KYBERBEZPEČNOST 101

Velmi stručný přehled rizik, útoků i obrany v kyberprostoru

Boleslav Vraný
bolek@bolekvrany.cz
6. října 2020

Zpracováno pro vnitřní potřebu Pracovní skupiny pro sociální otázky při České biskupské konferenci

Obsah

Shrnutí

Široké rozšíření počítačů, mobilních telefonů a nejrůznějších chytrých zařízení připojených k internetu s sebou přináší velké výhody, ale i mnohá rizika. Cílem tohoto dokumentu je velmi stručně shrnout hlavní způsoby selhání a napadení počítačových systémů a rizika z toho plynoucí, jakož i možnosti obrany na úrovni jednotlivců.

Některé rizika plynou ze selhání systémů v důsledku poruchy, chyb obsluhy, ztráty zařízení či postupné degradace nosičů dat (např. CD), která vede k nemožnosti data přečíst. Mnohem více rizik však plyne z napadení těchto systémů, které může být vedeno různými aktéry a s různými cíli. Především je třeba zdůraznit, že takové napadení nemusí být nutně provedeno člověkem. Existuje obrovské množství škodlivých kódů, které se samy šíří tak, že na internetu vyhledávají zranitelné nebo špatně zabezpečené systémy a napadají je. Jiné se automaticky stahují do počítače, pokud je uživatel vylákán k návštěvě webové stránky napadené takovým kódem. Uživatel může být vylákán k její návštěvě, jsou známé i případy, kdy byly takto infikovány zcela legitimní zpravodajské stránky.

Cíle útoků mohou být velice různorodé, stejně jako jejich aktéři. Kriminálním aktérům jde zejména o zisk, který mohou získat řadou způsobů. Velice nebezpečné jsou krádeže osobních údajů, které mohou umožnit až vydávání se za oběť útoku při komunikaci s bankami, úřady atd., tzv. krádež identity. Velice nebezpečné je i vydírání skrze útoky na data uživatelů, platby výpalného za zpřístupnění kriminálníky zašifrovaných dat nebo výpalného za nezveřejnění ukradených dat, zejména pokud jsou takovým softwarem napadeny počítače v klíčových službách jako nemocnice nebo správa města. Stále populární je získávání přístupových údajů do bankovnictví, těžba kryptoměn na napadených počítačích. Ale jsou i další způsoby získání peněz, zejména zapojení napadených počítačů do sítě, tzv. botnetu, který lze pronajímat dalším aktérům k jejich činnosti, např. k provádění jiných typů útoků nebo k provozování různých nelegálních burz apod.

Cíle státních aktérů se liší podle státu. Obecně zaujímají vysoké příčky špionáž a průmyslová špionáž. Speciálně v případě Ruska pak jde o šíření dezinformací, o zahlcení kyberprostoru šumem, o vytváření dojmu, že pravdy se nejde dopátrat. Čína ve velkém využívá online světa ke sledování vlastního obyvatelstva a jeho potlačování, speciálně v případě Ujgurů. Některé státy již sáhly k útokům na fyzickou infrastrukturu protivníka. V tomto směru bohužel výrazně přituhuje a již došlo i k útoku na vodárenskou soustavu v Izraeli, významný přístav v Íránu a elektrickou rozvodnou síť na Ukrajině. Obecně dochází ke zkoumání napadnutelných systémů a přípravě bojiště pro případný útok.

Pandemie Covid-19 situaci ještě výrazně zhoršila. Téměř okamžitý hromadný přesun zaměstnanců na home office způsobil, že miliony lidí najednou pracují ze svých osobních počítačů, které jsou obvykle mnohem hůře zabezpečeny než počítače firemní, a z nich se připojují k firemní sítím a datům. Osobní počítače zaměstnanců jsou obvykle sdíleny s dalšími osobami, např. i dětmi, slouží také ke hraní her atd. Firma jen těžko může kontrolovat či dokonce vynucovat úroveň zabezpečení na těchto počítačích, aktuálnost softwaru, zabezpečení domácí sítě atd. Naopak často musí dovolit přístup zvnějšku i k systémům, které doteď byly chráněny firemním firewallem. To vše přidává ohromné množství příležitostí pro útok na firemní sítě a data, jakmile se k nim zaměstnanec připojí.

Covid-19 navíc poskytl obrovské příležitosti pro nalákání uživatelů k návštěvě různých podvodných stránek s „informacemi“ o pandemii a následnému proniknutí škodlivého kódu do počítače, vylákání plateb za „zaručené“ léky, šíření politicky i jinak motivovaných dezinformací atd.

Rizika podle původu

Státní aktéři

Velmi aktivní jsou především Čína, Rusko, Írán, Severní Korea.

V případě **Číny** jde zejména o špionáž a průmyslovou špionáž a násilí proti vlastnímu obyvatelstvu prostřednictvím systému sociálního kreditu, kontroly obyvatelstva atd. V poslední době zřejmě stála i za masivním kyberútokem na Austrálli.

Rusko má asi nejširší spektrum aktivit v kyberprostoru včetně cílených kybernetických útoků na Estonsko 2007 a Ukrajinu 2017. V případě Estonska šlo o blokování systémů bank a státních institucí, což vedlo např. k nemožnosti provádět platební transakce. V případě Ukrajiny šlo o pokus na měsíce vyřadit rozvodnou síť. Dále obrovské množství špionáže, průniků do systémů, fake news, ovlivňování veřejného mínění, zasévání chaosu. Čína se snaží budovat lepší obraz Číny; Rusko se snaží zpochybnit existenci pravdy a možnost dopátrat se pravdy.

Severní Korea má tisíce hackerů, kteří provádějí útoky zejména za účelem získání peněz pro režim, tedy útoky na banky, kradení kryptoměn atd. Významné je také sledování a napadání uprchlíků.

Írán, USA a Izrael jsou také velice sofistikovaní aktéři se značnými kapacitami. Mezi těmito třemi zeměmi velmi výrazně přituhuje a dochází k eskalaci kybernetických útoků.

APT (Advanced Persistent Threat)

APT (Advanced Persistent Threat): doslova „pokročilá trvající hrozba“. Termín označuje pokročilé skupiny, které jsou schopny provádět velice sofistikované dlouhodobé kampaně i proti velmi kvalitně zabezpečeným systémům. Obvykle není přesně známo, kdo za nimi stojí, proto se označují čísly – APT28, APT29 nebo kódovými jmény jako Fancy Bear, Cozy Bear, Charming Kitten atd. Přesto je často mnoho důvodů je spojovat s určitým státem a pak se do názvu někdy promítá země – Bear (Rusové), Panda nebo Dragon (Čína), Kitten (kotě, Írán, Persie) atd.

Kriminální aktivity

Vydírání, zastrašování, šikana, krádeže peněz, krádeže přístupových údajů, krádeže identity, průmyslová špionáž mezi firmami, obchod s drogami a zbraněmi na nelegálních burzách tzv. DarkWeb. Typicky organizované skupiny, gangy, mafie, často ovšem jde i o kriminální aktivity mezi spolužáky, kolegy atd. – kyberšikana, pomluvy, špehování mezi manžely apod. Může jít i o pomstu propuštěného zaměstnance. Existují skupiny, které se specializují na kyberkriminalitu a hackování, na černém trhu existují komerční nástroje umožňující nabourat se do systémů oběti. Různé skupiny si kradou know-how i mezi sebou.

