TLAČOVÁ SPRÁVA č. 05/2025
27. OKTÓBER 2025

Najčastejšou obeťou hekerov nie sú firmy, ale obyčajní ľudia

Mnohí majú dojem, že hekeri si vyberajú bohatých podnikateľov a veľké spoločnosti. Opak je však pravdou. Podľa odborníkov z oblasti kybernetickej bezpečnosti je najčastejšou obeťou obyčajný používateľ, ktorý klikne na nesprávny odkaz alebo používa rovnaké heslo na viacerých účtoch. Stačí málo a váš digitálny život má v rukách niekto iný, varuje Mária Krauhlecová, spoluzakladateľka konferencie o kybernetickej bezpečnosti Qubit Conference®.

Bratislava, 27.10.2025

Filmový obraz hekera, ktorý sedí v tmavej miestnosti a cez webkameru sleduje svoju obeť, patrí do sveta mýtov. Skutočné útoky sú omnoho tichšie, no o to nebezpečnejšie. „Ľudia si často predstavujú hekerský útok ako akčnú scénu, no v realite ide o systematické a nenápadné prenikanie do našich digitálnych životov. Niekedy ani netušíme, že niekto sleduje naše správy, polohu alebo dokonca ovláda celé zariadenie," vysvetľuje Mária Krahulecová, spoluzakladateľka Qubit Conference®. Podľa nej dnes už nejde len o jednorazové útoky, ale často o dlhodobé sledovanie. Stačí, aby útočník získal prístup k vášmu e-mailu, sociálnej sieti či cloudovému úložisku. „V tom momente vie čítať správy, sledovať fotografie a ticho sa prizerať každodenným aktivitám obete. Ak sa mu podarí získať aj prístup k GPS alebo fitness aplikáciám, má prehľad, kedy ste doma, v práci či na dovolenke," upozorňuje Krahulecová.

Keď útočník ovláda celé zariadenie

Nepríjemné sú aj prípady, keď útočník získava úplnú kontrolu nad zariadením. „Vtedy môže zapínať kameru a mikrofón, sťahovať súbory, dokonca odosielať správy alebo meniť obsah v zariadení. V iných prípadoch prebieha nenápadný zber dát na pozadí. Sú to heslá, platobné údaje či fotografie, ktoré sa odosielajú na server hackerov bez toho, aby si to používateľ všimol," hovorí Krahulecová. Väčšina ľudí zistí, že niečo nie je v poriadku, až keď je neskoro. „Varovné signály sú pritom pomerne jasné. Ide o notifikácie o prihláseniach z neznámych zariadení, rýchle vybíjanie batérie, zvláštne správy od kontaktov, neznáme aplikácie v telefóne či výrazné spomalenie internetu. To všetko môže znamenať, že zariadenie je kompromitované," upozorňuje organizátorka konferencií o kybernetickej bezpečnosti.

Heknutie je v roku 2025 jednoduchšie, než kedykoľvek predtým

Rok 2025 priniesol zásadnú zmenu. „Kedysi musel byť heker špičkovým programátorom. Dnes si vie hotový softvér stiahnuť alebo kúpiť na internete aj úplný začiatočník. Nástroje majú grafické rozhrania podobné bežným aplikáciám, takže ich použitie je otázkou niekoľkých kliknutí. Hekeri už nemusia ručne skúšať heslá. Softvéry dokážu prehľadávať milióny účtov a hľadať slabé miesta. Hovoríme o credential stuffing útokoch, kde sa testujú uniknuté heslá z iných služieb," hovorí M. Krahulecová.

