„TAHÁK DO KAPSY“: HESLA A PŘIHLAŠOVÁNÍ

1.

Podoba hesla

Heslo může obsahovat velká a malá písmena, číslice i speciální symboly jako jsou +*?- atp. Je vhodné nedávat velké písmeno na začátek a číslici na konec hesla. Jsou to předvídatelné pozice.

2.

Délka hesla

Dobré heslo je složeno alespoň ze 12 znaků. Odborníci na kybernetickou bezpečnost tvrdí, že délka hesla je nejdůležitější faktor pro odolávání technikám, které mají za úkol heslo prolomit.

3.

Frázová hesla

Pomoci naší hlavě mohou tzv. frázová hesla. Fungují jako dobrá paměťová pomůcka. Vzpomeňte si na Nový epochální výlet pana Broučka, tentokrát do XV. století, tedy NevpB,td15.s.

4.

Správce hesel

Správci hesel jsou šikovné prográmky, které hesla vygenerují, ukládají na bezpečném místě a v případě potřeby je uživateli vydávají. Odborníci za dobrého správce hesel označují třeba Keepass.

„TAHÁK DO KAPSY“: ODEMYKÁNÍ MOBILNÍCH ZAŘÍZENÍ

1.

PIN

PIN je dobrá metoda pro odemykání mobilních zařízení. Aby dobře chránil, měl by být složený z alespoň šesti číslic, které netvoří triviální řadu jako třeba 123456. Dnešní zařízení na to často sama upozorňují.

2.

„Gesto“

Metoda, kdy spojujeme body na obrazovce do nějakého vzoru, nemá příliš dobrou pověst. Pohodlných kombinací je málo, lidé si volí za vzor například velká písmena a vzor může někdo okoukat.

3.

Otisk prstu

Otisk prstu je dobrá metoda pro odemykání mobilních zařízení. Moderní čtečky už nesledují otisk jako takový, ale jeho elektrický náboj. Proto jsou velmi spolehlivé. Nejlépe fungují společně se silným PIN.

4.

Sken obličeje

Když byla metoda nová, občas se podařilo ji přechytračit. Prošla ale vývojem. Záleží na typu zařízení a skeneru, ale spolehlivost metody je dnes vysoká. Také nejlépe funguje se silným PIN.

„TAHÁK DO KAPSY“: SOCIÁLNÍ INŽENÝRSTVÍ

1.

Sociální inženýrství

Techniky sociálního inženýrství se soustředí na manipulaci uživatele. Jejich cílem je manipulovat s emocemi a city uživatele tak, aby například prozradil své důvěrné, typicky přihlašovací, údaje.

2.

Phishing

Může vypadat jako podivná zpráva ze zahraničí i jako rafinovaná výzva z adresy IT oddělení. Maskuje se třeba jako notifikace o přeplněné e-mailové schránce. Je důležité sledovat, kam vedou odkazy.

3.

Vishing

Podvodná technika, která bývá realizována pomocí telefonního hovoru. Útočníci se maskují například za pracovníky banky nebo klientské podpory. Nenechte se vylekat ani vykolejit.

4.

Baiting

Oblíbené „flešky“ mohou způsobit mnoho problémů. Útočnici je podstrčí a čekají, kdo „flešku“ připojí k zařízení. Může být opatřená lákavým popisem. Raději se jim vyhněte obloukem.

„TAHÁK DO KAPSY“: DŮVĚRYHODNÁ KOMUNIKACE

1.

Elektronické podpisy

Není elektronický podpis jako elektronický podpis. Významně se liší právní a informatický pohled na tuto problematiku. Jen některé typy podpisů zvyšují důvěryhodnost komunikace.

2.

Prosté el. podpisy

Naskenovaný podpis a jeho různé variace nezaručují identitu podepsané osoby ani to, že dokument nebo zprávu po podpisu nikdo nezměnil. Z hlediska bezpečnosti nemají takové podpisy žádnou sílu.

3.

Zaručené el. podpisy

Zaručené el. podpisy jsou na tom z hlediska bezpečnosti lépe. Vyšší hodnotu mají zaručené el. podpisy založené na tzv. kvalifikovaném certifikátu. Ten můžeme získat u certifikační autority.

4.

Kvalifikované el. podpisy

Kvalifikovaný el. podpis je z hlediska bezpečnosti považován za nejsilnější. Certifikát bývá uložen třeba na zabezpečené čipové kartě, kterou připojujeme k zařízení. Musíme znát také PIN.

