Bezpečná hesla

On-line služby a portály v dnešní době vyžadují, aby si uživatel zvolil relativně bezpečné heslo. Hesla typu „jindrich38“ často není možné nastavit. Ochranné mechanismy dohlíží nad to, že má heslo určitý počet znaků, zpravidla alespoň 12, vyskytují se v něm velká i malá písmena, číslice a speciální symboly jako třeba +*?-. To bývá považováno za dobrý standard. Pozor by si uživatelé měli dát na předvídatelné pozice. Když se velké písmeno umístí na začátek a číslice naopak na konec hesla, usnadní to útočníkovi práci. Předvídatelné pozice snižují počet kombinací, kterými se musí prokousat. Je to jako zamknout a klíč dát pod rohožku. Je vhodné při tvorbě hesla projevit více kreativity. Za zmínku také stojí, že v současné době považují odborníci délku hesla za nejdůležitější faktor bezpečnosti.

Frázová hesla

Frázová hesla mají výhodu. Bývají lépe zapamatovatelná, protože jsou kreativní. Heslo totiž nemusí být jen řetězec náhodných znaků. Může fungovat jako paměťová pomůcka, se kterou dokáže uživatel pracovat. Paměťovou pomůckou může být cokoliv, třeba kniha, kterou před sebou máte v knihovně. Pro příklad Nový epochální výlet pana Broučka, tentokrát do XV. století. Teď stačí určit a zapamatovat si klíč, podle kterého heslo skládáme. Frázové heslo může mít následující podobu: Nový epochální výlet pana Broučka, tentokrát do XV. století, tedy NevpB,td15.s. Níže se můžete podívat, jak dlouho by prolomení tohoto hesla trvalo. V žádném případě však nedoporučujeme zadávat do podobných webů opravdová a aktuální hesla k orientačnímu otestování. V případě zájmu vždy zadávejte jen charakterem obdobná hesla.

Kontrola bezpečnosti hesla:

[How Secure Is My Password? | Password Strength Checker (security.org)]

Ilustrační obrázek ukazuje orientační výpočet doby potřebné pro prolomení modelového frázového hesla. V tomto případě by to trvalo a 63 000 let. Záleží však na výpočetním výkonu útoku. Zdroj: security.org/how-secure-is-my-password/

Správce hesel

Správci hesel jsou počítačové programy, které dokážou hlavě uživatele ulevit na maximum. Způsobů, jak mohou uživatelé se správci hesel pracovat, je více. Obvykle správce hesel umí hesla vymýšlet, ukládá je na bezpečném šifrovaném místě a v případě potřeby hesla vydává uživateli. Někteří uživatelé do správce hesel neukládají hesla, ale jen paměťové pomůcky a klíče k frázovým heslům. Uživatel si pamatuje pouze „superheslo“, kterým se správce hesel spouští. Říká se, že jsou jen dvě hesla, která do správce hesel nepatří. Heslo od e-mailu a od internetového bankovnictví.

Můžete mi nějakého správce hesel doporučit?

***Doporučení si zaslouží správce hesel KeePass**. Není to fešák, ale má své výhody. Je to open-source, což znamená, že programový kód KeePassu vyvíjí celosvětová komunita programátorů. Jeho kód je veřejně známý a průhledný. Aby do programového kódu nemohl nikdo přidat škodlivou část, existuje řada ochranných mechanismů a schvalovacích procesů. Proto odborníci na kybernetickou bezpečnost open-source řešením zpravidla více důvěřují. KeePass se spouští jako off-line soubor bez přístupu k internetu, což je také jeho plus. Tento soubor je však vhodné zduplikovat a uložit jeho kopii na bezpečné místo, například pro případ poškození původního souboru s hesly. Má i českou verzi. Není komerční, je zdarma.*

Videonávod na zprovoznění KeePass

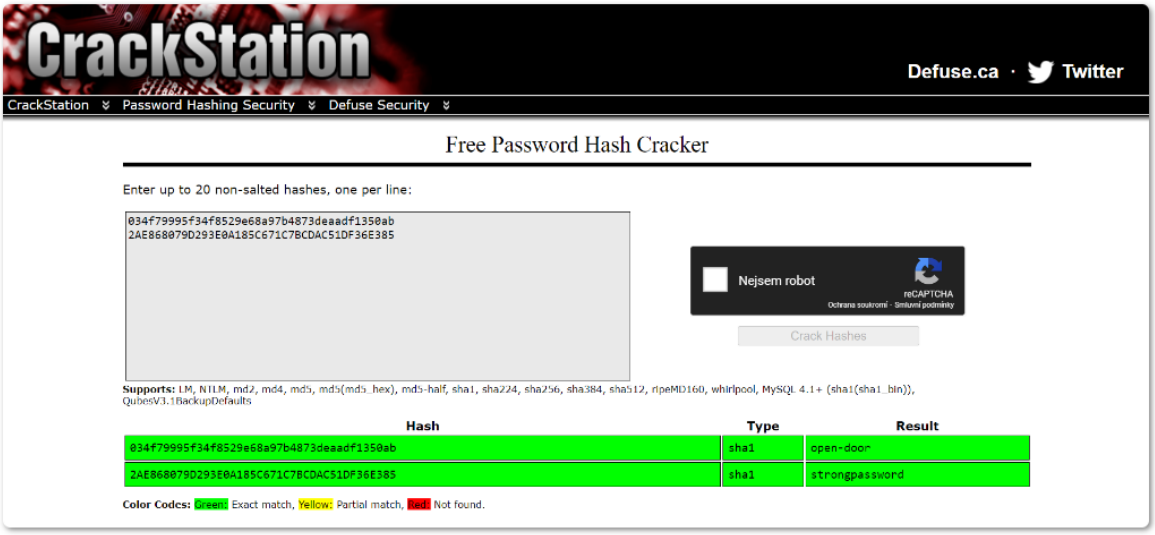
Už znáte správce hesel KeePass. Pro řadu uživatelů je však tento nástroj nový a vlastně neví, jak si jeho fungování představit. Vše přibližuje video s českým komentářem: https://www.youtube.com/watch?v=9QszkJh1CPc

Co funkce „zapamatovat heslo“, kterou nabízí webové prohlížeče?

Technické řešení této funkce se u webových prohlížečů liší. Obecně však platí, že se nejedná o příliš bezpečnou funkci, protože existuje několik postupů, jak uložená hesla vzdáleně odcizit. Za relativně bezpečné lze považovat řešení webového prohlížeče Safari. Také řešení webového prohlížeče Mozilla Firefox patří k těm bezpečnějším, pokud si uživatel nastaví tzv. hlavní heslo pro ochranu všech ostatních hesel. Všimněte si ale, že i v oficiálních návodech, které najdete v odkazech výše, jsou jmenována rizika s tímto řešením spojená.

Úniky přihlašovacích údajů

Hesla uživatelů mohou uniknout přímo on-line službě. Ta by neměla hesla uchovávat v prosté podobě, tedy v podobě, jakou zná uživatel. Neměla by vědět, že uživatel má heslo NevpB,td15.s. Řada služeb to však nerespektuje, čímž uživatele ohrožují. Správně má on-line služba znát jen zástupný řetězec hesla vytvořený pomocí matematické funkce. Takovému řetězci se říká hash a vypadá třeba takhle: *034f79995f34f8529e68-a97b4873deaadf1350ab.* Heslo a jeho hash jsou jako jednovaječná dvojčata. Jsou stejná, ale přesto rozdílná. V případě úniku údajů by tedy měly unikat „jen“ hashe. Jenže pokud daná služba používá zastaralé hashovací funkce, zase máme malér. Existují totiž nástroje, které takové hashe umí prolomit. I proto je důležité dát si s tvorbou hesla trošku práce, a také ho průběžně obměňovat.



Ilustrační obrázek ukazuje nástroj k prolomení hashe na heslo v prostém textu. Například hash 034f79995f34f8529e68a97b4873deaadf1350ab představuje heslo open-door. Nelze však tvrdit, že tímto způsobem je možné prolomit každý hash. Zdroj: crackstation.net

Dvoufaktorové ověřování

Dvoufaktorové ověřování je záchranná brzda, pokud se k heslu uživatele dostane někdo cizí. Doporučujeme ho nastavit všude, kde je to možné. Nejčastěji má podobu SMS kódu s časově omezenou platností, nebo výzvy v příslušné mobilní aplikaci. Při přihlašování do on-line služby zadá uživatel přihlašovací jméno, heslo a ještě musí opsat SMS kód, nebo potvrdit výzvu v aplikaci. To je ten druhý faktor. Od ověřování pomocí SMS kódů se pomalu upouští, protože SMS nejsou šifrované a není složité je odposlouchávat. Výzvy v mobilní aplikaci bývají důvěryhodnější. Zpravidla využívají šifrování a stále častěji využívají biometrické údaje, jako otisk prstu uživatele. Pokud můžete, zvolte ověřování mobilní aplikací.

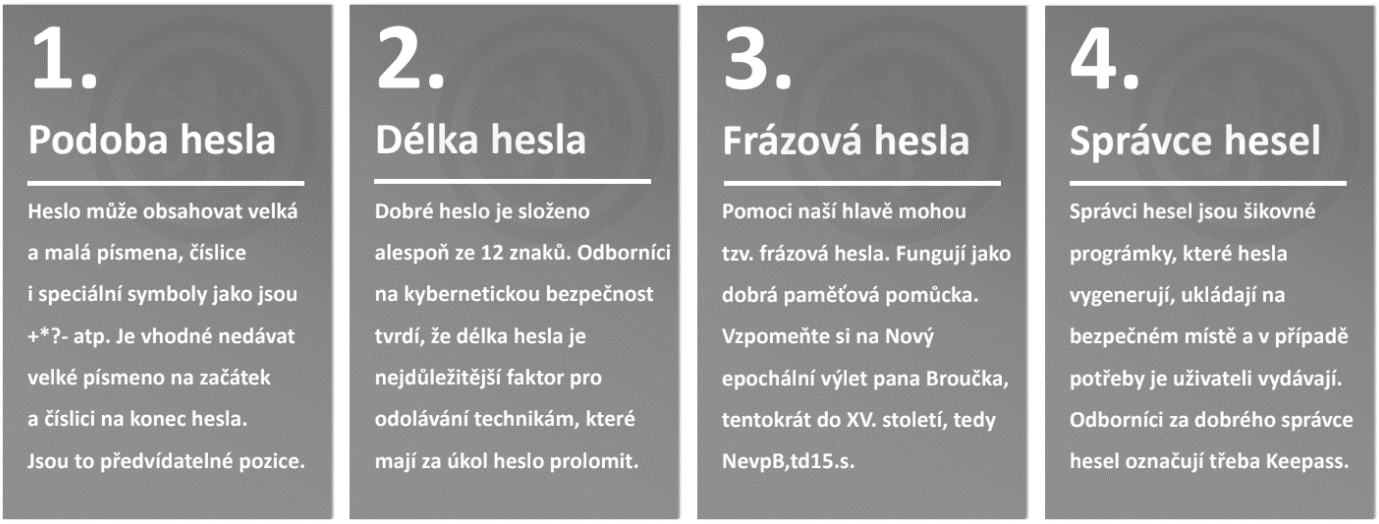
Má dvoufaktorové ověřování nějakou slabinu?

Účinnost tohoto ověření snižuje poměrně nenápadná věc v nastavení telefonu. Náhledy SMS zpráv. Pokud uživatel využívá jako druhý faktor SMS kód, měl by v nastavení zakázat náhled zpráv na uzamčeném zařízení. Pokud to zakázáno není, k SMS kódu se může dostat kdokoliv, kdo má k telefonu přístup, aniž by ho musel odemykat.

Co když mám dvoufaktorové ověřování aktivní a ztratím telefon?

Pro tyto případy bývají uživateli vystaveny tzv. záložní kódy. Mohou mít podobu číselného kódu, QR kódu atp. Je dobré si tyto záložní kódy bezpečně uložit, ideálně off-line. Problém totiž může vyvstat, pokud se útočník těchto kódů zmocní. To se může stát, pokud je má uživatel ledabyle uložené někde ve svém zařízení. Pokud útočník kódy získá, služba ho bude považovat za ověřeného uživatele, který kupříkladu ztratil telefon.

„TAHÁK DO KAPSY“: HESLA A PŘIHLAŠOVÁNÍ



Kontrola spárovaných služeb ke Google a Facebook účtu

Místo registrace a vytváření nového účtu se do řady služeb můžeme přihlásit přes Google nebo Facebook účet. Zkontrolujte, které služby a aplikace jste spárovali se svým účtem. Tato možnost přihlašování je oblíbená a uživatelsky přívětivá, ale je dobré si udržovat přehled, s čím máme účty spojené a zda je stále vše aktuální, nebo již přístup udělujeme zbytečně. Pro Facebook využijte tento odkaz: https://www.facebook.com/settings?tab=applications a pro Google využijte tento odkaz: https://myaccount.google.com/permissions

Úprava zobrazování notifikací na telefonu

Vyzkoušejte si přenastavit notifikace tak, aby se neukazovaly jejich náhledy na uzamčeném telefonu. Pro telefony se systémem Android může být užitečný návod od Google: https://support.google.com/android/answer/9079661?hl=cs#zippy=%2Coption-hide-sensitive-content-from-notifications-on-your-lock-screen Telefony Apple se systémem iOS mají návod také: https://support.apple.com/cs-cz/HT201925

Stalo se?