Umelá inteligencia navyše zmenila spôsob sociálneho inžinierstva. „AI dnes vie vytvoriť falošný e-mail, hlas alebo dokonca deepfake video. Predstavte si, že účtovníčka dostane telefonát od 'riaditeľa', ktorý ju presviedča, aby okamžite previedla peniaze a hlas znie úplne autenticky," hovoria príklady odborníci na kybernetickú bezpečnosť. Častým omylom je, že hekeri sa zameriavajú len na veľké firmy alebo bohatých ľudí. „Najčastejšou obeťou je obyčajný človek. Dôvod je prostý. Bežní používatelia majú slabú ochranu, používajú jednoduché heslá a často sa nechajú nachytať na podvodné správy. Pre útočníkov je jednoduchšie a výnosnejšie cieliť na tisíce takýchto obetí naraz," vysvetľuje Krahulecová.

Slovenské štatistiky hovoria jasne

Na Slovensku sa tento trend potvrdzuje aj v číslach. „Podľa NBÚ bolo v roku 2024 zaznamenaných viac než 4 000 kybernetických incidentov, väčšina z nich smerovala na bežných používateľov prostredníctvom phishingu a smishingu. ESET zase upozorňuje, že priemerné heslo používateľa má len osem znakov a až 20 percent ľudí používa rovnaké heslo na viacerých účtoch," uvádza Krahulecová.

Obete útokov často prichádzajú o peniaze práve cez podvodné SMS či e-maily. Môže ísť o správy že vaša zásielka čaká na colnici, alebo upozornenia na podozrivý prístup k účtu, to všetko sú klasické triky hekerov. Po kliknutí na odkaz si stiahnete škodlivý softvér alebo rovno odovzdáte svoje prihlasovacie údaje. Veľmi rozšírené sú aj falošné súťaže na sociálnych sieťach či škodlivé aplikácie v mobiloch.

Cielené útoky na konkrétne osoby a firmy

Okrem masových útokov existujú aj cielené. „Tu ide o pripravené kampane proti konkrétnym osobám alebo firmám. Útočníci sa vydávajú za člena rodiny cez deepfake hovor, predstierajú obchodnú ponuku na LinkedIne alebo posielajú špeciálne pripravený e-mail jednému jedinému človeku vo

firme. Typickými obeťami sú manažéri, účtovníci, novinári, právnici či politici," vymenúva Krahulecová.

Mnohí ľudia si myslia, že nemajú nič, čo by hekerov zaujímalo. „Opak je pravdou. Aj váš e-mail a heslo majú hodnotu. Môžu byť predané na čiernom trhu. Prístup k bankovému účtu je okamžitým ziskom, sociálne siete slúžia na šírenie ďalších podvodov a súkromné fotografie môžu byť využité na vydieranie. Stačí kliknúť na nesprávny odkaz, použiť slabé heslo alebo odložiť aktualizáciu systému a prístup k dátam je v rukách útočníka," upozorňuje.

Problém sa netýka len jednotlivcov, ale aj firiem. „Mnohé podniky si myslia, že ich sa to netýka. V skutočnosti sú však malé a stredné firmy čoraz častejším cieľom, pretože nemajú dostatočne vybudovanú ochranu. Riziká sú obrovské. Od úniku údajov zákazníkov cez poškodenie reputácie, finančné straty až po sankcie za porušenie GDPR. Prevencia sa pritom vo firmách často začne riešiť až po prvom útoku," upozorňuje Krahulecová.

Čo robiť, ak máte podozrenie na sledovanie

Čo robiť, ak máte podozrenie, že vás niekto sleduje? „Základom je okamžite odpojiť zariadenie od internetu. Potom z iného zariadenia zmeniť všetky heslá, zapnúť dvojfaktorovú autentifikáciu a spustiť antivírusovú kontrolu. V prípade firemného zariadenia treba kontaktovať IT oddelenie a pri vážnych útokoch sa obrátiť na políciu alebo SK-CERT," radí. Najčastejšou chybou je podľa Krahulecovej neopatrnosť používateľov: „Ľudia používajú slabé alebo rovnaké heslá, klikajú na neznáme odkazy, neaktualizujú si systémy a zdieľajú príliš veľa osobných údajov na sociálnych sieťach. Aj dátum narodenia či meno domáceho miláčika môže byť indícia pre hekera, ako prelomiť zabezpečenie účtu.

