Kapesní příručka pro boj s počítačovou havětí

verze ze dne 15.10.2018 – ke stažení z https://www.viry.cz/kniha

Igor Hák, viry.cz

Úvod

V roce 1998 jsem na internet umístil první verzi webových stránek nazvanou „Igiho stránka o virech“, která později přešla pod doménu **https://www.viry.cz**. Tehdy byl problém počítačové bezpečnosti okrajové téma a dodnes si pamatuji, jak se mě někdo ptal, jestli stojí za to, zabývat se něčím tak nepodstatným. Dnes musím konstatovat, že to za to stálo. Pohybuji se v oblasti kybernetické bezpečnosti, která se stále rozvíjí a z okrajového tématu se stalo jedno z hlavních. Nemluvě o tom, že stejně zajímavou problematiku řeším i v zaměstnání :-)

V médiích, včetně těch televizních lze dnes najít hromadu příspěvků různé kvality, které v horším případě uživatele pouze straší v lepším pak varují a navrhují nějakou prevenci. Celkově je toho tolik, že běžný uživatel nemá vůbec šanci rozpoznat, co je pro něj důležité a co nikoliv. Zároveň, pokud by měl dodržovat všechna doporučení, patrně by nedělal celý den nic jiného.

Tato publikace se tak snaží poskytnout ucelený pohled na prevenci domácích uživatelů v co možná nejstručnější podobě, aby byla jistá šance, že ji někdo dočte až do konce. Odborníci tak určitě v následujícím textu dohledají spousty nepřesností, chybějících informací atd. Nicméně toto je publikace pro BFU[1].

Celou publikaci jsem tvořil ve volném čase a dávám ji k dispozici ke stažení zdarma. Nebudu se ale bránit, pokud dílo finančně podpoříte dobrovolným příspěvkem a to v různé formě:

- převodem na účet: 107-275600267/0100 (Komerční banka)
- platbou kartou na https://platba.viry.cz/ jako forma příspěvku na provoz diskuzního fóra https://forum.viry.cz/
- využitím služby vzdálené pomoci NEŠLAPE.CZ na https://www.neslape.cz/
- nákupem zboží na internetovém obchodě https://obchod.viry.cz/
- zasláním nějakého toho Bitcoinu na adresu 1B5iLUJW2zyk8d2htqh7XjLwLmBD7VtF4U

Děkuji!

Přeji hezké čtení, zdraví Igor Hák (Igi) – https://www.viry.cz

[1] Dle wikipedie: BFU je výhradně česká iniciálová zkratka počítačového slangu označující běžného či naprosto nezkušeného uživatele. BFU se vykládá jako *Běžný Fyzický Uživatel* nebo *Běžný Franta Uživatel*, případně ostřeji *Blbý Franta Uživatel*. V 21. století se začíná objevovat podoba *Běžný Facebookový Uživatel*. Vzhledem k neexistenci tohoto pojmu v zahraničí lze předpokládat, že až následně vznikly anglické verze – *Bloody Fucking User* (sakra debilní uživatel), *Beginner For Unix* (unixový začátečník) či *BrainFree User* (uživatel bez mozku).

Obsah

Skoro za všechno si můžeme sami

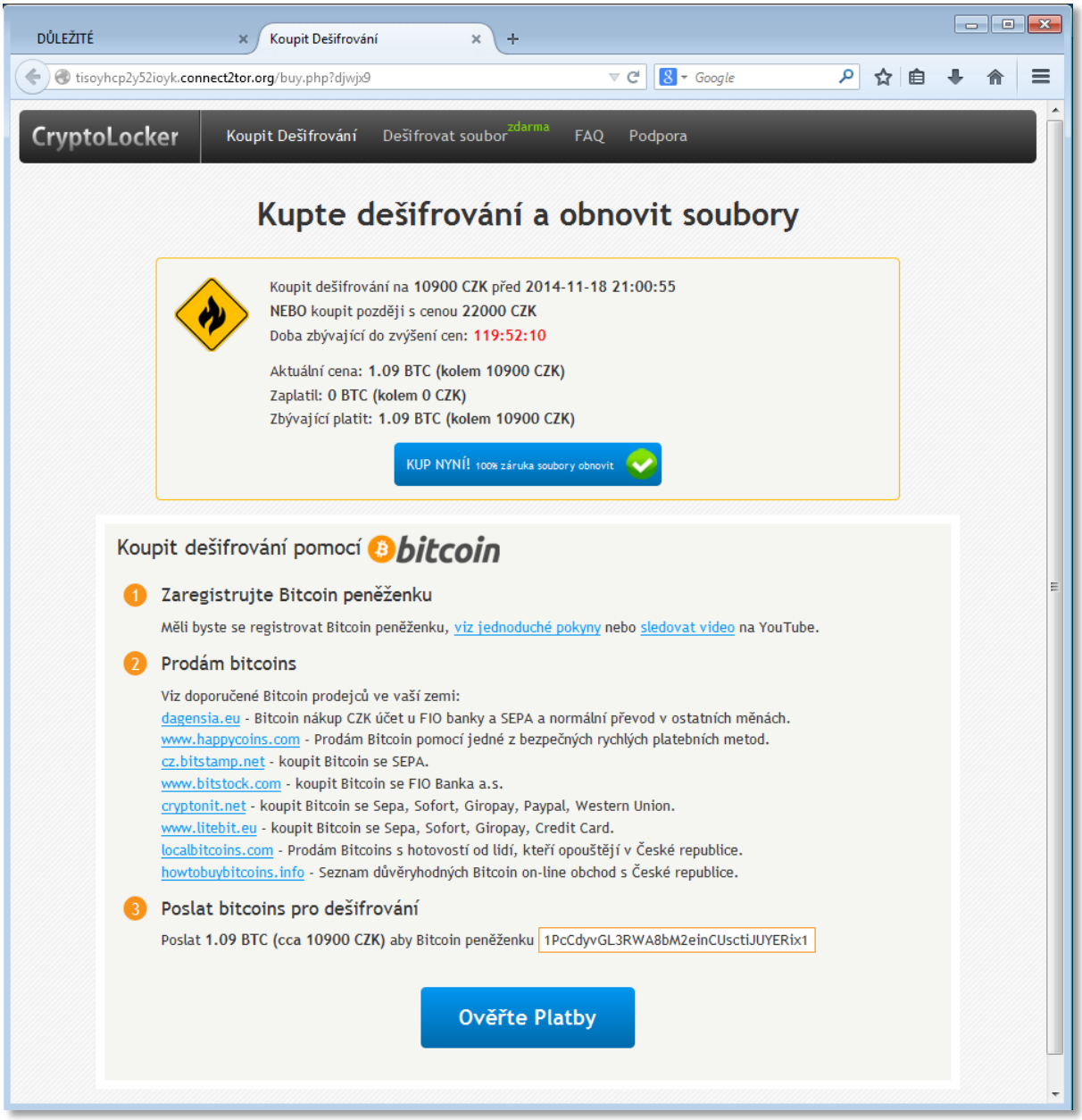
Úspěch celé řady útoků v počítačovém světě je založen na tom, **zda se necháte či nenecháte napálit**. V některých případech lze pak vysloveně hovořit o tom, že úspěch počítačové havěti je založen na **lidské blbosti**. Můžete tak mít nejlepší antivirus, záplatovaný operační systém a přesto se dostat do problémů. Často je to opravdu o chování samotného uživatele. Zda několik špatných rozhodnutí povede třeba až ke spuštění zavirované přílohy e-mailu či odkliknutí „nezdravého" množství varování. Odborně se tomu říká **sociální inženýrství**, hovorově „oblbovačky".

Menší část útoků se pak realizuje s využitím různých chyb v programech (v operačním systému Windows, v prohlížečích, ...), kdy opravdu nemusíte nikde na nic klikat, nic stahovat ani spouštět a přesto dojde k zavirování počítače. Nejhorší je pak situace, kdy útočník (resp. autor havěti) zneužije chybu v programu o které nevědí ani samotní jeho tvůrci. Odborně hovoříme o tzv. **zero-day exploit**. To laicky znamená, že na danou chybu neexistuje žádná záplata.

Co je typickým výsledkem útoku?

Přijdete o data, dokumenty, fotky z dovolených, videa, hudbu, ...

Havěť prostě taková data smaže, pravděpodobněji však zašifruje (tzv. havěť typu **ransomware**). V konečném důsledku v tom není rozdíl. Prostě nemáte dokumenty, fotky, prostě nic.



Obrázek 1 Typická ukázka havěti ransomware, která znehodnotí soubory uživatele formou šifrování (dokumenty, fotky, ...) a pro jejich navrácení vyžaduje „výpalné“ ve výši až několika desítek tisíc Kč. Útočník ale může pouze shrábnout peníze a uživatele nechat na holičkách...

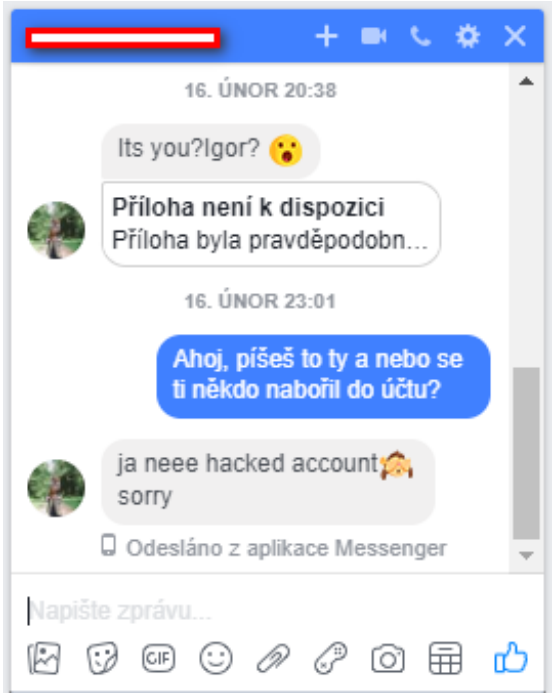
Data vám budou odcizena

Toto je pochopitelně taktéž nepříjemné, obzvlášť pokud jde o citlivé dokumenty (například s „know-how“).

Ztratíte identitu

Pod pojmem **ztráta identity** si představte situaci, kdy se útočník zmocní například Vaší e-mailové schránky, Facebooku, Instagramu, nedej bože datové schránky. Pod Vaším jménem (=pod Vaší identitou) Vám může způsobit problémy na několik let dopředu. Ostatní totiž stále vnímají, že to vše je Vaše práce, tj. že příspěvky či e-maily píšete Vy. Ve skutečnosti jde o dílo útočníka a vy se marně pokoušíte k odcizeným účtům přihlásit.

V reálném světě se můžete do podobné situace dostat v momentě, kdy Vám někdo ukradne občanku a zloději si pak na ní berou půjčky.



Obrázek 2 Ukázka ztráty identity na Facebooku. Místo známého Vám z jeho účtu píše útočník nebo nějaký bot.