Značná část pochází z Ruska, řada škodlivých kódů dokonce detekuje, zda běží na počítači s ruským jazykovým nastavením (např. ruská klávesnice) a pokud ano, tak neútočí. Existuje značné provázání mezi ruskými státními aktivitami v kyberprostoru a ruskými kriminálními hackery.

Existuje také velice rozsáhlý černý trh, na kterém je možné koupit prakticky vše včetně tohoto:

- Informace o dosud nepublikovaných zranitelnostech. Ne každý, kdo najde zranitelnost, s ní nakládá zodpovědným způsobem. Za zranitelnosti se platí od desítek po desítky tisíc dolarů, podle toho, jak jsou závažné, rozšířené a zneužitelné.
- Automatizované nástroje pro hackování

- Kapacity botnetů, tedy sítí infikovaných počítačů – za příslušný poplatek může být botnet využit pro vaše cíle, například útoky na další počítače, rozesílání spamu nebo cryptomining.
- Najmutí si hackerů
- Seznamy ukradených přístupových údajů (uživatelská jména, hesla) s desítkami milionů položek.
- Seznamy osobních údajů, čísel platebních karet

Vynesení (exfiltrace) dat

Vynesení dat zaměstnanci, subkontraktory atd., ale i hackery. Může jít o únik bez zlého úmyslu, např. si zaměstnanec stáhne si data na soukromý počítač kvůli práci z domova. Ovšem i to je problém. Jednak k soukromému počítači může mít přístup řada neoprávněných lidí a je obvykle celkově mnohem hůře zabezpečen, jednak jde o problém z hlediska regulací typu GDPR.

Může ovšem jít i o vynesení dat zaměstnancem s cílem data zneužít, jako např. využít seznam klientů při rozjetí vlastní firmy, předat data třetí straně, rozesílat klientům pomluvy nebo cíleně vydírat zaměstnavatele. Může jít také o získání dat třetí stranou díky neoprávněnému průniku do systému nebo nalezení nezabezpečené databáze někde na webu (pozoruhodně častý problém). Možnosti zneužití pak záleží na obsahu získaných dat.

Extenzivní nebo neoprávněný sběr dat.

Existují legitimní důvody pro vyžadování a uchovávání některých osobních údajů, např. e-shop potřebuje znát adresu zákazníka, aby mu mohl zaslat požadované zboží. Potřebuje uchovávat fakturu, která tyto údaje obsahuje. Zde je problémem hlavně možný nelegální přístup k datům.

Ovšem obrovské množství nejen osobních dat je sbíráno spíše proto, že to prostě jde, mohou se hodit, slouží k profilaci uživatele, cílení reklamy atd. Často je nutné tzv. opt-out, tedy aktivně odmítnout zařazení do programu sledování a sběru dat. Mnohdy platí, že ne služba, kterou používáte (obvykle zdarma) nebo věc, kterou jste si koupili, ale vy sami jste „produkt," o který jde. Příkladem může být zahlcení internetu cílenou reklamou, protože z ní plynou zisky stránkám, které jsou pro čtenáře zdarma. Příkladem mohou být i tzv. chytré televize, které jsou mnohdy levnější než ty „hloupé". Důvod je prostý – chytrá televize umí sbírat data o tom, na co se díváte a jak dlouho, a tato data je možné obchodně využít.

Jde o veliký etický, právní i technický problém, který je předmětem regulací jako GDPR. Z hlediska právního jde zejména o ochranu soukromí, z hlediska technického takový sběr dat zásadně rozšiřuje prostor pro útoky, ať už zneužitím sebraných dat nebo napadením nástrojů, které slouží ke sběru dat.

Hacktivismus

Hacktivismus je snaha prostřednictvím útoků v kyberprostoru dosáhnout nějakých politických, společenských nebo podobných cílů. Může mít řadu podob od prostého napadení webových stránek například vlády nebo banky DDoS útokem, který zabrání jejímu zobrazování, přes v podstatě vandalismus vedoucí k tomu, že jejich web zobrazuje zprávu, kterou hacktivisté chtějí (třeba sebekritiku banky) až po **velice závažné útoky typu cíleného vyzrazení utajovaných skutečností**, které aktivista získal – viz Julian Assange a jeho zveřejnění statisíců tajných zpráv americké vlády ve jménu aktivismu za novou, lepší, otevřenější budoucnost. Zajímavé je, že zveřejnil jen americká data,

a ne třeba ruská nebo čínská, dále že přes Wikileaks nakonec unikla i původní data bez začerněných osobních údajů, což vedlo ke ztrátám na lidských životech.

Velice závažný útok byly i BlueLeaks v roce 2020, kdy hackeři v reakci na zabití George Floyde policisty zveřejnili cca 270 GB dat z policejních spisů, videozáznamů a dalších zdrojů. Bohužel opět mnohdy včetně detailních osobních informací, které mohou poškodit značné množství osob, ať už policistů nebo civilistů.

Hrající si amatéři

Hrající si amatéři, anglicky označovaní jako script kiddies (skriptující děti), překvapivě představují vážný problém. Existuje celá řada nástrojů pro hackování, které si stačí stáhnout a začít experimentovat, což často dělají právě děti a teenageři. Podaří se jim průnik do systému, mohou i něco změnit, získat nějaká data atd. Může jít o snahu získat prospěch (například si upravují známky v systémech školy), ale i jen o „neškodné“ hraní. Bohužel tyto děti obvykle pořádně neví, co v systému dělají, a mohou ho vážně poškodit, aniž by chtěly.

Nedbalosti, chyby, ztráty zařízení apod.

Nedbalost, chyby operátorů, nedostatečná údržba, ztráty zařízení, chybná nastavení, chybné zabezpečení představují velice časté riziko, byť bez jakéhokoliv úmyslu. Ilustrativním příkladem z domácího prostředí je notebook politý čajem. Po nějaké době už se data z disku dají jen těžko zachránit bez velikých nákladů na specializované postupy. To se samozřejmě může stát i ve firmě a ztrátou dat nebo výpadkem systému mohou vzniknout značné škody. Jiným příkladem je selhání starých systémů nebo to, že operátor omylem smaže důležitá data nebo vypne klíčový systém. Rozsah škod se pak pohybuje od osobní nepříjemnosti kvůli ztrátě fotek z dovolené po mnohamilionové škody (viz. zrušení stovek letů British Airways z důvodu problémů s dodávkou proudu a nedbalosti technika.)

Zaměstnanec ztratí notebook včetně dat – může dojít ke ztrátě dat, pokud nebyla zálohována, nebo k prozrazení citlivých dat, pokud nebyla šifrována. Starý počítač je prodán do bazaru, aniž by někdo smazal data. Existují reálné případy, kdy se v bazarech objevily počítače z účetních firem nebo bankomatů včetně dat klientů a údajích o transakcích platebními kartami.

Velikou částí tohoto bodu je otázka chybného nastavení a zabezpečení, a to zejména z důvodu, že nikdo nezměnil výchozí nastavení. Výrobky přichází s nějakým výchozím nastavením, jinak to ani nejde. Výchozí nastavení je ale často děláno podle hesla „zapojíte a funguje to, netřeba se starat.“ Tudíž jsou povolené mnohé služby, které uživatel ve skutečnosti nepotřebuje. Více povolených služeb však znamená více potenciálně prolomitelných dveří do systému. Výchozí nastavení je známé a dokumentované ve veřejně dostupných manuálech včetně např. výchozích hesel pro správu zařízení. Kdokoliv se tedy může snadno připojit a konfigurovat zařízení dle svých potřeb, stačí mu k tomu běžně dostupné nástroje k vyhledání takového zařízení na internetu a znalost manuálu. To je ohromný problém např. a nejen u domácích internetových modemů, wi-fi sítí nebo internetových kamer. Instalaci je vhodné nechat profesionálovi, který ví, jaké služby budou potřeba a jak je bezpečně nastavit. Bohužel se tak mnohdy neděje ani ve firemním nebo státním prostředí.