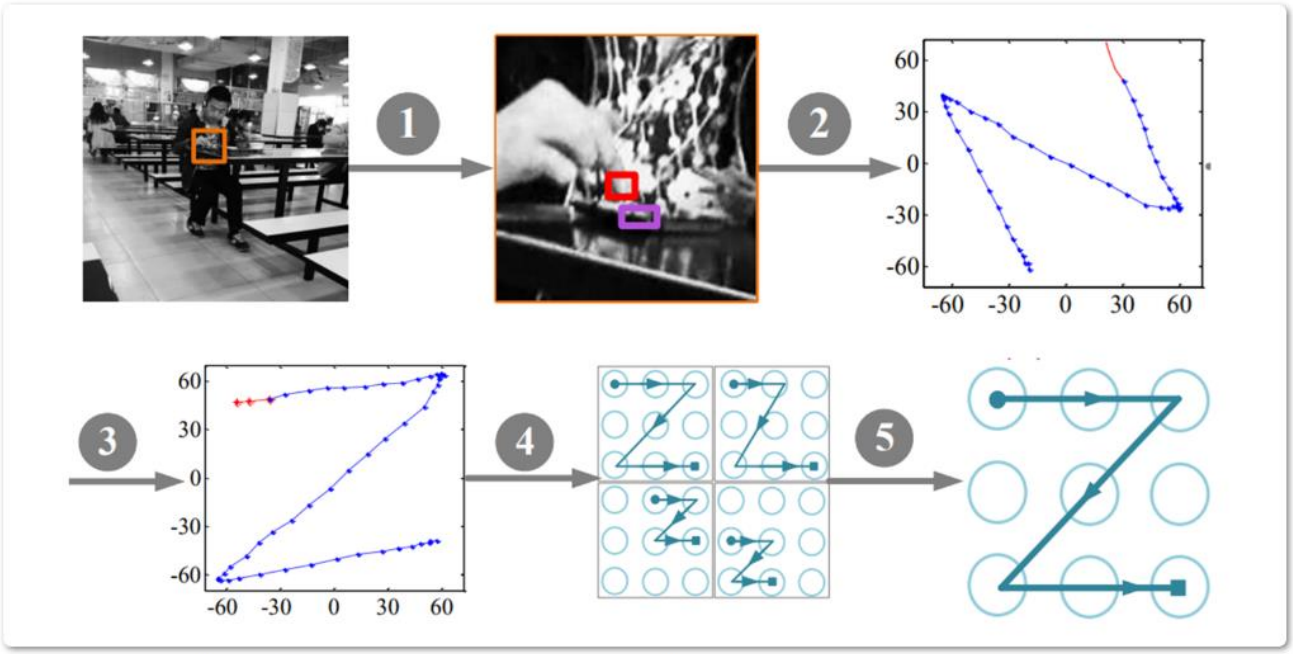
Markétě je 34 let a zastává funkci vedoucí oddělení mezinárodních vztahů nejmenovaného ministerstva. Pro pracovní účely dostala služební mobilní telefon. Již při prvním spuštění telefonu byla vyzvána, aby si zvolila metodu, kterou bude telefon odemykat. Vybrala si metodu gesta, kdy musí spojit několik bodů na displeji ve správném pořadí. Na tuto metodu byla zvyklá ze svého soukromého telefonu. Jednoho dne byla Markéta v šoku. Zjistila, že mnoho kontaktů ze seznamu zmizelo, a že z jejího telefonu bylo odesláno několik podivných SMS zpráv. Později vyšlo najevo, že se telefon přes víkend dostal do rukou dětí, které si hrály. Podařilo se jim ho odemknout. Myslely si, že je to hra.

Odemykání mobilních zařízení

Nastavení odemykání mobilních zařízení bychom neměli podceňovat. V případě ztráty či odcizení mobilního telefonu nebo tabletu budeme rádi, že jsou uzamčené některou z dostupných metod. Uzamčené zařízení nám totiž v krizových situacích poskytne čas jednat. Služební mobilní zařízení mohou být chráněna pojistkou pro případ ztráty, která umožní jejich dohledání nebo vzdálenou správu, promazání atp. Starší mobilní zařízení uživateli dovolovala, aby si žádný zámek nenastavoval a zařízení bylo stále odemčené. To je ale hrubá chyba, která odtajňuje naše účty, e-maily nebo kalendáře. Jak tedy zařízení uzamknout?

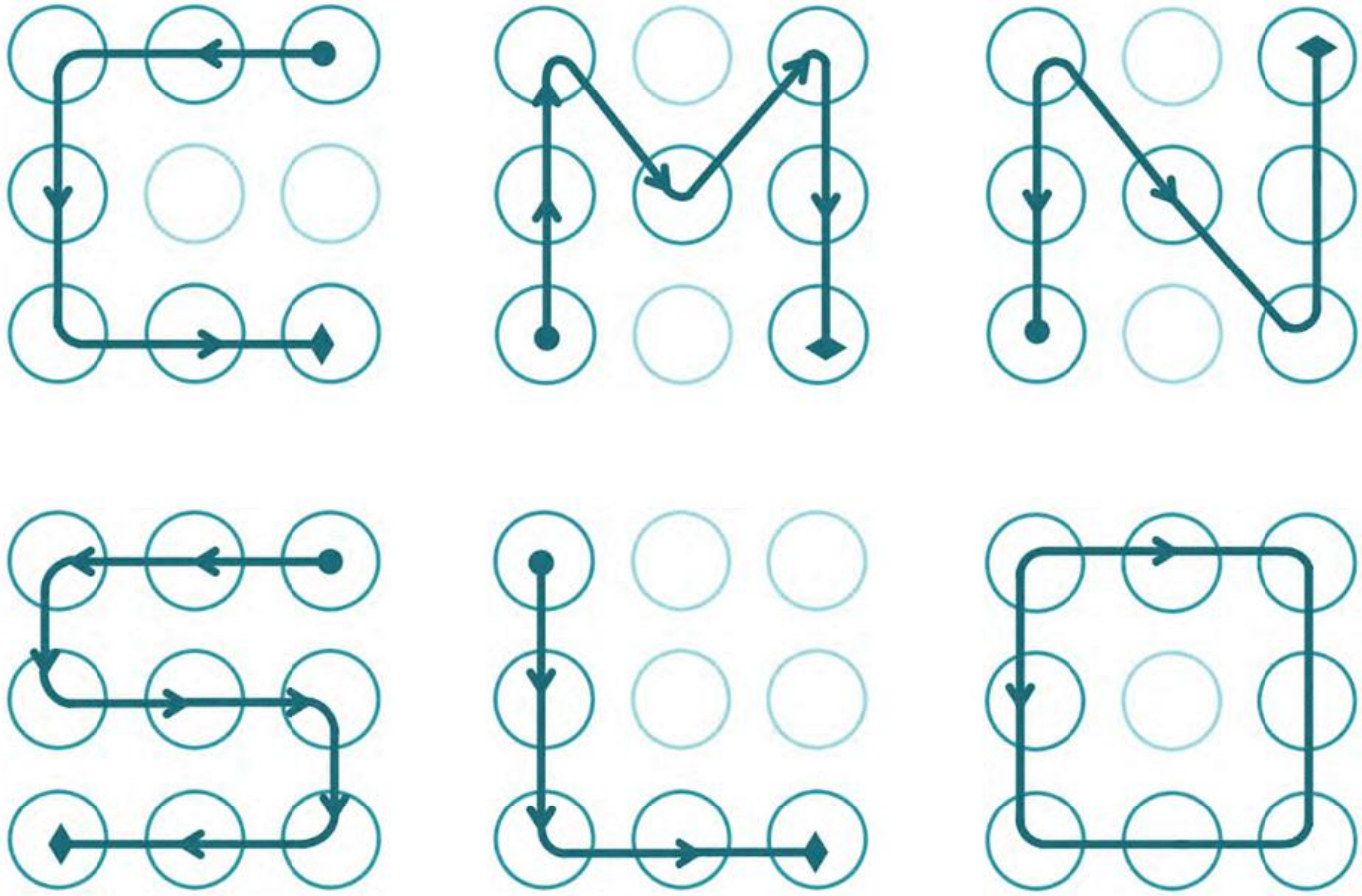
Zhodnocení tradičních metod odemykání

Sem patří PIN (číselný kód) a gesto (spojování bodů na displeji). Aby PIN zařízení dobře chránil, nesmí se skládat z méně než 6 číslic a nesmí se jednat o triviální řadu (111111, 123456 atp.). Dnešní zařízení se triviálním řadám sama brání a upozorňují, že jsou slabé. Okoukat řadu 6 číslic ve správné kombinaci je náročné, navíc číslice bývají zastoupeny puntíkem. Při splnění jmenovaných podmínek je PIN dobrou metodou odemykání. Oproti tomu gesto, kdy na displeji spojujeme body ve správném pořadí, považujeme za nejméně bezpečnou metodu. Proč? Protože není ničím kryté a je snadné ho okoukat. Kuriózní je, že gesto praváků i leváků zpravidla začíná v levém horním rohu. Každý desátý uživatel si navíc vybírá za vzor nějaké písmeno. A pohodlných kombinací není mnoho.



Ilustrační obrázek ukazuje, jakým postupem se v experimentu podařilo získat vzor pro odemykání. 1) videozáznam uživatele, 2) výběr sledované oblasti, 3) analýza směru a dráhy prstu, 4) otočení dráhy z pohledu uživatele, 5) pravděpodobné výsledky, 6) správný výsledek.

Zdroj: eprints.whiterose.ac.uk/151222/



Ilustrační obrázek ukazuje zřejmě nejpoužívanější vzory pro odemykání mobilního zařízení. Pravděpodobný zdroj: eprints.whiterose.ac.uk/151222/

Zhodnocení moderních metod odemykání

Sem patří odemykání otiskem prstu a skenem obličeje. Moderní metody odemykání fungují rozdílně, záleží na technologii výrobce a cenové kategorii zařízení. Jsou známy případy, kdy byly tyto metody přechytračeny fotkou uživatele nebo voskovým otiskem prstu. Zažívají ale rychlý vývoj. Například srovnávání 2D fotografického skenu obličeje s uloženou fotografií uživatele dávno není v kurzu. Nastupují 3D skenery s infračerveným senzorem, které vytváří hloubkovou mapu obličeje. Počítají, jak se infračervený paprsek od obličeje odráží, a porovnávají hloubkovou mapu obličeje s naskenovanou. Infračervený senzor řeší i dřívější problémy s fungováním za špatných světelných podmínek. Skenery otisku prošly podobným vývojem. Pokročilé skenery nesledují prostý otisku prstu, ale uchovávají si v paměti jeho elektrický náboj. Z elektrického náboje počítají, jestli je otisk uživatele, nebo někoho cizího.

Jaký způsob odemykání tedy doporučujete?

Je potřeba vzít do úvahy, že moderní metody odemykání využívají jako zálohu tradiční metody odemykání. Ani sebelepší skenery otisku prstu nebo obličeje uživatele neochrání, pokud jako zálohu bude mít zvolený slabý PIN nebo slabé gesto. Jako nejvhodnější způsob odemykání se jeví některá moderní metoda, ke které je pečlivě zvolený PIN.

Matematicko-logická hra na prolomení gesta

Vyzkoušejte matematicko-logickou hru BreakLock. Dokážete odemknout cizí mobilní telefon zabezpečený gestem? A kolik na to budete potřebovat pokusů? Vybrat si můžete z několika herních režimů: https://maxwellito.github.io/breaklock/

Vzdálená správa mobilního telefonu

Výrobci mobilních telefonů vyvíjejí také nástroje, se kterými mohou uživatelé svůj telefon lépe dohledat v případě ztráty nebo ho na dálku spravovat. Můžete si zavolat, vyvěsit vzkaz pro nálezce, vymazat obsah telefonu nebo se velmi přesně podívat, kde telefon zůstal. Aby nástroj fungoval, telefon musí být připojený k internetu.
Nástroj pro Android: https://www.google.com/android/find
Nástroj pro iOS: https://www.apple.com/icloud/find-my/

Sociální inženýrství

Vousaté moudro říká, že nejslabším článkem kybernetické bezpečnosti bývá nepoučený uživatel. Zatímco technické nástroje vždy postupují podle zadaných pravidel, uživatelé jsou mnohem méně předvídatelní. Především z důvodu, že mají emoce, znají strach, překvapení nebo pociťují lítost. Útočníci to ví. Proto část energie věnují manipulaci uživatelů s úmyslem získat důvěrné či interní informace. Souhrnně se techniky manipulace uživatelů označují jako sociální inženýrství. Dávno není pravda, že jsou techniky sociálního inženýrství vždy čitelné a na první pohled rozpoznatelné. A právě proto, že si je uživatelé dodnes představují jako legrační zprávy od strýčka Tomase z Texasu, původem z jižních Čech, z pátého kolene, který nám odkazuje pohádkové dědictví, jsou stále účinnější.

Phishing

Jedná se o techniku sociálního inženýrství, jejímž cílem je získat od uživatelů jejich důvěrné, nejčastěji přihlašovací, údaje. V angličtině má tento pojem blízko k „rybaření“, a přesně tak celý útok probíhá. Útočník rozhodí sítě a čeká, kdo z organizace se chytí. Moderní phishingové zprávy přitom dávají smysl. Maskují se například jako oznámení, že je kapacita naší e-mailové schránky naplněna. Pro její navýšení

máme kliknout na přiložený odkaz a přihlásit se ke svému účtu Microsoft. Dokud to neuděláme, nebudou nám chodit zprávy, které obsahují přílohy. Odcizené přihlašovací údaje pak může útočník zneužít k průzkumu nastavení uživatelských oprávnění nebo k rozesílání dalších phishingových zpráv, které budou na ostatní zaměstnance působit ještě důvěryhodněji.

Jaké další triky phishingové zprávy využívají?

Je logické, že když phishingová zpráva působí věrně, zvyšuje to její účinnost. Proto útočníci umí připravit zprávu na míru organizaci, na kterou se zaměřili. K tomu stačí prozkoumat webové stránky organizace. Představte si veřejný kalendář, ve kterém je zaznačený den otevřených dveří. A představte si stránku náboru nových zaměstnanců, kde je uvedené jméno vedoucího personálního oddělení. Abraka dabra, phishingový e-mail, ve kterém vedoucí personálního oddělení žádá o výpomoc při dni otevřených dveří je hotový. Stačí kliknout na odkaz, přihlásit se ke sdílené tabulce a zapsat se jako dobrovolník. Zaměstnancům taková zpráva nepřipadá zvláštní, protože den otevřených dveří se opravdu chystá.

Chodí phishingové zprávy jen e-mailem?

