INFORMÁCIA
K PREVENCII VOČI KYBERNETICKÝM HROZBÁM

EDYMAX Security Management s.r.o. po skúsenosti s útokmi hackerov na iné spoločnosti posilnil ochranu voči kybernetickým hrozbám. Najlepšia forma obrany je prevencia a zvýšenie povedomia o kybernetickej bezpečnosti. Informácia je určená najmä najohrozenejším skupinám používateľov internetu, ako sú neskúsení tínedžeri, seniori a malí a strední podnikatelia, ktorých chceme vystríhať pred počítačovou kriminalitou.

Čo je to hacker?

Jednoducho veľmi schopný programátor, ktorý je odborníkom na manipuláciu počítačových sietí a počítačových systémov. Naším cieľom je vystríhať pre hackermi, ktorí majú jednoznačne zlý úmysel ako poškodenie, manipuláciu, krádež alebo zneužitie identity alebo vydieranie.

O čo hackerovi ide?

Verte tomu alebo nie, vaše zariadenie obsahuje množstvo cenných údajov, ktoré môžu použiť alebo predať hackeri po celom svete:

- Osobné identifikovateľné informácie
- Obchodné informácie (obchodné tajomstvo)
- Internetová aktivita a návyky pri prehliadaní
- E-maily a sociálne siete
- Údaje, ktoré umožňujú prístup k pripojeným zariadeniam

Dnes je takmer nemožné vyhnúť sa dosahu hackerov alebo kyber zločincom. Každý jednotlivec však môže urobiť opatrenia, na ktoré nepotrebuje žiadne IT alebo technologické vzdelanie a ktoré dokážu útok minimalizovať, ideálne mu predísť. Hacker môže narobiť veľa škody, aj keď je napadnutý iba jeden účet alebo jedno zariadenie. Aby toho nebolo málo, hackerov je ťažké zastaviť, pretože sa často nachádzajú mimo krajiny, na ktorej obyvateľov útočia a využívajú najmodernejšie technológie, aby nebolo možné odhaliť ich identitu. Opatrnosť je na prvom mieste. Škodlivé odkazy môžu prísť od vašich priateľov, kolegov či obchodných partnerov na sociálnych sieťach, ktorých súkromné účty boli kompromitované alebo inak zneužité. Je dôležité brať na zreteľ, že ľudia, ktorých „stretnete“ na sociálnych sieťach, nemusia byť vždy tými, za koho sa vydávajú. Falošné profily na sociálnych sieťach sú populárnym nástrojom kyber zločincov.

Silné a unikátne heslo

Ideálny počet znakov v hesle je minimálne 16. Odporúčame taktiež používanie hesiel, ktoré obsahujú čísla alebo iné znaky. Nikdy nepoužívajte rovnaké heslo pre viacero stránok a služieb. Vytvorte si silné, hackermi neodcudziteľné heslo pre každý online účet. Na hesle si dajte záležať, čím originálnejšie a špecifickejšie, tým lepšie. Nikdy nepoužívajte rovnaké heslo do vašich účtov sociálnych sietí ako do vášho e-mailového konta. Ak hackeri prelomia prihlasovacie údaje, napríklad do vašej sociálnej siete, ľahko sa potom dostanú aj do vášho e-mailu. Platí to aj opačne.

Nainštalujte si antivírusový softvér

Antivírusový softvér zohráva hlavnú úlohu pri ochrane vášho systému tým, že zisťuje hrozby v reálnom čase, aby zaistil bezpečnosť vašich údajov. Niektoré pokročilé antivírusové programy poskytujú automatické aktualizácie, čím ďalej chránia váš počítač pred novými vírusmi, ktoré sa objavujú každý deň. Po nainštalovaní antivírusového programu ho nezabudnite použiť.

Sťahovanie neznámych súborov

Ak si nie ste istí zdrojom, nepoužívajte odkaz ani neotvárajte prílohu. Obľúbenou formou útoku od kyber zločincov je, aby ste si nevedome stiahli do svojho zariadenia malvér. Maskujú ho do programov a aplikácií, pričom po jeho stiahnutí sa snažia odcudziť informácie. Nesťahujte súbory a aplikácie z nedôveryhodných zdrojov a buďte skeptickí voči súborom, ktorých obsah nepoznáte.

Pravidelné aktualizácie

Aktualizácie môžu byť nepríjemné a časovo náročné, ale sú kľúčové, ak chcete zachovať bezpečnosť vášho systému na najvyššej úrovni. Aktualizácia zvyčajne opravuje zraniteľnosť systému alebo aplikácie, ktorú hackeri vytvorili. Môžete zvážiť povolenie automatickej aktualizácie, aby ste zaistili, že vaše zariadenie bude mať najaktuálnejšiu bezpečnostnú ochranu. Majte na pamäti, že aplikácie tretích strán by sa mali pravidelne aktualizovať, rovnako ako celý systém.

Znížená digitálna stopa

Venujte pozornosť informáciám, ktoré dávate online na svoje sociálne siete: zhromažďujú o vás viac údajov ako ktorákoľvek iná aplikácia. Čím menej informácií o vás môžu hackeri zhromaždiť, tým ste bezpečnejší. Zníženie množstva dostupných informácií o vašom živote online vám môže pomôcť znížiť riziko napadnutia. Na internete súkromie neexistuje. Všetko, čo uverejníte, tam aj zostane.