Zásahy vyšší moci, selhání systémů

Výpadky proudu, požáry, povodně apod. Výpadek proudu způsobí, že systém nefunguje. Stará data nejdou přečíst, protože vypálené CD/DVD časem degradovalo – běžný problém i v domácnostech, nepříjemné ztráty starých fotografií, nahrávek dětí atd. V prostředí firem nebo organizací mohou být škody velmi vysoké, viz již zmíněné rušení letů British Airways z důvodů problémů s dodávkou proudu.

Změny legislativy a zavádění sankcí

S rostoucím využíváním modelu, kdy se software nekupuje, ale pronajímá nebo je poskytováno roční předplatné, roste riziko ze změny legislativy a zavádění sankcí. Uživatel v důsledku těchto změn ztratí přístup k předplacenému sw. Příkladem může být Venezuela, kde firma Adobe v důsledku sankcí zrušila předplatné Photoshopu všem zákazníkům, včetně nevládních organizací bojujících proti režimu.

Napadení dodavatelského řetězce

Hardware, který přijde již zavirovaný, případně s nainstalovanu hardwarovou „štěnicí.“ Je smutnou skutečností, že spousta mobilních telefonů už přímo z výroby obsahuje celou řadu nechtěných a potenciálně zneužitelných aplikací. Napadením dodavatelského řetězce však bývá myšleno spíše to, že dodavatel do výrobku o své vůli přidá něco, nějakou „štěnici,“ která pak slouží k získávání dat. Populární článek agentury Bloomberg z roku 2019 o nálezu takových přidaných čipů na některých motherboardech z Číny se naštěstí ukázal jako nepravdivý, nicméně technicky to možné je.

Zranitelnosti a exploity

Zranitelností je myšlena chyba nebo slabina v návrhu, implementaci, provozu nebo řízení práce se systémem. Exploit znamená způsob, jak tuto zranitelnost využít. Oboje lze krásně ilustrovat na zabezpečení šuplíku zámkem (obrázek díky U.S. Air Force OPSEC Support Team)

- Návrhová chyba: autora nenapadlo, že toto zabezpečení lze obejít prostým vytažením horního šuplíku. Správné by bylo zamykat horní šuplík. Oděmčený zámek lze snadno odhalit, čímž se zabezpečení stane nefunkčním, dokud někdo nesežene další zámek. Mnohem lepší řešení by byl pevně přidělaný zámek, který vždy jde alespoň zacvaknout.
- Implementační chyba: šrouby na kování jdou vyšroubovat zvenčí. Správně by to mělo jít jen zevnitř.
- Chyba v řízení práce: zámek někdo odhalil a nejde to zamknout. Jiná možná chyba: zámek sice je na místě, ale klíče má příliš mnoho lidí.
- Slabá místa – i po odstranění chyb zůstanou slabá místa, třeba možnost přeštípnout kování dostatečně velkými nůžkami, otevřít zámek paklíčem nebo se provrtat dřevem.

Každý systém bude mít nějaká slabá místa a záleží na tom, jak vysokou úroveň bezpečnosti požadujeme. Trezor banky je podstatně kvalitnější než domácí trezor a ten je mnohem kvalitnější než šuplík. Ale do všech se dá při dostatečném úsilí dostat. Otázkou je vyvarování se chyb a volba dostatečné úrovně zabezpečení.

Exploity: vytažení horního šuplíku, vyšroubování kování, paklíč, nůžky, vrtačka.

Ve světě počítačů nejsou věci tak přehledné, ale software i hardware obsahují různé zranitelnosti. Jejich dopady se liší od zranitelností poměrně banálních až po takové, které umožní útočníkovi spustit na zranitelném počítači jakýkoliv kód, a to s nejvyšším oprávněním, což umožňuje úplné ovládnutí počítače. Bohužel i takové zranitelnosti skutečnosti existují.

Ne všechny zranitelnosti jsou stejně závažné, ne na všechny zranitelnosti existují exploity. Existují postupy pro tzv. zodpovědné odhalení zranitelnosti, kdy ten, kdo jí identifikuje, informuje nejprve výrobce dotčeného hw nebo sw, aby jim dal čas na opravu chyby. V ideálním případě je chyba brzy opravena a teprve pak je zranitelnost publikována. Podobně existuje i plné odhalení, kdy je zranitelnost publikována hned v celé šíři. Nejhorší je, pokud je vážná zranitelnost známá jen úzké komunitě, která se o ni nepodělí ani s výrobcem, ani se širokou veřejností. Je totiž značně pravděpodobné, že danou zranitelnost dříve či později objeví i někdo jiný, a ten ji pak může často velmi efektivně zneužít. Proto je mnohem lépe ji odhalit, ať už s časem na opravu nebo ihned.

Typy útoků a reakcí

Ne všechna rizika v kyberprostoru jsou útoky. Např. již zmíněná a velice častá rizika selhání systému, chyby operátora nebo zásahu vyšší moci nelze považovat za útok. Stejně tak např. nelegální burza nabízející zbraně a drogy není sama o sobě útokem na cizí počítač, i když může ke své činnosti zneužívat cizí napadený počítač.

Získání přístupových údajů

Získání přístupových údajů, typicky uživatelského jména a hesla, k nějakému systému či službě je velmi žádanou věcí. Umožňuje útočníkovi provádět celou řadu aktivit. Než se jim však budeme věnovat více, je nutné říci, že řada útoků může úspěšně probíhat bez znalosti přístupových údajů, např. využitím různých zranitelností. Také je třeba říci, že existují obrovské databáze uniklých hesel a že zdaleka ne všechna hesla jsou bezpečná.

Pokud útočník získá uživatelské jméno a heslo, umožňuje mu to provádět stejné věci, jako by prováděl oprávněný uživatel. Jaké konkrétní dopady to bude mít, záleží na účtu či systému, ke kterému získal oprávnění, a na oprávněních původního uživatele. Příklady:

- Vydávat se za původního uživatele
    - Např. si jménem a na účet původního uživatele něco objednat. Existují reálné příklady, kdy si útočník nechával posílat zboží z eshopů na svojí adresu, ale platil napadený. Díky chytře vytvořeným mailovým filtrům se napadenému maily z eshopů vůbec neukazovaly a byly rovnou posílány útočníkovi.
    - Jménem původního uživatele žádat o něco jeho přátele na Facebooku. Například o přeposlání autorizačního kódu, který mu zrovna přišel od banky, když útočník vykrádá jeho účet. Nebo o návštěvu nějaké podvodné platební brány.
    - Zasílat jménem původního uživatele zprávy. Může jít o urážky, výhružky, cokoliv. Extrémním případem pak je nedávný Twitter hack, kdy útočník získal **přístup k Twitterovým účtům řady známých osobností současného amerického viceprezidenta Joea Bidena, minulého amerického prezidenta Baracka Obamy, dále Elona Muska a Billa Gatese** a cca 150 dalších. Z jejich účtů mohl odesílat jakékoliv zprávy. Je velikým štěstím, že útočníkovi šlo jen o finanční zisk a odesílal jen banální zprávy o tom, že Elon Musk vám dá 2000 dolarů za každých 1000 dolarů, které pošlete kamsi. Stejně dobře totiž mohl posílat vymyšlená politická prohlášení, úvahy o vyhlášení války, přiznání k podvodům ve firemním účetnictví atd. Dopady na mezinárodní situaci nebo na akciové trhy by mohly být ohromné.
    - Krádež identity, tedy podvodné získání a úmyslné použití identity někoho jiného, zpravidla za účelem získání finanční nebo jiné výhody (například úvěru) jménem jiné osoby nebo dokonce k poškození postavení a dobrého jména této osoby.
- Číst, stahovat, monitorovat komunikaci, například emaily, a to i dost nepozorovaně.
- Stahovat nebo modifikovat data
- Pokud má napadený účet příslušná oprávnění, tak také instalovat software, měnit konfiguraci systémů, měnit oprávnění dalších uživatelů., vytvářet nové uživatelské účty. To vše obrovsky rozšiřuje možností dalšího napadení, průniku do firmy, špionáže apod.