Kdepak, uživatelé se s nimi mohou setkat třeba na sociálních sítích. Dobrým nástrojem sociálního inženýrství je probuzení zvědavosti uživatele. Představte si, že od někoho, koho znáte, dorazí krátká zpráva v Messengeru, která zní: „Jsi to ty v tom videu?“, a je k ní přiložený odkaz. Červíček už nahlodává naše svědomí. Jsme překvapení, trošku se bojíme, kdy a kde nás někdo natočil. Když odkaz otevřeme, jsme přesměrování na přihlašovací stránku sociální sítě, která nevypadá nijak zvláštně. Jenže když se přihlásíme, odevzdáme své přihlašovací údaje.

Rozpoznávání phishingu

Je důležité být ve střehu a phishing nepodceňovat. V případě, kdy se uživatel stane terčem prosté phishingové zprávy, má šanci ji rozpoznat kvůli krkolomné češtině. Tyto zprávy mívají původ v zahraničí a bývají automaticky překládány. Vodítkem také bývá adresa odesílatele. Pokud je na první pohled podezřelá nebo je zakončena neobvyklou doménou, například .ru namísto .cz, je vhodné zpozornět. Avšak propracované phishingové zprávy chodí i z důvěryhodných adres. Proto je nutné dávat pozor především při klikání na jakékoliv přiložené odkazy v e-mailu. V případě propracovaného phishingu to bývá jediné vodítko, na které se uživatel může soustředit. Útočníci také spoléhají na grafickou podobu, pokud uživatel vidí známou grafiku, je méně podezřívavý. Útočníci také rádi dostávají uživatele do časové tísně, vyvíjí nátlak, aby uživatelé úkol splnili rychle.

Jak se mám zachovat, když phishingovou zprávu rozpoznám?

Důležité je neotevírat přiložené odkazy. Pokud phishing objevíme až po otevření odkazu, je důležité nic nevyplňovat, nikam se nepřihlašovat. Dále postupujte podle vnitřních pravidel IT politiky, se kterými byste měli být seznámeni.

Jaké triky s odkazy útočníci používají?

Už jste určitě viděli odkazy schované za slovo zde či podobně ukryté. Text je estetičtější, ale útočníci tím umí uživatelům zamotat hlavu. Užitečným pomocníkem bývá náhledové okénko cíle odkazu. Když najedete na odkaz myší a nebudete klikat, vlevo dole se objeví cíl odkazu. Zkuste si to! Útočníci také rádi využívají přesmyčky a jiné chytáky. Z adresy microsoft udělají třeba rnicrosoft, z velkého „i“ udělají malé „l“, není lekarna jako Iekarna.

Vishing

Technika sociálního inženýrství, která je na vzestupu. Záměr je stejný jako u phishingu, vylákat z uživatele důvěrné, typicky přihlašovací, údaje. Provedení se však liší. Manipulace probíhá telefonicky. Útočník se maskuje například jako klientská podpora IT oddělení a informuje uživatele, že je nutné, aby provedl ověření svého účtu. Záminkou může být únik přihlašovacích údajů zaměstnanců a snaha o zmírnění následků. V zaměstnancích nezřídka zvítězí „smysl pro povinnost“ a spolupracují podle pokynů. Možná si říkáte, že na něco takového byste nepřistoupili. Nenechte se mýlit. Útočníci umí navodit dojem důvěryhodného callcentra. Pustí do sluchátka znělku a klidně si uživatele několikrát přepojí. Existují také nástroje, které zajistí, že uživatel vidí na displeji důvěryhodné číslo.

Jak mám vishingový hovor rozpoznat?

Pokud tušíte, že něco nehraje, zvolte ofenzivní rétoriku. Ptejte se na záležitosti, které by volající musel znát, pokud by vše byla pravda. Volá banka, že nám hrozí zablokování bankovního účtu? V tom případě chtějte vědět, kolik je na účtu peněz. Volá technická podpora, že je naše e-mailová schránka v ohrožení? Chtějte vědět, s kým se to řeší na IT oddělení. Podezřelé hovory také na IT oddělení ohlaste, hrozí, že organizaci zasáhnou masově.

Jaké další triky vishingové hovory využívají?

Útočníci mohou volat například v noci, kdy jsou lidé rozespalí a je jednodušší je šokovat, donutit ke spolupráci. Pokud se oběť nenechá nachytat prvním hovorem, může přijít druhý. V prvním podvodném hovoru se útočníci vydávají například za banku, ve druhém za policii, která volá na žádost banky. Poslechněte si také záznam vishingového hovoru, který publikoval server Seznam Zprávy.

Baiting

Technika, která cílí na zvědavost uživatelů. Představte si, že na chodbě nebo v zasedací místnosti najdete „flešku“. Strčili byste ji do svého počítače? Samozřejmě, že ne! Ale hodně se toho může změnit ve chvíli, kdy je na této „flešce“ popisek. Třeba „seznam propouštění zaměstnanců“ nebo „návrh ročních odměn“. Podle průzkumů takto označenou „flešku“ připojí dva z pěti zaměstnanců. A jak správně tušíte, často najdou něco úplně jiného, než očekávali. Třeba škodlivý soubor, kvůli kterému si IT oddělení ještě dlouho nevybere dovolenou. Uživatel dokonce nemusí škodlivý soubor ani otevřít, útočník vše dokáže narafičit tak, že se po připojení k zařízení spustí sám. A pokud se ptáte, jak se taková „fleška“ do zasedačky dostane, může ji sem přinést třeba podplacený zaměstnanec.

Jaké další triky s „fleškou“ mě můžou potkat?

Jsou známy případy, kdy se upravená „fleška“ po připojení k zařízení napájela elektrickou energii a jakmile získala dostatek energie, vyslala ji zpět do zařízení. To dokázalo zařízení zlikvidovat. Existují „flešky“, které umí pořizovat špionážní zvukové nahrávky, fungují jako zamaskovaný diktafon. Upravená „fleška“ se také dokáže maskovat jako klávesnice, takže i když je v rámci IT politiky organizace nastaveno, že se „flešky“ nedají spustit, toto maskování dokáže nastavení obelstít a fleška se spustí.

Jak mám postupovat, když najdu „flešku“?

Ať je popsaná jakkoliv, nepřipojujte ji k žádnému zařízení. I kdyby byla opatřená logem vaší organizace, nebo lákavým popisem Velikonoční kybervajíčko. Odneste ji na IT oddělení s upozorněním, kde jste ji našli. V organizaci se může povalovat více podezřelých „flešek“.

Rizika sociálních sítí

Sociální sítě navštěvuje alespoň občas většina z nás. Je součástí dnešní doby, že s přáteli rádi sdílíme momenty z osobního nebo pracovního života. Očima útočníků se však může jednat o cenné informace, které umí zneužít při plánování sociálního inženýrství. Ačkoliv to zní jako přízemní rada, pečujte o své soukromí a pečlivě příspěvky kontrolujte. Raději však počítejte s tím, že obsah, který sdílíte, se stává veřejným. Předvídejte. Při sdílení obsahu se zkuste sami sebe zeptat: „Co by mohlo být pro útočníka užitečné?“ Může to být adresa, číslo bankovního účtu, fotka před nástěnkou, fotka ze zasedací místnosti atp. Pokud něco takového objevíte, zkuste se zamyslet, jak obsah upravit.

Jak může být můj profil zneužit?

Jedním z triků, se kterým se uživatelé setkávají, je odcizení identity. Útočník si na základě veřejně známých informací vytvoří kopii našeho profilu a oslovuje naše přátele, kolegy atp. Snaží se od nich získat další informace nebo odcizit i jejich profily. Odcizené profily pak útočník může využívat k rozposílání škodlivých zpráv či odkazů nebo třeba pro dezinformační kampaně. Na základě zveřejněných informací na profilu a z obsahu, který sdílíme, umí také útočníci udělat databázi slov a využít ji k pokusu prolomit heslo. Říká se tomu slovníkový útok.

Jaké další triky na sítích číhají?

Jednou ze slepých uliček kybernetické bezpečnosti byly tzv. „bezpečnostní otázky“. Uživatelé si vybrali otázku a odpověď na ni mohli využít jako náhradní heslo, pokud své heslo zapomněli atp. Jednalo se třeba o příjmení matky za svobodna nebo jméno oblíbeného učitele ze školy. Jak tušíte, tyto informace jsou dohledatelné. Navíc se na sociálních sítích objevují podvodné ankety či soutěže, které se na zjišťování těchto odpovědí zaměřují. Uživatelé si to leckdy neuvědomí a odpověď na svou bezpečnostní otázku dobrovolně prozradí. Tuto metodu zabezpečení raději nepoužívejte.

Techniky sociálního inženýrství

Uznávaný kybernetický tým Masarykovy univerzity připravil otevřený on-line kurz, který podrobně rozebírá techniky sociálního inženýrství. Zdaleka jsme si je tady neukázali všechny. Pokud vás zajímají i další techniky, neváhejte kurz navštívit: https://security.muni.cz/socialni_inzenyrstvi

Test České bankovní asociace

Atraktivním cílem je pro útočníky i internetové bankovnictví. Proto vznikl interaktivní vědomostní test, kde si můžete vyzkoušet, kolik zákeřných fíglů sociálního inženýrství zacílených na internetové bankovnictví dokážete odhalit: https://kybertest.cz

Průzkum hlavičky e-mailu

Pokročilé techniky sociálního inženýrství bývá leckdy možné odhalit až technickými nástroji. Analýza tzv. hlavičky e-mailu v sobě nese důležité informace, které odborníci na kybernetickou bezpečnost potřebují často znát. Podívejte se pod pokličku jejich práce a vyzkoušejte si hlavičku nějakého nedůležitého e-mailu analyzovat. Použít můžete nástroj od Google: https://toolbox.googleapps.com/apps/messageheader/

Elektronické podpisy

Úskalím elektronické komunikace bývá nízká důvěryhodnost. Pro zvýšení její důvěryhodnosti byly vynalezeny elektronické podpisy. Elektronické podpisy dokazují, že jsme zprávu odeslali opravdu my, a že po cestě nebyla nijak změněna. Ale pozor! Pojem „elektronický podpis“ může být pro mnoho uživatelů matoucí. Někdo si totiž představí naskenovaný vlastnoruční podpis, někdo podpis na tablet pomocí elektronického pera, někdo zakliknutí políčka „souhlasím“, někdo opisování SMS kódu. Svým způsobem je elektronický podpis vše jmenované. Svým způsobem nic z toho. Zapeklité je, že právní pohled na věc bývá jiný než informatický. Pověst tvrdí, že jednou o elektronických podpisech debatovala skupina právníků a když se nedokázali shodnout, přizvali do debaty informatiky. Říká se, že spolu debatují dodnes. Pojďme se na to podívat blíže.

Prostý el. podpis

Jedná se o všechny metody výše uvedené. Tedy například zmíněný naskenovaný podpis přiložený k dokumentu. Je to známá praxe, která podle právních výkladů postačuje i pro uzavírání smluv. E-mailem obdržíme návrh smlouvy, vytiskneme ji, podepíšeme, naskenujeme a pošleme zpět. Právně je to v pořádku. Problém je, že takový podpis je snadné z dokumentu vyjmout a libovolně zneužívat. U prostého elektronického podpisu také nelze zaručit, že ho k dokumentu připojila osoba, které podpis patří. Stejně tak není možné zaručit, že dokument po podepsání nikdo neupravil. Pokud bychom takový podpis chtěli použít například pro oficiální komunikaci s českými úřady, nepochodíme.

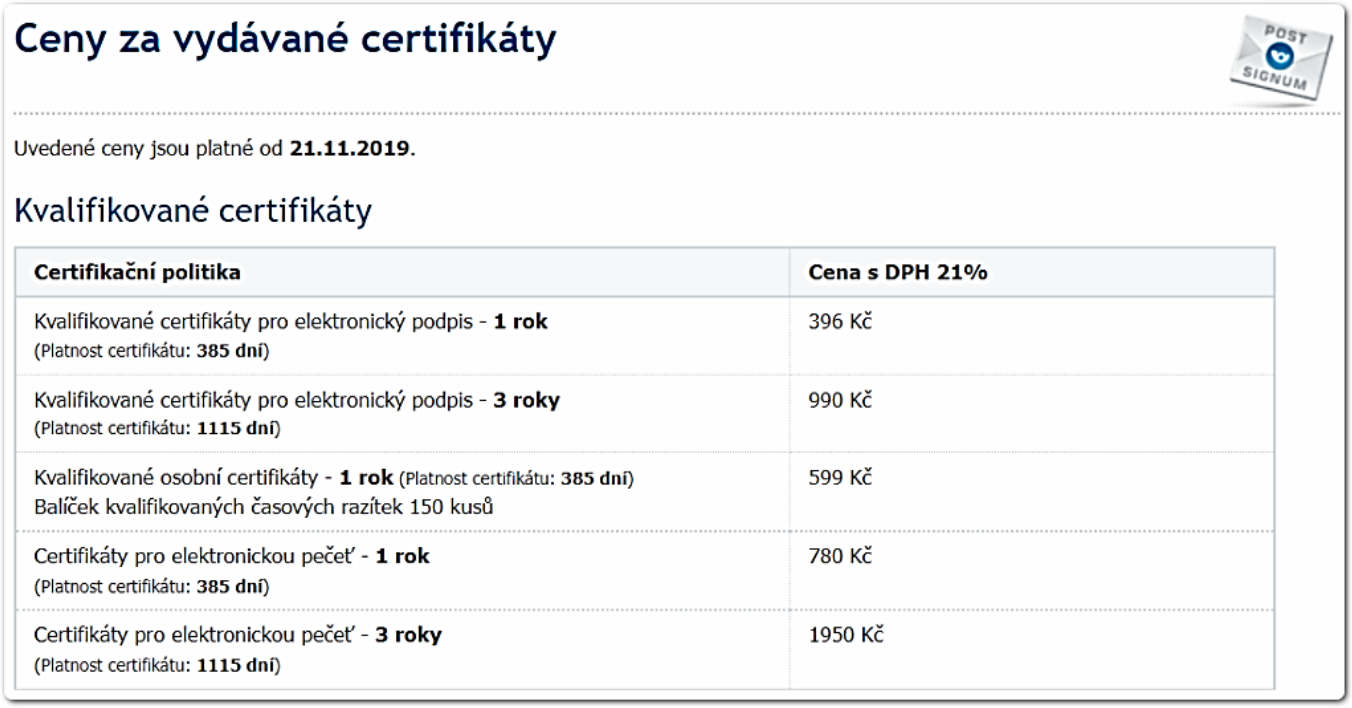
Zaručený el. podpis

Prostý elektronický podpis „vzniká propiskou“, zaručený elektronický podpis „vzniká certifikátem“. Jako uživatelé si certifikát můžeme koupit doslova za pár stovek. Dostaneme ho uložený třeba na kartě s čipem a instalujeme ho do svého zařízení. Certifikát má dvě části. Veřejnou a soukromou. Veřejná část se ptá: Podepsal dokument Jan Novák? A soukromá část odpovídá: Ano, podepsal ho Jan Novák. Zaručený elektronický podpis zaručuje, že ho z dokumentu není možné vyjmout, okopírovat a zneužít. A také zaručuje, že dokument nikdo po podpisu neupravil. Přesto, pokud bychom tento podpis chtěli použít pro oficiální komunikaci s českými úřady, nepochodíme. Proč? Není Jan Novák jako Jan Novák. Problém také je, že pokud nebude uživatel na své zařízení opatrný, může být jeho certifikát odcizen, zkopírován. Sice nikdo

nemůže z dokumentu vyjmout, okopírovat a zneužít náš podpis, ale může nám ukrást certifikát, tedy „propisku“.

