Vedeli ste že...

V súčasnosti využíva internet drvivá väčšina Slovákov, bohužiaľ málo kto z nich si uvedomuje, že môže byť cez jeho zariadenie (počítač, notebook, telefón,...) zraniteľný. Jeho dáta môžu byť odcudzené a zneužité. Preto je dobré dbať na bezpečnosť a mať tieto zariadenia zabezpečené a aktualizované. Preto odporúčame využívať aspoň nasledovné základné pravidlá zabezpečenia, na základe čoho viete predísť veľkému množstvu útokov a následnému zneužitiu vašich dát.

1. ...kliknutie bez premýšľania je riskantné ?

Internet poskytuje veľmi veľa možností, preto si dávajte pozor na to, čo vám pristane v e-mailovej schránke, prípadne čo nájdete na webových stránkach. To, že môžete kliknúť, neznamená, že by ste aj mali. Kliknutie na škodlivé odkazy vám môže spôsobiť veľa nepríjemností, ako napríklad zašifrovanie, stratu, odcudzenie a následné zneužitie vašich súkromných alebo firemných dát. Preto pred kliknutím na odkaz ho skontrolujte a uistite sa, že pochádza od dôveryhodných odosielateľov. V prvom rade si treba všimnúť, či adresa odkazu začína na HTTPS. Pri http je väčšia pravdepodobnosť možnosti škodlivého odkazu. Špecifickým znakom vyššej dôveryhodnosti stránky je zelený alebo šedý kľúčik (zámok) pri adrese web stránky.

Dávajte si pozor najmä na maličké preklepy alebo pridania písmeniek v známych slovách. Odkazy v e-mailoch sú bežným nástrojom, ktorý útočníci používajú na podvádzanie jednotlivcov. Tieto odkazy sú často prezentované ako smerujúce na bankové výpisy, faktúry, letové alebo hotelové rezervácie, e-maily na obnovenie hesla, výhry telefónov, peňazí a ďalšie. Tento typ útoku sa nazýva aj phishing. **Ak sa vo vašej emailovej schránke objaví podozrivý email ktorého legitímnosťou si nie ste istí, nepreposielajte ho kolegom. Nahláste to vášmu IT oddeleniu prípadne kontaktnej osobe ktorá je oprávnená na komunikáciu s Vládnou jednotkou CSIRT.**

2. ...je vhodné dávať pozor na svoje okolie ?

Dávajte pozor na svoje zariadenie. Zamknite ho (klávesová skratka „*Windows klávesa + L*“) vždy, keď od neho odchádzate čo i len na 2 minúty. Nikdy nenechávajte na vašom pracovnom stole a v jeho blízkosti citlivé položky, ako USB kľúče, externé disky. Svoje heslá si nepíšte na lístočky, alebo do diárov. Tak isto treba byť obozretný pri zadávaní hesla a overiť si, či sa niekto nepozerá.

3. ...je potrebné držať sa svojich vlastných pracovných zariadení ?

Pokúste sa obmedziť používanie zariadenia iného používateľa. Neodporúčame napríklad politiku viac používateľov pracujúcich na jednom fyzickom zariadení. Snažte sa vždy pracovať na vám pridelenom zariadení. Vyvarujte sa prihlasovaniu do svojich účtov alebo aplikácií prostredníctvom neznámych pracovných staníc alebo notebookov. Zdieľanie zariadenia viacerými používateľmi je bezpečnostné riziko. Nikdy nezdieľajte svoje prihlasovacie údaje s ostatnými a nikdy nikomu nedávajte vzdialený prístup k počítaču ani v rámci vášho IT oddelenia (pokiaľ interné dokumenty toto vášmu IT oddeleniu nepovoľujú).

4. ...je nutné držať krok s aktualizáciami ?

Opravy softvéru resp. aktualizácie systému Windows a softvéru tretích strán sa vydávajú vždy, keď sa zistia bezpečnostné chyby alebo zraniteľnosti v softvéri. Samozrejme všetci vieme, že upozornenia na aktualizácie Windows sú vyrušujúce, no reštart systému je v tomto prípade menšie zlo, ako riskovanie infekcie škodlivým kódom.

5. ...sa máte pripájať bezpečne ?