Útoky na fyzickou infrastrukturu

Nejzávažnější oblast, o které se naštěstí zatím spíše mluví. Bohužel už nejen teoreticky, existuje řada náznaků, že probíhá příprava bojiště a přítomnosti např. v elektrických rozvodných systémech, plynárenských systémech atd., a v roce 2020 už došlo dokonce k pokusům o otravu vody v Izraeli. Příklady útoků, ke kterým už skutečně došlo:

- Stuxnet (USA, Izrael): útok na íránské jaderná zařízení prostřednictvím viru Stuxnet, který vyřadil značnou část odstředivek používaných k obohacování uranu. Šlo o fyzickou likvidaci odstředivek skrze povely, které vedly k překročení jejich fyzických limitů.
- Triton (asi Írán s pomocí Ruska): útok na řídící systémy rafinérií v Saúdské Arábii, který naštěstí selhal díky chybě útočníků.
- Crash Override (Rusko): naštěstí neúspěšná snaha na dlouhou dobu (měsíce) vyřadit elektrickou ukrajinskou rozvodnou síť. Útok se pokusil vyřadit nadproudové a přepěťové ochrany v klíčových rozvodnách, což by vedlo k poškození transformátorů a dalších klíčových systémů, přičemž výroba nových by trvala měsíce.
- Íránský útok na vodárenské systémy v Izraeli, který by vedl k výpadku zásobování vodou nebo k otravě vody přílišným množstvím chlóru (duben 2020).
- Odvetný izraelský útok, který na několik dní vyřadil významný íránský přístav a způsobil výrazné ekonomické škody.

Provázání kybernetických a kinetických aktivit

- Kybernetické odpovědi na kinetické akce: po útoku íránských dronů na saúdská ropná zařízení v roce 2019 nařídil Donald Trump provést kybernetický útok proti řídícím systémům íránské protivzdušné obrany a zařízením Revolučních gard. Zdá se, že byly dosti úspěšné.
- Kinetické odpovědi na kybernetické akce: vybombardování íránského kybernetického pracoviště v Sýrii izraelským letectvem 2019

Sociální inženýrství

Sociální inženýrství je využití psychologické manipulace k tomu, aby lidé vykonali nějakou akci nebo vyzradili něco tajného. Cílem může být jak získání tajných informací přímo, tak získání přístupových údajů do firmy, banky apod., které pak poslouží k získání tajných informací, peněz atd.

Taková manipulace není nic nového. Učebnicový příklad najdeme již ve Švejkovi – plný text zde. Švejk chce získat vyhlédnutého psa přes svého přítele Bahníka, který se specializuje na krádeže psů. Ale pes je potvora, nežere obvyklé pochoutky, na které by se dal nalákat. Švejk si bere uniformu, aby vypadal důvěryhodně, a zapřede rozhovor se služkou, která psa venčí. Se svojí milou, dobráckou tváří předstírá, že není z Prahy a hledá cestu. Prostou otázkou „Vy také nejste zdejší?“ docílí, že služka začne vyprávět, odkud je. Švejk využije znalosti tamního místopisu, získané při vojenském cvičení, aby dále posílil její důvěru. Služka už mu pak sama nevědomky poskytuje vodítka; Švejk jen umně reaguje. Nakonec zapřede rozhovor o psu a dozví se, jakou pochoutku má rád. Hned ten den odpoledne Bahník psa ukradne, odláká ho přesně na tuto pochoutku.

Phishing

Phishing je snaha zlákat oběť k návštěvě podvodné stránky, na které zadá své přihlašovací údaje například do emailu nebo internetového bankovnictví. Podvodný mail naláká uživatele na stránky, které vypadají téměř stejně jako skutečné stránky banky, emailu, Facebooku apod. Uživatel zadá své přihlašovací údaje, ty jsou zaznamenány a později zneužity útočníkem k vysátí peněz. Stejným způsobem se získávají přístupové údaje i k jiným systémům: emailu, účtu na Facebooku, ale i přístupy do sítě zaměstnavatele atd. Vzniká pak obrovský prostor pro další využití těchto přístupů. Možnost vydávat se za napadeného, využít přístup do firmy ke krádeži dat, průmyslové špionáži, instalaci škodlivého software ve firmě apod.

Výhružné emaily

Někdy jsou k šíření škodlivého kódu využívány výhružné emaily kombinované se škodlivým kódem, který se nainstaluje do počítače oběti a umožňuje další útoky. Příklad z ČR 2018: výzva k okamžité úhradě poplatků exekutorovi. Nešlo o zisk peněz, číslo účtu bylo chybné a peníze na něj nešly odeslat, ale o to, že vystrašený uživatel otevřel email a tím se mu do PC dostal škodlivý kód, který mohl provádět další aktivity. Jindy je k vystrašení uživatele využita epidemie koronaviru, ale opět jde o to, aby si otevřel přílohu se škodlivým kódem.

Některé plošné vyděračské emaily. Prakticky nulové náklady, v poměru k nákladům velice vysoký výnos. Příklad z ČR 2019: stovkám tisíc lidí byl zaslán email tohoto typu: „natočili jsme vás masturbaci před počítačem. Pokud nechcete, aby se video dostalo dál, zaplaťte určitou částku v kryptoměně.“

Útočník skutečně získal několik set tisíc korun, přestože mail neměl reálný podklad a náklady na kampaň byly mizivé.

Podvodné emaily

Je překvapivě snadné poslat email jakoby z něčí adresy. Není k tomu vůbec potřeba přístup k jeho mailovému účtu, stačí prostě v jakémkoliv poštovním programu zadat adresu odesilatele např. reditel@nasefirma.cz. Potom poslat mail účetní, aby urgentně zaplatila nějakou podvrženou fakturu na účet útočníka. Poměrně často útočník uspěje.

Klasikou jsou zde tzv. nigerijské dopisy nabízející obrovské množství peněz za pomoc při ilegálním převodu peněz obvykle z Nigérie někam jinam. V nejlepším případě je potřeba zaplatit zálohu, po které se už kriminálníci neozvou.