Zaručený el. podpis s kvalifikovaným certifikátem

Tento typ podpisu zaručuje vše výše uvedené, ale navíc dokáže zaručit identitu podepisujícího. Zaručuje, že dokument skutečně podepsal Jan Novák, narozen 14. 12. 1992, s trvalým pobytem v Blansku. Proč? Protože kvalifikovaný certifikát si pořizujeme u tzv. certifikační autority, která při vydávání certifikátu důkladně ověřuje naši identitu oproti dokladům. Certifikační autority, mezi které patří například Česká pošta, tak mohou říct: „Zaručujeme, že jsme tohoto Jana Nováka ověřili oproti dokladům a vystavili jsme mu tento kvalifikovaný certifikát.“ Pokud bychom tento podpis chtěli použít pro oficiální komunikaci s českými úřady, pochodíme dobře. Nevýhoda podpisu ale zůstává. Certifikát, tedy „propiska“, může být odcizen.



Ceny za vydávané certifikáty

Uvedené ceny jsou platné od **21.11.2019**.

Kvalifikované certifikáty

Certifikační politika	Cena s DPH 21%
Kvalifikované certifikáty pro elektronický podpis - **1 rok** (Platnost certifikátu: **385 dní**)	396 Kč
Kvalifikované certifikáty pro elektronický podpis - **3 roky** (Platnost certifikátu: **1115 dní**)	990 Kč
Kvalifikované osobní certifikáty - **1 rok** (Platnost certifikátu: **385 dní**) Balíček kvalifikovaných časových razítek 150 kusů	599 Kč
Certifikáty pro elektronickou pečeť - **1 rok** (Platnost certifikátu: **385 dní**)	780 Kč
Certifikáty pro elektronickou pečeť - **3 roky** (Platnost certifikátu: **1115 dní**)	1950 Kč

Ilustrační obrázek ukazuje orientační ceny kvalifikovaných certifikátů od PostSignum k březnu 2022. Zdroj: postsignum.cz/certifikaty.html

Kvalifikovaný el. podpis

Nejvyšší úroveň elektronického podpisu. Zaručuje vše výše uvedené, ale s vylepšeným zabezpečením. Kvalifikovaný certifikát neinstalujeme do žádného zařízení. Zůstává na čipové kartě, kterou dostaneme při zřizování. Není technicky možné ho z karty odcizit. Samotná karta navíc k podpisu nestačí. Kartu připojujeme ke svému zařízení až v momentě, kdy se chceme podepsat. A podobně jako při placení platební kartou potřebujeme znát PIN. Lidé dávají větší pozor na věci, které mohou vzít do ruky než na něco, co je „někde nainstalováno“. Proto kartu s certifikátem chrání podobně jako třeba občanský průkaz. I proto mohou být současné občanské průkazy vydávány s čipem, který z nich udělá nosič kvalifikovaného certifikátu. Tento typ elektronického podpisu můžeme použít pro oficiální komunikaci s českými úřady.

Datová schránka

Datová schránka slouží k odesílání a přijímání důvěryhodných zpráv, tzv. datových zpráv. Při zřizování schránky se ověřuje identita žadatele, budoucího vlastníka. Proto má datová zpráva odeslaná datovou schránkou stejnou právní sílu jako zaručený elektronický podpis s kvalifikovaným certifikátem. Obdobné jsou také nevýhody v případě, kdy by někdo nepovolaný získal k datové schránce přístup. Jaké jsou zajímavé rozdíly? Elektronický podpis je možné spárovat s e-mailovou schránkou a posílat zprávy i do zahraničí. Datové zprávy je možné posílat jen do datových schránek, které jsou „českým vynálezem.“. E-mailem opatřeným náležitým elektronickým podpisem lze komunikovat přímo s konkrétním úředníkem, pomocí datové schránky lze komunikovat jen s celým úřadem jako celkem.

Ilustrační obrázek ukazuje podobu datové schránky k březnu 2022. Zdroj: mojedatovaschranka.cz/static/ISDS/help/page5.html#5

„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.

Kvalifikovaný certifikát od České pošty

Líbí se vám možnosti elektronických podpisů s kvalifikovaným certifikátem? Podívejte se na informační stránku jedné z certifikačních autorit, České pošty. Dozvíte se, jak kvalifikovaný certifikát získáte a jaké kroky je potřeba učinit: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/kvalifikovane-certifikaty

Služba MojeID

Autoritativní sdružení CZ.NIC, které má velký podíl na vývoji českého internetu, vyvinulo službu MojeID. Jedná se o elektronickou identitu, pomocí které můžeme přistupovat ke stovkám partnerských webů i do portálů státní správy bez dalšího přihlašování. Přihlašujeme se do MojeID, ne do samostatných webů, portálů a služeb. Ty naše přihlašovací údaje vůbec neznají. Pokud se dokážeme přihlásit k MojeID, dostanou jen vzkaz: „Ano, tento člověk je ověřený, můžete ho pustit.“ Podívejte se na web MojeID: https://www.mojeid.cz/cs/

Stalo se?

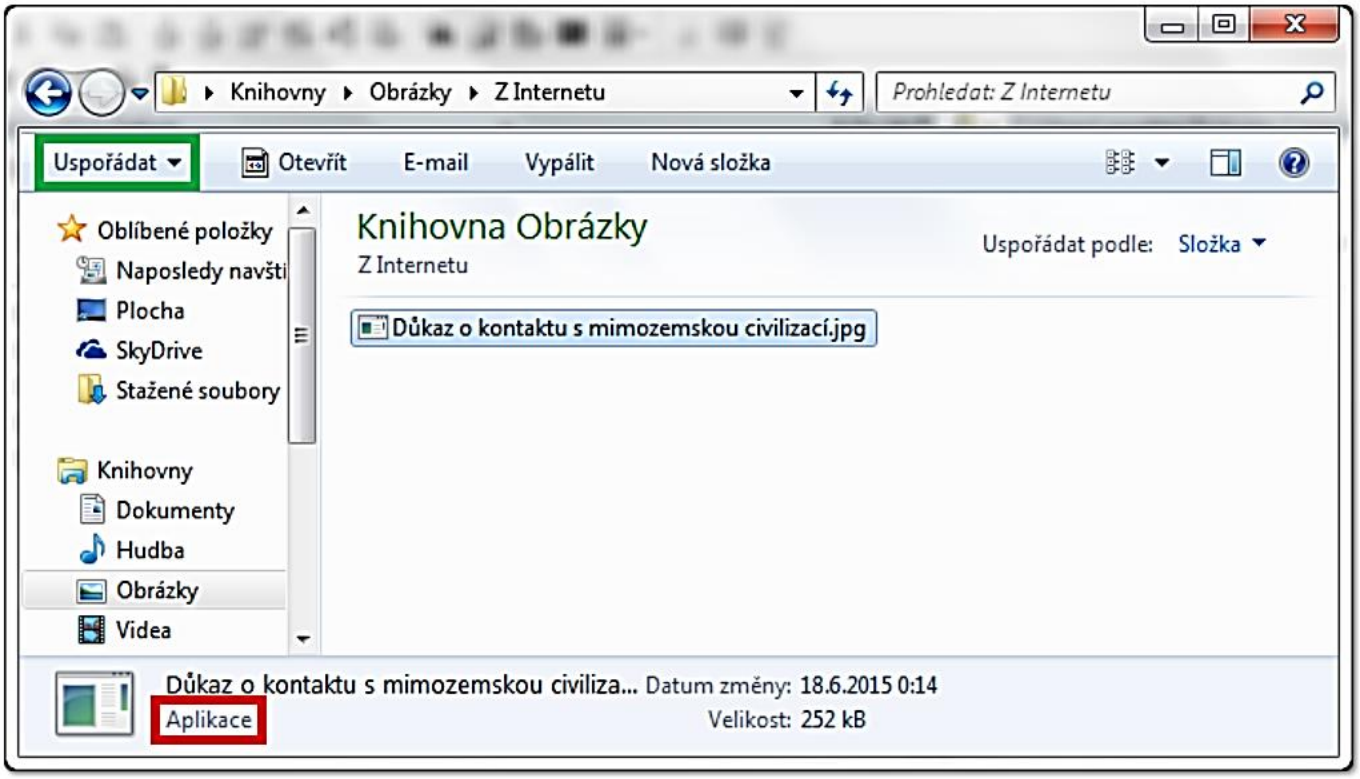
Radkovi je 44 let a pracuje jako účetní blíže neurčeného finančního úřadu. Zpracovává desítky podkladů, které mu přichází e-mailem. Nejčastěji v podobě tabulek v Excelu. Když otevřel jednu z tabulek, objevila se výzva, aby povolil tzv. makra. U výzvy bylo uvedeno, že makra zajistí správné fungování vzorců. Protože Radek zná Excel dobře, hláška ho nepřekvapila a makra povolil. Následně se mu zpomalil počítač. Ale protože byl počítač starší, nepřikládal tomu váhu. Rozhodl se, že když technika stávkuje, odejde dřív a práci dodělá ráno. Ráno se však nespustily účetní systémy, se kterými běžně pracuje. Po příchodu kolegů zjistil, že v tom není sám. Při odstraňování problému se zjistilo, že za vším stálo povolené makro.

Škodlivé soubory

Škodlivé soubory odeslané v příloze e-mailu jsou oblíbeným trikem útočníků. Protože uživatelé zpracovávají přílohy jako na běžícím pásu, útočníkům se leckdy poštěstí, že někdo jejich škodlivý soubor stáhne a otevře. Nejhorší bývají tzv. spustitelné soubory. Snad nejznámější spustitelný soubor mívá příponu .exe. Nutno zmínit, že spustitelné soubory nejsou samy o sobě špatné. Slouží třeba pro instalaci programů do počítače. Útočníci je ale umí zneužívat. Připraví spustitelný soubor, uživatel ho otevře a tím nainstaluje škodlivý program do svého zařízení. V zaměstnání bývá zvykem, že běžní uživatelé tyto soubory spouštět nemohou, nemají k tomu oprávnění. V ideálním případě by se k nám takový soubor neměl přes filtry vůbec dostat. Občas ale i takový soubor pronikne.

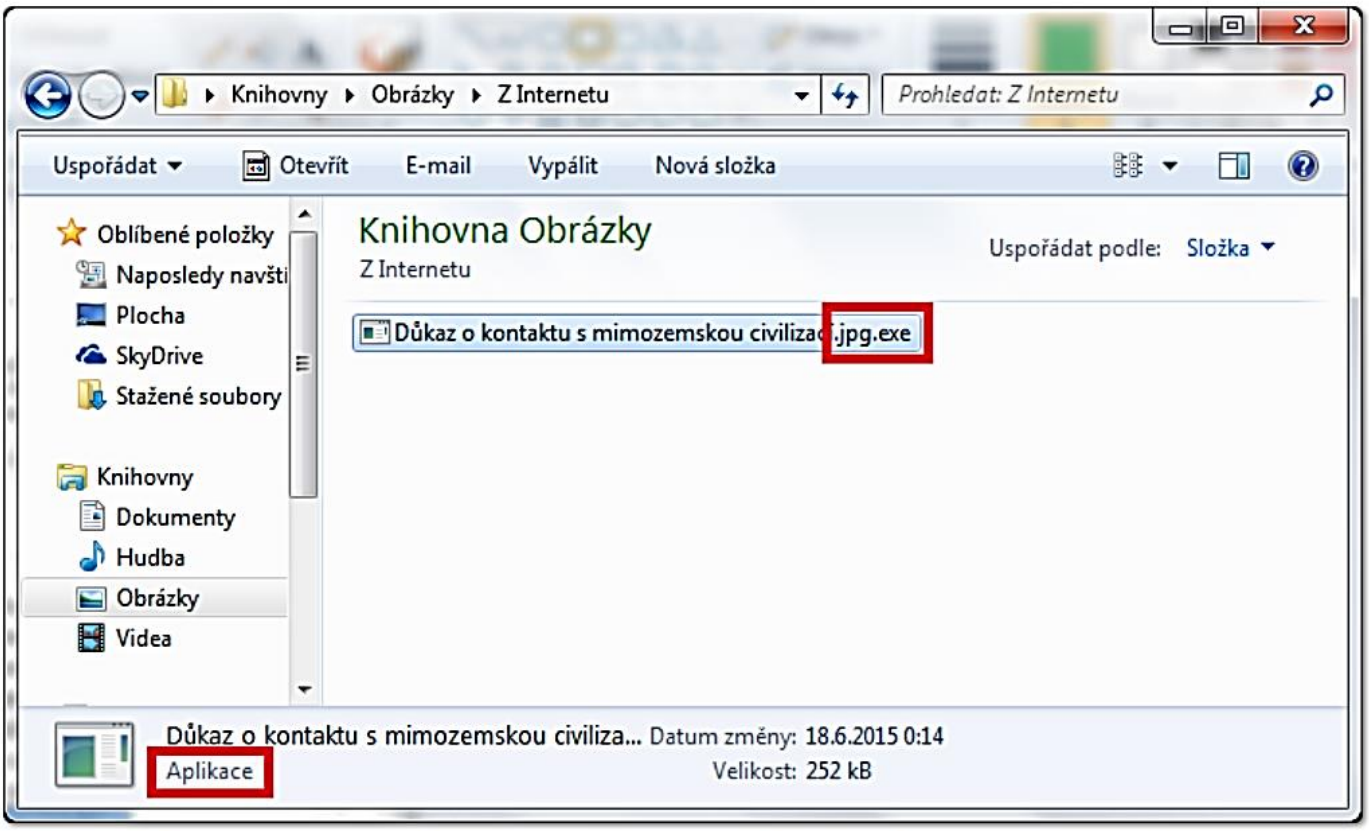
Maskování škodlivých souborů

Aby útočníci zvýšili pravděpodobnost, že uživatel škodlivý soubor otevře a spustí, maskují ho. Může být ukryt třeba v archivu, který umí zabalit více souborů do jednoho. Archivy mívají nejčastěji přípony .rar nebo .zip, například faktura.zip. Znovu platí, že archivy nejsou samy o sobě špatné, ale jako uživatelé bychom k nim měli přistupovat s rozvahou. Může se tam ukrývat černý Petr, třeba faktura.exe. A nemusí to být na první pohled patrné. Přípony se totiž dají také různě schovávat. To znamená, že vidíme například soubor obrazek.jpg, ale ve skutečnosti je to skodlivysoubor.exe, u kterého není vidět skutečná přípona, ale název je doplněn o následující: ".jpg".



