ABECEDA
BEZPEČNOSTNÉHO POVEDOMIA

A AKTUALIZUJTE A PLÁTAJTE

Váš počítač, smartfón, wifi router a všetky IT zariadenia musia mať vždy nainštalované posledné verzie aktualizácií a záplat operačného systému. Týka sa to aj internetového prehliadača a všetkých aplikácií. Hackeri ako prvé hľadajú známe zraniteľnosti v neaktualizovaných systémoch, čiže bezpečnostné diery, a tie treba plátať.

B BUĎTE OSTRAŽITÍ

Pred kliknutím na akýkoľvek odkaz v správe elektronickej pošty si overte, kam tento odkaz naozaj smeruje.

C COOKIES PATRIA DO KOŠA

Pravidelne vymazávajte cookies a vymažte históriu internetového prehliadača. Aj keď je technológia „cookies" regulovaná európskym právom, mnohí prevádzkovatelia svoje povinnosti nedodržiavajú.

D DODRŽUJTE PRAVIDLÁ

Bezpečnostné politiky vašej organizácie a odporúčania informatikov a „bezpečákov" nie sú samoúčelné. Obchádzanie pravidiel vám možno zvýši používateľský komfort, avšak pravidlá vám zaručia súkromie a bezpečnosť vašich cenných údajov.

E E-MAIL NIE JE BEZPEČNÝ

Správa elektronickej pošty je ako korešpondenčný lístok. Nikdy nemáte istotu, že odosielateľom je ten, za koho sa vydáva. Obsah správy môže prečítať množstvo neznámych ľudí. Pokiaľ nepoužívate šifrovaný e-mail, vážte informácie, ktoré odosielate.

F FILTRUJTE SPAM

Nástroje na „odchytávanie" nevyžiadaných a škodlivých správ elektronickej pošty znižujú riziko infiltrácie a ohrozenia vášho systému.

G GROOMING

Chráňte sa pred groomingom. Výraz „groom" znamená „pripraviť na špecifickú pozíciu alebo účel" či „pripraviť na budúcu rolu alebo funkciu". Groomingom si útočník „pripravuje" dieťa, rodinu, komunitu tak, aby mohol neskôr realizovať sexuálne zneužívanie. Iným slovami je to pestovanie si vzťahu a budovanie dôvery medzi sexuálnym predátorom a jeho obeťou.

H HESLÁ A HESLOVÉ VETY

Silné heslá sú tie, ktoré nikto neuhádne a zároveň si ich pamätáte. Vytvorte heslá, ktoré majú aspoň 15 znakov a obsahujú kombináciu veľkých a malých písmen, číslic a symbolov, ak to aplikácia umožňuje. Heslovou vetou môže byť napríklad citát, alebo text skladby, kde nahradíte aspoň jedno písmeno špeciálnym znakom a pridáte číslice.

CH CHRÁŇTE SÚKROMIE

Sociálne siete navádzajú k tomu, aby ste prezradili o sebe čo najviac. Výsledkom bývajú vykradnuté domácnosti počas dovolenky, odcudzené peniaze z bankových účtov, ale aj sexuálne vydieranie či ujma na duševnom zdraví dieťaťa, napríklad prostredníctvom kyberšikany. Rešpektujte zároveň právo na súkromie iných ľudí.

I INŠTALUJTE SI ANTIVÍRUS

Voči útoku škodlivým kódom vás obránia najmä antivírusové aplikácie. Nainštalujte si niektorú z nich a nastavte ju tak, aby automaticky kontrolovala prístupy na webové stránky, sťahované súbory, prílohy e-mailov a pamäťové médiá.

J JE TO PRAVDA?

Hoax je podvodná správa, zámerne konštruovaná tak, aby pôsobila ako dôveryhodná a objektívna pravda. Táto technika využíva manipuláciu na zneužitie vlastností ľudského rozhodovania.

K KONTROLUJTE ADRESY

Pred otvorením webovej stránky vždy najprv skontrolujte adresu. Nespúšťajte neznáme odkazy. Podhodenie adresy a presmerovanie na nebezpečnú webstránku je typickým spôsobom prípravy útoku. Neotvárajte neznáme prílohy a linky v správach, väčšinou je ich obsahom škodlivý kód.

L LIMITUJTE ZDIEĽANIE

Obmedzte množstvo zdieľaných dát, či už prostredníctvom sociálnych sietí, alebo rôznych cloudových služieb. Ak niečo zdieľate, vymedzte presne osoby, ktorým zdieľané údaje sprístupníte. A po čase prehodnotíte, či zdieľanie zdroja je naďalej potrebné – a ak nie je, ukončite zdieľanie.

