Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j.: 537/2019-NÚKIB-E/210 Brno 22. března 2019

Věc: Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane xxxxxxxxxx,
Národní Úřad pro kybernetickou a informační bezpečnost(dále jen „**Úřad**“) obdržel dne 5.2.2019 Vaši žádost z téhož dne podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. V žádosti požadujete poskytnutí informací týkajících se počtu útoků ransomware, dalších informací k problematice ransomware (zejména o obraně, prevenci a možnosti odstranění závadného stavu), případně statistiku o kybernetické kriminalitě na území ČR. V odpověď na Vaši žádost Vám sděluji následující informace:

1. Statistická data kybernetických incidentů ve struktuře evidované Úřadem, vztahující se k subjektům povinným podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), naleznete ve zveřejněných Zprávách o stavu kybernetické bezpečnosti za uplynulé roky, dostupné na internetových stránkách Úřadu v kapitole „Publikace“ (https://www.nukib.cz/cs/informacni-servis/publikace/). Konkrétně se jedná o:
    a. Kapitola 5.2 Zprávy o stavu kybernetické bezpečnosti za rok 2013
    b. Kapitola 8.3. Zprávy o stavu kybernetické bezpečnosti za rok 2014
    c. Příloha č. 2 Zprávy o stavu kybernetické bezpečnosti za rok 2015
    d. Kapitola 7.2 Zprávy o stavu kybernetické bezpečnosti za rok 2016
    e. Příloha č. 2 Zprávy o stavu kybernetické bezpečnosti za rok 2017

    Úřad ransomware incidenty ve smyslu použité kategorizace eviduje jako „Škodlivý obsah“. Podrobnější rozlišení jednotlivých kategorií Úřad neeviduje.
2. Problematice ransomware v obecné rovině se věnuje rovněž Základní kurz kybernetické bezpečnosti vytvořený Úřadem pro zaměstnance státní správy v kapitole č. 8. Kurz přikládám jako přílohu tohoto sdělení.
3. Statistikami ohledně kybernetické kriminality na území České republiky Úřad ve své působnosti nedisponuje a doporučuji se tak v této věci obrátit na Policii ČR.

S pozdravem

Národní úřad pro kybernetickou a informační bezpečnost

Digitálně podepsal Mgr. Otakar Horák
Datum: 2019.03.22 16:55:56 +1'00'

v z. Mgr. Otakar Horák

Mgr. Pavel Král
ředitel odboru právního

Příloha:

Základní kurz kybernetické bezpečnosti

Obdrží:

xxxxxxxxxx, e-mailem

ZÁKLADNÍ KURZ KYBERNETICKÉ BEZPEČNOSTI

Obsah

Kapitola 1: FYZICKÁ BEZPEČNOST

V první kapitole se budeme věnovat tématu fyzické bezpečnosti, která je základním prvkem kybernetické bezpečnosti a seznámí vás s pravidly, bez kterých se nelze bezpečně pohybovat v kyberprostoru.

Než si otevřete první přednášku, je nezbytné znát následující základní pojmy, které se v obsahu kapitoly vyskytují. Pokud si některým z nich nejste jisti, využijte odkaz na náš "Slovník kybernetické bezpečnosti", kde je všechny najdete. Na jednotlivé položky se dostanete tak, že na ně kliknete v níže uvedeném seznamu.

DNS server	Kybernetické riziko
HTTP/HTTPS protokol Internet IP adresa	Kybernetický incident Kybernetický útok Kyberprostor
Kybernetická hrozba	Zranitelnost

Pracovní místo a jeho úprava

Jak ke kybernetické bezpečnosti přispívá uklizený stůl? Ačkoliv se na první pohled může zdát, že fyzická bezpečnost tolik nesouvisí s bezpečností kybernetickou, opak je pravdou. Proto dodržujte následující zásady a rady:

- Hesla nepatří na papírky a už vůbec nesmí být viditelně vyvěšena.
  Vymyslete si unikátní heslo, které si budete pamatovat. Tvorbě hesel se budeme podrobně věnovat v kapitole č. 7 – Autentizace.
- Přihlašovací údaje se nikdy nesdělují ani „nepůjčují".
  Ani přátelům, kolegům apod.
- Nenechávejte své dokumenty volně přístupné.
  I poznámky a rozpracované dokumenty mohou obsahovat citlivé informace.
- Omezte přístup dalších osob k vašim soukromým i pracovním zařízením.
  Tedy počítači, telefonu, tiskárně a dalším.
- Při každém odchodu z kanceláře zamykejte obrazovky svých zařízení. Zamknutím obrazovky o rozdělanou práci nepřijdete. Nejjednodušší způsob rychlého zamknutí je zkratka WIN + L.
- V kanceláři nenechávejte bez dozoru cizí osoby a při odchodu vždy zamykejte.
  Z pohledu bezpečnosti a ochrany soukromí byste se ke své kanceláři měli chovat stejně, jako ke svému domu.
- Buďte ostražití vůči okolí a zejména vůči neznámým osobám v objektu.
  Pokud v práci na chodbě potkáte neznámého člověka bez viditelně nošené identifikační karty a bez doprovodu, vždy se ho zeptejte, koho hledá a co potřebuje.

PŘÍKLAD – Odezírání hesel z klávesnice a čtení z displeje

Existují osoby, pro které je odezírání hesel či čtení z displeje zábavou nebo dokonce technikou k pozdějšímu útoku. Pro tuto činnost se vžil vlastní termín „**shoulder surfing**". Každému z nás asi hned dojde, že jde o trochu závažnější činnost, než je pouhé čtení novin přes rameno v hromadném dopravním prostředku. Avšak i to je nám nepříjemné a zpravidla, jakmile si toho všimneme, tak dotyčnému zvědavci jeho zábavu znemožníme.

Byť bez nekalých úmyslů, geniálními shoulder surfery PINů a hesel mobilních zařízení jsou bezesporu malé děti včetně batolat. Aniž často ještě umí číst a psát, mají excelentní postřeh i vizuální paměť a zpravidla již vyvinutou jemnou motoriku. Zadat odkoukaný PIN, či heslo a odemknout si bezprizorní zařízení pro ně tedy není žádný problém. I takový návštěvník, byť je nám v životě drahý, nám může v našem počítači nebo mobilu udělat pěkný nepořádek. Děti rády mažou, píší i volají a asi se shodneme na tom, že jsou situace, kdy se nám to nehodí. Ne každý šéf má pro něco takového pochopení, a to zcela oprávněně.

PŘÍKLAD – Zamykání obrazovek

Zamknutí obrazovky je záležitostí několika sekund, navíc vás v práci nijak neomezuje. Po zamknutí obrazovky se vám rozdělaná práce nepřeruší. Stejně tak při práci v internetovém prohlížeči zůstanou všechny otevřené panely ve stavu, jak jste je ponechali.

Pokud je pro vás požádání kolegy o pohlídaní vašeho zařízení stále jednodušší způsob než stisknout klávesové zkratky: WIN + L. Měli byste si uvědomit, kolik citlivých informací (hesla, kontakty, osobní SMS zprávy a e-maily, kopie důležitých dokumentů, osobní fotografie a další důvěrné informace) ve svých zařízeních dnes uchováváte. Ukázali byste je dobrovolně i cizím osobám?

Podobně jako počítače dnes mají funkci zamknutí obrazovky i ostatní mobilní zařízení. V případě mobilních telefonů se nejčastěji používají PINy, gesta či otisky prstů. PINy bychom měli volit dostatečně dlouhé (většinou se nabízí 4místné či 6místné kombinace), nicméně čísla by nás neměla nijak vystihovat (v opačném případě by mohla být snáze odhadnuta).

Dokumenty a nosiče informací

Jak přistupovat k informací v tištěné podobě i v elektronické podobě a k jejich nosičům:

- Souborové adresáře identifikující místa a osoby nesmíme zpřístupnit neoprávněným osobám.
- Vytištěné citlivé dokumenty ihned odebíráme z tiskárny, nepotřebné tištěné dokumenty skartujeme.
  Na odchodu tiskárnu zkontrolujeme, abychom měli jistotu, že se tisk skutečně dokončil.
- Nosiče informací jako jsou například USB flash disky, nenecháme v jednací místnosti, šatně, kuchyňce ani jiných společných prostorách, a to ani, když jsou prázdné.

Čtení přes rameno

Na displej notebooků a dalších přenosných zařízení, zvláště pokud na nich pracujete na veřejných místech, lze aplikovat speciální folii nepropouštějící světlo vyjma pohledu zepředu pod kolmým úhlem. Při pohledu ze strany pak displej vypadá vypnutý a nelze odečítat přes rameno.

Kapitola 2: BĚŽNÁ ZAŘÍZENÍ

V této kapitole se podíváme na rizika, se kterými se setkáváme při používání počítačů a dalších elektronických zařízení a samozřejmě i na opatření, která nám pomohou těmto rizikům předcházet, a úspěšně čelit hrozbám.

RIZIKA POUŽÍVÁNÍ ICT ZAŘÍZENÍ

Doporučení pro ochranu dat

Stejně jako vynakládáte nemalé úsilí zabezpečení svých zařízení věnujte svou pozornost i zabezpečení dat, která jsou obvykle cennější. Koupit nové zařízení je relativně snadné, ale data jako pracovní dokumenty nebo rodinné fotky jsou často nenahraditelná, proto využijte následujících rad:

- **Chraňte přístupy heslem.**
  Kdekoli používáte nějaký uživatelský účet, vyžadujte k němu i heslo.
- **Oddělte privilegovaný účet.**
  Správcovský účet, kterým lze měnit konfiguraci celého zařízení, nepoužívejte pro běžnou práci.
- **Aktualizujte software.**
  Zajistíte tím opravu známých zranitelností a vylepšíte jeho stabilitu.
- **Používejte bezpečnostní software.**
  Firewall vás ochrání před útoky ze sítě, a antivirus před známými druhy malwaru.
- **Zamykejte obrazovku.**
  Kdykoli se vzdalujete od počítače, i když je to jen na pár minut.
- **Vypínejte Wi-Fi, Bluetooth a další bezdrátová rozhraní.**
  Pro útočníka představují potenciální cestu do vašeho systému. Zapínejte je jen, když je potřebujete.
- **Šifrujte úložiště.**
  Šifrování úložiště zajistí, že data budou nečitelná pro kohokoli, kdo nezná vaše heslo.
- **Zálohujte data na jiném úložišti.**
  Využít můžete například externí disk, cloud apod. Vnímejte rizika společná pro primární data i zálohu: například při vykradení bytu bude váš externí disk pravděpodobně odcizen spolu s počítačem.
- **Nepřipojujte neznámá zařízení.**
  Mohou být poškozena nebo obsahovat malware a díky tomu poškodit i vaše zařízení.

Pracovní cesta na konferenci

Představte si, že jste vysláni na pracovní cestu na zahraniční konferenci. Přepravujete se letecky a na místě strávíte dvě noci v hotelu. Ročně se na podobný výlet vydávají tisíce lidí, takže co by zrovna vám mohlo hrozit? Přestože naprosté většině cestujících se nepřihodí nic špatného, ohrožení zde rozhodně existují.

Při čekání na letišti používáte svůj laptop či tablet a mnoho lidí a kamer sleduje vaše přihlášení. Stejní lidé mohou vidět a nahrávat vše, co si na displeji prohlížíte. Použijete-li letištní bezdrátovou síť, je váš počítač v přímém dosahu ostatních zařízení využívajících stejnou síť, které jej mohou napadat. Při přepravě může v důsledku neopatrného zacházení se zavazadly dojít k mechanickému poškození nebo zničení vašeho zařízení.

V hotelovém pokoji může dojít k odcizení vašich zařízení. Pravděpodobně budete hotelem odškodněni, nicméně data ze zařízení jsou pro vás ztracena. Další ohrožení číhají na samotné konferenci. Máme tady mnoho dalších přihlášení a další spoustu lidí, kteří vidí váš displej. Většina lidí také nechává svá zařízení bez dohledu, když odchází pro kávu nebo na toaletu.