Ilustrační obrázek ukazuje škodlivý spustitelný soubor, který se maskuje příponou obrázku. (1. část).

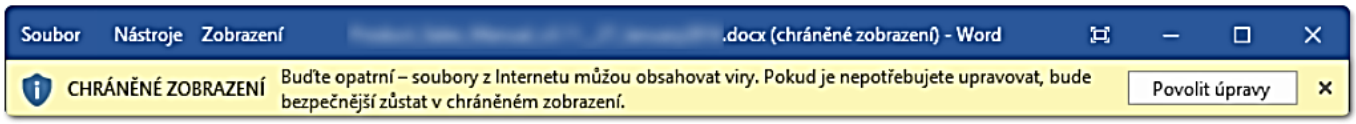
Zdroj: support.zcu.cz/index.php/Skrývání_přípon_v_systémech_Windows



Ilustrační obrázek, který ukazuje škodlivý spustitelný soubor, který se maskuje příponou obrázku. (2. část).

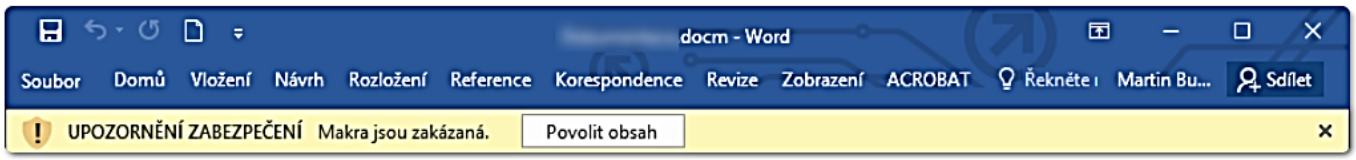
Makra

Uživatelé bývají překvapeni, že nebezpečné mohou být i soubory z balíčku Microsoft Office jako zmíněný Excel, Word nebo PowerPoint. Podle dostupných dat z České republiky tyto soubory umí napáchat paseku. Především v případě, kdy jako uživatelé povolíme spuštění tzv. makra. Makra jsou pokročilé sady pravidel, které si můžeme vytvořit, aby za nás vykonávaly opakující se úkony. Opět platí, že sama o sobě nejsou špatná. A opět také platí, že je útočníci umí zneužít. Mohou makru říct: „Stáhni z tohoto odkazu tento škodlivý soubor, počkej v úkrytu na tohle, a pak vykonej tohle.“ I proto se Microsoft rozhodl, že makra v základním nastavení vypne a uživatel je musí sám povolit. Pokud dobře neznáte historii souboru, který vyžaduje povolení makra, nepovolujte ho. Na obrázcích níže si všimněte, že soubory s makrem mají příponu .docm, bez makra .docx, podobně tu funguje i u Excelu nebo PowerPointu. „M“ jako „makro“.



Ilustrační obrázek lišty chráněného zobrazení.

Zdroj: servis.eset.cz/knowledgebase/article/View/596/0/jak-zabranit-spoustni-maker-v-dokumentech-stazenych-z-internetu



Ilustrační obrázek lišty, která umožňuje povolení a spuštění makra.

Zdroj: servis.eset.cz/knowledgebase/article/View/596/0/jak-zabranit-spoustni-maker-v-dokumentech-stazenych-z-internetu

Ransomware

Škodlivé soubory mohou nést a spouštět škodlivé programy. Ransomware je škodlivý program, který zašifruje data, soubory, nebo celé systémy, aby k nim uživatelé ani administrátoři neměli přístup. Poté vyžaduje výkupné za dešifrování. O výkupné si ransomware zpravidla řekne v momentě, kdy už nic nefunguje. Pokud se jedná o firmu nebo nemocnici, dostane se pod obrovský tlak. Představte si, že nefunguje ani rentgen, jde o lidské životy a zaplacení výkupného se jeví jako nejrychlejší řešení. Obecně se ale doporučuje výkupné neplatit. Jak se k běžnému uživateli takový škodlivý program dostane? Třeba jako soubor v příloze e-mailu nebo na „flešce“. Pokud takový soubor naneštěstí otevřeme a podaří se nám ransomware rozpoznat, jediná použitelná rada je okamžitě celé zařízení vypnout nebo ho vypojit přímo ze zásuvky.

Proč se doporučuje výkupné neplatit?

Dříve útočníci zvyšovali motivaci k zaplacení výkupného příslibem, že po zaplacení vše dešifrují. Byla to „etiketa“ útočníků, kteří po zaplacení výkupného často poskytli dešifrovací klíče. Dělali to mj. právě proto, aby se vědělo, že platit výkupné má smysl. Jenže této „etikety“ se nedrží všichni útočníci, takže se obecně začalo doporučovat výkupné neplatit, ale požádat o pomoc renomované odborníky a zaplatit raději jim. Proto nastoupilo víceúrovňové vydírání, třeba výhružkami zveřejnění všech dat. Například zdravotních dokumentací. Na černém trhu dokonce existují i služby „RaaS“, Ransomware as a Service, které si je možné koupit za pár desítek dolarů. Využívá se to například pro konkurenční boj.

Existují nějaká preventivní opatření před ransomwarem?

Bezpečnostní komunita se shoduje, že účinnou prevencí před ransomwarem je pravidelné, nejlépe zautomatizované, zálohování. Pokud máme důležité soubory uložené ještě mimo zařízení, abychom je v případě potřeby mohli obnovit, máme eso v rukávu. Nezapomeňte však zálohy čas od času vyzkoušet, aby se v případě potřeby nezjistilo, že jsou nefunkční.

Ilustrační obrázek ukazuje, jak vypadá obrazovka ransomware, která žádá o výkupné.

Zdroj: bankinfosecurity.com/blogs/avaddon-ransomware-operation-call-quits-releases-keys-p-3057

„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.

Robot, který prozkoumá web

Dalším nástrojem, který můžete uplatnit, je Screenshot Machine. Využití v praxi je jednoduché. Stačí vložit libovolnou webovou adresu a tento robot ji navštíví místo nás. Co se stane? Uvidíme snímek obrazovky cílového webu. Tak si ověříme, kam se dostaneme, když na daný odkaz klikneme. Vyzkoušejte: https://www.screenshotmachine.com/

50 antivirů v 1

Podezřelý odkaz/soubor můžeme bez otevření prověřit pomocí nástroje VirusTotal. Pokud sem odkaz/soubor vložíme, porovná ho VirusTotal s databázemi více než 50 antivirových programů. Když odkaz/soubor některá z databází eviduje, jsme informováni. Ale pozor, není dobré sem nahrávat nic interního nebo citlivého. Uživatelé, kteří platí premium verzi, mohou nahrané soubory libovolně stahovat. Vhodnější je tedy vytvořit hash souboru, který chceme zkontrolovat. Pokud máte nainstalovaný program 7-Zip, klikněte pravým tlačítkem na daný soubor, vyberte CRC SHA a vložte vygenerovaný SHA-1 nebo SHA-256 hash do vyhledávání ve VirusTotal. Získáme stejný výsledek, aniž bychom soubor někam odeslali. Nástroj najdete zde: https://www.virustotal.com/gui/home/upload

Bezpečnostní nástroje

Aniž bychom o tom přemýšleli, na naši bezpečnost v kybernetickém světě dohlíží různé nástroje. Dávají pozor na technické záležitosti, kterým my, běžní uživatelé, moc nerozumíme. Kolik požadavků z našeho zařízení odchází, kolik požadavků přijímáme, jestli program nezahájil neobvyklou činnost atp. V zaměstnání se tyto nástroje řídí bezpečnostní politikou IT. Někdo za nás pečuje o nastavení bezpečnostních nástrojů, aby fungovaly, jak mají. Proto zpravidla platí, že zaměstnanecká zařízení bývají chráněna lépe než naše domácí. V našem vlastním zájmu však je, abychom základy bezpečnostní politiky IT dodržovali i doma.

Aktualizace

Aktualizace si uživatelé spojují s vylepšením programu, s novými funkcemi nebo grafikou. A mají pravdu. Aktualizace skutečně slouží k vylepšování. Takže i pro opravu bezpečnostních děr a chyb v programu. Ty vznikají při vývoji. Vývojáři si někdy prostě neuvědomí všechny souvislosti svých kroků. Nebo se vývojem technologií stane nebezpečné něco, co bývalo bezpečné. Když se taková chyba objeví, připraví se pro ni záplata, aktualizace. Pokud je uživatel oddaluje, dává útočníkům doslova náskok. Vynalézaví útočníci se totiž zaměřují na objevování ještě nezáplatovaných chyb a učí se je využívat. Je to závod vývojářů a útočníků. Dokonce existují nástroje, které umí vyhledávat neaktualizovaná zařízení připojená k internetu.

Firewall

Představte si hrad a hradby kolem. Jediná možnost, jak přes hradby projít, je hlavní brána se stráží. Brána se otevírá jen těm, koho stráž zkontroluje. Takhle funguje firewall. Naše zařízení je hrad, firewall jsou hradby s bránou a stráží. Všechny požadavky, které naše zařízení z internetu přijímá, jsou směřovány ke stráži na kontrolu. Firewall za uživatele tedy řeší rozhodnutí, kterým by nerozuměli a nevěděli by, co s nimi dělat. Firewall rozhoduje, co pustíme dovnitř zařízení a co ven, abychom zůstali v bezpečí. Opatření provádí na základě daných pravidel. Je proto důležité nevypínat firewall ani na domácích zařízeních. Firewall si uživatelé někdy pletou s antivirovým programem, nedělají ale totéž.

Antivirový program

Zůstaneme-li u přirovnání k hradu, antivirový program jsou vnitřní stráže, které neustále prochází místnosti hradu. Když najdou někoho, kdo sem nepatří, zajmou ho a zavřou. Antivirový program má v sobě něco jako knihovnu virů a dalších hrozeb, proti kterým nás umí dobře bránit. Pokud antivirový program vyhodnotí, že jsme v ohrožení, podívá se do knihovny, načte si doporučený postup a koná. To je hlavní úkol každého antivirového programu. Placené a neplacené verze se liší především škálou funkcí, základ zůstává v principu stejný. Aby antivirový program věděl o novinkách ve světě, musí mít dokonale aktualizovanou knihovnu. Aktualizace už znáte.

Který antivirový program je nejlepší?

Jedná se o antivirový program značky „jsem aktualizovaný“. Jen o antivirovém programu to totiž není. Běžný uživatel jen těžko pozná rozdíly mezi jednotlivými programy. Některé mají tendenci spustit planý poplach, když se nic neděje. Ale není to lepší než nespustit poplach v momentě, kdy se něco děje? V tomto případě také neplatí, že více je lépe. Antivirový program mějte jen jeden, když je jich více, vzájemně se matou.