M MONITORUJTE

Ak sa vám stala nepríjemná udalosť v online priestore, uistite sa, že máte všetky dôkazy o bezpečnostnom incidente napr. e-maily, faktúry, potvrdenky, kópie reklamy atď. Nahláste podvod. Vaše informácie môžu pomôcť chytiť podvodníka a zabrániť ďalším incidentom.

N NEDÔVERUJTE

Mnohé z toho, s čím sa v elektronickom svete stretnete, je pochybné a nedôveryhodné. Internet je slobodným neregulovaným priestorom a každý si v ňom môže písať, publikovať a tvrdiť takmer čokoľvek. Preto je k internetovým médiám dobré pristupovať so zdravou skepsou a odstupom.

O ONLINE NÁKUPY

Skontrolujte, či sa adresa e-shopu začína na „https", a všímajte si pravopisné či gramatické chyby. Overte si, či sú v rubrikách, ako napríklad „O nás" alebo „Kontakt" uvedené legitímne kontaktné údaje. Dávajte si pozor na mimoriadne ponuky a informujte sa, aké skúsenosti majú s e-shopom iní zákazníci.

P PRIHLASUJTE SA 2-STUPŇOVO

Ak to webová služba umožňuje, používajte na prihlasovanie tzv. dvojfaktorovú autentizáciu (napríklad pomocou SMS kódu). Samotné heslo nie je už dostatočnou ochranou pred zneužitím prístupových práv.

R RANSOMVÉR JE VYDIERANIE

Ransomvér je druh malvéru, ktorý napáda počítačové systémy používateľov a zaobchádza s nimi tak, aby tieto systémy alebo dáta na nich uložené obeť nemohla (čiastočne alebo úplne) používať. Väčšinou sa to deje zašifrovaním veľkej časti údajov. Obeť zvyčajne neskôr dostane výhražnú správu, ktorá ju tlačí k zaplateniu výkupného, pokiaľ chce získať plný prístup k systému a súborom späť.

S SOCIÁLNE INŽINIERSTVO

Ľudská dôvera sa ľahko zneužíva na získanie prístupu k citlivým informáciám. Typická je forma podvodných mailov – phishing. Najlepšou ochranou pred sociálnym inžinierstvom je zvyšovanie bezpečnostného povedomia.

T TRÓJSKY KÔŇ

Škodlivý softvér, ktorý je podobný trójskemu koňovi známemu zo starovekých gréckych bájí. Aby zakryl svoju skutočnú funkciu, využíva maskovanie alebo presmerovanie. Tento malvér sa najčastejšie dostane do počítača nezodpovednosťou alebo neopatrnosťou samotného používateľa. Neotvárajte e-maily a nespúšťajte súbory, ktoré nepoznáte.

U UZAMYKAJTE ZARIADENIA

Zariadenie, ktoré nie je pod vašou fyzickou kontrolou, dáva priestor útočníkovi. Odomknuté zariadenie bez dozoru dáva komukoľvek priestor k manipulácii s ním a s jeho obsahom. Toto je potrebné uvedomiť si nielen v kancelárii, ale predovšetkým na verejných miestach (napr. na konferencii, vo vlaku a pod.).

V VZDELÁVAJTE SA

Kybernetické hrozby sú každodennou súčasťou online života, nielen v práci, ale aj v súkromí. Aby sme ich vedeli rozpoznať a účinne sa proti nim brániť, je dôležité sa pravidelne vzdelávať aj v oblasti kybernetickej bezpečnosti.

W WIFI NIE JE BEZPEČNÁ

Wifi sieť môže byť bezpečná, len ak je správne nakonfigurovaná. Nechránené wifi siete bez hesla a šifrovania sú ako dokorán otvorené dvere do bytu. Zmeňte aj pôvodný továrenský názov vášho routera a zároveň sa vyvarujte použitiu takého názvu, ktorý by vás identifikoval. Oboje totiž hackerovi zjednoduší útok.

Z ZÁLOHUJTE DÁTA

Aj pamäťové médiá sa občas pokazia a ich obsah sa stratí. Zároveň sa zvyšuje počet tzv. ransomvérových útokov, keď hackeri zašifrujú údaje a za ich vrátenie vyžadujú výkupné. Proti týmto hrozbám je účinná len obnova údajov z pravidelne vytváraných záloh.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

CSIRT.SK www.csirt.gov.sk

SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI www.sk-cert.sk

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY www.dataprotection.gov.sk

AKB www.akb.sk

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti www.cybercompetence.sk

ISBN 978-80-69011-17-5

Verzia V.1