„TAHÁK DO KAPSY“: ŠKODLIVÉ SOUBORY

1.

Škodlivé soubory

Škodlivé soubory typicky spouští škodlivé programy, které dokážou poškodit naše zařízení nebo systém. Útočníci je rádi šíří v příloze e-mailu nebo pomocí internetových úložišť.

2.

Maskování souborů

Aby útočníci uživatele zmátli, škodlivé soubory maskují. Třeba jako fakturu nebo jiný důležitý dokument, jako jeden z mnoha souborů v archivu typu .rar nebo .zip, případně kamuflují přípony souborů.

3.

Škodlivá makra

Pro uživatele bývá překvapení, že škodlivý soubor může být také soubor Excel, Word či PowerPoint. Útočníci v nich umí připravit škodlivá makra, sadu pokročilých pravidel, která útok dokážou zahájit.

4.

Ransomware

Obávaný škodlivý program, který uživatele může zaskočit třeba právě kvůli makru, je ransomware. Dokáže zašifrovat soubory nebo celé systémy, které se pak jen obtížně obnovují.

„TAHÁK DO KAPSY“: OCHRANA ZAŘÍZENÍ

1.

Aktualizace

Aktualizace jsou důležité, díky nim udržují vývojáři programy v kondici. To platí i ve věci bezpečnosti. Aktualizace totiž mohou opravovat objevené bezpečnostní nedostatky. Je důležité je neoddalovat.

2.

Firewall

Firewall je nástroj, který dohlíží na bezpečnost zařízení. Má za úkol kontrolovat požadavky, které zařízení z internetu přijímá a vyhodnotit je podle určených bezpečnostních pravidel.

3.

Antivirový program

Antivirový program neustále dohlíží na to, že v našem zařízení není žádný známý škodlivý soubor. Pokud se tam takový soubor objeví, má za úkol provést potřebné akce, které zařízení ochrání.

4.

Zálohování

Jako uživatelé můžeme o svá data a soubory i nenávratně přijít. Právě v tento moment se hodí průběžné zálohy. To znamená, že si důležité soubory alespoň čas od času uložíme „ještě někam jinam“.

„TAHÁK DO KAPSY“: STAHOVÁNÍ APLIKACÍ

1.

Oficiální obchody

Když stahujeme aplikace do mobilních zařízení, vždy bychom je měli stahovat z tzv. oficiálních obchodů. To je Google Play pro systém Android a AppStore pro systém iOS. Jsou to oficiální zdroje.

2.

Kritéria aplikací

U aplikací je důležité sledovat recenze uživatelů a jejich hodnocení. Vyplatí se vyfiltrovat si špatné recenze a podívat se, na co konkrétně si uživatelé stěžovali. To je dobré vodítko.

3.

Oprávnění aplikací

Každá aplikace ke svému fungování potřebuje tzv. oprávnění. Ty jako uživatelé udělujeme. Oprávnění bychom však měli udělovat s rozvahou a hodnotit je selským rozumem.

4.

Maskování aplikací

Útočníci leckdy podstrčí škodlivý kód do aplikace, u které to uživatelé nečekají. Třeba do aplikace pro úpravu fotek, které se dobře šíří. Nebo do aplikace, která se tváří jako „antivirová ochrana“.

„TAHÁK DO KAPSY“: PŘIPOJENÍ A SOUKROMÍ

1.

Veřejné wi-fi sítě

Veřejné wi-fi sítě bez hesla je vhodné používat jen pro základní úkony. Třeba k vyhledání otevírací doby nebo odjezdů MHD. Přihlašovací údaje je lepší pomocí nich neodesílat.

2.

HTTPS

HTTPS nám říká, že je komunikace mezi naším webovým prohlížečem a webovou stránkou šifrovaná. Neznamená to ale, že je stránka dokonale a za všech okolností bezpečná.

3.

Koncové šifrování

Koncové šifrování se využívá především k šifrování zpráv. Díky tomuto šifrování je dokáže číst jen odesílatel a příjemce. Ne všechny komunikační aplikace toto šifrování podporují.

4.

VPN

VPN funguje jako pomyslný tunel, kterým proudí náš internetový provoz. Útočníci ho nedokážou sledovat a číst. Zajišťuje maximální míru soukromí. VPN připojení si můžeme pořídit za pár stovek.