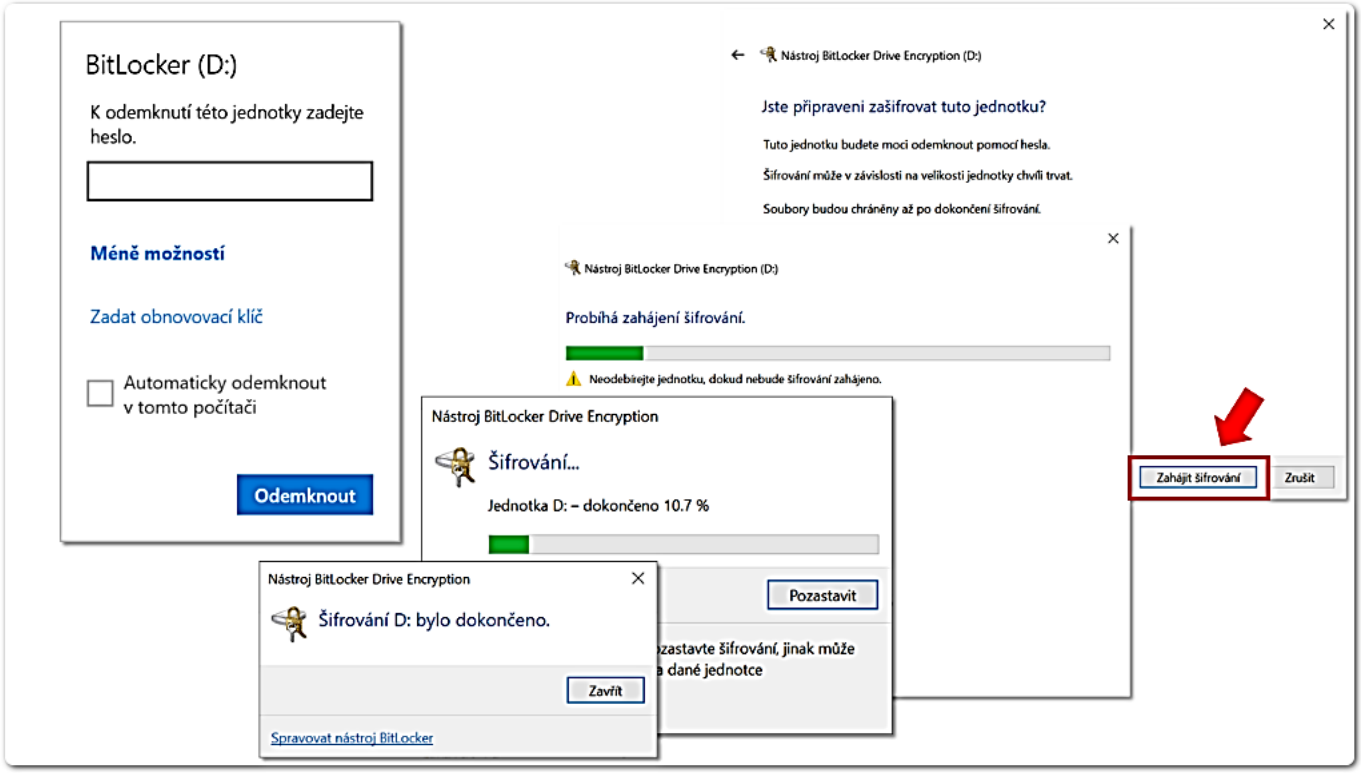
Stačí mi mít doma jen neplacený antivirový program?

Aktualizovaný a spolu se zodpovědným chováním uživatele? Ano. Microsoft Windows má navíc od řady 10 vlastní antivirový program Defender, který funguje dobře sám o sobě. V některých žebříčcích a nezávislých recenzích se dokonce Defender umisťuje na prvních příčkách.

Zálohování

Nikdo není neomylný, ani stráže. Jak z historie víme, mnoho hradů padlo i přes důmyslné zabezpečovací systémy. Může se stát, že do našeho zařízení pronikne něco, co opatření přechytračí a udělá neplechu. Proto je vhodné alespoň důležité soubory zálohovat. Jenže co to prakticky znamená? Je dobré mít nějaké

dobře zabezpečené místo, kam čas od času nahrajeme důležité soubory a dokumenty. V zaměstnání za nás zálohování zpravidla řeší bezpečnostní politika IT a nastavené procesy. Pro domácí účely můžeme zvolit zabezpečené cloudové úložiště nebo důvěryhodnou „flešku“. „Flešku“ je nejlepší zašifrovat, s tím může pomoci třeba nástroj BitLocker, který je součástí posledních verzí Windows. Zálohování je veledůležité, pokud se staneme obětí dříve zmíněného ransomware.



Ilustrační obrázek ukazuje nástroj BitLocker a šifrování USB flash disku. Zdroj: Vlastní tvorba

„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“.

Automatické aktualizace aplikací

Aktualizace jsou důležité samozřejmě i pro mobilní aplikace. V nastavení chytrého telefonu můžete nastavit, aby se aktualizace vykonávaly automaticky. Podívejte se na návody pro zařízení s operačním systémem

iOS: https://support.apple.com/cs-cz/HT202180 nebo s operačním systémem Android: https://support.google.com/googleplay/answer/113412?hl=cs

Kanárek, který varuje před hackery

Své soubory, složky nebo e-maily můžete chránit také nástroji, kterým se říká Canary Tokens. Označení „Canary" odkazuje na kanárky, kteří se kdysi používali v dolech. Varovali horníky před unikajícím plynem. Canary Tokens fungují podobně. Pokud se děje něco, co by se dít nemělo, vyskočí upozornění. Vše ukazuje tutoriál: https://www.youtube.com/watch?v=apixhc43JuE

Obchody s aplikacemi

Kromě předinstalovaných aplikací můžeme do telefonu stahovat a instalovat také další. Je více než vhodné využívat jen oficiální zdroje, tzv. obchody s aplikacemi. Slovo „obchod" sice zavání placením, větší část aplikací je však bezplatná. Oficiální obchod pro telefony se systémem Android je Google Play. Android využívá mnoho značek telefonů. Oficiální obchod pro telefony se systémem iOS je App Store. iOS využívají jen telefony značky Apple. Aplikace v nabídce oficiálních obchodů prošly bezpečnostní kontrolou, jenže ani ta není stoprocentní. Občas škodlivá aplikace do nabídky proklouzne. Nebo se objeví zneužitelné nedostatky, o kterých se nevědělo. Trendem jsou fiktivní pobídky k testování vyvíjených aplikací s příslibem odměny. Jenže takové aplikace neprošly ještě žádnou kontrolou a mohou být velmi nebezpečné. Škodlivé aplikace nebo jejich části nabízí útočníci k dispozici také na černém trhu. Možná vás překvapí, že mají dokonce své produktové stránky i marketing.

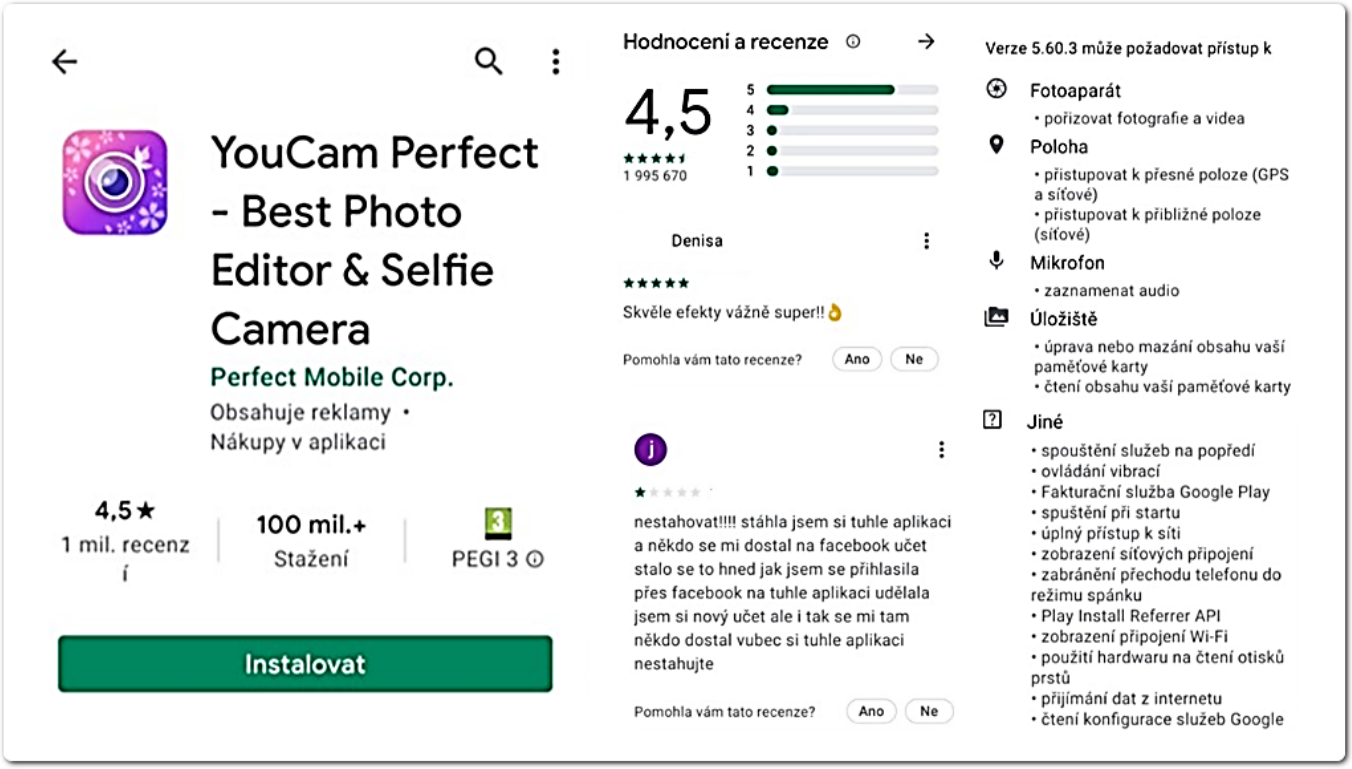
Jak se škodlivé aplikace projevují?

Projevují se rozmanitě. Některé zablokují telefon třeba tím, že změní odemykací PIN. Některé fungují na první pohled správně, ale na pozadí dělají neplechu. Třeba zachytávají a odesílají útočníkovi, co píšeme na klávesnici a poskytují mu přístup k našim SMS. Tímto způsobem je možné získat přihlašovací údaje uživatele včetně SMS kódu pro dvoufaktorové ověřování. Některé zaplaví uživatele nevyžádanou reklamou. Jiné rozešlou stovky drahých MMS zpráv.

Ilustrační obrázek ukazuje propagační web a dovednosti škodlivé aplikace. Umí například smazat všechny SMS zprávy, nahrávat audiozáznam nebo zobrazovat podvodná upozornění. Zdroj: forbes.cz/jestli-mate-v-telefonu-tyhle-aplikace-okamzite-je-smazte-chytili-jste-trojsky-kun-rogue/

Výběr aplikací

Neexistuje žádný seznam aplikací, které bychom stahovat neměli. Za pár minut už by nebyl aktuální. Proto je důležité aplikace před instalací kontrolovat. Škodlivé aplikace mohou být maskovány i jako aplikace, které slouží k editaci fotografií, nebo právě jako antivirový program, u kterého nečekáme, že by mohl být škodlivý. Vždy bychom ještě před stažením aplikace měli sledovat její hodnocení a recenze dalších uživatelů. Vyplatí se vyfiltrovat špatná hodnocení, špatné recenze a podívat se, v čem nespokojenost vězí. Pokud budou v pořádku, je dobré se při samotné instalaci aplikace zamyslet i nad tím, jaká vyžaduje oprávnění vůči telefonu.

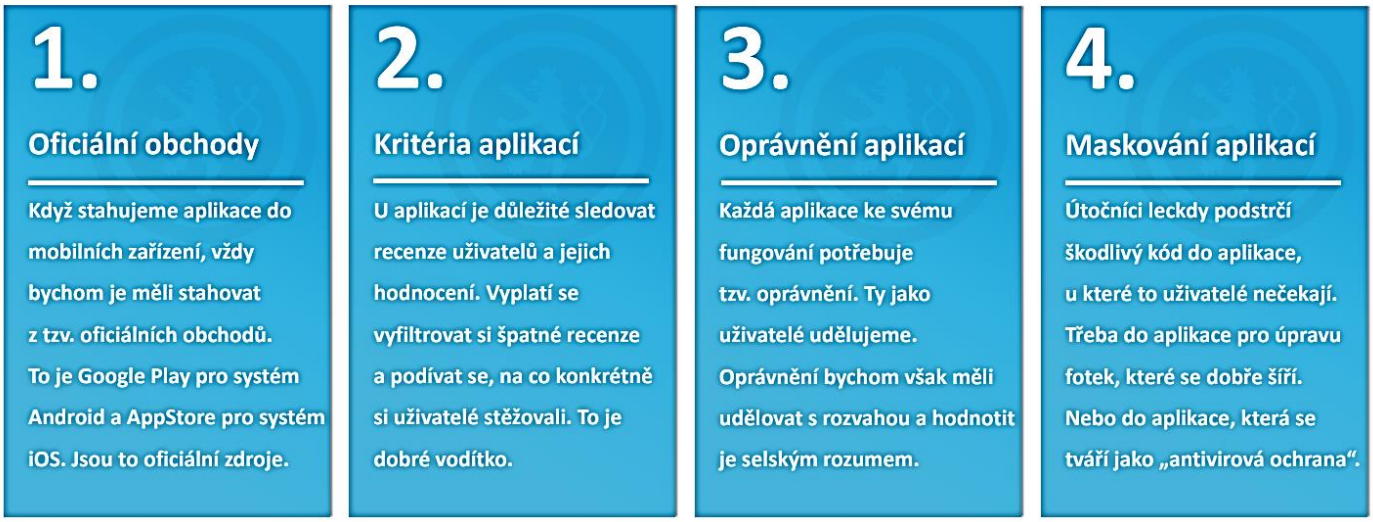


Ilustrační obrázek ukazuje podezřelou aplikaci a její hodnocení. Na aplikaci upozorňoval mj. článek: idnes.cz/mobil/aplikace/zkrasleni-mobilni-aplikace-malware-spehovani-spyware.A200124_102127_aplikace_LHR Zdroj: Vlastní tvorba

Oprávnění aplikací

Znovu platí, že oprávnění nejsou sama o sobě špatná. Bez patřičných oprávnění nemůže aplikace fungovat. Aplikace pro úpravu fotografií, která nemá přístup do galerie, nenaplní očekávání. Taktéž aplikace pro navigování, která nemá přístup k poloze. Ale je v pořádku, že hudební aplikace vyžaduje přístup ke zprávám? Pravdou je, že kontrola oprávnění se uživatelům komplikuje. V době, kdy můžeme telefon ovládat hlasem, může být v pořádku, že chce kalendář přístup k mikrofonu. Proto se nám vývojáři Androidu i iOS snaží pomáhat. I pro ně je to ale zapeklitá situace. Kdyby se aplikace stále dokola dotazovala na vše, co chce udělat, nebudou ji uživatelé používat. Budou se uchylovat k aplikacím, které budou komfortnější, i kdyby byly méně bezpečné. Vývojáři tedy hledají zlatou střední cestu. Například když si aplikace vynutí spuštění mikrofonu, objeví se puntík, který znamená „pozor, běží mikrofon“.

