HOSPODÁRSKE NOVINY
UTOROK 14. DECEMBRA 2021

Virtuálnym útokom sa počas pandémie darí

Dôležité je nielen účinne sa brániť, ale prípadný útok vôbec detegovať. SNÍMKA: DREAMSTIME

KORONAVÍRUS

Pandémia vo svete akcelerovala potrebu digitalizácie vo firmách, priamym následkom je rastúci počet hackerských útokov.

Gabriela Alenová ©hn
gabriela.alenova@mafraslovakia.sk

Počet hackerských útokov počas pandémie narástol. Celosvetový počet incidentov sa medziročne zvýšil až o 125 percent, uvádza v správe Accenture. Kybernetický útok je možné definovať ako akékoľvek úmyselné správanie, respektíve konanie útočníka v rámci kyberpriestoru. Útočí na osoby používajúce technológie s hlavným cieľom ich poškodiť a získať informácie. Môže ísť o skupinový útok, prípadne aj o útok cudzej mocnosti. Motivácia je veľakrát rôzna. Napríklad prelomenie zabezpečenia online systémov, organizovanie akcií rôznych vlád alebo získanie informácií o kriminálnych činoch.

Podľa odborníka na kyberbezpečnosť je jedným z dôvodov pandémia a s tým súvisiaci presun aktivít firiem do online prostredia. „Pandémia spôsobila revolúciu pri prechode firiem z analógového sveta do online prostredia. Firmy, ktoré zmeny plánujú na mesiace až roky, boli nútené robiť zmeny rýchlo, čo so sebou prináša aj chyby. Práve tie sa snažia využívať hackeri, ktorých cieľom je primárne obohatiť sa," vysvetľuje Daniel Suchý, odborník na kyberbezpečnosť zo spoločnosti Aliter Technologies.

Útočia na firmy a inštitúcie

V súčasnosti je väčšina kybernetických útokov vedená s cieľom zisku. „Je to mýtus, že sa hackeri zaujímajú o bežných ľudí, práve naopak, vo väčšine prípadov útočia na firmy či inštitúcie, využívajú pritom buď zraniteľnosť v systéme, či napríklad aj nedostatočné zabezpečenie zamestnancov, ktorí pracujú z domu. Hackeri svoje úsilie smerujú tam, kde vidia potenciál zisku," hovorí odborník na kyberbezpečnosť. Ako dodáva, na útoky využívajú často práve takzvaný vydierací program. „Stretávame sa najmä s ransomvér útokmi, keď hacker zašifruje firme dáta a následne za ne požaduje

> Je to mýtus, že sa hackeri zaujímajú o bežných ľudí, práve naopak.
>
> **Daniel Suchý,**
> odborník na kyberbezpečnosť zo spoločnosti Aliter Technologies

výkupné, v prípade neúspechu sa ich pokúsi predať na čiernom trhu."

Najväčší ransomvér útok na svete sa odohral práve v tomto roku, keď hackeri zaútočili na americkú IT spoločnosť Kaseya a za dešifrovanie požadovali výkupné vo výške 70 miliónov dolárov. Incident ovplyvnil stovky firiem po svete, ktoré využívali ich aplikáciu, napríklad švédsky reťazec supermarketov Coop musel zavrieť 800 svojich prevádzok, pre ochromenie pokladničných systémov.

Takéto útoky pritom boli v minulosti zaznamenané aj na Slovensku, keď hackeri zaútočili a zašifrovali počítače v nitrianskej nemocnici. Zabrániť kyberútoku nie je jednoduché, firmy, ale aj inštitúcie by mali predvídať, tvrdí Suchý. „Nemali by sme podceňovať hrozby, ale preventívne sa chrániť, existujú mnohé riešenia, ktoré sú výrazne lacnejšie v porovnaní s odstraňovaním škôd po hackeroch, dôležitá je aj edukácia zamestnancov a pravidelné zálohovanie dát."

Obrana nestačí

Odborník upozorňuje, že dôležité je nielen účinne sa brániť, ale prípadný útok vôbec detegovať. Útočníci okrem viditeľného blokovania využívajú aj kradnutie citlivých dát. Podľa správy M-Trends 2021 je čas potrebný na odhalenie útočníka v systéme v priemere 24 dní, počas ktorého útočníci zbierajú veľké objemy firemných dát bez toho, aby o tom spoločnosť vôbec vedela.