Tu je niekoľko tipov, ktoré môžete použiť na zvýšenie bezpečnosti:

- Vypnite sledovanie polohy a automatické geografické označovanie. Používajte ich len v prípade potreby.
- Webové prehliadače - Dodržiavajte overené zásady bezpečnosti. Všímajte si štruktúru adresy webstránky. Ak adresa začína s https://, jedná sa o zabezpečenú komunikáciu v počítačovej sieti. Rozhodne však neklikajte na rôzne odkazy, ktoré vás tvrdia, že vás po kliknutí čaká akási výhra.
- Video konferencie - Svoje videohovory si zabezpečte heslom alebo PIN kódom a zamedzte možnosť pripojiť sa cudzím ľudom. Uistite sa, že na hovore sú len účastníci, ktorí boli pozvaní.
- Odhláste sa zo starých alebo nechcených služieb a e-mailov.
- Nereagujte na podozrivo vyzerajúce emaily, ktoré môžete obdržať napríklad aj v mene vašej banky, poisťovne, či operátora.
- Udržujte svoje účty súkromné a obmedzte obsah iba na skutočných priateľov.
- Venujte pozornosť žiadostiam o priateľstvo. Ak je to možné, obmedzte, kto vám môže posielať tieto žiadosti.
- Nikdy nezdieľajte osobné informácie alebo informácie súvisiace s účtom, buďte opatrní pri tom, čo uverejňujete na sociálnych sieťach a čo hovoríte ostatným.
- Buďte opatrní pri fotografiách, nezobrazujte žiadne identifikačné informácie, ako sú adresy alebo telefónne čísla.
- Používajte bezpečné WiFi pripojenie. Verejná WiFi môže byť nebezpečná. Hacker môže vytvoriť vlastné WiFi pripojenie s rovnakým názvom ako oficiálna sieť a kradnúť údaje každému, kto sa pripojí. Všetka komunikácia totiž v tom prípade ide cez

útočníkov počítač. Verejnú WiFi používajte len v prípade, ak potrebujete nájsť nevyhnuté údaje a v žiadnom prípade sa cez verejnú WiFi neprihlasujte na stránky, ktoré vyžadujú prihlasovacie údaje, taktiež nerealizujte žiadne platby alebo prihlásenia do internet bankingu a pod.

Čo mám robiť, ak sa stanem obeťou útoku?

- Odpojte všetky zariadenia a prístroje od elektrickej siete.
- Kontaktujte správcu Vašich zariadení a prístrojov (IT podpora).
- Nekomunikujte sami s hackerom, neplaťte výkupné.
- Neobnovujte dáta, nezapínajte zariadenia a prístroje predtým, ako ich skontroluje IT podpora.
- Oznámte Úradu na ochranu osobných údajov únik osobných údajov - bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín od okamihu, ako sa dozvedel, že došlo k porušeniu ochrany osobných údajov – jedná sa o povinnosť vyplývajúcu z všeobecného nariadenia o ochrane osobných údajov – Nariadenia GDPR.

Sú škody spôsobené kybernetickým útokom kryté v poistení majetku a zodpovednosti firiem?

Štandardné poistenie majetku a zodpovednosti za škody nekryje náklady spojené hackerským útokom. Poisťovne ponúkajú Poistenie kybernetických rizík, ktoré kryje napr. nasledovné:

- ✓ Porušenie ochrany dát (náklady na manažéra celého incidentu, IT forenzných expertov, komunikáciu so štátnymi orgánmi, PR služby, právnu obhajobu).
- ✓ Obnova dát (náklady na obnovu dát a poškodeného softvéru).
- ✓ Prerušenie prevádzky (ušlý zisk, fixné náklady).
- ✓ Vydieranie (úhrada výkupného, ak je to potrebné).
- ✓ Zodpovednosť za porušenie ochrany dát (nárok poškodeného z dôvodu porušenia ochrany dát v súvislosti s dôvernými informáciami alebo z dôvodu porušenia platnej legislatívy - GDPR).
- ✓ Zodpovednosť za bezpečnosť sietí (nárok poškodeného z dôvodu kyber-útoku na PC systém poisteného, ktorý spôsobil poškodenie, zničenie, odcudzenie údajov poškodeného alebo útok typu DoS na PC systémoch poškodeného).
- ✓ Kybernetický zločin (náhrada odcudzených peňažných prostriedkov z bankového účtu).
- ✓ Štandardy PCI-DSS (penále od poskytovateľa platobnej karty – VISA, MASTERCARD – a náklady na dokázanie porušenia štandardov, opätovnú certifikáciu a vystavenie platobnej karty poškodenému) – vhodné prípade, ak spracovávate platby cez platobné terminály
- ✓ Zodpovednosť z používania médií (nárok poškodeného z dôvodu ohovárania/ poškodenia dobrého mena, porušenia autorského práva a porušenia práv na ochranu súkromia) v prípade Vašich aktivít v online prostredí.