„TAHÁK DO KAPSY“: STAHOVÁNÍ APLIKACÍ



Revize oprávnění aplikací

Udělejte digitální úklid. Oprávnění aplikací, které máte v telefonu nainstalovány, můžete řídit i zpětně.
Návod pro telefony s Android: https://support.google.com/googleplay/answer/9431959?hl=cs
Návod pro telefony s iOS: https://support.apple.com/cs-cz/guide/iphone/iph251e92810/ios

Naučte aplikace spolupracovat

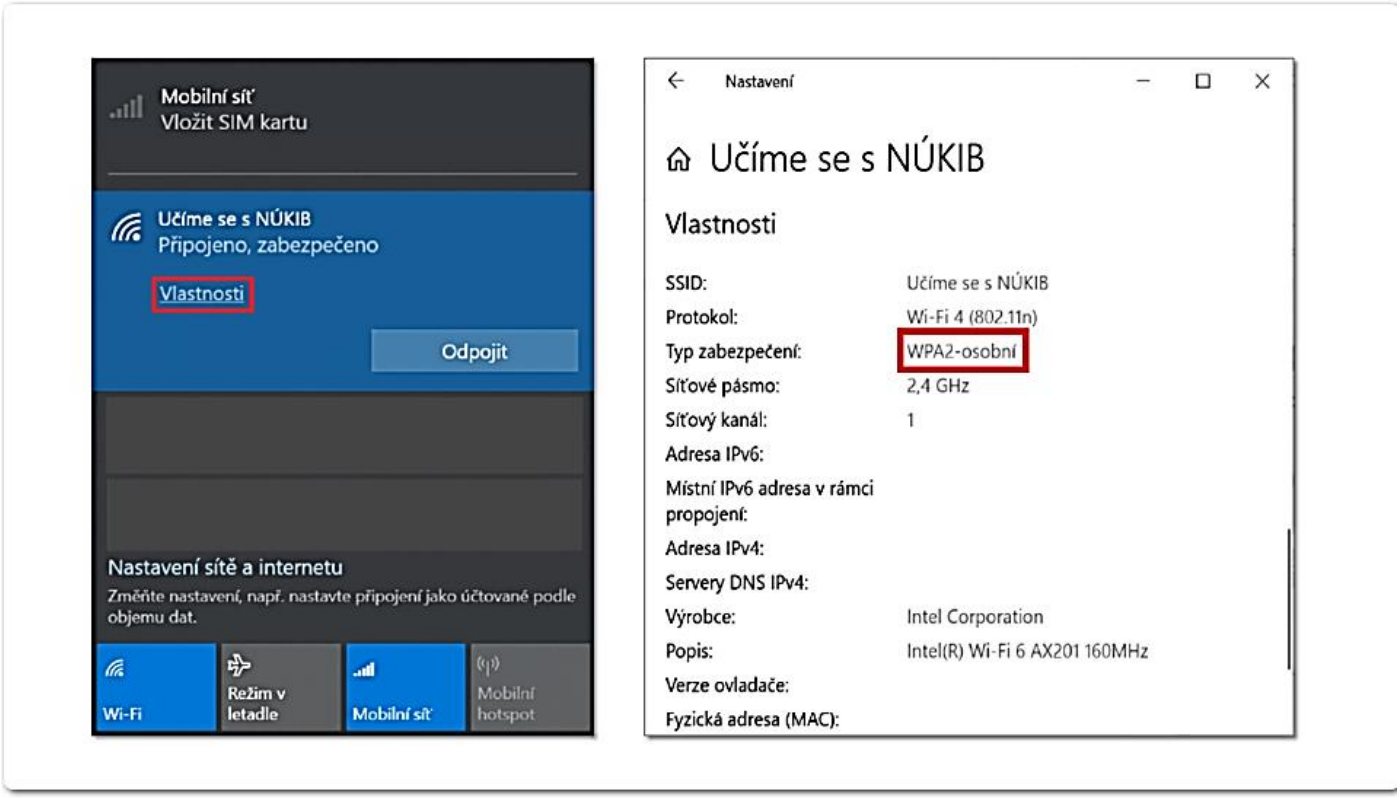
Jaké by to bylo, kdyby se aplikace dokázaly propojit a vzájemně využívat své dovednosti? Automatické zapnutí wi-fi po příchodu domů a čerstvě uvařená káva z chytrého kávovaru? Spuštění relaxační hudby vždy ve 22:00? Se službou IFTTT (if this, then that) žádný problém. Vše je uživatelsky přívětivé, řada šablon je již připravena od jiných uživatelů. Vyzkoušejte: https://ifttt.com/

Veřejné wi-fi sítě

Smyslem veřejných wi-fi sítí, které pro připojení nevyžadují žádné heslo, je poskytnout třeba hostům v kavárně rychlý a pohodlný přístup k internetu. Jenže otevřenost těchto sítí je také jejich slabina. Jsou totiž otevřené opravdu všem. Technicky zdatný uživatel dokáže bez větších obtíží sledovat, co na síti děláme a co odesíláme. Pokud takovou síť připraví přímo útočník a pojmenuje ji „kavarna-na-rohu“, má hotovo. Veřejné wi-fi sítě slouží spíše pro zjištění, kdy jede vlak nebo do kdy má cukrárna otevřeno. Když veřejnou wi-fi síť musíme využít, je lepší se vyhnout odesílání jakýchkoliv přihlašovacích údajů. Pokud se někam přihlašovat musíme, je nutné, aby daná stránka byla opatřená protokolem HTTPS.

Jak jsou na tom wi-fi opatřené heslem?

Pokud je wi-fi opatřená heslem, znamená to, že mezi naším zařízením a zařízením, které vysílá wi-fi signál, prochází data v zašifrované podobě. Ale není pravda, že je toto automaticky dostatečné zabezpečení. Záleží totiž na tom, jak je nastavené šifrování. Některé typy šifrování jsou již překonané. To znamená, že se dají prolomit a stejně někdo může sledovat, co na internetu děláme. Optimální je, když je nastaveno alespoň šifrování WPA2.



Ilustrační obrázek ukazuje nastavení wi-fi sítě, jejíž šifrování lze označit za silné Zdroj: Vlastní tvorba

Pomůže mi na veřejné wi-fi síti anonymní režim prohlížení?

Nepomůže. Nenechme se ošálit pojmem „anonymní“, nejsme více anonymní než při obyčejném prohlížení. Rozdíl je pouze v tom, že se v našem webovém prohlížeči neukládá historie toho, co jsme dělali a na co jsme se dívali. Směrem do internetu se vlastně nic nemění. Anonymita prohlížení končí v našem prohlížeči. Anonymní režim nám pomůže jen s tím, že na nás webový prohlížeč neprozradí, jaký dárek jsme vyhledávali atp.

K čemu je z hlediska kybernetické bezpečnosti dobrý anonymní režim?

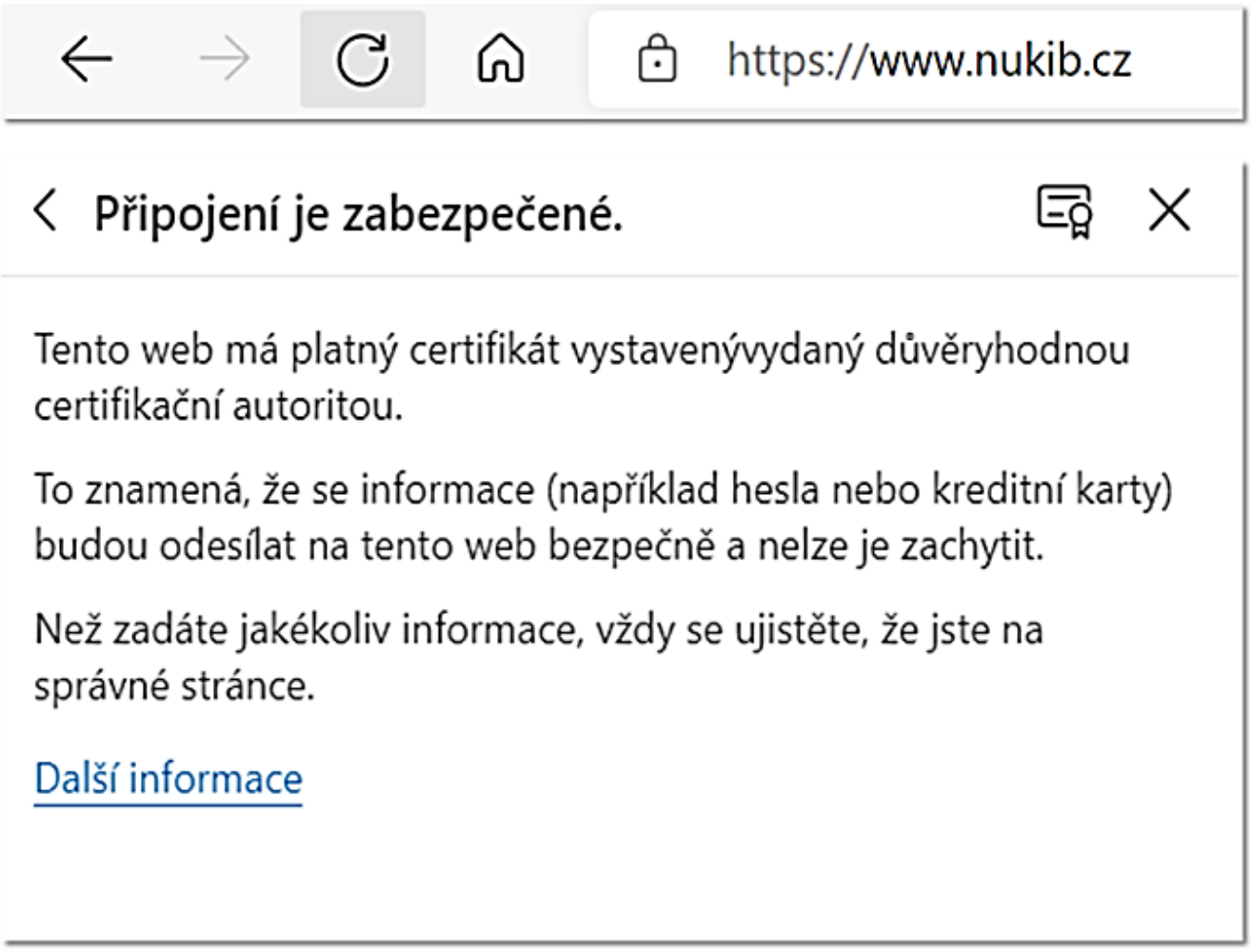
Anonymní režim je dobrý, pokud jsme na cizím zařízení, kterému ale důvěřujeme, a ze kterého se chceme přihlásit do svých služeb. Anonymní režim má z hlediska kybernetické bezpečnosti tu výhodu, že si po zavření okna prohlížeče nepamatuje naše přihlašovací údaje a odhlásí nás ze služby. Další výhodou je, že když se popleteme a zadáme heslo do kolonky uživatelské jméno, nebude se naše heslo ukazovat v našeptávači.

Protokol HTTPS

Na soukromí uživatelů dohlíží také protokol HTTPS. Webová stránka opatřená HTTPS nám říká, že je komunikace mezi stránkou a naším webovým prohlížečem šifrovaná. Že je čitelná jen pro nás a pro webovou stránku. HTTPS můžeme vídat jako součást adresního řádku, například: **https:// nukib.cz**. S HTTPS bývá spojen také symbol zámečku. Pokud by nás někdo sledoval, třeba na veřejné wi-fi síti v kavárně, může zjistit, že jsme odešli na stránku **https:// moje-bankovnictvi.cz**, ale tím končí. HTTPS je tedy důležité u webových stránek, kde se přihlašujeme nebo třeba platíme platební kartou. Současné webové prohlížeče už HTTPS nezdůrazňují, zámečky postupně mizí. Je vnímáno jako norma. Uživatelé budou do budoucna upozorněni jen na weby, které HTTPS nemají.

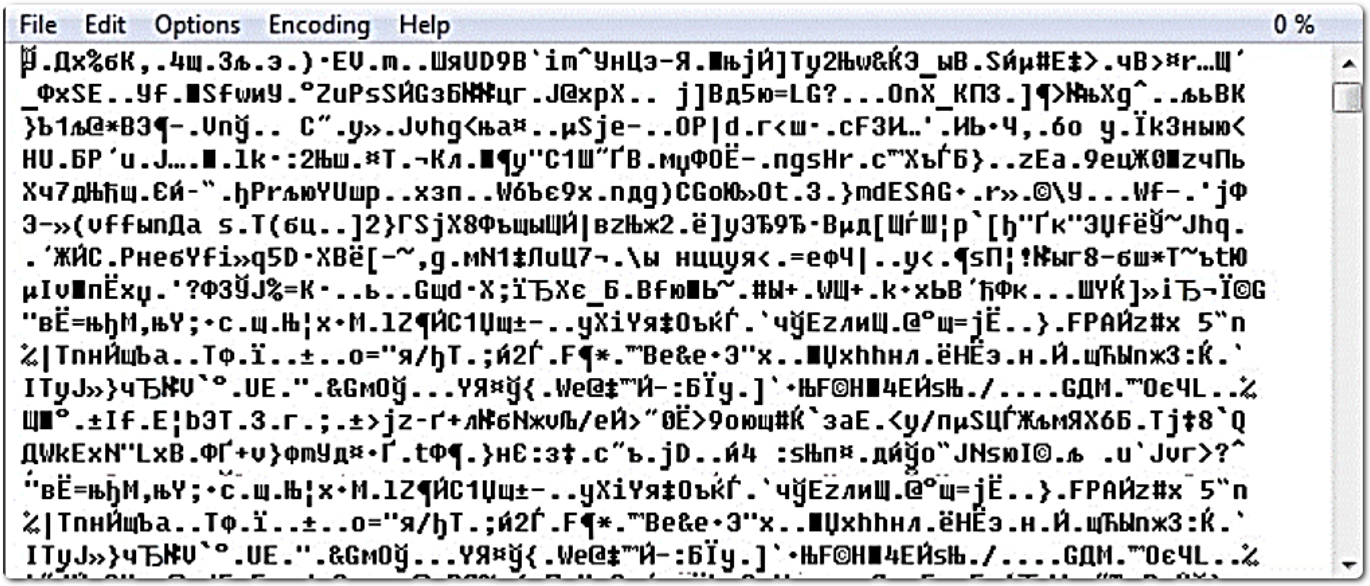
Umí útočníci HTTPS nějak zneužít?