Uhodnutí přístupových údajů

Ačkoli nejde o sociální inženýrství, je na místě zmínit také uhodnutí přístupových údajů nebo zkoušení obvyklých kombinací. Pokud někde unikne databáze uživatelů včetně čitelných hesel – což je samo o sobě velký problém – pravidelně se objevují hesla jako 12345, heslo, abcde, qwertz apod. Jako heslo také často slouží informace, kterou lze snadno vylákat – třeba datum narození dítěte – nebo ji lze získat zkoušením slov ze slovníku. Slovník možných odpovědí přitom často ani není příliš obsáhlý. Populární „bezpečnostní“ otázka na příjmení matky za svobodna je ukázkovým příkladem. Pokud bude mít útočník tři pokusy na uhodnutí odpovědi, tak mu Nováková, Svobodová a Novotná dávají šanci na úspěch téměř 1%. Pokud je jeho cílem např. prolomit účet jakéhokoliv zaměstnance velké firmy a zkouší jeden účet za druhým, tak se do firmy dostane téměř určitě.

Data jako rukojmí, likvidace dat, modifikace dat, vynesení dat

Ransomware

Ransomware je škodlivý software, který zašifruje data oběti a jeho původci pak požadují výpalné za jejich zpřístupnění. Čím dál častěji je navíc zašifrování doprovázeno krádeží dat a jejich postupným zveřejňováním s cílem vyvíjet tlak na oběť, aby zaplatila, případně vymáháním výpalného za to, že data nebudou zveřejněna.

- WannaCry: ransomware, který zašifroval data mnoha firem po celém světě a požadoval výpalné za dešifrování. Škody stovek milionů až miliard dolarů, připisován Severní Koreji, která se snažila získat z výpalného peníze. Velkou obětí byl britský National Health System, kde došlo k napadení desítek tisíc zařízení jako MRI, CT a další. Tato zařízení nebylo možné používat. Podobná situace, jen s jiným virem, nedávno nastala v nemocnici ve středočeském Benešově. Nemocnice v takové situaci nemohou přistupovat k rentgenovým snímkům, laboratorním výsledkům a dalším datům uloženým v počítačích a jsou nuceny odkládat péči. Extrémním dopadem pak může být i smrt pacienta, jak se nedávno stalo v Düsseldorfu.
- Rostoucí množství útoků na americká města, typicky menší města, která nemají kvalitní IT, nebo velká města v problémech (Baltimore). Na dlouhou dobu ovlivní chod města, placení daní z nemovitostí, převody nemovitostí, placení za služby včetně vodného a stočného, může ovlivnit i tísňová volání a další kritické prvky.
- U firem ohromné ztráty z nemožnosti provozovat např. logistické systémy.

- Poslední dobou vyděrači stále častěji data napřed ukradnou a pak šifrují. Mají tak možnost je postupně zveřejňovat a tím zvyšovat tlak na oběť. Dále mohou data zpeněžit na černém trhu.
- Někdy je možné data dešifrovat pomocí nástrojů od antivirových společností, protože útočníci udělali chybu v procesu šifrování. Ale rozhodně na to nejde spoléhat.
- Kriminální aktéři obvykle po zaplacení výpalného skutečně dodají dešifrovaná data. Jde o důvěryhodnost jejich činnosti – proč by jim někdo platil výpalné, když data stejně nejspíš neuvidí? Placení výpalného se pochopitelně nedoporučuje, ale i když je zaplaceno a data vrácena, můžeme si být, jist, že nebyla modifikována? To je ohromné riziko.
- Aktéři typu Severní Korea už data nedešifrují, jde o vylákání peněz a tečka.

Likvidace dat

Příkladem je útok na Saudi Aramco, při kterém byla vymazána data z desítek tisíc počítačů najednou. Data se týkala zejména logistiky a firma utrpěla značné ztráty z nemožnosti přepravovat a obchodovat s ropou.

Modifikace dat

Nepozorovaná modifikace dat je obecně obrovské riziko, které může být zneužito k čemukoliv. Příkladem v oblasti státních aktérů může být útok Ruska na OPCW – Organizaci pro zákaz chemických zbraní – při kterém zřejmě bylo cílem modifikovat data o chemických útocích na Sergeje Skripala a v Sýrii, aby byly zameteny stopy. Opačným extrémem na škále závažnosti a sofistikovanosti jsou celkem časté a někdy i úspěšné pokusy dětí měnit si své školní známky háčkováním.

Vynesení (exfiltrace) dat

Vynesení tajných údajů, obchodních tajemství, seznamů klientů atd. Využití může být různé, od využití seznamu klientů pro rozjezd své firmy, přes vydírání zaměstnavatele až po špionáž a průmyslovou špionáž. Umné vynesení dat je často je začátkem dalších útoků a zneužití včetně takových jako Wikileaks, jejich zveřejnění statisíců tajných amerických depeší a následné zabití některých agentů nepřáteli.

Sledování, odposlechy, špehování

Analýza a sledování veřejně nebo téměř veřejně dostupných dat

Záměrně uvádím jako první analýzu a sledování veřejně nebo téměř veřejně dostupných dat. Neuvěřitelně mnoho věcí se totiž lze dozvědět bez jakýchkoliv útoků jen pouhým sledováním toho, co bylo zveřejněno nebo co bylo tak špatně zabezpečeno, že je to prakticky veřejné. Příklady:

- Nedostatečně zabezpečené kamerové systémy připojené k internetu umožňují komukoliv sledovat, kam se dívají, včetně některých plaveckých bazénů nebo soukromých objektů. Příklady z ČR viz zde. Problém není jen narušení soukromí, ale i možnost na dálku sledovat, kdy například dotyčný odešel z domu a kdy se vrátí, tedy možnost pak naplánovat třeba vykradení domu nebo i horší věci.
- Příspěvky typu „Příští týden všichni jedeme na dovolenou do Řecka“ na sociálních sítích. Skvělé lákadlo pro zloděje, kteří vědí, že byt bude prázdný. Spousta lidí se tím pochlubí stovkám přátel na sociální síti, které zhusta pořádně neznají, ideálně ještě v příspěvku

otevřeném přátelům přátel nebo všem. Takové příspěvky se dají i automaticky vyhledávat a existují služby, které to skutečně dělají.

- **Sledování polohy osob na základě toho, co samy o sobě prozradí**, a vyhledávání zájmových osob v okolí. Hojně užívané služby, které vám umožní se po příchodu do restaurace apod. přihlásit a říci všem „já jsem v restauraci U dubu." Výborné ke sledování osob, ale třeba i k hledání žen v okolí za účelem v nejlepším případě seznamování, aniž by tyto vůbec chtěly. Byla jen otázka času, kdy někdo vytvoří aplikaci jako Girls Around Me v odkazovaném článku, která najde ženy v okolí, a nic nebrání tomu vytvořit podobné další. **Extrémně nebezpečným příkladem** bylo zjištění, že z veřejně dostupných dat na sociální síti Strava, kde sportovci mohou sdílet své atletické výkony v běhu či cyklistice, měřené fitness náramky včetně GPS trasy, se dají rekonstruovat pohyby hlídek po vojenských zařízeních, umístění tajných vojenských zařízení, a dokonce i sledovat pohyb vojáků poté, co se z mise vrátí domů.
- Fotografie opatřené GPS souřadnicemi nebo obsahující dobře identifikovatelné objekty v pozadí a nahrané na sociální sítě či internet obecně mohou prozradit ledasco, třeba polohu indické letadlové lodě (foto sdíleli sami námořníci), přesné souřadnice právě dodaných bojových vrtulníků v Iráku (sdíleli vojáci) nebo základnu bojovníků ISIS (sdíleli bojovníci ISIS). Vrtulníky byly obratem zničeny palbou teroristů, základna ISIS byla obratem vybombardována koaličními silami.
- Nezabezpečené WiFi sítě. V nich může kdokoliv odposlouchávat provoz včetně třeba hesel.