Digitálna hygiena pre všetkých

Prevencia sa dá prirovnať k hygiene. Odborníci sa zhodujú. Že kybernetická bezpečnosť by mala byť rovnako samozrejmá ako umývanie rúk. Deti by mali vedieť rozoznávať podvodné správy, tínedžeri by mali používať dvojfaktorovú autentifikáciu a premýšľať, čo zdieľajú online. Seniori si musia dávať pozor na falošné hovory z 'banky' a neotvárať podozrivé e-maily. Firmy zase potrebujú pravidelné školenia, simulované phishingové útoky a jasné bezpečnostné politiky. Vzdelávať sa v oblasti kyberbezpečnosti je podľa Krauhlecovej nevyhnutné : „Len tak môžeme držať krok s útočníkmi, ktorí využívajú stále sofistikovanejšie metódy. Jedným z podujatí, kde možno získať praktické vedomosti, je Qubit Conference®, ktorá je už tradične platformou pre odborníkov aj širokú verejnosť."

Najčastejšie spôsoby sledovania

Prístup k súkromným účtom – získanie prístupu do e-mailu, sociálnych sietí, cloudov, Messengera či WhatsAppu.

Sledovanie polohy – zneužitie GPS, fitness aplikácií alebo prihlásení cez Google/Apple/Facebook.

Odpočúvanie hovorov a správ – pri sofistikovaných útokoch môže útočník monitorovať komunikáciu v reálnom čase.

Úplná kontrola zariadenia – aktivácia kamery/mikrofónu, sťahovanie súborov, odosielanie správ.

Tichý zber dát – pozadie, kde sa odosielajú heslá, platobné údaje a fotografie na server útočníkov.

5 varovných signálov, že môžete byť heknutý

Nezvyčajná aktivita účtov — notifikácie o prihláseniach z neznámych zariadení, zmenené heslá alebo správy odoslané bez vášho súhlasu.

Rýchle vybíjanie batérie/prehriatie zariadenia — na pozadí môže bežať škodlivý softvér.

Podivné správy od vašich kontaktov — známi dostávajú od vás neznáme odkazy alebo správy.

Neznáme aplikácie alebo programy — v zariadení sú aplikácie, ktoré ste neinštalovali.

Spomalenie internetu alebo zariadenia — náhle výrazné spomalenie bez zjavnej príčiny.

Najčastejšie formy útokov na bežných ľudí

Smishing (podvodné SMS) — výzvy k stiahnutiu príloh alebo kliknutiu na škodlivé odkazy.

Phishing e-maily — falošné správy pôsobiace ako od bánk alebo inštitúcií.

Falošné súťaže a formuláre so žiadosťami o osobné údaje.

Malware v aplikáciách — obzvlášť na Android zariadeniach.

Čo robiť, ak máte podozrenie, že vás sledujú

Okamžite odpojte zariadenie od internetu.

Z iného (bezpečného) zariadenia zmeňte heslá ku všetkým účtom — používajte dlhé a jedinečné heslá.

Zapnite dvojfaktorovú autentifikáciu (2FA) na všetkých službách, kde je to možné.

Spustite antivírusový a antimalware sken.

Kontaktujte odborníka alebo IT oddelenie, ak ide o firemné zariadenie.

Pri vážnych útokoch nahláste incident polícii a Národnému centru kybernetickej bezpečnosti (SK-CERT).

Najčastejšie chyby používateľov

Používanie slabých a opakujúcich sa hesiel.

Klikanie na neznáme odkazy a prílohy.

Nepoužívanie 2FA a neaktualizovanie OS a aplikácií.

Nadmerné zdieľanie osobných údajov na sociálnych sieťach (dátumy, mená domácich zvierat atď.).