Snad jste v nastíněných situacích rozpoznali velmi reálná nebezpečí. Přestože riziko pro většinu lidí není vysoké, rozhodně není zanedbatelné a jsme mu vystavování téměř každodenně. Je tedy otázkou času, kdy se nějaký problém bude týkat i vás.

Internet věcí

Internet věcí (IoT) je síť propojených zařízení, jež v sobě mají zabudovaný procesor, software, senzory a síťovou konektivitu, které jim umožňují sběr, zpracování a sdílení dat. Co si pod těmito pojmy představit? Může jít o chytré televize, moderní auta, webkamery, drony, chytré hodinky, virtuální asistenty, ledničky, systémy chytrého vytápění domu, dětské chůvičky a další techniku s připojením k Internetu.

S IoT však souvisí dobře známé i nové hrozby:

- Útočníci mohou napadnout naše zařízení a zcizit naše data.
- Zařízení může napadnout malware s cílem zneužít ho k dalším útokům.
- Útočník může zařízení vyřadit z provozu a požadovat výkupné. Například v případě inteligentního vytápění domu to může být skutečný problém.

Internet věcí

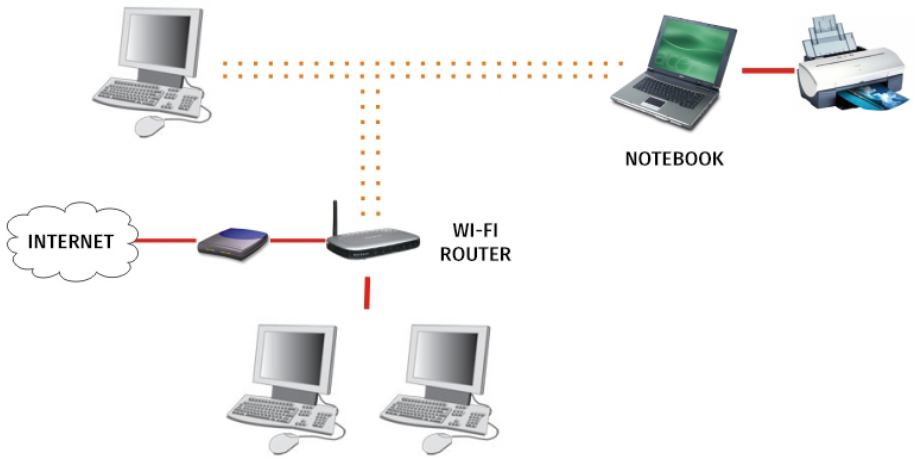
Zařízení, která pracují s IoT jsou stále populárnější a značně nám ulehčují život, ale jejich používání s sebou nese bezpečnostní rizika. Proto je nutné dobře zvážit, co do naší domácí sítě zapojujeme. O tomto stále se rozšiřujícím trendu pojednává jednoduchým a netechnickým jazykem níže přiložené video.

https://youtu.be/0OZhms7lR9U

Wi-Fi

WI-FI je technologie, která slouží k bezdrátovému přenosu informací.

Wi-Fi usnadnila vznik internetu věcí a mohou ji využívat rozličná zařízení od stolních počítačů po tiskárny. **Wi-Fi nemusí být nutně spojena s Internetem, může zajišťovat třeba jen bezdrátovou komunikaci mezi počítačem a tiskárnou.** Její rizika pro běžné uživatele jsou ale většinou spojena právě s Internetem. Nyní si řekneme, na co si dávat pozor jako uživatel.



Veřejné Wi-Fi

V dnešní době mají vlastní Wi-Fi síť rozličné instituce od kaváren po letiště. Pokud tyto sítě použijeme a necháme skrze ně putovat svá data, svým způsobem vkládáme důvěru do jejich provozovatele.

Bezpečnostní rady pro používání Wi-Fi

- **Pro bezpečné připojení doporučujeme používat VPN, neboli Virtual Private Network.** Tato virtuální privátní síť Vám díky šifrované komunikaci umožní bezpečně fungovat i s využitím nedůvěryhodné Wi-Fi. Zejména u firem a úřadů je používání VPN velmi elegantním řešením pro zaměstnance, kteří jsou často mimo kancelář či úřadují například z letištní haly, nádraží nebo hotelu.
- **Kdykoliv Wi-Fi nepoužíváte, vypněte ji.** Budete tak mít jistotu, že se zařízení bez vašeho vědomí nepřipojí k síti.
- **Je-li to možné, vyhněte se používání otevřených (lze se k nim přihlásit bez zadání hesla) či veřejných (heslo je volně přístupné komukoli) Wi-Fi sítí.** Wi-Fi se slabým jednoduchým heslem je stejně nebezpečná jako obě předchozí.
- **Kontrolujte názvy Wi-Fi sítí, k nimž se připojujete.** Měli byste vědět, kdo je provozuje, a nepřipojovat se k náhodným sítím v nabídce.
- **Když už využijete veřejnou síť, měli byste ji po použití smazat a nejlépe ji vůbec neukládat.** Zamezíte tak situaci, kdy útočník vytvoří Wi-Fi síť se stejným názvem, přiblíží se k nám a využije toho, že se k ní vaše zařízení automaticky připojí.

Webová kamera

- Webkamera je dnes běžnou součástí počítačů a chytrých telefonů a slouží především ke zprostředkování videohovorů. **Bohužel existují typy malware, pomocí nichž lze kameru na dálku spustit a natáčet s ní video nebo pořizovat snímky.** Některé kamery mají světelnou diodu, která svítí, pokud je kamera činná. Útočníci ale umí tuto diodu vypnout, takže se na ni není možné spolehnout.
- Že jde o vážné a reálné nebezpečí, potvrdil i ředitel americké FBI, který v roce 2016 veřejně prohlásil, že on sám si kameru vždy zakrývá a je to vyžadováno i v amerických veřejných institucích. Nutno poznamenat, že obdobně zneužitelná je i kamera, fotoaparát a mikrofon v chytrém telefonu.

Rozšiřující materiály – Ředitel FBI radí: Zakryjte si webkameru na počítači, mohou vás sledovat.

https://www.zive.cz/bleskovky/reditel-fbi-radi-zakryjte-si-webkameru-na-pocitaci-mohou-vas-sledovat/sc-4-a-184258/default.aspx

PŘÍKLAD – Malware a webkamera

V roce 2014 bylo v USA zatčeno 100 lidí v souvislosti s malware Blackshades. Šlo o trojského koně, jenž vykonával mnoho škodlivých aktivit. Mezi ně se řadilo i „špehování“ obětí prostřednictvím webových kamer. Tento nástroj bylo možné zakoupit za několik desítek až stovek dolarů. Pořídilo si ho odhadem několik tisíc uživatelů a infikováno bylo přes půl milionu počítačů. Samozřejmě nejde o jediný malware, který cílí na webkamery.

Jak zabezpečit webkameru?

- Nikdo z nás určitě nechce, aby se potenciální útočník naboural do našeho soukromí. Jakou ochranu v případě webové kamery zvolit? Řešení je několik. Pokud vlastníte externí webovou kameru, stačí ji vypojit z počítače. V případě kamery integrované přímo do zařízení je nutné ji zakrýt buď lepicí páskou nebo speciální krytkou.
- **Zakrývání webkamery není paranoidním jednáním, ale odůvodněným opatřením, kterým chráníme své soukromí.**

Webkamera zakrytá speciální krytkou.

Webkamera zakrytá speciální nálepkou.

Webkamera zakrytá speciální krytkou, která umožňuje kameru v případě nevyužívání zakrýt.

Shrnutí

Ochrana vašeho soukromí na elektronických zařízeních spočívá především v ochraně přístupu. K tomu používáme především heslo pro všechny naše účty. Aby byla tato ochrana opravdu účinná, je důležité se odhlašovat ze zařízení, či případně zamykat obrazovku zařízení, pokud práci na něm pouze přerušujeme a neukončujeme.

Musíme provést i opatření pro případ, kdy nebudeme mít zařízení pod svou kontrolou – mohou být odcizena nebo zničena. V případě neoprávněné manipulace se zařízením chrání naše data šifrování úložiště a pro případ zničení nebo poškození zařízení bychom měli provádět pravidelnou zálohu. Velkou hodnotu představují data na zařízení. Nahradit zařízení je snadné – data nikoli.

Kapitola 3: (NE)BEZPEČNÁ ZAŘÍZENÍ

Kapitola tři se zaměřuje především na zařízení, která pro uživatele mohou znamenat zvýšené bezpečnostní riziko v podobě nakažení škodlivým software nebo kompromitace jeho dat.

V rámci této kapitoly budou zdůrazněna rizika sdílených nebo použitých zařízení a doporučeny postupy, jak s nimi zacházet. Dozvíte se také, jaká další bezpečnostní zařízení používat k zajištění své bezpečnosti i bezpečnosti svých zařízení. V neposlední řadě budete seznámeni s jednotlivými externími zařízeními, která jsou již ze své podstaty označována za nebezpečná, a dozvíte se také, v čem jejich zákeřnost spočívá.

Použitá zařízení

Použitá zařízení mohou být pořízená v bazaru, vyřazená z firem nebo ta, která dříve používal kamarád či známý.

Rizika na straně původního majitele:

Původní majitel by měl chránit své soukromí a nenechávat na zařízení svá soukromá data. Vedle fotek a dokumentů to může například být osobní nastavení aplikací nebo jména uživatelů. **Soukromí zajistí pouze kompletní smazání úložiště a čistá instalace operačního systému**. Mějte na paměti, že nepředáváte jen fyzický stroj (hardware), ale i data na jeho úložišti.

Rizika na straně nového majitele:

Rizikem na straně nového majitele je neznámý stav software. To znamená, že nemá kontrolu nad tím, jaký software byl na zařízení nainstalován. Může to být skrytý sledovací software nebo může být zařízení nakažené malware. **Smazání a přeinstalování operačního systému by proto mělo proběhnout jak na straně předávajícího, tak na straně nového majitele.**

Sdílená zařízení

Sdílená zařízení pravidelně používá více než jeden uživatel. Rizik je hned několik. Především nemáme kontrolu nad tím, jak se chovají ostatní uživatelé. Nejjednodušším případem je sdílení zařízení v rámci skupiny, která si navzájem důvěřuje, například v rámci rodiny.

V ideálním případě mají všichni uživatelé dobré povědomí o bezpečnosti a jen nejzkušenější z nich má přístup k privilegovaném účtu, který může měnit nastavení systému a instalovat nový software. Všichni ostatní používají pouze neprivilegované uživatelské účty chráněné heslem. Při dodržení těchto pravidel může sdílené zařízení vcelku dobře a bezpečně fungovat.

Komplikace nastávají v případě, kdy zařízení používá širší skupina lidí, kteří se ani navzájem neznají. Příkladem může být počítač umístěný ve veřejné knihovně. Jediný relativně bezpečný způsob, jak takové zařízení provozovat je použití tzv. účtu host (v angličtině *„Guest account“*). Jde o jeden univerzální účet s nízkými oprávněními, který po odhlášení smaže všechna uživatelská data a nastavení.

Ujistěte se, že se předchozí návštěvník odhlásil a vy používáte *„čistý“* účet hosta. Nezapomeňte se také po skončení práce sami odhlásit. I přes tato opatření bychom měli takto sdílená zařízení považovat za nedůvěryhodná a neprovádět na nich žádné citlivé úkony jako přihlašování do internetového bankovnictví.

USB & Malware

Jde o USB flash paměť obsahující speciální soubory, které na nezabezpečeném systému okamžitě po připojení spustí škodlivý kód (viz kapitola č. 10 – Škodlivý software). Povaha škodlivého kódu může být různorodá – od mazání dat až po podrobné mapování činnosti uživatele.