„Skutočnosť, že firma má prísne bezpečnostné opatrenia, ešte neznamená, že sa nestane terčom útoku. Dôležité je, aby takýto útok vedela odhaliť, eliminovať a následne sa vrátiť do stavu podobného ako pred útokom," uzatvára Suchý.

SEVEROATLANTICKÁ ALIANCIA

Preverili nás v boji proti kybernetickým atakom

Bratislava – Národný bezpečnostný úrad, Centrum pre kybernetickú obranu, Národná agentúra pre sieťové a elektronické služby aj vládna jednotka Computer Security Incident Response Team Slovakia si preverili svoje schopnosti v boji proti kybernetickým hrozbám na cvičení Severoatlantickej aliancie Cyber Coalition 2021 s účasťou viac ako 1 000 partnerov z 26 členských štátov NATO, zo štyroch partnerských štátov a 16 organizácií. TASR o tom informovala Kristína Garaiová z kancelárie Národného bezpečnostného úradu.

Cieľom pravidelného cvičenia NATO je posilniť schopnosti čeliť hrozbám v kybernetickom priestore. Krajiny si vďaka nemu môžu overiť svoje zručnosti, taktiku a postupy. Slovenský tím tento rok koordinoval riaditeľ odboru vzdelávania, podpory a medzinárodnej spolupráce z Národného centra kybernetickej bezpečnosti SK-CERT Matej Šalmík.

„Nedávne výročné správy Slovenskej informačnej služby a Vojenského spravodajstva, ale aj poznatky Národného bezpečnostného úradu sú jasným dôkazom toho, že musíme neustále pracovať na profesionálnej a flexibilnej reakcieschopnosti nielen na národnej, ale najmä na medzinárodnej úrovni," skonštatoval riaditeľ úradu Roman Konečný. Ako doplnil Národný bezpečnostný úrad, kybernetická obrana je jednou z hlavných priorít Severoatlantickej aliancie v tomto desaťročí. Od svojho vzniku kladie dôraz na rýchlu, spoločnú a koordinovanú reakciu na akýkoľvek útok. Kybernetické hrozby nie sú výnimkou, ich sila a intenzita každý rok rastú. (TASR)

ANALÝZA

Firmy nezverejňujú krádeže dát pracovníkov

Bratislava – Hoci organizácie pravidelne čelia úniku údajov zamestnancov, 45 percent z nich tieto incidenty radšej nezverejňuje. Podobné je aj percento firiem, ktoré ponúka svojim zamestnancom školenia v oblasti kyberbezpečnosti, zamestnancom preto môžu chýbať základné vedomosti z tejto oblasti. Vyplýva to z globálneho prieskumu kyberbezpečnostnej spoločnosti Kaspersky.

Experti upozornili, že technológie sú síce dôležité pri predchádzaní kybernetickým útokom, ale ľudský faktor zohráva kľúčovú úlohu, keďže je spojený s 85 percentami incidentov. Aj keď sú u podvodníkov viac populárne krádeže údajov klientov, kyberzločinci obľubujú aj podvody spojené s odcudzením dát zamestnancov.

„V roku 2021 viac ako tretina organizácií nebola schopná

45
PERCENT

organizácií nezverejňuje úniky údajov zamestnancov.

zabezpečiť úplnú bezpečnosť údajov svojich zamestnancov a čelila incidentom súvisiacim s týmto typom informácií," poznamenala spoločnosť.

Skutočnosť, že 45 percent dotknutých organizácií nezverejnilo únik osobných údajov zamestnancov, je podľa expertov znakom toho, že problém je väčší, než sa zdá. Zvyšných 43 percent zverejnilo incidenty proaktívne a 12 percent po tom, ako to uniklo do médií. Odborníci pritom upozorňujú, že krízová komunikácia je v týchto prípadoch dôležitá, môže zmierniť priame finančné straty. (TASR)

PRIESKUM

Digitalizácia je podľa Európanov podstatná

Brusel – Prevažná väčšina občanov krajín EÚ si myslí, že internet a digitálne nástroje budú v budúcnosti zohrávať dôležitú úlohu. Vyplýva to z výsledkov osobitného prieskumu zo septembra a z októbra 2021, ktoré v pondelok zverejnil Eurobarometer. Prieskum na vzorke 26 530 respondentov z 27 členských štátov EÚ naznačil, že veľká väčšina Európanov považuje za užitočné, aby EÚ vymedzila a podporovala európske práva a zásady s cieľom zabezpečiť, aby bola digitálna transformácia úspešná.