Mnoho tipov a upozornení týkajúcich sa tejto časti kybernetickej bezpečnosti, bolo prezentovaných odborníkmi na kybernetickú bezpečnosť, no i napriek tomu to málo kto dodržiava. Na neznáme WiFi siete chránené heslom sa prihlasujte len vo výnimočných prípadoch. Pokiaľ pracujete s citlivými dátami alebo firemnými dátami a e-mailmi, nemali by ste takéto pripojenie vôbec využívať. **K nezabezpečeným WiFi sieťam sa nepripájajte vôbec na žiadnych zariadeniach.** V prípade že nemáte inú možnosť a musíte sa pripojiť na verejnú WiFi, tak sa pripájajte výhradne len cez Virtual Privat Network, skrátene VPN. Viac o prípadnej potrebe používania VPN pripojenia sa obráťte na vaše IT oddelenie, ktoré Vám poskytne potrebné informácie.

6. ...aj mobilné zariadenie treba mať zabezpečené ?

Zabezpečenie nekončí len pri vašom počítači. Je dôležité si zvyknúť zabezpečovať aj svoje mobilné zariadenie. Odomykanie mobilného zariadenia „vzorom“ už nie je v súčasnosti dostatočne bezpečné. Odporúča sa zabezpečenie minimálne PIN kódom/heslom. Ochrana odomknutia PIN kódom/heslom, by mala byť dnes samozrejmosťou na každom vašom zariadení. Optimálne je pridať takúto ochranu aj pri štarte zariadenia, prípadne zapnúť šifrovanie zariadenia. Pokiaľ ide o mobilné zariadenia, je odporúčané pridať aj dodatočné biometrické funkcie zabezpečenia. Odomykanie tvárou (ak to výrobca odporúča), IRIS sken očnej dúhovky prípadne odomykanie otlačkom prstu. Taktiež je dobré mať vypnutý Bluetooth na zariadení a zabrániť, aby sa zariadenie pripájalo k verejným WiFi sieťam automaticky. Ideálne je vypnúť automatické pripájanie na WiFi siete úplne a pripájať sa vždy manuálne. Aj v tomto prípade platí, že ak sa pripájate cez telefón na verejné WiFi, tak ideálne za použitia VPN pripojenia. Ak si sťahujete do telefónu aplikácie, tak výhradne len cez autorizovanú digitálnu distribučnú platformu (Google Play, Apple AppStore, Microsoft Store).

7. ...si musíte dávať pozor na sociálne inžinierstvo ?

Keď útočníci nemôžu nájsť zraniteľnosť v zabezpečení, zaútočia inými spôsobmi. Sociálne inžinierstvo je umenie využívať psychológiu človeka, namiesto **technických spôsobov útoku** na získanie prístupu do budov, systémov, zariadení. Napríklad namiesto toho, aby sa sociálny inžinier - útočník snažil nájsť zraniteľnosť softvéru, môže jednoducho zavolať zamestnancovi a predstaviť sa ako osoba pracujúca na vašom IT a pokúsiť sa vás oklamať, aby ste prezradili vaše prihlasovacie údaje, osobné alebo firemné informácie pod zámienkou pomoci.
Tento typ útoku je skôr útokom na myseľ používateľa, ako na jeho zariadenie. Najmä s informáciami verejne dostupnými online a prostredníctvom sociálnych médií prichádzajú počítačoví zločinci s tvorivými spôsobmi, ako napodobňovať používateľov, alebo vašich známych. **Majte na pamäti, že vaši pracovníci IT oddelenia nepotrebujú od vás nikdy vaše heslo k zariadeniam**. Ak niekto zavolá alebo pošle e-maily so žiadosťou o citlivé informácie, je nutnosťou povedať nie. Pred poskytnutím akýchkoľvek informácií si overte komu ich naozaj poskytujete. Napríklad tým, že takýto telefonát prerušíte a zavoláte konkrétnej osobe, ktorá tieto informácie požaduje. Týmto overíte, či to naozaj bola ona.

8. ...už osem znakov nestačí ?