Keylogger

Termín *„keylogger“* je odvozen ze spojení slov *„key“* - klíč nebo klávesa, a *„log“* - zaznamenat. **Keylogger je tedy nástroj na zaznamenávání stisků kláves a může mít jak fyzickou, tak softwarovou podobu.** Fyzický keylogger vyobrazený níže lze nenápadně zapojit mezi kabel klávesnice a samotný počítač. Následně zaznamená všechny stisky kláves na dané klávesnici, což v důsledku znamená, že útočník zná naší kompletní komunikaci na sociálních sítích a e-mailu, ale hlavně veškerá uživatelská jména a hesla do našich e-mailových schránek, internetového bankovnictví nebo sociálních sítí, do kterých může posléze nahlížet a dokonce měnit jejich obsah.

V nejlepším případě nám útočník *„pouze“* změní přístupová oprávnění a my už se nedostaneme ke svým účtům. Horší případy zahrnují sociální inženýrství, krádež identity nebo manipulaci s bankovním účtem a další druhy kybernetické kriminality. Připomínáme kapitolu č. 2 – Fyzická bezpečnost. I kvůli keyloggerům je důležité zamykat za sebou dveře a hlídat si svá zařízení. Skutečně málokdo po návratu do otevřené kanceláře kontroluje kabeláž. I kdyby, jen málo z nás by keylogger našlo a rozpoznalo.

Příklad fyzického keylogeru

PŘÍKLAD – Keylogger

Abychom demonstrovali, že použití keyloggeru není jen záležitostí sci-fi, uvádíme případ muže ze Západní Virginie, který se rozhodl řešit manželskou krizi velmi nestandardním způsobem. Ze strachu, že jej manželka podvádí, se rozhodl ověřit její věrnost za pomoci keyloggeru, který připojil k jejímu pracovnímu notebooku. Situace byla o to vážnější, že manželka tohoto muže pracovala jako zaměstnankyně okresního soudu a její počítač tedy obsahoval citlivé pracovní informace. Díky polehčujícím osobním okolnostem muž vyvázl pouze s dvouletou podmínkou a pokutou 1000 dolarů.

Rozšiřující materiály – Cop installs keylogger on his wife's sensitive work computer, gets probation. Does the punishment fit the crime?

https://nakedsecurity.sophos.com/2014/01/07/cop-installs-keylogger-on-his-wifes-sensitive-work-computer-gets-probation-does-the-punishment-fit-the-crime/

Killer USB

Toto zařízení (v překladu „zabijácké" USB) je na první pohled neodlišitelné od klasické USB flash paměti. **Uvnitř však není úložiště dat, ale řada kondenzátorů, které se během velmi krátké doby nabijí z USB portu počítače a následně energii opačným směrem uvolní v jediném silném impulsu.** Dochází k poškození obvodů v počítači a zničení jeho vnitřních komponent Kdo by takové zařízení mohl použít a proč? Propuštěný zaměstnanec, zákeřný kolega, zhrzený partner jako pomstu? Nebo zkrátka kdokoli jiný a úplně jen tak – ze zvědavosti, zda to „opravdu funguje" a co se stane?

What is a USB Killer ? Why They Use It?

https://youtu.be/pstHYmlZM9I

Další nebezpečná zařízení

- **ROGUE USB ACCESS POINT** - záškodnický přístupový bod do USB. Místo paměti je však na zařízení umístěn adaptér bezdrátové sítě, který dovolí útočníkovi bezdrátové připojení a otevře tak prostor k útoku na váš počítač.
- **KEYSNIFFER** - jedná se o výkonný USB Wi-Fi modul, který zachycuje stisknuté znaky na některých modelech bezdrátových klávesnic a myší.

Doporučení

Námi uvedená zařízení zahrnují opravdu jen ty nejčastější příklady, s nimiž se můžeme setkat. Nebezpečné zařízení však může být téměř cokoli a motivovaní útočníci umí být velmi vynalézaví. Proto je z našeho pohledu dobré držet následujících doporučení:

- **Pro ověření, zda konkrétní externí USB nosič neobsahuje malware, používejte tzv. *„pračku".***
  Jedná se o samostatný počítač oddělený od sítě, který obsahuje pouze aktuální antivirový software.
- **Blokujte připojení výměnných zařízení nebo zápis na připojená zařízení.**
  V případě vložení zakázaného zařízení pak dojde k jeho blokaci, nebo k pouhému čtení dat bez možnosti zápisu.
- **Možností je i nasazení DLP (Data Loss Prevention) systémů schopných zamezit úniku citlivých dat.**
  V rámci těchto systémů se nadefinují pravidla pro citlivá data (např. vybraná složka je tajná) a na ně se uplatní zvláštní omezení

Kapitola 4: BEZPEČNOSTNÍ SOFTWARE

Čtvrtá kapitola se zaměřuje na bezpečnostní software a vysvětluje, proč je pro uživatele důležitý. Vedle antiviru, firewallu a HIDS/HIPS se věnuje šifrování, programům zabraňujícím cílené reklamě a programu na digitální skartaci. Druhá část pojednává o bezpečnosti mobilních aplikací, uvádí jejich rizika a poskytuje doporučení, jak jejich bezpečnost udržovat.

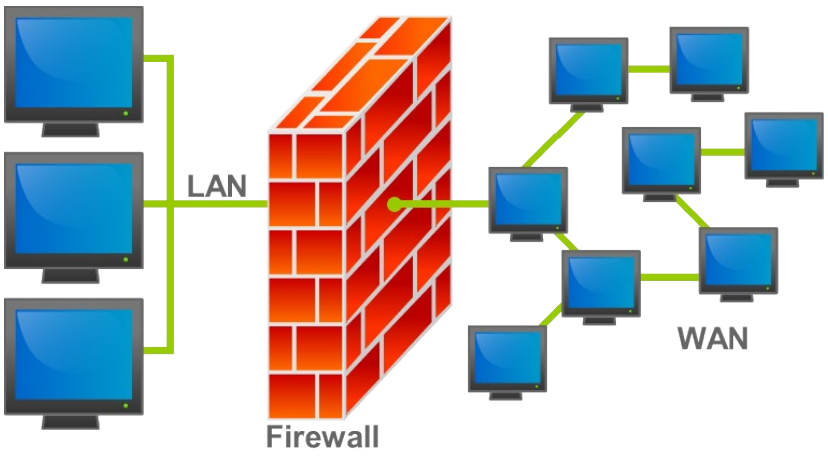
Bezpečnostní software

Bezpečnostní software je označení programu, jehož primárním účelem je zajištění bezpečnosti vašeho systému. Protože je však bezpečnost systému komplexní záležitost, jediný program ji nemůže obsáhnout. Proto se používá celá řada různých programů, které řeší rozdílné aspekty bezpečnosti.

Jedním ze základních programů zaměřených proti malware je antivirus, který funguje mimo jiné na principu rozpoznávání signatur známých virů (více o Malware v kapitole č. 10).

Firewall

Firewall na základě stanovených pravidel chrání systém před útoky z vnější sítě. Lze si jej představit jako ochrannou zeď:



LAN - zkratka anglických slov Local Area Network, česky lokální síť. Je to síť menšího rozsahu, zajišťující propojení menšího množství počítačů. Například v jedné domácnosti, na jednom ministerstvu či v jedné firmě.

WAN - zkratka anglických slov Wide Area Network, česky rozsáhlá síť. Je to geograficky rozsáhlá síť, zajišťující propojení počítačů. Pokrývá rozsáhlejší území, typicky větší než město. Příkladem může být Internet.

Šifrovací program

Jeho účelem je umožnit uživateli snadné šifrování souborů nebo celých úložišť pro zajištění důvěrnosti dat.

Správce hesel

Jednoduchá aplikace, která uchovává uživatelská hesla do ostatních služeb. Bezpečnost uložení je zajištěna šifrováním databáze hesel. Typicky obsahuje i doplňkové funkce jako generování bezpečných hesel nebo připomínání nutnosti změnit heslo po určité době (viz kapitola Autentizace).

Digitální skartovačka

Pouhé "smazání" dat umožňuje jejich obnovu a to i tehdy, když jste vysypali koš. Proto je nutné používat program, který bezpečně odstraňuje citlivá data. Místo pouhého přesunutí do koše s možností zpětného obnovení je zvolený soubor důkladně odstraněn a přepsán bez možnosti obnovení.

AdBlock

AdBlock je rozšíření webového prohlížeče. Program blokující zobrazování cílených reklam a sledování aktivit uživatele na webu, typicky ve formě doplňku pro webový prohlížeč. Podílí se na ochraně soukromí uživatele.

Host-based Intrusion Detection System, Host-based Intrusion Protection System

HIDS je softwarové řešení, které slouží k detekci nežádoucí komunikace z a do internetu. **HIPS** bývá označována jako novější verze HIDS. Oba systémy pozorují chování ostatních programů a varují uživatele, pokud některý z nich provádí podezřelé akce. Například může jít o zásah do chráněných systémových složek nebo otevření nového síťového spojení. Uživatel následně může rozhodnout, zda akci povolit či nikoli. Je tak možné odhalit i malware, který antivirus dosud nezná. Toto je však doporučeno pouze pro zkušené uživatele, kteří jsou schopni rozpoznat podezřelou aktivitu programů.

Aplikace

Aplikace, které používáme, mohou být zdrojem problémů a snižovat bezpečnost celého systému. Každá aplikace má určitá oprávnění – přistupuje k vybraným souborům, vytváří síťová spojení či mění nastavení systému. Čím vyšší oprávnění aplikace má, tím více je systém ohrožen její případnou škodlivou aktivitou. Rizika jsou zde dvojího druhu:

- **Aplikace může obsahovat zranitelnost, tedy nedokonalost ve zdrojovém kódu.** To může vést k nestandardnímu chování aplikace a pokud je zranitelnost odhalena, ke zneužití útočníkem ke škodlivé činnosti.

- **Aplikace provádí škodlivou aktivitu zcela záměrně.** Může například bez vědomí uživatele pořizovat snímky jeho obrazovky nebo odesílat soubory s citlivými daty (čísla platebních karet apod.) útočníkovi.

Doporučení pro software

- **Aktualizujte operační systém a aplikace, zajistíte tím opravu objevených chyb a zranitelností.**
  Aktualizace nahrajte co nejdříve po jejich zpřístupnění.
- **Používejte bezpečnostní software.** Základem je firewall a antivirový program, které sníží riziko zanesení škodlivého software do systému.
- **Používejte aplikace důvěryhodných vydavatelů.** Získáte dlouhodobou podporu minimálně ve formě aktualizací a výrazně snížíte riziko chyb a výskytu zranitelností.
- **Vyhněte se neoficiálním distribučním kanálům.** Získat jinak drahý software zcela zdarma stažením z Internetu je velmi lákavé. Takové aplikace však často obsahují škodlivý kód, případně mají problémy se získáním aktualizací. Takové jednání je navíc nelegální z důvodu porušení licenčních podmínek a autorského práva.
- **Odinstalujte nepotřebný software.** Každá aplikace nebo jiný software, který je ve vašem systému, může být zdrojem problémů. Pokud máte nainstalovány čtyři webové prohlížeče nebo přehrávače hudby, odeberte ty, které nepotřebujete – snížíte tím riziko pro váš systém a ještě uvolníte místo na úložišti.

Doporučení pro mobilní aplikace

- **Používejte pouze aplikace dostupné z oficiální distribuce**. Volně stažený malware se může tvářit například jako bezplatná zjednodušená verze placené aplikace nebo její vylepšení. Oficiální obchody jako Google Play nebo App Store aplikace kontrolují a ty škodlivé odmítají, i když úspěšnost kontrol není stoprocentní.
- **Kontrolujte oprávnění aplikací.** Každá aplikace si během instalace (případně používání) musí požádat o přístup k částem systému. Může to být žádost o oprávnění přístupu ke kameře, mikrofonu, kontaktům, apod. Pokud aplikace žádá o něco, co nesouvisí s její funkcí – například aplikace pro předpověď počasí žádá přístup ke kameře – je to podezřelé a oprávnění byste neměli udělit.
- **Neprovádějte zásahy do operačního systému (jailbreak, root).** Mobilní platformy přidělují samotnému uživateli nižší oprávnění. Nejvyšší oprávnění má pouze systém samotný. Oprávnění uživatele lze eskalovat, což uživateli umožní například odinstalovat výrobcem dodávané aplikace či instalovat jiné verze systému. Poruší se tím však oddělení běhu aplikací a sníží celková bezpečnost systému.