Přijdete o peníze

Některá havěť (odborně **banking trojan**) se snaží dostat k penězům na Vašem bankovním účtu. Nejde o nic neobvyklého, což dokládá i kauza „exekuční příkaz“ (níže).

Jak se nenechat oblbnout

Základem úspěchu je používání **zdravého rozumu** a nespoléhání se plně na antiviry a další bezpečnostní nástroje ve vašem zařízení. Nic není stoprocentní. Ač často oplývají opravdu moderními technologiemi, je potřeba je brát pouze jako součást pomyslné mozaiky bezpečnostních opatření.

Celá řada útoků je úspěšná jen v případě, že mu pomůžete vy, jakožto uživatel počítače, notebooku, mobilu či tabletu. „Oblbovačky (odborně **sociální inženýrství**) jsou velice úspěšné v momentech, kdy se motají kolem témat:

- **peníze**
- **zdraví**
- **sex**

Jeden z nejúspěšnějších útoků v minulosti byl podpořen tématem exekučního příkazu (tedy téma peněz). O exekucích slyšíme zleva zprava a víme, že pokud je na nás uvalena, je to špatně a je potřeba z ní co nejrychleji vybruslit. Proto, pokud někdo vede útok skrze hromadně rozeslanou e-mailovou zprávu s předmětem typu „Uvalení exekučního příkazu“ a v příloze je soubor s detaily exekuce na náš majetek, je skoro jasné, že se necháme zvyklat a přílohu spustíme. Tím si ale do počítače zaneseme havěť, která se za vhodně zvolené téma schová.

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor Mgr. Ing. Jiří Prošek, Exekutorský úřad Plzeň – město, IČ 87560921, se sídlem Rychtaříkova 15, 336 00 Plzeň pověřený provedením exekuce: č.j. 22 EXE 233/2014 -18, na základě ustanovení: Příkaz č.j. 066457/2014-416/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá exekuční titul, stejně tak, jako i povinnosti uhradit náklady na nařízení exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 5 818,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 104,00 Kč včetně DPH 21% Náklady exekuce paušálem: 3 968,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 389654709/2600, variabilní symbol 44129402, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 10 890,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Adriana Tauschová

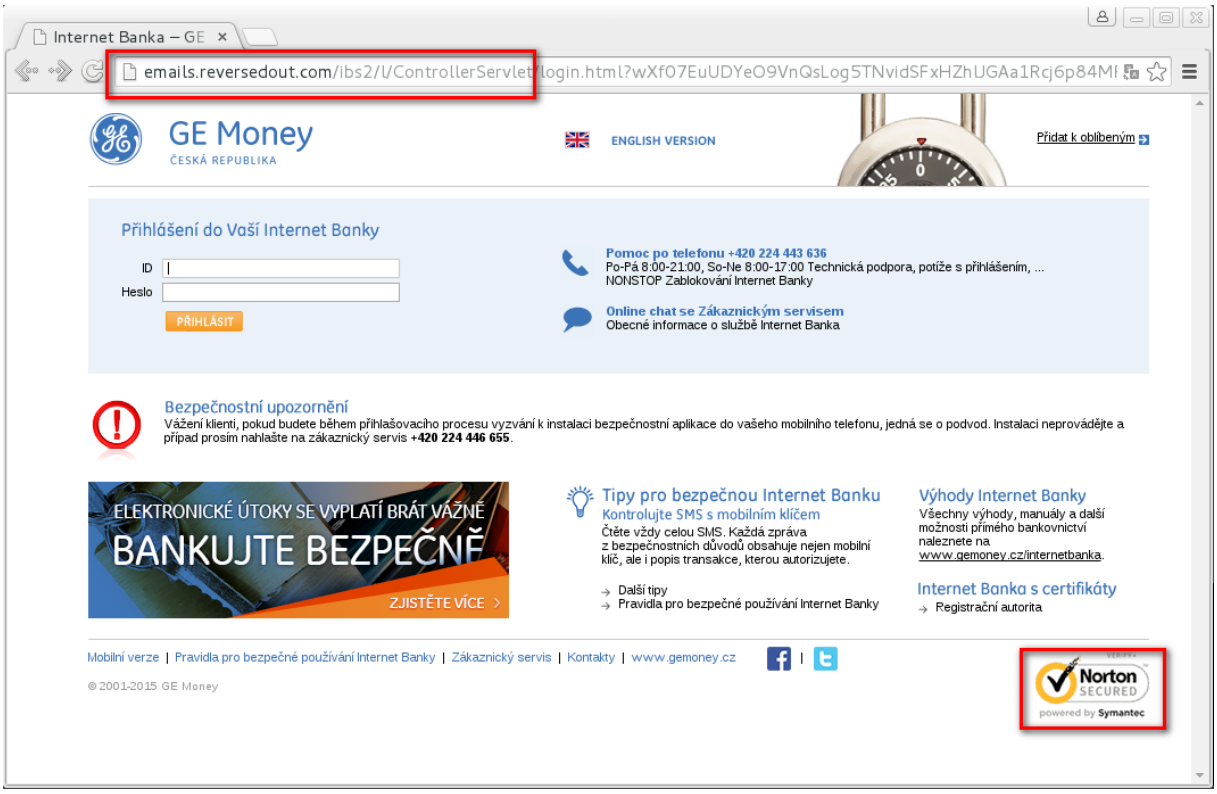
Obrázek 3 Ukázka v minulosti vedeného útoku na téma "exekuce". Toto dorazilo e-mailem. V příloze byl zavirovaný soubor, jehož spuštěním jsme si zadělali na problém...

Podobně je tomu v případě bankovních účtů, kdy se nás někdo snaží přesvědčit o tom, že je znova nutné ověřit PIN kód, číslo bankovní karty, znovu zadat jméno/heslo, v opačném případě hrozí zablokování přístupu k penězům. Této formě útoku říkáme **phishing**.

Výsledkem je, že se útočník dostane k přihlašovacím údajům, které pak využije k „vytunelování“ bankovního konta. Citlivé údaje totiž nezapisujeme do formuláře banky, ale do podvrženého formuláře

útočníka. **Pozor i před nucením instalace vylepšeného zabezpečení pro Váš chytrý telefon!** Některé pokročilejší útoky se snaží využít i Váš mobilní telefon a ošálit **dvoufaktorové ověření** (více informací dále v textu). To byl koneckonců i případ kauzy „exekuční příkaz“.

Ucelený pohled na kauzu lze najít na webu viry.cz: http://bit.ly/exekucni-prikaz



Obrázek 4 Typická phishingová - podvodná stránka vydávající se za banku. Vše co vyplníte, odchází útočníkovi. Všimněte si nesprávné adresy stránky! Pravá toho času běžela na www.gemoney.cz. Logo antivirové společnosti (vpravo dole) nemusí být zárukou bezpečí.

Nevěřte všemu, co obdržíte e-mailem či jiným komunikačním kanálem

Pokud si nejste jisti, ověřte si jinou cestou, zda jde o hloupost nebo legitimní věc. Třeba telefonátem na info linku banky, či kamarádovi, který od Vás začal náhle vyžadovat něco, co nikdy nevyžadoval (možná právě někdo odcizil jeho identitu).

Na začátku je též vhodné zamyslet se nad tím, zda by daný subjekt opravdu volil takový způsob komunikace. Že by exekutor posílal tak důležité informace e-mailem, kde není zaručeno, že ho obdržíte? Že by banka opravdu ztratila Váš PIN a chtěla ho znovu zaslat zpět? A to pro jistotu i včetně čísla účtu, čísla platební karty atd.? Pokud to není zrovna phishing, tak se došlé „kraviny“ e-mailem označují jako **hoax**. Ucelený přehled hoaxů tvoří kolega Josef Džubák na serveru http://www.hoax.cz. Když si nejste jisti, zda je to pravda nebo nesmysl, začněte tam!

Nikdy a nikomu neposílejte hesla, PINy, čísla platebních karet a žádné další citlivé informace

I kdyby na tom stál provoz firmy, žádal to po Vás ředitel, není žádný důvod citlivé informace vydávat. Vždy existuje oficiální způsob řešení.

Nikdy nepřeposílejte zprávy, které „omylem“ dorazily k Vám a nyní je někdo jiný požaduje

Tenhle útok se v praxi děje hlavně u SMS zpráv. Prostě Vám náhle dorazí SMS, avšak nejste schopni pochopit její význam. Pak Vám zavolá / napíše někdo, že se spletl v čísle a omylem poslal právě tuto SMS na Vaše telefonní číslo a požádá, zda mu ji můžete přeposlat. I kdyby to bylo podáno tak, že díky tomu nevyhrajete hlavní cenu v losování, nic nepřeposílejte! Je zde riziko, že naopak o peníze přijdete.

Typickým scénářem je, že někdo cizí (=útočník) si zakoupil zboží na e-shopu a požaduje platbu přes mobil. Jako telefonní číslo ale uvedl právě to Vaše a je tedy jasné, kdo to všechno zaplatí (v případě přeposlání potvrzovacího kódu).

Odkud havěť přichází

Dost bylo strašení, nyní se pojďme podívat jak se vlastně taková havěť šíří. Většina havěti se k nám dostane pochopitelně z internetu. Konkrétně jde o tyto cesty (tzv. **vektory útoku**).