Používajte bezpečnú kombináciu znakov a nepoužívajte rovnaké heslo na viacerých weboch alebo systémoch. Heslo by malo ideálne obsahovať aspoň 16 znakov. Nezdieľajte svoje heslo s ostatnými. Najideálnejšia forma uchovávania hesla je si ho zapamätať. Ak to nie je možné, tak si ho zapíšte a odložte na bezpečné miesto, ideálne uložené v zalepenej obálke podpísanej cez prelep a zamknuté v skrini alebo trezore. Buďte kreatívni. Heslá môžu byť ľahko zapamätateľné a súčasne ťažko prelomiteľné. Nepoužívajte výhradne ťažko zapamätateľné znakové heslá, zbytočne by vám to sťažilo život. Nedávajte si krátke a ľahké heslá ako napríklad „*12345, qwerty, asdf, Admin1234*“ prípadne dátumy narodenia vás alebo vašich blízkych a podobné. Slovenčina je nádherný jazyk a zahraniční útočníci ju nemajú radi. Vždy je lepšie mať komplexné heslo napríklad: „***3ModréGulôčkyPadli3KrátPoSebeDo2Jamiek!***“ prípadne „***A ty mor ho hoj mor ho detvo môjho rodu***“, (heslo si ale nepospevujte nahlas). Naviac útočník väčšinou na klávesnici ani nemá znaky ako ä alebo ô. Tieto komplexné ľahšie zapamätateľné heslá pre vás, sú omnoho odolnejšie voči útokom. Pre istotu ešte raz pripomenieme - heslá nikdy s nikým nezdieľajte. Ani s vašim IT oddelením. Pre zvýšenie bezpečnosti vašich zariadení odporúčame používať dvojfaktorovú autentifikáciu. V systémoch Windows 10 je možné v súčasnosti už pridať biometrické overenie prístupu do systému napríklad otlačok prstu, či skenom tváre, prípadne overenie hardvérovým zariadením USB. Pri zadávaní svojho hesla vo webovom prehliadači vás môže prehliadač vyzvať, aby ste si uložili vaše heslo automaticky – túto možnosť nevyužívajte aj keď je to pohodlné. Vždy si radšej heslo zadajte ručne. V prípade že používate veľa hesiel a je pre Vás zložité si také množstvo zapamätať, odporúčame používať softvér na uchovávanie a správu hesiel, napríklad KeePass*.

9. ...by ste mali zálohovať svoje údaje ?

V dnešnej dobe, kedy externé ukladacie zariadenia (USB kľúče, harddisky prípadne CD/DVD nosiče) sú cenovo dostupné, nie je ľahké ospravedlniť absenciu zálohy dôležitých dát. Zálohujte si vaše dáta na fyzických zariadeniach. Neodporúčame dávať dáta do Cloudových služieb. Pamätajte, že hrozby ako aj útočníci nechcú vždy vaše údaje len ukradnúť a zneužiť, ale že konečným cieľom môže byť ich zašifrovanie, alebo úplné vymazanie. Pri zálohovaní svojich dát, či už na fyzické zariadenie alebo Cloud myslite na to, že je vhodnejšie dáta zašifrovať, alebo zaarchivovať (do ZIP súboru, RAR súboru) v ideálnom prípade aj s heslom ktoré viete príjemcovi dát zaslať iným komunikačným kanálom napríklad SMS správou. Zvýšite tak bezpečnosť zálohovaných alebo zdieľaných súborov. Externé zariadenia so zálohami vašich dát skladujte odpojené od počítača. Ak by útočník napadol dané zariadenie, dostal by sa aj k zálohám vašich dát.

10. ...nie ste imúnni ?

Najnebezpečnejšia myšlienka, ktorú môžete mať, je „to sa mi nestane“, „nenavštívim nebezpečné webové stránky“ alebo „veď ja nie som ničím zaujímavý pre takých hackerov“. Počítačoví zločinci nerobia rozdiel pri zacielení na najrôznejších používateľov. Buďte aktívni. Nie všetky chyby môžu byť vrátené pomocou „CTRL + Z“. Vždy používajte antivírovú ochranu prípadne aktivujte bezplatnú antivírovú a antimalware ochranu v systéme Windows – Microsoft Defender. Opäť **pripomíname - dávajte pozor, aké stránky navštevujete, čo a odkiaľ sťahujete, na aké odkazy klikáte a čo v systéme spúšťate alebo otvárate**. V prípade že si nie ste niečím úplne istí, obráťte sa na vaše IT oddelenie.

11. ...bezpečnosť prenosných zariadení je základ ?

Dávajte pozor na to, čo pripájate k počítaču. Škodlivý softvér sa môže šíriť prostredníctvom infikovaných USB Flash diskov, externých pevných diskov a dokonca aj smartfónov alebo CD/DVD nosičov. Dávajte veľmi veľký pozor na to, od koho si beriete USB disk. Určite nepripájajte do svojho zariadenia USB Flash disk, ktorý nájdete niekde pohodený na „zemi“. Zvýšenú pozornosť a opatrnosť venujte aj USB Flash diskom, ktoré môžete dostať, ako „darček“ na rôznych konferenciách. Ak takéto zariadenie pripájate do počítača, tak ho dajte skontrolovať antivírusovou ohranou, prípadne vaším IT oddelením. Dôležité je, aby nebolo v operačnom systéme nastavené automatické otváranie pripojených externých zariadení ako sú USB, externé disky a podobne.

12. ...zdieľať sa dajú aj menej citlivé informácie ?