Shrnutí

- **Bezpečnostní software** chrání systém před škodlivou aktivitou aplikací a útočníků.

- **Antivirus** hledá a odstraňuje známé škodlivé programy na vašem zařízení.
- **Firewall** filtruje síťový provoz a tím snižuje riziko napadení zařízení.
- **Aplikace** mohou obsahovat zranitelnosti, které mohou být zneužity.
- **Bezpečnostní software** nezaručuje bezpečnost! Předpokladem je vždy opatrnost uživatele.

Kapitola 5: BEZPEČNOST NA INTERNETU

Pátá kapitola pojednává o bezpečném pohybu na internetu. Důraz klade na používání zabezpečeného protokolu při pohybu na webu, správu tzv. cookies a nabídne další doporučení, jak můžeme svoji internetovou komunikaci ochránit. Představí rovněž užitečnou službu Moje ID, poskytovanou sdružením CZ.NIC a uvede její výhody. Druhá část je zaměřená na sociální sítě a jejich možná rizika. Vysvětlí také pojem digitální stopa a uvede možnosti, jak ji ochránit.

Webový prohlížeč

Pokud mluvíme o používání internetu, většina z nás si představí prohlížení webových stránek. Web je však jen jednou ze služeb, které Internet poskytuje. A jak web funguje? Jde o obsah zpřístupněný pomocí komunikačního protokolu HTTP (HyperText Transfer Protocol). Na straně poskytovatele služby se tímto protokolem řídí tzv. webový server, který je naplněn webovým obsahem a tento obsah zpřístupňuje každému, kdo si o něj při dodržení pravidel protokolu řekne. Uživatel používá webový prohlížeč (Internet Explorer, Google Chrome, Mozilla Firefox a další), který komunikuje s webovým serverem a příslušná data zobrazí jako webovou stránku.

Hlavním problémem protokolu HTTP je špatné zabezpečení. Při komunikaci s webovým serverem může útočník zaznamenat vaše heslo při přihlášení do e-mailu a stejně tak při online nakupování může získat údaje z platební karty. Nedostatek v zabezpečení protokolu HTTP řeší protokol HTTPS (HTTP over SSL/TLS). Provozovatel webového serveru požádá o vydání zaručeného certifikátu pro jeho internetovou doménu, váš prohlížeč certifikát rozpozná a od té chvíle je zaručena důvěrnost spojení pomocí šifrování. Jinými slovy informace odesílané v rámci komunikace přes HTTPS nejsou čitelné pro nikoho krom nás a webového serveru, se kterým komunikujete. **Použití protokolu HTTPS je ve webovém prohlížeči typicky indikováno symbolem zeleného zámku v adresním řádku prohlížeče. (viz obrázek níže):**

Bezpečnost webových služeb

Webové služby jsou poskytovány online pomocí webového rozhraní - webové stránky, oproti klasickým stránkám ale vyžadují interakci uživatele. **Může se jednat například o služby elektronického bankovnictví, e-mailu nebo internetových obchodů.** Rizikem je zde především to, že službě předáváme osobní a citlivé informace. **Do většiny webových služeb je nutné se přihlásit a informace o vašem chování mohou být využity například k výběru zobrazovaného obsahu a reklamy.**
Pozor si tedy musíme dávat na propojování aktivit, které propojovat nechceme. Příkladem může být míchání soukromé a pracovní pošty. Pokud se po dokončení úkonu ze služby neodhlásíme, můžeme nechtěně dávat poskytovateli služby další informace. Příkladem jsou e-mailové služby poskytovatelů, kteří zároveň provozují webový vyhledávač (Seznam, Google apod.). Veškeré vyhledávání, které provedeme s přihlášením v e-mailu, se zaznamená v našem profilu.

K tomu, aby bylo možné tyto informace do uživatelského profilu uložit, slouží tzv. cookies. Tyto soubory jsou často považovány za cestu k narušení soukromí. Jedná se o textový soubor, který webová stránka odešle vašemu prohlížeči. Při každé další návštěvě webové stránky pak prohlížeč tato data posílá zpět. Cookies tak zaznamenávají vaší aktivitu, a to i bez přihlášení do specifické webové služby. Sledují například jaké stránky navštěvujete, jaké typy informací vyhledáváte, jaké zboží kupujete. Následně tyto informace analyzují a vyhodnocují. Cookies slouží ke sbírání informací o uživatelích, vytváření statistik pro webové analytiky a cílené reklamy.

Webové prohlížeče dnes umožňují ve svých nastaveních smazat cookies a údaje o prohlížení u vybraných nebo všech navštívených stránek.

Doporučení k bezpečnosti na webu

- **Aktualizujte webový prohlížeč**

Stejně jako ostatní software i webový prohlížeč může obsahovat zranitelnosti, které mohou být zneužity k poškození vašeho systému. Pravidelné aktualizace odstraní známé zranitelnosti.

- **Preferujte weby zabezpečené pomocí HTTPS**

V prohlížeči jsou vyznačené pomocí zeleného zámečku. Tento protokol zajišťuje důvěrnost komunikace mezi vámi a provozovatelem webu. Pokud na dané stránce zadáváte přihlašovací údaje nebo provádíte citlivé akce, je HTTPS naprostou nutností.

- **Nenavštěvujte nedůvěryhodné weby**

Nedůvěryhodné weby často obsahují závadný obsah a malware, který se navíc mohou snažit dostat do vašeho počítače například nevyžádaným zahájením stahování neznámých souborů. Rozpoznat nedůvěryhodný web je někdy obtížné. Mezi typické znaky patří velké množství reklamy, vyskakovací okna, stránky měnící se bez akce uživatele, zahájení stahování bez vědomí uživatele apod.

- **Kontrolujte URL odkazy**

Pokud je vám předložen odkaz na stránku (link) například ve zprávě nebo e-mailu, vždy kontrolujte, kam odkazuje. Text, na který je možné kliknout, nemusí odpovídat odkazu samotnému. Kam opravdu odkazuje, zjistíte většinou po najetí myší. Zaměřte se na doménu, kde se web nachází a na případnou záměnu písmen: jednička místo malého písmene L, dvě písmena n namísto písmene m apod.

- **Pozor na zkracovače URL**

Jde o služby zkracující dlouhé URL na krátké odkazy pevné délky. Problémem je, že takto zkrácený odkaz není možné zkontrolovat. Klikejte tedy pouze na zkrácené odkazy z důvěryhodných zdrojů. Například zaslané lidmi, kterým věříte, a kteří to dělají pravidelně například z důvodu omezeného počtu znaků ve zprávě.

- **Neotevírejte neznámé soubory**

Pokud se ve složce, kam se stahují soubory z webu, objeví neznámý soubor, neotevírejte ho. Může jít o infikovaný soubor, bez vašeho vědomí stažený z nedůvěryhodné stránky. Pro lepší přehled všechny soubory po stažení co nejdříve přemístěte do příslušných složek - obrázků, dokumentů a jiných - a samotnou složku pro stahování udržujte prázdnou.

- **Mějte jednu extra e-mailovou adresu určenou pro nepořádek**

Množství webových služeb vyžaduje pro zpřístupnění obsahu nějakou formu registrace nebo zadání emailového kontaktu. Rizikem je následné zasílání spamu a dalších nevyžádaných zpráv. Proto je dobré mít kromě své hlavní e-mailové adresy ještě jednu určenou pouze k jednorázovým registracím.

MojeID

MojeID je služba poskytovaná sdružením CZ.NIC - správcem národní domény .cz. Můžete si založit vlastní MojeID účet, který podporuje vysokou úroveň zabezpečení včetně dvoufaktorové autentizace. Tento jeden účet pak můžete využít k přihlášení do řady partnerských webů jako idnes.cz, alza.cz, regiojet.cz a mnoho dalších. Výhodou pro uživatele je jednoduchost při přihlášení jednotným účtem, záruka vysoké bezpečnosti a fakt, že vaše heslo spravuje pouze MojeID (CZ.NIC). Ostatní služby pouze obdrží od MojeID potvrzení, že jste se úspěšně přihlásili a informace, které si vyžádaly, například vaše jméno nebo e-mail.

Rozšiřující materiály – MojeID (poskytovatel)
https://youtu.be/cq31QTrWcQ8

Sociální sítě

Sociální sítě jsou webové služby zaměřené na komunikaci, sociální kontakt a sdílení fotografií a dalšího obsahu, který zpravidla vytváří sami uživatelé.**Nejvýznamnějšími zástupci jsou Facebook, Twitter a Instagram.** Sociální sítě motivují uživatele ke sdílení informací a tvorbě obsahu. **Nesdílejte více informací než je vhodné, a sdílejte jen se správnými lidmi.** Je třeba rozlišovat, koho na sociální síti opravdu znáte, a co o něm s jistotou víte.

Díky své povaze a obrovskému množství citlivých údajů jsou sociální sítě doslova ideálním prostředím pro manipulaci prostřednictvím metod sociálního inženýrství a současně častým terčem hackerských útoků. Musíme tedy neustále zvažovat, jak moc věříme lidem, se kterými komunikujeme, a do jaké míry se můžeme spolehnout na zabezpečení služby, za které zodpovídá provozovatel.

Digitální stopa

Stejně jako za sebou zanecháváte stopy chůzí v písku, tak svým chováním a veškerou činností on-line za sebou zanecháváte tzv. digitální stopu. Ta zahrnuje webové stránky, které navštěvujete, e-maily, které posíláte a informace, které poskytujete v rámci různých online služeb. Jednou z forem rozšiřování digitální stopy je vaše aktivita na sociálních sítích.

Každý příspěvek (tweet, facebookový status, foto), který na nich publikujete, je součástí vaší digistopy. Při jejich využívání byste proto měli být obezřetní, jaký obsah zveřejníte, a to i přes to, že jde ve většině případů z vašeho profilu odebrat. Vašim propojeným kontaktům obsah viditelný již nebude, nicméně v kyberprostoru v rámci vaší digitální stopy zůstane a bude potenciálně dohledatelný.

Zneužity mohou být i informace ze sportovních aplikací - například při sdílení vaší běžecké aktivity na sociálních sítích zároveň sdílíte citlivé informace týkající se vaší polohy a návyků, které mohou sloužit potencionálnímu útočníkovi. Ten si může k fyzickému napadení vybrat například ženu, která chodívá k večeru běhat nefrekventovanou částí města či obce.

Doporučení

Oblíbenost sportovních aplikací svědčí o tom, že je uživatelé považují za přínosné, a doporučovat jejich úplné vymazání by se zřejmě minulo účinkem. To platí i o sdílení fotek ze zahraničních cest. Jak rizika spojená s jejich užíváním alespoň minimalizovat? Zde je základní doporučení:

- **Vždy se zamyslete, zda je nutné publikovat informace například o vašem běhu nebo jiné aktivitě na sociálních sítích.**
- **Využívejte nastavení soukromí v rámci různých sociálních sítí.**
  Omezte okruh uživatelů, kteří vidí vaše příspěvky.
- **Při každém sdílení příspěvku zkontrolujte, zda zároveň s ním nebude sdílena i vaše poloha.**
  Sdílení polohy s příspěvkem se dá na většině sociálních sítí vypnout. Zakázat sdílení polohy aplikaci můžete i ve svém mobilním telefonu.
- **Zbytečně na sociálních sítích neuvádějte, kdy a na jak dlouho nebudete doma.**
  Fotky z vašich cest publikujte, až když už budete zpátky z cest.