Skutečné špehování

Sledování komunikace zájmových osob, např. disidentů v totalitních režimech, plošné sledování populace, sledování polohy osob

- Co se státních aktérů týče, tak – aniž bych chtěl bagatelizovat taková rizika zde na Západě – jde zejména o totalitní země. Tam dochází k věcem typu povinné sledovací a šmírovací programy v mobilech (Ujgurové v Číně), povinné využití státem dodané šifry pro šifrovanou komunikaci v Kazachstánu. Taková státem dodaná šifra má stále určitý smysl pro ochranu před odposlechem nestátními aktéry, ale zároveň umožňuje státu naprosto libovolně šmírovat.
- Bohužel ale nemusí ani zdaleka jít jen o zájem státu. Ke špehování a pronásledování dochází i mezi manžely a jinými blízkými osobami, např. z důvodů podezření na nevěru či žárlivosti, mezi obchodními rivaly i partnery atd.

Technické prostředky pro špehování mohou být překvapivě triviální, např. „zapomenutý" notebook s běžícím skypem, ale může jít i o velice sofistikované nástroje, které je těžké najít, a ještě těžší odstranit. Mezi nástroje pro špehování patří tzv. keyloggery, tedy programy nebo i speciální hardware, které zaznamenávají veškeré stisky kláves na počítači, mnohdy včetně obsahu oken. To umožňuje získat hesla, texty mailů a dalších dokumentů, obrázky stránek, které si zájmová osoba prohlíží apod.

Podvržená komunikace

V jednoduchém případě třeba mail z adresy reditel@nasefirma.cz, který požaduje zaplatit přiloženou fakturu, a kterou nebohá účetní skutečně zaplatí, obzvlášť pokud už ji skutečný šéf předtím pár takových mailů poslal (reálné případy z ČR). Existují ovšem i mnohem sofistikovanější útoky ať už na lidi, nebo na počítačové systémy. Je potřeba si ověřit, zda komunikace opravdu pochází od toho, od

koho údajně pochází. V jednoduchém případě stačí zavolat řediteli a zeptat se ho. Jindy je potřeba využít softwarových nástrojů, které umožní ověřit pravost a nezměněnost dokumentu (elektronický podpis).

Odeslání emailu z adresy reditel@nasefirma.cz je příkladem naprosto triviálního útoku. Opačným extrémem jsou tzv. **kolizní útoky**. Ty vychází z toho, že pro data je možné vytvořit jakési otisky, velice dlouhá čísla s desítkami až stovkami číslic. Pokud data jen maličko změním, otisk bude úplně jiný. Tím, že je otisk tak dlouhý, je velmi malá pravděpodobnost, že různá data budou mít stejný otisk. Vždy je však nenulová. Pokud se mi podaří vygenerovat jiná data, která mají stejný otisk, mohu je podvrhnout cílovému systému a ten nepozná, že byla změněna nebo že mu dokonce byla podvržena úplně jiná data. Generování takových kolizních dat je náročné a rozhodně to není běžná záležitost, nicméně bylo reálně využito pro velmi vysokoprofilové špionážní operace, kdy byl špionážní software podepsán podvrženým digitálním podpisem důvěryhodné instituce, a tudíž se zdál legitimní.

Zajímavou variantou podvržené komunikace je tzv. **GPS spoofing**, tedy vysílání falešných signálů GPS, které vedou ke zmatení navigačních systémů vojenských i civilních. Nejde o prosté rušení, že by GPS bylo nepoužitelné. Jde o vysílání signálů, které jsou silnější než správné signály z družic systému GPS a které vedou navigační systémy oběti k tomu, že si myslí, že jsou jinde než ve skutečnosti. Mnohokrát demonstrováno v praxi i úspěšně využito. Pravděpodobně použito 2011 Íránem k navedení amerického dronu na přistání na íránské letecké základně téměř bez poškození.

Distributed Denial of Service (DDoS)

Na cílový server je posláno ohromné množství požadavků, které ho zahltí a server přestane odpovídat a tím plnit svoji funkci. Zahlcení serverů internetového bankovnictví po dobu několika dnů vede k nemožnosti provádět platby, u burzovních serverů k nemožnosti obchodovat na burze. Zahlcení zpravodajských serverů vede k nemožnosti dozvědět se po internetu, co se děje. Výsledkem pak jsou značné ekonomické škody i dopady na společnost obecně.

Jde o velice rozšířený útok, populární mezi státními aktéry i hacktivisty, ale využitelný i pro kriminální aktivity – např. vydírání možným znepřístupněním služeb skrze DDoS. Státem použito např. v roce 2007 Ruskem proti Estonsku.

Naprostá většina ostatních útoků vyžaduje proniknutí do systému nebo alespoň znalost nějaké zranitelnosti, která např. umožní útočníkovi zobrazit data, ke kterým by neměl mít přístup. Naproti tomu DDoS je příkladem útoku, při kterém cílový systém není nijak kompromitován. Do bankovního, zpravodajského nebo jiného cílového serveru se nikdo neproboural, jen je zvenku zahlcen takovým množství požadavků, že většinu musí odmítnout a tím přestává plnit svoji funkci.

Požadavky nepřichází z jednoho nebo několika málo počítačů, ale z desítek tisíc zařízení, typicky infikovaných počítačů zapojených do nějakého botnetu. Proto nejde jednoduše odfiltrovat požadavky z pár míst.

Cryptomining

Získávání kryptoměn na zařízení oběti bez jejího vědomí. Jde o výpočetně dosti náročný proces, který vyžaduje náročný hardware a značné množství času a energie. Proto se útočníkovi vyplatí raději zneužít spoustu cizích počítačů. Hlavním rizikem pro oběť však není vyšší spotřeba energie, ale to, že je zapojena do sítě botnetů, tedy na dálku ovládaných počítačů. Počítač oběti je otevřen mnoha dalším útokům.

Různé druhy škodlivých kódů

Malware

Škodlivý software obecně, program určený k poškození nebo vniknutí do počítačového systému. Zkratka ze slov malicious software, škodlivý software. **Pozor: malware se rychle vyvíjí a vznikají až desetitisíce nových variant denně.** Z toho mj. plyne, že je potřeba bezpečnostní software jako antiviry pravidelně a velmi často aktualizovat (většinou to dělají samy) a používat aktuální verze.

Virus

Škodlivý kód, který sám sebe vkládá do jiných programů. Když je napadený program spuštěn, virus se bez vědomí a souhlasu uživatele replikuje do dalších programů. Aby se mohl šířit, uživatel musí nevědomky spustit infikovaný program. Dal by se přirovnat k viru chřipky. Množí se v hostiteli, ale na další hostitele se přenáší pasivně kapénkovou infekcí, nevyhledává cíleně nové hostitele.

Červ

Škodlivý kód, který je samostatný (na rozdíl od viru se nepřidává do jiných programů) a aktivně se šíří skrze síť, aby infikoval další počítače. Pro své šíření aktivně vyhledává různé díry v zabezpečení sítě. V biologické analogii by šlo o nějaký invazní druh, který se sám aktivně šíří, vyhledává nová místa k životu, důmyslně zkoumá, kudy proniknout dál. Třeba potkan.

Trojský kůň

Škodlivý program, který se tváří jako obyčejný, k něčemu užitečný program, ale zároveň nese nějakou škodlivou funkci, která je při jeho spuštění aktivována. Touto funkcí často je otevření zadních vrátek do systému pro další útoky. Trojany se obvykle šíří pomocí sociálního inženýrství, například jako přílohy mailů, které si uživatel spustí, protože ho vylekala zpráva, že má okamžitě zaplatit exekutorovi a detaily jsou v příloze. Analogie mimo svět počítačů je zřejmá – trojský kůň z řeckých bájí, kterého si obyvatelé Tróje sami v dobré víře vtáhli do města.