Ano, umí. Mylně se totiž vžilo do povědomí uživatelů, že web opatřený HTTPS je dokonale bezpečný. To není pravda. HTTPS nezaručuje, že obsah webové stránky, na kterou přicházíme, není sám o sobě škodlivý. Ani to, že stránka není podvržená. Útočníky tak napadlo, že paradoxně uživatele nachytají lépe s podvrženou webovou stránkou, naplněnou škodlivým obsahem, která je opatřena HTTPS. Právě kvůli mýtu, který kolem HTTPS koluje.



Koncové šifrování (též end-to-end šifrování)

Velký význam v on-line komunikaci má tzv. koncové šifrování, které slouží pro komunikaci mezi uživateli. Odeslané zprávy s koncovým šifrováním, včetně obrázků a souborů, dokáže číst jen jejich odesílatel a příjemce. Nikdo mezi nimi. Ani provozovatel služby, přes kterou komunikují. Ale pozor. Ne všechny komunikační nástroje koncové šifrování využívají. Klasické SMS nevyužívají koncové šifrování. E-mailové schránky, které si můžeme zdarma založit, obvykle nevyužívají koncové šifrování. U e-mailových klientů typu Outlook je možné koncové šifrování nastavit, ale aby fungovalo, musí ho umět klient příjemce i odesílatele. Některé messengery toto šifrování využívají, některé tvrdí, že ho používají, některé ho nepoužívají. Při výběru nástrojů pro komunikaci je dobré si zjistit, zda koncové šifrování nabízí.



Ilustrační obrázek ukazuje, jak může vypadat zašifrovaná zpráva pomocí koncového šifrování. Takto zprávu vidí někdo, kdo ji dokáže zachytit, ale nedokáže ji přečíst. Zdroj: dvojklik.cz/k-cemu-je-sifrovani-a-sifrovana-komunikace-na-internetu/

VPN (též virtuální privátní síť)

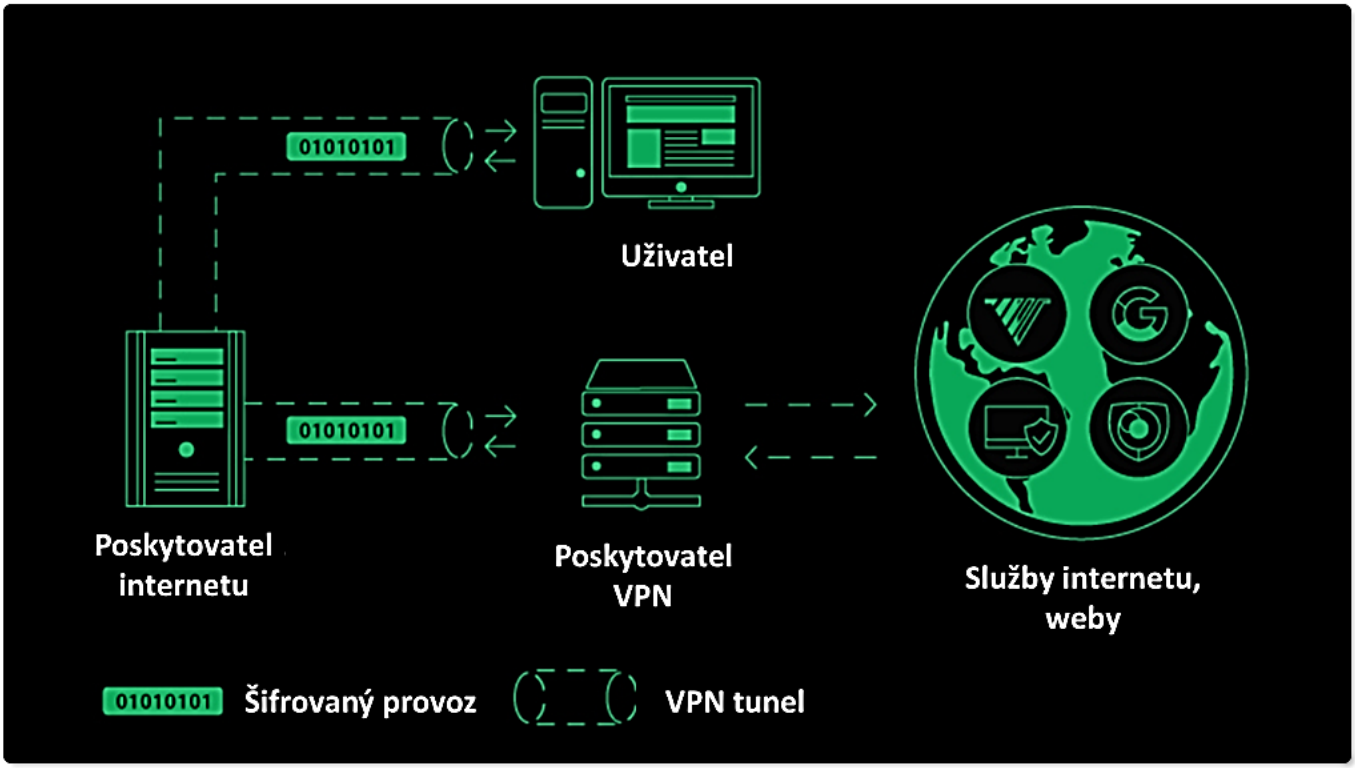
Službu, která zajišťuje maximálně soukromé připojení uživatele k internetu, nazýváme VPN. VPN si můžeme představit jako šifrovaný tunel. Vše, co na internetu děláme a odesíláme, prochází tímto tunelem a pro útočníky je to nečitelné. Nedokážou to špehovat. Do tunelu se vleze i naše připojení k veřejné wi-fi síti v kavárně. Od veřejné wi-fi se pomyslně oddělíme. Jako bychom si v divadle koupili lístek do soukromé lóže. Jsme v divadle, využíváme jeho prostory, ale jsme bokem a máme soukromí. S VPN se často setkáváme v zaměstnání, kdy ho nastaví IT oddělení. My pak můžeme z domova nebo ze služební cesty vzdáleně přistupovat třeba na sdílené pracovní disky nebo do spisové služby. Pro tento účel původně VPN vzniklo.

Jaký je rozdíl mezi VPN a koncovým šifrováním?

Koncové šifrování se využívá pro šifrování komunikace. Šifruje zprávy mezi odesílatelem a příjemcem. VPN šifruje naše internetové připojení a vše, co v něm protéká. Šifruje komunikaci mezi naším zařízením a zařízením poskytovatele VPN. Poskytovatel VPN vystupuje na internetu jako náš zamaskovaný dvojník. Obě technologie se nenahrazují, vzájemně se doplňují.

Jak získám VPN pro osobní účely?

VPN si může každý uživatel bez problému pořídit sám. Je to otázka pár kliknutí. Stačí si pročíst recenze a vybrat důvěryhodného poskytovatele služby. Služba bývá typicky zpoplatněna v řádu stovek korun. K VPN se pak přihlašujeme jako ke kterékoliv jiné službě, čímž se šifrovaný tunel aktivuje. Existují i neplacené varianty, ale leckdy bývají s funkčností nebo důvěryhodností na štíru. Důvěryhodnost a reputace poskytovatele je pro VPN klíčová.



Ilustrační obrázek ukazuje, jak funguje VPN. Komunikace od nás k poskytovateli VPN (a obráceně) je šifrovaná. Dále do internetu za nás vystupuje poskytovatel VPN, který nás směrem do internetu jako zastupuje. Upraveno, původní zdroj: cybernews.com/what-is-vpn/

„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.

Vyhledávač DuckDuckGo

DuckDuckGo dbá na soukromí uživatelů. Tvrdí, že nesbírá a nevyužívá data o uživatelích ani o jejich vyhledávání. Vyhýbá se i reklamám, žádné neukazuje. Nevýhodou vyhledávače je, že nemá tak přesné výsledky, jak jsme zvyklí třeba od Googlu. Je to daň za soukromí, které poskytuje.
Vyzkoušejte: https://duckduckgo.com/

Portál PrivacyTools.io

Portál shromažďuje na jedno místo služby a aplikace, které na bezpečnost uživatelů dbají. Ať už jsou to doplňky webových prohlížečů, VPN, vyhledávače, messengery, platební aplikace nebo jiné. Podívejte se, co zaujme vás: https://www.privacytools.io/

Zranitelnosti

Zranitelnosti jsou slabiny v aplikaci, systému nebo jiné programové výbavě. Vznikají například proto, že jsou programová vybavení stále sofistikovanější a komplexnější. Je náročné kontrolovat, že úpravou na jedné straně nevznikne zranitelnost na straně druhé. Je logické, že útočníci zranitelnosti aktivně vyhledávají. Aktivně je vyhledávají také vývojáři, kteří se v případě objevení zranitelnosti snaží co nejrychleji připravit opravu, vyvinout aktualizaci. Útočníci zase vyvíjí tzv. exploit. Exploit je zlý sourozenec aktualizace. Má za úkol škodit. Zneužít zranitelnost. Vývoj aktualizací i exploitů může trvat několik hodin i několik let. Moment, kdy někdo zranitelnost objeví, se nazývá zero-day.

K vyhodnocení zranitelností se využívá metrika „CVSS“, tedy „Common Vulnerability Scoring System“. Zranitelnosti mají přidělené kategorie a skóre. Nejhorší jsou zranitelnosti z kategorie kritické, jejichž nejvyšší, tedy nejhorší, skóre je 10. Některé takto ohodnocené zranitelnosti dokáže útočník zneužít i bez účasti uživatele. Jen tím, že uživatel programové vybavení se zranitelností využívá, může útočník převzít kontrolu. Příkladem je nedávná kauza zranitelnosti „Log4Shell“, která se týkala až stovek milionů systémů po celém světě. Byla kritická, skóre měla 10.0. Velkou výzvou ve věci zranitelností je tzv. internet věcí. Vzhledem k tomu, že dnes může být připojena k internetu lednička, auto, nebo dokonce záchod, přibývá samozřejmě více zranitelností i pokusů o jejich zneužití. Odhaduje se, že automobilový průmysl zaostává v řešení kybernetické bezpečnosti o 5 až 10 let.

DDoS

Jedná se o typ kybernetického útoku, jehož cílem bývá konkrétní webová stránka nebo služba. Nejčastějším záměrem útoku je webovou stránku nebo službu znepřístupnit uživatelům, vyřadit ji z provozu. Také proto zkratka „DoS“, „Denial of Service“ tedy „odmítnutí služby“. Při útoku obdrží webová stránka nebo služba tolik požadavků k vyřízení, že je nezvládne zpracovat a zhroutí se. Odtud pramení „D“DoS. „D“ jako distribuovaný. Je to útok hrubou silou, do kterého mohou být zapojeny desetitisíce zotročených zařízení z celého světa a jejich vypůjčený, distribuovaný, výpočetní výkon. Webovou stránku nebo službu si můžete představit jako kruhový objezd, na který přijíždí další a další auta, až vznikne kolona, která se zasekne.

Uživatel přitom nemusí tušit, že je také jeho zařízení zotročené a zneužívané pro provedení DDoS útoku. Kontrolu nad zařízením uživatele může útočník získat třeba pomocí škodlivého souboru, který přišel e-mailem. Pro DDoS přitom nemusí být zneužita jen standardní zařízení jako počítače nebo notebooky. Pomocí zranitelností je možné ovládnout a do útoku zapojit i chytré hračky, hodinky nebo už zmíněnou ledničku. Zkrátka vše, co je připojeno k internetu a má vlastní výpočetní výkon. Čím více zotročených zařízení je do útoku zapojeno, tím je DDoS silnější.

Úspěšný DDoS útok má také psychologický efekt. Pokud se útočníkům podaří vyřadit z provozu například webové stránky klíčové státní organizace, může to vést ke snížení její důvěryhodnosti ze strany veřejnosti.

5G sítě

Velkým tématem kybernetické bezpečnosti jsou 5G sítě. Řeší se především nároky na dodavatele infrastruktury a také na její zabezpečení. Kybernetická bezpečnost uživatele je až na konci celého řetězce.
5G sítě svou rychlostí, stabilitou a nízkou odezvou znamenají velký krok pro celou informační společnost. Chirurgické operace na dálku, využití virtuální reality nebo autonomní řízení dopravních prostředků a robotizace továren. To vše rozvoj 5G sítí znamená. I běžní uživatelé internetu však s 5G sítěmi získávají nové možnosti. Třeba živý přenos 3D videa nebude nic neobvyklého.

Není to tak, že by 5G sítě přinášely pro kybernetickou bezpečnost zcela nové hrozby, kterým jsme doposud nečelili. Přináší ale zcela nové výzvy. 5G sítě a jejich technické parametry je důležité co nejlépe zabezpečit především z toho důvodu, že mají potenciál již známé hrozby mnohonásobně zesílit a akcelerovat. Získat kontrolu nad chirurgickou operací na dálku je nesrovnatelně větší problém než získat kontrolu nad e-mailovou schránkou.

5G sítě mohou změnit naše životy. Obrovský nárůst chytrých zařízení připojených k internetu věcí znamená obrovský nárůst zranitelností. Obrovský nárůst zranitelností znamená obrovský nárůst kybernetických útoků. A obrovský nárůst kybernetických útoků může změnit naše životy. Je to kruh. Například jako cestujícím v autonomním vozidle, kterému někdo odpojí brzdy.

Vzhledem k tomu, že komponenty potřebné pro fungování 5G sítě dokáže dodávat jen málo výrobců na celém světě, je nutné včas ošetřit, aby tito výrobci nezačali zneužívat svého postavení. Proto je velmi důležité, aby infrastruktura 5G sítí vznikla koordinovaně a v součinnosti států, úřadů, výrobců i dodavatelů.