Kapitola 6: AUTENTIZACE

Šestá kapitola si klade za cíl, seznámit uživatele se základními prvky autentizace, a s ní souvisejícími procesy - identifikace a autorizace. V rámci této kapitoly se seznámíme se zásadami pro tvorbu silného hesla, s vícefaktorovou autentizací a dalšími metodami autentizace, jako je například elektronický podpis a časové razítko, které jsou používány v úřední komunikaci.

Identifikace

Identifikace je proces, při kterém se na základě porovnání nezaměnitelných charakteristik určí nebo vyloučí totožnost určité osoby. Příkladem charakteristik jsou otisky prstů, barva očí nebo DNA. Těchto charakteristik využívá biometrická autentizace, která bude probrána v další části této kapitoly.

Autentizace

Autentizace slouží k jednoznačnému určení uživatele, který přistupuje do informačního systému. Každý uživatel se autentizuje proti databázi, ve které je vytvořen jeho vlastní jedinečný profil. Nejčastěji je uživatel autentizován na základě uživatelského jména a hesla, ale využívají se i další možnosti k přihlášení, které budou probrány v další části této kapitoly.

Autorizace

Pokud již systém ví, kdo jsme, přidělí nám oprávnění k určitým úkonům - **autorizuje**. Jinými slovy: přestože proběhne autentizace a my se do počítače přihlásíme jako uživatel XY, neznamená to, že jsme autorizováni ke všem úkonům, například k mazání souborů. Abychom si celý proces názorněji ukázali, předvedeme si ho na příkladu

Tvorba bezpečného hesla

V odborné komunitě se dnes více než o **password** z anglického slova *„word“* znamenající heslo, hovoří o **passphrase** od slova *„phrase“* označující slovní obrat nebo frázi. **Z hlediska bezpečnosti, ale i zapamatovatelnosti, je žádoucí používat více slov či větu namísto dlouhého jednoslovného hesla.** Následující doporučení vám ukáže několik možností, jak si silné heslo vytvořit:

Doporučení

- **Zvolte si unikátní větu nebo souvětí, které si snadno zapamatujete.** Mohou to být například humorné verše, hlášky z filmů, věty, ke kterým máte navázanou nějakou vzpomínku, ideálně nedávající smysl ostatním, které vznikly přeřeknutím, zkomolením nebo zpřeházením pořadí. Například z věty *„Tekutý hrnek za tmy pukl vztekem“* můžete vytvořit heslo: Thztpv18. Používání vět namísto jednoho slova vám dovoluje být ve výběru slov i jazyka opravdu rozmanitý. Navíc takto přirozeněji budete používat interpunkční znaménka či emotikony, např.: :/, :(a jiné.

- **Nepoužívejte pouze obecně známá kompoziční pravidla pro tvorbu hesla.** Nechte svoji fantazii vytvořit silné heslo, které nemá logické uspořádání. Díky tomu bude jeho prolomení těžší.

- **Silné heslo není nutné pravidelně měnit.** K jeho změně přistupujte v případě, že jste ho zapomněli a museli jste si ho nechat vygenerovat znovu, nebo pokud máte podezření nebo víte, že jste se stali obětí phishingového útoku. Příliš častá obměna silného hesla může vést k tomu, že budete používat stejné heslo do více služeb, nebo více různých hesel, u kterých jen jednou za čas kosmeticky upravíte jen některý ze znaků.

- **Nikdy si jako alternativu k heslu neaktivujte žádné kontrolní otázky typu *"jméno za svobodna"* nebo *"příjmení učitele nebo učitelky z první třídy"*.** Tyto informace jsou většinou dohledatelné z veřejných zdrojů.
- **Nikdy nevyužívejte nástroje či online služby pro kontrolu síly hesla.** Výsledkem může být pouze to, že heslo jen předáte útočníkovi.

Slovníkové útoky

Jde o techniku hádání hesla, pro kterou existuje řada specializovaných programů. **Funguje na principu opakovaného zkoušení různých hesel z obsáhlých seznamů jednoduchých, intuitivních a nejvíce používaných hesel.** Díky automatizaci je program schopen prolomit slabé heslo v řádu dnů, hodin nebo dokonce minut. Jak lze takový slovníkový útok na slabé heslo provést, se podívejte v následující ukázce.

https://youtu.be/Unc4T1KGfo4

Slabá hesla

Ta nejslabší hesla jsou obvykle postavena okolo následujících údajů: jména rodinných příslušníků, data jejich narození nebo rodná čísla, různá identifikační čísla jako datum narození nebo rodné číslo, přezdívky, jména mazlíčků, koníčky a záliby, oblíbené předměty a barvy, název základní školy nebo třídní učitelky, či název ulice bydliště nebo zaměstnání.

Další metody autentizace

Vedle loginů a hesel existují ještě další formy autentizace. Nejrozšířenější z nich jsou buď USB token nebo čipová karta s nahraným klíčem. Často lze setkat i s kontrolními dotazy (CAPTCHA), které slouží k tomu, aby odlišily reálnou osobu od robota. Tyto metody jsou součástí následující podkapitoly Vícefaktorová autentizace. Jak tento ochranný prvek funguje ukazuje přiložené video:

https://youtu.be/MWu2UiLLJI8

Vícefaktorová autentizace

V současnosti nejvyužívanějším způsobem zabezpečení citlivých informací je tzv. vícefaktorová autentizace neboli Multi-Factor Authentication (MFA). Poskytuje vyšší úroveň zabezpečení než pouhý login a heslo. Principem vícefaktorové autentizace je, že po klasickém zadání přihlašovacích údajů jste ještě vyzváni k potvrzení přihlášení třeba prostřednictvím SMS nebo jiným nezávislým komunikačním kanálem. S MFA se setkáte například ve službách internetového bankovnictví, cloudových služeb nebo interních informačních systémů ve vašem zaměstnání.

Okruhy ověřování

Tři druhy faktorů, které vícefaktorová autentizace využívá k ověření identity uživatele, a které jsou vysvětleny dále, jsou:

- znalost nějaké informace,
- vlastnictví nějakého předmětu,
- biometrie - unikátní vlastnost našeho těla.

Všechny tyto okruhy si stručně představíme na následujících stránkách.

Rozšiřující materiály – 2x video

What is Two-Factor Authentication? (2FA)
https://youtu.be/0mvCeNsTa1g

Multi-factor Authentication as Fast As Possible
https://youtu.be/07mRDyydCNY

Znalost

Jde o nejpoužívanější autentizační faktor. Systém ověřuje znalost určité informace, kterou si musí uživatel pamatovat, aby se mohl přihlásit. Patří sem například heslo, číselná kombinace v podobě PINu, kontrolní otázka, nakreslení gesta atd.

Vlastnictví

Další způsob vícefaktorové autentizace je ověření vlastnictví nějakého předmětu, který uživatel nosí u sebe, a kterým při přihlašování elektronicky ověří svoji identitu. Takovým předmětem neboli bezpečnostním tokenem může být USB disk nebo čipová karta s nahraným kryptografickým klíčem, nebo třeba mobilní aplikace. Nevýhodou tokenu je, že ho musí mít uživatel při přihlašování do systému vždy při sobě. Další nevýhodou může být pořizovací cena nebo nutnost pravidelné aktualizace software.

Čipové karty

Plastové karty, jejichž součástí je integrovaný čip umožňující digitální identifikaci uživatele. Tyto karty mohou být paměťové nebo mikroprocesorové a proti padělání bývají doplněny o hologramy a další bezpečnostní prvky

USB token

Existuje celá řada USB tokenů, s tlačítky nebo bez. Tokeny je možné propojit s více účty a využívat k přihlášení do Windows, e-mailu nebo na sociální sítě. Princip fungování je takový, že po zadání přihlašovacích údajů jste vyzváni k vložení tokenu do USB portu, u některých tokenů i ke stisknutí tlačítka. Token je obvykle možné propojit i s chytrým telefonem.

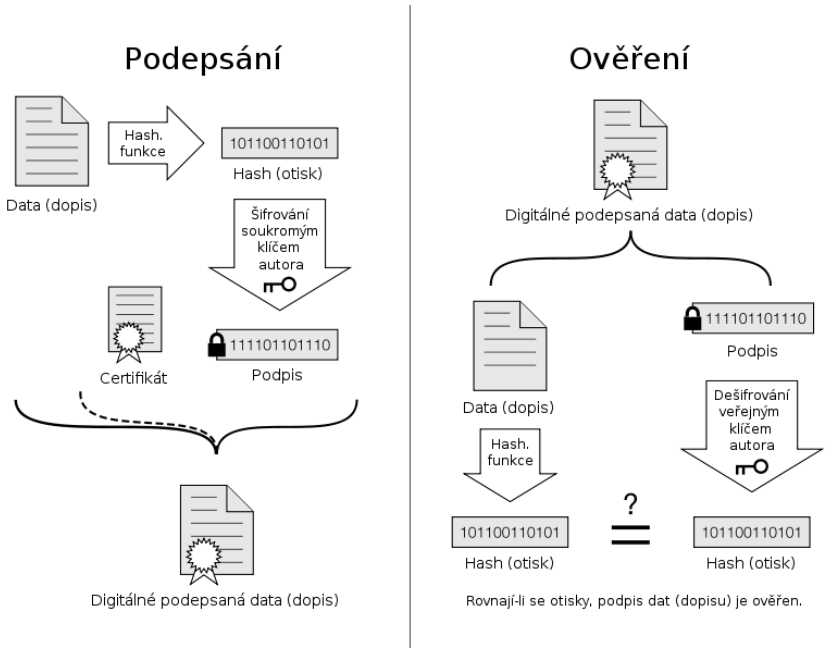
Biometrie

Při tomto postupu systém ověřuje biologické charakteristiky uživatele, tedy nějakou unikátní vlastnost jeho těla. Každý z nás má jedinečný otisk prstů, duhovku, tvar obličeje nebo hlas, což umožňuje uživatele ověřovat následujícími technikami

- **Diaktyloskopická biometrie**
- **Biometrie obličeje**
- **Biometrie hlasu**
- **Biometrie sítnic**

Elektronický podpis

Stejně jako u klasického podpisu, i ten elektronický ověřuje totožnost autora určitého elektronického dokumentu nebo zprávy. Díky tomu lze šifrovat komunikaci, jednat s úřady a odevzdat tak například daňové přiznání.



Ukázka fungování elektronického podpisu

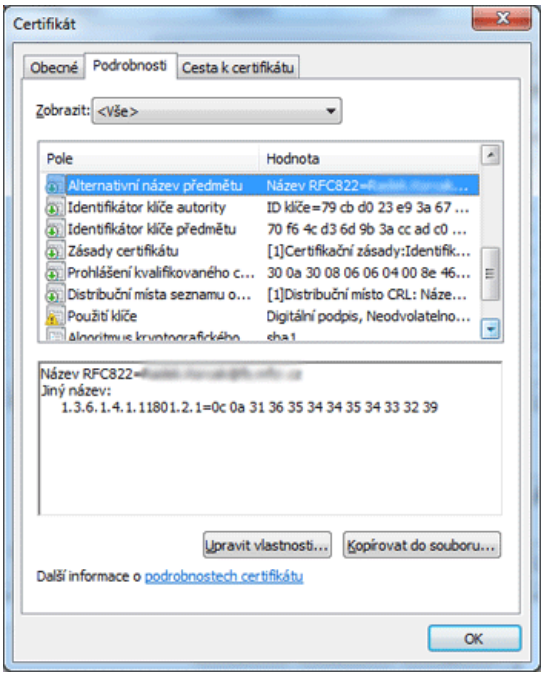
Časové razítko

Elektronický dokument může být opatřen i tzv. *„časovým razítkem“*, tedy ověřenou informací o tom, kdy byl vytvořen. Díky němu je zaručeno, že dokument nebyl po tomto datu upraven. Časové razítko může a nemusí být kombinováno s elektronickým podpisem.