Botnet

Síť počítačů napadených škodlivým sw, které mohou být na dálku ovládány a zneužity k útokům na jiné počítače, kriminálním aktivitám, šíření škodlivého sw dále atd.

Backdoor

Ddoslova zadní vrátka. Jimi může nepozorovaně vcházet do systému ten, kdo je zná. Metoda, která umožňuje obejít normální procedury, kterými se uživatel autentizuje do systému. Často bývaly v systému zanechány přímo výrobcem, aby do systému mohla například technická podpora. Dnes ale mnohem větší problém, a to zadní vrátka vytvořená malwarem, škodlivým kódem. Uživatel neví, že do jeho počítače může ještě někdo jiný, kdo může počítači zadávat příkazy, nenápadně ho využívat atd.

Scareware

Software, který používá sociální inženýrství k tomu, aby vystrašil uživatele a přesvědčil ho, aby si koupil nějaký produkt, typicky další bezpečnostní produkt (falešný anitvirus apod.) Docela často se lze setkat s webovými stránkami, které varují, že váš počítač je napaden a je třeba si stáhnout ten a ten produkt, abyste ho odstranili. Reálně jde o snahu vylekat uživatele, aby zaplatil za něco, co nepotřebuje. V nejlepším případě ten produkt nedělá nic, v horším bombarduje dalším strašením a platbami, v nejhorším jde o trojan, který otevírá zadní vrátka a sám instaluje další škodlivý software.

Legitimní nástroje zneužité k nelegitimní cílům

Pokud se útočník dostane do systému, může velmi dobře využít zcela legitimní nástroje, aby dosáhl svého (např. obyčejné kopírování souborů pro vynesení dat.)

Bloatware

zbytečné funkce navíc, které mají zákazníkovi poskytovat nějakou službu, kterou naprostá většina lidí nepotřebuje. Často je předinstalovaný na zařízení a je mnohdy obtížné se ho zbavit nebo tyto zbytečné služby vypnout. Sám o sobě může být legitimní, ale jednak zbytečně zabírá místo a ubírá výkon zařízení, ale především zvyšuje prostor pro nějakou infekci zařízení nebo útok na něj. Čím více služeb a programů totiž na zařízení běží, tím větší je riziko, že některé z nich budou obsahovat zneužitelnou chybu.

Komu připsat útok (atribuce)

Co bývá ve fyzickém prostoru snadné, to je v kyberprostoru dosti složité. Z mnoha technických důvodů se často dá jen těžko říci, že za daný malware nebo útok může ta a ta skupina nebo ten a ten stát. Některé bezpečnostní firmy se cíleně brání říkat, kdo za útokem stojí. Na původ útoku je obvykle třeba usuzovat z kombinace několika faktorů a vždy říci, jak moc jsme si atribucí jisti.

Přesto je mnohdy třeba říci, kdo je za útok zodpovědný. Pak se vychází ze způsobu, jakéhosi rukopisu, jakým útočníci pracovali, protože ten změnit je těžší než změnit konkrétní nástroje. Dále se vychází z komunikační infrastruktury, kterou použili pro doručení útočných nástrojů na místo a pro řízení a kontrolu útoku. Za třetí se vychází z vlastností použitého malware, za čtvrté z úmyslu za útokem, za páté z údajů a hypotéz poskytnutých dalšími zdroji. Teprve když jsme si dostatečně jisti více takovými faktory dohromady, můžeme říci, že za útokem stojí nějaký hráč, např. Severní Korea za WannaCry, a podle toho dále postupovat. Problematiku stručně shrnuje tento článek na stránkách amerického Office of the Director of National Intelligence.

Jak se chránit

Na závěr trochu o tom, jak se lze bránit na úrovni jednotlivců. Konkrétních technických řešení je mnoho, zde se soustředíme spíše na principy, jak se chránit.

Zálohovat, zálohovat, zálohovat. Stará rada, která pomáhá jak proti riziku selhání nebo ztráty systému (např. notebooku), tak proti zničení či poškození dat např. ransomwarem.

- Především vůbec nějak a alespoň občas zálohovat. Půl roku stará záloha třeba kontaktů, mailů nebo účetnictví je sice hodně nedostatečná, ale pořád lepší než vůbec žádná záloha.
- Identifikovat data, která jsou naprosto nezbytná, která je dobré mít a o která můžete přijít. Podle toho je zálohovat.
    - Naprosto nezbytná data jsou třeba kontakty, důležité dokumenty, účetnictví, rozdělaná práce nebo datové soubory správce hesel. Ty budete chtít zálohovat často a zároveň jich nejspíš není moc. Hotovou práci pak můžete třeba vypálit na 2 DVD, každé dát jinam a nemusíte ji zálohovat znovu, dokud se nezmění.
    - Data, která je dobré mít, ale nejsou nezbytná. Není to nějaká jedna jasně vymezená skupina, spíš široká oblast různé důležitosti.
    - Data, o která můžete přijít. Raději si místo nich vyhraďte místo a čas na důležitá data. Mezi tisíci fotek, které jsem pořídil, je pár desítek fakt super fotek a pár stovek vzpomínek, o které bych nerad přišel. Ty zálohuji pravidelně. Pak je pár set celkem dobrých fotek, a pak spousta průměrných. Ty sice také zálohuji, protože místo zatím je, ale velký význam nemají. Nakonec je určité množství dalších fotek, které jsem měl už dávno smazat, protože jen zabírají místo. Třeba jsem si mobilem vyfotil program kina, abych se k němu mohl snadno vrátit – ale dva roky poté jen zabírá místo. Rozostřená letící kachna není žádný unikát, který by měl cenu i v tomto stavu.
- Zálohovat pravidelně, mít několik posledních záloh a vědět, kde je mám. Ransomware apod. se často nějakou dobu skrývají. Je vám k ničemu, pokud máte zálohované již zašifrované soubory, potřebujete zálohu z doby před zašifrováním dat. Takže důležitá data zálohovat třeba denně.
- Zálohovat tak, aby data nešla přepsat – např. vypálené DVD. Záloha na disku je k ničemu, pokud ji ransomware přepsal spolu s daty nebo pokud selhání či ztráta disku zničila data i zálohu.
- Od každé zálohy mít dvě kopie na dvou různých místech. Dvě kopie, protože médium může selhat, nepůjde přečíst apod. Na dvou různých, fyzicky oddělených místech, protože na jednom místě ji někdo může ukrást, může shořet apod.
- Zálohu mít šifrovanou vám známým heslem. Zálohovat data na USB klíčenku je fajn, ale pokud z ní zloděj může všechno přečíst, není to to pravé.
- Existuje řada způsobů, jak tohle vše technicky provést.

Dvoufaktorová autentizace, silná hesla, různá hesla, ověřování si např. příkazů k platbě.
Dvoufaktorová autentizace znamená, že nestačí jen znát heslo, musíte ještě něco mít – např. mobil, na který vám přijde autentizační smska, nebo generátor nějakého klíče. To podstatně zvyšuje bezpečnost, protože i když útočník získá heslo, pořád se musí dostat k té fyzické věci nebo z vás autentizační kód nějak vylákat (pozor, i to se děje!). Mohli bychom sem zařadit i zpětné ověřování si různých příkazů, třeba mailů k urgentnímu zaplacení platby. Zkuste šéfovi zavolat a zeptat se, zda to skutečně poslal on.