E-mailová zpráva

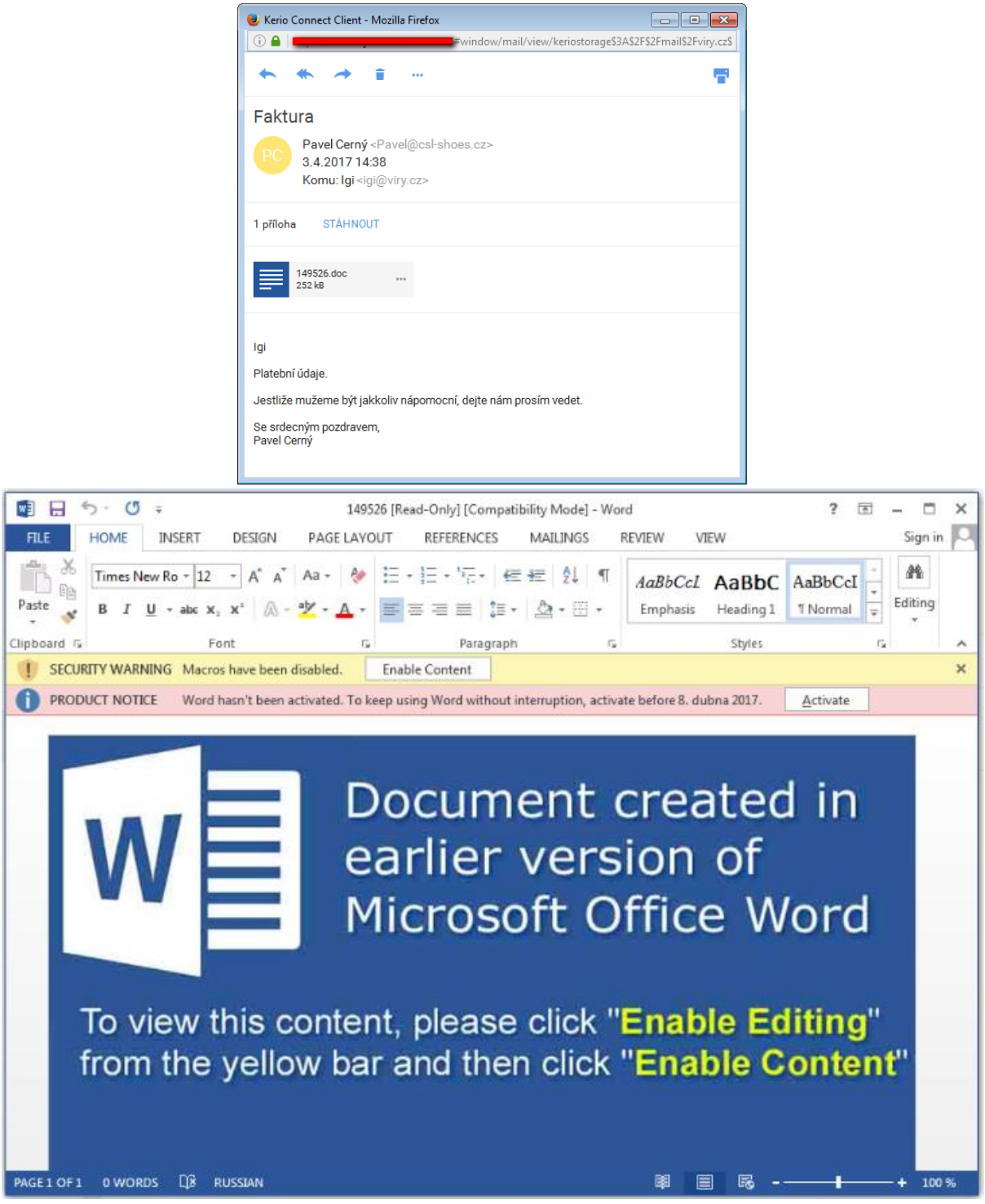
Zavirovaná příloha

V e-mailové zprávě může být zavirovaná příloha, tedy soubor. Typické je, že soubor s havětí je zabalen do archivu (ZIP, RAR, ...). Díky tomu se zvyšuje šance, že dorazí až do schránky potenciální oběti. Zavirovaný soubor nemusí být nutně přímo spustitelný (přípona souboru je EXE). Problém mohou způsobit jakékoliv další soubory, jejichž přípona je asociována s aplikací v počítači. Pár příkladů:

- přípona PDF – Adobe Acrobat Reader
- přípona DOC/DOCX – Microsoft Word
- přípona XLS/XLSX – Microsoft Excel
- přípona JS – JavaScript – prohlížeče Mozilla Firefox, Google Chrome, ...
- přípona VBS – Visual Basic Script – Microsoft Windows Based Script Host
- přípona HTML – prohlížeče Mozilla Firefox, Google Chrome, ...
- ...

Pokud na takové soubory poklepete myší (případně stisknete ENTER), dojde ke spuštění asociované aplikace, která obsah souboru vhodně zobrazí. V případě, že jde o PDF soubor, obvykle se spustí Adobe Acrobat Reader. U DOC/DOCX dokumentu pak Microsoft Word. Zde může následně dojít ke dvěma scénářům:

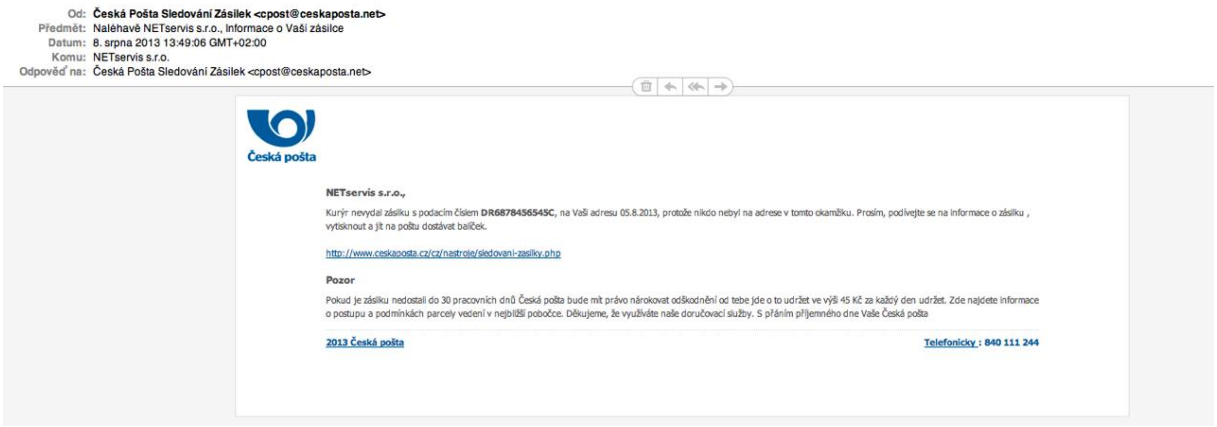
- Útočník Vás bude prostřednictvím sociálního inženýrství = oblbovaček přesvědčovat, jaké další kroky musíte provést. Ve skutečnosti vedou pouze k definitivnímu spuštění havěti a jejímu zavedení do počítače.
- Dojde ke zneužití bezpečnostní chyby (tzv. exploitace) v asociované aplikaci bez vašeho vědomí a k automatickému spuštění havěti a jejímu zavedení do počítače. To může být způsobeno tím, že používáte starší verzi takové aplikace a nebo sice novou, ale útočník využil tzv. zero-day zranitelnosti. Více v kapitole o záplatování.



Obrázek 5 Nebýt té podivné češtiny e-mailu (obrázek nahoře), dalo by se tomu skoro i uvěřit. I tak měla tahle havěť úspěch a údajná faktura v příloze dokázala způsobit pěknou neplechu - do systému totiž zavedla ransomware a tahle havěť se pak postarala o znehodnocení fotografií či dokumentů uživatele. Bez oblbovaček uživatele by to ale nešlo – ten totiž musel v Microsoft Word povolit makra přesně tak, jak ho o tom informují útočníci (dolní obrázek). ***Pozor na útoky přes Word a Excel! Prostě se vyvarovat zbytečných souhlasů a nepovolovat makra u dokumentů získaných na internetu či z neznámých zdrojů!***

Závadné odkazy

V e-mailu nemusí být nutně příloha, ale i závadné odkazy, které otevřou webový prohlížeč a případná zkáza nastane až tam. Tohle je typické pro útoky typu phishing, kdy se podvodníci vydávají za bankovní instituce apod.



Obrázek 6 Tohle opravdu není oficiální e-mail od České pošty...

Webová stránka

Na škodlivý kód můžete narazit i na webových stránkách. Riziko se zvyšuje na webech, které se věnují oblasti warezu či pornografii. Obecně lze ale škodlivý kód najít na jakékoliv webové stránce třeba v případě, že ji útočník úspěšně napadl a získal nad ní kontrolu (hacknul). Ačkoliv vizuálně vypadá jako legitimní, servíruje i škodlivý obsah (tzv. **drive-by download**). Škodlivý kód se občas podaří útočníkovi distribuovat i prostřednictvím reklamního systému, jehož škodlivé bannery pak mohou „rotovat" i na celé řadě hojně navštěvovaných webů.

Pokud je útok veden z webových stránek, útočníci se často snaží zneužít známé zranitelnosti v prohlížečích, či aplikacích jako Adobe Flash, Oracle Java, (tzv. exploit)... K zavirování tak může dojít pouhou návštěvou webových stránek bez toho, abyste kdekoliv klikali či cokoliv spouštěli! Opět platí totéž - je nutné záplatovat! Více v kapitole o záplatování.

Vyjímatelná média

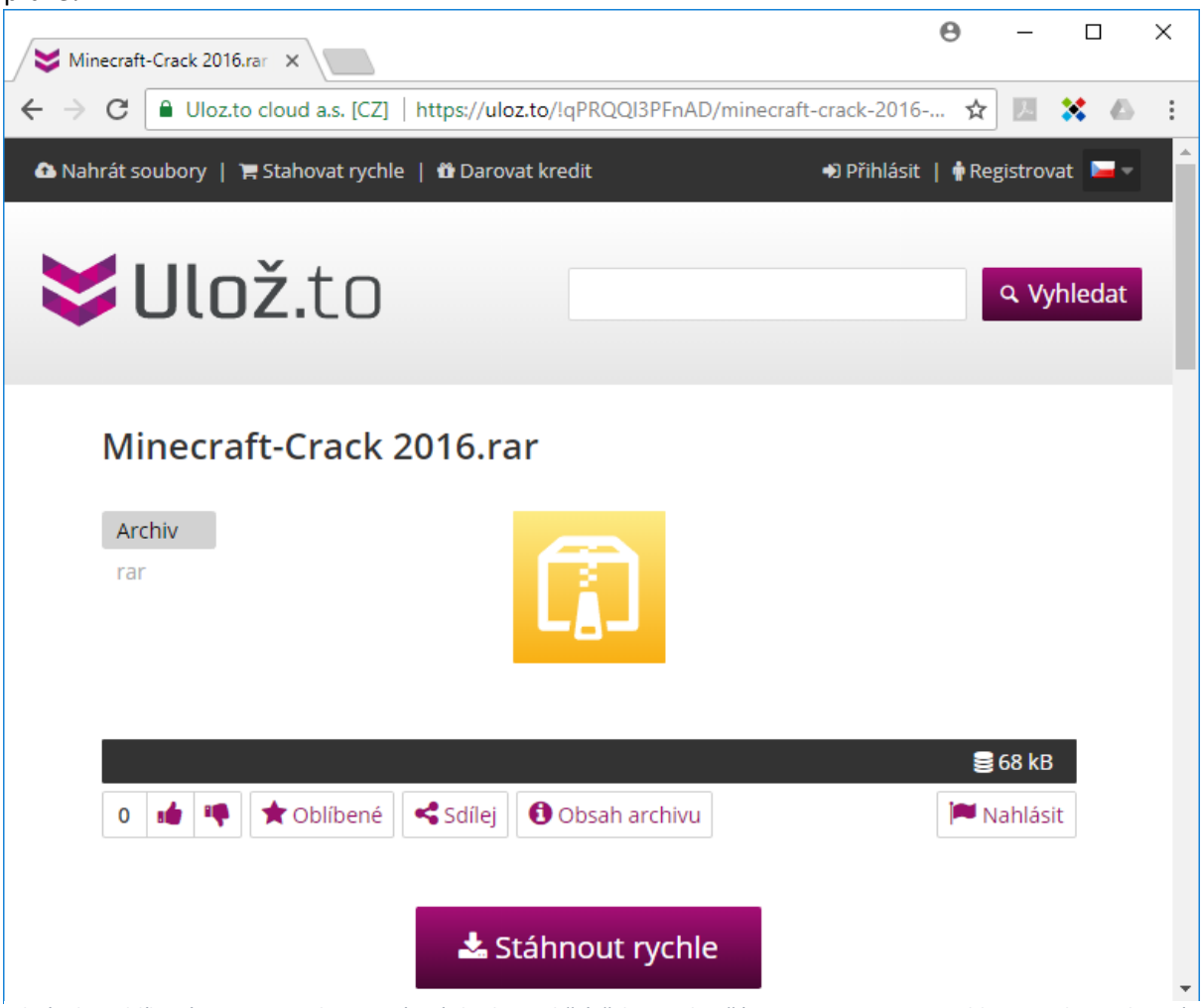
Havěť může být uložena na výměnných médiích jako CD, DVD nebo USB flash disku. Taková havěť může mít opět několik podob. O podobě souborů platí totéž, co v části o e-mailových zprávách.