Sledujte a kontrolujte, čo zdieľate, sledujete alebo „lajkujete“ na sociálnych sieťach. Profily na sociálnych sieťach si zabezpečte tak, aby neboli verejné. Zločinci sa s vami môžu spriateliť a ľahko získať prístup k obrovskému množstvu informácií - kam chodia vaše deti do školy, kde pracujete, kedy a kde ste na dovolenke, **čo im môže pomôcť získať prístup k hodnotnejším údajom o vás, vašej rodine alebo vašej práci, formou sociálneho inžinierstva.**

13. ...by ste nemali používať debetné karty online ?

Ďalší dôležitý tip v oblasti kybernetickej bezpečnosti sa točí okolo online platieb. Dávajte si obzvlášť pozor na malé a neznáme e-shopy, ktoré nemusia mať dostatočné zabezpečenie. Taktiež je dobré voliť radšej e-shop, ktorý je na trhu už nejaký čas alebo ho poznáte. Pri platbe online nepoužívajte debetné karty. Alebo čokoľvek viazané priamo na váš bankový účet.
Namiesto toho použite možnosti, ktoré poskytujú ďalšiu úroveň ochrany medzi útočníkom a vašimi bankovými účtami. Môže ísť o kreditnú kartu s poistením, alebo o druh online spôsobu platby, ako je napríklad PayPal. Platby vykonávajte len na zariadeniach, ktoré sú vaše resp. im dôverujete. **Nikdy nezadávajte žiadne platobné údaje na neznámych zariadeniach, ani neznámych WiFi sieťach.**

14. ...informácie o platobnej karte by ste nemali ukladať ?

Mnoho webových stránok vám dnes umožňuje ukladať informácie o vašej platobnej karte, aby ste si nákup v budúcnosti rýchlejšie a ľahšie spracovali. Je to síce pohodlné, no nerobte to. Ak je vaša platobná karta na webe uložená a web je napadnutý, alebo z neho niekto ukradne dáta, získa ľahko prístup aj k údajom vašej karty. Neukladať kartu na web sa môže zdať ako nepohodlné, no sľubujeme, že to nie je také zlé, ako ukradnutie vašich platobných informácií.

15. ...je potrebné používať antivírusový softvér ?

Vírusy, spyware, malware, phishingové útoky a ďalšie chuťovky. Existuje mnoho spôsobov, ako môžu byť vaše údaje a dáta ohrozené. Inštalácia antivírusového softvéru (napríklad ESET, Kaspersky, BitDefender, McAffee, MalwareBytes, a iné) do zariadenia pomôže v boji proti týmto útokom. Uistite sa, že softvér je aktívny a aktuálny. Mal by zabrániť digitálnym bezpečnostným hrozbám skôr, ako k nim dôjde. Vždy môžete využiť služby Microsoft Defender, ktorý je zdarma v rámci systému Windows 10. Softvér nesťahujte z neznámych stránok, ale vždy z oficiálnych stránok, prípadne priamo od výrobcu.

16. ...byť prehnane podozrievavý – dostatočne paranoidný je správne ?

Aj keď je veľa vecí vo svete online dnes už bezpečných, ako nakupovanie online alebo platenie účtov, je lepšie byť aj tak podozrievavý než potom ľutovať. Nezabudnite kontrolovať všetky odkazy, na ktoré klikáte, softvér ktorý sťahujete a inštalujete, ako aj webové stránky, ktoré navštevujete. Udržiavanie trochu zdravej **paranoje** voči e-mailu, sociálnym médiám a internetu vám môže pomôcť zachytiť nebezpečenstvá, ktoré by vám inak unikli. V prípade, že sa niečo takéto stane, obráťte sa na vaše IT oddelenie. **IT oddelenie považujte za vášho priateľa, ktorý je vám vždy ochotný pomôcť**. Ak potrebujete získať viac informácií o zabezpečení údajov alebo zálohovaní, požiadajte tím technickej podpory o pomoc. Je vhodné pokiaľ na pracovnej stanici uvidíte upozornenie alebo varovanie z vášho bezpečnostného softvéru, napríklad antivírusový softvér toto varovanie pre istotu nahlásiť aj vášmu IT oddeleniu. Každá nezrovnalosť alebo vec v ktorej si nie ste istí, by mala byť konzultovaná s vaším IT oddelením. Bohužiaľ pracovníci IT nie vždy vedia o každom probléme, alebo si ho nemusia všimnúť v reálnom čase, preto určite ocenia vašu pomoc s hlásením. V prípade komunikácie s vaším IT neexistujú dobré a zlé otázky. Vždy je lepšie spýtať sa zbytočne, ako vôbec.
Ide o vašu kybernetickú bezpečnosť.

* https://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/navody-a-odporucania/sprava-hesiel-8a7.html