Zo zistení prieskumu vyplýva, že 81 percent Európanov si myslí, že do roku 2030 budú digitálne nástroje a internet v ich živote dôležité, a viac ako 80 percent si myslí, že ich používanie prinesie aspoň toľko výhod ako nevýhod. Len malá menšina opýtaných očakáva, že pokiaľ ide o používanie digitálnych nástrojov a internetu do roku 2030, nad výhodami budú prevažovať nevýhody.

Viac ako polovica opýtaných má obavy z kybernetických útokov a počítačovej kriminality v podobe krádeže či zneužitia osobných údajov, škodlivého softvéru, phishingu. 53 percent z nich uviedlo, že má obavy o bezpečnosť a duševnú pohodu detí na internete. 46 percent občanov EÚ má zase obavy v súvislosti s používaním osobných údajov a informácií zo strany spoločností či verejnej správy.

Približne tretinu občanov EÚ znepokojujú ťažkosti súvisiace s odpojením sa a nájdením rovnováhy medzi životom online a offline a 26 percent má obavy zo získavania nových digitálnych zručností. Väčšina občanov si myslí, že EÚ chráni ich práva v online prostredí dobre. Takmer 40 percent si však nie je vedomých toho, že ich práva, ako sú sloboda prejavu, súkromie alebo nediskriminácia, by sa mali dodržiavať aj na internete. Občania by sa však chceli o nich dozvedieť viac. (TASR)

PREVENCIA

Kúpa darčekov sa stáva elektronickou záležitosťou, treba dbať na bezpečnosť

Bratislava – Nakupovanie darčekov pod stromček sa pre aktuálny lockdown vo veľkej miere presúva do online prostredia. Aj tu však treba dbať na bezpečnosť, aby sa predvianočné nákupy zbytočne nepredražili. Právnička z Inštitútu alternatívneho riešenia sporov Slovenskej bankovej asociácie Sylvia Ďatelinková napríklad radí platiť za objednaný tovar kartou. Umožní to pri nedodaní tovaru domáhať sa vrátenia peňazí. Ideálne je však vyhnúť sa pri nakupovaní cez e-shopy aj rôznym kyberpodvodom, vyzdvihla spoločnosť Flowmon Networks.

Aj nakupovanie darčekov môže byť nebezpečné. SNÍMKA: SHUTTERSTOCK

Ďatelinková spomenula, že platba kartou za online objednávky má viacero výhod. Ide napríklad o doplnkové služby, ktoré sú k nej často poskytované, ako napríklad poistenie zodpovednosti za škody pre prípad odcudzenia, straty, zneužitia alebo krádeže platobnej karty. „Platba kartou je výhodná aj v tom, že v prípade, ak natrafíte na nepoctivého obchodníka, ktorý vám objednaný tovar či službu nedodá alebo vám ich dodá v rozpore s dohodnutými podmienkami, máte ako držiteľ platobnej karty možnosť domáhať sa vrátenia peňažných prostriedkov prostredníctvom služby spätného zúčtovania platby, tzv. chargeback," vysvetlila Ďatelinková.

Pri platbe kartou, napríklad kuriérovi, treba podľa nej dbať na kontrolu výšky sumy uvedenej na termináli. Takisto radí zakryť klávesnicu terminálu pri zadávaní PIN kódu a hlavne nikomu svoj PIN kód neposkytovať ani si ho nikam nezapisovať. „Platobnú kartu môže používať výlučne jej držiteľ, preto ju neposkytujte iným osobám, a to ani rodinným príslušníkom," upozornila Ďatelinková. Hlavný konzultant Flowmon Networks Roman Čupka však upozornil aj na to, na čo by ľudia mali dbať pri nakupovaní, čo sa týka zabezpečenia kybernetickej bezpečnosti. Radí využívať výlučne osvedčených obchodníkov, a keď už si spotrebiteľ objednáva od neznámej značky, je dobré si overiť jej reputáciu a vyhľadať si recenzie. Takisto je podľa neho dôležité všímať si pred URL adresou ikonu zámku, ktorá signalizuje, že prenos údajov je zašifrovaný. „Ak ikona zámku chýba, je nebezpečné na takejto stránke zadávať údaje platobnej karty, heslá či iné osobné údaje," zdôraznil Čupka.

Nakupujúcim radí nevyužívať možnosť zapamätania si platobných údajov s cieľom urýchlenia ďalších nákupov. Pripomenul aj dôležitosť používania silných hesiel a aktualizácie operačného systému. „Povinnou výbavou každého počítača by mal byť aktualizovaný antivírusový program," dodáva hlavný konzultant Flowmon Networks. (TASR)