Silná hesla znamenají něco, co se nedá uhádnout (takže ne jméno matky za svobodna, jméno dítěte, datum narození apod.).

Různými hesly myslím, že pro různé služby používáte různá hesla. Jiné heslo pro soukromý email, jiné pro pracovní email, jiné pro internetové bankovnictví vaše, ještě jiné pro firemní bankovnictví atd. Kdyby nic jiného, tak alespoň tahle čtyři hesla by měla být každé jiné a neměli byste je používat pro žádnou další službu. Když totiž někdo získá heslo třeba k vašemu soukromému mailu, pořád se nebude moci nabourat do firemního mailu a už vůbec ne do banky. A co když heslo zapomenete? Je daleko lepší chodit zbytečně do banky, protože jste zapomněli heslo, než chodit zbytečně na policii, protože vám vykradli účet. Spousta služeb je zabezpečená daleko hůř než bankovnictví a maily. Byl jsem v šoku, když mi nejmenovaný internetový obchod při každé objednávce připomněl mailem mé heslo. Znamená to, že ho museli mít uložené, být schopní ho získat a kdokoliv si ho mohl přečíst cestou. Představte si, že bych ho používal i pro bankovnictví.

Bezpečná hesla jsou ideálně náhodné kombinace písmen, číslic a speciálních znaků, dlouhé dnes alespoň 15 znaků. Jak si je máte pamatovat? Svěřit to počítači, speciálnímu programu, který se nazývá správce hesel. Existuje jich více, někdy jsou i součástí balíčků antivirových programů. Vy zadáváte jen jedno heslo, program si ale pamatuje libovolné množství dalších hesel i adresy služeb, pro které je používáte. Takže pokud například navštívíte email, dokáže vyplnit správné heslo. Program tato hesla ukládá v šifrované podobě, bez zadání hlavního hesla je nejde přečíst. Pro hlavní heslo opět platí, že by nemělo být triviální, snadno získatelné nebo uhodnutelné. Může to být nějaká náhodná fráze, kterou si vymyslíte a která se lépe pamatuje – ne oblíbený citát z knihy, ale delší fráze, která vůbec nemusí dávat smysl.

Změnit výchozí nastavení. Když si přinesete nové zařízení, například internetový modem, tiskárnu, IP kameru, mobil, … tak změnit výchozí nastavení. Určitě změnit výchozí hesla a vypnout nepotřebné služby. Ideálně nechat konfiguraci odborníkovi.

Používat legální, výrobcem podporovaný software a pravidelně ho aktualizovat. Software obsahuje chyby, z nichž některé mohou být zneužity útočníky. Pokud je taková chyba nalezena, výrobce obvykle vydá záplatu, která ji opraví. Pokud si ji však uživatel nenainstaluje, počítač nebo jiné zařízení zůstává nechráněný. Světem se dodnes šíří škodlivé kódy, které zneužívají dávno opravené chyby. Podobně některé velké útoky byly vedené přes dávno záplatované zranitelnosti. Bohužel řada uživatelů ty záplaty neinstalovala, nebo používají zastaralé a výrobci již nepodporované systémy, pro které záplata není k dispozici.

- Ve Windows 10 se záplaty operačního systému ve výchozím nastavení stahují a instalují automaticky. Existuje ovšem řada verzí Windows 10, označených rokem a měsícem, např. 1803. Ne všechny jsou stále podporovány. Ke 3. září 2020, kdy tento text píšu, jsou podporovány jen verze 1809 a novější. Windows XP, Windows 7 ani jiné starší verze Windows už nejsou podporované a záplaty pro ně Microsoft nevydává.
- Při aktualizaci Windows se může aktualizovat i Microsoft Office, je-li to nastaveno. Ke 3. září 2020 jsou podporované jen Office 2013, 2016 a 2019, starší verze už ne.
- Bohužel to nejsou jediné záplaty, které potřebujete. Záplatovat potřebují také webové prohlížeče třetích stran (Chrome, Firefox apod.), Skype, Adobe Acrobat Reader a řada dalších aplikací, speciálně pak Java, pokud ji z nějakého důvodu máte instalovanou. Chrome, Firefox, Adobe Reader i poslední verze Javy se také normálně aktualizují samy.

- Aktualizace se týká i bezpečnostního softwaru (antivirů apod.). Ty se většinou aktualizují samy, a to i několikrát denně. Vzhledem k extrémně rychlému vývoji malwaru rozhodně nestačí mít instalovanou nějakou starou verzi, je opravdu nutné mít verzi aktuální a podporovanou výrobcem.
- Záplatování je potřeba také u mobilních telefonů, tabletů, modemů, k internetu připojených tiskáren atd. Vzhledem k široké škále těchto zařízení tu nejde stručně uvést návod.

Vypnout nepotřebné služby. Řadu služeb nepoužíváte nebo používáte jen někdy. Vypnutí takových služeb omezí prostor, přes který se někdo může do zařízení nebo sítě nabourat, a množství informací, které může získat. Plus vám dále vydrží baterie. Chcete, aby se váš mobil připojoval automaticky k jakékoliv veřejné wifi síti, protože tím možná ušetříte trochu těch mobilních dat, ale můžete si být skoro jistí odposlechem dat? Potřebujete v notebooku zapnuté sdílení souborů, obzvlášť když jste na cizí wifi síti? Potřebujete zapnuté GPS v mobilu pořád, nebo jen když zrovna jdete podle mapy? Potřebujete Bluetooth stále zapnutý, viditelný pro okolí a hledající okolní zařízení, nebo ho potřebujete jen tu a tam a stačí ho zapnout jen na potřebnou dobu?

Přemýšlet o tom, co instaluji a zda to vůbec potřebuji. Existuje spousta zbytečného softwaru, některý je dokonce přímo předinstalován výrobci zařízení. Jen zvyšuje prostor pro napadení. Speciálně u mobilních aplikací se pak podívat na požadovaná oprávnění. Je překvapivé, kolik oprávnění chtějí banální aplikace. Proč potřebují mnohé aplikace na zvýšení výkonu baterky (typické lákadlo) přístup ke kontaktům, identitě, historii volání? Proč potřebují stejný přístup mnohé šachové programy, sudoku, proč je po mě chtěly ručičkové hodiny, které jsem si nakonec nenainstaloval? Protože vy jste ten produkt. Vyplatí se zkontrolovat požadavky a pokud jsou přehnané, hledat dál a najít aplikaci, která taková zbytečná oprávnění nechce.

Nesdílet, nedělat to, co nechci, aby někdo zaznamenal, nebo to dělat mimo dosah počítače a mobilu.

Nesdílet intimní fotky atd. Zakrýt webkameru. Sebelepší útočník nemá šanci získat intimní fotky, když mobil leží ve vedlejší místnosti, je v neprůhledném pouzdře nebo je webkamera překrytá kouskem neprůhledné izolepy.

Nesdílet svoji polohu. Nesdílet fotky dětí, speciálně ne v nějakých roztomilých pozicích. Nesdílet informace typu „příští týden všichni jedeme k moři“ – a tedy byt bude prázdný a bez kontroly.

Když už něco sdílíte, ověřte si, co sdílíte a s kým. Nemáte náhodou nastavenou veřejnou dostupnost vašich příspěvků na sociální sítě? Opravdu znáte lidi, se kterými se přátelíte na sociálních sítích? A jak moc můžete věřit přátelům přátel?