Ukázka fungování časového razítka

Certifikát

K využívání elektronického podpisu, který uznají i české úřady, je potřeba mít v počítači nebo na externím úložišti uložen tzv. kvalifikovaný certifikát. Ten potvrzuje platnost elektronického podpisu. Lze ho získat od některé z certifikačních autorit - v ČR například První certifikační autorita, Česká pošta nebo eIdentity. Přehled certifikačních autorit včetně poskytovaných služeb zde.



Příklad kvalifikovaného certifikátu.

Doporučení

Vaše autentizační údaje slouží výhradně vám. Mají vám pomáhat, nikoli komplikovat život. Při tvorbě hesel se proto vyvarujte dlouhé změti náhodných znaků, které budete mít problém si zapamatovat. Při tvorbě a nakládání s hesly postupujte podle uvedených rad v kapitole. Shrňme si je následovně:

- **Heslo má být silné a nepatří na papírky.**
- **Heslo musí být unikátní, nepoužíváme ho u žádné jiné služby nebo aplikace.**
- **Silné heslo není nutné pravidelně měnit.**
- **Nevyužíváme internetové služby pro ověření síly hesla.**
- **Přihlašovací údaje nesdělujeme ani *„nepůjčujeme“*.**
- **U kritických služeb jako online bankovnictví nebo e-mail upřednostňujeme dvoufaktorovou autentizaci.**
- **Svá zařízení a přístupové údaje k nim si pečlivě chráníme**.

Doporučení

Pokud máte spoustu účtů a hesel a nejste schopni si je zapamatovat, požádejte kompetentní osobu o instalaci tzv. správce hesel. Mezi nejoblíbenější patří 1Password, KeePass nebo LastPass. S vlastními verzemi správců přicházejí i známé antivirové společnosti. Správce hesel stojí na principu, že vám stačí mít v hlavě pouze jedno vstupní heslo do aplikace, která schraňuje hesla do všech dalších účtů a služeb. Do správců hesel doporučujeme *"vystěhovat"* méně důležitá hesla, ta zásadní do emailu nebo internetového bankovnictví sem nepatří. Při přihlašování zadává správce vaše uživatelské jméno a heslo za vás, čímž urychluje proces přihlašování a minimalizuje riziko odkoukání hesla. Někteří správci hesel ukládají šifrované informace o vašich heslech do počítače, jiní do cloudu - takové přihlašovací údaje jsou tak přístupné z více počítačů a mobilních zařízení. Většina správců disponuje i funkcí generátoru hesel, takže už si nemusíte lámat hlavu, jak poskládat super bezpečné heslo. **Pozor - máte-li správce hesel nainstalovaný na mobilním zařízení, důsledně dodržujte zásady fyzické bezpečnosti a zařízení chraňte heslem či PINem.**

Rozšiřující materiály – Co používat pro správu hesel? Jaké jsou alternativy pro LastPass?

https://365tipu.cz/2017/03/03/tip735-co-pouzivat-pro-spravu-hesel-jake-jsou-alternativy-pro-lastpass/

Kapitola 7: OCHRANA DAT

Kapitola sedm se věnuje ochraně dat - tedy jak si má uživatel zajistit, aby o svá data nepřišel nebo nedošlo k jejich kompromitaci, případně zneužití. V první části si rozebereme základní rady jak zabezpečit e-mail a cloud computing.

Pravidla zabezpeční e-mailu

Pojďme si představit několik pravidel, která se vyplatí dodržovat, pokud chceme zabezpečit přístup do e-mailu:

- **Jak jsme si již řekli, platí diskrétnost při jejím používání a zveřejňování. E-mail nedáváme každému, kdo požádá.**

Pokud nepředpokládáme delší komunikaci, ale jde jen o účel registrace, pak máme další schránku, ve které není naše soukromá konverzace a ani hesla k bankovním účtům a další údaje.

- **Používáné heslo má být dostatečně silné.**

Při jeho tvorbě můžeme využít postup z kapitoly č. 6 - Zásady pro tvorbu silného hesla.

- **Pokud máme náznaky, že došlo k narušení bezpečnosti naší e-mailové schránky, heslo si ihned změníme.**

Může jít o situaci, kdy jsme se přihlašovali v počítačové kavárně nebo se zapomněli odhlásit na veřejném počítači. Můžeme také kontaktovat provozovatele.

- **Do e-mailu se přihlašujeme pouze prostřednictvím nám známé stránky, ne skrze podezřelé odkazy.**

Při přihlášení by měl být využit bezpečný přenosový protokol „HTTPS“.

- **Většina kvalitních veřejných e-mailových služeb nabízí dvoufaktorovou autentizaci.**

Kromě hesla tak musíme přihlášení potvrdit typicky nějakou akcí v mobilním telefonu, a to buď jednoduchým potvrzením přihlášení na displeji, nebo opsáním kódu z SMS.

- **Náš počítač udržujeme aktualizovaný, stejně tak i prohlížeč a aplikace.**

Dostupné aktualizace mohou opravovat známé zranitelnosti. S jejich instalací nijak neotálíme.

- **Pokud se už musíme k e-mailu přihlásit z veřejného počítače, dbáme zvýšené opatrnosti.**

Neumožníme prohlížeči uložit si naše heslo a po ukončení práce se z e-mailu odhlásíme.

Tipy zabezpeční e-mailu

Rozlišujte a nesměšujte soukromou a pracovní poštu. Zejména pracovní pošta nepatří na soukromý e-mail. Takové konání může být i právně problematické a přinést pracovní sankci. E-mail je údaj, který povinně uvádíme při nákupu v téměř každém e-shopu, stejně jako při rozličných registracích**. Pokud se registrujete jednorázově a dále už s provozovatelem služby nechcete komunikovat, využijte tzv. desetiminutový e-mail.** Při jeho použití se pouze ujistěte, že jde skutečně o jednorázovou registraci. K obsahu takového emailu totiž ztratíte po uplynutí deseti minut přístup - někdy je možné přístup o dalších pár minut prodloužit, ale tak jako tak po uplynutí určené doby zmizí.

Služby nabízející desetiminutové emaily:

- https://10minutemail.com/
- https://dropmail.me/cs/

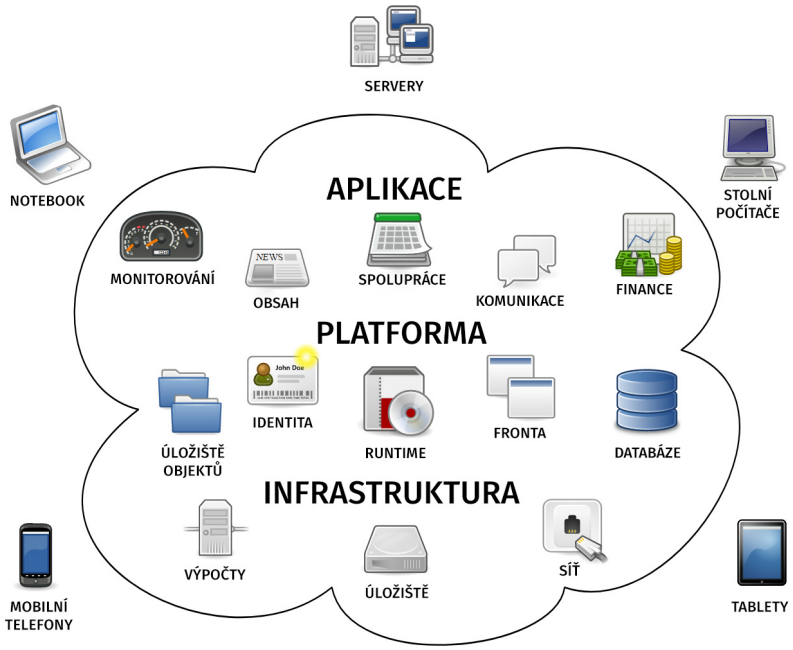
Rozšiřující materiály – 2x článek

Postup pro zabezpečení Gmail účtu:
https://support.google.com/accounts/answer/46526?hl=cs

Tipy k lepšímu zabezpečení mailu u Seznamu:
https://365tipu.wordpress.com/2016/01/22/tip387-jak-lepe-zabezpecit-e-mail-u-seznamu-proti-kradezi/

Cloudová řešení

Cloud computing označuje služby, ke kterým mohou uživatelé přistupovat vzdáleně přes Internet, často pomocí webového prohlížeče. Poskytovatel může nabízet sdílení a používání všech prostředků od infrastruktury, přes vývojové a aplikační platformy až po software. Produkt je však vždy poskytován on-line a bývá sdílený více uživateli zároveň. Příkladem mohou být poštovní služby *Seznam.cz* nebo cloudová úložiště *s*polečnosti *Google.*



Ukázka fungování cloudu

Výhody cloudového řešení

- **Nízké nebo žádné pořizovací a udržovací náklady na provoz**
  Mnoho služeb je bezplatných, aktualizaci a údržbu zajišťuje provozovatel.
- **Flexibilita**
  Služby, data a další nástroje jsou prostřednictvím Internetu k dispozici ihned a odkudkoliv.
- **Možnost zálohování dat**
  Díky tomu, že se u nás data fyzicky nenachází, nemůžeme o ně přijít stejně jako v případě napadení počítače ransomware.
- **Pohodlné sdílení a možnost spolupráce**
  Ke stejným datům může přistupovat několik uživatelů z různých míst.

Nevýhody cloudového řešení

- **Neoprávněná osoba získá přístup k našim datům**.
  Jen někteří poskytovatelé cloudových úložišť data šifrují. Je dobré si vždy prostudovat podmínky, za kterých je služba nabízena.
- **Neexistuje žádná standardizace**.
  Podmínky různých poskytovatelů, byť stejných služeb, se často liší. Opět si projděme podmínky nabízené služby. U menších společností může dojít k rychlému zániku, a tím i nedostupnosti našich dat a služeb.
- **Většina poskytovatelů nabízí minimální podporu**
  Toto se týká přirozeně především neplacených služeb.
- **Víme, kde jsou naše data fyzicky uložena?**
  Zjistit, kde se naše data nachází, nebývá jednoduché. Při výběru poskytovatele projděme recenze uživatelů a jejich renomé.
- **Výpadky služby**.
  Cloudová služba může být nedostupná z důvodu údržby, technické poruchy nebo kybernetického útoku. V ideálním případě máme data zálohována i na fyzickém úložišti.

Kapitola 8: ŠKODLIVÝ SOFTWARE

Úvodem osmé kapitoly je představen malware, vysvětlen princip jeho činnost a uvedeny jeho nejčastější druhy i charakteristiky. Pro lepší orientaci jsou jednotliví zástupci malware doplněni o konkrétní příklad. Podstatná část kapitoly se také zabývá tím, kde se může uživatel s malware setkat, jak by se měl zachovat a co učinit. V závěru kapitoly jsou shrnuty doporučující informace, jak se před malware chránit.

Malware

Slovo **malware** vzniklo spojením slov *„malicious“* (škodlivý, zákeřný) a *„software“*. Jde o obecné pojmenování jakéhokoliv škodlivého softwaru, nejčastěji šířeného prostřednictvím nevyžádané pošty formou příloh, stahováním z nedůvěryhodných serverů a úložišť nebo nakaženými reklamami vloženými do webových stránek

Malware může

- odcizit nebo zašifrovat data nebo poškodit počítač,
- zneužít počítač pro rozesílání spamu, k DDoS útokům nebo k těžbě kryptoměn,
- sbírat informace v podobě přihlašovacích údajů do emailu nebo internetového bankovnictví.

Zkrátka může dělat téměř cokoliv. Malware je výdělečně obchodován ilegální cestou a fantazie jeho tvůrců nezná hranic - podívejme se nyní na jeho druhy.

Ransomware

Název je odvozen od anglického ***„ransom“*** - *„výkupné“*. Ransomware cíleně zamkne či zašifruje data napadeného počítače a jejich znovuzpřístupnění podmiňuje zaplacením výkupného, typicky v kryptoměně (například Bitcoinech) nebo prostřednictvím klasické online platby. V českém prostředí se výkupné nejčastěji pohybuje v rozmezí 7 500 – 17 000 CZK. Ransomware zároveň udává poměrně krátký čas, do kterého je nutno výkupné zaplatit, čímž zvyšuje tlak na vydíraného.

Ransomware se neustále vyvíjí. Starší verze se nazývaly *„lockery“*, protože *„pouze“* zamykaly. Jejich znovuodemčení bylo často možné i bez zaplacení výkupného. S vývojem technologií a především šifrování se však původní lockery vyvinuly do tzv. *„crypto-lockerů“*, které data kompletně a kvalitně zašifrují. Obnovení je tak podstatně složitější a někdy zcela nemožné.

Ukázka Ransomware s policejní tématikou tzv. "Policejní virus"

Jak na ransomware?

- Nejčastěji se k postiženým dostává jako soubor přiložený k e-mailu, například faktura. Zde je na místě použít selský rozum: očekávám podobný email? Není příloha zvláštně nazvána? Kdo mi ji posílá? Výrazné markanty jako špatný pravopis nebo nerelevantní loga už bohužel vymizely a ransomware používá korektní jazyk.
- Zásadním opatřením je na neznámé přílohy neklikat a u dokumentů nepovolovat makra. Právě povolení maker velmi často stojí za nechtěnou instalací ransomware.

Rozšiřující materiál – Do boje proti kyber vyděračům nekompromisně zasáhly orgány činné v trestním řízení a významné společnosti z oblasti IT bezpečnosti. Díky iniciativě No More Ransom! lze zdarma odstranit velké množství ransomware včetně jeho historických verzí. Naleznete jej na stránkách: https://www.nomoreransom.org/ransomware-qa.html

PŘÍKLAD – Wanna Cry

Dne 12. května 2017 došlo dosud k jednomu z nejrozsáhlejších kybernetických útoků. Malware, který útočníci použili, byl právě ransomware s názvem „Wanna Cry“. Jen od 12. do 14 května proběhlo cca 45 000 útoků v 74 zemích světa. Nejvíce byla zasažena Ruská Federace, která se stala terčem 57% všech útoků. Ransomware zde kompromitoval především systémy Federálního ministerstva vnitra či systémy telefonního operátora Megafon. Dále byly četnými útoky zasaženy například Velká Británie, kde došlo k narušení systémů zdravotnických zařízení, španělská Telefónica a americký FedEx. Útok zasáhl i Českou republiku, ale pouze okrajově, přičemž nedošlo k ohrožení žádných zásadních systémů.

Z technického hlediska se jednalo o propracovaný malware, který byl schopen šířit se samostatně bez zásahu uživatele. To způsobilo jeho velký dopad. Vzhledem k rozsáhlosti a počtu zasažených států lze tvrdit, že se nejednalo o diskriminační, přesně cílenou, hrozbu s konkrétním politickým motivem. Experti však odhadují, že šlo jen o první vlnu a další útoky budou následovat.

Spyware

Neboli špionážní malware od anglického *"spy"* - *"špion"*, je škodlivý program, který v napadeném počítači provádí nežádoucí špionáž a využívá Internet k odesílání citlivých a osobních dat bez vědomí uživatele. Spyware například cíleně vyhledává:

- přístupové prvky k vašim službám: internetové bankovnictví, e-maily, sociální sítě,
- osobní a citlivé údaje: údaje o kreditních kartách, rodná čísla, data z důležitých interních databází,
- produktová registrační čísla vašeho software.

Spyware může být součástí i jinak užitečného programu. Proto zvažujme, co si do počítače nebo chytrého telefonu nainstalujeme a hlavně odkud. Největší pozor si dávejme na nelegální pirátský software stažený buď přes sdílená úložiště, nebo Peer2Peer sítě.

Červ

Červ je ještě zákeřnější než virus. Dokáže se totiž sám replikovat a šířit sítí. Kromě této vlastnosti může ještě vykonávat sekundární činnost, například:

- vyřadit z provozu počítač nebo jeho součásti,
- odstraňovat soubory uložené v počítači,
- šifrovat soubory uživatele jako nátlak k zaplacení poplatku s příslibem opětovného dešifrování (ransomware),
- prohledávat počítač a získávat osobní data ke zneužití útočníkem,
- vytvářet „zadní vrátka“ (backdoors) do systému jako přímou cestu k infikování počítače dalšími nákazami.

Solar Sunrise

- Jedním z historicky neznámějších červů je červ Solar Sunrise. V únoru 1998 zjistilo americké ministerstvo obrany, že se v jeho síti nachází malware. Ten byl postupně detekován v dalších státních i soukromých institucích.
- Šlo o koordinovaný útok, který cílil na Pentagon právě v době, kdy v Perském zálivu panovalo zvýšené napětí související s irácký programem na výrobu zbraní hromadného ničení. Do této oblasti se tedy právě přesouvaly některé americké jednotky. Panovaly tak obavy, že by mohlo jít o cílený útok Iráku proti sítím ministerstva obrany. Červ cílil na známou zranitelnost v operačním systému UNIX Solaris (SunOS), podle něhož také dostal název. Zranitelnost byla v době útoku dobře známá a byl vydán i tzv. patch, který ji opravoval. Pentagon ale svůj systém neaktualizoval.
- Zpočátku byl původce útoku i jeho účel neznámý. Červ v nakaženém počítači shromáždil data (např. přihlašovací údaje) a předal je útočníkům. Stopa nakonec vyšetřovatele zavedla přes několik zemí až do Izraele a Kalifornie. Za útokem stáli dva američtí a jeden izraelský teenager, kteří pojali proniknutí do sítě ministerstva obrany jako výzvu. Motivací tedy naštěstí nebylo zcizit data nebo narušit fungování Pentagonu.
- Útok ale odhalil slabé zabezpečení státní správy. Ministerstvo obrany nemělo dostatečný systém pro detekci vniknutí ani kapacity pro rychlé vyšetření incidentu. Šlo tak o jeden z budíčků, který poukázal na nutnost více se věnovat kybernetické bezpečnosti.

Botnet

- Termín botnet je složeninou slov „bot“ (robot) a „net“ (síť). Botnet je tedy síť napadených a „zotročených“ počítačů – robotů zneužitých k páchání dalších útoků. Takto napadeným počítačům se též říká „zombies“. Program běžící na zotročeném počítači je ovládaný centrálním „Command-and-Control serverem“ (C&C nebo C2).
- Počítač může být nakažen a zapojen do botnetu stahováním pirátského softwaru, zneužitím bezpečnostních mezer systému a dalšími způsoby. Botnety jsou využívány zejména k páchání DDoS útoků, kdy síť zotročených počítačů zahltí cílový systém kvantem nesmyslných požadavků a způsobí tak jeho nedostupnost pro regulérní uživatele. Boti stojí také za nevyžádanou poštou a šířením SPAMu.

STORM BOTNET / DORF BOTNET / ECARD MALWARE

- Prvně byl objeven v roce 2007 a podobně jako předchozí příklady malware se i on šířil pomocí spamového e-mailu. Předmět tohoto e-mailu nesl název „230 Dead as storm batters Europe“ – odtud tedy vžité označení Storm botnet. Napadal hlavně počítače s operačním systémem Windows a byl jedním z prvních fungujících na principu peer-to-peer. Jednalo se o vzdálenou síť „zombie“ počítačů nakažených červem a trojským koněm.
- Operátoři tohoto botnetu jej využívali zejména k páchání finančních podvodů a krádežím identity. Celkový počet počítačů, které Storm botnet ovládal, se pohybuje v řádech desítek milionů. Jeho specifikum spočívalo v tom, že byl svými operátory poměrně dlouho a intenzivně chráněn proti pokusům IT bezpečnostních odborníků o jeho „prolomení“ a znefunkčnění. Později však byly jeho části operátory postupně rozprodány operátorům jiných botnetů.

Trojský kůň

Analogie s antickou Trojou je namístě - v programu, který se tváří jako užitečný a dokonce tak i funguje, se skrývá další škodlivá funkcionalita. Nakažení tímto druhem malware by měl odhalit váš antivirový program. V některých případech může nákazu poznat i sám uživatel, když se jeho počítač začne chovat zpomaleně a *„divně“*. Pokud se chceme trojanům vyhnout, opět zapomeňme na nelegální stahování.

TROJAN ZEUS / Z-BOT

První trojan s tímto jménem se objevil v roce 2007 v USA a největší boom pak zaznamenal o dva roky později. Jednalo se zároveň o botnet, který se šířil klasicky především v důsledku stahování a phishingu. Škodlivý software, který byl velmi důkladně propracován, tajně odchytával hlavně hesla, čísla účtů, a přihlašovací údaje do internetového bankovnictví. Další verze malware ZeuS získávaly též například přihlašovací údaje k e-mailovým schránkám či sociálním sítím. Historicky se jedná o jeden z nejrozšířenějších druhů malware ve své době. Například jen z největších trojských koní, který jen za rok 2009 infikoval miliony počítačů v USA, řádil však po celém světě.

Jak se chránit přes škodlivým softwarem?

Představili jsme si hlavní reprezentaty škodlivého software. Bohužel neexistuje ucelený návod, jak 100% uchránit počítač od jakékoli vnější infiltrace. Své šance v boji proti malware však můžeme výrazně zvýšit:

- Neotevíráme přílohy e-mailů s neočekávaným typem přiložených souborů, jejichž obsah není přesně znám. Pokud odesílatele známe, ověříme si důvěryhodnost poslané zprávy jinou cestou než přes e-mail. V případě podezření kontaktujeme své IT oddělení.
- Nespouštíme odkazy na neznámé/podezřelé stránky. Na těchto webech se ani nepohybujeme.
- Nestahujeme nelegální obsah.
- Používáme aktuální antivirový a antispywarový software.
- Používáme aktuální firewall.
- Používáme aktuální verzi operačního systému s instalovanými opravnými balíčky.

Kapitola 9: ŠKODLIVÝ OBSAH

Kapitola devět seznamuje se zprávami typu spam, scam a hoax včetně zajímavých odkazů a stránek, které plní osvětovou funkci proti šíření a sdílení podobně škodlivého obsahu. Čtenář je také poučen, jak k takovým zprávám přistupovat, ať už jde pouze o náhodný marketingový pokus, bezdůvodné zahlcování e-mailové schránky, klamavou reklamu nebo o cílený podvod.

Spam

Spam je **nevyžádaná elektronická pošta, obvykle v podobě reklamního sdělení**. Nemusí být šířena pouze emailem, ale i prostřednictvím sociálních sítí nebo SMS zpráv. Spam kromě reklamy často obsahuje i malware.

- **Osobní i cizí e-mailovou adresu bychom měli používat diskrétně**. Tedy neměla být viditelná pro všechny uživatele na sociálních sítích, pokud posíláme zprávu více příjemcům, kteří se navzájem neznají, měli bychom zvážit, zda je nezařadíme do skryté kopie atd.
- **Na spam ze zásady neodpovídáme**. Nevyžádaná pošta je běžně rozesílána na obrovské množství e-mailových adres a mnoho z nich není platných. Pokud tedy odpovíme, tak mimo jiné potvrdíme, že naše adresa je používána a příliv nevyžádaného obsahu se spíše zvýší.
- **Spam hlásíme provozovateli e-mailové schránky**. Přispíváme tak k vylepšení filtrů, které nás v budoucnu před podobnými e-maily ochrání.

Jak vypadá spam?

Rozesíláme v práci e-mail dvaceti osobám, které se navzájem neznají. Nevyužijeme skrytou kopii, takže všichni vidí všechny ostatní příjemce. Jeden z adresátů chce odpověď, klikne ale omylem na „odpovědět všem“. Všech dvacet osob dostane jeho odpověď, která se jich ale vůbec netýká a pouze obtěžuje. Druhý příjemce chce zprávu přeposlat svému kolegovi. Obsahem přeposlané zprávy budou i e-mailové adresy původních dvaceti adresátů a jejich e-mailová adresa – soukromý údaj – se šíří dál. Poslední adresát se zachová nejméně eticky a rozhodne se všechny adresy využít a zařadí je ve své firmě na seznam adres, kterým je pravidelně zasílána reklamní pošta. Díky naší neopatrnosti tak budou dvě desítky osob dostávat nevyžádanou poštu – spam.

Scam

Odvozen od anglického "scam" - podvod. Typickým příkladem jsou známé *"Nigerijské dopisy",* které existovaly a šířily se už v listinné podobě. Za Scamming lze tedy označit podvádění či podvodné praktiky s cílem vylákat z obětí peníze. V elektronické formě se scam obvykle šíří prostřednictvím e-mailu a můžeme ho tedy vnímat jako formu spamu.

PŘÍKLAD – Postaráte se mi o dceru?

Odesílatel se v podvodném e-mailu v anglickém jazyce představuje jako starý muž, který je v posledním stádiu leukémie a hledá opatrovníka pro svoji nezletilou dceru, jenž by se o ni postaral po jeho smrti. Slibuje, že má tučný bankovní účet, ze kterého zaplatí všechny náklady spojené s výchovou a zároveň opatrovníka štědře odmění. Podvodník dále žádá o zaplacení „drobných“ poplatků (v tomto případě v řádu tisíců dolarů), které jsou nutné, aby bylo možné přepsat údajný bankovní účet s tučným obnosem na nového majitele.

Hoax

Hoax je poplašná, nebezpečná a hlavně zbytečná řetězová zpráva. Do češtiny můžeme termín přeložit jako mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu nebo výmysl. I k šíření hoaxů je hojně využívána e-mailová komunikace.

Znaky hoax

- **apeluje na emoce,** typicky jde o srdceryvné příběhy, jejichž hlavními aktéry jsou děti nebo domácí mazlíčci,
- často používá technický a sofistikovaný jazyk, čímž zprávě dodává na přesvědčivosti,
- vyvolává **důvěryhodnost skrze asociaci**, jinými slovy odkazuje se na osoby nebo organizace, které vzbuzují důvěru,
- bývá šokující, jde o otázku **života a smrti,** například upozornění na potravinu, která má neznámé karcinogenní účinky apod.

Jak hoax škodí?

- primárním cílem není zahltit maily, ale napáchat informační škodu,
- uvádí nás v omyl a může tak mimo jiné i negativně ovlivnit naše jednání, jak uvidíme dále v příkladu,
- pokud někdo hromadně přeposílá hoax, může vyzradit e-mailové adresy dalších adresátů a posílit spam,
- šířením hoax utrpí vaše pověst - ověřujte, co sdílíte.

Skandál s mlékem? Úřady to tají!

Věděli jste to?!! Mléko v tetrapaku, které se nespotřebuje do konce trvanlivosti, prodejce vrátí zpracovateli. Zpracovatel otevře obal, mléko opětovně převaří a opět zabalí. Mohou tak učinit max. 5 krát! Zespodu krabice je pod zalepeným záhybem číslo 12345, kde jedno z čísel chybí. Tato chybějící cifra udává, kolikrát už bylo mléko "recyklováno". Tj. 12 45 znamená, že bylo převařeno 3 krát. Tak dobrou chuť.

Mrkla jsem na to a opravdu. Na krabicích plnotučného mléka, které bylo "v akci" za 11,90 Kč, chybí v řadě č. 4. Doufám, že alespoň u mléka prodávaného jako čerstvé, nechybí v řadě žádné číslo. Datum spotřeby je cca 1 rok, takže je v krabicích i 5 let staré mléko!!!!!! A protože se krabicové mléko dělá ze sušeného fabrikátu s dobou použitelnosti 5 let, pijete lidičky mléko i 10 let staré!!! Takže si ty s***** za 9,90 Kč kupujte! Dobrou chuť...

Jak se bránit?

Základní pravidla se de facto shodují s těmi, které bychom měli dodržovat u ostatního spamu a vyjmenovali jsme si je výše. U hoaxu se nám ale může stát, že jeho odesílatelem může být někdo, koho osobně známe. V takovém (a pouze takovém) případě je možné na e-mail odpovědět. Dotyčného obeznámit s tím, že rozesílá nepravdivou, či polopravdivou zprávu, případně ho poprosit, ať nám podobné e-maily neposílá. Je možné ho i odkázat na stránku www.hoax.cz, kde jsou uvedeny historicky i aktuálně šířené hoaxy včetně jejich rozboru a uvedení na pravou míru.

Rozšiřující materiály – 3x

Hoax:
http://www.hoax.cz/hoax/

Místo vyhlídek na dědictví přišla žena o peníze:
http://jindrichohradecky.denik.cz/zlociny-a-soudy/misto-vyhlidek-na-dedictvi-prislapenize20100111.html

Vysvětlení hoaxu modrá velryba:
https://www.e-bezpeci.cz/index.php/temata/socialni-sit/1230-modra-velryba

Kapitola 10: SOCIÁLNÍ INŽENÝRSTVÍ

Poslední desátá kapitola pojednává o psychologických aspektech, tricích a konkrétních podnětech, které mohou uživatele zmanipulovat a nepříznivě ovlivnit při pohybu v on-line prostředí. Poskytuje praktické příklady takového druhu podvodného jednání včetně nejčastějších modů operandi útočníků.

Sociální inženýrství

Sociální inženýrství je manipulativní technika, která k ovlivňování uživatelů využívá specifické psychologické metody ve spojení s komunikačními a informačními technologiemi. Útočníci mohou jejím prostřednictvím páchat velké množství podvodů, které zasahují do normálního i on-line světa. Metody sociálního inženýrství se zaměřují na nejslabší místo zabezpečení celého systému - člověka. Nejčastěji využívané techniky sociálního inženýrství jsou: phising, pharming, baiting, pretexteng, a trashing. Všechny tyto praktiky jsou popsány na dalších stránkách.

Rozšiřující materiál – Sociální inženýrství (ESET MSTSN)
https://youtu.be/ktfDjnDIeo8¨

Phising

Phishing je druhem **podvodné techniky, díky které může útočník získat citlivé údaje nebo i peníze.** Hlavním principem je rozesílání e-mailových zpráv, které předstírají, že jsou například od vašeho IT oddělení, z jiného ministerstva, úřadu nebo od vašeho síťového správce. **Phishingový e-mail může obsahovat některé z těchto nápadných znaků:**

- **Webové stránky nejsou zabezpečené certifikátem HTTPS.**
- **Nachází-li se v obdrženém e-mailu odkaz na nějaké webové stránky, je důležité zkontrolovat si správnost takového odkazu (domény) v adresním řádku.**
- **Oslovení je nejčastěji psáno formou „Vážený pane/í“ bez uvedeného jména, případně „Vážený zákazníku“.**
- **Dříve byla výrazným znakem podvrženého e-mailu lámaná a často nepříliš dokonalá čeština obsahující gramtické a stylistické chyby.**
- **Tělo e-mailu nebude korespondovat s vaší dosavadní komunikací s daným subjektem.**
- **Žádná vám známá organizace po vás při vzájemné komunikaci nikdy nesmí chtít vaše přihlašovací údaje, osobní údaje, ověření informací o účtu s pohrůžkou jeho zablokování apod.** Pro tuto komunikaci jsou ve většině případů používána speciální hesla, která si zákazník zvolil při zřizování účtu pro danou službu.
- **Mnohé z těchto bodů platí i pro zasílané phishingové SMS zprávy, které dnes útočníci také hojně využívají.**

Rozšiřující materiál - Varování! PayPal phishing podvodné emaily | EduTV
https://youtu.be/qsuzTnRfvLY

Podvodná technika - PHARMING

- Pharming je druhem podvodné techniky, která má za cíl získat citlivé údaje od uživatele. Stojí na principu napadení DNS serverů a přesměrování nic netušícího uživatele na podvržené webové stránky například webového emailového rozhraní ministerstva. Rozdíl oproti phishingu je v tom, že uživatel ani nemusí kliknout na přiložený odkaz, aby k přesměrování došlo. Díky napadení DNS a změně IP adresy je přesměrování uskutečněno i po zadání správné adresy do prohlížeče.
- Obranou proti pharmingu je podrobné zkoumání internetové stránky, jejích případných nestandardních požadavků a chování. Opět si překontrolujte přítomnost bezpečnostního certifikátu vedle adresy v prohlížeči. Pokud budete mít kdykoliv pochybnosti, kontaktujte vaše IT oddělení a nastalou situaci jim popište.

Podvodná technika - BAITING

- Při baitingu útočník ponechá infikované přenosové paměťové médium v podobě paměťové karty, USB flash paměti nebo CD na místě, kde uživatel pracuje nebo bydlí. Cílem je, aby nalezené médium našel a vložil do svého zařízení. Po vložení do zařízení se spustí tajně umístěný škodlivý program, který má za úkol získat citlivá data, umožnit útočníkovi přístup do systému nebo zaznamenávat stisknuté klávesy. V neposlední řadě existují USB flash disky, které dokáží fyzicky poškodit základovou desku počítače, popsané v kapitole č. 4 Riziková zařízení.

Podvodná technika - PRETEXTING

- Jedná se o základní vytváření fiktivního scénáře, pomocí kterého se útočník snaží nic netušící uživatele zmanipulovat, aby mu sdělili určité informace nebo udělali, co po nich žádá. Při tzv. psaní scénáře využívá útočník fragmentů skutečnosti, aby jeho lež působila více realisticky. Může například využít jméno skutečného IT administrátora ministerstva a zavolat úředníkovi, aby mu pro kontrolu sdělil své přihlašovací údaje.

Podvodná technika - TRASHING

- I této techniky využívá útočník pro získávání důležitých informací, které mu mohou sloužit k pozdějšímu útoku. Jejich zdrojem jsou odpadky, vyhozené složenky, dopisy a další dokumenty, které útočníkovi pomohou působit před uživatelem důvěryhodněji. Z tohoto důvodu je nutné všechny důležité dokumenty (pracovní, dokumenty s identifikačními údaji, osobními a citlivými informacemi atd.) před vyhozením skartovat. Skartované dokumenty je sice možné opět poskládat, ale na to útočník většinou nemá čas ani chuť. Útok musí být efektivní při porovnání vynaloženého úsilí a výsledků, kterých je dosaženo.

Doporučení

- **Pokud vám přijde phishing do pracovní e-mailové schránky, vždy o něm informujte vaše ICT oddělení.**
- **Důvěřuj, ale prověřuj** Pokud se vám na příchozí zprávě cokoliv nezdá, telefonicky se zeptejte přímo odesílatele, nebo vašeho IT oddělení. Nic tím nezkazíte.
- **Nedat se zastrašit.** U podezřelých telefonátů, pokud si nejste jisti, zda vám skutečně volají například z IT oddělení vašeho ministerstva, zavěste a zavolejte zpátky na telefonním čísle z oficiálního seznamu. Nebojte se v případě pochybností vše ověřit a to i v případě, že vůči vám vystupuje autorita v podobě nadřízeného nebo jiného úřadu.
- **Nespěchat.** Útočníci rádi pracují s časovou tísní - hned teď je třeba něco vykonat, spravit, sdělit. Klid - škoda z prodlení bývá menší, než důsledky neuvážených činů.
- **Nebýt líný.** Jedno krátké a dobře zapamatovatelné heslo k několika účtům a službám je ideální způsob, jak přijít o všechno najednou.
- **Nebýt zbytečně zvědavý / ani zbrkle neklikat na vše, co vám přijde**. Každá zajímavá příloha nebo odkaz může být past. Opravdu potřebujete vidět právě tohle? Nepotřebujete. To samé se týká i nalezených paměťových karet či jiných datových nosičů.
- **Nebýt zbytečně sdílný.** Vše, co na sebe prozradíte na internetu (diskusní fóra, webové stránky, sociální sítě) mohou útočníci využít proti vám. Schválně si zkuste zadat do vyhledávače Google vaše jméno.
- **Nikdo vám nic nedá zadarmo**. Rozhodně vám nikdo nedá velký finanční obnos.