Pokud se bude někde na zemi válet neznámý flash disk, byl bych hodně opatrný s jeho zasouváním do počítače. Existují techniky, které způsobí, že pouhé zapojení do počítače spustí automaticky kód (třeba škodlivý) z flešky.

„Trojanizovaná" aplikace

Trojanizované aplikace jsou typické u mobilních telefonů s operačním systémem Android. Ač se všechny programy stahují z knihovny Google Play, kterou má pod kontrolou společnost Google, přesto dochází k situacím, kdy tam krátkodobě proniknou i falzifikáty oblíbených aplikací. Ty sice fungují jako originály, nicméně navíc přidávají i vlastní záškodnickou činnost. U Apple Store je situace podstatně lepší, aplikace tam před umístěním prochází důkladným testováním. Riziko nastává až v momentě, kdy je telefon ve stavu „jailbreak", pak lze do něj instalovat i neoficiální aplikace a ty mají plná práva (ekvivalent, kdy je telefon s Adroidem tzv. „rootnutý"). V takových případech nemusí zafungovat ani tzv. factory reset. Tj. kdy vrátíte celý telefon do „továrního" nastavení! Připomeňme ale, že v tomto „otevřeném" stavu se nenachází žádný běžně využívaný telefon. Jeden příklad trojanizované aplikace z praxe: https://bit.ly/qrecorder.

Do této kategorie bych si dovolil zařadit i jakousi trojanizaci cracků. Crack je přitom malý program, který dokáže některé demo verze programů „přepnout“ na plnohodnotné a za jeho používání není třeba nic platit. Bohužel jeho činnost je v některých ohledech podobná havěti, tedy i antivirové programy zde produkují vyšší množství falešných poplachů (crack označí za zavirovaný, ač není). Taková zkušenost může vést uživatele k tomu, že antivirus prostě vypnou, aby „neprudil“. Co když ale měl antivirus zrovna pravdu a šlo o havěť typu ransomware vydávající se za crack? Bohužel hodně rozšířená praxe!



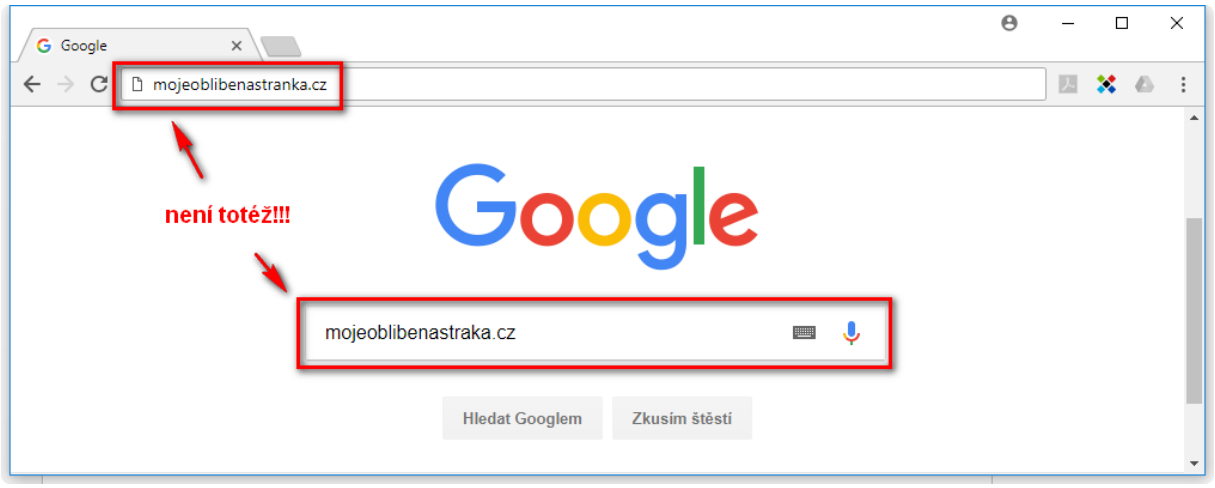
Obrázek 7 Oblíbené programy a hry se stávají vhodnou obětí třeba pro havěť typu ransomware... Tohle opravdu crack není a ze hry Minecraft plnou verzi nevytvoří!

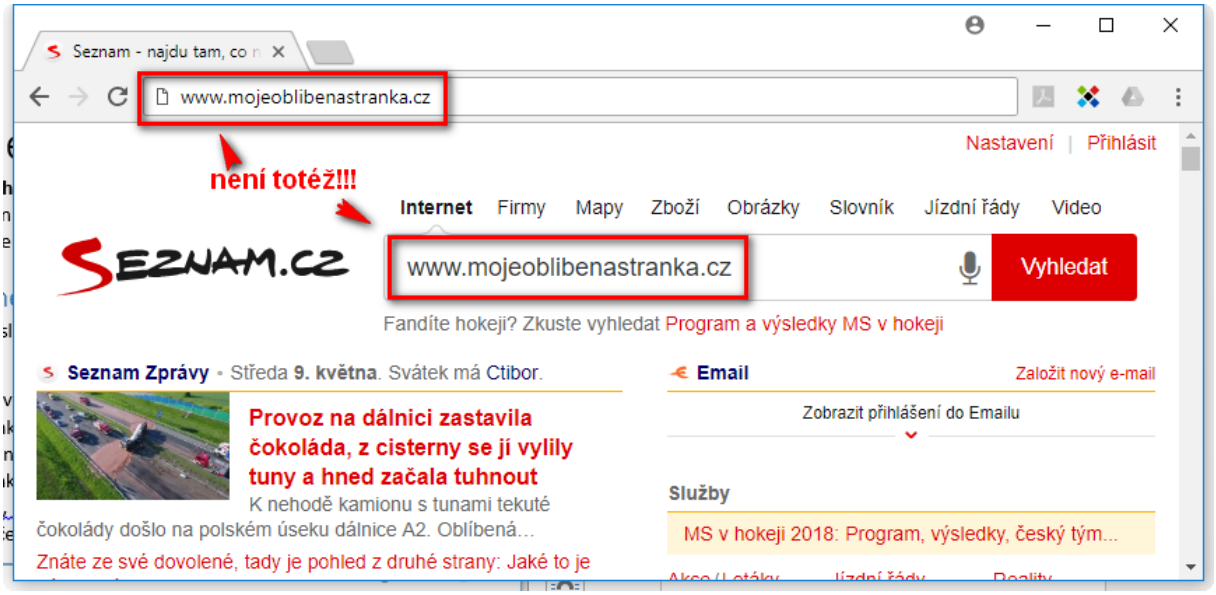
Útok může být veden i pomocí zřetězení výše uvedených „cest“. Může tak dorazit například e-mail, v němž jsou závadné odkazy. Tyto otevírají podvodný web, kde je ke stažení zavirovaný soubor.

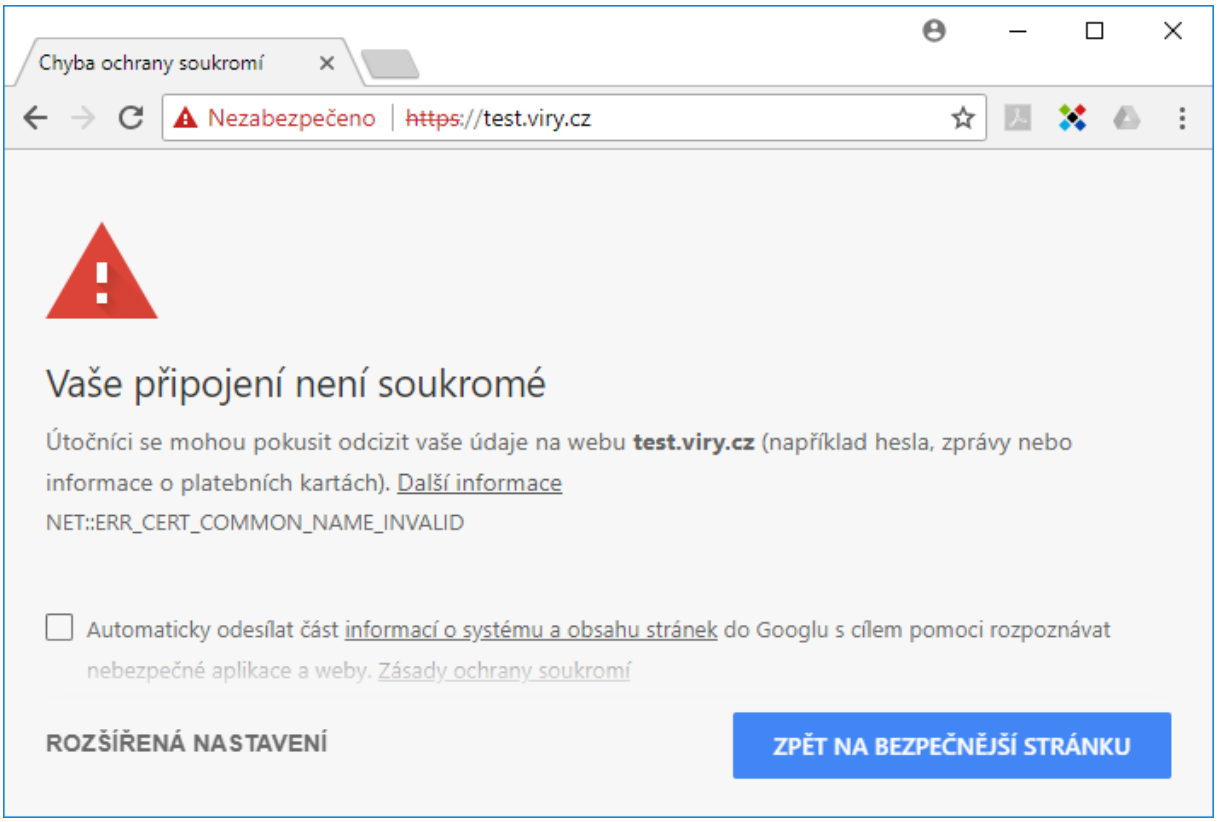
Zadáváme citlivé údaje...

Pokud někam zadáváte PINy, hesla, čísla platební karty nebo další citlivé informace, zadávejte je na internetu jen v případě, že:

- je na začátku webové adresy uvedeno https:// a prohlížeč nehlásí chybu certifikátu,
- zároveň jde o webové stránky daného subjektu (tj. například heslo od internetového bankovnictví zadáváme pouze na webu internetového bankovnictví a nikde jinde),
- zároveň jde o webovou stránku, jejíž adresu jste „vyťukali“ do prohlížeče ručně. Tj. prostě postupně namačkali klávesy w, w, w, ., ... a stiskli ENTER. Pozor na to, že tímto není myšleno naťukání adresy do vyhledávače google.com či seznam.cz, protože to není totéž a útočník toho může zneužít (dobře zaplacenou reklamou se dokáže „nacpat“ do výsledků hledání před legitimní stránky):







Obrázek 8 Problém s HTTPS zabezpečením. Foto z prohlížeče Google Chrome.

Pokud se u http**s** stránky zobrazí něco podobného jako výše, tedy informace o nezabezpečeném připojení / neplatném certifikátu, určitě na takové stránky žádné citlivé údaje nezadávejte! Ideálně ani nevstupujte! Na nezabezpečené stránky http (bez **s** na konci) nezadávejte osobní / citlivé údaje tak jako tak. Výše uvedené obrázky mohou znamenat dočasnou chybu serveru, ale i dílo útočníka, který zrovna realizuje tzv. **MITM útok** (man in the middle).

Jsme v terénu mimo domov nebo firmu

Na cizím počítači

Pokud se potřebujete někde v terénu přihlásit z cizího počítače k Facebooku, e-mailu apod., asi bych to hodně zvážil. I kdyby to byl počítač nejlepšího kamaráda, je potřeba si uvědomit, že v podobné kondici nemusí být jeho počítač. Havěť typu **keylogger** / **password stealer** dokáže zaznamenávat zadaná jména / hesla, případně stisky jakýchkoliv kláves. Pokud má kamarád / kamarádka podezřívavého partnera, tak pak bych se tomu vyhnul zcela. Keylogger tam může být skrytě nainstalován úmyslně. Nemluvě pak o počítači na recepci hotelu.

Na veřejné WiFi (bezdrátové) síti

Stejně tak buďte pozorní v případě, kdy jste připojeni k veřejné WiFi síti někde v restauraci či na letišti (nezáleží, zda mobilem, tabletem či notebookem). Vyvarujte se zadávání citlivých informací, zapisování hesel, čísel platebních karet, PINů, ... Pokud je to nezbytně nutné, mělo by jít o bezpečnou formu šifrované komunikace. Tj. v případě webových stránek musí jít o http**s** a zároveň nesmí prohlížeč hlásit problém s certifikátem.

Je potřeba si uvědomit, že bezdrátovou komunikaci lze velice jednoduše odposlouchávat a útočník tak může přesně zjistit, kde se přihlašujete, co kam píšete atd. Není přitom nutné, aby tam byl fyzicky ve stejný moment. Komunikaci může dlouhodobě sbírat do nějakého schovaného zařízení a analyzovat ji kdykoliv později. Vzhledem k dosahu sítě až několika desítek metrů nemusí být ani v bezprostřední blízkosti.

Obdobná situace se týká veřejných WiFi sítí opatřených heslem (typicky WPA2-PSK), kdy heslo získáte například od obsluhy restaurace. Neznalost hesla zabrání pouze přihlášení do sítě, ničemu dalšímu. Pokud jste již přihlášeni (a přihlášen je i útočník), platí naprosto shodná fakta jako výše. Vaši nešifrovanou komunikaci vidí i okolí a lze ji odposlouchávat.

Hesla, hesla, hesla a dvoufaktor

Pravidla pro hesla

Všude tam, kde se na internetu někam přihlašujete, je často potřeba zadat heslo. Když takové heslo vytváříte, je potřeba zajistit, že **bude dostatečně bezpečné**, tudíž těžce prolomitelné a zároveň bude existovat šance, že ho nezapomenete :-) Nicméně pokud přidáme další podmínku a to tu, že **pro každou službu používejte zcela odlišné heslo**, pak to už bude horší.

Bezpečné heslo by nemělo obsahovat například tyto údaje (výtažek z wikipedie):

- název účtu, ke kterému slouží heslo jako ochranný prvek
- vlastní jméno či jméno někoho z rodiny, jméno psa, milenky apod.
- rodné číslo či datum narození
- č. domu, adresa, telefonní číslo…
- často užívané výrazy jako např. „12345“, „heslo“, „qwertz“ nebo názvy programů
- běžná slova (ani jejich obdoba v tzv. l33t žargonu) či fráze (např. „iloveyou“ bylo vyhodnoceno jako 9. nejnebezpečnější)

Nejbezpečnější hesla jsou tedy „nesmyslné“ kombinace znaků. O to hůře si ale heslo zapamatujeme i my sami a pokud ho pravidelně nepoužíváme, brzy ho zapomeneme. Vhodnější je vymyslet si k heslu nějakou **mnemotechnickou pomůcku**, podle které si ho snáze zapamatujeme (tato pomůcka ovšem musí zůstat stejně tajná jako heslo samotné).

Při tvorbě hesla doporučuji použít i kombinaci malých / velkých písmen, případně číslic nebo speciálních znaků (!@#$%^...). **Při dodržení výše uvedených podmínek doporučuji tvořit hesla minimálně o délce osmi znaků.**

Pozor, Vaše heslo může útočník hádat programově (tedy hrubou silou – brute force). I běžné hardwarové vybavení dokáže vyzkoušet několik desítek milionů kombinací znaků/číslic/symbolů během jedné sekundy! I na první pohled silné heslo tak může být prolomeno během několika sekund až hodin.

Spousta služeb = spousta hesel

Doporučení: pamatujte si silná hesla pouze u služeb, které používáte na denní bázi (typicky pro přihlášení k e-mailové schránce). Ostatní hesla (ovšem stále splňující výše uvedené podmínky) **svěřte správci hesel** (viz. kapitola pomocníci).

Používejte dvoufaktorové (dvoufázové) ověření

Ač název vypadá složitě, jde o skvělou věc a vřele doporučuji dvoufaktorové ověření zapnout všude tam, kde je to možné. Dvoufaktorové ověření je samozřejmostí u internetového bankovnictví. Nejprve se do webové aplikace bankovnictví přihlásíte nějakým jménem a heslem (první fáze) a pak musíte pro potvrzení peněžní transakce opsat kód z mobilního telefonu (druhá fáze), který Vám dorazí například v podobě SMS zprávy. Důvodem je ochránit Váš bankovní účet v momentě, kdy se útočník zmocní přihlašovacího jména a hesla. Pak mu bude k ničemu, neboť pro převod peněz by potřeboval i Váš mobilní telefon. **Pozor! Pokud Vám k první i druhé fázi stačí používat shodné (=jedno) zařízení, nelze hovořit o dvoufázovém ověření a zadělváte si na problém!** Důkaz z praxe: https://bit.ly/qrecorder.

V podobném duchu funguje dvoufaktorové ověření i u Vašich účtů na Facebooku, Instagramu, Gmailu, ... V tomhle případě tak snížíte riziko krádeže identity. **Je ale nutné ho manuálně zapnout!**

Středobodem je vaše e-mailová schránka!

V této souvislosti je nutné zmínit, že pomyslným středobodem všeho je Vaše e-mailová schránka. Všechny další služby, které používáte, jsou téměř vždy svázány s Vaší e-mailovou adresou. Tedy Facebook, Instagram, Twitter, ... Pokud v těchto službách zapomenete heslo, vždy je tam k dispozici nějaká ta funkce typu „Zapomněli jste heslo?“ či „Lost password?“, která Vám pošle na e-mailovou adresu další instrukce, jak si nastavit nové heslo.

Je snadné si domyslet, co může nastat v případě, kdy útočník získá přístup do Vaší e-mailové schránky. Během chvíle může přebrat kontrolu nad spoustou dalších služeb a to bez znalosti hesel. Kde jinde tak začít se silným heslem a dvoufaktorovým ověřením, než u e-mailové schránky?

Dvoufázové ověření na Google (Gmail, ...)

Pokud používáte služby Google, například Gmail, začít můžete zde:

http://bit.ly/google-2faktor

Spárujte si účet s Vaším mobilním telefonem a **též si nechte vystavit záložní kódy**! Záložní kódy si vytiskněte a pečlivě uschovejte. Myslete na to, že můžete mobilní telefon ztratit a pak se výhody dvoufaktorového ověření mohou stát významnou komplikací a nemožností přihlásit se k účtu! Případně svažte účet i s jiným telefonním číslem někoho blízkého.

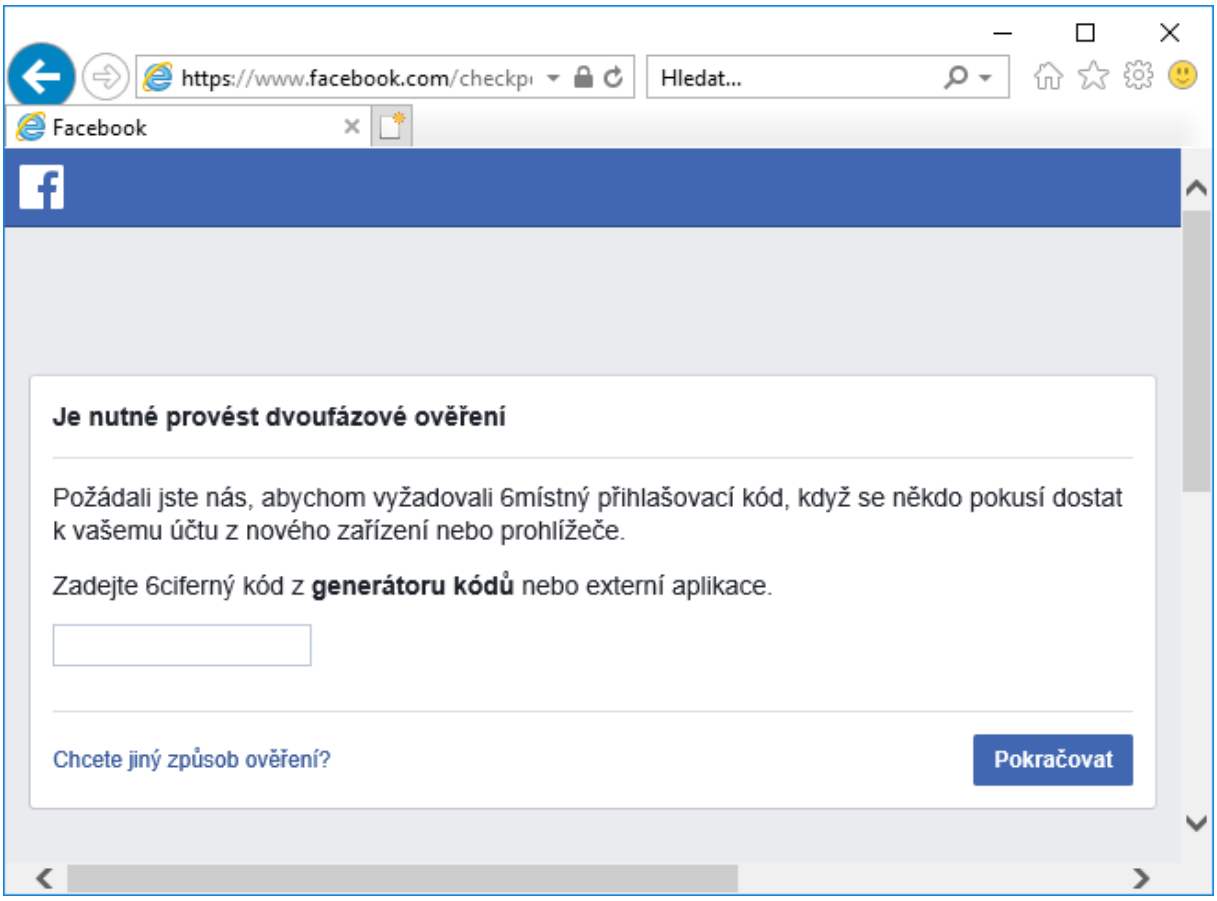
Dvoufázové ověření na Facebooku

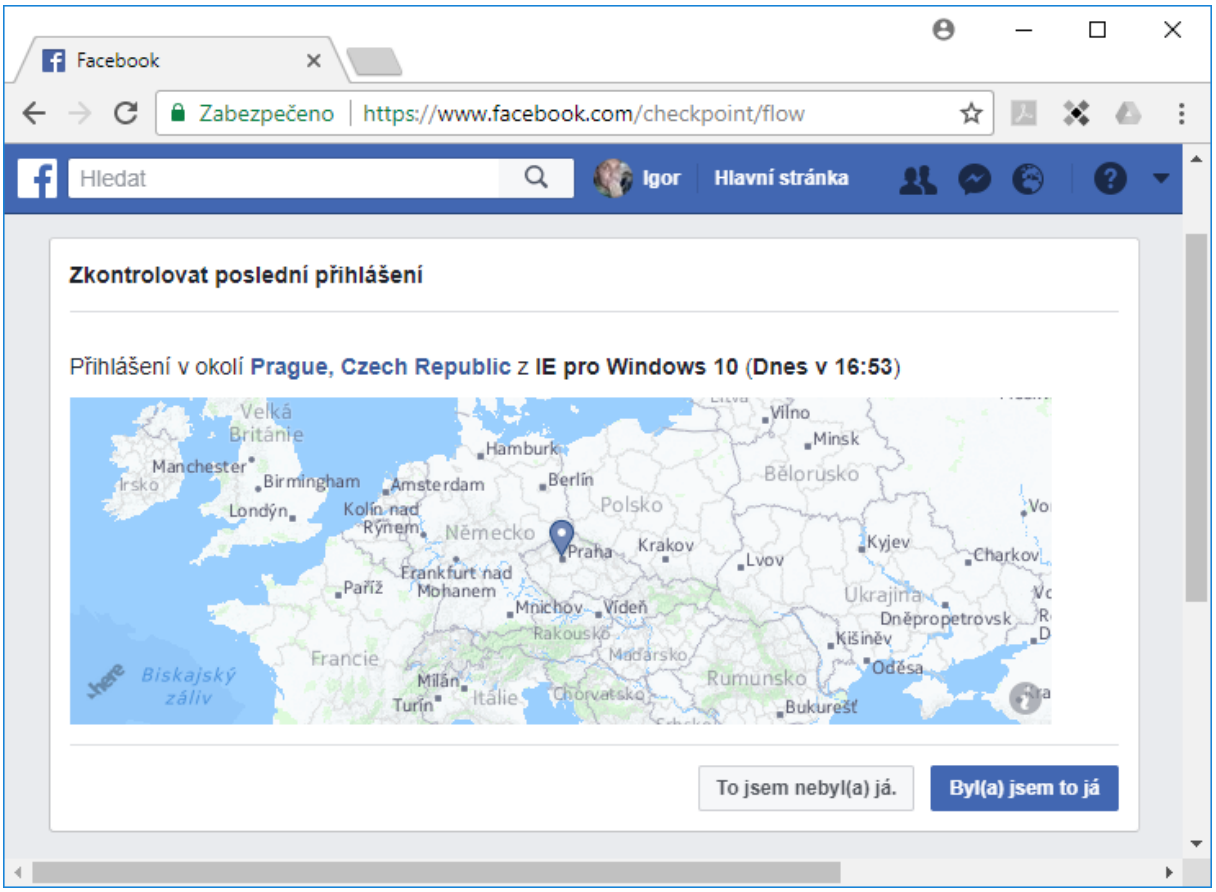
V nastavení profilu, menu „Zabezpečení a přihlášení“ naleznete položku týkající se nastavení dvoufázového ověření. Přesně zde: http://bit.ly/facebook-zabezpeceni

Fungování v praxi

Dvoufázové ověření je v případě internetového bankovnictví hodně „obtěžující“ a vyžaduje opisovat kódy z SMS při každé transakci. V případě výše popsaných služeb (a spousty dalších) se toho ale bát nemusíte. Mobilní telefon budete potřebovat vlastně jen v případě, že se hlásíte z nového počítače. Třeba v případě služby Facebook to pak vypadá tak, jak ukazuje první obrázek na následující straně. Teoreticky se může do podobné situace dostat útočník, který se snaží Vašeho účtu zmocnit.

Je potřeba obezřetně postupovat i v případě, že se objeví něco jako na obrázku níže. Tedy správně odpovědět na otázku, zda jsem se v ten čas do služby hlásil(a) já nebo nehlásil(a) já. **Je to klíčový moment!** Mohl to být totiž právě pokus útočníka!


https://www.facebook.com/checkp
Hledat...
Facebook
Je nutné provést dvoufázové ověření
Požádali jste nás, abychom vyžadovali 6místný přihlašovací kód, když se někdo pokusí dostat k vašemu účtu z nového zařízení nebo prohlížeče.
Zadejte 6ciferný kód z generátoru kódů nebo externí aplikace.
Chcete jiný způsob ověření?
Pokračovat


Facebook
Zabezpečeno | https://www.facebook.com/checkpoint/flow
Hledat
Igor
Hlavní stránka
Zkontrolovat poslední přihlášení
Přihlášení v okolí Prague, Czech Republic z IE pro Windows 10 (Dnes v 16:53)
Velká Británie
Manchester
Birmingham
Londýn
Amsterdam
Hamburk
Berlín
Kolín nad Rýnem
Německo
Polsko
Praha
Krakov
Lvov
Vilno
Minsk
Bělorusko
Kyjev
Charkov
Frankfurt nad Mohanem
Paříž
Mnichov
Vídeň
Rakousko
Maďarsko
Ukrajina
Dněpropetrovsk
Kišiněv
Oděsa
Francie
Biskajský záliv
Milán
Turín
Itálie
Chorvatsko
Rumunsko
Bukurešť
To jsem nebyl(a) já.
Byl(a) jsem to já

Co je na internetu, to už nesmažete

Soukromí

Po internetu se nepohybujete anonymně. Typicky se dříve nebo později někam přihlásíte a do té doby zanechané stopy dokonale spojíte se svoji identitou. Sice existuje spousta technik a nástrojů, jak si anonymitu udržet, ale to je nad rámec této publikace.

Pokud něco na internet umístíte (fotku, text, ...), nemusí to jít úplně snadno odstranit. Pokud jsou Vámi publikované věci veřejně dostupné, dříve nebo později si jich mohou všimnout vyhledávače typu google.com, seznam.cz a zaindexovat je. Jednoduše řešeno, pořídí si kopii, která může existovat i bez Vašeho originálu. A co teprve pak, pokud si toho všimne „archiv internetu“ na www.archive.org.

Přenastavte si Facebook a další služby!

Doporučuji tak projít nastavení soukromí všude tam, kde nějaké informace sdílíte. Pokud používáte Facebook, pak určitě navštivte http://bit.ly/facebook-soukromi a zjistěte si, kdo všechno vidí Vaše příspěvky a co všechno dalšího je zcela veřejné, případně to omezte.

Pokud už jste došli do fáze, kdy výskyt na sociálních sítích omezujete a dokonce rušíte účty, pak vězte, že například na Facebooku se odstraněním účtu můžete dostat do situace, kdy se o sobě paradoxně dozvíte více informací než s ním. Facebook totiž drží tzv. stínové profily. Pokud účet máte, můžete alespoň kontrolovat a ovlivňovat to, kdo Vás kde označuje, komentuje apod. Bez účtu nikoliv, pouze můžete pasivně přihlížet.

Taktéž si je potřeba uvědomit různé technické limity. Tj. když někde něco smažete, nemusí jít nutně o fyzické smazání z disku. Může to být pouze označeno jako smazané a kdykoliv to může posloužit třeba jako důkaz při vyšetřování trestného činu.

Buď Safe Online

Pro mládež a jejich rodiče je dobrým zdrojem informací web www.budsafeonline.cz, projekt bývalého youtubera Jirky Krále společně s Avastem.

Zabezpečení domácí sítě

Extra péče by měla být věnována tzv. routeru, typicky “krabičce”, která zajišťuje přístup všech zařízení v domácnosti k internetu. Ať už po kabelu, nebo po wifi. Na zabezpečení routeru nelze napsat zcela univerzální postup vzhledem k tomu, že existuje celá řada jejich výrobců. Nemluvě o různém způsobu zapojení. Následuje tak alespoň výčet toho, na co se je třeba soustředit:

- Pravidelně aktualizovat firmware (software uvnitř zařízení).
- Mít bezpečné heslo pro přístup do administrace – tuto dostupnou pouze z vnitřní sítě, nikoliv z internetu.
- Vypnout WPS (resp. funkcionalitu WPS PIN – obvykle dohromady) – jednoduché párování zařízení.
- V ideálním případě zajistit, že z venku (internetu) nebude žádný otevřený port.
- Pokud to router dovoluje, provozovat dvě oddělené wifi sítě (jednu pro hosty, druhou pro vlastní zařízení).
- Bezdrátovou wifi provozovat minimálně v režimu WPA2-PSK se silným heslem.

Pomocníci v prevenci

Účet s omezenými pravomocemi

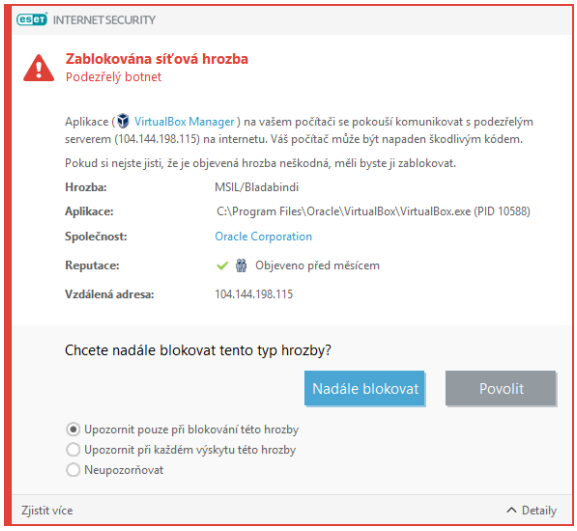
Obecně je dobré nepracovat na počítači s nejvyššími oprávněními, tedy s právy administrátora. Kdo má práva administrátora, ten může vše. Pokud pak uživatel pod takovým účtem spustí havěť nebo dojde k jejímu spuštění bez jeho vědomí (např. díky chybě v internetovém prohlížeči), i tato havěť bude moci následně provádět vše.

Je tedy vhodné opatřit účet administrátora heslem a pracovat pod účtem s běžnými uživatelskými právy. Sice nebudete schopni bez znalosti hesla administrátora instalovat nové aplikace, avšak na stejný limit narazí i případná havěť. V praxi tak nemusí takhle omezená havěť „přežít“ restart počítače, ani napáchat tak velké škody.

Ve Windows 10 lze nastavení vyvolat stisknutím kombinace kláves ⊞+I a dále pak přes menu Účty (Accounts) – Rodina a jiní uživatelé (Family & other people). Jeden účet administrátora musí existovat vždy, nicméně nic nebrání ve vytvoření dalších uživatelů typu „standardní uživatel“. Do Windows se pak hlaste přes ně. „Old school“ pohled nabízí kombinace kláves ⊞+R – zde napište *netplwiz* a stiskněte enter.

Antivirus

Antiviry dokážou významně omezit průnik havěti do počítače na různých úrovních. Na znalost uživatele přitom klade minimální nároky. Stačí ho v podstatě jen nainstalovat. Antivirus obvykle monitoruje síťový provoz během brouzdání po internetu. Další vrstvou je ochrana souborového systému. Veškeré soubory, které spouštíte, vytváříte či otevíráte, jsou taktéž kontrolovány na výskyt havěti. Pokud se i přes tyto proaktivní vrstvy podaří havěti proniknout, pak nastupují tzv. reaktivní vrstvy detekce. Takovou může být například monitoring chování běžícího programu v paměti.



Obrázek 9 Placené verze antivirů obvykle nabízejí více vrstev ochrany. Tahle vymoženost například umožní preventivně zablokovat komunikaci s již dříve škodícím serverem (ESET Internet Security).

Pro kvalitní antivirus není potřeba chodit daleko. Doporučit lze například bezpečnostní řešení společnosti ESET (Slovensko) nebo „tuzemského“ Avastu.

Ač je součástí Microsoft Windows antivirus Windows Defender, nedosahuje takové úrovně detekce havěti. Doporučuji ho tak nahradit při nejmenším řešením Avast Free Antivirus (pro domácnosti zdarma). Pokud ale chcete víceúrovňovou ochranu, což vřele doporučuji, placenému řešení se tak jako tak nevyhnete. Obvykle pak takové placené řešení obsahuje i firewall, antiphishing a další moduly. Jedná se například o produkty:

- ESET Internet Security
- ESET Family Security Pack (včetně ochrany pro mobily)
- Avast Internet Security

Na Apple iMac či Apple MacBook je situace s havětí o poznání příjemnější, nicméně sociálnímu inženýrství, oblbovačkám a phishingu lze stejně snadno naletět i tam. Navíc, pokud sdílíte data s kolegy, co pracují pod systémem Windows, nestanete se přenašečem havěti.

- ESET Cyber Security
- Avast Security pro Mac

Pokud se chystáte nějaký ten antivirus zakoupit, budeme rádi, pokud tak učiníte na stránkách https://obchod.viry.cz! Děkujeme :-)

Antivirus v mobilech

Co se týká mobilních telefonů Apple iPhone, díky uzavřenosti platformy je tento systém v podstatě zapovězen i pro havěť (a případné antiviry taktéž). Výjimkou jsou telefony ve stavu jailbreak (v takovém stavu ale standardně nejsou). Naopak telefony se systémem Google Android jsou pro havěť velice oblíbené. Důvodem je vyšší podíl na trhu, ale i naprostá otevřenost systému, kdy můžete instalovat jako oficiální, tak i neoficiální aplikace mimo Google Play. Pokud používáte chytrý telefon pouze na volání, stahování pošty a neinstalujete do něj každou kravinu, asi to nebude s havětí tak horké. Přesto bych doporučoval antivirus pořídit. Jednak je za zlomek ceny antiviru pro počítač či notebook, ale především obsahuje i řadu zajímavých funkcí v případě ztráty telefonu.

- ESET Mobile Security
- Avast Mobile Security

Nastavení nechat jak je

Dalším doporučením je nesnažit se měnit nastavení antiviru. V praxi je pak typické, že změny provedené neznalým uživatelem vedou buď ke snížení kvality detekce a nebo k výraznému zpomalení chodu počítače. Naopak, pokud se během instalace nabízí možnost zapnutí reputačních systémů či jiných technologií pro zajištění rychlejších reakcí výrobce, tyto určitě podpořte (ESET: LiveGrid, Avast: Community IQ). Získáte tím lepší detekci havěti.

Více znamená méně a zdravý rozum uživatele

Dále není vhodné provozovat na jednom počítači / mobilu více antivirů zároveň. Kromě nestability celého systému může dojít i k tomu, že správně nebude fungovat ani jeden z nich!

V neposlední řadě si je potřeba uvědomit, že antivirus je pouze „hloupý“ program a nelze se na něj plně spoléhat. I když oplývá opravdu moderními technologiemi, žádný nenabízí 100% detekci škodlivého kódu. Vždy existuje riziko, že narazíte na něco, co není antivirus schopen zachytit. Jak už bylo uvedeno, antivirus je potřeba brát pouze jako součást pomyslné mozaiky bezpečnostních opatření a důležitou částí mozaiky je hlavně **zdravý rozum uživatele**!

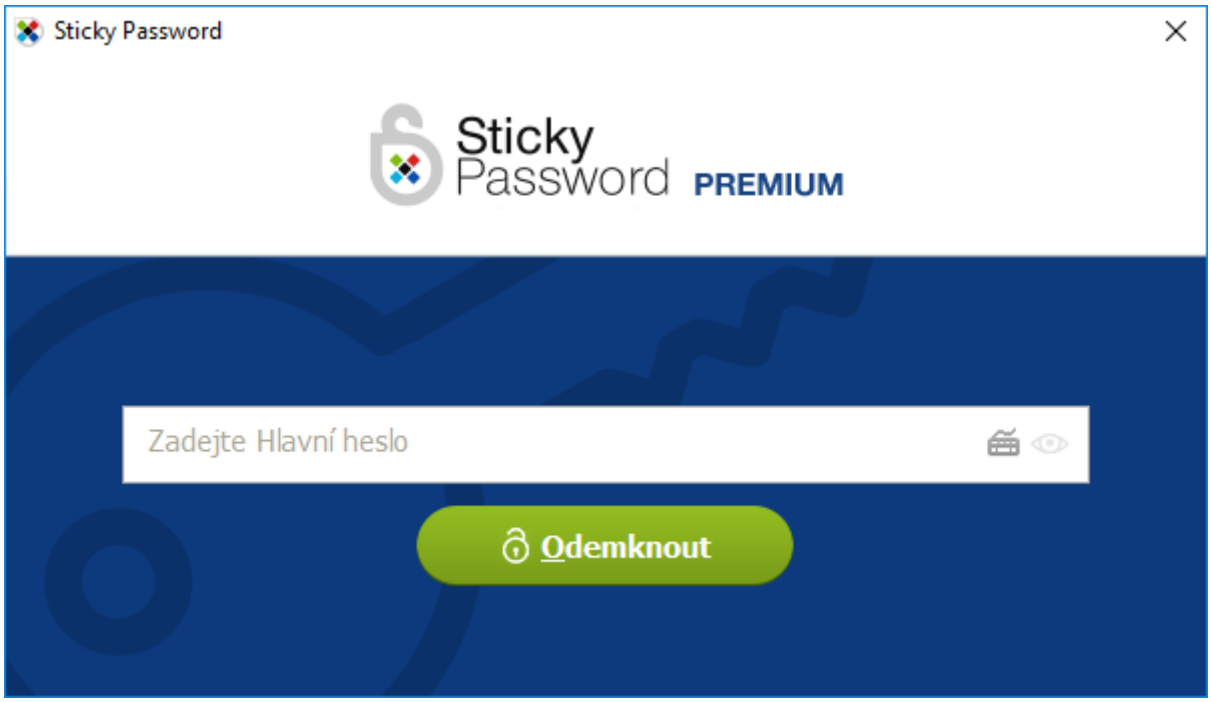
Správce hesel

Pokud budeme dodržovat pravidla v kapitole věnované heslům, nemáme šanci si je všechny zapamatovat. Z tohoto důvodu existují aplikace pro správu hesel, které nám fungování výrazně usnadní.

Jako trezor

Princip jejich fungování je jednoduchý. Abyste se dostali ke všem heslům, je potřeba si zapamatovat jediné hlavní heslo (master password). Pokud ho správně vyplníte, odemknete tím přístup k ostatním.

Bez hlavního hesla se k žádným dalším nedostanete, neboť ty jsou tímto heslem zašifrovány (tudíž jsou k ničemu i případnému útočníkovi). Hlavní heslo si obvykle nastavíte při prvním spuštění správce hesel.



Obrázek 10 Tohle je jediné heslo, které si musíte u správce hesel pamatovat. Jeho zadáním odemknete přístup ke všem dalším. Programů na správu hesel je spousty. Ale jenom zakoupením Sticky Password podpoříte kapustňáky :-)

Dbejte na to, aby bylo opravdu extra silné a bezpečné! Rozhodně ho nepoužívejte nikde jinde a především si ho zapamatujte! Jeho ztráta by znamenala ztrátu všech ostatních uložených hesel!

Celý princip lze přirovnat k běžnému fyzickému trezoru, kdy musíte nacvakat správnou číselnou kombinaci (zde hlavní heslo), abyste se dostali k jeho obsahu (zde další hesla). Oproti fyzickému trezoru je zde ale několik výhod:

- Správce hesel se z bezpečnostních důvodů automaticky uzamkne po několika minutách nečinnosti (lze opět odemknout hlavním heslem).
- Hesla se mohou automaticky bezpečnou formou přenášet mezi několika vašimi zařízeními. Není tak problém si podobného komfortu užívat na stolním PC, notebooku či tabletu. Zároveň se jedná o formu zálohy.
- Správci hesel obsahují doplňky pro internetové prohlížeče. Díky nim pak nemusíte zadávat jména/hesla pro každou službu (e-maily, Facebook, ...), kterou právě navštěvujete. Pokud jsou hesla odemčena hlavním heslem, vkládají se automaticky.

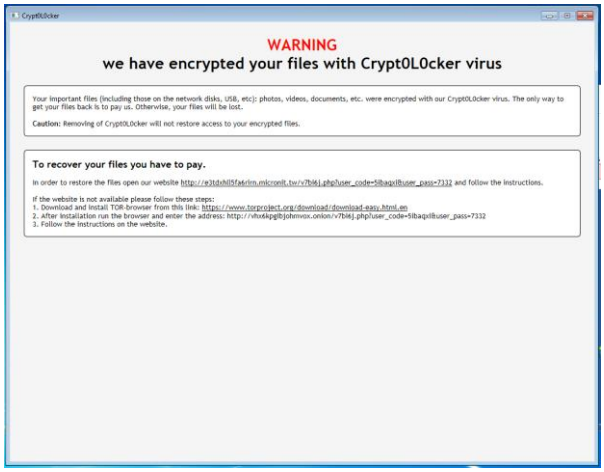
Doporučení správci hesel:

- Sticky Password
- Avast Passwords (i součástí antiviru)
- ESET Smart Security Premium

Pokud se chystáte správce hesel zakoupit, budeme rádi, pokud tak učiníte na stránkách https://obchod.viry.cz! Děkujeme :-)

Zálohování

Přemýšleli jste někdy nad tím, jak byste reagovali například v momentě, kdy zjistíte, že jste zrovna přišli o veškeré fotografie z dovolených, historické fotografie, důležité dokumenty, ... (prostě data)? Pokud by Vám to nevadilo, můžete tuto kapitolu rovnou přeskočit :-)



Obrázek 11 Představte si, že jste přišli o roky učetnictví, fotografie z dovolených, důležité dokumenty, ... To lze bohužel lehce zažít po útoku havěti typu ransomware!

Zálohování je prevencí před ztrátou důležitých dat vlivem selháním hardware. Dříve nebo později například odejde do „věčných lovišť“ pevný disk, na kterém jsou uloženy. Počítač, resp. data mohou být též zlikvidována přepětím v elektrické síti či zásahem blesku. Zálohování je i vhodnou prevencí před útokem havěti a to především typu **ransomware**. Ta totiž veškerá důležitá data znehodnotí tím, že je zašifruje a po uživateli vyžaduje výpalné v hodnotě až několika 10 tisíc Kč. Zjednodušeně řečeno, prostě jsou fuč.

Nutností je automatizace – ruční zálohování „omrzí“

Praxe ukázala, že pokud má zálohování fungovat, musí být zautomatizováno. Nelze se spoléhat na to, že budete den co den něco manuálně spouštět. Časem to omrzí a pak se na to zapomene zcela. Taktéž nelze za zálohování považovat to, že soubory/složky vezmete a nakopírujete je na stejný disk o složku vedle. Za zálohování nelze považovat ani tzv. RAID1, kdy jsou v počítači například dva pevné disky a probíhá mezi nimi automatické zrcadlení (=na obou je totéž).

Zálohování jako prevence před havětí typu ransomware, jenž zanechává spoušť...

Situaci se zálohováním změnila havěť typu **ransomware**. Pokud zálohujete na externí disk připojený přes USB, či na další disk, který je uvnitř počítače, jako prevence před ztrátou dat vlivem selhání hardware je to dostatečné. Jako prevence před ztrátou dat vlivem ransomware nikoliv.

Pokud se havěť typu ransomware do počítače dostane, tato detailně prochází veškeré připojené disky a všechny nalezené dokumenty, obrázky (fotografie), archivy, ..., zašifruje=znehodnotí. Znehodnotí tak i samotné zálohy! A připojovat disk manuálně jen v době záloh a pak ho zase odpojovat, to nevydržíte dělat věčně...

Synchronizace pomocí cloud služeb

Částečným řešením může být využití služeb, které dokáží zajistit synchronizaci (=kopírování) vybraných složek napříč vašimi zařízeními (PC, notebook, tablet, ...) skrze internetové úložiště. Pokud do takových složek zahrnete i složky pro vás důležité (s dokumenty, fotografiemi, ...), tyto se budou v podstatě automaticky zálohovat. Při nízkém objemu dat jsou tyto služby zdarma, při vyšším pak za peníze.

Pokud pak, nedej bože, prorazí ransomware a zašifruje soubory na disku, tato zašifrovaná podoba souborů se zákonitě dostane i do internetového úložiště. V ten moment ale stále existuje několik způsobů, jak data zachránit:

- Máte jiný počítač (notebook, stolní PC, ...), který byl do synchronizace taktéž zapojen a v době útoku nebyl zapnut. Pokud takový počítač spustíte a nedovolíte spuštění synchronizace

(například odpojením od internetu), můžete nepoškozené soubory z doby před útokem najít přímo na něm. Otázka: jsou tam zaneseny i poslední změny těsně před útokem?

- Využijete funkce těchto synchronizačních služeb, které dokážou držet několik předchozích verzí od každého souboru. Budete se tak schopni vrátit k verzi fotografie před útokem a verzi po útoku (nečitelnou) zlikvidovat. Nevýhodou je, že tuto operaci nelze obvykle provádět hromadně na větším množství souborů.

Příklady těchto služeb:

- Microsoft OneDrive
- Google Drive
- Dropbox

Síťové zálohování na zařízení typu NAS

Plnohodnotným řešením je pak zálohování na síťový disk, který může být umístěn například na zařízení typu NAS (Network Attached Storage). Pokud to není vysloveně špatně nastaveno, dnešní ransomware se k zálohám na síťovém disku nedokáže dostat a nemůže je tak znehodnotit. Pro odborněji založené: zálohovat se musí přes tzv. UNC cestu se striktně nastavenými právy.

Obrázek 12 Dovnitř se "loupne" jeden nebo více pevných disků (podle modelu). Ideální pro zálohy a nejen to!

NAS je přitom malá krabička, ve které je pevný disk. Kromě funkce domácího úložiště může sloužit třeba i jako zdroj filmů do televize či hudby pro sound systém. Prvotní investice je vyšší, pak ale máte na několik let klid, nemluvě o širokých možnostech využití.

Příklady značek NAS:

- Synology
- Qnap.

Možnost zakoupit NAS nabízíme i na https://obchod.viry.cz včetně případné pomoci s konfigurací a nastavením.

Záplatování

V podstatě jakýkoliv program obsahuje nějaké ty chyby. Některé pak mohou být kritické a způsobit to, že se havěť do počítače dostane bez vašeho přispění (nemusíte na nic klikat ani nic spouštět). Vše závisí na tom, co nastane dříve: zda ji opraví tvůrce programu prostřednictvím aktualizace, a nebo zneužije útočník. Pokud je rychlejší útočník, hovoříme o tzv. **zero-day exploitu**. Takové útoky jsou pak velice nebezpečné, neboť ještě na chybu neexistuje oficiální záplata a nelze se tak jednoduše bránit. Vydání záplaty výrobcem programu je jedna věc, důležitá je ale především její včasná instalace do Vašeho počítače.

Bohužel neexistuje společný kanál na aktualizaci veškerých programů ve vašem počítači. Každý výrobce programů tak má vlastní aktualizační proces v různě pokročilém stádiu (novou verzi musíte stáhnout manuálně z webu výrobce a nebo se prostě nainstaluje automaticky) anebo nemají žádný.

U chytrých mobilních telefonů je to jednodušší díky existenci knihoven aplikací jako Google Play či Apple Store, tzn. telefon vám jednou za čas oznámí, že některé aplikace zaktualizoval, případně že je můžete jedním ťuknutím hromadně zaktualizovat vy. V případě aktualizace samotného telefonu (aktualizace firmware) už to tak slavné být nemusí. Hodně záleží na značce a typu telefonu a jeho stáří. Proč by měl výrobce aktualizovat starý model telefonu? Jen si hezky kupte nový!

V případě operačního systému Microsoft Windows tak určitě zapněte pravidelné a automatické stahování aktualizací (kombinace kláves ⊞+I a tam „Aktualizace a zabezpečení“).

Záplatované by měly být všechny programy, které ať už přímo (webové prohlížeče + doplňky) nebo nepřímo souvisí s internetem (prohlížeč PDF, obrázků, dokumentů, ...). Pro běžného „smrtelníka“ je ale docela problém určit, které to jsou a vlastně jich může být tolik, že se to stává problémem pro téměř kohokoliv.

Z tohoto důvodu vzniklo několik aplikací, které celý počítač kompletně projdou a umožní aktualizovat nejznámější programy velice jednoduše a to i bez ohledu na to, kdo je jeho výrobcem.

Příklady:

- Kaspersky Software Updater

Paranoia?

IoT – Internet of Things – internet věcí

Čím dál častěji se setkáváme s pojmem **IoT (Internet of Things) – „internet věcí“**. Sem patří různá fyzická zařízení včetně některých automobilů, ledniček, televizorů, žárovek a dalších zařízení, které lze připojit k internetu a která si mezi s sebou dokážou vyměňovat data. Více o IoT naleznete například na http://bit.ly/iotzarizeni. Zní to sice skvěle, že si lednička dokáže sama objednat nové zboží a upozorní Vás na staré prošlé k vyhození, že automobil sám přijede před dům když zjistí, že máte jít do práce, že žárovky přestanou automaticky svítit v momentě, kdy jiný IoT senzor zaznamená dostatečný přísun slunečního záření, ALE...

Každé takové inteligentní zařízení tvoří člověk a člověk dělá chyby. Dělá je sám a zanáší je i do programů, které vytvořil. Chyby tak zákonitě budou obsahovat i IoT zařízení. Je potřeba se připravit, že to, co se nyní děje na mobilech, tabletech, počítačích a popisuje to tato publikace, to se v budoucnu bude dít i na automobilech, ledničkách, televizorech, žárovkách a dalších zařízeních! Nevěříte? Už v roce 2015 se podařilo přes internet ovládnout „IoT“ automobil Jeep Cherokee a poslat ho i s bezmocným řidičem do příkopu! Více na https://www.viry.cz/zavirovani-automobilu-pres-internet/

Každé zařízení připojené k internetu je další potenciální dírou do sítě

Dále si je potřeba uvědomit, že každé zařízení připojené do internetu je potenciální díra do naší domácí či firemní sítě. V zařízení může být chyba a pokud se do něj útočník naboura, bude uvnitř sítě. Zcela se tak vyhne například firewallu na routeru, který čeká na útoky zvenčí, nikoliv zevnitř sítě. Běžné jsou pak „šmírovací“ funkce některých IoT zařízení. Konkrétně chytré televizory, tzv. smart TV tím byly v minulosti vyhlášené.

Závěr

Používejte zdravý rozum, šetřete s klikáním, nevěřte každé kravině, používejte antivirus, záplatujte a zálohujte a občas se podívejte na **https://www.viry.cz**.

Publikace by se dala nafukovat o desítky až stovky dalších stran. Detailnější informace tak budu postupem času umísťovat na adresu **https://www.viry.cz/kniha**, v podobě extra článků zaměřujících se na konkrétní věci (například na instalaci a použití konkrétního antiviru, zálohovacího SW, ...). Kromě toho tam bude vždy k dispozici poslední verze této publikace i soupis toho, co v ní bylo v rámci každé revize doplněno.

Nebudu se bránit, pokud dílo finančně podpoříte dobrovolným příspěvkem a to v některé z forem, která je uvedena v úvodu.

No a pokud byste se přeci jenom stali obětí útoku, můžete využít službu **https://www.neslape.cz** pro vzdálenou pomoc.

Děkuji za pozornost a zdravím,

Igor Hák (Igi)

Rejstřík pojmů


VIRY.CZ
...když se havěť stává obětí !