODHALÍTE, ŽE VAŠA FIRMA JE POD KYBERNETICKÝM ÚTOKOM?

V dnešnej digitálnej ére, keď sa technológie stali základnou súčasťou podnikania, sa kybernetické útoky stávajú alarmujúcou realitou pre firmy všetkých veľkostí. S narastajúcim počtom hrozieb a sofistikovanosťou útokov je nevyhnutné, aby firmy investovali do vzdelávania zamestnancov a zabezpečenia svojich systémov.

Bratislava, 28.8.2024

S narastajúcim počtom digitálnych zariadení a online služieb sa zvyšuje aj riziko kybernetických útokov, ktoré môžu mať závažné následky pre jednotlivcov aj organizácie. Prevencia a včasná detekcia sú kľúčové pre ochranu citlivých údajov a zníženie rizika finančných strát. Rôzne formy hrozieb, ako sú phishing, ransomware a DDoS útoky, sú čoraz sofistikovanejšie a vyžadujú si proaktívny prístup k ochrane údajov.

NAJČASTEJŠIE KYBERNETICKÉ ÚTOKY

Kybernetické útoky sa zvyčajne odohrávajú v niekoľkých fázach. Najprv ide o prípravu a prieskum, kde útočníci zbierajú informácie o cieľi. „Môže ísť o analýzu verejných profilov na sociálnych sieťach, webových stránkach firmy alebo o zistenie technických špecifikácií a systémov. Po zhromaždení potrebných informácií sa útočníci snažia získať prístup k systémom firmy. Môže to zahŕňať phishingové e-maily, ktoré obsahujú škodlivé odkazy alebo prílohy, ale aj využívanie zraniteľností v softvéri. Ak majú útočníci prístup, začínajú s krádežou údajov, inštaláciou malvéru alebo priamym útokom na servery. V prípade ransomwaru sa údaje zašifrujú a útočníci požadujú výkupné,“ vysvetľuje Ondrej Kreheľ, spoluzakladateľ Qubit Conference®, ktorá sa venuje organizovaniu konferencií o kybernetickej bezpečnosti.

DDoS útoky sú zamerané na preťaženie serverov a sietí, čím spôsobujú výpadok služieb. Môžu mať za následok stratu produktivity a finančné straty pre organizácie.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava

AKO ROZPOZNAŤ A ODHALIŤ KYBERNETICKÝ ÚTOK

Útočníci sú veľmi šikovní a dôslední, preto je pre firmy kľúčové mať zavedené mechanizmy na detekciu a prevenciu kybernetických hrozieb. „Zamestnanci by mali byť pravidelne školení v oblasti kybernetickej bezpečnosti, aby vedeli rozpoznať phishingové e-maily a iné podvodné techniky. Taktiež by sa mala monitorovať a analyzovať sieťová aktivita. Implementácia systémov na monitorovanie sieťovej prevádzky môže pomôcť pri identifikácii nezvyčajných aktivít, ktoré by mohli naznačovať pokus o útok. Pomôže aj pravidelné aktualizovanie a zálohovanie. Udržiavanie softvéru a systémov aktuálnych a pravidelné zálohovanie údajov sú základnými krokmi pre ochranu pred kybernetickými útokmi,“ vymenúva Ondrej Kreheľ, top odborník na kybernetickú bezpečnosť, ktorý pôsobí v New Yorku.

VYDIERANIE A VÝKUPNÉ NIE JE TABU ANI NA SLOVENSKU

Krádež či zašifrovanie citlivých údajov spoločnosti a následná žiadosť o výkupné nie je nič nové ani na Slovensku. „Deje sa to aj slovenským firmám, ide aj o miliónové čiastky za obnovenie systémov a vrátenie záloh na to, aby firma mohla pokračovať ďalej. Otázkou teda nie je, či sa to niekedy udeje aj vám, ale kedy sa stanete obeťou kybernetického útoku,“ hovorí O. Kreheľ. Pripomína zároveň, že dôležité je aj vypracovanie plánu reakcie na incidenty, ktorý môže pomôcť firmám rýchlo reagovať na útoky a minimalizovať ich dopady.

KONFERENCIA PONÚKA BOHATÚ ŠKÁLU ODBORNÍKOV

Kybernetická bezpečnosť je dynamický a neustále sa vyvíjajúci proces a v prípade podnikateľov a firiem je nevyhnutné sa ňou zaoberať. Prednášky odborníkov a tréningy so špičkami z odboru ponúka Qubit Conference®, ktorá sa koná 13.-14.11.2024 vo Wellness Hoteli Chopok v Jasnej.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava