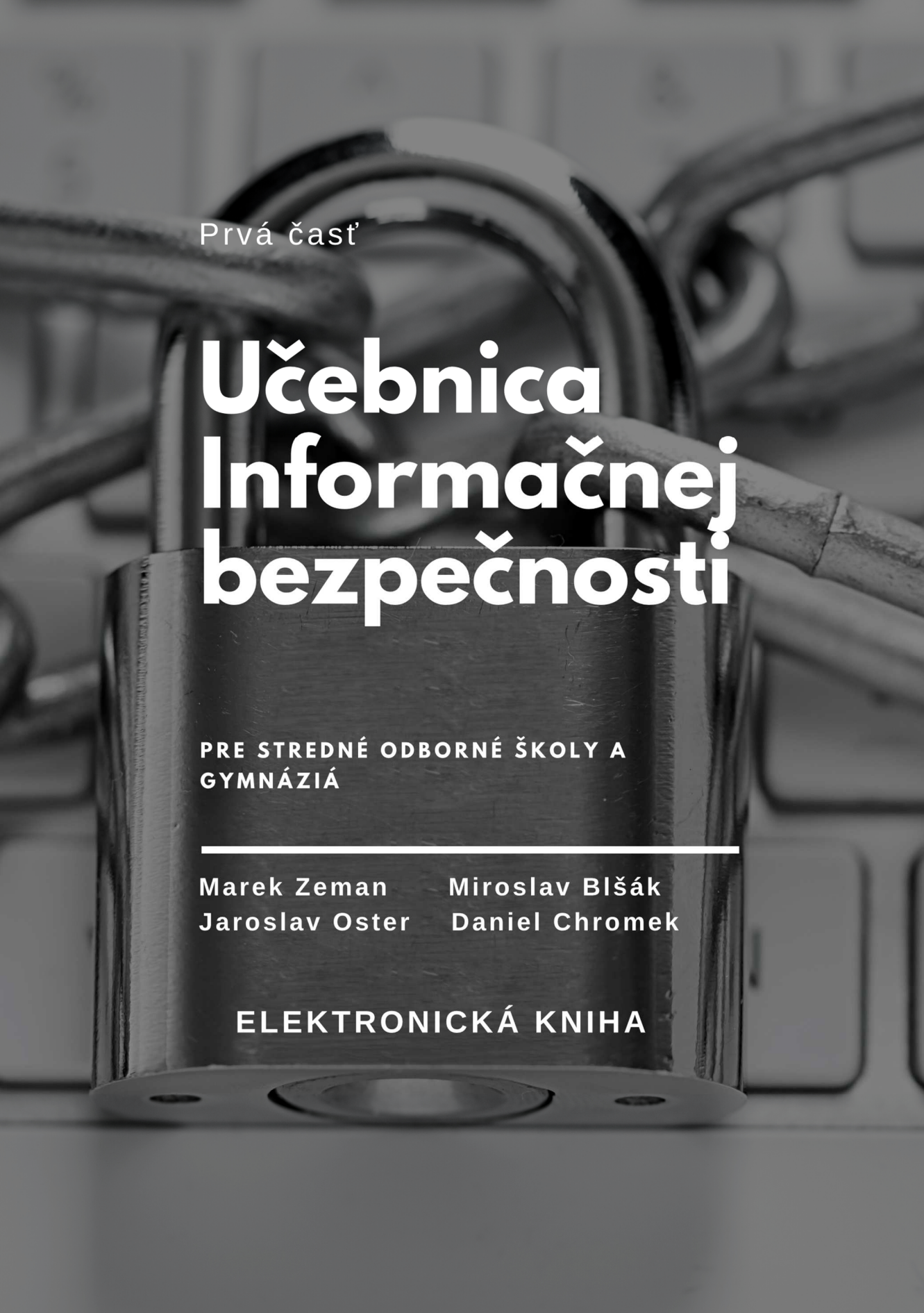


Prvá časť

Učebnica Informačnej bezpečnosti

PRE STREDNÉ ODBORNÉ ŠKOLY A GYMNÁZIÁ

Marek Zeman
Miroslav Blšák
Jaroslav Oster
Daniel Chromek

ELEKTRONICKÁ KNIHA

Partneri projektu Preventista.sk

Dynamický vývoj informačných technológií prináša aj rad rizikových faktorov pri ich využívaní v reálnom živote a teda aj požiadavky na vývoj bezpečnosti. Tento trend prirodzene predpokladá aj potrebu zvyšovania vzdelanosti v tejto oblasti ako na úrovni bežných používateľov v pracovnom i domácom prostredí, tak aj na úrovni profesionálov so zameraním na budovanie a riadenie procesov informačnej bezpečnosti.

Práve potreba zvyšovania bezpečnostného povedomia a najmä potreba jej dynamizácie nás v rámci aktivít nášho občianskeho združenia viedla k rozhodnutiu podporiť a zmanažovať vydanie ďalšej publikácie z našej série bezpečnostnej literatúry určenú pre 1. ročník gymnázií a stredných škôl.

Veríme, že bude silným základom pre tak potrebnú zmenu vzdelávania v oblasti informačnej a kybernetickej bezpečnosti a zároveň kvalitnou pomôckou pre pedagógov.

Prajem Vám príjemné a poučné čítanie

Ing. Jaroslav Oster

predseda správnej rady OZ Preventista.sk

E L E K T R O N I C K Á K N I H A

Učebnica Informačnej bezpečnosti

pre stredné odborné školy a gymnáziá

prvá časť

Marek Zeman

Miroslav Blšák

Jaroslav Oster

Daniel Chromek

Autori

Mgr. Marek Zeman, PhD. CRISC

Zameriava sa na riadenie Informačnej bezpečnosti a vzdelávanie informačnej bezpečnosti. Technická špecializácia: bezpečnosť nových technológií, umelej inteligencie a biometrických systémov.

Mgr. Miroslav Blšák

Učiteľ matematiky a informatiky. Venuje sa zatraktívneniu edukačného procesu implementáciou informačných a komunikačných technológií do vzdelávania.

Ing. Jaroslav Oster

Venuje sa problematike vzdelávania v témach Informačnej bezpečnosti a prevencie počítačovej kriminality. Špecializuje sa tiež na problematiku forenzie a digitálnej stopy.

Mgr. Daniel Chromek CISA, CISM, CISSP, MBCI

Manažér informačnej bezpečnosti. Špecializuje sa na riadenie rizík a súlad s normami v oblasti informačnej bezpečnosti.

Recenzenti:

prof. Ing. Ivan Kotuliak, PhD.

JUDr. RNDr. Pavol Sokol, PhD.

Jazyková korektúra:

PhDr. Slavka Dudášová

PaedDr. Katarína Valičková, MBA

Vydavateľ: OZ Preventista - združenie pre bezpečnosť a prevenciu

Vydanie: prvé

Rok vydania: 2021

V knihe boli použité ilustrácie zo systému canva.com

ISBN: 978-80-972100-6-9

EAN: 9788097210069

Použité ikonky:

 Úloha

 Príklad

 Pojem

 Zaujímavý fakt

 Zhrnutie hlavných myšlienok

Obsah

1. Namiesto úvodu 12

1.1. Európsky digitálny compas 13

1.2. Čo sa deje vo svete? 15

1. Ransomware útok na firmu Garmin 19
2. British Airways napadli hekeri 21
3. Útoky na najvyššej úrovni 22
4. Ukradnuté dáta zo sociálnej siete 23

1.3. Manipulatívne techniky 24

1. Sociálne inžinierstvo 25
2. Príklady útokov 27

1.4. Zásada dobrého mena „na nete" 29

1. Digitálna identita 29

2. Informačná verzus kybernetická bezpečnosť 35

1. Disruptívny rozvoj 40
2. Dáta a informácie 44

2.2. Kybernetická bezpečnosť 45

2.3. Internet, ďalší priestor pre život 47

2.4. Záznamy internetových aktivít 49

1. Cookies - dáta, ktoré nás poznajú 50
2. Logovanie systémov a aplikácií - nezmazateľná stopa 52
3. Logovanie zmien v systéme 53
4. Logovanie práce v aplikáciách 55
5. Spracovanie logovacích záznamov 55
6. Digitálna stopa 56
7. Čo robiť, aby sme boli pred uchovávaním digitálnej stopy chránení? 59

2.5. Nekonečná virtuálna realita 66

2.6. Informačná bezpečnosť 67

2.7. Princípy informačnej bezpečnosti 68

1. Princíp: Need to know (Nevyhnutné vedieť) 69
2. Princíp: Need to do (Nevyhnutné spracovávať) 69
3. Princíp: Čo nie je zakázané je povolené 70
4. Princíp: Kontrola štyroch očí 70

2.8. Triáda CIA (dôvernosť, integrita, dostupnosť) 71

2.9. Prvky informačnej bezpečnosti (ľudia, technológie, procesy) 73

2.10. Ľudia 73

2.11. Technológie 74

2.12. Procesy 75

2.13. Riziko, aktívum, zraniteľnosť 78

2.14. Životný cyklus a kontrola bezpečnosti 82

3. Bezpečnostné štandardy a ochrana osobných dát.....86

3.1. Bezpečnostné štandardy 87

3.2. Kybernetická bezpečnosť na Slovensku 88

3.3. Osobné údaje 90

1. Ako si môžeme chrániť osobné údaje? 94
2. Čo nám hrozí, ak sa citlivé informácie prezradia? 94
3. Ako sa máme brániť? 95
4. Príklady zo života 96

3.4. Správanie na sociálnych sieťach 100

1. Odporúčania pre sociálne siete 101
2. Aplikácie a členstvo v skupinách nie je zadarmo 103
3. Ako sa správať na internete 104
4. Útočníci, útoky a obrana na sociálnych sieťach. 105
5. Správanie sa v diskusiách 107
6. Nebezpečenstvo číhajúce na sociálnych sieťach 110

3.5. Počítačová kriminalita 110

4. Ochrana počítača 113

4.1. Čo je počítač 113

4.2. Typy útokov 115

1. Útoky zamerané na hardvér 119
2. Škodlivý softvér 120

4.3. Zraniteľnosti a záplaty 124

1. Prečo útočníci zneužívajú zraniteľnosti? 125
2. Záplaty 126
3. Manažment záplat 126

4.4. Web a prehliadač 127
1. Čo je to doména a prečo je to dôležité? 127
2. Od domény k webu 130
3. Vyhľadávací systém (search engine) 144

4.5. Email 146
1. Doručenie elektronickej pošty 147
2. Autentickosť 148
3. Dôvernosť a integrita elektronickej pošty 150
4. Výber poskytovateľa elektronickej pošty 152
5. SPAM 153
6. Hoax 156
7. Phishing 162

4.6. Súkromie v kybernetickom priestore 167
1. Cookies 169
2. Zachovanie súkromia 170

4.7. Heslá 174

4.8. Multifaktorová autentizácia 181
1. Praktické spôsoby MFA 182
2. Útoky na MFA 185

4.9. Ochrana a starostlivosť o počítač 188
1. Ochrana voči škodlivému softvéru pomocou antivírusu 188
2. Ochrana aplikovaním záplat 190
3. Ochrana pri prehliadaní webu 191
4. Ochrana voči spamu a phishingu 192
5. Súkromie 193

5. Ochrana mobilného telefónu 197

5.1. Aké údaje sú zaujímavé pre útočníkov? 198

5.2. Infiltrácie 201

5.3. Typy útokov na mobilné zariadenia 205
2. Bluetooth 211

5.4. Ochrana mobilného telefónu 214
1. Odhaľovanie zlého správania mobilného zariadenia 215
2. Riadenie bezpečnosti mobilného zariadenia 215

5.5. Správa systému a aplikácií 216
1. Záplaty 217
2. Rootkity 218

3. Lokalizácia strateného/ukradnutého mobilného telefónu 219
4. Zálohovanie, darovanie mobilného telefónu a cloud..... 221

5.6. Zhrnutie - ochrana mobilného zariadenia 223

6. Namiesto záveru..... 225

7. Otázky pre testovanie znalostí..... 226

8. Správne odpovede testov..... 244

9. Literatúra..... 245

9.1 Zoznam použitých kníh..... 245

9.2 Odporúčaná literatúra..... 245

Vítame vás pri čítaní knihy, v ktorej sa naučíme spoznať tajomstvá Informačnej bezpečnosti. V tejto kapitole si vysvetlíme dôležitosť informačnej bezpečnosti a jej postavenie v Európskej únii. Spomenieme hrozby, ktoré boli naplnené a súviseli s útokmi na informačné technológie. Útoky zamerané na technológie je možné rozšíriť o útok na človeka, ktorý digitálnu technológiu ovláda, či už počítač, alebo mobil. Ako to útočník môže využiť sa dozvieme v kapitole Manipulatívne techniky. Koniec kapitoly je venovaný návykom, ktoré nás ochránia či už pred zlým správaním na internete, alebo aj pred tým, aby sme pomohli útočníkom.

Európsky digitálny kompas

Keď sa pozrieme okolo seba, vidíme všadeprítomné digitálne technológie, ktoré sa netýkajú len komunikačnej sféry, ale aj ďalších oblastí bežného života. Už to nie je len všadeprítomný mobil a počítač. Začali sme žiť v priestore sociálnych sietí, nakupujeme v internetových obchodoch, dokonca chladnička za nás vie objednať jedlo. Všetko toto sa mení prakticky zo dňa na deň. Takýto rozvoj technológií je rýchly a ťažko kontrolovateľný. Často vznikajú a zanikajú spoločnosti, ktoré majú obrovský vplyv v digitálnom svete. Vzhľadom na nekontrolovaný rast Informačno-komunikačných technológií (IKT) vo všetkých smeroch je veľmi ťažké držať pod

kontrolou toto bujnenie. Vlády majú na internetový priestor iba minimálny dosah, keďže hranice sú v digitálnom priestore stierané. Preto sa do ochrany zapája systém väčší ako sú jednotlivé štáty, a to je Európska únia (EÚ). EÚ používa pojem „**digitálna suverenita**". Tento pojem zahŕňa komplex vlastných pravidiel, jednotný digitálny trh, možnosť definovania vlastných rozhodnutí v digitálnom priestore a vytvárania vlastných riešení.

1.1. Európsky digitálny compas[1]

V súčinnosti sa s pojmom digitálna suverenita EÚ rozhodla vytvoriť Digitálny kompas a stanovila si ciele a ambície v rôznych oblastiach digitálneho priestoru, a to do roku 2030. Medzi hlavné otázky, ktorými sa dokument zaoberá, patrí:

- spracovanie údajov a umelá inteligencia,
- balík právnych predpisov o digitálnych službách, právny predpis o správe údajov.

Stratégia digitálnej transformácie

V súčasnosti sa zavádza pojem **digitalizácia života**, ktorá sa dotýka všetkých oblastí bežného života, práce, zábavy, štúdia. Digitalizácia riešení má vplyv na vývoj v oblasti pracovných miest. Niektoré vznikajú, iné zanikajú. Vzhľadom na uvedenú skutočnosť sa mení aj prístup ku vzdelávaniu. Dobre uchopené digitálne zručnosti znamenajú zvýšenú

[1] "Europe's Digital Decade: Digitally empowered Europe by 2030." [online]. [cit. 22.05.2021]. Dostupné na internete: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983.

konkurencieschopnosť pre kmeňových, ale aj potenciálnych zamestnancov. Priľnutie k digitálnym technológiám a inováciám, ktoré digitálne technológie prinášajú, vedie k zlepšeniu kvality života občanov a zvýšeniu ich konkurencieschopnosti na pracovnom trhu.

Vláda Slovenskej republiky má záujem zmeniť spoločnosť na digitálnu a tiež má záujem kontrolovať digitálny priestor. Z uvedeného dôvodu schválila uznesením č. 206/2019 zo dňa 7. mája 2019 rámcovú nadrezortnú Stratégiu digitálnej transformácie Slovenska 2030. Dokument sa opiera o transformáciu z industriálnej spoločnosti na informačnú spoločnosť. Tento dokument sa venuje predovšetkým inovatívnym technológiám. Patrí sem napríklad implementácia 5G mobilných sietí, internetu vecí, umelej inteligencie, analytického spracovania dát a iné. Jeho cieľom je podporiť podnikateľov i bežných obyvateľov a znížiť administratívnu záťaž na nich.

Vedieť ochrániť seba a svojich blízkych sa stáva najvyšším záujmom v čase digitálneho rozvoja. V dnešných dňoch nielen jednotlivé spoločnosti, ale aj každý z nás žije v neustálom riziku. Firmy sa obávajú napadnutia hekerom, napr. prienikom do systému, zničenia alebo ukradnutia dát. Zničenie dát môže znamenať koniec pre firmy, dokonca môže mať ohromný dopad na ľudské životy - napr. pokiaľ sa udeje v nemocnici alebo pri krádeži profilu na sociálnych sieťach.

Hrozby, ktoré na nás číhajú, sú obrovské, my však máme ochranné účinné nástroje. S pomocou týchto nástrojov vieme prežiť v *online* svete. Umeniu, ako prežiť v online svete a ako používať bezpečnostné nástroje, sa budeme učiť počas nasledujúcich rokov. Našou úlohou je priblížiť si a naučiť sa robiť jednotlivé kroky tak, aby

sme boli chránení a aby sme vedeli, ako robiť prirodzene preventívne kroky, ktoré nás chránia pred útokmi malvéru a hekerov. Budeme vedieť, ako sa správať a žiť v digitálnom svete bezpečne, pracovať s vybraným softvérom tak, aby sme vedeli chrániť seba, svoje zariadenia, svoju rodinu a zariadenia svojich blízkych.

Veríme, že naučené zručnosti vás posunú a budete sa vedieť nielen správne správať, ale aj chrániť svoje zariadenia a aj dáta, ktoré v nich máte uložené, pred zničením. Našim cieľom je, aby ste sa vedeli správať v online svete bezpečne a boli v ňom dobre chránení. Veríme, že potom budete vedieť odovzdávať svoje skúsenosti aj iným ľuďom.

- *Nájdite definíciu digitálneho priestoru.*
- *Ktoré oblasti zahŕňa Digitálny kompas, ktorý predložila EÚ v roku 2021 a čoho sa týka?*
- *Vytvorte analýzu a prezentujte ako, v akých oblastiach a prečo je potrebné znásobiť potenciál v digitálnej transformácii SR na základe dokumentu: Stratégia digitálnej transformácie Slovenska 2030.*

1.2. Čo sa deje vo svete?

Posledné roky sú zviazané s novými a novými útokmi. Informácie o úspešných útokoch k nám prichádzajú prakticky každý deň. Často sa zameriavame na škody, ktoré útok spôsobí a na hekerov, ktorí útok uskutočnili. Málokto sa zaoberá opatreniami, ktoré firmy urobili, aby takýto útok nenastal. Bezpečnosť digitálneho priestoru však zahŕňa aj aktivity, ktoré je potrebné robiť preventívne,

pred začatím útoku, nielen počas neho. Kybernetické útoky sú vedené neustále a veľká časť z nich je automatizovaná. Orientované sú na akýkoľvek cieľ. Nezáleží na tom, či ide o kritickú infraštruktúru štátu, softvér a hardvér firiem alebo o vaše mobilné zariadenie. Každá získaná informácia je zapísaná a neskôr využitá. Útoky sú v súčasnosti už zriedka jednoduché, zneužívajúce iba konkrétnu zraniteľnosť. Útočníci sa zameriavajú na komplexné riešenie, to znamená, že využívajú všetky dostupné komunikačné kanály od emailu, cez volanie, až po systém na posielanie správ. Komunikácia malvér je dobre ochránená a riadená cez internet a často si malvér vie vybrať z dostupných sietí a zamerať sa na dostupné zariadenia používateľa.

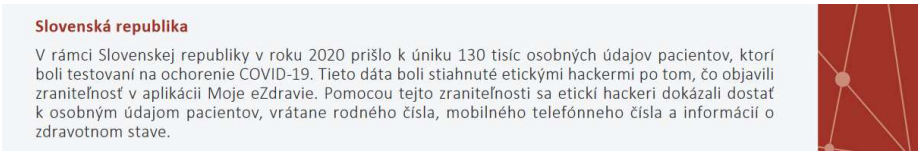
Malvér (malware): druh škodlivého kódu, ktorého hlavným cieľom je podporiť nekalý úmysel autorov malware a prevádzkovateľov. Zameriava sa na odcudzenie, zničenie, blokovanie dát alebo poškodenie zariadenia. Poznáme viacero typov malware napr. vírus, trójsky kôň, reklamný softvér, červ, špionážny softvér,...

Kto sú teda vlastne útočníci, ktorí nás neustále ohrozujú? Útočníci môžu mať rôzne podoby a delia sa podľa oblasti ich záujmov. Zoznam je veľmi pestrý, takže si predstavme tých najčastejších:

- **heker -** hľadá zraniteľnosti v zariadeniach a softvéroch a následne sa pomocou poznania zraniteľností snaží prelomiť obranu zariadenia a využiť dáta na zariadení a zariadenie samotné vo svoj prospech. Často preberá kontrolu nad zariadením. Konanie hekera môže byť aj etické, pokiaľ koná za účelom nahlásenia zraniteľnosti výrobcovi softvéru alebo hardvéru, a tým pádom zlepšenia bezpečnosti produktu.
- **podvodník** - je osoba, ktorá sa podvodom snaží vymámiť informácie alebo dáta od obete vo svoj prospech. Podvodník často manipuluje obeť, aby mu zároveň poskytla svoje služby v prospech podvodníka (napr. poskytnutie použitia bankového účtu).
- **organizované skupiny** - podvodníci sa môžu spájať do organizovaných skupín a vytvárať prostredie, kde kradnú dáta klientov. Tieto dáta následne zneužijú alebo ponúknu na

predaj (napr. podvodný obchod s obrovskými zľavami, alebo podvodná firma na ponúkanie údajov).

- **scriptkiddies** - heker, väčšinou začiatočník, ktorý používa nástroje naprogramované inými hekermi bez toho, aby im rozumel. Často sa dostane do nebezpečenstva sám, pretože použité aplikácie a scripty sú nebezpečné aj pre toho, čo ich spúšťa, ak sa nevie dostatočne ochrániť.
- **insider** - človek, ktorý je členom organizácie, alebo sa stane členom organizácie, ktorú chce poškodiť, môže byť sám alebo členom organizovanej skupiny. Následne spoznáva organizáciu a robí záškodnícku činnosť s cieľom preniknutia do najdôležitejších systémov, ukradnutia alebo poškodenia dát.
- **kybernetický predátor** (stalker) - zvyčajne anonymná osoba, ktorá obťažuje, vyhráža sa, či iným spôsobom prenasleduje obeť (napr. ohovára, uráža, krivo obviňuje, sleduje, nabáda k aktivitám so sexuálnym kontextom, …)[2].
- **(kyber)terorista** - vytvára kybernetické útoky s cieľom zastrašenia, vytvárania tlaku na vládu alebo tlaku na obyvateľstvo s cieľom podpory svojho politického alebo sociálneho kybernetického cieľa.



Informácia o odhalení možnosti ukradnutia osobných údajov hekermi z aplikácie eZdravie v roku 2020[3]

Do skupiny prenasledovateľov radíme aj útočníkov (sociálno-patologické osoby), často so psychickými poruchami, ktorí pôsobia negatívne na skupiny obyvateľstva alebo jednotlivcov. Vytvárajú

[2] Téme sa budeme podrobne venovať vo vyššom ročníku.
[3] SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE V ROKU 2020 [online]. [cit. 07.06.2021]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-2020.pdf

prostredie zastrašovania, prenasledovania a nahovárajú na ubližovanie sebe, okoliu, na vraždy a samovraždy.

Do nekalého správania sa zaraďujú aj firmy, ktoré bezohľadne predávajú svoje produkty predovšetkým ľuďom s nízkou počítačovou gramotnosťou. Príkladom sú bezpečnostné firmy, ktoré motivujú nekonečnými reklamami a pobádaním zákazníka nainštalovať desiatky svojich ochranných softvérov, bez ohľadu na reálne potreby zákazníka a jeho schopnosti využiť všetky služby, pričom následne žiadajú platby za poskytnutý softvér.

Vytvorte štruktúrovanú tabuľku s údajmi tak, aby boli porovnané spôsoby vedenia útokov a ciele útočníkov.

Predstavili sme si rôzne druhy útočníkov. Neskôr sa v knihe dozviete o rôznych druhoch útokov. Teraz si predstavme ten, ktorý bol použitý v prvom: ransomware. Príklady, ktoré budú nasledovať nevyužívajú len ransomware, ale sú pri nich použité rôzne typy zraniteľností systémov a aplikácií a aj dôverčivosť ľudí, pričom škodlivý kód kradol alebo zneprístupňoval údaje firiem.

Ransomware je škodlivý softvér (malware), ktorý dokáže zablokovať počítač s možnosťou odblokovania po zaplatení výkupného. Zvyčajne zablokovanie predstavuje zašifrovanie dát v počítači neznámym kľúčom alebo zablokovaním celého počítača, napr. uzamknutím obrazovky.

Slovo ransomware je zložené zo slova ransom - výkupné, žiadať výkupné a z konca slova software „ware". Blokovanie počítača ransomware bez šifrovania sa považuje za jednoduchý a ľahko prekonateľný hack. Po uzamknutí počítača ransomware oznámi používateľovi, kde a akým spôsobom musí zaplatiť výkupné a akým spôsobom bude počítač odomknutý. Často sa stáva, že zločinci šifrujú disky len jednosmerne, kvôli chybe v programe alebo úmyselne. Dáta po zašifrovaní sú nenávratne stratené. Prípadná platba výkupného preto nemá význam.

Ochrana pred ransomware prebieha na viacerých úrovniach, od zvyšovania bezpečnostného povedomia zamestnancov, cez

kvalitné a časté zálohovanie dát, nasadzovanie softvérových záplat, až po implementáciu viacvrstvového bezpečnostného riešenia.

Príklady ransomware:

- Diskcoder ransomware zašifruje celý disk a zamedzí používateľovi prístup k operačnému systému.
- Screen locker zablokuje prístup k obrazovke zariadenia.
- Crypto-ransomware zašifruje dáta uložené na disku obete.
- PIN locker sa zameriava na zariadenia so systémom Android a mení prístupové kódy s cieľom „vymknúť“ používateľov z ich zariadení.[4]
- Fusob - napáda smartfóny so systémom Android, iOS. Po inštalácii skontroluje jazyk zariadenia. Ak má používateľ nastavený ruský jazyk, alebo akýkoľvek jazyk z východnej Európy, Fusob sa odinštaluje.[5]

Pripomeňme si niektoré útoky:

1. Ransomware útok na firmu Garmin

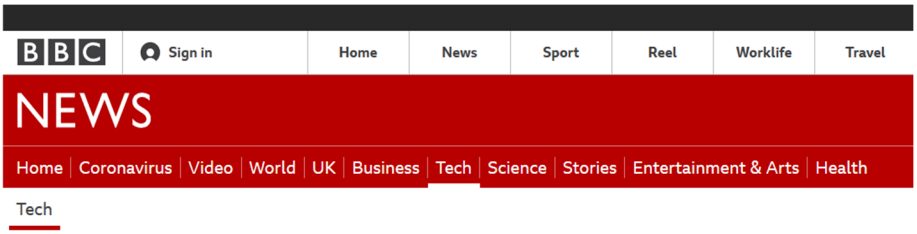
23. júla 2020 prístroje, ktoré zaznamenávajú športové aktivity a plnohodnotnú funkčnosť leteckých navigácii prestali pracovať online a prepli sa do offline módu. Podľa ZDNet napadol internú sieť a výrobné systémy spoločnosti Garmin ransomvér označený ako WastedLocker, ktorý blokuje a šifruje cieľové zariadenia a žiada výkupné. Za týmto ransomware stála ruská hekerská skupina Evil Corp., ktorá žiadala za odblokovanie 10 miliónov dolárov. Majitelia zariadení, ktorí využívali službu Garmin Connect, oficiálny web spoločnosti, aplikáciu pre smartfóny či aktualizácie máp a ďalšie serverové aplikácie, tieto služby nemohli používať. Útok taktiež ovplyvnil call centrá firmy, emailové schránky a zákaznícku podporu.[6]

[4] Ransomware [online]. [cit. 19.6.2021].Dostupné na internete: https://www.eset.com/sk/ransomware/

[5] Ransomware [online]. [cit. 19.6.2021].Dostupné na internete: https://sk.wikipedia.org/wiki/Ransomware

[6] Garmin oficiálne priznal útok hekerov, no žiadne dáta ľudí neunikli. Ktoré služby teraz fungujú? [online]. [cit. 16.5.2021].Dostupné na internete:

Ransomware prenikol do systémov pomocou kliknutia na linku v podhodenej emailovej správe. Podľa internetových médií spoločnosť požadované výpalné uhradila.



Oznam o začatí opravy dát v spoločnosti Garmin po úspešnom ransomware útoku[7]

Vysvetlite, prečo je zlé a nebezpečné uhrádzať výkupné hekerom? Zamyslite sa, či existuje situácia, kedy je vyplatenie výkupného nevyhnutné alebo akceptovateľné.

Nájdite na webe: ako funguje ransomware?

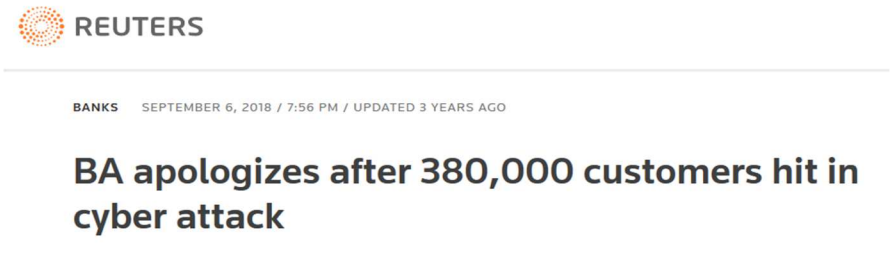
https://fontech.startitup.sk/garmin-priznal-utok-hackerov-no-ziadne-data-ludi-neunikli-ktora-sluzby-teraz-funguju/

[7] Garmin begins recovery from ransomware attack [online]. [cit. 30.5.2021].Dostupné na internete: https://www.bbc.com/news/technology-53553576

2. British Airways napadli hekeri

Asi 380 tisícom zákazníkov British Airways, ktorí si v ostatných týždňoch objednávali letenky na webstránke týchto britských aerolínií, hekeri možno odcudzili finančné i osobné údaje. Krádeže sa dotkli objednávok vykonaných medzi 21. augustom a 5. septembrom 2018, informovala letecká spoločnosť International Airlines Group (IAG), vlastník British Airways.

„*Vieme, že údaje, ktoré boli ukradnuté sú: meno, adresa, e-mailová adresa a údaje z kreditnej karty: ako jej číslo, platnosť, a trojmiestny kód na zadnej strane*“. Hekeri prenikli i do mobilnej aplikácie spoločnosti, ale nedostali sa k údajom z cestovných pasov. British Airways o útoku informovali už vo štvrtok večer a upovedomili o ňom svojich zákazníkov. Prienik hekerov odhalili až 5. septembra a podľa vedenia sa ho následne podarilo zastaviť.[8]


REUTERS

BANKS SEPTEMBER 6, 2018 / 7:56 PM / UPDATED 3 YEARS AGO

BA apologizes after 380,000 customers hit in cyber attack

Informácia o útoku na British airways[9]

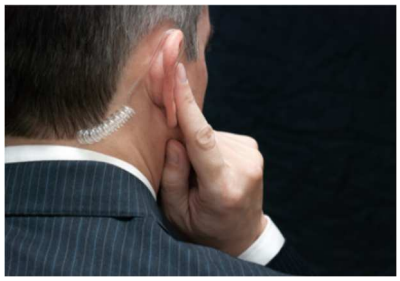
[8] British Airways napadli hekeri, ukradli údaje o 380-tisíc kreditkách [online]. [cit. 18.5.2021]. Dostupné na internete: https://www.trend.sk/biznis/british-airways-napadli-hackeri-ukradli-udaje-380-tisic-kreditkach

[9] BA apologizes after 380,000 customers hit in cyber attack [online]. [cit. 18.5.2021]. Dostupné na internete: https://www.reuters.com/article/us-iag-cybercrime-british-airways-idUSKCN1LM2P6

Ako by ste sa zachovali, keby ste boli manažérom British Airways?

Ako by ste presvedčili zákazníkov, že po tomto incidente majú stále využívať vaše služby?

3. Útoky na najvyššej úrovni



Izraelská tajná služba podľa všetkého spáchala kybernetický útok na jadrové prevádzky v iránskom Natanze. Teherán hovorí o teroristickom útoku začiatkom roka 2021.

Iránske jadrové zariadenie v Natanze malo vážne problémy, hovorí sa o úplnom výpadku dodávky elektrickej energie (blackout). Izraelský verejnoprávny rozhlas citoval zdroje z prostredia tajných služieb, podľa ktorých išlo o úmyselný „kybernetický útok, do ktorého bol zapojený Mosad […], škody na iránskom zariadení sú väčšie, ako informoval Teherán". Útok prerušil napájanie zariadenia a spôsobil výpadok prúdu, uviedol predtým pre štátne médiá hovorca Iránskej organizácie pre atómovú energiu Behrouz Kamalvandi. Ali Akbar Salehi, šéf Iránskej organizácie pre atómovú energiu, označil túto udalosť za „jadrový terorizmus".[10]

[10] Mosad spáchal kybernetický útok na kľúčovú jadrovú prevádzku v Iráne [online]. [cit. 18.5.2021].Dostupné na internete: https://dennikstandard.sk/58541/mosad-zautocil-na-iran-kyberneticky-utok-vyhodil-elektrinu-v-jadrovom-zariadeni/

The Washington Post
Democracy Dies in Darkness

PowerPost • Analysis

The Cybersecurity 202: Hacking tensions with Iran are surging again after nuclear site fire

By Joseph Marks
Anchor of The Cybersecurity 202 newsletter

July 6, 2020 at 2:01 p.m. GMT+2

Informácia o útoku na Iránske nukleárne zariadenia[11]

Zamyslite sa nad tým, ako vysvetlite, prečo je dôležité, aby v prípade 1.2.3 zostali pôvodcovia útoku v utajení, a prečo je dôležité, aby aj dôsledky útokov v tomto prípade zostali v utajení?

4. Ukradnuté dáta zo sociálnej siete

Neznáma osoba zverejnila začiatkom roka 2021 na hekerskom online fóre údaje 533 miliónov používateľov online služby Facebook. Zverejnené dáta, okrem telefónnych čísel, obsahujú identifikačné údaje pre Facebook, celé mená, lokality, dátumy narodenia, životopisné údaje a v niektorých prípadoch aj emailové adresy. Údaje boli ukradnuté ešte v roku 2019 zneužitím technického nedostatku Facebooku. Následne sa objavili ponuky rôznych robotov, ktorí vedia pracovať s týmito dátami, analyzovať ich a vyťažiť z nich veľmi kvalitné výsledky.[12]

[11] The Cybersecurity 202: Hacking tensions with Iran are surging again after nuclear site fire [online]. [cit. 18.5.2021].Dostupné na internete: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/07/06/the-cybersecurity-202-hacking-tensions-with-iran-are-surging-again-after-nuclear-site-fire/5f0232eb88e0fa7b44f6defd/

[12] Únik z Facebooku: Na webe sú telefónne čísla, e-maily aj ďalšie dáta pol miliardy ľudí [online]. [cit. 18.5.2021].Dostupné na internete: https://zive.aktuality.sk/clanok/151936/unik-z-facebooku-na-webe-su-telefonne-cisla-e-maily-aj-dalsie-data-pol-miliardy-ludi/

- *Na čo sa dajú využiť dáta, ktoré útočníci ukradli?*
- *Aké odporúčania navrhujte, aby ste do budúcna znížili škody z takéhoto úniku?*

- *Nájdite podobné príbehy, ktoré sa stali a ktoré sa týkali*
  - *ukradnutia dát alebo*
  - *napadnutia firmy cez ransomware alebo*
  - *úspešného napadnutia a dočasného znefunkčnenia sociálnych sietí alebo*
  - *ukradnutia dát zo sociálnych sietí.*

1.3. Manipulatívne techniky

Jednou z metód útokov využívaných útočníkmi sú aj tzv. manipulatívne techniky často označované aj ako metódy sociálneho inžinierstva .

Základným princípom tohto útoku je identifikovanie formy komunikácie medzi útočníkom a potenciálnou „obeťou", ktorou je „obeť" vhodným spôsobom motivovaná, aby vykonala nejakú aktivitu, ako napríklad:

- poskytnutie osobných údajov, ktoré môže útočník následne zneužiť,
- poskytnutie finančnej pomoci,
- zaplatenie domnelej pokuty, výkupného alebo platby za domnelú službu,
- kliknutie na link/prílohu v e-mailovej správe spôsobujúcej zavlečenie infiltrácie (ransomware) do počítača,
- poskytnutie súčinnosti útočníkovi, napríklad sprístupnením počítača prostredníctvom vzdialenej správy.

1. Sociálne inžinierstvo

Sociálne inžinierstvo patrí medzi manipulatívne techniky, pretože primárnym cieľom je netechnickými prostriedkami oklamať obeť. Prostredníctvom klamstiev a detailného popisovania fiktívnych aktivít útočník navedie obeť tak, aby porušila aj elementárne zásady bezpečnosti.

„*Sociálne inžinierstvo je jedným z najnebezpečnejších spôsobov útoku, napriek tomu, že nevyžaduje veľké technické zručnosti, je zamerané na človeka. Heker využíva inteligenciu a znalosť osobnosti človeka.*"[13]

Počas útoku pomocou sociálneho inžinierstva sa využívajú poznatky a vedomosti o vlastnostiach ľudí, ktoré sú pokladané za tzv. dobré (často používaný pojem „kognitívne chyby úsudku"), napríklad:

- neistota, konanie v časovom strese,
- netrpezlivosť,
- nesústredenosť,
- dôverčivosť,
- ľútosť,
- láskavosť,
- zvedavosť,
- ochota pomáhať,
- podpora vzťahov,
- podvolenie sa autorite,
- ochrana svojej bezúhonnosti,

[13] Zeman, M. (2019): Odborná príručka pre učiteľa, Podporná literatúra pre didaktiku informačnej bezpečnosti pre 5 ročník ZŠ; Preventista.sk; ISBN: 978-80-972100-2-1. str. 23

- obava z dôsledkov konania (niečo som neurobil),
- dôvera v technické vymoženosti a dôvera v internetový obsah /internetovú komunikáciu,
- snaha o zlepšenie svojho sociálneho statusu (tzv. pasívny alebo bezprácny príjem, ponuka na dedičstvo, pracovná ponuka, ponuka na zhodnotenie úspor a ďalšie motívy).

Hlavné metódy práce manipulatívnych techník sociálneho inžinierstva:

- **Silný afekt.** Ak obeť cíti silný hnev alebo je prekvapená, rozrušená, či v panike, bude s menšou pravdepodobnosťou rozmýšľať o prezentovaných argumentoch.
- **Preťaženie.** Útočník v rýchlom slede odovzdá množstvo informácii naraz, pričom zahltí obeť a tá nevie rozlíšiť reálne predpoklady od mylných, ale presvedčivých banalít. Obeť radšej absorbuje informáciu, akoby ju mala vyhodnotiť.
- **Opätovanie resp. Reciprocita**. Útočník presvedčí obeť, že jej niečo dal a vyžaduje spätne danú vec. Obeť často nevie rozlíšiť alebo nerozlišuje, že dar bol vynútený, a že „vrátená" vec je má oveľa vyššiu hodnotu.
- **Klamlivé vzťahy.** Útočník nadviaže kontakt s obeťou a komunikáciu nastaví tak, aby obeť uverila, že má s útočníkom podobné vlastnosti. Obeť bude cítiť silnú potrebu komunikovať a jednať s útočníkom kladne a dôverovať mu bez opodstatneného dôvodu.
- **Rozšírenie zodpovednosti a morálnej povinnosti.** Obeť je zmanipulovaná spôsobom, že nadobudne presvedčenie, že svojou činnosťou a rozhodovaním ovplyvní úspech či zlyhanie spoločnosti.
- **Autorita.** Útočník sa vydáva za vysoko postavenú osobu, tak dokáže zmanipulovať obeť, ak táto nevyužije možnosť overiť si identitu útočníka.
- **Bezúhonnosť a dôslednosť.** Zamestnanci majú sklon pokračovať v práci na pracovisku a plniť pridelené úlohy, aj keď majú podozrenie, že požiadavka nie je oprávnená. [14]

Existuje veľké množstvo typov útokov, ktorých podstatou je sociálne inžinierstvo. Veľmi nebezpečné sú najmä tie, ktoré spájajú

[14] Zeman, M. (2019): Odborná príručka pre učiteľa, Podporná literatúra pre didaktiku informačnej bezpečnosti pre 5 ročník ZŠ; Preventista.sk; ISBN: 978-80-972100-2-1. str. 28-30, skrátené.

manipulatívne praktiky s technickým útokom. Podrobne sa téme budeme venovať v 2. ročníku.

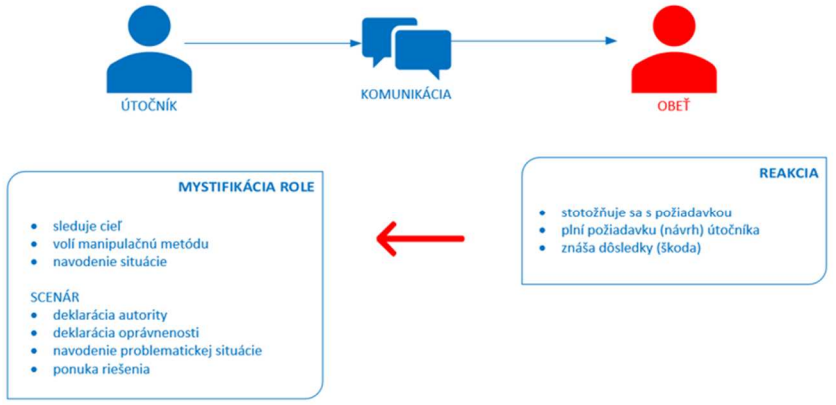
Vymyslite príklady, ako by mohli útočníci využiť metódy sociálneho inžinierstva v prípade vami používaných sociálnych sietí.

Navrhnite spôsoby ochrany, ako rozoznať manipulatívne techniky a ako sa proti nim brániť.

2. Príklady útokov

Komunikácia útočník - obeť

- útočník vždy volí takú formu komunikácie, aby jej obsah dokázal „upútať" pozornosť potenciálnej obete a motivoval ju k vykonaniu požiadavky (viď obr. *Scenár manipulatívnej komunikácie zameranej na získanie dôvery*)

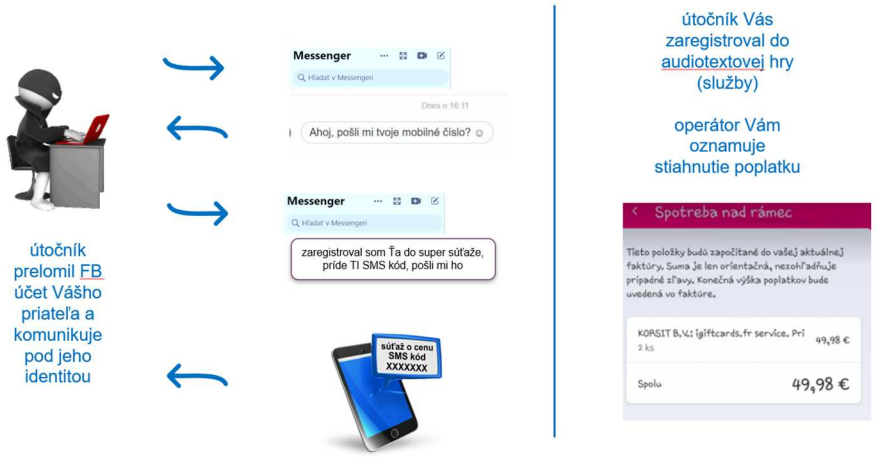


Scenár manipulatívnej komunikácie zameranej na získanie dôvery[15]

Zneužitie dôvery v rámci Facebook priateľstva:

[15] Manipulácie naše každodenné..., [online]. [cit. 14.6.2021]. Dostupné na internete: https://www.infoconsult.sk/n/manipulacie-nase-kazdodenne-alias-viem-kam-si-sa-pozeral

- útočník získava neoprávnený prístup ku profilu používateľa vystupujúceho ako FB priateľ obete (prelomením účtu, získaním uniknutých údajov o prístupe k FB profilom),
- komunikovaním prostredníctvom FB Messenger s obeťou (komunikáciu obeť vníma ako rozhovor so svojim FB priateľom) získava informácie potrebné pre zaregistrovanie obete do audiotextovej hry,
- obeť je, bez toho, aby o tom vedela, zaregistrovaná do audiotextovej hry (služby) a poplatky sú zaúčtované v najbližšej zúčtovacej faktúre od používateľa.



Schematické znázornenie priebehu útoku so zneužitím dôvery FB priateľa[16]

Ochrana pred tým, aby sme sa dostali na zoznam obetí podobných útokov, cez sociálne siete, tkvie vo vedomosti (uvedomení si): **Neposkytovať žiadne citlivé, hlavne osobné alebo bankové!**

[16] Oster, J. (2020): článok Podvod s telefónnym číslom na FB [online]. [cit. 14.10.2020]. Dostupné na internete: https://www.infoconsult.sk/n/podvod-s-telefonnym-cislom-na-fb

1.4. Zásada dobrého mena „na nete”

Informácie o vás na internete sú dlhodobo dohľadateľné (je ich možné vyhľadať) a zvyšku sveta povedia to, čo je o vás dôležité. Ľudia na internete trávia hodiny a často zisťujú o iných osobách ich osobné údaje. Následne sú tieto údaje často zneužité v neprospech ich vlastníkov. Aby bol človek čo najviac chránený, je vhodnejšie zanechať pozitívny obsah v rámci služieb internetu a obmedziť množstvo osobných údajov o sebe. Pamätajte si, že ak je raz informácia na internete, bude tam navždy.

Komunikačný reklamný banner Európskej digitálnej identity[17]

1. Digitálna identita

Digitálna identita sa chápe a používa v rozličných podobách.

- Digitálna identita je súbor elektronických informácií používaných na identifikáciu užívateľa v operačnom systéme a aplikáciách. Tieto informácie jednoznačne, nezameniteľne určujú konkrétneho užívateľa. Pozostáva z certifikátu obsahujúceho „verejný kľúč“, ktorý je možné zobraziť a zo „súkromného kľúča“, ktorý je uchovaný v tajnosti.[18]

[17] Digitálna identita pre všetkých Európanov [online]. [cit. 18.8.2021]. Dostupné na internete: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_sk#digitlna-identita-pre-vetkch-eurpanov

[18] Čo je digitálna identita? ..., [online]. [cit. 14.6..2021]. Dostupné na internete: https://support.apple.com/sk-sk/guide/mac-help/mchlp2695/mac

- Európska digitálna identita
    - je k dispozícii pre všetkých občanov EÚ, občanov s pobytom alebo podnikom v EÚ, ktorí ju chcú používať.
    - je použiteľná na identifikáciu osoby alebo na potvrdenie určitých osobných atribútov za účelom prístupu k verejným a súkromným digitálnym službám v celej EÚ.
    - umožňuje používateľom mať plnú kontrolu nad tým, ktoré aspekty svojej identity, údaje a certifikáty chcú poskytnúť tretím stranám a získať prehľad o tomto zdieľaní údajov.[19]
- Digitálna identita môže byť chápaná ako zoznam všetkých informácií o osobe (identite) v digitálnej podobe (napr. všetkých citlivých a osobných údajov, prístupových údajov, biometrická identifikácia, ...).
- Digitálna identita môže byť chápaná v ponímaní koncepcie stôp, t.j. zoznamu informácií o osobe (identite) v digitálnej podobe, ktoré zanechala v informačných systémoch. Môžu to byť priamo zmeny, ktoré daná identita robila, môžu to byť zaznamenané jednotlivé kroky, ale aj preferované správanie (behavioral scoring) v systémoch. Digitálna stopa nielen určuje človeka a to, čo robil, ale rovnako presne popisuje jeho správanie, preto je nevyhnutné tieto údaje chrániť.

Aké typy overenia používajú vami používané sociálne siete?

Ktoré typy overovania identity (klienta) pomocou biometrického overovania sa používajú v Slovenskej republike?

[19] Digitálna identita pre všetkých Európanov ..., [online]. [cit. 14.6..2021]. Dostupné na internete: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_sk#preo-je-to-potrebn

Napíšme si základné odporúčania pre uchovanie pozitívnej digitálnej stopy:

1. **Pozitívne informácie:** Píšte o sebe v pozitívnom duchu a nie úplne podrobne. Zamerajte sa skôr na pozitívnu emóciu ako podrobný opis prostredia a zúčastnených.
2. **Nastavenie pravidiel:** Nastavte si pravidlá, čo, komu a ako budete publikovať (napr. rodine, kamarátom, všetkým ľuďom). Tieto pravidlá poctivo dodržiavajte, aby potenciálni prenasledovatelia nemali všetky vaše dáta ihneď k dispozícii.
3. **Podporte zážitok:** Podporte informácie zážitkovou fotkou. Vytvárajte fotku tak, aby z nej dýchal život, pohyb a nie detailný popis prostredia. Nebojte sa rozmazať fotku, znemožníte tým jednoduché sledovanie stalkerom.
4. **Odstraňujte negatíva:** Nájdite si na internetovom prehliadači výskyt svojho mena, pokúste sa vymazať negatívny obsah, alebo stránku nahláste. Rovnaký postup využite na sociálnych sieťach. V prípade, že na web alebo sociálnu sieť niekto „postol“ (zverejnil) trápnu fotografiu a označil vás, požiadajte ho, aby vaše meno vymazal, alebo nahláste fotku či údaj, aby bol vymazaný správcom. Ak ide o vaše duševné právo, podajte *DMCA* sťažnosť (*Digital Millenium Copyright Act* - zákon v americkom práve zaoberajúci a autorským právom v nových technológiách).
5. **Zlepšujte ochranu:** Sledujte si ochranu vašich osobných údajov na sociálnych sieťach. Tieto nastavenia sa pravidelne menia a rozširujú. Obmedzte každý údaj a prístupy na vaše stránky len na nevyhnutnú skupinu ľudí.
6. **Správni kamaráti:** Pravidelne kontrolujte ľudí, ktorých máte medzi priateľmi, či sa do zoznamu nedostal cudzí človek.
7. **Kontrolujte aplikácie na sociálnych sieťach:** Aplikácie, ktoré ste povolili alebo nainštalovali, majú často povolené prístupy v rámci vášho konta na sociálnej sieti alebo aj vo vašom zariadení (na kamery, mikrofón alebo k zemepisným údajom). Tieto prístupy je možné veľmi ľahko zneužiť. Pravidelne kontrolujte prístupy aplikácií a ak niektorú aplikáciu nepoužívate, vymažte ju.

8. **Vaše meno je vaša značka**. Dobré meno každého človeka je status, ktorý sa dlho buduje a ľahko stratí. Ako príklad si zoberme športové značky, ktoré budujú svoje meno na niekoľkých paralelných frontoch (oblastiach). Majú tovar, starajú sa o životné prostredie, cez svoje nadácie pomáhajú núdznym. Našou úlohou je rovnako kvalitne, neustále a pozitívne budovať svoje meno ako značku.

Dodržiavaním predchádzajúcich pravidiel zabezpečíte, aby útočník nevedel ľahko a presne identifikovať vás, vaše správanie, a aby celkový obraz o vás (vaša reputácia) vyznel pozitívne.

Reputácia je mienenie o niekom/niečom. Predpokladá sa existencia pozitívnej reputácie. Ako synonymá sa používajú spojenia „dobrá povesť“, „dobré meno“, „úcta“, „vážnosť“. Dobrá a kvalitná reputácia sa buduje dlhodobo. V prípade firmy je to veľmi dôležitý nástroj marketingu, ktorý nesie prísľub kvality a zodpovedného prístupu danej firmy. V prípade webovej stránky alebo profilu v rámci sociálnych sietí pozitívna reputácia znamená, že webová stránka, aj profil, vydávajú len overené správy a názory, resp. informácie na ich stránkach sú podložené overenými faktami.

Ktorý obrázok (fotografia) poskytuje viac informácií o rodine zabávajúcej sa v prírode? Ktorú fotografiu je podľa vášho názoru vhodnejšie, použiť na sociálnych sieťach? Vysvetlite dôvody.

obrázok A

obrázok B

obrázok C

- *Navrhnite pre vlastnú potrebu súbor pravidiel, ktoré je dobré dodržiavať pri práci so sociálnymi sieťami. Nastavte ich podľa sietí a aplikácii, ktoré používate.*

- *Navrhnite pre vlastnú potrebu súbor pravidiel, ktoré je dobré dodržiavať pri práci s internetom. Nastavte ich podľa sietí a aplikácii, ktoré používate*

- *Nájdite vo vašom mobilnom telefóne aplikáciu, ktorá nevyžaduje žiadne alebo len malé privilégia. Následne nájdite aplikáciu, ktorá vyžaduje najviac prístupov k jednotlivým informáciám (povolených privilégií) vo vašom mobilnom zariadení.*

- *Zamyslite sa, ktoré aplikačné prístupy viete odobrať, ak danú funkcionalitu v aplikácii nevyužívate.*

- *Pripravte prezentáciu, ako sa na vašej obľúbenej sociálnej sieti dá nahlásiť neželaná správa tak, aby bola neskôr vymazaná.*

- *Pripravte si návrh, ako budete budovať svoje meno ako značku.*

- *Aké sociálne siete používate a aké požadujú prístupy vo vašom mobilnom telefóne?*

Ktoré vyobrazenie pri prezentácií seba ako značky v rámci sociálnych by ste si vybrali? A ako vám pomôže tento obraz vo vašej budúcej profesii?

obrázok A

obrázok B

obrázok C

obrázok D

obrázok E

Žijeme v dobe, kedy sa aj od bežných ľudí vyžaduje ovládanie digitálnych zariadení minimálne na používateľskej úrovni. Inteligentné hodinky, mobily, tablety či iné zariadenia tvoria každodennú súčasť našich životov. Sústavné zlepšovanie a vývoj týchto inteligentných zariadení (smart devices) si vyžaduje aj zdokonalenie, resp. nadobudnutie určitých zručností ich používateľov. Komplexná znalosť používania prostriedkov na technickej aj softvérovej úrovni sa volá *digitálna gramotnosť.* Digitálna gramotnosť sa stáva v súčasnom svete nevyhnutnou pre uplatnenie sa na trhu práce.

Digitálna gramotnosť „*nespočíva len v technickom zvládaní úkonov a znalostí spojených s ovládaním jednej technológie, napr. počítača, je javom značne zložitým, pozostávajúcim z kompetencií spojených s technickým zvládnutím informačných a komunikačných technológií, schopnosti práce s digitalizovaným obsahom, schopnosti zvládnutia* ***bezpečného používania*** *digitálnych technológií, komunikačných zručností a schopností*“[20].

[20] KOLLÁR, Vojtech - POLAKOVIČ, Peter - GASPEROVÁ, Jana. Digitálna gramotnosť občana ako fenomén súčasnej informačnej doby. In Sustainability - Environment - Safety 2015. Medzinárodná vedecká konferencia. Sustainability - Environment - Safety 2015: recenzovaný zborník príspevkov z medzinárodnej vedeckej konferencie konanej 4. decembra 2015 v Bratislave. Žilina : STRIX, 2015. ISBN 978-80-89753-01-7, s. 137-140.

Ovládanie práce s médiami patrí medzi dôležitú súčasť digitálnej gramotnosti, ale nie je to jediná schopnosť, ktorú človek potrebuje. Rovnako dôležitou schopnosťou je vedieť média bezpečne používať. Prečo je to potrebné? Na internete sa nachádzajú osobné údaje, citlivé dáta, ako aj iné dokumenty, ktoré sú dôležité a v nesprávnych rukách by dokázali spôsobiť veľa škody.

Na to, aby sme vedeli popísať jednotlivé časti bezpečnosti, musíme si zadefinovať priestor, v ktorom budeme pracovať. Tento priestor sa nazýva **informačný systém**, ktorý zbiera, spracováva, udržuje a poskytuje informácie. Pod informačným systémom si môžeme predstaviť rôzne veci, ako napríklad nejaká aplikácia alebo služba, ktorá spracováva informáciu za nejakým účelom.

Práve kvôli dôležitosti správneho využívania digitálnych zručností v rámci zachovania určitej digitálnej bezpečnosti by sme radi upriamili pozornosť na pojmy ako **informačná bezpečnosť** a **kybernetická bezpečnosť**, s ktorými sa budeme v nasledujúcich kapitolách stretávať pomerne často.

Informačná bezpečnosť je často sa vyskytujúci a veľmi dôležitý pojem. Používa sa v rozličných významoch, a preto je aj zdrojom viacerých nedorozumení. Tento pojem môžeme vymedziť viacerými spôsobmi, napríklad ako:

- „*procesy a metodiky, ktoré sú navrhnuté a implementované na ochranu tlačenej, elektronickej alebo akejkoľvek inej formy dôverných, súkromných a citlivých informácií alebo údajov pred neoprávneným prístupom, použitím, zneužitím, zverejnením, zničením, modifikáciou alebo narušením*”[21],
- želaný stav riadenia a kontroly informácií,
- interdisciplinárna oblasť, ktorá sa zaoberá riadením mechanizmov ochrany dát a informácií tak, aby boli minimalizované riziká, ktoré na ne pôsobia,
- činnosť smerujúca k dosiahnutiu ideálneho stavu ochrany organizácie,

[21] SANS. Information Security Resources – information security [online]. [cit. 30.3.2021]. Dostupné na internete: https://www.sans.org/information-security

- v širšom zmysle - medziodborová vedná disciplína, ktorá sa zaoberá vývojom metód ochrany informácií a informačno-komunikačných technológií.

Bezpečnostná norma ISO 27002 definuje Informačnú bezpečnosť nasledovne: „*Informačná bezpečnosť sa dosahuje implementáciou vhodného súboru opatrení, ktorými môžu byť politiky, procesy, postupy, organizačné štruktúry a softvérové a hardvérové funkcie.*"

Predchádzajúce body predpokladajú, že informačná bezpečnosť nie je statický jav, ale je chápaná ako nekonečný proces zlepšovania. Zlepšovanie sa predpokladá na miestach, kde je to aktuálne nevyhnutné, alebo tam, kde predpokladáme, že to nevyhnutné bude. V súčasnom stave sa začína používať slovné spojenie ***holistický pohľad***. Holistický pohľad znamená komplexný/úplný pohľad na celkovú bezpečnosť firmy. Pracuje sa s predpokladom, že informačná bezpečnosť je systém, ktorým je možné vytvoriť koherentný (súvislý) ochranný celok implementovaním (zavedením, prijatím a následným používaním) určitých opatrení.

Informačná bezpečnosť je ovplyvnená niekoľkými zdrojmi požiadaviek:

- **Ciele a zameranie firmy** - firma si v rámci firemnej stratégie určí (definuje), akým spôsobom bude viesť biznis (podnikanie). Vzhľadom na zvolený typ podnikania bude firma musieť riadiť riziká vyplývajúce z danej stratégie, napr. škola si vedie záznamy o všetkých študentoch v papierovej podobe. Dokumenty sú uložené v samostatnej miestnosti, s obmedzeným prístupom, len pre zodpovedné osoby zo školy, aby boli chránené pred odcudzením a dokumenty sú chránené pred požiarom.
- **Aktívny risk management** - v rámci risk managementu sa vyhľadávajú a identifikujú riziká, ktoré hrozia organizácii. Po definovaní, odsúhlasení a ohodnotení rizík sa následne manažment organizácie rozhodne, akým spôsobom riziká odstráni alebo zníži, napr. ak firma vyvíja softvér, potom musí zabezpečiť, aby vývojári neodchádzali z firmy a mali vysoké

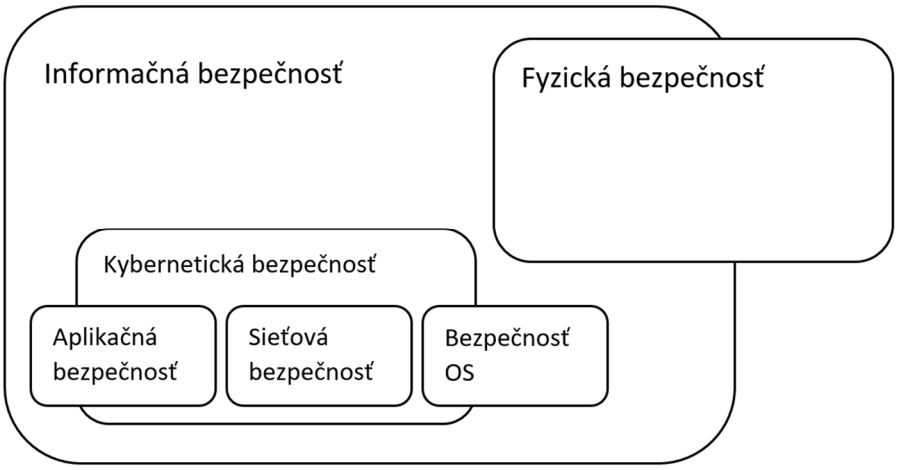
nasadenie, napríklad rôznymi benefitmi, ako sú príspevky na šport, časom na vzdelávanie alebo zdravotnými balíčkami.

- **Zákonné dôvody** - časť firiem na trhu je kontrolovaných a riadených zákonmi, ktoré vyžadujú dodržiavanie bezpečnostných požiadaviek. Často sú nariadenia zákonov prísnejšie ako bezpečnostné štandardy.
- **Požiadavky vyplývajúce z dodržiavania prijatých bezpečnostných štandardov.** Dodržiavanie bezpečnostných štandardov je zárukou pre odberateľov, že ich informácie a výsledky zakúpenej práce sú v bezpečí. Bezpečnostné štandardy majú tisícky požiadaviek na procesy, používateľov, aj systémy. Ich dodržiavanie môže byť v určitých situáciách v rozpore s cieľom podnikania. V takomto prípade je nevyhnutné hľadať dodatočné, ochranné riešenia a znižovať dopad vzniknutého rizika náhradnou ochranou. Príkladom môže byť riešenie, že prístup pre internetovú stránku firmy musí zostať otvorený, ale je nevyhnutné ochrániť komunikáciu nielen jedným, ale viacerými bezpečnostnými spôsobmi.
- **Požiadavky klientov a dodávateľov** - klienti a dodávatelia vytvárajú tlak na bezpečné služby, ktoré nakupujú od dodávateľov. Tieto služby musia byť chránené a monitorované podľa bezpečnostných štandardov a ich implementácia musí byť overená často nezávislým audítorom.

Audit predstavuje kritické skúmanie operácie, konkrétnej činnosti alebo všeobecnej situácie subjektu, ktoré sa spravidla opiera o stanovené a odporúčané normy a techniky príslušnej profesijnej organizácie. Je uskutočňovaný prostredníctvom preštudovania, kontrol alebo overovaní rozhodnutí a dokumentov manažmentu alebo ich zhody so zákonmi, normami alebo stanovenými pravidlami, a ktoré spravidla vedie k tomu, že audítor zostaví na konci audítorskej práce písomné oznámenie. V ňom uvedie svoj názor, stanovisko, záver alebo odporúčania či opatrenia, ktoré treba prijať. [22]

[22] Audit (fungovanie organizácie)[online]. [cit. 19.06.2021]. Dostupné na internete: https://sk.wikipedia.org/wiki/Audit_(fungovanie_organiz%C3%A1cie)

Kybernetická bezpečnosť je bezpečnosť zameraná **iba** na informačno-komunikačné technológie (IKT) a dáta v nich uložené a spracovávané. Môžeme povedať, že kybernetická bezpečnosť je podmnožinou informačnej bezpečnosti. Vzťah medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou znázorňuje nasledovný obrázok.



Základný rozdiel medzi spomínanými pojmami je v tom, že informačná bezpečnosť sa zaoberá materiálnou a aj virtuálnou povahou vecí, kým kybernetická bezpečnosť sa zaoberá len ich virtuálnou povahou.

Informačná bezpečnosť znamená zachovanie dôvernosti, integrity a dostupnosti informácií [ISO/IEC 27032, čl. 2.33]

Kybernetická bezpečnosť znamená zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore [ISO/IEC 27032, čl. 4.20]

Popíšte vzťahy jednotlivých typov bezpečností na predchádzajúcom obrázku.

Na základe vyššie písaných informácií rozdeľte nasledovné pojmy do dvoch kategórií: informačná bezpečnosť a kybernetická bezpečnosť a zapíšte výsledok do tabuľky:

pracovná zmluva, USB s dokumentmi, dokumenty v PC, ochrana tabletu, smartfón, elektronická triedna kniha, klasifikačný záznam, firemné aplikácie v mobilnom telefóne, vytlačená domáca úloha.

informačná bezpečnosť	kybernetická bezpečnosť

1. Disruptívny rozvoj

Digitalizácia preniká do všetkých oblastí spoločnosti, vo veľmi krátkej dobe vznikajú nové startupy, ktoré poskytujú služby v rámci celého sveta, komunikujeme online s dodávateľmi z rôznych krajín a kontinentov. Digitalizácia sa týka produktov, služieb, procesov, ovplyvňuje rozhodovanie a obchodné modely. Ako sa to premieta do bežného života? Napr. bolo vytvorené športové oblečenie obsahujúce snímače, ktoré posielajú nazbierané štatistiky na spracovanie do systémov spracúvajúcich veľké množstvo dát (big data systems). V systémoch je automaticky vyhodnocovaný nielen aktuálny zdravotný stav športovca, ale aj jeho pohyb. Tieto údaje sú kontrolované s nazbieranými historickými údajmi. Systém automaticky overuje nielen stav a kvalitu výkonu, ale rovnako vie identifikovať najlepší pohyb, ktorý následne tréner môže so športovcom korigovať.

Naša spoločnosť prechádza rozsiahlou zmenou. Táto zmena je naviazaná na digitalizáciu spoločnosti a neustály prísun nových

technológií, založených na digitalizácii. Zanikajú postupne celé odvetvia v priemysle a vznikajú úplne nové, menia sa zaužívané obchodné modely, a to všetko v stále kratšom a kratšom čase (prechod do cloudového prostredia, big data, robotika, autonómne autá či umelá inteligencia). Príkladom nových obchodných modelov je rast firiem ako Netflix, Spotify, či WhatsApp. Spomínané spoločnosti zmenili trh, našli nový pohľad na obchodnú stratégiu a vo veľmi krátkom čase nahradili pôvodné firmy. Napríklad firma WhatsApp zaznamenala disruptívny (rozvratný) rozvoj, keď posunula posielanie správ zo SMS (sú platené jednotlivo za zaslanú správu) do virtuálneho priestoru (platí sa za dátové pripojenie). Ďalšie rozšírenie firma zaznamenala, keď aplikovala rovnaký posun pre telefonické hovory. Takže zmeny v spoločnosti sú z tohto pohľadu vnímané nielen negatívne alebo pozitívne, ale hlavne progresívne.

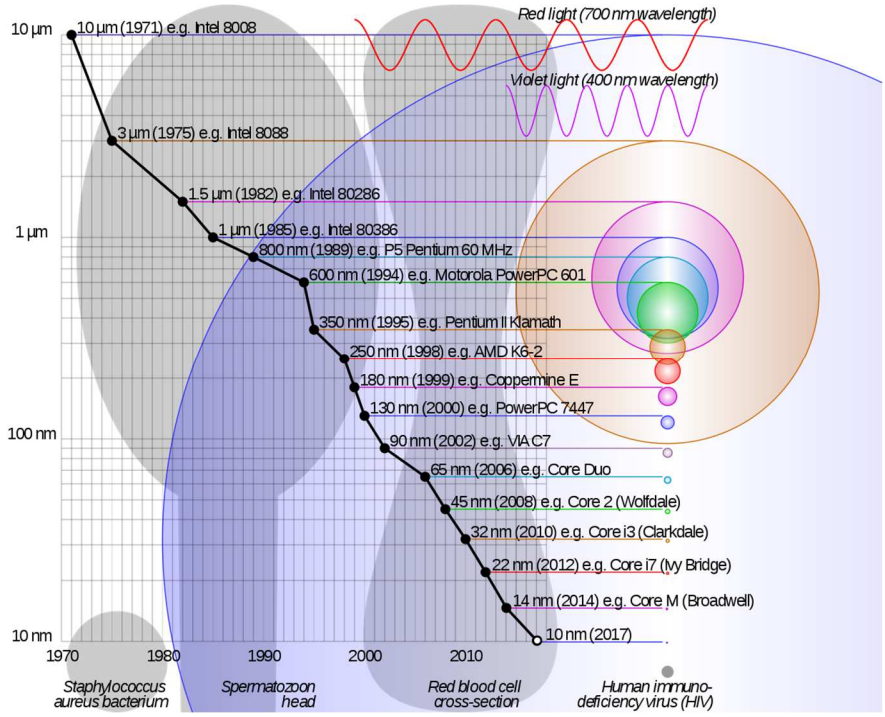
Zamyslite sa a popíšte, ako ovplyvnil disruptívny vývoj firmy WhatsApp operátorov telefonických služieb?

Nevyhnutnou súčasťou disruptívneho rozvoja je exponenciálny rast, pričom máme predovšetkým na mysli exponenciálny rast v informačných systémoch. Príkladom takéhoto rastu, ktorý sa dotýka priamo počítačov je Moorov zákon. Ide o empirické pravidlo, ktoré hovorí, že zložitosť integrovaných obvodov (počet tranzistorov integrovaných na nich) sa zdvojnásobuje približne každé dva roky.[23]

Exponenciálny rast sa netýka len digitálnej transformácie, ale aj ceny produktov a neustáleho zlacňovania a zmenšovania výpočtovej techniky. Ak by sme pred 20 rokmi chceli počítač s výkonom vášho smartfónu, zaplatili by sme milióny dolárov. Internet vecí (moderné prístroje ovládané na diaľku pomocou internetu) bol kedysi len hrubou predstavou, dnes je prirodzenou súčasťou nášho života, pričom každá jedna vec generuje dáta, ktoré je nevyhnutné

[23] Moorov zákon [online]. [cit. 30.3.2021]. Dostupné na internete: https://sk.wikipedia.org/wiki/Moorov_z%C3%A1kon

spracovať. Do budúcna predpokladáme ešte výraznejšie zlepšovanie a rozširovanie ich funkcionality. Príkladom sú *wearables (nositeľná elektronika na tele),* je orientovaná na špecifické veci ako je meranie tepu, tlaku, dychu, pohyb a iné. V budúcnosti sa predpokladá, že budú zbierať dostatočné množstvo dát, aby umelá inteligencia vedela identifikovať chorobu a mohla navrhnúť najefektívnejšiu liečbu.



Porovnanie rozmerov polovodičových spojov v procesore s mikroskopickými objektami (stafylokok, spermatozoid, červená krvinka a HIV vírus)[20]

Disruptívny vývoj znamená tiež spájanie rôznych odvetví. Na príklade wearables vidíme spojenie odevného priemyslu s vytvorením špeciálneho hardware a softvéru na spracovanie dát. Vytvárajú sa nové firmy (FinTech), ktoré vyvíjajú nové finančné riešenia, technológie a hľadajú úplne nové, vhodné obchodné modely pre tieto technológie na báze informačných technológií. Do budúcnosti bude

takýto typ rastu znamenať nielen zmenu charakteru a fungovania priemyslu a spájanie odvetví, ale aj veľké zmeny v spoločnosti. Nové prístupy narúšajú zabehané a spoločnosťou akceptované obchodné modely a pracujú na pravidlách mimo existujúcich hodnotových nastavení spoločnosti. Z tohto dôvodu sú nové pravidlá považované za neférové. Od zabehnutých firiem sa vyžaduje aktívne reagovanie na novovznikajúce situácie, neustále sa prispôsobovanie a upravovanie svojich výrobných a obchodných modelov. Takéto prispôsobovanie sa vyžaduje zo strany firiem veľa síl, neustály vnútorný vývoj a zároveň aj zmenu organizácie. Fintechy, ako modely, sú nestabilné a často rovnako rýchlo vznikajú ako aj zanikajú, pričom stiahnu so sebou aj pôvodné, zabehnuté firmy, ktoré sa nedokázali prispôsobiť trhu. Preto sa väčšina obyvateľstva pozerá na tento typ podnikania ako na neférové podnikanie, ktorého cieľom je zničenie zabehnutých obchodných konceptov.

Na druhej strane efektívnosť a celkový úspech nových obchodných modelov, ich cezhraničný dosah a znižovanie cien valcuje trh. Firmy, ktoré sa nevedia prispôsobiť, zanikajú, veľká časť sa preorientováva na inú časť trhu. Takýmto spôsobom sa z pôvodného malého startupu môže stať nadnárodný monopol. Monopolizácia trhu a platenie daní v krajine, kde existuje klientela, je významným motívom, prečo sa vlády jednotlivých štátov snažia kontrolovať tento priestor. Príčinou monopolizácie je aj vytvorenie pocitu, že klient dostane časť služieb zadarmo, to znamená, že používanie je v základnej forme bezplatné. Samozrejme, je to len pocit. Existujú rôzne formy ekonomiky tzv. zadarmo, napr. používateľ platí firme cez reklamu, ktorá sa mu zobrazuje alebo dostáva najnovšie produkty a je prvým testerom. Na druhej strane vznikajú celé komunity, ktoré si navzájom zdieľajú zdroje, vymieňajú vedomosti až na úroveň algoritmov aplikácií. Toto správanie vedie k významnému znižovaniu cien. Ďalším krokom vedúcim ku zlacneniu samotného vývoja a automatizovaniu zmien je crowdsourcing, ktorým dokážu firmy vybrať len tie najlepšie riešenia.

Crowdsourcing je novotvar na označenie spôsobu deľby práce, pri ktorom sa úloha, obvykle vykonávaná zamestnancom alebo kontraktorom v rámci outsourcingu, zadá bližšie nešpecifikovanej skupine ľudí ako všeobecná výzva. Napríklad sa verejnosť vyzve na spoluprácu pri vývoji novej technológie, uskutočnení dizajnérskej úlohy, zdokonalení algoritmu alebo pri pomoci so zachytením, roztriedením a analýzou veľkého objemu dát.[24]

Spomeňte mená aspoň 5 firiem, ktoré prešli disruptívnym vývojom a stali sa monopolnými vo virtuálnom svete a zistite koľko im to trvalo.

2. Dáta a informácie

Základnými prvkami informačnej bezpečnosti sú **dáta** a **informácie a znalosti**, ktoré chceme chrániť. Aj medzi týmito pojmami nachádzame rozdiely. Dáta nachádzame často vo forme čísla, znaku, symbolu, ktorý nám nedáva žiadny význam. V prípade, že dáta vložíme do kontextu, nadobúdajú zmysel a stávajú sa z nich **informácie**[25]. Informácie sú teda jeden alebo viac súvisiacich údajov. **Znalosti** sú komplexné informácie, postupy, ktoré prinášajú praktické využitie informácii, napríklad písanie návodu na bicyklovanie, čo vyžaduje nielen porozumenie jednotlivým informáciám, ale aj samotnému postupu bicyklovania a vyžaduje aj poznanie písanie návodov.

Príklad údajov: 4000, 27.3.1997, päť...

Príklad informácií: 4000 eur, dátum narodenia: 27.3.1997, päť stupňov…

[24] Crowdsourcing https://sk.wikipedia.org/wiki/Crowdsourcing
[25] MatLab FEI TUKE [online]. [cit. 30.3.2021]. Dostupné na internete: http://matlab.fei.tuke.sk/wiki/index.php?title=D%C3%A1ta,_inform%C3%A1cie,_znalosti

Zapíšte vo dvojiciach čo najviac údajov a informácií o škole. Čoho je viac, údajov alebo informácií? Vysvetlite dôvod.

Všeobecný cieľ informačnej bezpečnosti: Chceme, aby informácie boli

- k dispozícií v ľubovoľnom čase (vtedy, keď ich potrebujeme),
- spoľahlivé (na informácie sa môžeme spoľahnúť),
- sprístupnené len tomu, kto ich potrebuje a má na ne právo.

V ideálnom prípade sú údaje v plnej kvalite, úplnosti a kedykoľvek prístupné. Potrebujeme teda **chrániť** informáciu od jej vzniku (vytvorenia) až po jej zánik (zničenie).

Chrániť informáciu znamená zaistiť **dôvernosť údajov** (confidentiality), **integritu údajov** (integrity) a **dostupnosť údajov** (availability). Tieto pojmy patria k základným bezpečnostným požiadavkám. Zvyknú sa označovať ako triáda CIA (prvé písmená anglických ekvivalentov dôvernosti, integrity a dostupnosti).

Popíšte, ako sú zabezpečené a prečo sú dôležité jednotlivé prvky CIA pri ochrane triednej knihy, vysvedčenia, občianskeho preukazu a knihy „O psíčkovi a Mačičke".

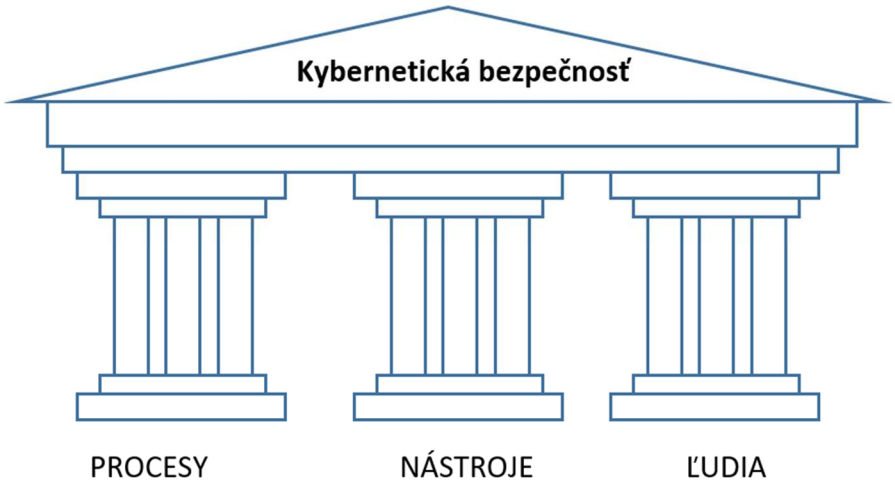
2.2. Kybernetická bezpečnosť

Je veľmi ľahké podľahnúť dobre pripraveným útokom. V úvodnej kapitole sme si predstavili príbehy, kde obeťami boli organizácie, ktoré míňajú milióny dolárov na ochranu. Napriek tomu podľahli pripravenému útoku. Nikto z nás neinvestuje takéto sumy do osobnej ochrany. Kybernetická bezpečnosť je zložená z dvoch základných pilierov: **procesov a nástrojov.** Procesy sú postupy, ktoré musíme dodržať na ochranu ľudí a zariadení. Vyžadujú si, aby sme sa ich nielen naučili, ale sa podľa nich aj správali. Zmena správania nie je ľahká, a preto jej budeme venovať zvyšok času, ktorý

spolu v škole strávime. Nástroje budú pre nás len cestou, spôsobom, ako naše zmenené a naučené správanie implementovať. Ideálna situácia nastane, ak sa oba piliere spoja do jedného veľkého, prirodzeného celku a naše správanie v digitálnej sfére bude nimi prirodzene podmienené.

Situácie, ktorým čelíme, sú stále nové a každou sekundou sa vyvíjajú. To, čo bolo postačujúce pred rokom, o rok už nestačí ani na základnú ochranu. Z tohto dôvodu neexistuje univerzálne riešenie a rovnako ani univerzálne spôsoby ochrany. Budú sa meniť podľa toho, akú situáciu budeme riešiť a aké dostupné nástroje budeme mať. Je nevyhnutné byť neustále pripravený na riešenie útoku alebo nebezpečenstva. Nástroje na obranu pred útokom sa každým dňom vyvíjajú, preto viac ako na naučenie konkrétnej funkcionality sa zameriame na procesy a dôvody existencie riešení vzniknutej situácie.

Čo máme teda robiť, ak neplánujeme míňať rovnakú sumu peňazí ako spomínané firmy na zabezpečenie pred zneužitím a mať platených odborníkov na ochranu, ako veľké spoločnosti. Musíme sa naučiť, ako si zabezpečiť svoju ochranu. Predovšetkým tak musíme urobiť za predpokladu, že sme sa stali súčasťou nekonečného online priestoru, ktorý sa nazýva internet.



Piliere kybernetickej bezpečnosti

Často je nevyhnutné rýchlo, jasne, efektívne a najmä vizuálne priblížiť procesy v počítačových systémoch. Pre tento typ procesov existuje špecializovaný jazyk: Unified Modeling Language (UML). Tento jazyk niekedy funguje ako popis funkcionality programu, inokedy sú to systémové funkcie, dokonca sa používa na popis programovacieho kódu.

2.3. Internet, ďalší priestor pre život

Prvé začiatky internetu sa datujú do konca 70. rokov minulého storočia. Na svojom počiatku bol internet určený pre vedcov na výmenu dát a informácii. Neskôr sa rozšíril do firemného i súkromného priestoru. Koniec druhého desaťročia 20 stor. v Európskej únii znamenal prekročenie 90% hranice pre prístup domácností k internetu[26], to znamená, že 9 domácností z 10 má prístup k internetu. Internet je veľký priestor. Môžeme si ho predstaviť ako veľké mesto, v ktorom sa nachádzajú firmy, obchody, knižnice, veľké obrazárne plné obrázkov, ale aj tmavé zákutia plné zlých a nepríjemných vecí. Internet sa od počiatku veľmi zmenil, avšak jeho podstata zostáva zachovaná. Ide o obrovský komplex vzájomne prepojených počítačových systémov, ktoré komunikujú medzi sebou presne určenými pravidlami. Bez týchto pravidiel by internet nefungoval tak, ako má (analógiu nachádzame napríklad v doprave, kde platia zákony, napr. dopravné značenie, ktoré musí každý vodič rešpektovať, pretože ich nerešpektovanie by prinieslo viac škody ako úžitku). Tieto pravidlá sú jasne definované aj v internetovom priestore. O týchto pravidlách hovoríme ako o tzv. viac-vrstvovom komunikačnom protokole, ktorý je dátovo orientovaný a poznáme ho pod menom **internetový protokol**. Inak povedané, internet je obrovský priestor alebo sieť na výmenu informácii.

[26] Digital economy and society statistics -households and individuals [online]. [cit. 17.04.2021].Dostupné na internete: https://ec.europa.eu/eurostat/statistics-explained/pdfscache/33472.pdf

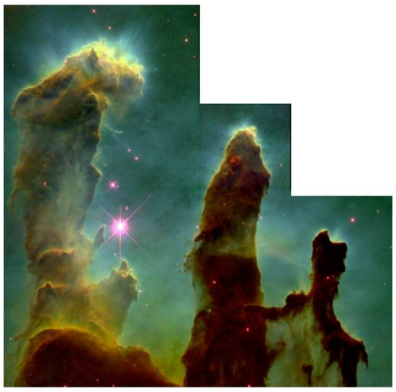
V súčasnosti poznáme množstvo typov protokolov použitých na internete, ktoré sa delia podľa použitia. Akokoľvek je internet prepojený a akokoľvek sú poprepájané jeho jednotlivé časti, aj tak nemá internet centrálnu správu a pravidlá, okrem riadenia pridelenia IP adries a názvov domén. To znamená, že existujú firmy, ktoré spravujú adresný priestor (IP adresy), prideľujú rozsah IP adries jednotlivým žiadateľom a spravujú doménový priestor (DNS). Takou firmou je celosvetovo rešpektovaná nezisková organizácia: Internet Corporation for Assigned Names and Numbers - ICANN. V rámci Slovenska máme doménu *.sk,* ktorá je spravovaná súkromnou spoločnosťou SK.NIC.

- Vznik internetu v skratke:

  V roku 1969 prišla agentúra ARPA (Advanced Research Project Agency) s myšlienkou, aby boli jednotlivé univerzity a výskumné strediská v USA navzájom prepojené. Vytvorili ideu vzniku siete ARPANETu, ktorá sa postupne rozrastala. V roku 1970 boli prepojené tri univerzity. Tento počet postupne rástol. Významný skok vo svete nastal v roku 1990, v ktorom bola sieť uvoľnená pre komerčné účely firmám.

- *Slovensko bolo pripojené k internetu prostredníctvom pomoci ministerstva školstva v Rakúsku, ktoré zabezpečilo pripojenie internetu a Slovenskej technickej univerzity v Bratislave. Vznikla slovenská sieť SANET (združenie slovenskej akademickej obce), ktorá pripojenie rozširovala po univerzitách v rámci Slovenska. Internet sa rýchlo rozširoval až do dňa 1.8.1996, kedy bola v Banskej Bystrici otvorená prvá internetová kaviareň. Obrovský skok na Slovensku bol zaznamenaný, keď operátori sprístupnili internet pre mobilné telefóny. Na začiatku to fungovalo cez protokol EDGE, neskôr sa to rozširovalo na protokol UMTS, HSPA, LTE. V roku 2020 malo pokrytie internetom 85,5% slovenských domácností*[27]*.*

[27] Vyše 90 percent mladých Slovákov a Sloveniek je na sociálnych sieťach [online] [cit. 30.04.2021]. Dostupné na internete: ttps://euractiv.sk/section/digitalizacia/news/vyse-90-percent-mladych-slovakov-a-sloveniek-je-na-socialnych-sietach-viac-ale-zaujimaju-dievcata/



Internetové protokoly sú navrhnuté nezávisle od typu pripojenia. Preto je možné čítať správy na mobilnej sieti cez mobilný telefón, cez pripojený kábel na počítači alebo cez WiFi na notebooku. Všetky pripojenia umožňujú prístup do obrovského priestoru, ktorý nie je centrálne riadený a spravovaný. Internet je súčasťou nášho života. V tomto prostredí vieme nájsť veľké množstvo informácií, od potvrdených, významných správ a pomoci, cez zábavu, ponuku tovarov, služieb, až po čierny trh, účelové klamstvá, hoaxy, ale aj zločinecké a teroristické aktivity. Predstava internetu, ako jedného veľkého všade priechodného priestoru, nie je úplne správna. Jedná sa skôr o viacero menších priestorov, ktoré sú navzájom pospájané a oddelené od seba. Do niektorých podpriestorov sa nikdy nedostanete, iné sú voľne prístupné. V ďalších kapitolách si povieme, ako pracovať a žiť v tomto priestore.

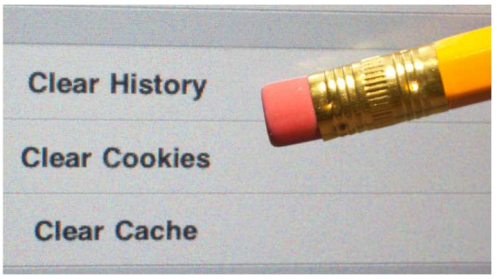
2.4. Záznamy internetových aktivít

Pri práci na počítači, či pri využívaní internetových prehliadačov a nakoniec aj pri samotnej práci s internetovými stránkami musíme počítať s tým, že o našej aktivite si každá služba ktorú stránka používa bude robiť záznamy. V prípade, že sa neprihlásime a systémy nás nepoznajú, je možné využívať aplikácie **anonymne**. Najčastejšie vieme ovplyvňovať vytváranie záznamov o našich aktivitách pomocou rôznych nastavení v prehliadači. Záznamy sa zachovávajú v cookies, ktoré sú vysvetlené nižšie, alebo pri samotnom prihlásení sa v internetovom prehliadači na strane webovej služby alebo v počítači, na ktorom pracujete. Všetky vaše kroky v internetových službách, ktoré využívate, budú presne identifikované a uchovávané, rovnako aj vaše výbery na stránkach a vaše rozhodnutia. Takéto pripojenie bude určite neanonymné. Preto je

dôležité, aby sme porozumeli, s akým typom dát pracujeme a kam si ich systémy ukladajú.

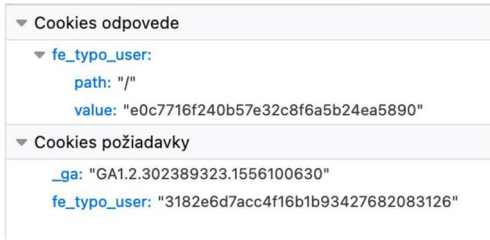
Anonymný - nepomenovaný, neznámy, nepodpísaný, bez uvedenia mena

1. Cookies - dáta, ktoré nás poznajú



Medzi štandardné vlastnosti prehliadačov patrí ukladanie si prezeraných súborov do histórie prehliadača, to však nie je všetko. Svoje informácie si o vás a vašom správaní ukladajú aj jednotlivé webové stránky. Tieto súbory uchovávajú základné informácie, ktoré ste mali uložené na stránke, ako sú meno, prezerané stránky, vaše výbery, jazyk a ďalšie. V technickej reči ide o stavové dáta, ktoré si webová stránka uloží na počítači. Nové prehliadače už na ukladanie nepoužívajú súbory, ale majú v sebe zakódovanú databázu a spravujú cookies centrálne. Webové stránky používajú cookies ako nástroj na lepšie identifikovanie klienta. Napríklad, keď sa prihlásite na stránku a zaškrtnete možnosť „Zostať prihlásený", v tom prípade sa vytvorí na vašom počítači súbor s informáciou o vás a pri ďalšom prihlásení systém priradí kód z cookies na počítači so svojim záznamom a prihlási práve vás. To znamená, že webová stránka vytvorila reláciu medzi konkrétnou cookie a prihláseným užívateľom. Tento typ cookies sa nazýva **relačná cookie**.[28]

[28]Čo sú cookies, na čo slúžia a máme sa ich báť? [online]. [27.5.2021]. Dostupné na internete: https://citadelo.com/sk/blog/co-su-cookies-na-co-sluzia-a-mame-sa-ich-bat/



Príklad nastavenia cookies na stránke www.uniba.sk (27.05.2021)

Cookies sa dajú rozdeliť podľa funkčnosti. **Základné** cookies ukladajú predvoľby a zabezpečenie. Používajú sa na zapamätanie prihlásenia, či stavu, kde ste úlohu zanechali. **Funkčné** cookies sa používajú na analýzu návštevnosti, zdieľanie medzi stránkami, resp. pri zdieľaní tretích strán na sociálnych sieťach, pre analýzu správania sa klientov na weboch (prenáša sa v nich často obsah nákupného košíka). **Reklamné cookies** patria medzi najobľúbenejšie, pretože vytvárajú priestor na ponúkanie rovnakých reklamných ponúk, ponúkanie reklám založených na vašich záujmoch. Tieto cookies sú často navzájom zdieľané medzi viacerými stránkami.

Niektoré prehliadače umožňujú nastaviť si nevytváranie cookies. To však neznamená, že sa cookies nevytvárajú, lebo nevytváranie by narušilo funkčnosť stránok. Cookies sa vytvárajú, ale po skončení práce všetky cookies prehliadač vymaže. Cookies tak vlastne predstavujú nielen históriu prihlasovania sa na stránky aj s kódom, ktorý zabezpečí prihlásenie do stránky, ale popisujú aj stránky, kam sa prihlasujete. Našťastie, prehliadače na to pamätajú a na základe využitia pravidla „Same Origin Policy" neumožňujú stránke pristupovať ku cookies, ktoré nevznikli na danej stránke. To znamená, že ak na jednej stránke napr. cez iframe spájate stránky z viacerých domén, tieto si navzájom nevidia cookies. Existuje veľa útokov na získanie cookies, najčastejšie útočníci využívajú kopírovanie dát, keď majú prístup na počítač alebo MIM (man in the middle) a v neposlednom rade XSS (Cross site scripting). O týchto útokoch si povieme v ďalších ročníkoch.

- *Nájdite históriu prehľadávania v prehliadači.*
- *Dohodnite sa so susedom, vymažte históriu prehliadača, určte, čo presne budete robiť: napr. naštartovanie prehliadača, prihlásenie do vyhľadávača (napr. google). Vyhľadajte známy internetový obchod, nájdite obľúbenú hru a dajte do košíka. Následne každý na svojom počítači pohľadá v histórii prehliadača postup, ako to bolo prevedené a o akej hodine bola každá akcia spustená. Nezabudnite analyzovať aj cookies, čo presne (aké informácie) si obidve firmy o vás uložili.*
- *Spomeňte si, čo ste dnes robili na mobilnom telefóne a pripravte si zoznam, čo by firma, ktorá spracováva aktivity klientov, o vás vedela zistiť. Nezabudnite aj na hry, sociálne média, navigácie, fitness aktivity a zariadenia.*
- *Aké zabezpečenie používate, aby ste boli dostatočne chránení pred sledovaním?*

2. Logovanie systémov a aplikácií - nezmazateľná stopa

Každý systém a každá aplikácia potrebuje informovať o svojom stave a funkčnosti. Väčšinou tieto zápisy zostanú nepovšimnuté, ale sú veľmi dôležité. Špeciálne v prípade, ak sa niečo stane, je každý *logovací zápis* podozrivej udalosti dôležitý. Za logovací zápis sa dá považovať ktorýkoľvek zápis, ktorý popisuje činnosť na počítači. Záznam o činnosti vytvára operačný systém, jednotlivé jeho prvky, ale aj aplikácie. Vytváranie stôp v jednotlivých systémoch zažilo obrovský, prevratný vývoj. Pôvodne, na prelome storočí, boli zápisy využívané na kontrolu funkčnosti systémov a aplikácií. Postupne sa ich využitie rozširovalo aj o zápis funkcionality, napríklad zápis pristupovania na webovú službu. V súčasnosti sa zápisy používajú tiež na kontrolu bezpečnostných narušení. Úroveň a hĺbku logovania je možné nastaviť buď na stálo, alebo dočasne. Zvyčajne je zapnutá základná verzia logovania, ktorá zapisuje spustenie a vypnutie hlavných služieb. Ďalšou úrovňou je obšírne

logovanie, kde je zapísané spustenie každej jednej služby. Posledná možnosť, ktorá sa používa len výnimočne, je úplné logovanie „debug mode".

Logovacie záznamy majú nasledovnú štruktúru[29]:

- *používateľské identifikátory (user ID, používateľské meno, atď.),*
- *popis, čo sa udialo,*
- *dátum a čas (prípadne časová zóna) záznamu,*
- *identifikátor zariadenia/zariadení alebo lokality (ak je to možné) a identifikátor systému/systémov,*
- *identifikátor procesov v systéme (spravidla názov a ID procesu - PID) a súborov, s ktorými sa narábalo,*
- *identifikátor sieťových adries a použitých protokolov (spravidla zdrojová/cieľová IP adresa, port a protokol),*
- *identifikátor transakcie v systéme (napr. v databázovom systéme)*.

Niekedy sa pridáva do záznamu *kategória záznamu* (Information, Administration, Error, Audit, Debug,...) a *priorita záznamu* (nízka/stredná/vysoká alebo číselné označenie).

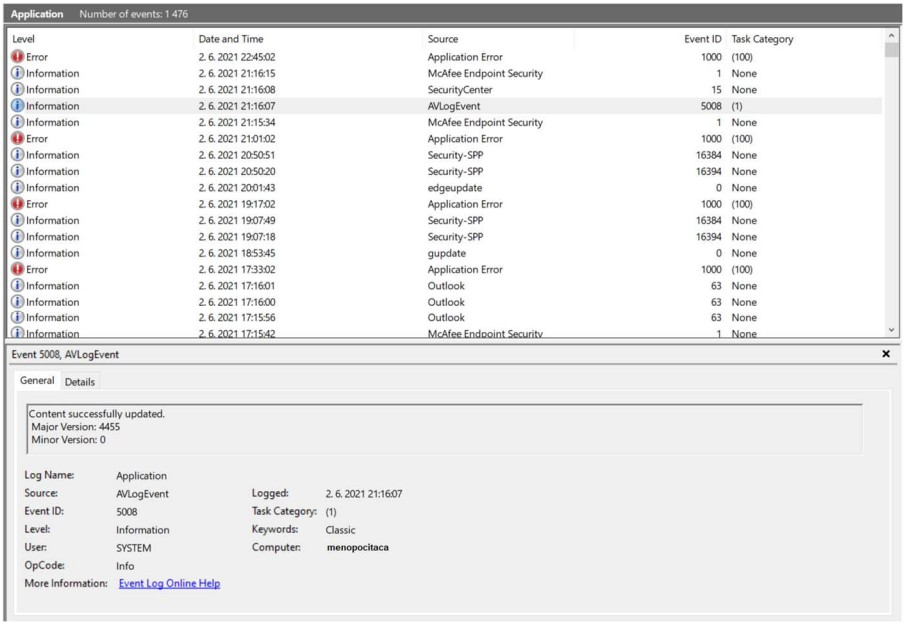
Vzhľadom na množstvo údajov, zápisy vytvárajú veľmi presný popis situácie v zariadení v presnom časovom slede. Priamo popisujú aktivitu na zariadení, a tým pádom aj aktivitu používateľa systému. Takto štruktúrované zápisy nazývame *Auditná stopa*.

3. Logovanie zmien v systéme

V praxi sa používa niekoľko spôsobov vytvárania logov. Najčastejší je formát *syslog*, ktorý je používaný hlavne v serveroch a v linuxovom svete. Formát je presne popísaný a štruktúrovaný. Pôvodný syslog je navrhnutý na posielanie otvorených nezašifrovaných záznamov, preto je pri používaní potrebné, aby ste nezabudli šifrovanie zapnúť.

[29] Prevzaté z ISO/IEC 27002:2013

V systéme Windows funguje logovanie, ktoré je zapisované do aplikácie *Zobrazovač udalostí (Event viewer)*. Zobrazovač udalostí obsahuje principiálne tri typy udalostí: Application, System a Security. Kategória Application je venovaná zápisu logovacích záznamov pre aplikácie, pričom do tejto kategórie je možné zapisovať. Kategória Systém je určená pre záznamy systémových procesov. Posledná kategória Security obsahuje záznamy, ktoré vygeneroval samotný systém. Do logu Security môže priamo zapisovať iba služba L*ocal Security Authority Subsystem Service (lsass.exe)*.



Ukážka záznamov zo Zobrazovača udalostí, kategórie Application na systéme Win10

Logovacie záznamy v systémoch MacOS nájdete v Konzole, kde je možné prehľadávať záznamy podľa typu aktivít, ktoré sú označené farebne.

Nájdite štruktúru syslogu na internete.

Nájdite systém, ktorý vytvára a posiela logy v systéme Windows a vytvorte v Zobrazovači udalostí na vašom PC záznam.

4. Logovanie práce v aplikáciách

Pri práci s aplikáciami je nevyhnutné myslieť na viacero častí bežného života aplikácie. Prvým je kontrola funkčnosti aplikácie. Kontrola je zabezpečená tým, že aplikácia v pravidelných intervaloch zapíše do logu, že pracuje. Druhým je kontrola vnútorných procesov v aplikácii. Ak zadáte do aplikácie úlohu, ktorá nevyžaduje vonkajšiu kontrolu alebo ide o automatizované procesy nevyhnutné na funkčnosť, potom je potrebné vedieť, či procesy bežia a ako skončili. Posledný typ logovania má za úlohu opísať prácu samotných používateľov aplikácii. Nezabúdajte, že popísať je nevyhnutné nielen to, čo používateľ požiadal, ale aj s akým úspechom či neúspechom skončila konkrétna akcia. Je preto potrebné rozlišovať situáciu, ak používateľ mal záujem o citlivé informácie a nezískal ich, lebo nemal oprávnenia alebo ich získal, lebo všetky oprávnenia mal.

5. Spracovanie logovacích záznamov

V zásade máme v súčasnosti dostatočné množstvo informácii o jednotlivých systémoch a aplikáciách. Vytváranie a spracovanie logovacích záznamov však nie je koordinované. Ich vývoj napreduje mnohými paralelnými cestami. Dôsledkom tohto vývoja je, že každá aplikácia a systém vytvára logovacie zápisy vo vlastnej forme. Táto rôznorodosť spomaľuje akékoľvek funkčné spracovanie log záznamov.

Zmeniť logovanie veľkých systémov a aplikácií sa nám asi nepodarí. Je však možné zabezpečiť, aby všetky vaše vlastné aplikácie vytvárali logovacie záznamy v jednom formáte. Spomínaná plošná štruktúra pre celú organizáciu zásadne uľahčí následné spracovanie záznamov. Na spracovanie logov je používaných viacero typov aplikácii. Z pohľadu bezpečnosti sú najdôležitejšie aplikácie typu SIEM (Security Incident and Event Management System). Týmto typom systémov sa budeme venovať vo vyšších ročníkoch.

Ukážka jednoduchého formátu:

Logovať sa budú záznamy do tabuľky *All_Logs* v schéme *LogAudit*:

- kto,
- čo,
- kedy,
- kde,
- s čím,
- ako presne urobil,
- s akým úspechom.

Zamyslite sa a navrhnite, ako by vyzerala výsledná forma (logovacia veta) logovacieho formátu, ak by sa zapisovali logy do súboru. Napríklad pre zápis jednotky v elektronickej žiackej knižke.

Navrhnite, ako zabezpečiť, aby sa súbor z predchádzajúcej úlohy nekonečne nezväčšoval. Dbajte na to, aby ste o žiadne záznamy neprišli.

6. Digitálna stopa

Pri využívaní informačných technológií je každý pohyb v zariadení v rámci internetu zaznamenávaný. Vytvára sa akýsi zápis informácie o každom pohybe. Tento zápis môže byť ukladaný:

- v zariadení, ktoré sa používa na prácu,
- pri operátorovi siete, ktorá je používaná na pripojenie do internetu,
- pri správcovi softvéru, ktorý je používaný klientom (napr. internetový obchod, hra, email,...).

Vzniká celá reťaz aktívnych aj pasívnych dôkazov, ktoré existujú na rôznych miestach. Tie sú časovo zreťazené a popisujú celú prácu,

ktorá bola vykonaná. Tieto zápisy nazývame **digitálna stopa**. Na termín digitálna stopa sa môžeme pozerať z dvoch rôznych uhlov pohľadu – z používateľského a analytického.

Používateľský pohľad

Z používateľského hľadiska vnímame tento pojem ako dátovú stopu, ktorú zanecháva každý používateľ od okamihu, kedy založí na internete svoj prvý účet a začne využívať rôzne internetové služby. Stopy sa delia na ovplyvniteľné (tie, ktoré môžeme ovplyvniť - napr. nezverejníme všetky údaje o sebe, pretože nie sú pre danú službu nevyhnutné), a neovplyvniteľné (tie, ktoré sú vytvárané bez akéhokoľvek nášho pričinenia).

Analytický pohľad

Každá systémová, aj používateľská aktivita na zariadeniach IKT pri využívaní internetových služieb zanecháva stopy vo forme záznamov v systémoch (logoch), zmenách dát uložených na úložiskách a dočasných súboroch použiteľných pri analýzach, napríklad bezpečnostných incidentov či trestnej činnosti. Z množiny zhromaždených a analyzovaných stôp je následne selektovaná podmnožina dát, ktoré sú, v súlade s legislatívou, využívané ako dôkazný prostriedok tzv. digitálny dôkaz.

V prípade, ak navštevujeme stránky, pričom vedome neprispievame žiadnym príspevkom (vstupom), ale len čítame stránky, hovoríme o **pasívnej stope**. Každý jeden záznam, ktorý vedome vytvoríme (napr. príspevok do konverzácie, zverejnenie názorov, pripomienok či fotografií) vytvára **aktívnu stopu.** Niektoré z týchto zápisov (logovacích záznamov) je možné ovplyvniť a vymazať, avšak ide iba o malú časť. Dokonca ani zápisy digitálnej stopy vo vašom vlastnom zariadení nie je jednoduché vymazať, často je to nemožné.

Nájdite vo vybranej aplikácii záznamy pasívnej stopy.

Ktoré záznamy patria medzi aktívne stopy vo vašom smartfóne a ktoré patria medzi aktívne stopy vo vašom laptope.

Digitálna stopa sama o sebe nie je nebezpečná. Problémom sa stáva až jej využitie a spracovanie rôznymi organizáciami a firmami. Digitálna stopa je v zásade nezmazateľná. Digitálna stopa sa pri práci s internetovou službou paralelne vytvára na zariadení, na ktorom pracujete a zároveň v prostredí internetovej služby. Dá sa preto predpokladať, že všetko, čo na internete uverejníte v rámci internetových služieb, aj v rámci internetových služieb zostane. Často sa tak deje aj na miestach a firmách, ktoré nie sú v priamej línii so službami, ktoré využívate. V súčasnosti je vyťažovanie dát digitálnej stopy využívané v maximálnej možnej miere. Firmy sa snažia spoznať zákazníka, jeho správanie, požiadavky a potreby. Analyzujú pohyby v rámci služieb a spoznávajú preferencie zákazníka. Na základe tohto poznania firmy menia a prispôsobujú ponuku svojich produktov a služieb potrebám zákazníkov. Firmy sa snažia využívať akékoľvek dáta, ktoré sú k dispozícií (z počítača, zo svojich stránok, zo stránok ostatných firiem), následne vytvárajú prepojenia a popisujú správanie klienta. Rovnako vedia použiť na sledovanie IP adresu, cookies z rôznych stránok, meranie polohy zariadenia. Výsledok, ktorý modelujú, nepopisuje presne človeka a jeho vlastnosti. Pre potreby zlepšenia predaja je postačujúce identifikovanie jednotlivých digitálnych stôp, na základe ktorých poskytli špeciálnu ponuku, pričom si zachovávajú informáciu, kde sú stopy uložené.

Vytváranie digitálnych stôp neovplyvňuje len ponuku pre klientov, ale prináša aj možnosť negatívneho vplyvu na klienta. Napríklad umožňuje ľahšie sledovanie človeka, často sa preklápajúce do prenasledovania. Niekedy môže takéto správanie vyústiť až do zneužitia osobných údajov, ktoré môžu končiť krádežou identity. Preto je, kvôli našej vlastnej bezpečnosti, nevyhnutné vždy sa zamyslieť, či je konkrétny údaj nevyhnutné zverejniť a čo sa stane, ak sa údaje dostanú do nesprávnych rúk. Najjednoduchším riešením je nezverejňovať všetko o sebe, aj vo virtuálnom priestore sa správať v hraniciach slušnosti, nastavovať si ochranu súkromia vo vašich prístupových službách a aplikáciách, vypnúť si sledovanie polohy v aplikáciách a zrušiť svoje účty v službách, ktoré nepoužívame a požiadať o vymazanie dát.

Požiadajte vami preferovanú službu o dodanie informácií, ktoré o vás vedie.

Požiadajte vami preferovanú službu druhý krát, so špecifickou žiadosťou o dodanie všetkých informácií, ktoré o vás vedie. Porovnajte rozdiel.

7. Čo robiť, aby sme boli pred uchovávaním digitálnej stopy chránení?

Informácie, ktoré o nás systémy zbierajú, sú pre nás potenciálne nebezpečné. Vymazať všetky informácie, ktoré zaznamenal náš počítač o nás, nie je vôbec jednoduché a často ani možné. Naša práca je aj o práci s internetom a webové stránky veľmi rady zaznamenávajú o nás množstvo údajov. Internetové prehliadače ukladajú dva typy údajov: cookies a dáta, ktoré sme prehliadali, aby nemuseli všetky dáta sťahovať viackrát zo stránky. Cookies sú sledovacie údaje o našej činnosti. Ukladanie dát o nás z webových stránok dlhodobo nie je dobré, pretože ak prídeme na stránku, ktorá má v sebe zakomponovaný malvér, môžeme si ho nevedome uložiť na disk. Ak neurobíme dostatočné opatrenia, bude tam uložený naozaj dlho. Je nevyhnutné si povedať, či tieto dáta naozaj potrebujeme, alebo vieme bez nich existovať. Vieme sa vzdať cookies, čím spôsobíme, že nebudeme mať reklamy na mieru? Vieme žiť bez lepšie cielenej reklamy? Aké sú vlastne dostatočné opatrenia?

Požiadavky na ochranu internetového prehliadača.

- Nepoužívajte staré verzie prehliadačov (napr. Internet explorer).
- Obmedzte ukladanie cookies na minimum a pravidelne ich vymazávajte.
- Nastavte si automatické vymazanie cache po ukončení internetového prehliadača.
- Využívajte v čo najväčšej miere privátny mód.
- Vzdelávajte sa, sledujte stránky, ktoré informujú o útokoch na obyvateľov (napr. www.preventista.sk, hoax.cz alebo www.hoax.sk).

Nikto zatiaľ nevymyslel opatrenie na úplnú ochranu pred útokmi. Internet predstavuje obrovský priestor, a preto je nevyhnutné zvyknúť si na pravidelné ochranné kroky a zároveň vedieť, ako sa máme brániť. V nasledujúcej kapitole si popíšeme priestor, v ktorom sa nachádzame, keď si zapneme internetový prehliadač.

Pojem kybernetický priestor vytvoril William Gibson v roku 1982 v krátkej poviedke s názvom „Burning Chrome", ktorá odkazovala na počítačom generovanú realitu. Tento pojem sa stal populárnym o dva roky neskôr, kedy bol použitý v Hibsonovej novele „Neuromancer"[30].

Podľa Gibsona je kybernetický priestor pomenovanie pre skutočný, mimopriestorový svet vyznačujúci sa schopnosťou virtuálnej prítomnosti a interakcie medzi ľuďmi.

Oxfordský slovník (Oxford dictionary) chápe kybernetický priestor ako fiktívny svet, v ktorom dochádza ku komunikácií pomocou počítačových sietí.

Kybernetický priestor je definovaný podľa § 3 písm c) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti ako globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.

Kybernetický priestor je teda virtuálny svet, ktorý nemá začiatok ani koniec. Ide o dynamický, neustále sa meniaci systém, ktorý je viazaný na hardvér. Je ohraničený používaním elektroniky na

[30] "(PDF) What is 'cyberspace'? - ResearchGate." 14 nov. 2018, https://www.researchgate.net/publication/328928631_What_is_'cyberspace'. [3. máj. 2021].

vytvorenie, uloženie, spracovanie a využitie dát prostredníctvom sietí, ktoré sú navzájom závislé a prepojené

Medzi vlastnosti kybernetického priestoru patria :

- **decentralizovanosť** - nie je riadený, okrem najvyššej úrovne prideľovania domén (viď. str. 37). Pravidlá si určuje v zásade každá webová stránka a každý poskytovateľ internetu. Vzhľadom na množstvo operácií, vymáhanie pravidiel je ťažké a často až nemožné.
- **globálnosť -** internet prekračuje svojim pôsobením hranice štátov, a preto je veľmi ťažké riadiť jeho vplyv. Štáty si určujú politiku (pravidlá) jeho používania na svojom území. Príchodom internetu, táto základná premisa skončila a v súčasnosti sa štáty snažia riadiť internet tak, aby chránili svojich občanov. Výsledkom je, že niektoré štáty, ktoré sa obávajú dopadov používania niektorých stránok, zakazujú prístup ku stránkam ako takým.
- **otvorenosť -** v rámci používania internetu je nemožné skontrolovať aktivitu každého účastníka. Stretávame sa často s príspevkami, ktoré sú urážlivé, poburujúce alebo aj klamlivé. Veľmi ťažko sa v takomto heterogénnom prostredí implementuje právomoc a vymáha zodpovednosť za príspevky. Preto je dôležité byť neustále v strehu a rozmýšľať nielen nad obsahom, ale aj cieľom príspevku.
- **interaktívnosť -** zmeny v rámci kybernetického priestoru nastávajú okamžite a zásadne sa menia v krátkom časovom slede (často sa spomína internetová diaľnica). Tieto zmeny majú dopad nielen na správanie používateľov, ktoré sa mení každou novou zmenou, majú dopad aj na zber dôkazov o akejkoľvek činnosti v prípade potreby. Nastavenie, ktoré je dnes, nemusí platiť zajtra.
- **bohatosť na informácie -** s internetom pracuje veľa rôznych skupín ľudí. Jedna časť sa zameriava na pridávanie vlastných článkov a informácií, iná časť publikuje čokoľvek. Je veľmi dôležité naučiť sa vyhľadávať správne informácie na základe posúdenia reputácie stránky.

Decentralizovanosť a prepojenosť internetu s vonkajšími sieťami si vieme predstaviť na nasledujúcom príklade. Slovenská akademická dátová sieť (SANET), ktorá stála pri zrode internetu na

Slovensku, je prepojená niekoľkými uzlami s okolitým svetom a prepojenie medzi hlavnými uzlami je vytvorené linkou s priepustnosťou 100Gb/s. Takýchto prevádzkovateľov máme v rámci krajiny niekoľko.

Ukážka rýchlosti internetu v SANETu a prepojenia liniek do zahraničia[31]

Predstavením siete SANET sme si predstavili rýchlosť v rámci jednej časti internetu len v rámci Slovenska. Atribúty internetu, napríklad decentralizovanosť, bohatosť na informácie, otvorenosť, či rýchlosť, ale aj ďalšie uľahčujú útočníkom možnosť útokov na jednotlivé prvky a služby, ktoré sú prístupné v rámci internetu. Nebezpečenstvo v rámci internetu je práve v tom, že útočníci sa môžu pokúsiť zneužiť zraniteľnosti týchto prvkov a služieb.

Nájdite na internete aspoň dva štáty, ktoré zabraňujú prístup k vybraným internetovým službám (stránkam) na území svojho štátu. Zistite typ zriadenia a dôvody, prečo sú stránky zakázané.

[31] SANET - Súčasná topológia siete [online]. [07.06.2021]. Dostupné na internete: http://web.sanet.sk/siet_topologia.shtm

- *Identifikujte webové stránky, ktoré sa venujú odhaľovaniu falošných informácii na Slovensku. Popíšte, čomu sa venujú.*
- *Ktoré média v rámci slovenského internetového priestoru sú považované za média, ktoré šíria falošné správy.*
- *Čo je to reputácia stránky a ako sa to dá použiť?*

Podľa dokumentu Cyberspace Operations: Concept Capability Plan 2016-2028 je kybernetický priestor zložený z troch vrstiev a to[32]:

- vrstvy fyzickej - všetok hardvér od káblov a ich infraštruktúry, rôznych switchov, routrov a iných zariadení,
- vrstvy logickej - všetky pravidlá a postupy ako jednotlivé komponenty komunikujú, prepojenie medzi sieťovými uzlami,
- vrstvy sociálnej - všetky osoby na sieti (radíme sem e-mailovú adresu, IP adresu…).

Z uvedeného vyplýva, že kybernetický priestor je akýkoľvek priestor, ktorý vieme ohraničiť a pracuje nad informačnými technológiami. Existujú rôzne uzavreté systémy, ako je vesmírne centrum NASA, alebo riadiace stredisko Hadrónového urýchľovača v CERNe. Za najznámejší kybernetický priestor môžeme považovať sieť Internet, ktorá je používaná celosvetovo, dennodenne v každej krajine.

Predstavme si veľký, masívny ľadovec plávajúci v mori. Tento bude pomyselne predstavovať náš kybernetický priestor. Malá časť spomínaného ľadovca je nad hladinou vody. Väčšia časť je pod hladinou, pričom táto časť je pre nás neviditeľná. Keď aplikujeme spomínanú analógiu do prostredia kybernetickej bezpečnosti, tak viditeľná časť je prístupná pre všetkých. Nachádzame tu všetky stránky cez google, facebook, amazon, instagram a iné. Vravíme o tzv. **surface web** (povrchový web), ktorý tvorí len 4 % celkovej

[32] "Cyberspace Operations Concept Capability Plan 2016-2028." 22 feb. 2010, [online]. [cit. 08.05.2021]. Dostupné na internete: https://fas.org/irp/doddir/army/pam525-7-8.pdf.

kapacity internetu. Táto časť internetu je prístupná širokej verejnosti a jej obsah je možné prehliadať internetovými prehliadačmi.

Omnoho väčšiu časť, a to až 90 % celkovej kapacity internetu, tvorí tzv. **deep web.** Ten je definovaný ako všetok obsah, ktorý nie je indexovaný webovým vyhľadávačom. To znamená, že pri vyhľadávaní ich používateľ nedostane, pretože ich vyhľadávač „nevie nájsť". Čo sem patrí? Webové fóra vyžadujúce registráciu, gmail účet, firemné intranety, univerzitné či vládne webové stránky. Na to, aby sa používateľ dostal do deep webu, potrebuje mať pre konkrétnu časť pridelené prístupové práva a linku, na ktorej sa bude prihlasovať. Do deep webu patria aj domény, ktoré nepatria do top-level domén, a ktoré nie sú indexované (nemajú priradený popis) prehliadačmi.

Top-level domény (v preklade domény najvyššej úrovne) sú domény rozdelené podľa písmen za poslednou bodkou. Organizácia Internet Assigned Numbers Authority (skr. IANA), zodpovedná za hlavné nameservre (root DNS), definuje top level domény, napr. .com (angl. commercial) pre komerčné organizácie, .org (angl. organisation) - neziskové organizácie, .mil (angl. military) - určené pre armádne účely, .gov (ang. government) - určené pre stránky vládnych organizácii. Slovenská top-level doména je má skratku .sk.

Ak by sme pokračovali v analógii nášho ľadovca a kybernetického priestoru, dostali by sme sa až na jeho spodnú časť, kde nachádzame **dark web.** Dark web je súčasťou Deep web prostredia. Toto miesto je označované ako miesto zločinu. Dark web nie je indexovaný prehliadačmi a nie je možné sa priamo napojiť do Darkwebu. Aby sme sa dostali do tejto temnej časti internetu, potrebujeme špeciálny softvér a nastavenie. Na rozdiel od deep webu tu vieme nájsť nezákonné činnosti a služby. Môžeme tu nájsť ukradnuté čísla kreditných kariet, falošné doklady, drogy a návykové látky či dokonca zbrane. Identita užívateľov je chránená šifrovaním, takže každý účastník je anonymný.

Zobrazenie rozdelenia internetu podľa prostredí [33]

2.5. Nekonečná virtuálna realita

Internet, surfaceweb, poskytuje prostredie pre nekonečnú komunikáciu o všetkom možnom, je to priestor pre život, reklamu a podnikanie. Zároveň môžu ľudia v tomto priestore robiť aj veci, ktoré sa ostatným javia ako negatívne pôsobenie. Právne pravidlá sa však z reálneho života premietajú aj do virtuálnej existencie (hovoríme o trestnom, správnom a občianskom práve a právnej zodpovednosti) a uplatňujú sa v ňom. Napriek tomu, anonymita prostredia intenzifikuje (zvýrazňuje) dobré, ale aj zlé vlastnosti používateľov. Zlé vlastnosti sa veľakrát z hrozieb pretavujú do kriminálnej aktivity, často veľmi závažnej. Všetky kybernetické hrozby a aj kriminálne aktivity sú v konečnom dôsledku zamerané na zvýšenie vplyvu alebo na nejakú formu zisku, najčastejšie je to peňažný zisk.

[33] "Deep Web & Dark Web Explained..!!! | Hacker Noon." 7 mar. 2019, [online] [cit. 06.5.2021]. Dostupné na internete: https://hackernoon.com/deep-web-dark-web-explained-dd3b1e6855e.

Pozrime sa na svet „normálnych" ľudí a svet útočníkov. Normálny človek pracuje s modernými technológiami, využíva sociálne siete a softvérové vybavenie preto, aby zvýšil kvalitu svojho života. Útočník robí to isté. Využíva rovnaké sociálne siete na lepšie spoznanie obete, tie isté moderné technológie na oklamanie obete a útoku na obeť. Hlavnou motiváciou útočníka je zisk. Či ide o získanie peňazí alebo ide o získanie nástrojov, ktoré sa dajú využiť pri ďalšom útoku. Pri hľadaní zdrojov peňazí útočník vyhľadáva ľudí, ktorí majú peniaze na účte. (napr. vyhľadáva ľudí, ktorí si chcú kúpiť auto, pretože to znamená, že majú pripravený vyšší obnos peňazí). Pri hľadaní prostriedkov na ďalší útok môže byť prostriedkom čokoľvek (napr. prístup do emailu, prístup do sociálnej siete, …). Z toho vyplýva, že na prvý pohľad rovnaká motivácia môže mať, vďaka odlišnému využívaniu kybernetického priestoru, úplne iný výsledok.

2.6. Informačná bezpečnosť

V konečnom dôsledku sa kybernetický priestor javí ako veľmi nehomogénny priestor, ktorý sa v zásade organizuje vlastnými pravidlami. Tento priestor prináša nielen nové možnosti, ale aj nový typ nebezpečenstiev. Každý z nás je súčasťou tohto priestoru, a preto sa musíme o bezpečnosť seba a svojich dát zaujímať. Problémom nie je len veľkosť priestoru, ale aj hrozby, ktoré sa v ňom vyskytujú. Niektoré hrozby odstráni jednoduché a lacné zabezpečenie, odstraňovanie iných hrozieb by nás stálo veľmi veľa peňazí, pričom sa dokážeme zamerať len na zníženie dopadov, to znamená zníženie pravdepodobnosti, že veľké riziko nám spôsobí veľké škody. Napríklad citlivé dáta budeme mať uložené na samostatnom počítači, ktorý nebudeme používať na nič iné a nebude pripojený na internet. Takéto použitie počítača by bolo veľmi nerentabilné, a preto skôr budeme uvažovať nad lepšou ochranou počítača ako nad nákupom počítačov pre každú príležitosť. Z uvedených dôvodov začneme pri

práci s kybernetickým priestorom používať pojem riziko, ktoré nám hrozí a tzv. mitigačné opatrenia (opatrenia na zníženie rizika). Pre ilustráciu nám poslúži príklad z bežného života: ak sa bojíme zhodenia a rozbitia pohára zo stola, musíme znížiť riziko a pohár uložíme do stredu stola a nie na kraj stola.

2.7. Princípy informačnej bezpečnosti

Každý subjekt, či už konkrétny človek alebo organizácia, si musí pri práci v kybernetickom priestore nastaviť **ciele informačnej bezpečnosti**, ktoré chce dosiahnuť. Konkrétny človek sa bude zameriavať na seba a svoje aktivity, preto bude chcieť chrániť zariadenia a údaje, ktoré na nich má uložené. Firma potrebuje zabezpečiť väčšie penzum vecí. Ochraňuje seba, svoje dobré meno, svoje aktíva, ale aj zamestnancov a najmä klientov a ich dáta. Preto bude mať viac cieľov a viac pravidiel, ktoré je nevyhnutné nastaviť a následne ich funkčnosť kontrolovať. Výsledkom naplnenia všetkých cieľov je dosiahnuť požadovanú úroveň bezpečnosti tak, aby jej ideálne nastavenie zohľadňovalo všetky riziká. Inak bude mať nastavenie informačnej bezpečnosti novinový stánok na rohu ulice, inak bude mať nastavenú bezpečnosť firma, ktorá prestavuje byty zákazníkom, inak nemocnica a úplne iné ciele a nastavenie bude mať armáda.

Niektoré firemné ciele sú jednoduché, sú definované vo forme pravidiel a nasadzujú sa okamžite. Iné sú kontinuálne, napr. spravovanie prístupov zamestnancov alebo zvyšovanie bezpečnostného povedomia a niektoré sú dlhodobé. Príkladom dlhodobého cieľa je príprava na certifikáciu a certifikácia podľa pravidiel štandardu. V prípade bezpečnosti pripadá do úvahy skupina noriem ISO 27k. Podrobne sa tejto skupine noriem budeme venovať v ďalších ročníkoch.

Ak sa budete riadiť podľa ktoréhokoľvek štandardu, vždy pre každého, každý systém, každý hardvér, každého človeka, ktorý používa technológie platia princípy informačnej bezpečnosti, ktoré treba mať neustále na pamäti a ktoré všetky štandardy používajú.

Princípy sú základné odporúčania, ktoré sú nevyhnutné, aby bola zaistená istota, že bezpečnosť je správne implementovaná a jednotlivé prvky sú chránené.

1. Princíp: Need to know (Nevyhnutné vedieť)

Pre nás sú v tejto chvíli najdôležitejšie základné princípy, ktorými sa riadi informačná bezpečnosť. Sú to jednoduché pravidlá, ktoré sú jasné, nemenné a priamo implementovateľné.

Prvým princípom je princíp ***need to know***. Je to princíp, ktorý vyžaduje, aby sa zamestnanec alebo klient dostal len k informáciám, ktoré sú pre neho nevyhnutné.

- *Vysvetlite, čo by znamenalo, ak by sa princíp need to know nedodržiaval v škole a čo by to znamenalo, ak by sa dodržiaval.*
- *Navrhnite organizácie, kde všade je nevyhnutné využívať princíp need to know.*
- *Predstavte princíp need to know na príklade Vami používanej sociálnej siete. Zamerajte sa na prácu so skupinami (TikTok, Instagram, Facebook).*

2. Princíp: Need to do (Nevyhnutné spracovávať)

Druhým princípom je princíp ***need to do***. V tomto prípade sú nastavené pravidlá tak, aby zamestnanec alebo klient vedel spracovávať dáta len v nevyhnutnom rozsahu podľa požiadaviek a úloh, ktoré musí napĺňať. Všetky ostatné prístupy mu budú automaticky zamietnuté.

V obidvoch princípoch musí existovať autorita, ktorá nevyhnutný prístup udeľuje a riadi. Princíp need to know a princíp need to do majú aj svoje nevýhody. Napríklad v prípade, keď sa autorita rozhodne svojvoľne odmietnuť prístup pre toho, kto ho nevyhnutne potrebuje, znemožní vykonať zamestnancovi požadovanú úlohu.

*Pripravte prezentáciu a predstavte spolužiakom princíp **need to do** na príklade vašej sociálnej siete. Zamerajte sa na prácu so skupinami (TikTok, Instagram, Facebook).*

3. Princíp: Čo nie je zakázané je povolené

Úplne opačným spôsobom je riadenie princípom **čo nie je zakázané, je povolené**. Toto je rovnako dôležitý princíp ako obidva predchádzajúce a používa sa napríklad v malých, špecializovaných firmách, napríklad v marketingovej agentúre. Agentúra pracuje na otvorenom tímovom základe, a preto akékoľvek utajovanie by proces kreovania marketingových stratégií zásadne obmedzilo.

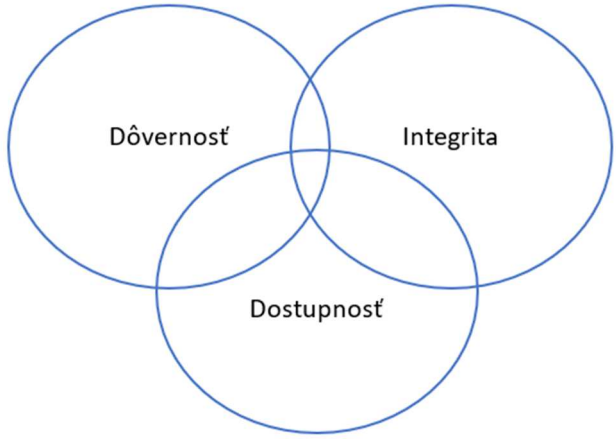
4. Princíp: Kontrola štyroch očí

Posledným vybraným princípom je ***princíp štyroch očí*** *(anglicky the Four eyes principle, skratka: K4O)*. Tento princíp je veľmi prísny. V reálnej situácii to znamená, že existujú dáta a služby aplikácií vo firme, ktoré vyžadujú dodatočné overenie ďalšou zodpovednou osobou. Prvá osoba vyhľadá údaje, pripraví ich, spracuje a v poslednom kroku, pred spustením záverečnej fázy, ďalšia poverená osoba skontroluje, čo bolo pripravené a potvrdí akciu kódom, alebo podpisom.

Navrhnite organizácie a činnosti v organizáciách, pri ktorých je nevyhnutné používať princíp štyroch očí.

2.8. Triáda CIA (dôvernosť, integrita, dostupnosť)

Cieľom informačnej bezpečnosti je chrániť informácie. Ochrana je zabezpečená využitím triády CIA. Ako sme už hovorili, skratka CIA vychádza z anglických slov dôvernosť, celistvosť a dostupnosť. Tieto slová definujú základné bezpečnostné ciele informačnej bezpečnosti. Vzťahujú sa nielen na virtuálny svet, ale aj na svet mimo virtuálneho prostredia. Napríklad dôvernosť je základným nástrojom pre právneho zástupcu, ktorý, ak má podporovať klienta, musí mať o klientovi úplne všetky informácie, aj tie nepríjemné. Klient musí pociťovať voči právnikovi dôveru. Ďalším príkladom je dostupnosť zdravotnej dokumentácie, ktorá je v súčasnosti dostupná pre každého lekára online. V prípade nedostupnosti zdravotnej dokumentácie by nemohla byť poskytnutá plánovaná zdravotná starostlivosť pre pacienta, ale len urgentná.



Piliere patriace do CIA tvoria neoddeliteľnú súčasť informačnej bezpečnosti.

Dôvernosť v bežnom slova zmysle chápeme ako schopnosť niečo udržať v tajnosti. V reálnom svete, ak chceme niečo skryť pred okolitým svetom, vieme zatiahnuť žalúzie na oknách, môžeme poprosiť kamaráta, aby si spoločné tajomstvo nechal len pre seba.

V prípade používateľa počítača vieme využiť rôzne VPS (virtuálna privátna sieť, angl. VPN - virtual private network) alebo rôzne iné šifrovanie dát, aby sme chránili súkromie. **Dôvernosť údajov** znamená, že k informáciám majú prístup len oprávnené osoby. Dáta sú prístupné len jednoznačne určenému subjektu. Typický prejav straty dôvernosti je neželané zverejnenie informácií.

Integritu môžeme chápať ako celistvosť, súdržnosť, neporušenosť. Ako príklad môžeme uviesť územnú integritu štátu. Pod tým pojmom rozumieme územnú celistvosť štátu v medzinárodnom práve. **Integrita údajov** (celistvosť údajov, úplnosť údajov) nám zjednodušene hovorí, že údaje nie sú modifikované. Vo svojej podstate je to ochrana dát proti neoprávnenému zásahu. V prípade, že nie je možné udržať integritu údajov následkom neoprávnenej zmeny, údaje považujeme za vážne poškodené alebo zničené.

Ak je niekto dostupný, tak je pre nás dosiahnuteľný. To isté platí aj v oblasti kybernetickej bezpečnosti. **Dostupnosť údajov** znamená mať aktuálny prístup k informáciám. Ak sa v danom okamžiku nevieme dostať k údajom, systém považujeme za nedostupný a chápeme to ako porušenie dostupnosti dát.

Okrem CIA existujú aj ďalšie atribúty, ako napríklad autentickosť, súkromnosť, anonymita, pseudonymita, nepopretie pôvodu, nepopretie doručenia, resp. v prípade ochrany systémov poznáme dosledovateľnosť. Ďalším pilierom informačnej bezpečnosti sa budeme venovať vo vyšších ročníkoch.

2.9. Prvky informačnej bezpečnosti (ľudia, technológie, procesy)

V dnešnom období sa často stretávame s názorom, že kybernetickú bezpečnosť zabezpečuje IT oddelenie[34]. Tento názor je mylný a ohrozuje samotnú firmu. Na jednej strane potrebujeme mať zástupcov informačnej bezpečnosti mimo IT oddelenia, pretože práve IT oddelenie musí napĺňať požiadavky oddelenia informačnej bezpečnosti. Na druhej strane, IT oddelenie je pre bezpečnosť dôležité, ale nie najdôležitejšie. Pokiaľ chceme dosiahnuť maximálny možný stupeň bezpečia v oblasti informačnej bezpečnosti, musíme zapojiť všetkých ľudí v našej firme a prideliť im rôzne úlohy resp. zodpovednosti. Nesmieme zabúdať, že každý človek potrebuje permanentné vzdelávanie.

Tieto tri prvky a ich spoločná interakcia umožňuje vytvoriť a udržať kybernetickú bezpečnosť. Patria sem:

- ľudia,
- technológie,
- procesy.

2.10. Ľudia

Ľudia na výkon svojej práce potrebujú využívať technológie. Doba prináša nielen požiadavku, ale aj možnosť neustáleho zlepšovania zručností, a to nielen zamestnancov a klientov, ale rovnako aj útočníkov. Zamestnanci majú prístup k informačným systémom a ku všetkým zdrojom v organizácii. Majú možnosť urobiť veľa dobrej práce, ale aj tej zlej (či už úmyselne alebo neúmyselne) a potrebujú permanentný vzdelávací program, ktorý ich osobne, a tým pádom následne aj firmu, udrží v bezpečí. Z tohto dôvodu je potrebné ľudí ochraňovať pred útokmi. Ochranu je nevyhnutné podporiť

[34] Podobná mylná myšlienka sa týka oddelenia ľudských zdrojov - v tomto prípade sa mylne predpokladá myšlienka: že oddelenie má chrániť osobné údaje.

súbormi pravidiel, technických opatrení a neustálym zvyšovaním povedomia. Z uvedených dôvodov je nevyhnutné každého zamestnanca školiť. Je nutné zabezpečiť, aby získal potrebné kompetencie a zručnosti v oblasti kybernetickej bezpečnosti, aby sme čo v najväčšej možnej miere znížili riziko kybernetických hrozieb v našej firme, škole, úrade. Ľudia sú najdôležitejším a najslabším článkom v kybernetickej bezpečnosti. Sú však zároveň najčastejším cieľom útočníkov. Preto práve ľudia určujú, ako efektívne budú fungovať procesy a technológie.

2.11. Technológie

Technológie chápeme v dvoch rovinách.

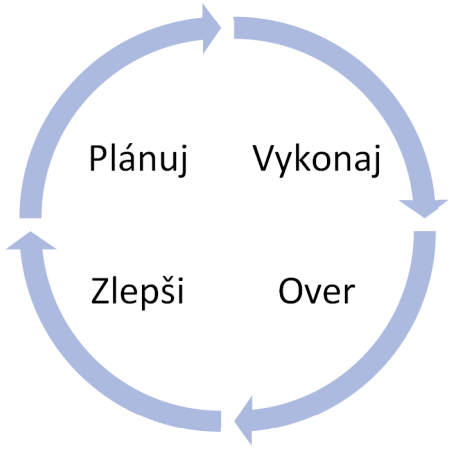
1) Prvou rovinou je chápanie technológie v ponímaní nástroja na prácu. V takomto prípade sú technológie chránené samé o sebe. Každý zamestnanec má svoj vlastný prístup (pozri princíp „*need to do*"), dáta s ktorými pracuje sú len tie, ktoré nevyhnutne potrebuje na prácu (pozri princíp need to know). Systém ako celok je chránený ďalšími prostriedkami, ako sú šifrovanie uložených dát, systém je uložený na oddelenej sieti s vypublikovanými nevyhnutnými linkami na prístup a všetky zmeny sú zapísané v logovacích záznamoch.
2) Druhým prípadom sú ochranné technológie. Tieto technológie najefektívnejšie pracujú s ľuďmi a procesmi tak, aby sme vedeli správne riadiť incidenty (incident - neštandardná udalosť, ktorá je narušením bezpečnostných pravidiel, napríklad pri porušení princípov informačnej bezpečnosti) a včas ich detegovať, identifikovať, zareagovať na ne a incidenty vyriešiť. Medzi technológie môžeme zaradiť hardvér a softvér, ktoré jednotlivé oddelenia vo firme používajú, aby dosiahli spoľahlivú kybernetickú bezpečnosť. Môžeme si tu predstaviť nástroje na sieťovú bezpečnosť, ako firewall, centrálna správa používateľov a ďalšie. Rovnako sem vieme zaradiť napríklad analýzu správania sa používateľov alebo zamestnancov. Tieto nástroje nestačí mať iba nainštalované a používať ich, ale neustále ich aj ladiť a zlepšovať, pretože

ich výpadok, alebo rozladenie bude znamenať výpadok systémov, čo bude mať dopad na funkčnosť celej firmy.

Firewall je sieťové zariadenie, ktoré zabezpečuje riadenie komunikácie medzi sieťami a zároveň prepája ďalšie siete. Firewall zabezpečuje v rámci kontroly povoľovanie a zakazovanie spojení medzi sieťami. Podľa typu firewall kontroluje prevádzku na rôznych sieťových úrovniach. Napríklad kontroluje posielanie sieťových paketov (packet filter) alebo aplikačný firewall riadi povoľovanie a zakazovanie aplikácií (application filter), atď.

2.12. Procesy

Procesy sú zavedené postupy, ktoré zabezpečujú rýchlu, presnú a organizovanú odpoveď zo strany organizácie. Každý proces má svoj presný život, od naštartovania, cez realizáciu, ukončenie a ponaučenie, po zlepšenie samotného procesu. Týmito krokmi zabezpečíme, že každý proces nezostarne, ale bude sa neustále zlepšovať, a tým pokrývať stále lepšie požiadavky organizácie.

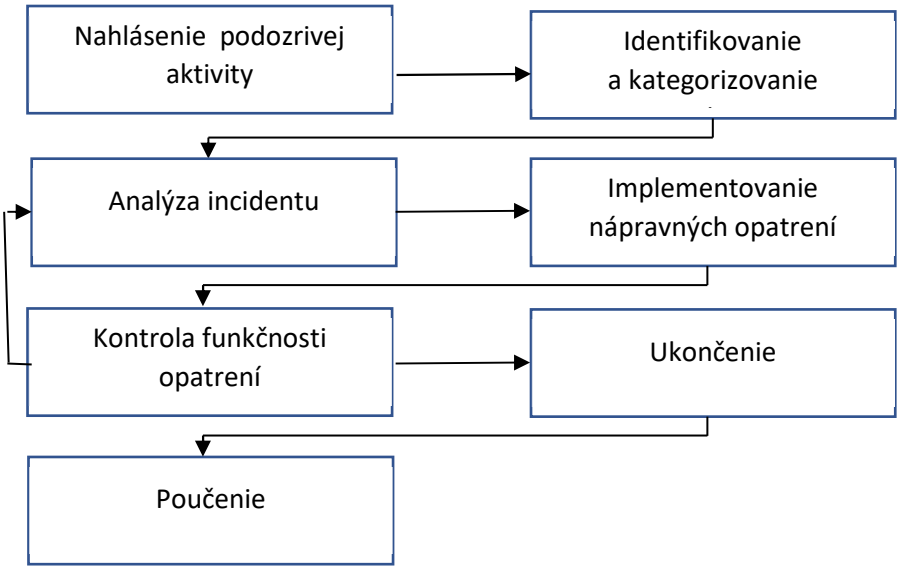


Schematický náčrt fáz procesu

Z pohľadu Informačnej bezpečnosti ide o dve veci:

- zabezpečenie činnosti, ktoré majú predchádzať kybernetickému útoku,
- ak útok nastane, budeme potrebovať presne a včas identifikovať útok a následne rýchlo a efektívne zareagovať.

Tím informačnej bezpečnosti s podporou IT tímu musí mať pripravený plán reakcie na kybernetické incidenty. Dobrý plán umožní opakovateľné postupy pri riešení kybernetických incidentov, s cieľom čo najrýchlejšie a najefektívnejšie obnoviť zabehnuté procesy. Po skončení riešenia incidentu vo fáze *zlepši* upravíme proces na odstránenie incidentu tak, aby pokrýval lepšie požiadavky organizácie.

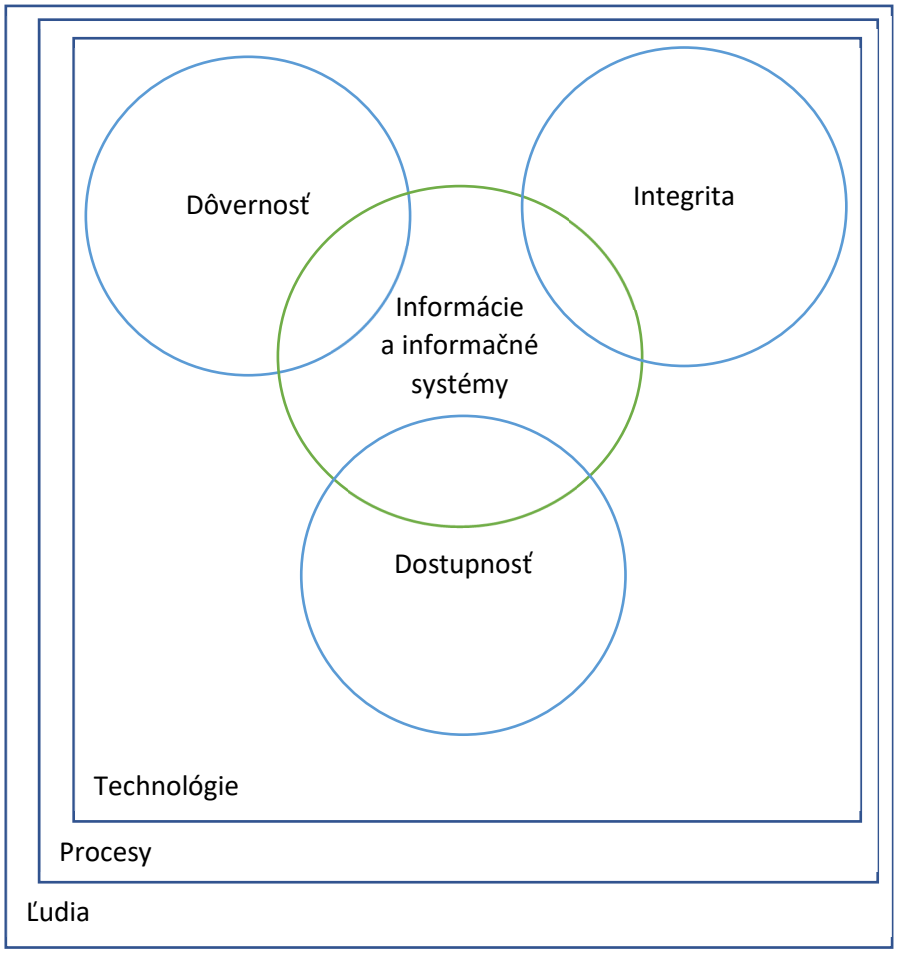


Základné kroky procesu odstraňovania bezpečnostného incidentu

Z pohľadu Informačnej bezpečnosti budeme pri prvku ľudia hovoriť o **personálnej bezpečnosti**. V prípade procesov ide o **organizačnú bezpečnosť**, pretože hovoríme o procesoch, ktoré riadia a organizujú bezpečnosť v organizácii. V prípade technológii ide o **technologickú bezpečnosť**. Pojem technologická bezpečnosť je zložitejší vzhľadom na to, že pod týmto pojmom sa skrýva viacej typov

bezpečností. Prvou je fyzická bezpečnosť, ktorá má za úlohu chrániť zariadenie pred fyzickým zničením či ukradnutím a ďalšou je informačná bezpečnosť, ktorá má za úlohu chrániť informácie v systémoch uložených, minimálne na úrovni cieľov CIA.

Predstavili sme si princípy informačnej bezpečnosti a jednotlivé prvky, ktoré do procesu vstupujú, ako sú technológie, procesy a ľudia. Tento svet je navzájom poprepájaný, pričom zabezpečenie dodržiavania triády CIA je považované za základ, na ktorom je postavená bezpečnosť jednotlivých prvkov, ktoré sú navzájom poprepájané.



Zobrazenie vzťahov cieľov a prvkov informačnej bezpečnosti

2.13. Riziko, aktívum, zraniteľnosť

Pojem riziko pozná každý z nás. Veľakrát sme sa s ním stretli v rôznych seriáloch, filmoch, kde hlavní protagonisti vyhodnocovali, či daná aktivita stojí za podstúpenie daného rizika. Hrdinovia vo filme navzájom bojovali a vyhodnocovali, či protivník pre nich predstavuje **hrozbu** alebo nie. Na to, aby predstavoval protivník hrozbu, musí mať vedomosť alebo nástroj, s ktorým vie škodiť a musí vedieť zaútočiť na miesto, kde je hrdina zraniteľný. **Zraniteľnosť** je priestor alebo možnosť, ako zásadne poškodiť, ovplyvniť hrdinu, napríklad Supermana oslaboval a zraňoval kryptonit. Zároveň protivník musí mať **motiváciu** na útok. Hrdina potrebuje **ochranu alebo ochranné opatrenia,** a tú vo filme predstavuje napríklad zbroj, alebo schovanie sa za betónový múr. Život hrdinu alebo objekt, ktorý ochraňuje je **aktívum**. Život hrdinu alebo objekt, ktorý chráni má svoju cenu resp. **hodnotu**. Otázkou je, či riziko nastane a prejaví sa ako bezpečnostný incident alebo nie, a preto je jedným z atribútov **pravdepodobnosť**. Druhým atribútom je **dopad** a ten je, ak sa vrátime späť do reálneho priestoru zabezpečenia bezpečnosti konkrétnej spoločnosti, zvyčajne finančný. To znamená, aké finančné alebo iné prostriedky bude musieť organizácia vynaložiť, ak sa riziko naplní.

Riziko môžeme charakterizovať ako pojem, ktorý označuje pravdepodobnosť, že sa hrozba naplní a zmení na incident. Samotné naplnenie hrozieb môže byť vytvorené nezávislo na okolnostiach alebo cielene konaním protivníka, v prípade cieleného naplnenia hrozby hovoríme o **útoku**. Niektoré riziká sú nezmeniteľné a nie je v nikoho silách ich zmeniť. Tieto riziká musíme len **akceptovať**. Dopady iných rizík sa dajú zredukovať (často: mitigácia, znižovanie dopadu rizika) ochrannými opatreniami, aby sa z veľkých rizík stali menšie s menším dopadom. Samozrejme, najlepšie riešenie je riziká odstrániť **vyriešením**.

Obyčajne sú riziká ukončené znížením na minimum. Väčšinu rizík nie je možné odstrániť na 100%. Predstavme si, čím všetkým sa zaoberáme pri popise rizika výpadku energie v datacentre. Štandardom pre datacentrum je mať vstupy elektrickej energie z dvoch rôznych elektrární. Počítajú sa dve dôležité

pravdepodobnosti, a to koľko percent z roka nebude dodávka elektrickej energie a pravdepodobnosť, že ak nastane výpadok, bude trvať dlhšie ako 1 hodinu (dĺžka závisí od nastavení ochranných opatrení v dátovom centre). Zároveň je v datacentre pripravený hlavný a záložný diesel agregát, ktorý vyrába elektrinu v prípade celkového výpadku elektrickej siete, u ktorého je tiež pravdepodobnosť, že nenaštartuje. Na vyhladenie výpadkov, t.j. preklenutie doby, keď vypadne elektrina zo siete a kým sa naštartuje diesel agregát, sa používa UPS (*uninterruptible power supply*), pričom UPS sa tiež dodáva s pravdepodobnosťou zlyhania. Presné pravdepodobnosti si každé dátové centrum exaktne meria. Čísla nás však môžu prekvapiť, napríklad ak budeme predpokladať výpadok elektrickej energie na úrovni 3% počas roka, tak dátové centrum musí riešiť výpadok elektrickej energie počas roka na 11 dní.

Zamyslite sa a napíšte, s akými rizikami pracuje pekáreň, autoservis a banka. Napíšte, ktoré riziká sú rovnaké pre všetky tri typy firiem, a ktoré riziká budú rozdielne.

Čo je to UPS a ako funguje?

Aké ďalšie riziká je nevyhnutné riešiť pri dlhodobom výpadku elektrickej energie v dátovom centre okrem spomínaných z príkladu.

Nezamieňajme si pojem riziko s neistotou. Sú medzi nimi určité rozdiely, napríklad:

- riziko je merateľné, neistota nie,
- riziko používa kvantitatívne ukazovatele (cena, rozmery, váha, rýchlosť…) a neistota kvalitatívne ukazovatele (chuť, krásu…)

S rizikom pracujeme vo svojom živote každý deň. Ak jazdíte na bicykli, tak používate prilbu. Prilbou znižujete dopad rizika pádu z bicykla. Nie je to zrušenie (používa sa uzavretie rizika), ale je to

jeho zníženie (minimalizácia). Za príklad zrušenia rizika a jeho dopadov by sa pokladalo to, ak by ste sa prestali bicyklovať. Niektorí cyklisti používajú nielen ochranu hlavy, ale aj ochranu lakťov a kolien, to znamená, že predpokladajú možnosť pádu a snažia sa znížiť v prípade naplnenia rizika dopad rizika na minimum.

V domácom prostredí môže byť dôležitá ochrana dát na domácom počítači. Dáta nám môžu byť ukradnuté aj s celým laptopom (strata dôvernosti a dostupnosti), dáta môže zašifrovať ransomver (strata dostupnosti), resp. sa môže pevný disk pokaziť (strata dostupnosti). Ako tieto riziká znížiť?

Príklady rizík a návrhov na zníženie rizika (mitigačných opatrení):

- Riešením pre zníženia rizika v prípade krádeže zariadenia môže byť:
    - zašifrovať pevný disk a použiť silné heslo (ochrana dôvernosti),
    - zálohovať dáta (zaistenie dostupnosti),
    - príp. použiť antitheft (a pokúsiť sa nájsť ukradnuté zariadenie).
- Na zníženie rizík útoku ransomweru je možné využiť antivírus a zálohovať dáta.
- Riziko straty dát spôsobené pokazeným diskom - pokazený disk vieme ošetriť zálohovaním a rýchlym nákupom nového disku.

Uveďte, aké riziká hrozia vášmu mobilnému zariadeniu a vysvetlite akým spôsobom riziká znižujete? Popíšte, aké ďalšie spôsoby je možné použiť?

Pojem „Aktívum" poznáme hlavne z oblasti účtovníctva. V oblasti kybernetickej bezpečnosti budeme pod týmto pojmom rozumieť všetko, čo má pre nás, či už ako pre osoby alebo firmy, určitú hodnotu. Samotná definícia nehovorí v akej forme sa aktívum vyskytuje. Vieme ho však rozdeliť na hmotné a nehmotné.

Do aktív organizácie môžeme zahrnúť:

- ľudí,
- softvér,
- hardvér,
- informácie/údaje (rôzne druhy dokumentov),
- služby (napr. internetové služby),
- papierové dokumenty,
- ... .

Uveďte vlastný príklad hmotného a nehmotného aktíva.

Zraniteľnosť môžeme chápať ako slabé miesto aktíva, prípadne jeho nedostatok. Ako príklad môžeme uviesť zastaranosť systému, nízke povedomie o bezpečnosti používateľov, nedostatočná údržba systému a iné.

Spíšte zraniteľnosti, ktoré sa nachádzajú vo vašej škole.

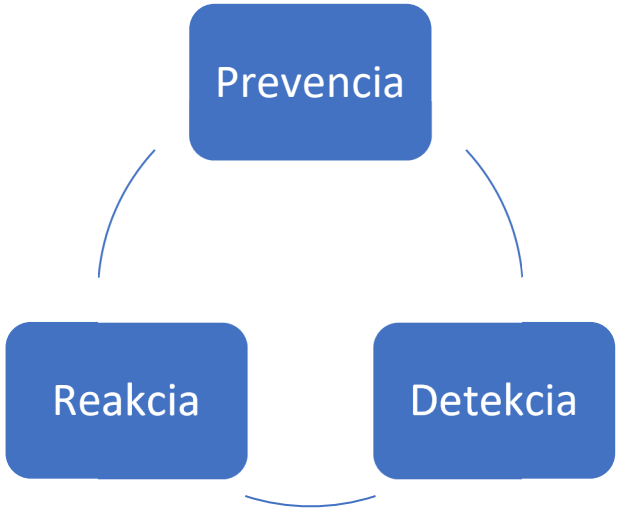
Navrhnite mitigačné opatrenia pre zraniteľnosti ktoré ste identifikovali vo vašej škole v predchádzajúcom prípade.

Veľmi často sa stretávame s útokom voči menu a heslu na sociálnych sieťach. Naše informácie na sociálnych sieťach sú veľmi hodnotné a dopad ich zneužitia by bol pre nás zrejme zničujúci. Z tohto dôvodu umožňujú sociálne siete používanie dodatočnej autentifikácie prostredníctvom napr. mobilnej aplikácie. To znamená, že sa prihlasujeme na počítači menom a heslom a dodatočné schválenie prebehne ešte aj pomocou aplikácie v mobile. Toto je jeden z moderných spôsobov znižovania rizika ukradnutia mena a hesla, pretože útočníkovi nestačí len odchytiť a použiť meno a heslo, musí vás tiež donútiť schváliť mu prihlásenie a toto schválenie prebieha v rámci oddeleného priestoru, mimo počítača, na vašom mobilnom telefóne. V prípade, že na prihlásenie používame nielen meno a heslo, ale aj ďalšie veci (faktory) ako je SMS, aplikácia alebo iné, sme sa dostali k viacfaktorovému overovaniu a to si vysvetlíme v kapitole 6.7 Multifaktorová autentizácia.

2.14. Životný cyklus a kontrola bezpečnosti

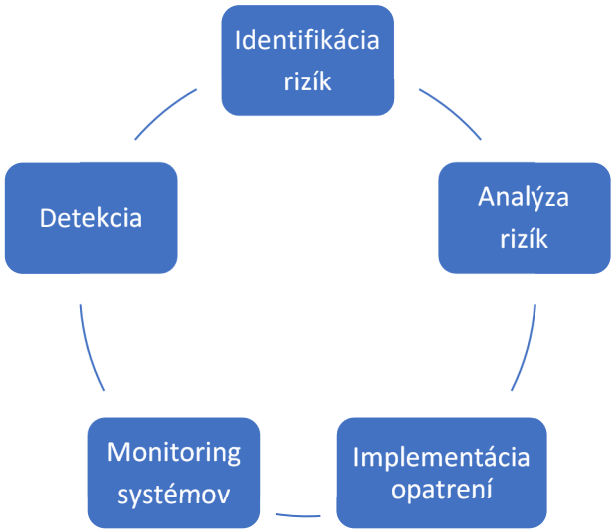
Kybernetická bezpečnosť zahŕňa rozsiahly komplex opatrení, metodík a kontrol. Nezameriava sa len na analýzu rizík, aj keď analýza rizík je veľmi podstatný nástroj informačnej a kybernetickej bezpečnosti. Správne nastavená kybernetická bezpečnosť je komplexný nástroj, ktorý pokrýva celú organizáciu. Vysvetlime si obrázok *„Zjednodušený cyklus kybernetickej bezpečnosti“.* Na vrchole trojuholníka je umiestnená Prevencia, pričom máme na mysli prevenciu vo všetkých jej podobách: nastavovanie ochrany riešení, správne nastavené pravidlá a tiež vzdelávanie. V časti Detekcia je zahrnutý sústavný monitoring, analýza incidentov a zraniteľností. No a na koniec všetko, čo sa identifikuje ako incident, hrozba alebo zraniteľnosť, sa musí pretaviť do konkrétnej Reakcie. Ak nastane incident, okamžite sa musí začať riešiť, zisťuje sa jeho kritickosť a dopad na fungovanie.

- V modelovej situácii s určitým rizikom incidentu je evidentný rozdiel, či padne zo stola pero alebo mobilný telefón. Pád pera na zem je pomerne častá a opakovaná udalosť, väčšinou bez následkov. Pád mobilného telefónu môže znamenať často nenávratné poškodenie zariadenia. Z uvedeného dôvodu je nutné jednoznačne viac kontrolovať a analyzovať incident súvisiaci s telefónom, pretože možná strata má väčší dopad a aj zariadenie má vyššiu mieru dôležitosti.
- Podobný rozdiel môžeme vidieť pri situácii so semaforom. Ak nefunguje semafor na dopravnom ihrisku, miera rizika je diametrálne odlišná od nefunkčnosti semaforu na križovatke veľkomesta. V rámci dopravného ihriska križovatka s pokazeným semaforom nespôsobuje nemožnosť používať dopravné ihrisko. Ak však nefungujú semafory na najväčšej dopravnej križovatke v meste, môže to znamenať dopravný kolaps celého mesta. Preto neustále zodpovedné zložky kontrolujú funkčnosť svetelného dopravného značenia a vyhodnocujú jeho odozvu, aby mohli predchádzať možným problémom.



Zjednodušený cyklus kybernetickej bezpečnosti

Predpokladom správneho fungovania životného cyklu kybernetickej bezpečnosti je zavedenie metodiky, procesov a opatrení do reálnej praxe. Pre zjednodušenie prístupu a zabezpečenie, že všetky dôležité kontroly budú nasadené, organizácia zvyčajne zavedie do procesov riadenia informačnej bezpečnosti bezpečnostnú normu. V prostredí strednej Európy je to zvyčajne komplex noriem ISO 27000. Je však nutné pripomenúť, že technické normy nie sú v našich podmienkach záväzné, ale majú len odporúčací charakter.



Cyklus manažovania rizík

Pre komplexné pochopenie stavu organizácie je nevyhnutne sústavne kontrolovať stav bezpečnosti a to na niekoľkých úrovniach:

- **sústavný monitoring prostredia**, sledovanie neželaných stavov a zneužití systému. Cieľom monitoringu je odhaliť nekalú aktivitu, napríklad útočníka.
- **pravidelná kontrola** rozdielu nastavenia bezpečnosti oproti želanému stavu, tak ako požadovaný stav organizácia určila vo svojich metodikách. Cieľom kontroly identifikovať nedostatky v nastavení bezpečnosti a vytvoriť prostredie na odstránenie.
- **hĺbkový audit** vybraných procesov voči zákonným požiadavkám a profesijným štandardom. Cieľom auditu je určiť zásadné rozdiely a nedostatky a kontrolovane ich odstrániť.

Výsledky jednotlivých kontrol sa pretavia do identifikovaných rizík. Na základe dopadu (ohodnotenia rizika) a na základe pravdepodobnosti materializovania rizika sa určí dôležitosť a zoradia sa riziká na riešenie. V prípade, že cena materializovaného rizika je ďaleko nižšia ako cena zníženia dopadu rizika (mitigácie), potom je na mieste zvážiť akceptáciu rizika. Ak je riziko akceptované, neznamená to že riziko zmizne (stratí sa), iba miera jeho možného

výskytu má nižší negatívny dopad ako jeho samotné predchádzanie. Každé riziko musí byť pravidelne prehodnocované. Všetko závisí od analýzy, ktorá bola vykonaná pri objavení rizika a od dopadov, pričom sa odporúča maximálne doba 12 mesiacov od akceptácie.

Identifikované riziko je možné ošetriť aj tzv. prenesením. Typickým príkladom prenesenia je poistenie rizika, pričom sa týmto spôsob zabezpečí čiastočná alebo aj úplná náhrada možných strát. V praktickom živote si prenesenie rizika takouto formou predstavte na príklade vášho mobilného telefónu - ak sa vám stáva často, že ho zničíte alebo stratíte a nedokážete toto riziko a jeho dopady znížiť opatreniami „u seba" - je možné ho poistiť. Prenesenie rizika však neznamená stratu zodpovednosti. Firma si môže znížiť stratu prenesením, ale zodpovednosť za prostriedky a ich ochranu je v kompetencii firmy.

Ak firma prevádzkuje eshop a nedostatočne chráni dáta svojich zákazníkov (a poistí sa voči pokute, ktorú dáva Úrad na ochranu osobných údajov), tak sa dostáva do situácie, že v prípade úniku osobných dát z eshopu bude pokuta uhradená poisťovňou. Nezbaví sa však zodpovednosti úplne. Ak vznikne na základe úniku týchto dát klientovi škoda, firma ju bude musieť nahradiť.

Kybernetická bezpečnosť je veda, ktorá sa zaoberá detegovaním (odhaľovaním a identifikáciou) rizík spojených s používaním počítača a ich eliminovaním. Prečo niečo také vôbec potrebujeme? Dnešný svet je založený na prepojení fyzického sveta so svetom virtuálnym (elektronická karta pacienta, možnosť objednať tovar z internetu, riadenie svetelných križovatiek počítačom a iné). Práve masívny nástup digitálnych prostriedkov do spoločnosti priam vyžaduje existenciu oblasti, ktorá sa bude starať o ich ochranu (napr. prevencia pred neoprávneným manipulovaním s dátami...).

- Nákup z obchodov sa presúva do internetového priestoru. Pre obchodníka je to rýchlejšie a jednoduchšie. Stráca sa nevyhnutnosť vlastniť predajňu, potreba dopĺňania skladu s tovarom, znižuje sa počet zamestnancov o zaškolených zamestnancov. Nie je potrebné riešiť spletitú sieť dodávateľov tovaru. Celý obchod je schovaný v kancelárii, kde sa zabezpečuje prijímanie objednávky, vyskladnenie z centrálneho skladu a odovzdanie prepravnej službe. Celkovo sa náklady na prevádzku eshopu zásadne znížia, a preto môže majiteľ znížiť aj cenu tovaru a zvýšiť tak svoju konkurencieschopnosť.

- V dávnych rokoch bola banková lúpež jedným z mála spôsobov, ako prísť k značnému finančnému obnosu. Na divokom západe ľudia museli naplánovať trasu vlaku, zistiť počet ochrancov trezora. No a na koniec bolo nevyhnutné mať pripravenú aj

únikovú cestu a spôsob, ako peniaze nenápadne použiť, aby to nebolo šerifom podozrivé. Dnes, prostredníctvom internetu, je možné ukradnúť peniaze „ťukaním do klávesnice“. Banky začínajú vyžadovať od ľudí čoraz viac používanie internetového bankovníctva – všetky informácie sú dostupné na internete. Rušia sa tiež fyzické pobočky (z dôvodu zníženia nákladov – banky nepotrebujú platiť za prenájom budov, kde sú umiestnené pobočky), zároveň sa zjednodušuje a zrýchľuje narábanie s peniazmi (finančné transakcie) a vo fyzických pobočkách sa naďalej poskytujú už len dôležité, náročné a zákonom stanovené úkony. Avšak zmenili sa aj zlodeji, stali sa neviditeľní, presunuli sa do priestoru internetu a vypátrať ich je náročnejšie než pri fyzickej krádeži.

3.1. Bezpečnostné štandardy

Najužitočnejšie poznatky, praktické rady a iné informácie sú navrhované, vytvárané a vydávané ako tzv. štandardy. Štandard je dokument, ktorý obsahuje pravidlá, smernice, procedúry a definície, ktorými sa musíme riadiť. Vznikajú ako dohoda medzi akademickou obcou, odborníkmi z praxe, špecialistov, zástupcov vlád, obchodu a iných subjektov.

Štandard je zverejnený dokument, ktorý obsahuje technické špecifikácie alebo iné presné kritériá, ktoré sa môžu používať ako pravidlá, smernice alebo definície. Štandardy majú podobu špecifikácií, metód, slovníkov, zásad dobrej praxe alebo návodov. Všetky formálne štandardy združujú názory a odborné znalosti z veľmi širokej škály záujmov zo strany spotrebiteľov, akademickej obce, špecialistov, vlády, obchodu a priemyslu. V dôsledku toho normy predstavujú konsenzus o súčasných osvedčených postupoch.[35]

[35] Štandardy informačnej bezpečnosti [online]. [cit. 13.6.2021]. Dostupné na internete: https://www.csirt.gov.sk/bezpecnostna-studovna/sulad/standardy-informacnej-bezpecnosti-877.html

Štandardy v oblasti informačnej bezpečnosti sú dokumenty, ktoré obsahujú procesy a odporúčania o spôsoboch (ako), predmete (čo) a dôvodoch (prečo) implementovania jednotlivých informácií a procesov do nášho bezpečnostného systému. Medzi najznámejšie štandardy patrí ISO 27000, FISMA/FIPS/NIST a BSI IT-Grundschutz. Podrobnejšie sa budeme zaoberať skupinou noriem ISO 27000 v ďalších knihách.

Do našej bezpečnostnej praxe sú princípy ISO noriem ISO 27000 implementované aj v niektorých vykonávacích vyhláškach k zákonom, ako napríklad:

- zákon o ochrane osobných údajov,
- zákon o informačných systémoch verejnej správy,
- zákon o kybernetickej bezpečnosti.

Vypíšte zoznam názvov všetkých štandardov v skupine ISO 27000 a popíšte zameranie jednotlivých štandardov.

Ktorá vyhláška týkajúca sa zákona o kybernetickej bezpečnosti pochádza zo štandardu ISO 27k? (zdroj: www.slov-lex.sk/)

Vysvetlite skratky FISMA, FIPS, NIST a BSI.

3.2. Kybernetická bezpečnosť na Slovensku

Na Slovensku bola prijatá koncepcia kybernetickej bezpečnosti na roky 2015 - 2020 a aktuálne pre roky 2021 - 2025, ktorá je východiskovým dokumentom pre tvorbu nových zákonov, štandardov, vyhlášok, pokynov či bezpečnostných politík potrebných k zabezpečeniu kybernetickej bezpečnosti Slovenskej republiky. Dôvod, prečo kompetentné orgány vybrali pomenovanie kybernetická a nie širšie informačná bezpečnosť je nejasný, hlavne ak časť aktivít koncepcie je zameraná na prechod z papierovej do digitálnej formy.

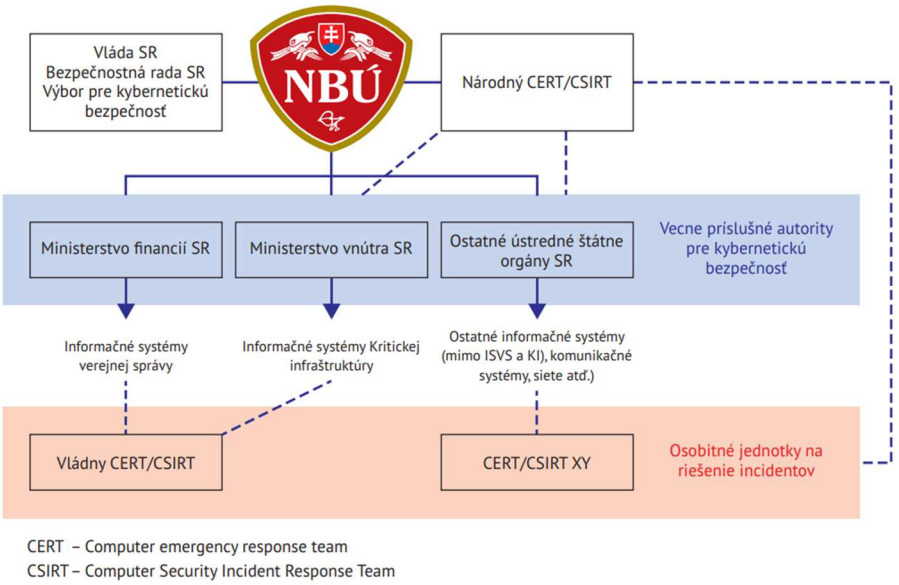
Vychádzajúc z aktuálneho stavu kybernetickej bezpečnosti v Slovenskej republike, cieľom koncepcie je dosiahnutie stavu, kedy:

- ochrana národného kybernetického priestoru je systémom fungujúcim koncepčne, koordinovane, efektívne, účinne a na právnom základe,
- bezpečnostné povedomie všetkých zložiek spoločnosti sa systematicky zvyšuje,
- súkromný a akademický sektor, ako aj občianska spoločnosť, sa aktívne zúčastňujú na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti,
- je zabezpečená efektívna spolupráca na národnej, ako aj medzinárodnej úrovni,
- prijaté opatrenia sú primerané a rešpektujú ochranu súkromia a základné ľudské práva a slobody.

Orgánom štátnej sféry, ktorý bol vytvorený pre potreby kyberbezpečnosti, je Národný bezpečnostný úrad. Tento má svoje kompetencie, pričom tu sú niektoré z nich[36]:

- vo svojej kompetencii má všetky úlohy v oblasti kyberbezpečnosti na národnej úrovni,
- vypracováva Správu o stave kybernetickej bezpečnosti v SR a predkladá ju Výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR,
- navrhuje postup v prípade kybernetického útoku počas krízovej situácie v SR,
- monitoruje a analyzuje kybernetický priestor a jeho možné hrozby.

[36] "Domov -NBU." [online]. [cit. 5.5.2021]. Dostupné na internete: https://www.nbu.gov.sk/.



Návrh rámcovej štruktúry riadenia kybernetickej bezpečnosti[37]

V rámci vypracovania Národnej stratégie kybernetickej bezpečnosti sa teda vytvoril koncept jednotky CERT/CSIRT pre analýzu stavu kybernetickej bezpečnosti a tiež pre analýzu a koordinované riešenie incidentov. Úlohou tejto jednotky je zabezpečovať systém včasného varovania, permanentne zvyšovať povedomie o rizikách spojených s aktivitami vykonávanými v on-line priestore a organizovať kampane v oblasti bezpečnosti sietí a informácií.

3.3. Osobné údaje

V bežnom živote sa vo svete nachádza množstvo rôznych údajov a informácií, či už o spoločnosti alebo o priestore, v ktorom žijeme. Všetky tieto údaje sa snažíme chrániť. Do tejto skupiny údajov patrí napríklad nákres budov aj s popisovaným zabezpečením (ten nikomu nedáme, ak nechceme uľahčiť vstup zlodejom do nášho

[37] "Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky ...." [online]. [cit. 5.5.2021]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf.

domu). Rovnako neposkytujeme len tak heslá od našich zariadení. Toto všetko boli príklady z bežného prostredia. Existuje však špecifická skupina údajov, ktoré sa týkajú priamo nás. Tieto údaje sú veľmi citlivé, popisujú nás, náš život, správanie a priestor, v ktorom žijeme.

Ochrana pracovného, súkromného, ale aj rodinného života, rovnako ako ochrana pred neoprávneným zhromažďovaním a spracúvaním citlivých údajov je základným ľudským právom, ktoré je definované tiež ako ústavné právo Ústavou Slovenskej republiky. Detailnejšie sú práva jednotlivcov (tzv. dotknutých osôb), ako aj podmienky narábania s osobnými údajmi v podmienkach Európskej únie, riadené nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov - GDPR[38]. Toto nariadenie je účinné, a teda záväzné od 25.mája 2018.

Citlivé **osobné údaje** sú informácie, ktoré umožňujú identifikovanie konkrétnej osoby. Musia byť chránené pred neoprávneným prístupom. Údaje týkajúce sa osoby, ako sú meno, adresa, rodné číslo, telefónne číslo, mailová adresa atď. sa považujú za citlivé podľa práva EÚ v oblasti ochrany údajov a sú osobitne chránené.

Vezmime si meno Anna. S týmto pomenovaním nevieme presne určiť osobu. Môžeme pridať ďalšie informácie, býva blízko školy, chodí na cvičenia z matematiky raz do týždňa. V zásade takýchto dievčat je veľa. Ak však povieme, že Anna je žiačka 3C z gymnázia v Zlatých Moravciach, počet ľudí sa zredukuje na konkrétneho človeka a Annu budeme vedieť presne identifikovať, ak pridáme k údajom adresu bydliska.

Existuje však **osobitná kategória osobných údajov**, špeciálne takých, ktorých zneužitie by viedlo k diskriminácii a ich prezradenie by viedlo k poškodeniu subjektu (osoby) samotného. Z uvedeného dôvodu sa pri použití týchto informácií vyžaduje zvláštna

[38] "32016R0679 - EN - EUR-Lex - EUR-Lex." [online]. [cit. 3.6.2021]. Dostupné na internete: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679.

ochrana pri ich spracovaní a ukladaní. Do tejto skupiny patria informácie ako zdravotný stav, náboženstvo, sexuálna orientácia, politické postoje, trestné delikty a aj genetické a biometrické informácie, ale len v prípade, že sa používajú na jedinečnú identifikáciu subjektu (napr. overenie pomocou biometrie).

Pre začatie spracúvania osobných údajov potrebuje mať prevádzkovateľ dôvod na ich spracovanie. Spracúvanie osobných údajov by malo byť zákonné, to znamená vykonávané v súlade so zákonom a dobrými mravmi a tiež by malo byť vykonávané na relevantnom právnom základe. Zákonný dôvod je ten, ktorý vyplýva zo zákona a predpokladom je nevyhnutné vedenie evidencie (napr. z dôvodu reklamácie produktov alebo evidencie študentov školou, evidencia zamestnancov). Druhou možnosťou je písomný súhlas so spracovaním osobných údajov, ktorý dáva **dotknutá osoba**. Súhlas musí obsahovať aj všetky spracovateľské činnosti, to znamená činnosti, ako sa bude s údajmi nakladať, ako a kde sa budú spracovávať. Napríklad pre účely vedenia študentskej a zamestnaneckej dokumentácie nie je potrebné mať súhlas, pretože spracovanie a uchovávanie údajov vychádza zo zákona, avšak analýza správania zamestnancov zo zákona nevychádza, preto je pre ňu potrebný vyžiadaný súhlas. Pri objednávaní z eshopu je realizácia spracovania mojich údajov na dodanie tovaru, na základe zmluvného vzťahu.

Na priloženej adrese je tabuľka účelov spracúvania osobných údajov na Univerzite Komenského v Bratislave:

https://uniba.sk/fileadmin/ruk/uradna_vyveska/oou/Tabulka_ucelov.pdf

Vysvetlite, prečo patrí uchovávanie správania v systémoch medzi veľmi citlivé osobné údaje, teda do osobitnej kategórie osobných údajov (pomôžte si kapitolou Digitálna identita)?

Navrhnite rôzne množiny údajov, na základe ktorých viete identifikovať konkrétnu osobu a teda by mohli byť považované za osobný údaj a chránené podľa GDPR.

Citlivé osobné dáta sú teda osobné dáta, ktorých únik, zneužitie a použitie môže poškodiť konkrétneho človeka. Ujma, ktorá sa môže človeku stať, môže byť:

- finančná,
- majetková,
- psychická,
- kombinovaná.

Pod úlohou je zoznam údajov, roztrieďte ich podľa citlivosti na skupinu citlivé osobné údaje a osobitnú kategóriu osobných údajov:

meno, priezvisko a adresa / číslo občianskeho preukazu / hlasová vzorka potrebná na identifikáciu konkrétneho človeka / hlasové vzorky ľudí nad 30 rokov z okresu Zlaté Moravce/ dátum narodenia / tri najčastejšie choroby študentov 1A triedy / meno priezvisko, adresa a zdravotné informácie / emailová adresa v tvare meno_priezvisko@menofirmy.sk

Rozdeľte údaje z predchádzajúceho príkladu na dáta a informácie.

Popíšte, aké typy citlivých dát má vaša rodina doma.

Popíšte, aké typy citlivých dát spracováva vaša škola.

Popíšte, aké typy citlivých dát potrebuje firma a za akých okolností.

Aké riziká hrozia dátam z predchádzajúcej úlohy a aké zmierňovacie (mitigačné) opatrenia doma používate na ochranu týchto dát?

Ktoré údaje sú chápané ako citlivé v rámci sociálnych sietí?

Aké ochranné postupy odporúčate používať na ochranu citlivých údajov?

Stretli ste sa s útokmi na sociálnych sieťach s cieľom využiť alebo zneužiť osobné dáta?

1. Ako si môžeme chrániť osobné údaje?

Ochrániť si svoje osobné údaje by malo byť prioritou každého človeka, preto ***majte svoje osobné doklady stále pod kontrolou***. Poskytuje ich len na nevyhnutnú dobu, pričom ich nikdy nespúšťajte z očí. Ak niekto kopíruje vaše doklady, zistite dôvod tejto potreby a zvážte oprávnenosť požiadavky.

- Všetky ***dokumenty*** s citlivými, osobnými údajmi ***pred ich odstránením (vyhodením) zničte***. Nevyhadzujte ich do koša v celej forme, pretože neviete, kto ich bude čítať.
- V rámci internetu ***vypĺňajte len nevyhnutný počet osobných, citlivých údajov.*** Nepovoľujte spracovanie svojich informácií na dlhšiu dobu ako nevyhnutne plánujete využívať službu a len v rozsahu, ktorý potrebujete. Zvážte prenos spracovania vašich údajov na tretie strany.
- ***Neposkytujte osobné údaje pri telefonických rozhovoroch***, pokiaľ ste si volajúceho neoverili a nie je na 100% isté, kto je volajúci.
- ***Neposkytujte osobné údaje pri priateľských rozhovoroch*** neznámym alebo práve predstaveným osobám. Rovnako neprezrádzajte zaujímavé zážitky alebo iné okolnosti, ktoré by mohli byť zneužité proti vám.
- **Ak podpisujete (virtuálne, resp. fyzicky) dokument, dobre si ho prečítajte** a skontrolujte, či obsahuje všetky dohodnuté dáta a nevyhnutné náležitosti. V prípade, že podpisujete súhlas na spracovanie osobných údajov, musí súhlas obsahovať aj spôsob spracovania a adresáta (komu), ktorému budú vaše údaje poskytnuté na spracovanie.

2. Čo nám hrozí, ak sa citlivé informácie prezradia?

Často zabúdame, že rovnako, ako sa správame na ulici, v každodennom živote, je nevyhnutné správať sa v digitálnom priestore. Na ulici nikto nikomu bez vyzvania neukáže občiansky preukaz a nedovolí mu urobiť kópiu, vo virtuálnom priestore sa to bežne stáva. Pripomeňme si zásadné poznanie z prvej kapitoly.

Internet je anonymný. Preto, ak ktokoľvek získa vaše údaje, môže s nimi urobiť čokoľvek a málokedy urobí niečo dobré (pozitívne). Čo nám teda hrozí?

- Pri zverejnení kontaktných údajov môže ktokoľvek kontaktovať obeť.
- Prezradenie osobných údajov môže vytvoriť z obete terč s cieľom urážania, posmechu a pohŕdania, často aj vydierania.
- Pri získaní hesla na free email alebo sociálne siete útočník preberie konto, a tým aj riadenie komunikácie.
- Fotografie spojené s konkrétnym človekom môže použiť ktokoľvek, kdekoľvek a môže si ich upraviť akýmkoľvek spôsobom.
- Čím viac informácií o sebe obeť prezradí, tým viac je možné ju vydierať a tým ľahšie bude jej prenasledovanie, pričom často ide o prenasledovanie so sexuálnym podtónom (sextortion).

3. Ako sa máme brániť?

- Nad všetkými radami vládnu tri poučky:
    - *Len ja sám si vytváram obraz o sebe.*
    - *Nezverejňujte o sebe informácie a fotografie, ktoré by ste neukázali o sebe svojim rodičom.*
    - *Ak niektoré dáta nechcete zverejňovať, potom takéto dáta by ani nemali vznikať.*
- Zvažujte, čo o sebe poviete, komu a kde, vždy počítajte s tým, že tento údaj zostane na internete navždy a ktokoľvek môže mať k nemu prístup. A to nielen na sociálnych sieťach, ale aj pri četovaní.
- Fotografie a videá podrobne preskúmajte pred ich vydaním, aby neprezradili viac, ako je potrebné. Videá a fotky môžu poskytnúť množstvo informácií z nášho súkromia.
- Osobné údaje: adresa, telefón, kontakty, kontakty v sociálnych sieťach nie sú vhodné na zverejnenie.
- Neposkytujte emailovú adresu na sociálnych sieťach, resp. komukoľvek, vyhnete sa tak obťažovaniu a zbytočnému kontaktovaniu.
- Čítajte všetky povolenia na internete o spracovaní osobných údajov a cookies, nepovoľujte automaticky všetky možnosti pre všetkých dodávateľov.

- Internet nie je miesto na publikovanie vyhranených a urážlivých príspevkov.
- Pre komunikáciu na chatoch, fórach, internetových diskusiách a blogoch používajte neurážlivú, nevyzývavú prezývku a emailovú adresu, ktorá nie je vaša prioritná (hlavná).
- Ak publikujete fotky kamarátov, žiadajte si od nich schválenie publikácie a to isté vyžadujte recipročne (spätne od nich). Platí to aj v prípade publikovania detských fotografií rodičmi. Rodičia si by si mali pýtať povolenie od detí.
- Riaďte (rozhodujte o povoleniach) prístup k svojim informáciám na sociálnych sieťach: kto, čo a ako dlho môže vidieť zvolenú informáciu.

4. Príklady zo života

Krádež identity

Predátor na sociálnej sieti pomocou neoprávnene získaných osobných údajov vytvára svoju falošnú identitu (falošný profil) a prostredníctvom tohto profilu nadväzuje komunikáciu s inými používateľmi rôznych sociálnych sietí za účelom nelegálnych aktivít (kyberšikanovanie, šírenie škodlivého kódu, šírenie nelegálnej reklamy, získavanie dôverných informácií za účelom vydierania).

Často sa získanie osobných údajov pretaví do veľmi nebezpečných útokov ako je sextortion a cyberstalking.

Sextortion je vymáhanie informácií rôznymi spôsobmi, napríklad zneužitím alebo vyžiadaním obrázkov či videí sexuálnej povahy. Takéto správanie je trestným činom podľa § 376 trestného zákona - poškodzovanie cudzích práv. Často sa tak stáva dobrovoľne, ak partner/partnerka pošle takýto materiál svojmu partnerovi/partnerke. Ak je priateľstvo ukončené násilne (vynútene) jedným z partnerov, ten druhý sa mu chce pomstiť a zverejní materiál. Na internete sa následne objavujú vyzývavé fotky označené drsným jazykom, z dôvodu zaujatia pozornosti

(aby boli „in“). Sexuálny útok na internete však môže mať aj podobu krádeže identity. Vyskytli sa dokonca prípady, keď za profilom umierajúceho dvanásťročného dieťaťa sa ukrýval sexuálny násilník. Základnou ochranou pred sextortion je:

1. nikdy neposielajte nikomu intímne fotky alebo videá,
2. nikdy neposielajte nikomu vyzývavé správy alebo emaily,
3. ak máte priateľov, ktorých ste nikdy nevideli, potom im neposielajte nič dôverné,
4. ak máte problém s vydieračom vy alebo niekto z vášho okolia, kontaktujte svojich rodičov, učiteľa, školského psychológa alebo linku dôvery.

Cyberstalking je druh prenasledovania, pri ktorom sa využívajú informačno-komunikačné technológie (IKT). Hlavnými dôvodmi je obťažovanie, prenasledovanie alebo vydieranie. Takéto činy sú trestné, podľa § 360a (1) trestného zákona, sú kategorizované ako nebezpečné prenasledovanie. Tento druh prenasledovania je populárny najmä kvôli anonymite, potenciálne veľkému objemu prístupných dát a v neposlednom rade aj nízkej prevádzkovej cene. Ide o opakovanú činnosť, ktorá sa zvyčajne stupňuje.

1. Predátor opakovane kontaktuje obeť: SMS, email, messenger, telefonáty.
2. Demonštrovanie moci a rozsievanie strachu - stalker sa začne vyhrážať obeti, kontrolovať obeť, často aj fyzicky. Cieľom je presvedčiť obeť, že sa nemôže zachrániť pred prenasledovaním, pretože je sústavne atakovaná vyjadreniami: viem, kde si, viem čo robíš, sledujem ťa na každom kroku a podobné.
3. Stalker sa snaží poškodiť alebo zničiť majetok obete, napríklad rozbíjaním okien, poškrabaním auta, rozrezaním pneumatík, preniknutím do zariadení obete a ich ničením.
4. Stalker sa v určitej chvíli snaží prebrať obeti jej kontá alebo vytvoriť falošné, podobné. Následne sa za obeť vydáva.

5. Očiernenie obete a prebratie priateľov - stalker sa dostáva stále bližšie k obeti, snaží sa presvedčiť blízkych priateľov a príbuzných, že obeť je zlá a robí zle, za účelom, aby zostala obeť sama. Niekedy vystupuje ako poškodený obeťou, a preto vyžaduje pomoc od ostatných.

Ak máte problém so stalkerom vy alebo niekto z vášho okolia, kontaktujte svojich rodičov, učiteľa, školského psychológa alebo linku dôvery.

Následná schéma popisuje priebeh konania útočníka v 4 základných fázach:

- **príprava** - útočník z rôznych zozbieraných dát vytvára svoj fiktívny profil používaný na následné kontaktovanie potenciálnych obetí,
- **komunikácia** - útočník ju využíva za účelom na prvotného kontaktu a následné prehlbovanie dôvery smerujúcej k vytvoreniu silného „virtuálneho" priateľstva a dôvery,
- **získavanie kompromitujúcich informácií** – útočník, stále v roli dôverného priateľa, získava od potenciálnej obete informácie použiteľné pre vydieranie (najčastejšie intímne fotografie a videosnímky),
- **vydieranie** - útočník odhaľuje svoj skutočný zámer (nie identitu) a požaduje od obete splnenie požiadaviek - osobné stretnutie, zaplatenie „výpalného" a podobne.

Priebeh konania útočníka

Zneužitie osobných údajov na sociálnych sieťach je častým problémom. Jedným z pomerne závažných, s nie malým finančným dopadom, je odcudzenie FB účtu a jeho následné zneužitie. V roku 2020 sa prvýkrát objavila informácia o probléme nedostatočne zabezpečených osobných FB účtov[39], ktoré boli previazané na firemné účty a využívané na objednávanie reklám na FB.

Útočník, ktorý získal prístup k účtu mal tak možnosť:

- vystupovať pod týmto účtom (akoby bol vlastníkom),
- zablokovať prístup skutočnému vlastníkovi,
- objednávať na tento účet reklamy,
- robiť finančné transakcie - nakoľko v prípade využívania reklamných služieb FB je účet automaticky (povinne) naviazaný na účet v banke resp. inej platobnej služby ako napr.PayPal - dochádzalo automaticky k sťahovaniu finančných prostriedkov z bankového účtu skutočného vlastníka účtu (zakladajúceho).

[39] Prípad ukradnutia dát je popísaný v článku: After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users [online]. [15.08.2021] Dostupné online: https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users?t=1628519702921

3.4. Správanie na sociálnych sieťach

V súčasnosti je internet prirodzenou súčasťou nášho života. Zapájame sa do tohto života rôznymi spôsobmi, od vyhľadávačov, cez rôzne systémy na posielanie správ, až po zdieľanie našich životných príbehov a pocitov. Vzhľadom na typ tohto priestoru a obmedzenia v ňom, musíme sociálne siete považovať za verejný priestor. Naši kamaráti a aj široká verejnosť spoznáva cez „lajkovanie“ a „publikovanie“ našich postojov nás samotných i naše najtajnejšie názory. Nesmieme však zabúdať, že tie isté nástroje ako my, používajú aj útočníci a často sociálno-patologické osoby pre svoje pobavenie, resp. obohatenie sa. Zároveň o nás zbiera a spracováva informácie samotná sociálna sieť. Tieto sú neskôr použité na marketingové účely a záleží už len na forme, akou budú poskytnuté ďalším subjektom (tretej strane). Sociálne siete, vrátane ich aplikácií, predstavujú jednu z najrizikovejších foriem internetových služieb z viacerých dôvodov:

- existencia veľkého počtu sociálnych sietí s rôznou úrovňou bezpečnosti garantovanej zo strany prevádzkovateľa – jedná sa o zabudované bezpečnostné funkcie, ale aj schopnosti reagovať na bezpečnostné incidenty,
- existencia veľkého počtu používateľov rôzneho veku, s rôznymi úrovňami bezpečnostných vedomostí a návykov,
- výskyt používateľov sociálnych sietí, ktorí majú nekalé zámery - podvodníci, predátori.

Pre zvyšovanie bezpečnosti používania sociálnych sietí je preto nutné osvojiť si nielen pravidlá slušného správania na internete (netiketu), ale tiež základné princípy bezpečnosti.

Na príklade sociálnej siete Facebook si predstavme, aké typy dát sociálna sieť zbiera a spracováva. Rozdeľme si ich do niekoľkých typov:

1. osobné údaje: meno, priezvisko, adresa, dátum narodenia, rodina, pohlavie, email, vzdelanie, práca, platobné karty, vzťah
2. správanie: príspevky, vyhľadávanie, chat, odkiaľ sa prihlasujete, politické názory, vývoj správania (cez vymazané príspevky), cookies, stav baterky, informácie o prehliadači
3. sociálny status: kamarátov, prepojenia s kamarátmi, záujmové skupiny

Samozrejme, príkladov môže byť aj viac, avšak už z tohto zoznamu je jasné, aké je dôležité o sebe nezverejňovať priveľa vecí. Na jednej strane síce pomôžete sociálnej sieti na vás lepšie cieliť reklamu a možno z časti aj záujmové príspevky (presné cielenie príspevkov podľa vášho záujmu však môžu pre vás znamenať prílev len jedného typu údajov, a teda aj to, že časť dát z bežného života vám bude chýbať). Na strane druhej je dôležité dbať na správny výber priateľov, pretože všetko, čo sa rozhodnete zverejniť, bude niekto vidieť. Ten niekto by nemal mať potrebu alebo motiváciu zneužiť vaše dáta. No a nakoniec, naozaj veľmi dobre zvažujte, aké dáta budete zverejňovať pre verejnosť. Verejnosti dostupné dáta budú zverejnené naveky, aj v čase vašej dospelosti a aj starobe. Možno niektoré príspevky budú čítať vaši budúci zamestnávatelia, budúci partner, deti či vnuci, a preto je lepšie používať pravidlo: „*Dvakrát meraj a raz strihaj*.".

Na základe predchádzajúceho článku, vysvetlite, v čom tkvie myšlienka: Sociálne siete nie sú zadarmo.

1. Odporúčania pre sociálne siete

Náš svet, ktorý si popisujeme, je virtuálny a my sa snažíme v ňom vyznať. Keďže v tomto svete neexistujú jasné pravidlá, zadefinujme si zásadu.

Zásada: akýkoľvek záznam, fotografia, nahrávka, kde sa nachádza aj iná osoba ako vy, táto osoba musí o nahrávke vedieť a súhlasiť s ňou.

Priatelia (každý jeden) musia súhlasiť so zverejnením fotografie na sociálnej sieti, ak ju zverejňujete vy. Zároveň musia súhlasiť s videom, na ktorom sa nachádzajú, s nahrávkou alebo aj citáciou, ktorú od nich prevezmete. V opačnom prípade ich zverejňovať nesmiete. Ak to urobíte, tak nielenže prídete o priateľov, ale zároveň porušíte zásady spracovania osobných údajov.

Prečo treba neustále sledovať čo, kto, kedy a ako zverejňuje? Pretože existuje veľa hrozieb, ktoré nás obklopujú. Predstavte si, že niekto zoberie fotografiu, pozmení jej obsah a vám alebo vášmu kamarátovi tým uškodí. Predstavte si, že sa toto stane s vašou zverejnenou intímnou fotkou, ktorú ste poslali najlepšiemu kamarátovi alebo kamarátke. Nemusí ju ďalej poslať kamarát, kamarátovi môže „heknúť" počítač, mobil, účet na sociálnej sieti niekto iný a vaše dáta budú zverejnené, pričom vy ani neviete komu.

Rovnako narábajte správne s označovaním priateľov na fotografiách. Predstavte si, že vás niekto označí na fotografii v určitej skupine, ktorá sa po istom čase začne venovať terorizmu. Ak sa vám to stane, neschvaľujte dané označenie alebo požiadajte dotyčnú osobu o vymazanie označenia.

- **Nezabúdajte**: zodpovednosť za príspevky nesie ten, kto príspevok uverejňuje. Zverejnenie negatívneho, alebo ohováračského príspevku má dopad na vás aj z trestnoprávneho pohľadu, môže sa to kategorizovať ako trestný čin Ohovárania podľa § 373 trestného zákona. Napríklad ohováranie sa veľmi často rieši s dotknutou osobou v občiansko-právnom spore, teda súdnou cestou. Ak používatelia sociálnych sietí zverejňujú rôzne obrázky, knihy, videá, či nahrávky piesní, ktoré im nepatria, porušujú tým práva autora a vlastníka diela, čo je rovnako trestný čin. Do takýchto aktivít patrí aj používanie značiek známych spoločností, ako sú výrobcovia sladených nealkoholických nápojov alebo značky áut. Tieto značky sú chránené a ich používanie je regulované.

Predchádzajúce vety upozorňujú na zákaz zverejňovania autorských diel, presné možnosti upravuje Autorský zákon. Existujú tieto

základné možnosti, kedy je možné použiť dielo autora bez súhlasu autora:

1. pri komentovaní, citovaní a recenzovaní diela,
2. pri voľných dielach, to znamená, že autor publikoval svoju prácu s neobmedzeným povolením alebo od smrti autora ubehlo viac ako 70 rokov.

2. Aplikácie a členstvo v skupinách nie je zadarmo

Povedali sme si, aké nebezpečné je prezentovať svoje vlastné názory v negatívnych konotáciach (okolnostiach). To však nie je všetko, v rámci sociálnych sietí existujú rôzne skupiny, ktoré prezentujú nielen pozitívne, ale často aj negatívne názory. Veľmi často sú to názory extrémistické či teroristické. Členstvom v extrémistických skupinách dávate najavo svoj postoj, ktorý môže byť konfrontovaný v prípade podozrenia skupiny zo spáchania trestného činu aj s orgánmi činnými v trestnom konaní (polícia). Často sa stáva, že zameranie skupiny sa zmení po výmene administrátora a zo skupiny s dobrým zameraním sa stane skupina podporujúca nenávistné správanie. Rovnako zverejnenie vlastného postoja, resp. vyjadrenie kladného názoru na nejakú vec, môže byť kontraproduktívne. Dobrým pozitívnym postojom k produktom konkurencie a kritickým postojom ku produktom vlastnej firmy dávate najavo svoj nestabilný postoj voči zamestnávateľovi.

Najlepšou prevenciou pred problémami je sledovať jednotlivé skupiny, kde ste prihlásení. Ak nesúhlasíte s príspevkami v konkrétnej skupine a smerovaním skupiny, odhláste sa z nej.

Sociálne siete umožňujú rôznym spoločnostiam vytvoriť aplikácie pre používateľov. V prípade získania informácií na používateľskej úrovni si stačí uvedomiť, že svojim súhlasom s používaním aplikácie súhlasíte aj s odovzdaním vašich dát ďalšiemu spracovateľovi, ktorý môže byť kdekoľvek na zemeguli.

Vždy, keď povoľujete prístup novej aplikácie v rámci sociálnej siete k vašim dátam, presvedčte sa, ktoré dáta budú poskytnuté a

komu. Následne si položte otázku, či je to naozaj nevyhnutné a či aplikácia, ktorú chcete, prináša požadovaný úžitok. Takto odovzdané dáta sa často používajú v útokoch, napr. útok ako je phishing, viď kapitola Phishing.

3. Ako sa správať na internete[40]

Základné pravidlá slušného spoločensky akceptovateľného správania voči ostatným používateľom internetových služieb sa začali formovať už pri vzniku prvých sociálnych sietí, kedy sa javilo potrebné zadefinovať principiálne zásady vzájomného správania sa. Vznikol tak súbor pravidiel, podobne ako v reálnom živote, pre ktorý sa používa slangový názov NETIKETA. Jej princípy sú:

- Nikdy nezabúdajte, že na druhom konci sú ľudia a nie počítač. To, čo anonymne napíšete stroju, by ste možno nikdy nepovedali dotyčnému do očí.
- Dodržiavajte všetky pravidlá slušnosti z každodenného života. Čo je zlé v bežnom živote, bude určite nevhodné aj na internete.
- Zistite si, v akej spoločnosti sa nachádzate. Cez internet totiž komunikujete s ľuďmi z celého sveta a čo je v jednej skupine na internete dovolené, iná to môže považovať za neprípustné. Politika, náboženstvo a iné rozporuplné témy by mali byť diskutované s maximálnou ohľaduplnosťou a taktom.
- Majte ohľad k druhým. Nie každý má rýchle internetové pripojenie ako vy. Často, hlavne v zahraničí je pripojenie spoplatnené a je nevyhnutné kupovať balíky dát. Neposielajte zbytočné a neprimerane veľké správy.
- Nebuďte grobianom, práve naopak, ukážte, že ste inteligentná bytosť. Aj keď píšete bez diakritiky (bez dĺžňov a mäkčeňov) snažte sa o správny pravopis. Publikovať nepravdivé informácie, alebo niekoho ohovárať, tiež nie je vhodné.

[40] Netiketa [online]. [26.6.2021]. Dostupné na internete: https://sk.wikipedia.org/wiki/Netiketa

- Pomôžte, ak viete. Zaujíma vás nejaká téma a sledujete nejakú diskusiu k nej? Niekto z diskusnej skupiny má nejaký problém. Ak viete odpoveď, pomôžte. Nabudúce pomôže niekto vám. V diskusnej skupine platí zásada „Najprv počúvaj, až potom píš."
- Rešpektujte súkromie iných. Omylom vám prišla správa, ktorá vám nepatrí? Správajte sa tak, ako by ste chceli, keby niekto iný našiel vašu poštu.
- Nezneužívajte svoju moc a vedomosti. Používatelia so špeciálnymi privilégiami, napr. správcovia serverov, ktorí majú prístup k pošte ostatných, musia mať dôveru bežných používateľov.
- Odpúšťajte druhým chyby. Aj vy ste niekedy začínali. Nemusíte hneď reagovať výsmešne alebo so zlosťou.
- Nerozosielajte reťazové listy a poplašné správy typu hoax. Upozornite aj ostatných, že takéto správanie je nevhodné.
- Nerozosielajte spam – správy s reklamným textom. Upozornite i ostatných, že takéto správanie je nevhodné.
- Rešpektujte autorské práva iných. Nepublikujte cudzí text pod svojim menom, vždy uvádzajte meno pravého autora a zdroj odkiaľ citujete. Nevydávajte za svoju prácu niekoho iného. Obrázky, texty a rôzne iné súbory sa z internetu dajú ľahko stiahnuť. Akoby sa vám páčilo, keby niekto iný vydával vaše dielo za svoje? Ak využijete prácu iných, mali by ste spomenúť ich autorstvo.

4. Útočníci, útoky a obrana na sociálnych sieťach.

Medzi používateľov sociálnych sietí nepatria len takí, ktorí majú záujem o slušnú komunikáciu, zábavu či vzdelávanie. Sociálna sieť je zároveň miesto, kde sa môžu nachádzať aj ľudia so zámerom škodiť a ubližovať ostatným (tzv. kriminálne živly). Našou úlohou je rozpoznať zlé správanie a vedieť, ako správne reagovať, alebo ako sa zlému správaniu vyvarovať.

Veľmi častým spôsobom zneužívania sociálnej siete je napadnutie pomocou metód sociálneho inžinierstva. Tieto metódy sú rozsiahle a komplexne pokrývajú správanie každého človeka. Metódy sme si priblížili v časti manipulatívne techniky. Ako však predchádzať útoku uskutočnenému prostredníctvom sociálneho inžinierstva? Najbezpečnejšie je, ako sme už spomínali, nezverejňovať o sebe žiadne podstatné dáta, aby útočník o nás vedel čo najmenej a nemohol sa dobre pripraviť na možné zneužitie našich osobných informácií. Základné pravidlá sú:

1. Nepoužívajte jedno heslo pre viacero služieb.
2. Vami zvolené heslo musí byť silné (popis je v kapitole: 6.6.1.2 Bezpečnostné odporúčania pre nastavenie hesiel).
3. Zverejňujte o sebe čo najmenej.
4. Ak ste niečo zverejnili, zvážte, či to môžete sprístupniť všetkým.
5. Ak sa niekto cudzí tvári ako kamarát, nezverujte sa mu s citlivými a osobnými vecami.
6. Vyhýbajte sa formulárom z neznámeho zdroja a s neznámym určením.
7. Vyhýbajte sa reťazovým správam.

V prípade, ak vaše konto bolo prebraté útočníkom, oznámte svojim kamarátom túto skutočnosť, aby nereagovali na kontakty a neklikali na linky, ktoré by potenciálne mohli z „heknutého“ konta dostávať.

Samozrejmou súčasťou sociálnych sietí sa stáva podhadzovanie malvéru v rámci sociálnych sietí. Najčastejšie je malvér schovaný za obrázky, videá, virálne videá, ale je možné ho prijať aj cez messenger systémy ako prílohu alebo linku na malvér. Prostredie sociálnych sietí je žičlivé pre tvorcov škodlivého kódu. Pripomeňme si aspoň niektoré postupy, ktoré nás budú chrániť:

- Kontrolujte aplikácie na sociálnych sieťach a riaďte ich prístupy.
- Pravidelne si kontrolujte priateľov na sociálnych sieťach. Ak ich nepoznáte alebo im nedôverujete, zrušte ich zo zoznamu.
- Zálohujte si všetky svoje údaje na nezávislý pamäťový nosič.

Samozrejmosťou pre vašu prácu je mať pod kontrolou zariadenie, ktoré používate, a preto nezabúdajte na ochranu svojho zariadenia minimálne prostredníctvom používania Antivírusu a firewallu.

Všetky predchádzajúce rady sa vám môžu zdať veľmi prísne. Avšak dopady prípadnej straty kontroly nad kontom na sociálnej sieti alebo straty údajov z tohto konta sú oveľa väčšie a môžu byť pre vás veľmi nebezpečné.

5. Správanie sa v diskusiách

Ako sa správať v rámci sociálnych sietí, to už vieme, zoznámme sa teraz so zaujímavým spôsobom, ako narúšať diskusiu v rámci četu.

Sociálne siete sú plné dobrého a povzbudzujúceho, ale aj zvláštneho správania. Za pozornosť stojí napríklad jedna z foriem správania sa, ktoré je používané v diskusiách veľmi často a považuje sa za najnebezpečnejšie: **trolling**. Osoba (pomenovávame ho **troll**), používajúca trolling má za cieľ provokovať, urážať, zmeniť tému, jednoducho chce za každú cenu narušiť diskusiu. V súčasnosti už nejde iba o jednotlivcov, ktorí si propagujú vlastné ciele. Stále častejšie hovoríme o tzv. organizovanej propagande, ktorá má za cieľ dezinformovať, propagovať tovar, zavádzať. V súčasnosti sa bežným stáva používanie slovných spojení ako trollie farmy alebo trollie armády. Títo organizovaní „trollovia“ sú platení firmami alebo štátmi a svoje útoky nerobia z vlastného presvedčenia. Implementovaním stále aktívnejšej robotiky do všetkých sfér ľudskej činnosti sa čoraz častejšie používajú na trollovanie roboty, ktoré sú naprogramované na konkrétne témy, alebo vyhľadávanie diskusií s určitým zameraním, do ktorých následne vkladajú stále rovnaké vety.

Symbol: Nekŕmte trollov[41]

S trollmi je veľmi ťažké bojovať, ak neriadite konkrétnu diskusiu. Existuje niekoľko skratiek, ktoré znamenajú označovanie trollov alebo reakcie na trollov. Aktivita boja proti trolom má svoj symbol, viď obrázok: *Symbol: Nekŕmte trollov*.

Toto sú skratky používané pri označovaní trollov:

Výzva, často používaná ako odpoveď na trollov príspevok.

- DNFTT. – Do not feed the trolls. (Nekŕmte trolov.)

Odpoveď na reakciu na trollov príspevok:

- YHBT. – You have been trolled. (Bol si trolovaný.)
- YHL. - You have lost. (Prehral si.)
- HAND. - Have a nice day. (Prajem krásny deň.)

Najlepšia obrana pred trollovaním ja označovanie trollovacích príspevkov alebo nereagovanie na takýto príspevok. Vo virtuálnom svete existujú aj tzv. bojovníci proti trollom. Bojovníci proti trollingu sa

[41] Internet troll; dostupné online [online]. [25.06.2021]. Dostupné na internete: https://en.wikipedia.org/wiki/Internet_troll

nazývajú **elfovia**, ktorí pod falošnými profilmi bojujú s trollingom a odhaľujú klamstvá v jednotlivých príspevkoch.

Úlohou každého účastníka virtuálnej diskusie je viesť slušnú konverzáciu. Pre komunikáciu s jedným človekom sme si zopakovali Netiketu. Najčastejšie a najživšie konverzácie však prebiehajú v skupinových četoch. Prejdime si jednotlivé kroky, ako sa v nich správať, pričom sa musíme vyvarovať situáciám, že našu komunikáciu budú ostatní považovať za trollovanie. Aby sa toto nestalo, zaužívali sa nasledovné body:

- Nezačínajte komunikovať v noci, keď väčšina ľudí spí. V tomto prípade je veľká pravdepodobnosť, že na diskusiu budú členovia skupiny nahliadať ako na otravnú a nebudú k nej pristupovať konštruktívne.
- Udržujte jednu tému, neodbočujte od témy a nekošaťte ju (zbytočne ju nerozvíjajte). Zbytočným košatením sa jednotliví členovia začnú strácať a cieľ diskusie sa dosiahne veľmi ťažko.
- Konverzujte so všetkými členmi skupiny, aby sa ostatní členovia necítili ostrakizovaní (vylúčení z diskusie).
- Neprerušujte tok vysvetľovania diskutujúceho v rámci konverzácie, neskáčte inému do reči, nechajte ho vyjadriť sa.
- Nehodnoťte iný príspevok, stavajte sa vecne ku každému príspevku a zaoberajte sa len témou.
- Píšte čo najmenej správ, nerozbíjajte svoje texty do jednotlivých správ, je to otravné a smajlík žiadnu hodnotnú informáciu neprinesie.

Nezabudnite si vypnúť notifikácie z chatov, pretože nič tak nepokazí zážitok z kina, ako stále pípajúci mobil.

ostrakizovať - vylúčiť zo spoločnosti, ignorovať, zbaviť sa, dať bokom.

6. Nebezpečenstvo číhajúce na sociálnych sieťach

Pripomeňme si najčastejšie útoky, ktoré sa vyskytujú na sociálnych sieťach:

- falošné súťaže, ktoré žiadajú o vyplnenie kartových alebo osobných údajov,
- virálne videá, obrázok so schovaným linkom so škodlivou stránkou,
- zdieľanie citlivých dát o sebe napr. fotky, osobné údaje a pod.,
- možnosť nabúrania sa útočníka narušiteľa do vašich účtov - prihlasovanie sa cez sociálne siete je nebezpečným správaním. A ak sa niekto hekne do vášho konta, môže sa heknúť aj do ďalších aplikácii,
- manipulácia pomocou techník sociálneho inžinierstva.

Sociálne siete napriek všetkým hrozbám prinášajú obrovské výhody a otvárajú úžasné množstvo príležitostí na kooperáciu a zdieľanie nápadov, skúseností a know-how. Našou úlohou je tieto príležitosti využiť, a aby to boli naozaj príležitosti bez nebezpečenstva, v predchádzajúcich kapitolách sme sa naučili, na čo si máme dávať pozor.

3.5. Počítačová kriminalita

Nie všetko s čím sa stretávame na internete je pozitívne. Niektorí používatelia využívajú internet na aktivity, ktoré môžu presahovať hranice etiky, morálky alebo až hranice zákona, čo sa už definuje ako trestná činnosť. Pre pochopenie významu pojmu počítačová kriminalita môžeme využiť informácie z Dohovoru o počítačovej kriminalite[42], vydaný Radou Európy a ktorého signatármi sú krajiny, kam patrí Slovensko, USA, Izrael, Austrália a ďalšie. Tento dokument nepriamo nahliada na počítačovú kriminalitu ako

[42] "Dohovor o počítačovej kriminalite [Slovak] - OSCE POLIS." [online]. [cit. 3.5.2021]. Dostupné na internete: https://polis.osce.org/file/11321/download?token=VGFwDdzP.

nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu.

Je nutné zdôrazniť, že v čase písania tejto učebnice pojem „*počítačová kriminalita*" nie je definovaný v trestnom práve Slovenskej republiky.

Práve v čase tvorby tejto učebnice boli finalizované práce nad 2. dodatkom k Dohovoru o počítačovej kriminalite. Jeho závery budú po ratifikácií členskými krajinami EÚ postupne zapracované do právnych systémov jednotlivých krajín.

V kriminalistickej praxi sa využíva zjednodušené rozdelenie počítačovej kriminality na 3 základné skupiny:

- **PC (IKT) ako objekt, tiež tzv. priama kriminalita** - kedy je IKT (PC, notebook, tablet, mobilný telefón a ďalšie) **cieľom** útoku, a teda dochádza k jeho poškodeniu, zničeniu, odcudzeniu, neoprávnenému používaniu či poškodeniu jeho činnosti.

  príklady: rozbitie, zničenie, zavlečenie malvéru, poškodenie činnosti a ďalšie,

- **PC (IKT) ako nástroj, tiež tzv. nepriama kriminalita** - kedy je IKT používané ako **nástroj** na vykonanie činu, ktorý je vykonateľný aj bez použitia techniky.

  príklady: rôzne formy kyberšikany, falšovanie, podvody a ďalšie,

- **PC (IKT) ako nositeľ informácie** - kedy je IKT **nositeľom** informácie o priebehovom deji, ktorá preukazuje aktivity/konanie súvisiace s vyšetrovanou udalosťou (činom).

  príklady: komunikácia, informácie o pohybe (GPS) a ďalšie.

Téma informačnej (kybernetickej) bezpečnosti, resp. téma počítačovej kriminality, sa úzko dotýka aj zákonov (legislatívy) - detailne sa problematike budeme venovať vo vyšších ročníkoch. Tu je krátke východisko:

Postupnosť vnímania zákonných noriem súvisiacich s témami informačnej (kybernetickej) bezpečnosti by bolo možné v stručnosti definovať v nasledujúcej postupnosti:

- etika a morálka,
- základné ľudské a ústavné práva,
- občianske a spotrebiteľské práva,
- obchodné práva,
- sektorová legislatíva,
- trestný zákon.

4.1. Čo je počítač

Väčšina z nás pracuje s počítačom každý deň. Počítač, ako taký, môže vyzerať rôzne. Každý z vás už videl klasickú šedú krabicu s monitorom alebo notebook. Počítač je veľmi často schovaný aj na mieste, kde by ste s ním nepočítali. Rovnako väčšina elektroniky používanej v domácnosti obsahuje počítač. Patrí sem napríklad televízor, prehrávač DVD/Blueray, práčky, chladničky alebo smart žiarovky. Pre efektívnu prácu s touto technológiou musíme rozlišovať nasledujúce pojmy, ktoré sa pokúsime zadefinovať:

Počítač je stroj, ktorý je možné naprogramovať tak, aby vykonával postupnosť aritmetických alebo logických operácii.

Informačné a komunikačné technológie (IKT) sú technológie, ktoré umožňujú elektronicky zaznamenávať, uchovávať, vyhľadávať, spracovávať, prenášať a šíriť informácie.

Počítač používame na to, aby sme spracúvali a vyhodnocovali informácie - či už vo forme pozerania videa, ukladania a spracúvania fotografii alebo písania úloh do školy. Takto zachytené informácie sa nazývajú **dáta**.

Vyhľadajte na internete, ako sa volá prvý turingovsky úplný elektrónkový počítač. V čom sa líši od moderných počítačov?

Vyhľadajte na internete, kedy vznikli prvé stolové počítače.

Nájdite na internete informáciu o filme Enigma. Ako sa volala hlavná postava tohto filmu? Čím je tak dôležitá pre oblasť informatiky?

Vyhľadajte na internete, kedy vznikli prvé mobilné telefóny. Aký bol rozdiel medzi súčasnými smartfónmi a prvými mobilnými telefónmi?

Ako sme sa mali možnosť presvedčiť, pojmy počítač a IKT sú pomerne široké. Počítač môže byť čokoľvek, čo sa dá naprogramovať - od kalkulačiek, cez autá, až po klasické stolové počítače, notebooky a samozrejme servery. IKT zas môže byť čokoľvek, čo spracúva dáta. Z uvedených možností vyplýva, že obidva pojmy sa výrazne prekrývajú. Rôzne zariadenia (chladničky, žiarovky, termostaty, monitory bábätiek, smart hračky, atď.), ktoré je možné pripojiť na internet nazývame súhrnne **IoT zariadenia**. IoT je skratka z anglického pojmu „internet of things", čiže internet vecí.

Ktoré zo zariadení, ktoré máte doma, spĺňa požiadavku definície počítača alebo IKT a vysvetlite prečo.

Ktoré zo zariadení, ktoré poznáte, by ste mohli označiť za IoT? Akým spôsobom je toto zariadenie pripojené na internet?

Z pohľadu informačnej bezpečnosti nie je podstatné, ako počítač či IKT prvok vyzerá. Akákoľvek funkčná časť IKT je aktívum (viď. kapitola Riziko, aktívum, zraniteľnosť)**.** Patrí sem počítač, zariadenie, ale aj proces práce s počítačom. V tejto skupine nájdeme všetko, čo môže byť vystavené bezpečnostným hrozbám a čo môže čeliť riziku zraniteľnosti. Úlohou informačnej bezpečnosti je nájsť všetky zraniteľnosti každého aktíva, popísať hrozby a vyhodnotiť riziká s aktívom spojené. Následne je nevyhnutné aplikovať také opatrenia, aby sme aktívum ochránili. Viac o konkrétnych hrozbách, zraniteľnostiach a následných opatreniach si povieme v tejto časti učebnice.

Vymyslite hrozbu, ktorá sa vzťahuje na váš mobilný telefón. Akú zraniteľnosť využíva táto hrozba? Aké opatrenia by bolo možné aplikovať na zmiernenie rizika?

Niektoré hrozby sú prirodzené a riziko ich realizácie závisí len od nás, našej pozornosti a nášho vzdelania. Napríklad, ak necháme mobil na priamom slnku, pokazí sa nám baterka. Toto poznanie patrí do základných vedomostí fyziky. Niektoré hrozby však nezávisia od nás. Napríklad, ak malvér nájde chybu v kóde, na ktorú neexistuje záplata, nevieme ovplyvniť danú skutočnosť a opraviť chybu, ale musíme sa naučiť, aké opatrenia máme urobiť navyše, aby sa problém tohto druhu už nevyskytol.

Väčšina útokov na kybernetický priestor je realizovaná na úrovni softvéru, avšak niektoré útoky môžu byť realizované aj prostredníctvom podstrčeného hardvéru (napr. USB kľúča) alebo môžu byť cielené na hardvér. Príkladom útoku prostredníctvom podstrčeného hardvéru je **baiting** (od anglického „bait" - návnada), pri ktorom útočník nechá podhodený USB kľúč a čaká, kým ho používateľ zapojí do počítača.

Vyhľadajte na Youtube príklad pre baiting útok.

- *Čo môže útočník dosiahnuť a čo bolo v príklade cieľom útočníka?*
- *Je možné cez baiting útok znefunkčniť počítač?*
- *Aké odporúčania by ste navrhli na zníženie rizika baitingu?*

4.2. Typy útokov

V predchádzajúcej kapitole sme si povedali niečo ohľadom útokov na hardvér. V tejto kapitole tému rozvinieme aj o ostatné typy útokov, pričom sa budeme opierať o informácie o tom, čo tvorí hodnotu počítača. Na počítači sú cenné tri veci:

- **cena samotného hardvéru** - hlavne „high spec" (super výkonné) herné počítače, v ktorých sa serverový či špecializovaný hardvér vie cenovo vyšplhať naozaj vysoko,
- **výkon počítača** - aj keď kriminálnik nevie ukradnúť priamo hardvér, tak vie ukradnúť výkon počítača napr. za účelom ťažby kryptomeny na počítači,
- **dáta** - naše dáta sú spravidla to najcennejšie, čo je v počítači uložené, či už ide o fotografie rodiny alebo heslá k internet

bankingu, príp. iným systémom (vždy si vieme kúpiť nový laptop, ale nevieme si kúpiť fotku z dovolenky).

Kybernetickým útokom nazývame pokus o sprístupnenie, modifikáciu, zničenie, krádež alebo získanie informácie prostredníctvom neautorizovaného prístupu alebo neautorizovaného použitia aktíva. Typickým útokom je útok na niektorú časť CIA.

V definícii o kybernetickom útoku je podstatný aj jej záver, nakoľko jedným zo spôsobov útoku môže byť aj autorizovaný používateľ, ktorý zneužije svoje oprávnenia v informačnom systéme.

Nájdite na internete informácie o ľubovoľnom útoku na počítač alebo IKT. Vysvetlite spolužiakom, ako útok fungoval a aké boli dopady? Aké riziko sa prejavilo pri útoku? Aké opatrenia aplikovala organizácia na zníženie rizika?

Kybernetické útoky môžeme kategorizovať podľa rôznych kritérií[43], napr. podľa:

- **vektora útoku** - vektor útoku môže zneužívať zraniteľnosti v operačnom systéme (kernel flaws), aplikačnom a programovom vybavení (napr. buffer overflow), ale aj nevhodnú konfiguráciu informačného systému (napr. nevhodne nastavené oprávnenia) alebo samotného používateľa (sociopatická manipulácia),
- **prevádzkového dopadu** - prevádzkový dopad sa môže líšiť od kompromitácie aplikácie, (privilegovaného) užívateľa, inštalácie škodlivého softvéru alebo útoku denial of service,
- **spôsobu ochrany voči útoku** - útok vieme buď zmierniť (napr. blacklistingom) alebo zastaviť (napr. aplikovaním záplaty),
- **dopadu na informácie** - pozri definíciu kybernetického útoku,
- **cieľa útoku** - cieľom útoku môže byť hardvér, operačný systém, sieť, užívateľská aplikácia alebo samotný používateľ.

[43] vybrané podľa taxonómie AVOIDIT

Pre útok z predchádzajúceho cvičenia uveďte vektor, prevádzkový dopad, spôsob ochrany voči útoku, dopad na informácie a cieľ útoku.

Útoky sa v kybernetickom priestore odohrávajú každý deň. Niektoré sú úspešne odrazené, iné majú dopad na organizácie a o časti útokov je následne verejnosť informovaná prostredníctvom samotných organizácii, regulátorov alebo tretích strán. V rámci Slovenska úlohu regulátora a zbierania informácií o útokoch má vo svojej kompetencii Národný bezpečnostný úrad (NBÚ). Úlohou NBÚ je aj koordinovať obranné opatrenia s ostatnými bezpečnostnými úradmi v ostatných krajinách sveta a pripravovať Slovensko na obranu pred novými hrozbami.

Počet detegovaných, nahlásených a riešených incidentov v Národnom bezpečnostnom úrade v roku 2020[44]. Nie všetky kybernetické útoky sú detegované a riešené ako incident.

Vyhľadajte na internete poslednú verziu Verizon Data Breach Report a zodpovedzte nasledovné otázky:

- *Identifikujte a vysvetlite význam anglického pomenovania útoku a nájdite jeho slovenský ekvivalent.*
- *Aký je najčastejší vektor útokov?*
- *Aká je primárna motivácia útočníkov?*
- *Kto sú najčastejší útočníci?*

[44] SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE V ROKU 2020 [online]. [cit. 30.05.2021]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-2020.pdf

Kybernetické útoky sa líšia čo do zložitosti - od jednoduchých útokov, pri ktorých je po kliknutí na linku v phishingovom emaile stiahnutý škodlivý softvér, až po komplexné útoky prostredníctvom kompromitácie dodávateľských reťazcov. Príkladom komplexného útoku z konca roku 2020 je útok na spoločnosť FireEye prostredníctvom kompromitovaného softvéru SolarWinds Orion[45]. Tento softvér slúži primárne na kontrolu funkčnosti a riadenie záťaže aplikácií. Organizácie ho využívajú pre kontrolu funkčnosti najdôležitejších aplikácií.

 Poďme sa pozrieť na tento útok bližšie, v jeho jednotlivých krokoch:

1) Jedna z knižníc[46] produktu SolarWinds obsahovala tzv. zadné vrátka (backdoor). To znamená, že každý, kto si tento softvér nainštaloval, bol zraniteľný a cez jednu chybu, ktorýkoľvek útočník mohol napádať počítače a servery, kde bol softvér nainštalovaný.
2) Po inštalácii na systém prostredníctvom automatických aktualizácii bol škodlivý softvér 2 týždne nečinný. Po dvoch týždňoch sa zobudil. Následne si stiahol zoznam úloh, pričom komunikáciu maskoval ako Orion Improvements Program protokol.
3) Potom sa začal škodlivý softvér rôznymi technikami šíriť na ďalšie systémy v rámci siete FireEye, pričom preferovaný spôsobom bolo použitie odchytených prihlasovacích údajov.

[45] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor [online]. [cit. 30.05.2021]. Dostupné na internete: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[46] Jedným z cieľov pri písaní počítačových programov je opakovateľnosť napísaného zdrojového kódu, aby programátori nemuseli dookola písať ten istý kód. Preto je možné využívať aj funkcie a objekty z iných súborov. Funkcie a objekty, ktoré logicky robia podobné veci sa dodávajú vo forme knižníc - napr. knižnica pre načítanie obrázku v definovanom formáte do pamäte.

4) Po získaní prístupu k interným nástrojom FireEye používaným na realizáciu tzv. red-team[47] cvičení u zákazníkov. Tieto nástroje môžu byť zneužité útočníkmi na realizáciu útokov voči iným organizáciám.

Spoločnosť FireEye je špičkou v informačnej bezpečnosti, a preto vydala o útoku rozsiahlu správu, ktorá pomohla organizáciám využívajúcim softvér Orion v identifikácii kompromitácie vo svojich IT prostrediach.

1. Útoky zamerané na hardvér

Útoky zamerané na hardvér sú spravidla cielené na narušenie dôvernosti spracúvaných dát alebo sa snažia kompromitovať zariadenia, ktoré nie sú pripojené k počítačovej sieti (air-gapped devices). Izolácia od počítačovej siete alebo využitie fyzicky oddelenej počítačovej siete sa využíva ako opatrenie voči kompromitácii veľmi citlivých zariadení, ako sú napr. zariadenia ovládajúce výrobu v priemyselnom podniku.

Dôvernosť spracúvaných dát môže byť na úrovni hardvéru kompromitovaná viacerými spôsobmi:

- **elektromagnetickým vyžarovaním** - súčiastky počítača môžu vyžarovať elektromagnetické vlnenie, ktoré je možné zachytiť anténou. Útočník vie takto zachytené elektromagnetické vlnenie analyzovať, pričom dochádza ku snahe zrekonštruovať spracúvanú informáciu.
- **tepelným vyžarovaním** - pokiaľ vie útočník zaťažiť zariadenie a zároveň snímať teplotu zariadenia, tak vie veľmi pomalým spôsobom vysielať informácie zo zariadenia - napr. zaťažené/ vysoká teplota je 1, nezaťažené/nízka teplota je 0.
- **využitie signalizačných diód** - pokiaľ vie útočník využiť signalizačnú diódu v zariadení a zároveň snímať vzdialene, či dióda svieti, môže takto vysielať informácie zo zariadenia. Na

[47] Red-team cvičenie je typ bezpečnostného testu, pri ktorom organizácia zmluvne dohodnutá útočí na infraštruktúru zákazníka. Red-tím je tím, ktorý útočí. Tím, ktorý bráni infraštruktúru je blue tím.

tento účel sa dajú využiť diódy napr. signalizujúce prácu pevného disku alebo diódy na klávesnici (napr. CapsLock).

Špecifické útoky sa realizujú najmä na hardvér plniaci špecifické úlohy - napr. čipové karty alebo hardvérové kryptografické moduly. Tieto útoky spravidla využívajú postranné kanály, nakoľko hardvér môže byť fyzicky chránený, napr. zaliatím v plaste ako vaša platobná karta.

 **Útok postranným kanálom** je typ útoku založený na informáciách získaných z počítačového systému a nie na informáciách o zraniteľnostiach v implementovanom (vloženom) algoritme.

Príkladmi využívaných kanálov sú:

- **časové útoky (time-based)** – ich podstatou je fakt, že zložitá operácia trvá dlhšie než jednoduchá a pokiaľ útočník vie, ako hardvér funguje, môže sa snažiť určovať zloženie spracúvaných dát - napr. privátneho kľúča.
- **útoky na spotrebu energie** (voltage) - ich podstatu opäť tvorí fakt, že zložitá operácia spotrebuje viac energie než jednoduchá operácia, a pokiaľ útočník vie, ako hardvér funguje, môže sa snažiť určovať zloženie spracúvaných dát - napr. privátneho kľúča.

2. Škodlivý softvér

Škodlivý softvér (inak malvér alebo malvér) je počítačový softvér, ktorý je navrhnutý tak, aby poškodil používateľa, počítačový systém alebo počítačovú sieť. Pojem malvér zahŕňa širokú škálu softvéru bez ohľadu na spôsob šírenia (napr. prostredníctvom inštalovania používateľom alebo samostatne zneužitím bezpečnostnej zraniteľnosti) a na vznik škody (napr. únik dát, vymazanie dát, odchytávanie hesiel atď.).

Škodlivý softvér je možné rozdeliť, podľa správania sa, na viacero skupín[48], ktoré sa navzájom môžu prekrývať:

- **advér** (adware) - škodlivý softvér, ktorý zobrazuje alebo sťahuje užívateľovi reklamný obsah,
- **backdoor** / **remote access tool (RAT)** - škodlivý softvér, ktorý útočníkovi umožňuje neautorizovaný prístup k počítaču,
- **bot** - škodlivý softvér zapojený do siete (botnetu), ktorý vie prijímať a vykonávať príkazy operátora,
- **keylogger** - škodlivý softvér, ktorý zaznamenáva stlačenia kláves na klávesnici,
- **ransomvér** (ransomware) - softvér, ktorý zneprístupní (napr. zašifruje) súbory na počítači a požaduje na dešifrovanie zaplatenie „výkupného" (ransom),
- **rootkit** - škodlivý softvér, ktorý využíva vysoké práva v operačnom systéme na to, aby sa skryl pred antivírusom,
- **spyware** - škodlivý softvér, ktorého cieľom je zaznamenávať a špehovať správanie sa užívateľa a následne ukradnúť citlivé informácie, napr. polohu zariadenia, stlačenia kláves a pohyby myši, záznam z kamery alebo mikrofónu zariadenia, príp. dešifrovať dáta zasielané šifrovane cez počítačovú sieť,
- **počítačový červ** (worm) - škodlivý softvér, ktorý je schopný replikácie a šírenia sa medzi počítačovými systémami alebo prostredníctvom počítačovej siete. Spôsob šírenia môže zahŕňať zneužívanie bezpečnostných zraniteľností, prenosné médiá alebo komunikačné platformy (email, instant messaging, sociálne siete),
- **trójsky kôň** (trojan horse, trojan) - typ škodlivého softvéru, ktorý sa nešíri samostatne ako červ, ale vyžaduje iný spôsob spustenia - napr. návštevou infikovanej webovej stránky (drive-by-download), spustením infikovanej prílohy emailu alebo IM správy,
- **vírus** - škodlivý softvér, ktorý modifikuje iný program tak, aby obsahoval kópiu vírusu.

[48] Neexistuje však ustálená taxonómia delenia a označovania malvéru.

Nájdite na internete príklad škodlivého softvéru, ktorý kombinuje viacero skupín škodlivého softvéru. Aké je označenie vami nájdeného malvéru rôznymi antívírusmi?

Antivírusový softvér je počítačový softvér, ktorý zisťuje, odstraňuje a chráni počítač pred všetkými skupinami škodlivého softvéru. Antivírusový softvér sa skrátene nazýva aj antivírus, prípadne antimalvér (antimalware).

Antivírus spravidla kontroluje bežné spôsoby, ako sa škodlivý softvér môže dostať do počítača (napr. prenosné médiá, emailovú komunikáciu, komunikáciu pri surfovaní na webe atď.). Kontrola, ktorú vykonáva antivírus, musí byť dostatočná, aby zachytil väčšinu škodlivého softvéru, avšak optimalizovaná tak, aby nezaťažovala zariadenie, na ktorom antivírus beží. Kontrola sa vykonáva viacerými spôsobmi:

- porovnaním voči známym malvérom, ktoré sú definované signatúrami alebo odtlačkom (haš)[49],
- spustením kontrolovaného/podozrivého softvéru v kontrolovanej časti počítačovej pamäte (sandboxe) a následné pozorovanie správania kontrolovaného softvéru,
- sofistikovanými algoritmami - heuristika[50], machine learning atď.

[49] **Kryptografický odtlačok (haš)** je binárny reťazec, ktorý je priradený k dátam. K ľubovoľným dátam je možné vytvoriť haš, avšak kryptografický haš má takú vlastnosť, ktorá komplikuje spôsob ako nájsť dáta ku konkrétnemu hašu alebo nájsť dvoje rôznych dát s rovnakým hašom. Napr. v počítači sú dáta reprezentované (zachytené) vo forme binárneho reťazca, a tým pádom sa na ne dá pozerať ako na veľké binárne číslo. Môžeme povedať, že haš je napr. zvyšok po delení 2^8 a tak napr. k dátam 1111010101010 je haš 10101010 (posledných 8 bitov). Tento haš však nie je kryptografický, pretože v našom prípade vieme ľahko vytvoriť rôzne reťazce s rovnakým hašom.
Signatúra je inteligentný odtlačok, pretože neberie do úvahy niektoré dáta, ale len tú časť, ktorá identifikuje malvér. Ak teda máme malvér, ktorý mení svoj kód, tak dynamická časť nemusí vstupovať do signatúry, aby jedna signatúra mohla pokrývať všetky mutácie malvéru.

[50] Heuristika je spôsob približnej detekcie malvéru, ktorý má dostatočnú spoľahlivosť a rýchlosť (v prípade, keď iné typy detekcií sú príliš pomalé).

Navrhnite rôzne spôsoby hašovania dát. Vymeňte si navrhnuté hašovacie algoritmy a analyzujte, či viete:

- *nájsť k hašu dáta, z ktorých haš vznikol,*
- *alebo nájsť dvojicu dát s rovnakým hašom.*

Tvorcovia malvéru sa snažia oklamať kontrolu antivírusu tak, aby malvér vedel infikovať počítač a/alebo mohol vykonávať na počítači zamýšľanú škodlivú činnosť. Preto je potrebné, aby bol antivírus pravidelne aktualizovaný na úrovni antivírusovej databázy (spravidla obsahuje signatúry) a na úrovni jednotlivých komponentov obsahujúcich sofistikovanejšie algoritmy.

Napríklad malvér chce niečo spustiť v príkazovom riadku - napr. *vssadmin*. Je známe, že daný program spúšťa štandardne ransomvér, ktorý sa snaží zmazať akékoľvek zálohy operačného systému, resp. súborového systému. Antivírusový program teda hľadá text vssadmin a malvér sa to snaží obísť úpravou textu - zmena kódovania na base64 – „dnNzYWRtaW4=“.

Tým, že tvorcovia malvéru neustále vytvárajú nové spôsoby oklamania antivírusového softvéru a vzhľadom na limitovaný výkon, ktorý môže antivírus využívať, nie je možné, aby antivírus fungoval na 100%. Z uvedených dôvodov sa budú v IT prostredí vyskytovať/objavovať škodlivé softvéry, ktoré antivírus nezachytí (falošne negatívne výsledky kontroly) a neškodný softvér, ktorý je naopak označený za malvér (falošne pozitívne výsledky). Z pohľadu informačnej bezpečnosti je antivírus nevyhnutnou súčasťou procesu, ako sa vyhnúť problémom, ale nie je jedinou. K efektívnemu použitiu antivírusu musíme pridať ešte užívateľovo obozretné správanie a ďalšie typy ochrany, ako je napríklad firewall.

Nájdite na internete príklad testu, ktorý preveruje antivírusové softvéry na falošne negatívne a falošne pozitívne výsledky.

Vo firemnom prostredí sú antivírusové softvéry spravidla inštalované a manažované centrálne cez dedikovanú konzolu (samostatná konzola s vyšším výkonom), ktorá umožňuje nastavovať konfiguráciu antivírusu a vizualizovať zistené problémy. V domácom

prostredí môže byť alternatívou webový portál, s ktorým je možné antivírus prepojiť a v obmedzenej miere konfigurovať.

4.3. Zraniteľnosti a záplaty

Zraniteľnosť je slabé miesto v počítačovom systéme, ktoré umožní útočníkovi vykonať útok na počítačový systém.

Existuje veľké množstvo útokov na bezpečnostné zraniteľnosti a rovnako aj veľké množstvo tried zraniteľnosti. Projekt OWASP delí webové zraniteľností do tried[51] a najčastejšie zneužívané zraniteľnosti sú vymenované v projekte OWASP TOP 10[52].

Nájdite na internete, ktorá je prvá z tried zraniteľností v OWASP Top 10 a vyberte si príklad jednej zraniteľnosti. Vysvetlite, aká je príčina tejto zraniteľnosti a čo je potrebné spraviť na odstránenie vybranej zraniteľnosti.

Existuje množstvo typov zraniteľností, ktoré umožňujú útočníkovi:

- predstierať identitu alebo autentickosť dát - príkladom je posielanie emailov v mene inej osoby,
- neautorizovane modifikovať dáta - príkladom je napr. zapísanie väčšieho vstupu, ako program očakáva, prepísanie iných dát,
- poprieť vykonanie nejakej akcie - napr. zmeny dát,
- pristupovať k dátam, ktoré nemajú byť prístupné - napr. prostredníctvom directory traversal[53] zobrazovať súbory na operačnom systéme, ktoré nie sú bežne prístupné,

[51] Vulnerabilities [online]. [cit. 30.05.2021]. Dostupné na internete: https://owasp.org/www-community/vulnerabilities/

[52] OWASP Top Ten [online]. [cit. 30.05.2021]. Dostupné na internete: https://owasp.org/www-project-top-ten/

[53] Directory traversal je útok, pri ktorom útočník vie prechádzať adresáre a súbory, ktoré by nemali byť dostupné. Väčšinou sa to deje prostredníctvom sekvencii "..\" a "../", ktorá v príkazovom riadku znamená „o adresár vyššie". Príkladom môže byť nasledovná URL: www.zranitelnaaplikacia.sk/?report=../../../etc/passwd

- vyťažiť (až zneprístupniť) informačný systém alebo ho využiť na vyťaženie iného informačného systému - napr. posielaním veľkého množstva dotazov na server, ktorých vykonanie je náročné na výkon,
- spustiť vlastný počítačový program (*code execution*).

Nájdite na internete, aké dáta ukladá operačný systém UNIX/Linux v súbore /etc/passwd a vysvetlite, prečo sú dôležité.

Špeciálnym typom bezpečnostnej zraniteľnosti je tzv. **0-day zraniteľnosť** - t. j. bezpečnostná zraniteľnosť, ktorá je známa útočníkovi, zatiaľ však je neznáma výrobcovi softvéru, a teda môže byť zneužívaná skôr, ako výrobca vytvorí a dá k dispozícii jej opravu.

Exploit - je počítačový program, ktorý zneužíva bezpečnostnú zraniteľnosť. Proces zneužitia tejto zraniteľnosti sa nazýva exploitácia.

1. Prečo útočníci zneužívajú zraniteľnosti?

Každý počítačový program, ktorý je publikovaný na internete, je cieľom etických a neetických výskumníkov, ktorí sa v ňom snažia nájsť bezpečnostné zraniteľnosti. Motiváciou pri takomto výskume môže byť:

- popularita - publikované zraniteľnosti sú označené číslom (tie známejšie aj menom a logom) a publikované v databáze zraniteľností, čo autorom prinesie vysokú mieru popularity na sociálnych sieťach,
- publicita - na publikovaní zraniteľností si môžu spoločnosti zaoberajúce sa počítačovou bezpečnosťou budovať značku (image) technických expertov,
- finančná odmena získaná eticky - niektorí výrobcovia počítačových programov majú definovaný tzv. „bug bounty" program, v rámci ktorého vyplácajú finančné odmeny výskumníkom (etickým hekerom, alebo aj „white hat" hekerom), ktorí nahlásia bezpečnostné zraniteľnosti,

- finančná odmena získaná neeticky - mimo oficiálne nahlásených bezpečnostných zraniteľností existuje trh s bezpečnostnými zraniteľnosťami, kde rôzni útočníci skupujú zraniteľnosti, ktoré následne vedia využívať na rôzne útoky. Títo útočníci môžu byť kriminálnici, ale aj štátom sponzorované organizácie. Ľudia, ktorí neeticky predávajú a využívajú zraniteľnosti, sú nazývaní „black hat" hekeri.

Nájdite na internete, aké základné tri typy hekerov poznáme a v čom sa navzájom líšia.

2. Záplaty

Poznáme dve základné ochrany proti zraniteľnostiam. Prvou je nájdenie ochrany rekonfiguráciou systému (**workaround**), napríklad ak má služba (*service*) v počítači chybu a túto službu nevyužívame, môžeme ju vypnúť. Druhou je vytvorenie záplaty výrobcom, pričom táto rieši konkrétnu zraniteľnosť.

Záplata (patch) je súbor (rad) zmien počítačového programu a/lebo dát, s ktorými počítačový program pracuje, s cieľom aktualizovať, opraviť alebo zlepšiť počítačový program. Tieto zmeny môžu zahŕňať aj opravu bezpečnostných zraniteľností. Niekedy sa počet záplat nahromadí, pričom záplaty majú navzájom veľa závislostí, a preto vydá výrobca systém (balík) záplat, ktorý sa volá Service pack.

Service pack - je súbor záplat alebo zmien, ktoré výrazne menia správanie sa počítačového programu, radu programov alebo operačného systému.

3. Manažment záplat

Čím je softvér rozšírenejší, tým je väčšia šanca, že sa na neho zameria výskumník hľadajúci bezpečnostné zraniteľnosti. Z uvedeného dôvodu organizácie, ktoré majú vyspelejšie procesy vývoja softvéru, podnikajú kroky, aby odhalili čo najviac bezpečnostných zraniteľností ešte pred publikovaním počítačového programu na internet. Napriek tomu sa stáva, že zraniteľnosť je

odhalená až v momente, kedy už je softvér publikovaný. Následne je potrebné, aby organizácia pripravila záplatu (patch) a vypublikovala ho pre svojich zákazníkov alebo užívateľov. V takýchto prípadoch je dôležitá príprava a vydanie patchu, pričom ide o súboj s časom, aby sa zabránilo masívnemu zneužívaniu zraniteľnosti v počítačových systémoch zákazníkov. Preto sa stáva, že vydaný patch nemusí byť stabilný a/lebo obsahuje ďalšie zraniteľnosti a musí sa vydávať opravná záplata.

Okrem spomínaných okolností existuje spôsob, ako procesom (a prostredníctvom) reverzného inžinierstva[54] zo záplaty zistiť, akú bezpečnostnú zraniteľnosť opravuje a ako je možné túto bezpečnostnú zraniteľnosť využiť. Kvôli tejto možnosti je potrebné nasadiť patch v pomerne krátkom čase, skôr než začne byť zraniteľnosť masovo zneužívaná (exploited in the wild). Viac o odporúčaní na riadenie záplat si povieme v kapitole Odporúčania.

Nájdite na internete postup, ako si overíte, že váš operačný systém má nainštalované všetky potrebné záplaty.

4.4. Web a prehliadač

1. Čo je to doména a prečo je to dôležité?

Počítače pracujú na báze núl a jednotiek. Nie je preto prekvapujúce, že v počítačovej sieti, vrátane internetu, sa počítače identifikujú skupinou čísiel, ktorá sa volá IP adresa. Väčšina ľudí nemá rada čísla a má problém si ich zapamätať. Preto bol vymyslený spôsob, ako dať počítačom na počítačovej sieti zapamätateľné názvy ako napr. www.preventista.sk. Tento spôsob sa volá systém doménových mien (domain name system - DNS). Zapamätateľnejší názov www.preventista.sk je doména, alebo presnejšie súbor domén, ktorá pozostáva z vrcholovej domény (top-level domain) .sk, domény

[54] t.j. zistenia, čo program robí z jeho binárnej podoby

preventista a subdomény www. Jednotlivé časti domény sú oddelené bodkami. Pri doménach je potrebné zapamätať si nasledujúce fakty:

1) **Každá doména niekomu patrí**. Registrátor vrcholovej domény umožňuje ďalším subjektom kúpiť si doménu na definovaný čas - spravidla rok.
2) **Keď vlastníme nejakú doménu, neznamená to, že vlastníme aj ostatné domény u ostatných registrátorov**. Takže ak si kúpim doménu janosik.sk, tak doménu janosik.cz alebo janosik.com môže vlastniť niekto úplne iný. Rovnako vlastníctvo domény janosik.sk nič nehovorí o tom, kto vlastní doménu jurajjanosik.sk alebo janosikovbudzogan.sk. Tento trik je často zneužívaný na podvody, kedy internetbanking banka.sk je nahradený podvodnou stránkou banka.xyz alebo mojabanka.sk.
3) **Kto si zakúpi doménu, môže si vytvárať subdomény** - takto si vie firma Google vytvárať subdomény ako www.google.com, mail.google.com, dokonca aj janosik.google.com

Dôsledkom bodov 2) a 3) je, že existuje veľký rozdiel medzi doménami:

- moja.banka.sk
- mojabanka.sk

Jedna malá bodka v názve (alebo akákoľvek zmena nejakého znaku) spôsobí, že doména môže patriť niekomu úplne inému. Tento trik často využívajú podvodníci na registráciu podvodných domén. Nie je totiž v ľudských a finančných silách skúpiť všetky domény, ktoré sa podobajú na banka.sk[55]. Z uvedených dôvodov môže útočník „obsadiť" doménu, ktorá sa tvári ako doména nejakej organizácie[56]. Toto konanie sa nazýva anglickým termínom **squatting**. Okrem hosťovania škodlivého obsahu alebo phishingovej stránky na squattovanej doméne existuje aj iný spôsob získania peňazí legálnym spôsobom - jej predajom, spravidla za výrazne vyššiu cenu

[55] Hlavne, ak niektorí znalí užívatelia nakúpia takéto domény „do rezervy" a následne ponúkajú ich predaj za výrazne vyššie sumy.
[56] alebo osobnosti - v minulosti bol napr. na dagmaghavlova.cz hostovaný nevhodný a kompromitujúci obsah

organizácii, ktorej meno napodobňuje. Doména za pár dolárov môže mať pre organizáciu cenu aj niekoľko tisíc dolárov[57].

Druhým trikom je takzvaný **typosquatting**, to znamená, že útočník použije doménu, ktorá vznikla preklepom z pôvodnej domény - v našom prípade napr. bamka.sk namiesto banka.sk. Bežný človek potom pri phishingovej linke tento rozdiel často prehliadne. Na zdokonalenie kamufláže je možné využiť znaky, ktoré sú si vizuálne podobné napr. „l" a „1" alebo „b" a „h". Tento spôsob zamaskovania sa nazýva **homomorfný útok** a prostredníctvom neho z domény moja.banka.sk vyrobíme napríklad moja.hanka.sk. Do úplnej dokonalosti sa dá dotiahnuť tento útok prostredníctvom tzv. Unicode súboru znakov, ktoré umožňujú napr. zobrazovať písmená azbuky a iných cudzích jazykov. Rôzne znaky v Unicode môžu vyzerať úplne rovnako, majú však iný kód, napr.: (v latinke) **a**: U+0061, (v azbuke) **а**: U+0430. Takýmto spôsobom môže útočník zaregistrovať doménu, ktorá vyzerá v prehliadači ako banka.sk, avšak kódovanie má úplne odlišné, a preto sa jedná aj o úplne odlišnú doménu. Tieto útoky užívateľ len ťažko odhalí. Práve kvôli tomuto potenciálnemu nebezpečenstvu by mal byť na počítači nainštalovaný antivírus, ktorý vie prístupy na takého škodlivé domény odhaliť.

Posledným trikom je využitie veľkého množstva subdomén na zamaskovanie, že ide o podvodnú doménu. Najmä na mobilných telefónoch totiž webový prehliadač zobrazí len obmedzené množstvo znakov. Pokiaľ je užívateľ zvyknutý pristupovať na internet banking prostredníctvom mobilu, tak útočník si vie zaregistrovať doménu ako napríklad:
moja.banka.sk.internetbanking.nejaka.zla.domena.z.deep.web.

Používateľovi v mobilnom telefóne sa však objaví len URL: *moja.banka.sk/internetbanking.* Máloktorý používateľ však dokáže byť sústavne dostatočne obozretný, aby neustále kontroloval URL adresu, či nie je podhodená útočníkom.

Pri doménach preto platia tieto bezpečnostné zásady:

1. Pokiaľ je správna doména napr. *banka.sk*, tak jej subdomény sú tiež správne - napr. m*oja.banka.sk, www.banka.sk, mail.banka.sk, internetbanking.banka.sk* a dokonca aj *pozickazavsetkydrobne.banka.sk.*

[57] Is Domain Squatting Still A Factor in 2021? Here's The Lowdown [online]. [cit. 30.05.2021]. Dostupné na internete: https://digital.com/domain-registrar/domain-squatting/

2. Pri doménach je potrebné všímať si preklepy a umiestnenie bodiek „.” a lomiek „/”. Pokiaľ nie sú tam, kde majú byť, môže ísť o úplne inú doménu. Preto *moja.banka.sk/internetbanking* je iný web ako *moja.bamka.sk/internetbanking, mojabanka.sk/internetbanking* alebo *moja.banka.sk.internetbanking.com.*

Základnou obranou proti podvrhnutiu falošnej domény útočníkom môže byť uloženie domény dlhodobo v predvolených záložkách prehliadača a používanie práve týchto záložiek pri práci s doménou. V prípade, ak narazíte na podvodnú doménu[58], použite možnosti prehliadača a označte doménu v prehliadači ako podvodnú.

Špeciálnym podvodom v rámci internetu je špeciálny typ vydierania v rámci domén. Útočníci zakúpia doménu, o ktorej predpokladajú, že ju bude konkrétna, úspešná firma potrebovať a následne ju ponúkajú za rádovo vyššiu sumu. Zakúpenie domény ich stojí zopár desiatok EUR a následná ponuka na odpredanie pre lukratívne firmy sa môže vyšplhať do sumy tisícok EUR.

Vyhľadajte na internete aké top level domény (TLD) existujú a odpovedzte na otázky:

- *Sú niektoré TLD vyhradené pre jednotlivé štáty? Ak áno, uveďte príklad.*
- *Je niektorá TLD vyhradená pre vzdelávacie inštitúcie? Ak áno, ktorá?*
- *Ktorú TLD doménu by ste použili pre svoju firmu venujúcej sa kybernetickej bezpečnosti a prečo?*

Pripravte prezentáciu, ako sa vo vašom prehliadači nahlasuje podvodná doména.

2. Od domény k webu

Domény samotné sú veľmi zaujímavým prvkom, ale skutočne pravú užitočnosť nadobúdajú, až keď sa naplnia obsahom a ten je závislý na službách, ktoré poskytujú systémy, na ktoré domény ukazujú - mailové servery, webové servery, FTP servery, atď. Na to,

[58] Pokiaľ neviete, čo sa na doméne nachádza, využite napr. službu https://urlscan.io/

aby sme tieto služby mohli využívať, väčšinou potrebujeme **klienta**, ktorý sa pripojí na **server** s definovaným **protokolom**, ktorý zabezpečí prepojenie klienta (programu na vašom zariadení) a služby v internete. Pri elektronickej pošte je klientom napr. Outlook alebo Thunderbird a protokolom môže byť IMAP, POP3 alebo SMTP. Pri prehliadaní webových stránok je klientom webový prehliadač ako Google Chrome, Mozilla Firefox alebo Microsoft Edge a protokolom HTTP a jeho šifrovaný variant HTTPS.

Ak chceme prehliadať stránky v prehliadači, musíme zvoliť iný postup. Prehliadaču musíme napísať webovú stránku, ktorú chceme vidieť alebo kliknúť na pojem, ktorého obsah sa nám má vo webovej stránke zobraziť. Formát tejto stránky je napr. *https://www.aktuality.sk/spravy/zahranicne/.* Táto URL pozostáva z:

- protokolu - HTTPS
- domény - www.aktuality.sk
- lokality webovej stránky na webovom serveri - /spravy/zahranicne/[59]

Na to, aby sa v prehliadači zobrazila konkrétna stránka, prehliadač musí vykonať množstvo operácií, ktoré sa dejú po tom, ako stlačíte ENTER:

1) zistiť, kam smeruje (kde je umiestnená v internete) doména a požiadať webový server o konkrétnu stránku,
2) stiahnuť a prečítať kód[60] stránky a zistiť, aké ďalšie súbory je potrebné stiahnuť - obrázky, videá, dynamický kód napr. v jazyku JavaScript, JAVA, ActiveX alebo flash[61],
3) zobraziť všetky komponenty popísané v zdrojovom kóde stránky, alebo generované dynamicky aj s multimediálnymi súbormi na obrazovku - na tento účel musí vedieť prehliadač zobraziť obrázky a video v rôznych formátoch,

---

[59] meno súboru je vynechané schválne webovým serverom

[60] kód v jazyku HTML - hypertext markup language

[61] ActiveX a Flash sú zastaralé a nepodporované programovacie frameworky, ktoré môžu byť využité na realizáciu dynamickej funkcionality na webovej stránke. V minulosti boli cieľom útočníkov vzhľadom na veľký výskyt bezpečnostných zraniteľností.
JAVA je objektový programovací jazyk, ktorého výhodou je portabilita - jeden krát napísaný a skompilovaný Java program vie bežať na každom operačnom systéme, ktorý má podporu pre Java.
JavaScript (alebo len JS) je programovací jazyk, ktorým vieme dosiahnuť dynamickú funkcionalitu na webovej stránke. Spolu s HTML a CSS je jednou zo základných technológií, na ktorých beží World Wide Web.

4) spustiť dynamický kód - napr. kontrolu zadávaných údajov do formulára a zvýraznenie chýb alebo dotiahnutie ďalších a ďalších príspevkov na sociálnej sieti.

Ako vidieť, tento proces je pomerne komplikovaný, a preto sa natíska otázka: čo zlé, či neočakávané, sa môže stať?

1. Zlé veci na webe - http

Protokol HTTP[62] je používaný na surfovanie na webe od roku 1991 a jeho nevýhodou je, že nie je nijako ochránený. Pokiaľ teda sedíte na otvorenej WiFi (otvorenej v zmysle nezašifrovanej) vo vašej obľúbenej kaviarni, tak ktokoľvek vie pozerať, čo si práve prehliadate a zároveň aj dynamicky meniť obsah. Na vyriešenie tejto chyby a po viacerých útokoch bol v roku 1994 vymyslený protokol SSL (secure socket layer) a odvtedy sa neustále vylepšuje jeho zabezpečenie a ochrana voči útokom. Momentálne (v roku 2021) sa tento bezpečnostný protokol nazýva transport layer security (TLS) (v roku 2021 je vo verzii 1.3). Bez ohľadu na názov protokolu si stačí zapamätať, že písmeno „S" v protokole HTTPS znamená „secure" (bezpečný). Čo teda protokol HTTPS rieši nad rámec protokolu HTTP? Najčastejšie sú to tieto dve veci:

- **autentickosť webového servera** - t.j., že doména, napr. Google je naozaj doména, kam sa chcete prihlásiť, teda Google a nie nejaký podvodník, ktorý sa za Google vydáva.
- **šifrovanie a podpisovanie komunikácie**, aby komunikáciu a dáta v nej nebolo možné čítať, falšovať alebo zmeniť.

Ikona zamknutého zámku neznamená, že webová stránka, ktorú si zobrazujete, je správna. Stále môže ísť o podvodnú stránku mojabanka.sk (v tomto odkaze chýba bodka), ako sme si hovorili v kapitole o doménach. Táto ikona znamená len to, že komunikácia so zobrazovanou stránkou je zabezpečená.

Celá operácia prebieha s využitím kryptografie a použitia **certifikátov verejného kľúča** (skrátene certifikátov).

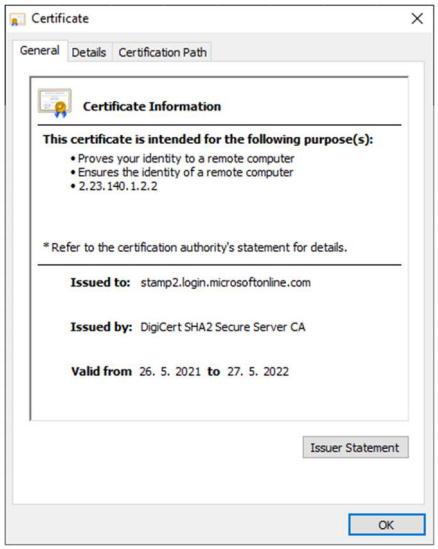
V prípade prehliadača je viditeľné delenie, ako sa prehliadač špecializuje podľa jednotlivých častí. Prehliadač sa orientuje na

[62] hypertext transfer protocol: Hypertext Transfer Protocol -- HTTP/1.1 [online]. [11.08.2021]. Dostupné online: https://datatracker.ietf.org/doc/html/rfc2616

zobrazovanie stránky, pričom šifrovanie má na starosti TLS a na využitie špecifických komponentov na stránke je nevyhnutné použiť špeciálny *addon* (prídavný doplnok programu) do prehliadača (často práve addony sú vhodné objekty pre hekerov).

Certifikát je vylepšený „občiansky preukaz" webového servera, v ktorom je uvedené jeho:

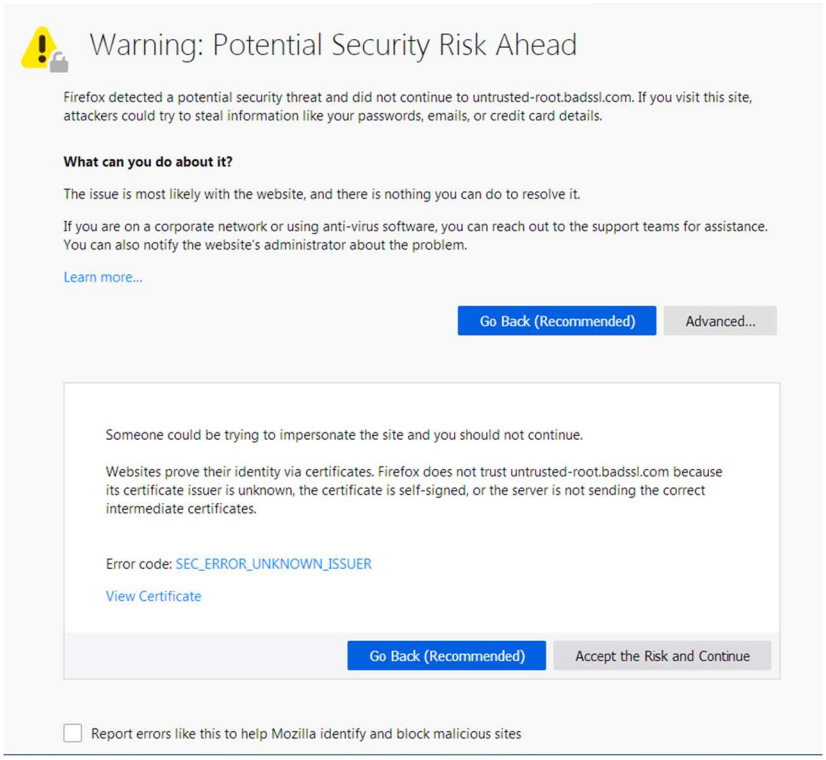
- meno - t. j. doména webového servera,
- ktorá certifikačná autorita (napr. polícia – v našom vnímaní dôveryhodná inštitúcia) ho vydala,
- odkedy a dokedy platí.



Zobrazenie X.509 certifikátu v OS Windows

- meno je v poli **Issued to,**
- certifikačná autorita v poli **Issued by,**
- doba platnosti v poliach **Valid From** a **Valid to.**

Webový prehliadač overí automaticky certifikát a v prípade, že sa vyskytne nejaký problém, zobrazí chybu, ktorá je zobrazená na nasledovnom obrázku.



Ukážka zobrazenia chyby pri overovaní certifikátu v prehliadači Firefox

Pokiaľ máte v prehliadači pri URL ikonu zamknutého zámku, tak certifikát bol overený a spojenie je šifrované. Šifrovanie prebieha po takzvanom podaní rúk (handshake), pri ktorom si komunikujúce strany overia certifikáty a dohodnú sa na tom, akým algoritmom a kľúčom budú šifrovať. Nešifruje sa priamo kľúčom z X.509 certifikátu, pretože použitá asymetrická kryptografia je príliš pomalá. Kľúč z certifikátu slúži len na zašifrovanie symetrického kľúča (tzv. key encryption key).

Aj keď niektoré stránky stále umožňujú pripojenie aj cez HTTP, drvivá väčšina z nich už poskytuje pripojenie výhradne cez HTTPS z dvoch dôvodov:

1. webové prehliadače zobrazujú oznam, že HTTP stránka nie je bezpečná (a to naozaj nie je dobrá reklama),
2. vyhľadávače znižujú ranking HTTP stránok a posúvajú ich pri vyhľadávaní nižšie v poradí, takže ich málokto nájde (opäť to nie dobrá vizitka pre obchod).

Pokiaľ chcete vynútiť, aby sa prehliadač pripojil ku stránke vždy najskôr cez HTTPS, tak je možné použiť plugin ako napr. HTTPS Everywhere.

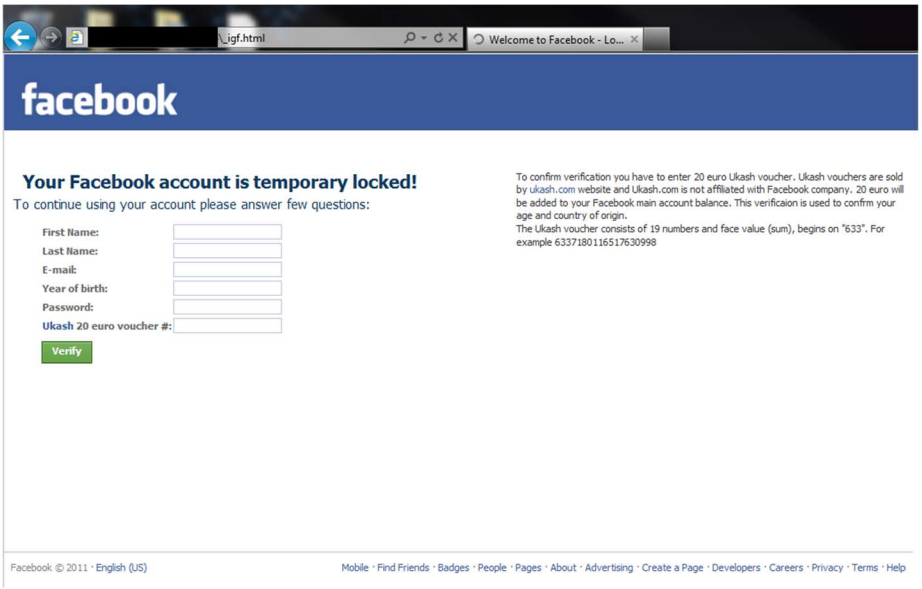
Stretli ste sa pri surfovaní na webe s chybami v overovaní certifikátu? Ak áno, čo by ste odporúčali robiť pri zobrazení chyby?

2. Zlé veci na webe - podvodné stránky a stránky šíriace malvér

V predchádzajúcej kapitole sme si povedali, že ak sa bezpečným spôsobom pripojíme na webovú stránku, neznamená to, že webová stránka je bezpečná a originálna. Môže byť vytvorená za účelom spáchania podvodu alebo inštalácie škodlivého softvéru; webová stránka môže byť napadnutá a pozmenená alebo šíriť obsah, ktorý „nie je v súlade s očakávaním rodiča, resp. školy". Poďme sa pozrieť na jednotlivé možnosti bližšie.

Na špici (vrchole) pyramídy sú stránky šíriace malvér. Pri prístupe na tieto stránky je cieľom donútiť vás kliknúť na časť stránky a akceptovať spustenie alebo nahranie malvéru na počítač. Druhým typom stránok sú stránky, ktoré chcú získať a následne zneužiť vaše údaje. Tieto stránky nazývame podvodné stránky. Podvodné stránky sa snažia napodobňovať legitímne webové stránky vybraných služieb za účelom získania prístupových údajov a/alebo peňazí (napríklad portál na nákup hier, samozrejme zlacnených, alebo internetový obchod s veľkou zľavou na všetko, alebo platobný portál banky, kde sa platí kartou).

Pripraviť web, ktorý vyzerá ako prihlasovacia stránka napr. na Google alebo Office 365 nie je žiadny problém - k dispozícii je množstvo voľne šíriteľných programov, ktoré vedia vytvoriť dokonalú kópiu pôvodnej prihlasovacej stránky. Potom stačí rozposlať verne vyzerajúci phishingový email s odkazom, ktorá vedie na podvodnú stránku a užívatelia sa prihlasujú, aby „vyriešili problém so svojím kontom".



Falošný web napodobňujúci Facebook

Čo by ste odporúčali spraviť v prípade, že by váš známy zadal prihlasovacie údaje do podvodnej stránky?

- *Čo robiť v prípade, ak zadal prihlasovacie údaje zo sociálnych sietí?*
- *Čo robiť, ak zadal údaje o svojej platobnej karte?*
- *Čo robiť, ak zadal svoje osobné a kontaktné údaje?*

Pripraviť zložitejšiu funkcionalitu, ktorá bude napr. kopírovať správanie sa internet bankingu je trochu zložitejšie, ale útočník spravidla len potrebuje v „mene užívateľa" uskutočniť prihlásenie do internet bankingu a platbu - akurát na iný účet a aj v inej sume, najlepšie v sume blížiacej sa čo najviac k limitu obete. Tieto útoky sú veľmi nebezpečné, ale na ochranu vám väčšinou postačí vaša **pozornosť** a **obozretnosť**. Stačí si všímať, či odkazy na stránkach sú funkčné, resp. si čítať, čo vám píše banka. Väčšinou útočníci využívajú jednoduché triky, ako je zmena sumy zo 6,99 EUR na 699 EUR alebo namiesto obyčajného kódu chcú potvrdenie platobného príkazu, pričom sa tvária, že je to potrebné na prihlásenie (títo útočníci si na potvrdenie nevyžiadajú nízku sumu, napr. 0,01 EUR, ale skúšajú veľmi vysoké sumy – napr. od 3000 EUR vyššie).

Stránky, ktoré šíria malvér vieme rozdeliť podľa zložitosti technickej implementácie. Najdokonalejšie pripravené a najzložitejšie sú tie, ktoré si zistia verziu prehliadača a operačného systému a následne použijú pripravený kód, exploit, ktorý zneužije zraniteľnosti v prehliadači (prípadne operačnom systéme, ak je to potrebné) a stiahne do počítača samotný škodlivý softvér - napr. na ťaženie kryptomien alebo ransomvér, ktorý zašifruje dáta na disku. Toto sú však veľmi, naozaj veľmi dobre pripravené stránky, ktoré si vyžadujú veľa vývoja a testovania, a to znamená aj investície. Takéto stránky sú používané pri cielenom útoku, a takýto typ útoku určite nezostane iba pri využití webovej stránky, ale zapojí aj telefonovanie, prehľadávanie sociálnych sietí a získavanie informácií o obeti a podobne.

Načo je dobré prehľadávanie sociálnych sietí pri štartovaní útoku?

Vymyslite komplexný útok. Ako by ste ho realizovali a aké všetky zdroje dát by ste do útoku zahrnuli?

Nie všetky škodlivé softvéry sú tak technicky dokonalé a pokiaľ je potrebná nejaká interakcia od používateľa, tak nasledujú techniky sociálneho inžinierstva - napr. vyskočí oznam o chýbajúcich záplatách, príp. víruse na zariadení. „Riešenie" je jednoduché - stačí kliknúť na linku, stiahnuť a nainštalovať program, ktorý vás bude presviedčať, že problém vyrieši. Ďalšou možnosťou je pribaľovanie škodlivého softvéru k legitímnym programom alebo podstrčenie „lákavého" obsahu do archívu - napr. nový film z obľúbenej nemenovanej zdieľacej služby, ktorý sa však nedá prehrať, kým si nenainštalujete „správny" (a pohotovo pribalený) prehrávač videa. Predpokladať, že na neznámej stránke so špeciálnym najnovším videom z kín, ktoré je samozrejme zadarmo, vám pribalia nástroj na prehrávanie, ktorý je tiež zadarmo a minimálne kodek (zariadenie slúžiace na transformáciu signálu) nebude napadnutý, je asi zbytočné.

Obrana je v tomto prípade náročnejšia, pretože útočník všetko pripravil tak, aby ponuky boli príťažlivé a neodmietnuteľné. Vyskúša všetky možné spôsoby útoku, od zaujímavej ponuky, cez jednoduchosť, nevyhnutnosť, okamžitú reakciu a podobne. Jedinou obranou je vyvarovať sa sťahovania škodlivého obsahu. Nerobiť veci, ktoré od vás firma, ktorá sa tvári, že vám volá jej zástupca, zrazu

požaduje a doteraz nikdy nepožadovala. V prípade, ak čo len trochu pochybujete, kto vám volá, oznámte to skutočnej dotyčnej osobe, prihláste sa na oficiálnu stránku firmy, ktorá vám volá a zavolajte si na uvedené kontaktné čísla. Adresu stránky firmy použite tú, ktorú máte uloženú v prehliadači a nie tú, ktorú vám nadiktuje útočník.

Stránka šíriaca autorsky chránené diela ponúka inštaláciu codec, ktorý obsahuje malvér

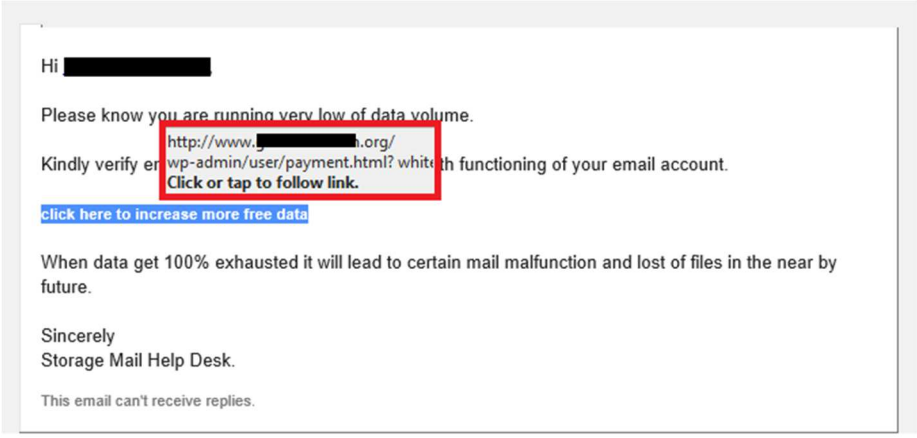
3. Zlé veci na webe - dynamický kód

Nainštalovať, nastaviť a vypublikovať celý webový server, vytvoriť stránke históriu a reputáciu tak, aby bola hostovaná jedna podvodná stránka alebo malvér, je celkom namáhavé. Keďže útočníci sa snažia prácu si zjednodušiť, hľadajú iné možnosti, ako dosiahnuť svoj cieľ. Jednou z možností je využiť infraštruktúru, ktorú už niekto postavil. Existujú minimálne tri možnosti, ktoré majú k dispozícii:

1) **kompromitovať (heknúť) cudzí server** a poskytovať škodlivý obsah z neho. Keďže správcovia webových serverov často nedodržiavajú pravidlá a neaplikujú dostatočne často záplaty, niektoré webové servery[63] dostupné cez internet sú zraniteľné, čo útočníci vedia využiť. Často sa pri menej významných stránkach, najčastejšie malých internetových obchodoch stáva, že kamarát vytvorí internetový obchod, ktorý používa

[63] Webový server má už dnes na starosti naozaj veľa vecí napr. súčasťou býva domáca kamera.

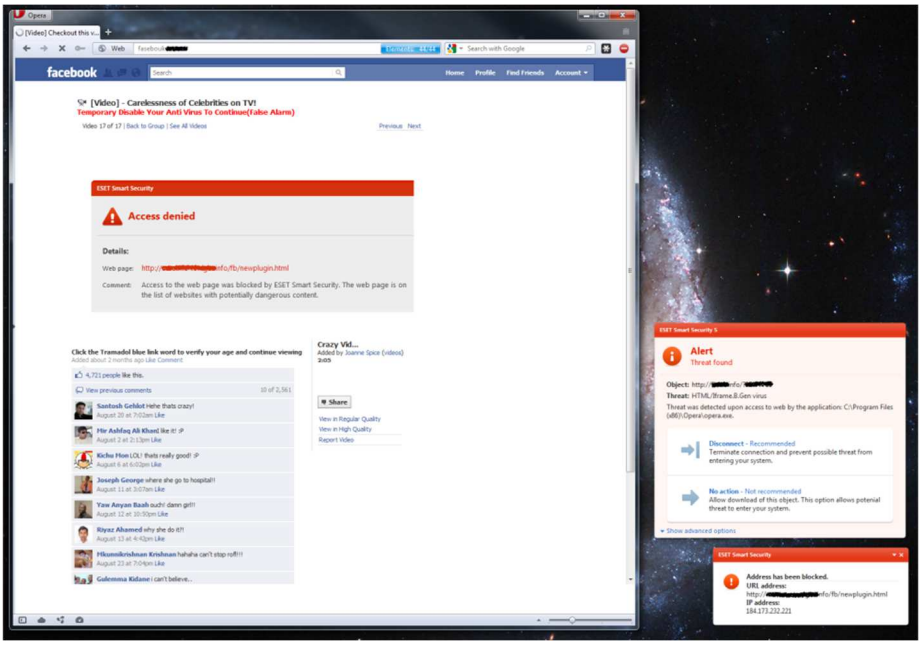
určité služby (operácie) a tvorca sa viac o stránku a používané aplikácie nestará. Internetový obchod následne zastaráva a kopia sa v ňom chyby, ktoré nemá kto opraviť.



Ukážka linky, ktorá vedie na kompromitovaný Wordpress server. Na servery je umiestnený formulár, ktorý zbiera prihlasovacie údaje

2) **využiť reklamu** (malwaretizing) - tento typ útoku bol častý hlavne v časoch flashových reklám[64], kedy útočníci vedeli do flashového bannera pribaliť aj sťahovanie škodlivého softvéru. Potom už stačilo len nájsť neopatrného človeka z marketingu, odcudziť mu účet a začať šíriť škodlivý softvér z úplne legitímneho webu.
3) **využiť možnosť pridávať vlastný obsah** - pokiaľ webová služba umožňuje pridávať užívateľom súbory alebo linky, môže byť táto funkcionalita zneužitá na šírenie odkazov na falošné stránky alebo šírenie škodlivého softvéru. Typickým príkladom sú napr. sociálne siete, kde si každý môže písať a linkovať (zdieľať odkazy), čo chce[65]

[64] Flash už nie je podporovanou technológiou a prehliadače resp. operačné systémy ho vyraďujú z ďalšieho použitia.
[65] Samozrejme, v súlade s pravidlami sociálnej siete.



Príklad šírenia phishingových odkazov prostredníctvom Facebook. Odkazy sú blokované antivírusom.

V prípade scenárov 1) a 2) samozrejme útočníci nechcú kopírovať celý podvodný web aj s obrázkami na kompromitovaný server (a do reklamy už vôbec nie). Z tohto dôvodu často využívajú dynamické prvky webovej stránky, napr. JavaScript, aby sa užívateľ sám presmeroval na škodlivú stránku alebo stiahol škodlivý obsah.

Čo by ste odporúčali urobiť v prípade, ak by si váš známy nainštaloval doplnok z podvodnej stránky?

4. Zlé veci na webe - obsah

Aj keď webová stránka nie je podvodná, stále nemusí byť jej obsah v súlade s tým, čo je v súlade s našou morálkou. Napríklad v súlade s tým, čo rodičia chcú, aby ich deti na internete videli a zažili. Internetové stránky sú obrazom skutočného sveta, a preto vieme nájsť stránky venované záhradkárstvu, rybárčeniu, receptom, ale aj domácej výrobe výbušnín. Na to, aby sme sa vedeli orientovať medzi množstvom stránok, boli vytvorené dva prístupy k vyhľadávaniu:

- **zaradenie do kategórií podľa obsahu** - to znamená, že webové stránky sú rozdelené podľa zamerania do kategórii napr. nakupovanie, literatúra, vzdelávanie a pod.

- **zaradenie do kategórii podľa veku** - existuje systém hodnotenia a zaradenia aplikácii a webových stránok podľa vhodnosti pre určitú vekovú kategóriu - napr. PEGI[66].

Na vynútenie filtrovania podľa kategórii vieme využiť viacero technológii, v ktorých je implementovaná tzv. aplikačná kontrola. Táto môže byť zabudovaná do rôznych technológii, ako je antivírus, užívateľské proxy[67], DNS filtering alebo dedikovaná aplikácia na rodičovskú kontrolu. V domácom prostredí spravidla využívame na blokovanie nevhodných kategórii funkcionalitu **domáceho smerovača (*router*) a antivírusu/rodičovskej kontroly**.

Tieto technológie nám, zvyčajne, umožňujú nastaviť dve veci:

1. **aké kategórie vieme povoliť / zakázať,**
2. **nastaviť časové obmedzenie** - napr. dieťa nebude pozerať Youtube videá dlhšie ako 30 minút denne.

Vyhľadajte na internete systém hodnotenia PEGI. Do akých skupín zaraďuje PEGI hry a webové stránky?

Vyhľadajte, či umožňuje vami používaný antivírusový softvér kategorizáciu webových stránok?

5. Prehliadač, témy a doplnky

V predchádzajúcich kapitolách sme sa venovali prehliadaču, povedali sme si, že vieme nainštalovať do prehliadača rôzne témy a doplnky. Doplnky prehliadača (v angl. *plugin*) sú programy, ktoré dopĺňajú prehliadač o ďalšiu funkcionalitu, ktorú štandardná inštalácia prehliadača neobsahuje. Niektoré doplnky môžu byť užitočné, niektoré nie a niektoré sú vyslovene škodlivé. Prehliadače ako Firefox alebo Chrome umožňujú obmedziť oprávnenia[68] doplnkov v rámci samotného prehliadača. Tieto oprávnenia môžu zahŕňať aj prepísanie

[66] Pan European Game Information - viz. [online]. [11.08.2021]. Dostupné na internete: https://pegi.info/

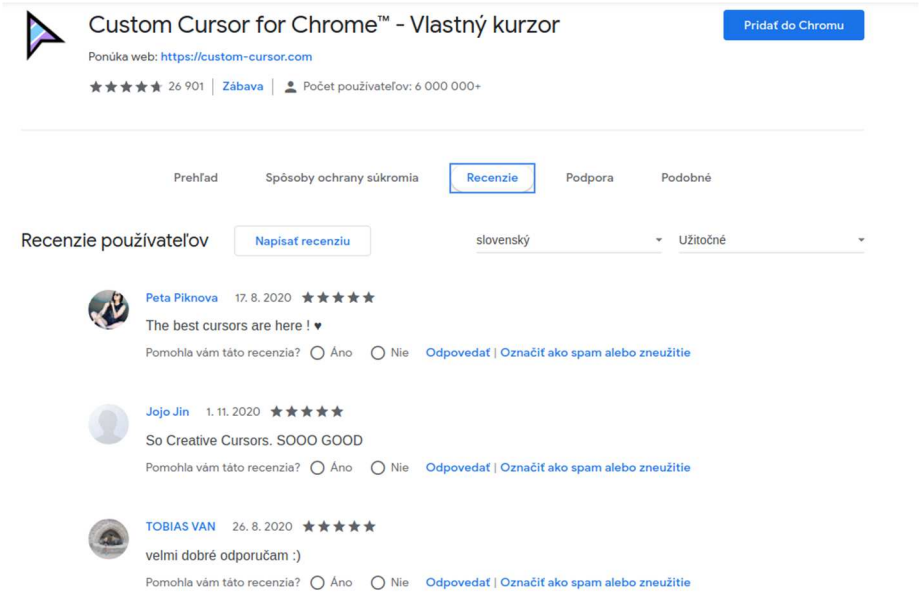
[67] Väčšinou sú používané vo firmách, ale je možné kúpiť si domáci smerovač s takouto funkcionalitou.

[68] Firefox [online]. [11.08.2021]. Dostupné na internete: https://support.mozilla.org/cs/kb/zpravy-s-zadosti-o-opravneni-pro-rozsireni Chrome [online] [11.08.2021] Dostupné na internete: https://vosveteit.sk/chrome-dostava-funkciu-ktora-vam-pomoze-lepsie-identifikovat-potencialne-nebezpecne-rozsirenia/

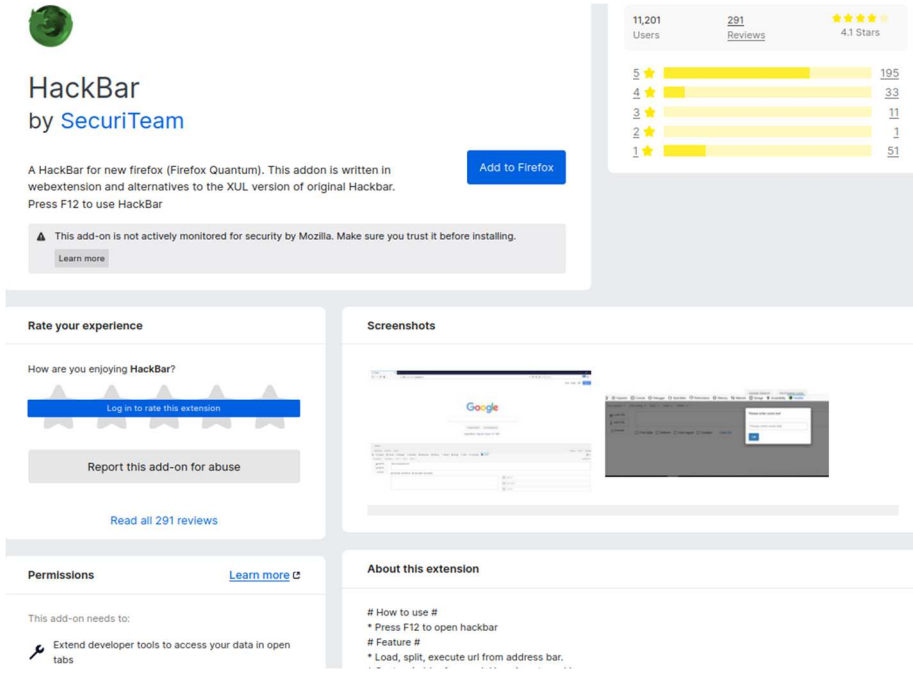
zdrojového kódu zobrazovanej stránky (napr. na blokovanie reklám) alebo čítanie/zápis dát, ktoré zadávame do formulárov (napr. manažér hesiel číta a vkladá za vás heslá).

Škodlivé doplnky by mali byť identifikované vaším antivírusom, alebo samotným prehliadačom. Toto je jedna z dôležitých vlastností antivírusu. V rámci vnútornej kontroly firiem, ktoré vydávajú prehliadač, existuje kontrola tzv. „zlých doplnkov", ktoré sú po identifikovaní automaticky vyradené zo zoznamu doplnkov. Prehliadače vytvorili systém, ako lepšie spoznať bezpečnosť doplnkov, ktoré si môžeme nainštalovať. Je to vlastne súbor hodnotení zložený z:

1. **reputácie/hodnotenia** - systém nula až päť hviezdičiek, podobne ako napr. v obchodoch pre mobilné aplikácie. Čím viac hviezdičiek, tým lepšie,
2. **počet stiahnutí** - čím viac stiahnutí je zrealizovaných, tým väčšia je šanca, že nejde o podvodný doplnok,
3. **recenzie** - čím viac pozitívnych hodnotení, tým sa pravdepodobnosť dôveryhodnosti doplnku zvyšuje,
4. **požadované oprávnenia** - čím viac oprávnení doplnok chce, tým viac škody môže narobiť, ale ako bolo uvedené na príkladoch vyššie, niekedy sa pomerne zásadným oprávneniam nedá vyhnúť.



Príklad doplnku pre prehliadač Google Chrome



Príklad doplnku pre prehliadač Mozilla Firefox

Niektoré doplnky nie sú vyslovene škodlivé, avšak nerobia úplne to, čo by si človek predstavoval a pri jeho povoľovaní je potrebné si prečítať popis doplnku s celou funkcionalitou resp. licenciu k použitiu doplnku. Príkladom môžu byť niektoré doplnky na VPN služby zdarma, ktoré ale zdieľajú internetové pripojenie každého užívateľa - váš prehliadač sa tak stáva výstupným bodom VPN pripojenia niekoho iného. Takéto pripojenie môže byť nebezpečné, ak ten niekto iný je napr. útočník alebo heker. Týmto službám je lepšie sa vyhýbať, aby ste sa nestali súčasťou organizovanej skupiny, ktorej činnosť sa bude schovávať za vašu IP adresu. Samozrejme existuje veľa užitočných doplnkov - o niektorých z nich si povieme v ďalšom texte.

Vyhľadajte, aké doplnky sú použité v prehliadačoch na počítači v počítačovej učebni?

Vyhľadajte, aké doplnky sú použité v prehliadačoch na vašom počítači?

Aké bezpečnostné doplnky používate a ktoré by ste odporučili používať priateľom a prečo?

3. Vyhľadávací systém (search engine)

Vyhľadávací systém (search engine) je nástroj, ktorý prehľadáva webové stránky a indexuje ich obsah, to znamená, že umožňuje rýchle prehľadávanie veľkého množstva stránok, a to na základe kľúčových výrazov. Pri vyhľadávacích systémoch sú dôležité nasledovné atribúty:

1) **kvalita vyhľadávania** - kvalita vyhľadávania závisí od viacerých atribútov, napr. počtu indexovaných stránok, personalizácie výsledkov vyhľadávania, možnosti vyhľadávania v rôznych jazykoch[69] atď.,
2) **prepínače** - sú to veľmi užitočné skratky používané vo vyhľadávacích systémoch, ktorými sa dá zlepšovať presnosť vyhľadávania. Príkladmi užitočných atribútov, napríklad pre vyhľadávací systém google, sú:
    a) site: - prepínač zúži vyhľadávacie výsledky len na konkrétnu stránku. Napr. „kyberneticka bezpecnost site:nbu.gov.sk" vyhľadáva kľúčové slová „kyberneticka bezpecnost" na stránke nbu.gov.sk.
    b) inurl: - zúži výsledky vyhľadávania na konkrétne reťazce v URL. Napr. „inurl:wp-admin" vyhľadáva reťazec wp-admin v URL, t.j. example.com/wp-admin. Pretože URI /wp-admin smeruje na administrátorské rozhranie WordPress CMS, je možné takto nájsť exponované WordPress administrátorské rozhrania.
    c) filetype: alebo ext: - zúži výsledky vyhľadávania na typ súboru alebo príponu súboru.
    d) Ak viete, ako presne vyzerá výraz, ktorý hľadáte, potom vhodným prepínačom je dať tento výraz do úvodzoviek napr. „*Nicola Tesla"*.

Zaujímavú pomôcku na používanie prepínačov nájdete napr. na tejto adrese:

https://ahrefs.com/blog/google-advanced-search-operators/

[69] napr. problémom je používanie skloňovania v slovenčine

Používanie prepínačov je samozrejme možné kombinovať v jednej vyhľadávacej požiadavke.

3) **obsah**, v ktorom je vyhľadávací systém schopný vyhľadávať. Určite ste sa stretli s vyhľadávaním slov na webových stránkach. Vyhľadávať sa však dá aj iný obsah, napr. obrázky cez reverse image search (https://images.google.com/), emotikony, telefónne čísla a profily na sociálnych sieťach, atď.

Vyhľadajte článok o MFA na stránke www.preventista.sk, obmedzte vyhľadávanie pomocou prepínačov.

V časti učebnice Kvality vyhľadávania sme sa dotkli pojmu personalizácia výsledkov. Vyhľadávacie systémy sú spravidla zviazané so zobrazovaním reklamy - čím efektívnejšie vie organizácia dostať zákazníka na svoje stránky (a ku kúpe produktu alebo služby), tým lepšie. Takéto vyhľadávacie systémy vedia prispôsobiť výsledky vyhľadávania histórii používateľa. Vyhľadávacie systémy potrebujú vytvárať obrovskú analýzu na pozadí o správaní každého používateľa. Niekedy takéto systémy, ale aj internetové obchody, vedia o nás viac ako si my vieme o sebe vôbec predstaviť. Práve toto obrovské penzum informácií sa stále častejšie stáva hrozbou a odborníci zaoberajúci sa bezpečnosťou dát majú čoraz väčšie obavy, že vyhľadávacie systémy môžu tieto údaje zneužiť. Príklad: Ak človek pozerá na športové oblečenie nemenovanej značky a následne začne vyhľadávať napr. športové topánky, je pomerne isté, že sa mu zobrazia ponuky od tej istej nemenovanej značky. Takýmto spôsobom fungujú viaceré vyhľadávače ako napr. google, bing, yahoo.

Opakom spomínaného vyhľadávania je použitie vyhľadávacieho systému, ktorý je priateľský k súkromiu, ako je napr. DuckDuckGo. Výsledok takéhoto vyhľadávania je spravidla oveľa menej presný, avšak je garantované súkromie v zmysle, že sa história vyhľadávania nepridáva do veľkej databázy o návykoch užívateľa.

Pozreli sme si teda, čo robia vyhľadávacie systémy na to, aby vedeli všetky novinky o všetkých stránkach. Na druhej strane tohto vyhľadávania sú však internetové stránky s informáciami a autormi, ktorí stránky vytvorili. Autori stránok sa snažia, aby ich stránky boli indexované vyhľadávacími systémami a nezapadli medzi miliónmi iných internetových stránok. Z tohto dôvodu sa snažia optimalizovať stránku pre vyhľadávací systém (search engine optimization - SEO) tak, aby sa ich stránka objavila vo výsledkoch vyhľadávania čo

najvyššie. V prípade vyhľadávačov prepojených s reklamou, samozrejme, posúva výsledky nahor aj čiastka zaplatená za reklamu.

Pri hľadávaní informácie na internete by sme si mali vždy uvedomiť, že stránky, ktoré sú najvyššie pri vyhľadávaní, nemusia byť najlepšie a najkvalitnejšie z pohľadu obsahu, len v danom čase majú teda zaplatenú reklamu. Ďalšou možnosťou, okrem zaplatenia si reklamy, ako sa posunúť v ponuke vyhľadávania stránok čo najvyššie, je vytvoriť si dobré hodnotenie (angl. *ranking*). Získaním domény, ktorá má dobré výsledky vo vyhľadávaní (*page rank*) si vytvárame priestor pre šírenie nášho obsahu väčšej skupine ľudí. Rovnaký spôsob „získavania" väčšieho množstva adresátov používajú pri svojej práci aj internetoví zločinci. Ak vytvoria alebo vlastnia webovú stránku s čo najvyšším hodnotením, ľahšie môžu šíriť škodlivý obsah (škodlivý softvér, podvodný obsah alebo spam). Veľmi zaujímavou možnosťou na podobné obohatenie sa vďaka „popularite" je speňaženie (odpredaj) domény s perfektným (top) hodnotením. Preto niektorí autori pristupujú k používaniu nekalých praktík, označovaných ako Black (hat) SEO[70], aby si pomohli zvýšiť hodnotenie a mohli si tak zvýšiť síce krátkodobé, ale aj tak zaujímavé zisky.

Nájdite na internete rôzne vyhľadávače. Popíšte, ako sa líšia výsledky vyhľadávania pre jednotlivé vyhľadávače. Ktoré vyhľadávače vracajú najpresnejšie výsledky pre slovenské stránky?

Spustite vyhľadávanie konkrétnej informácie v normálnom a privátnom režime. Zistite či sa líšia ak áno, vysvetlite prečo.

Popíšte rozdiel pri spracovaní osobných údajov klientov v rámci prehliadačov: www.yahoo.com, www.google.com, www.duckduckgo.com, www.ecosia.org.

4.5. Email

Služba elektronickej pošty (alebo len email, e-mail) je s nami od „praveku" internetu, teda od jeho vzniku, a jej počiatok sa datuje

[70] Blackhat SEO znamená využitie neetických praktík (ktoré môžu porušovať pravidlá poskytovateľa vyhľadávacieho engine) na to, aby sa webová stránka dostala čo najvyššie vo výsledkoch vyhľadávania.

do roku 1961[71]. Táto služba je navrhnutá tak, aby vedela preniesť správy od odosielateľa k adresátovi. Napriek závratnému vývoju rôznych aplikácií a modelovaniu ich používania, bezpečnosť emailovej komunikácie zodpovedá dobe jej vzniku. Pri používaní elektronickej pošty totiž:

- **nie je garantované doručenie správy** - a to aj napriek tomu sa väčšina e-mailov, ktoré posielame „nestratí". To znamená, že ak vám nepríde email, tak vám ho buď neposlali, alebo sa stratil/zablúdil počas prenosu.
- **nie je zaistená autentickosť správy** - je možné posielať e-maily v mene niekoho iného. Ktokoľvek vie vytvoriť a poslať správu za kohokoľvek, stačí si nájsť vhodnú internetovú službu, alebo u seba vytvoriť poštový server. Toto správanie využívajú legitímne služby - napr. zdieľaný odkaz na cloudové úložisko v mene používateľa; avšak je možné zneužiť toto správanie aj na šírenie podvodných alebo phishingových emailov.
- **nie je chránená správa samotná** - ktokoľvek sa podieľa na doručení e-mailu si vie e-mail prečítať alebo ho pozmeniť. Predstavte si email ako pohľadnicu, ku ktorej môže ktokoľvek, kto ju doručuje, čokoľvek pripísať alebo z nej vygumovať. Pri samotnom doručení však nie je možné zistiť, kto to bol, kedy a ani čo presne na pohľadnici bolo napísané a čo pozmenené.

Všetky uvedené bezpečnostné problémy boli postupne doplnené ďalšími technológiami tak, aby sa zvýšila bezpečnosť takejto komunikácie. Spolu s vývojom internetu sa teda zvyšovala aj bezpečnosť emailu. Tieto doplnené technológie pracujú nad protokolmi elektronickej pošty a my si ich vysvetlíme v nasledujúcich podkapitolách.

1. Doručenie elektronickej pošty

Na doručovanie elektronickej pošty slúži protokol **SMTP** (simple mail transfer protocol). Rovnaký protokol sa používa na odoslanie emailu od e-mailového klienta smerom na server, ako aj na komunikáciu medzi servermi navzájom. Pokiaľ server odošle e-mail a

[71] https://sk.wikipedia.org/wiki/E-mail

ten „blúdi v hlbinách internetu“ (prípadne ho cieľový server zahodí a neoznámi to), pokúša sa server poslať e-mail znova, až kým nenarazí na nastavený limit pokusov. Práve tento mechanizmus zaručuje, že e-mail je v drvivej väčšine prípadov doručený, pokiaľ nie je zahodený napr. z bezpečnostných dôvodov (predstavte si to ako malý guľomet emailov, ktoré sa budú vysielať, kým sa neminú všetky „náboje”, teda kým sa nedosiahne počet stanovených možností).

2. Autentickosť

Na autentickosť e-mailu je možné sa pozerať z troch pohľadov. Predstavme si, že ideme odoslať nasledovnú tajnú správu:

od: M@mi5.gov.co.uk

pre: agent_007@mi5.gov.co.uk

predmet: tajna sprava

správa: Zajtra o šiestej bude čaj o piatej.[72]

Autentickosť správy je teda postavená na tom, že:

1. správu posiela užívateľ M,
2. správa je odoslaná zo servera tajnej služby mi5.gov.co.uk,
3. predmet správy a samotná správa je autentická.

Bodu č. 3 sa budeme bližšie venovať v ďalšej kapitole, a teraz sa poďme pozrieť na prvé dva body. Venovať sa bližšie prvým dvom bodom bude v našom prípade znamenať, že podnikneme „prvé krôčky ku hackovaniu“. V prvom kroku nám bude stačiť emailový server „len” s obyčajným zabezpečením a aplikácia telnet. Položme si otázku: Je možné, aby v mene M poslal správu niekto iný?

Žiaľ, v štandardnej konfigurácii SMTP servera je odpoveďou áno. Keď sa používateľ overí voči SMTP serveru a začne zadávať príkazy na odoslanie e-mailu (to je to, čo robí váš e-mailový klient na pozadí, keď stlačíte tlačidlo „Odoslať”) , tak to môže vyzerať nejako takto:

$ telnet smtp.mi5.gov.co.uk 25

[72] Autormi výroku sú Milan Lasica a Július Satinský.

220 smtp.mi5.gov.co.uk ESMTP Sendmail
> HELO local.domain.name
250 smtp.mi5.gov.co.uk Hello local.mi5.gov.co.uk [11.22.33.44], pleased to meet you
> MAIL FROM: M@mi5.gov.co.uk
250 2.1.0 M@mi5.gov.co.uk... Sender ok
> RCPT TO: agent_007@mi5.gov.co.uk
250 2.1.5 M@mi5.gov.co.uk... Recipient ok
> DATA
354 Enter mail, end with "." on a line by itself
> SUBJECT: tajna sprava
Zajtra o siedmej bude čaj o piatej

Ako si môžete všimnúť, **odosielateľa aj adresáta si vyberá ten, kto sa pripojí na SMTP server**. „Zlý agent_008“ (agent 007 je prijímateľ) sa môže teda pokojne prihlásiť pod svojim účtom a odoslať e-mail v mene M. Pokiaľ server neoverí príslušnosť e-mailovej adresy odosielateľa voči účtu, tak nič nebráni odosielať e-mail v mene iného používateľa.

Podarilo sa nám teda oklamať časť e-mailovej adresy „pred zavináčom”. Je ale možné e-mail odoslať z nejakého úplne iného servera a oklamať aj časť e-mailovej adresy „za zavináčom”? V niektorých prípadoch to možné je. Ako by malo vyzerať overenie časti „za zavináčom” zo strany prijímajúceho SMTP servera?

1. Server sa pozrie na IP adresu, z ktorej mu prišiel email.
2. Skontroluje tzv. MX záznam pre doménu, z ktorej sa email tvári, že prišiel - v našom prípade mi5.gov.co.uk.
3. V prípade, že sa adresy z riadkov 1 a 2 zhodujú, tak je autentický a môžeme ho doručiť.

V praxi sa tento jednoduchý mechanizmus komplikuje aj tým, že organizácia môže chcieť využiť rôzne služby tretích strán, aby mohla posielať e-maily v mene organizácie. To si vyžaduje nutnosť pridávať ďalšie konfigurácie do tzv. SPF (Sender Policy Framework) záznamu, ktoré toto umožňujú.

SPF záznam - obsahuje informácie o tom, ktoré SMTP servery (IP adresy) sú oprávnené odosielať emaily z určitej domény. Systém bol navrhnutý ako ochrana pred SPAMom.

Nastaviť takýto záznam dobre je zložitejšie a existuje množstvo organizácií, ktoré ho majú nastavený nesprávne. Avšak aj v prípade, že organizácia nastaví všetky záznamy perfektným spôsobom, je na SMTP serveri prijímateľa, či sa rozhodne tieto nastavenia skontrolovať. A ak aj správcovia odosielajúceho, aj prijímajúceho SMTP servera urobia všetko správne, nič nebráni útočníkovi na svojom SMTP serveri zadať príkaz v tvare:

> MAIL FROM: M@mi5.gov.co.uk
<M@zly.skaredy.smtp.server.sk>

V tomto prípade sa budú kontroly realizovať pre doménu zly.skaredy.smtp.server.sk a nie pre mi5.gov.co.uk! Potom je už len na šikovnosti „agenta 007“ (prijímateľ/používateľ), aby si všimol, že email neprišiel od „*M@mi5.gov.co.uk*“, ale od „*M@mi5.gov.co.uk <M@zly.skaredy.smtp.server.sk>*“.

Zistite IP adresu webového servera minedu.sk. Ako sa líši od IP adresy servera elektronickej pošty?

Je pre doménu minedu.sk nastavený SPF záznam a ako vyzerá?

Aké ďalšie bezpečnostné prvky ste si všimli pri verifikácii domény minedu.sk?

Odprezentujte svojim spolužiakom, ako ste vyriešili úlohy vyššie a v čom (ne)pomohli nástroje, ktoré ste použili?

3. Dôvernosť a integrita elektronickej pošty

Z dôvodu, že technológie ako SPF chránia autentickosť správy z pohľadu SMTP servera, tieto technológie nemôžeme použiť pri modifikovaní tela e-mailovej správy. SMTP servery medzi sebou môžu komunikovať aj bezpečnou alternatívou prostredníctvom protokolu SMTP**S** (Simple Mail Transfer Protocol Secure), avšak táto sa dá vo väčšine prípadov ľahko obísť vďaka nevhodnému nastaveniu alebo spätnej kompatibilite so SMTP v prípade, že sa správu cez SMTPS nepodarí doručiť. To znamená, že útočníkovi stačí počkať na vhodnom mieste v sieti (na SMTP serveri, na Wifi routri v kaviarni, na

konci VPN spojenia,...) na SMTP komunikáciu a môže začať počúvať alebo meniť čokoľvek.

SMTPS je spôsob zabezpečenia SMTP. Tento protokol zabezpečuje autentifikáciu komunikačných partnerov a rovnako aj integritu a dôvernosť údajov.

Na to, aby sme ochránili telo e-mailovej správy, slúžia riešenia na šifrovanie a podpisovanie e-mailov. Výhodou riešení na šifrovanie a podpisovanie e-mailov je, že koncový užívateľ má na svojom počítači (de)šifrovacie a podpisovacie kľúče[73]. V tomto prípade je možné vyhnúť sa riskovaniu spoľahnutia sa iba na server a je poskytovaná najvyššia možná úroveň ochrany e-mailovej správy.

Nevýhodou takéhoto riešenia je, že koncový užívateľ má na svojom počítači dešifrovacie a podpisovacie kľúče. Z uvedeného vyplývajú dve hlavné kľúčové aktivity/fakty:

1. Kľúče si potrebujeme chrániť pred neautorizovaným prístupom, ale aj zmazaním, či zničením.
2. Ak nie je isté, že šifrovacím a podpisovacím kľúčom disponuje len odosielateľ alebo prijímateľ e-mailu, musíme si kľúče znovu vygenerovať a doručiť si (vymeniť si) ich bezpečným spôsobom.[74]

Vo svete existujú dva štandardy na šifrovanie a podpisovanie e-mailov - PGPMIME a S/MIME. V obidvoch štandardoch je možné spoľahnúť sa pri overení vlastníctva kľúčov na tretiu stranu - pri S/MIME je to spravidla certifikačná autorita, pri PGPMIME kľúčový server a používatelia, ktorí verifikujú kľúče. PGP je teda založené na zdieľanej dôvere. Ak dvaja moji kamaráti dôverujú cudzej osobe, tak aj ja jej budem dôverovať. V obidvoch prípadoch je však možné nastaviť dôveru v šifrovací kľúč ručne. Práve častá potreba ručných

[73] V prípade firemných prostredí to môže riešiť zariadenie nazývané mail encryption gateway.

[74] Rovnaký proces funguje pri bezpečnostnom zámku vo vašom dome. Ak vám niekto ukradne kľúč, zámok s kľúčmi je nevyhnutné okamžite vymeniť, aby ste zabránili vykradnutiu domu. V prípade emailu to znamená výmenu kľúčov a doručenie si ich bezpečným spôsobom a iným kanálom, napríklad si ich vymeníte na USB.

zásahov bráni väčšiemu rozšíreniu PGPMIME a S/MIME. Používanou alternatívou voči S/MIME a PGPMIME je zašifrovanie prílohy elektronickej pošty - napr. kompresia s heslom.

Vyhľadajte na internete, v čom sa líši certifikát verejného kľúča používaný na webovom serveri a certifikát verejného kľúča používaný v SMIME.

Vyhľadajte na internete, akým doplnkom do vášho emailového klienta viete umožniť šifrovanie prostredníctvom PGPMIME? Potrebujete doplnok aj na podporu S/MIME?

Vyskúšajte skomprimovať súbor s heslom. Aké možnosti šifrovania ponúka program, ktorý ste zvolili?

4. Výber poskytovateľa elektronickej pošty

Z predchádzajúcej kapitoly týkajúcej sa konfigurácie SMTP servera bolo možné nadobudnúť (správny) dojem, že prevádzkovať SMTP server vlastnými silami nie je úplne jednoduché[75]. Preto sa väčšina jednotlivcov spolieha na poskytovateľov elektronickej pošty ako napr. Google (gmail), Microsoft (Outlook), Zoznam, Pobox a množstvo ďalších. Z pohľadu bezpečnosti sú podstatné nasledujúce atribúty služby:

1) **podmienky služby** – tieto podmienky predstavujú určitú „zmluvu" medzi používateľom a poskytovateľom služby (elektronickej pošty). V nej je uvedené, za čo je poskytovateľ zodpovedný a čo garantuje, ale aj čo môže a nemôže robiť s dátami používateľov[76]. Poskytovatelia služby spravidla „zdarma" využívajú vaše emaily na reklamu.
2) **Ako bezpečne sú uložené emaily** - niektorí poskytovatelia tvrdia, že emaily šifrujú, avšak väčšinou tak robia spôsobom, aby ich následne vedeli pre používateľa aj dešifrovať. Vybraná skupina poskytovateľov však poskytuje služby na princípe „žiadnych znalostí" („zero knowledge"), tzn. že nemajú žiadnu

[75]Je nutné si uvedomiť, že sem patria aj ďalšie úlohy, ako sú zálohovanie, nasadzovanie záplat a používateľov, ktorí majú sústavne nejaké požiadavky.
[76] Keďže podmienky väčšinou klient nečíta, je možné využiť aspoň služby ako https://tosdr.org/ (terms of service, didn't read), ktoré vedia zhrnúť podmienky do známky podobnej ako v škole.

možnosť, ako sa dostať ku emailom používateľov[77]. V kombinácii s PGPMIME alebo S/MIME ide o najbezpečnejší spôsob uloženia emailov. Týchto poskytovateľov zvyčajne spoznáte podľa nasledovných vecí:

- ich služby nie sú poskytované zadarmo (aspoň nie v plnom rozsahu),
- pri strate hesla nevedia poskytnúť možnosť obnovy dát,
- integrácia s klientom elektronickej pošty nie je priamočiara a niekedy podporujú len webmail rozhranie.

3) **Ako bezpečne sú prenášané emaily smerom ku klientovi elektronickej pošty** - ako sme sa dočítali vyššie, samotný SMTP protokol nie je veľmi spoľahlivý, avšak je dobré zabezpečiť aspoň komunikáciu medzi klientom a serverom elektronickej pošty - už len z dôvodu, aby útočník na sieti nemohol odchytiť prihlasovacie meno a heslo. Používateľ preto chce mať nakonfigurované bezpečné verzie protokolov ako je SMTPS, IMAPS alebo POP3S.
4) **Podpora MFA** - viď kapitolu o MFA.

Popíšte, ktoré bezpečnostné atribúty spĺňa váš poskytovateľ emailovej služby?

Vyhľadajte na internete príklad poskytovateľa zero knowledge emailovej služby.

Pripravte prezentáciu a vysvetlite princíp fungovania PGPMIME alebo S/MIME.

5. SPAM

Spam je nevyžiadaná elektronická pošta. Spamový email nemusí byť nutne škodlivý, avšak zaberá priestor v schránke a stojí používateľa čas na jeho odstránenie. Spam môže mať veľa podôb ako napr.:

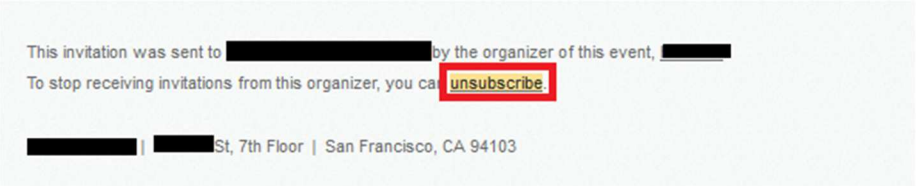
[77] Nepočítame rozbíjanie a odpočúvanie slabo zabezpečeného SMTP protokolu

From: cw@abod.de <cw@abod.de>
Sent: streda, 10. júla 2019 6:21
To: Recipients <cw@abod.de>
Subject: Re

Join the Illuminati and have all your heart desires come through, Fast cars, Spot Lights, Money, Influence and power. Earn $1 million dollars weekly for becoming a member, No blood shared

Príklad SPAM mailu

V SR je nevyžiadaná pošta zakázaná zákonom č. 147/2001 Z. z. o reklame, ktorý zakazuje šírenie reklamy automatizovaným spôsobom cez telefón, telefax alebo elektronickou poštou bez predchádzajúceho súhlasu príjemcu reklamy[78]; komerčná nevyžiadaná pošta je tiež zakázaná zákonom č. 22/2004 Z.z. o elektronickom obchode, ktorý rovnako vyžaduje predchádzajúci súhlas príjemcu. Zákon č. 351/2011 Z.z. o elektronických komunikáciách naviac vyžaduje, aby bol tento súhlas preukázateľný - tzn. Slovenská obchodná inšpekcia, ktorá vykonáva dozor nad dodržiavaním ustanovení zákona o reklame aj zákona o elektronickom obchode, môže vyžiadať od organizácie záznam o udelenom súhlase[79]. Ďalším atribútom zákona o elektronických komunikáciách je možnosť kedykoľvek odvolať súhlas - preto reklamné emaily obsahujú linky[80] na odhlásenie sa z odberu reklamy (Unsubscribe link).

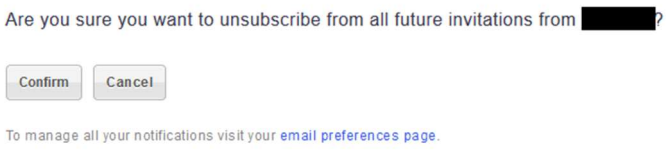


Ukážka linku na odhlásenie odberu reklamy v emaile

[78] Zákon pokrýva aj časť nad rámec tejto učebnice, a to problém s tzv. robocalls - reklamu šírenú prostredníctvom automatického telefónneho systému. Tento zákon zakazuje tiež vhadzovanie letákov do schránok označených, že si adresát nepraje reklamu.
[79] Vzhľadom na geografický dosah SOI na subjekty sídliace v rámci SR je však dosah obmedzený, keďže internet nemá hranice.
[80] Napísané čo najmenším písmom v pätičke emailu.

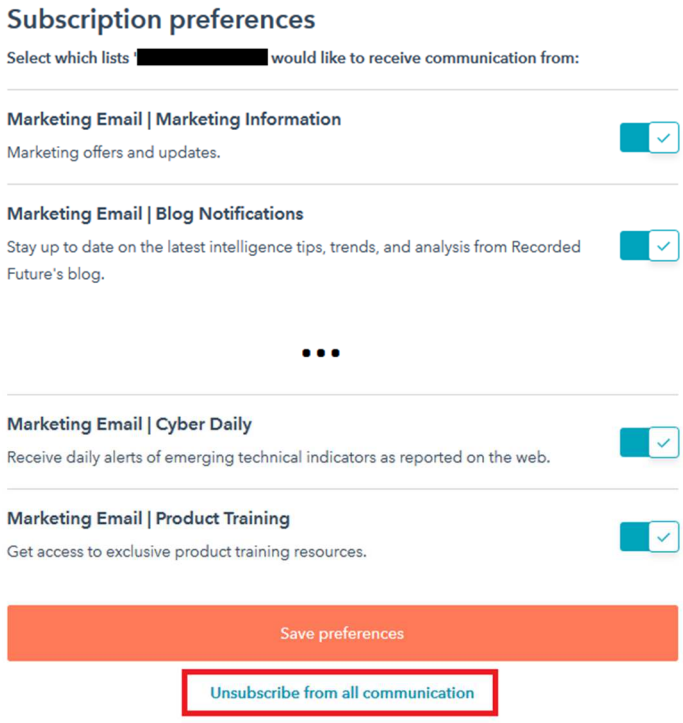
Stretli ste sa s nevyžiadanou elektronickou poštou? Ak áno, popíšte ako vyzerala a či obsahovala linku na odhlásenie.

Teoreticky by mala byť cesta vedúca k odhláseniu priamočiara.



Ukážka jednoduchého formuláru na odhlásenie sa z newslettra

V praxi to môže byť však komplikovanejšie, nakoľko organizácia môže mať viacero reklamných kanálov, odhlásenie z ktorých je potrebné potvrdiť individuálne:



Ukážka zložitého formuláru na odhlásenie sa z newslettra

Čo musí spraviť organizácia, pokiaľ sa odhlásite z odoberania marketingovej komunikácie? Svoju odpoveď zdôvodnite.

Čo sa môže stať po kliknutí na Unsubscribe linku v prípade, že organizácia, ktorá posiela reklamné emaily sa zaoberá rozposielaním podvodných emailov?

6. Hoax

Hoax znamená: falošná správa, fabulácia, novinárska kačica, podvod, poplašnú správu, výmysel, žart, kanadský žartík.

Hoax má niektoré z nasledujúcich znakov:

1) **snaží sa tváriť dôležito** - zasielateľom hoaxového emailu je dôveryhodná osoba alebo firma napr. Microsoft, Úrad vlády SR, FBI, známy lekár, … .
2) **prináša nečakanú informáciu** - napr. šokujúca novinka, uniknuté informácie, exkluzívna akcia - niečo, čo má zaujať a donútiť ľudí hoax čítať,
3) **chce, aby ho ľudia posielali ďalej** - hoax môže obsahovať frázy, ktoré priamo nabádajú na šírenie napr. „pošli ďalším 10 osobám", „zdieľaj, než to zmažú" a pod.

Hoax môže byť, neškodný, avšak niektoré typy hoaxov môžu mať určité dopady na život človeka, ktorý sa nimi riadi. Okrem vytvorenia nepríjemného obrazu o sebe pred rodinou, známymi a kamarátmi, môže informácia v hoaxe viesť aj k vážnejším dopadom napr.:

- poškodeniu zdravia - medicínske hoaxy na lieky, ktoré zaručene fungujú,
- finančné straty - zaručené investície, ktoré prinášajú nečakané zisky,
- strata slobody - hoaxy, ktoré sa prekrývajú s podvodnými emailami môžu ľudí naviesť na participáciu na kriminálnej činnosti.

V prípade rozlišovania, či ide o hoax alebo nie, existuje dôveryhodná stránka, ktorá sa venuje hoaxom. Pre slovenský web je to www.hoax.sk a český web www.hoax.cz, a kde je možné nájsť napr.:

Medicínsky hoax

V Německu se konečně našel lék na CORONA VIRUS. Němečtí lékaři neuposlechli zdravotní zákon WHO, který požaduje, neprovádět pitvy při úmrtích na koronavirus a zjistili, že smrt NEDĚLÁ VIRUS, ale BAKTERIE,. Vede ke krevním sraženinám a ke smrti pacienta. Německo poráží takzvanou Covid-19, což není nic jiného než „široká intravaskulární koagulace" (trombóza). A způsob jak ji léčit, znamená léčit ji antibiotiky, protizánětlivými léky a antikoagulaci. PRVNÍ - ASPIRIN. Tuto senzační zprávu pro celý svět přinesli němečtí lékaři pitvou mrtvých těl produkovaných Covid-19. Němečtí patologové navíc říkají, že mechanické větrání a jednotky intenzivní péče nikdy nebylo třeba. V Německu začala změna protokolu KDO identifikoval a odstranil mezinárodní globální epidemii Lék už byl znám, ale WHO o tom Číňany neinformoval, je to jen obchod!!!	viacnásobné šokujúce informácie ● nový liek, ● COVID-19 je bakteriálna infekcia ● pandémia je obchod
Zdroj: Německo, Ministerstvo zdravotnictví.	dôveryhodná organizácia
Sdílejte!!!!!! Ať se to dostane do celého světa! Předejte to své rodině, sousedům, známým, kamarádům, kolegům, do okolí.	posielajte ďalej...
Prevence? Užívejte 100 mg aspirinu a apronexu nebo paracetamolu. Proč? Protože bylo prokázáno, že Covid-19 stimulací podporuje vývoj trombózy. Protože krev není nasycená kyslíkem. Krev houstne, její	šokujúca informácia o novej liečbe

proudění v srdci a plicích zpomaluje, člověk nemůže dýchat a rychle umírá.	
V Německu byl porušen protokol o doporučení WHO a byla provedena pitva těla, která zemřela na Covid-19. Tělo, paže, nohy a další části těla byly otevřeny a bylo zjištěno, že krev se rozšířila a žíla a krevní sraženiny ve všech žilách a krevní sraženiny v tepně zasahují do normálního průtoku krve a zabraňují dodání kyslíku do všech orgánů, zejména mozek, srdce a plíce a pacient nakonec zemře. Německé ministerstvo zdravotnictví okamžitě změnilo protokol léčby Covid -19 a začalo předepisovat infikovaným pacientům 100 mg aspirinu a apronaxu - výsledek: pacienti se začali zotavovat a došlo ke zlepšení.	opakovanie informácií o dôveryhodnej organizácii šokujúca informácia o zmene liečby
Poskytněte tyto informace, okamžitě je zpřístupněte veřejnosti v celé zemi. Německo /naštěstí/ porušilo normu, po celém světě budou soudní spory za skrytí tolika úmrtí a za kolabující ekonomiky mnoha zemí po celém světě.	posielajte ďalej...
A všichni pochopí proč byl vydán rozkaz pohřbít mrtvé okamžitě bez pitvy a označit je jako velmi znečišťující.	šokujúca informácia
Je v našich silách konat spravedlnost a doufat, že můžeme zachránit mnoho životů.	
Proto fungují antibakteriální gel a oxid chloru.....	uvedený iný šokujúci spôsob liečby
Všechna PANDEMICKÁ PSYCHIS byla potřeba, protože byznys je byznys. Stínová vláda chce očkovat vakcínu a implantovat čip, který zabíjí masy k ovládání populace a snížení světové populace. Je to plánované a kruté, ale neskryje se to, jen na nějaký čas - A J E T O V E N K U	ďalšia šokujúca informácia

Tento hoax nájdete aj s vysvetlením na www.hoax.cz[81].

Zárobkový hoax

Hello Net Transaction Systems (NTS ,inc) is a Lithuanian company, dealing with the software elaboration, web-design and Internet commercials. NTS ,inc began to work in 2000 and now it is considered to be the one of the leaders among IT- service providers in Internet. Large selection of service, high quality of our work, professionalism of our employees and affordable prices attract new clients every day.	dôveryhodná organizácia
The fact is that despite the US market is new for us we already have regular clients also speaks for itself. WHAT YOU NEED TO DO FOR US? The international money transfer tax for legal entities (companies) in Lithuanian is 25%, whereas for the individual it is only 7%. There is no sense for us to work this way, while tax for international money transfer made by a private individual is 7% .That's why we need you! We need agents to receive payment for products in money orders, cheque or bank wire transfers) and to resend the	zaujímavé informácie: ● „klienti" sú k dispozícii ● šokujúca možnosť bezprácneho zárobku

[81] Němečtí lékaři neuposlechli zdravotní zákon WHO a našli lék na CORONA VIRUS [online] [11.08.2021] Dostupné online: https://hoax.cz/hoax/nemecti-lekari-neuposlechli-zdravotni-zakon-who-a-nasli-lek-na-corona-virus/

money to us via Wire Transfer or Western Union Money Transfer. This way we will save money because of tax decreasing.	
JOB DESCRIPTION? 1. Recieve payment from Clients 2. Cash Payments at your Bank 3. Deduct 10% which will be your percentage/pay on Payment processed. 4. Forward balance afer deduction of percentage/pay to any of the offices you will be contacted to send payment to(Payment is to forwarded either by Wire transfer or Western Union Money Transfer). HOW MUCH WILL YOU EARN? 10% from each operation! For instance: you receive 7000 USD via cheques or money orders on our behalf. You will cash the money and keep $700 (10% from $7000) for yourself! At the beginning your commission will equal 10%, thoughlater it will increase up to 12%! ADVANTAGES You do not have to go out as you will work as an independent contractor right from your home office. Your job is absolutely legal. You can earn up to $3000-4000 monthly depending on time you will spend for this job. You do not need any capital to start.You can do the Work easily without leaving or affecting your	šokujúce informácie: ● možnosť ľahkého zárobku - len sa posielajú peniaze ● vysoký zárobok ● všetko je „legálne”

present Job.The employees who make efforts and work hard have a strong possibility to become managers. Anyway our employees never leave us. MAIN REQUIREMENTS 18 years or older legally capable responsible ready to work 2-4 hours per week. with PC knowledge e-mail and internet experience (minimal) And please know that Everything is absolutely legal,that's why You have to fill a contract!	
If you are interested in our offer, please reply to the following email address: manager@ntssystems.com ,Thanks for your anticipated action. And we hope to hear back from you. Regards, Mr Matthew Booth	opäť dôveryhodná organizácia

Tento hoax nájdete aj s vysvetlením na https://hoax.cz/hoax/wellpaid-job-opportunity/ [82]. V tomto hoaxe nie je nič o tom, že je potrebné ho zdieľať - inak by záujemcovi mohla táto príležitosť ujsť.

Prerozprávajte a vysvetlite text zárobkového hoaxu. V čom spočíva jeho nekalá činnosť?

Mohol by byť človek, ktorý využije ponuku ntssystems.com stíhaný trestne? Ako áno, prečo?

[82] Wellpaid job opportunity [online]. [11.08.2021]. Dostupné online: https://hoax.cz/hoax/wellpaid-job-opportunity/

Stretli ste sa s hoaxom? Ak áno, popíšte, čo bolo predmetom hoaxu a ako ste zistili, že ide o hoax?

Ako by ste overili pravdivosť alebo nepravdivosť konkrétneho hoaxu? Vyskúšajte si svoje znalosti napr. na https://datujzodpovedne.o2.sk/

Vyhľadajte na internete, aký je rozsah škôd spôsobených podvodmi za predchádzajúci kalendárny rok.

7. Phishing

Phishing je typ počítačového útoku, pri ktorom sa útočník prostredníctvom návnady v elektronickej komunikácii snaží získať od obete citlivé údaje, alebo ju prinútiť otvoriť súbor so škodlivým softvérom, prípadne kliknúť na škodlivú linku. Cieľom phishingu je teda vždy škodlivá aktivita.

Phishing sa nešíri len v podobe elektronickej pošty. Variant phishingu v podobe SMS nazývame **smishing** (prefix SMS + phishing). Variant phishingu v podobe telefonátu sa nazýva **vishing** (**v**oice ph**ishing**).

Problémom phishingu je, že sa častokrát tvári ako legitímny email a napodobňuje štandardné typy správ, ktoré posielajú prevádzkovatelia služieb a/alebo výrobcovia produktov. Tento problém sa rovnako aplikuje aj na smishing aj na vishing, pretože podvrhnúť telefónne číslo volajúceho/odosielateľa SMS je rovnako jednoduché ako podvrhnúť email.

Phishing môže spĺňať jeden alebo viacero z nasledujúcich znakov:

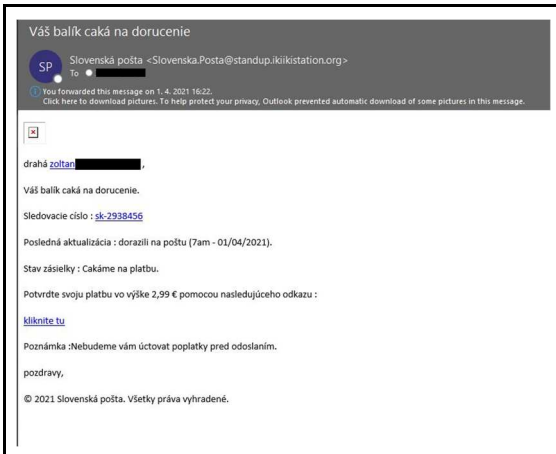
- **Odosielateľ správy je neznámy, alebo sa snaží napodobniť** známe meno napr. „Microsoft support <gates1@gmail.com>”.

- Správa **obsahuje prílohu, ktorá je spustiteľná**. Podozrivé prílohy sú napr. súbory z koncovkou .exe, .cmd, .bat, .msi, .img, .scr, .jar[83] príp. sú spustiteľné a zabalené do archívu .zip alebo .rar. Spustiteľný kód však môžu obsahovať aj súbory MS office a PDF.
- Správa **obsahuje linku na neznámu alebo nedôveryhodnú webovú adresu**, pozri kapitolu Web.
- Správa je **formulovaná všeobecne** - napr. Vážený zákazník, Milý peter.novy@mojaadresa.sk, ...
- Správa **požaduje zaslanie citlivých údajov** emailom alebo ich vloženie do formulára na webe.
- Správa obsahuje **gramatické chyby** - podobne ako pri preklade cez Google Translate.
- Správa požaduje **vykonanie okamžitej akcie**. Napr. okamžitá inštalácia bezpečnostných záplat, overenie stavu doručenia balíka.

Pozrime si tieto znaky na príkladoch:

❖ Príklad neobsahuje daný znak phishingu.

✓ Príklad obsahuje daný znak phishingu.


Váš balík caká na doručenie

SP Slovenská pošta <Slovenska.Posta@standup.ikiikistation.org>
To [redacted]

You forwarded this message on 1. 4. 2021 16:22.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

drahá zoltan[redacted],

Váš balík caká na doručenie.

Sledovacie číslo : sk-2938456

Posledná aktualizácia : dorazili na poštu (7am - 01/04/2021).

Stav zásielky : Cakáme na platbu.

Potvrdte svoju platbu vo výške 2,99 € pomocou nasledujúceho odkazu :

kliknite tu

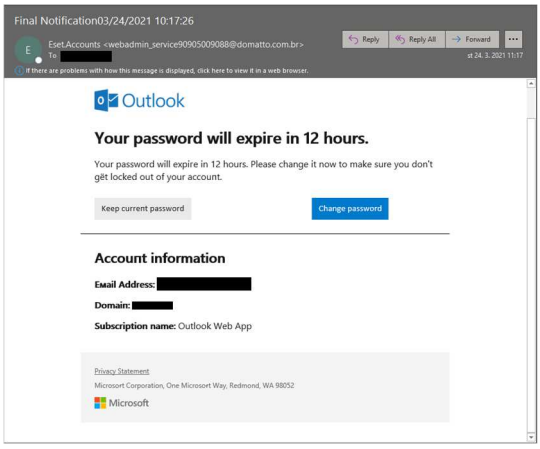
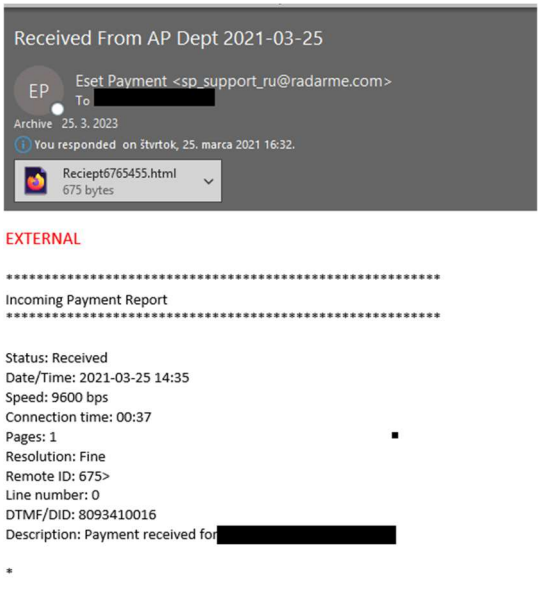
Poznámka :Nebudeme vám účtovat poplatky pred odoslaním.

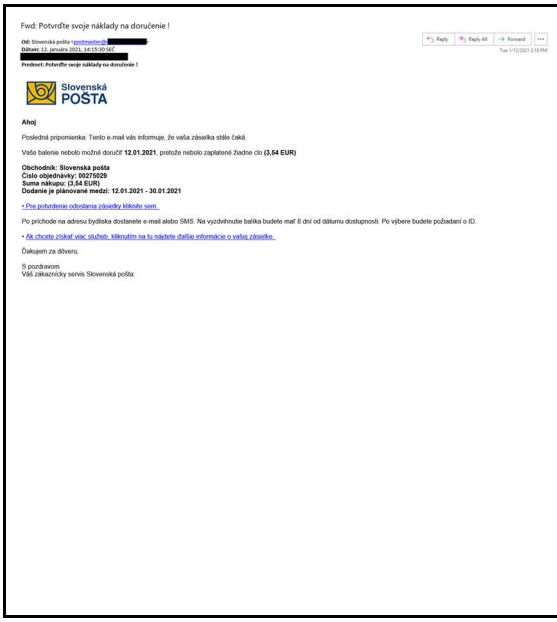
pozdravy,

© 2021 Slovenská pošta. Všetky práva vyhradené.

✓ Odosielateľ správy je neznámy.
❖ Správa obsahuje spustiteľnú prílohu.
✓ Správa obsahuje podozrivú linku.
✓ Formulácia je všeobecná.
❖ Požaduje sa zaslanie citlivých údajov.
✓ Obsahuje gramatické chyby.
✓ Požaduje vykonanie okamžitej akcie.

[83] dlhší, nie však konečný zoznam je napr. k dispozícii tu: https://www.lifewire.com/list-of-executable-file-extensions-2626061

	✓ Odosielateľ správy je neznámy. ❖ Obsahuje spustiteľnú prílohu. ✓ Obsahuje podozrivú linku. ✓ Formulácia je všeobecná. ❖ Požaduje sa zaslanie citlivých údajov. ❖ Obsahuje gramatické chyby. ✓ Požaduje vykonanie okamžitej akcie.
	✓ Odosielateľ správy je neznámy. ✓ Obsahuje spustiteľnú prílohu. ✓ Obsahuje podozrivú linku. ✓ Formulácia je všeobecná. ❖ Požaduje sa zaslanie citlivých údajov . ❖ Obsahuje gramatické chyby. ✓ Požaduje vykonanie okamžitej akcie.


Fwd: Potvrďte svoje náklady na doručenie !

Od: Slovenská pošta <postmaster@[redacted]>
Dátum: 13. januára 2021, 14:15:30 SEČ
[redacted]
Predmet: Potvrďte svoje náklady na doručenie !

Slovenská POŠTA

Ahoj

Posledná pripomienka: Tento e-mail vás informuje, že vaša zásielka stále čaká.

Vaše balenie nebolo možné doručiť **12.01.2021**, pretože nebolo zaplatené žiadne clo **(3,64 EUR)**

Obchodník: Slovenská pošta
Číslo objednávky: 00275029
Suma nákupu: (3,64 EUR)
Dodanie je plánované medzi: 12.01.2021 - 30.01.2021

• Pre potvrdenie odoslania zásielky kliknite sem.

Po príchode na adresu bydliska dostanete e-mail alebo SMS. Na vyzdvihnutie balíka budete mať 8 dní od dátumu dostupnosti. Po výbere budete požiadaní o ID.

• Ak chcete získať viac služieb, kliknutím na tu nájdete ďalšie informácie o vašej zásielke.

Ďakujem za dôveru.

S pozdravom
Váš zákaznícky servis Slovenská pošta.

- ❖ Odosielateľ správy je neznámy.
- ❖ Obsahuje spustiteľnú prílohu.
- ✓ Obsahuje podozrivú linku.
- ✓ Formulácia je všeobecná.
- ❖ Požaduje sa zaslanie citlivých údajov.
- ✓ Obsahuje gramatické chyby.
- ✓ Požaduje vykonanie okamžitej akcie.

Špecifickým typom phishingového útoku je takzvaný **business email compromise** (BEC) útok. Tento vznikne kompromitovaním jedného emailového účtu v organizácii a následne rozposielaním phishingových emailov z tohto účtu, ideálne v súlade s procesmi spoločnosti - napr. účtovníčka posiela odkaz na problémové faktúry, generálny riaditeľ „žiada" o urýchlené zrealizovanie platby atď.. BEC útok môže spôsobiť obrovské škody, nakoľko kolegovia medzi sebou štandardne komunikujú a vzájomne si dôverujú. Preto je jednoduchšie priviesť ich k tomu, aby klikli na linku a/alebo otvorili si prílohu.

Vyhľadajte na internete poslednú verziu Verizon Data Breach Report a zodpovedzte, aký je priemer strát pre business email compromise (BEC) útoky?

Ochrana pred phishingom spočíva v rozpoznaní falošnej správy ako takej a nereagovanie na správu, resp. označenie správy ako falošnej. Napríklad: Ak dostanete oficiálny email od kohokoľvek, tento musí pochádzať z oficiálnej adresy odosielateľa a gramatické chyby sú viac ako prekvapivé, preto email s gramatickými chybami je podozrivý. Email, či SMS sú komunikačné kanály, pri ktorých sa

nepredpokladá neustále kontrolovanie, často sa označujú ako offline kanály. Ak vás niekto osloví cez offline kanál a vyžaduje okamžitú reakciu, takýto tlak sa považuje za podozrivý. V prípade akéhokoľvek podozrenia na phishing, vishing alebo smishing, neváhajte prerušiť komunikáciu a obrátiť sa priamo na danú inštitúciu cez oficiálne komunikačné kanály a požiadajte o vysvetlenie, či vás naozaj kontaktovali. V žiadnom prípade si kontakty nežiadajte od človeka, ktorý vás kontaktoval, t.j. neodpisujte z emailu, nevolajte späť na to isté číslo alebo na číslo SMS, resp. kontakt z SMS, použite vždy oficiálny kontakt z webovej stránky inštitúcie.

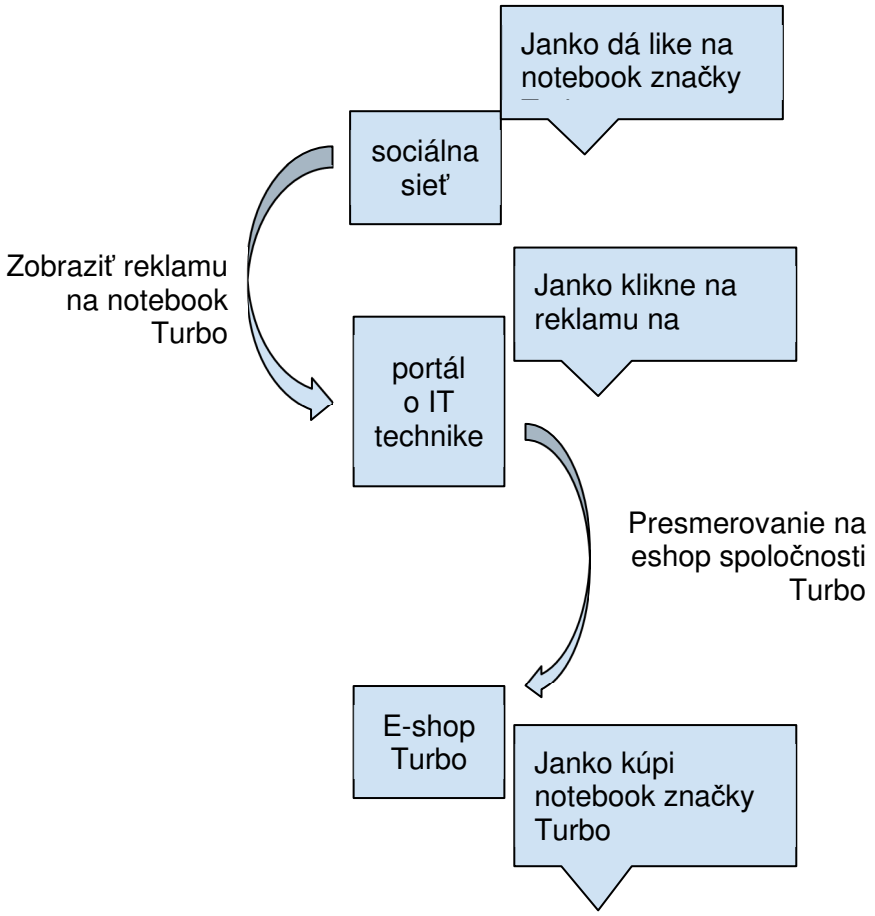
Prečo pri pochybnostiach, či ide o útok alebo nie a pri potrebe vyjasniť si, dôvod kontaktu nesmieme použiť kontakty priamo z phishingového emailu?

Akým spôsobom navrhujete nájsť kontakty na inštitúcie, ktorých meno bolo zneužité na phishingový, vishingový resp. smishingový útok?

4.6. Súkromie v kybernetickom priestore

Ako sme spomínali pri emailoch - na internete sú k dispozícii služby „zdarma”, ktoré sú len zdanlivo zdarma a kde používateľ platí svojimi dátami. Dotýka sa to napr. freemailových služieb, sociálnych sietí, platforiem na zdieľanie súborov, videa a iného obsahu a pod. Niektoré z týchto služieb fungujú v rôznych úrovniach napr. majú obmedzenie objemu uložených dát, alebo obmedzujú dostupné vlastnosti. Vyššiu úroveň služieb si musí používateľ priplatiť. Niektoré služby sú však úplne zadarmo a v takomto prípade je spravidla cieľom prevádzkovateľa služby získať prístup k dátam používateľa, analýza týchto dát a následné zobrazovanie cielenej reklamy, ktorú si môžu zaplatiť ľubovoľné organizácie. Objem dát, ktoré môže takýto predajca reklamnej plochy získať v rámci svojej plaftormy (freemailu, sociálnej siete) je však limitovaný, a preto je skutočne vhodné rozšíriť sledovanie používateľa aj mimo platformy. Z tohto dôvodu vedia reklamné spoločnosti poskytnúť prevádzkovateľom webových stránok možnosť sledovania návštevníkov a generovanie detailných štatistík správania sa návštevníkov, napr. za účelom optimalizácie webovej stránky alebo zobrazovania vhodnej reklamy.

Ideálny scenár z pohľadu predajcu reklamy a produktu môže vyzerať takto:



Scenár sledovania správania používateľa

Výsledkom takejto operácie je predaný tovar, zisk pre predajcu reklamy a zároveň odmena za kliknutie pre prevádzkovateľa portálu o počítačovej technike, pričom v niektorých prípadoch môže byť spokojný aj používateľ tovaru, ktorý si slobodne kúpil. Samozrejme, odhaliť, čo je pre používateľa predmetom záujmu, sa dá viacerými spôsobmi - z lajkov, zdieľaných príspevkov, kľúčových slov, ktoré vyhľadáva, atď. Zároveň používateľ nemusí pridávať lajk len na sociálnej sieti - lajkovať sa dá priamo aj na webových stránkach.

Vyhľadajte na internete rebríček najväčších online reklamných spoločností.

Čím presnejšie vie reklamná spoločnosť identifikovať človeka, tým lepšie vie zobraziť reklamu na tovar alebo služby, ktoré chce alebo môže chcieť kúpiť. Identifikácia je riešená viacerými spôsobmi, napr.:

1) **IP adresa -** IP adresa je veľmi nepresný identifikátor, pretože za jednou IP adresou sa môže nachádzať viacero zariadení.
2) **nastavenie prehliadača** - pri načítaní webovej stránky je možné prostredníctvom viacerých metód zistiť, aký operačný systém, prehliadač, rozlíšenie, doplnky atď. sú použité a v kombinácii s IP adresou, z ktorej používateľ pristúpil, identifikovať používateľa ešte presnejšie.
3) **cookies** - cookie je malý kus dát, ktoré si uloží webový server na počítači klienta. Cookie môže obsahovať jednoznačný identifikátor používateľa, čím vie prevádzkovateľ webovej stránky identifikovať jeho pohyb po webe.
4) **Tracking pixel** - pixel je najmenšia zobraziteľná jednotka na vašej obrazovke. Cieľom, samozrejme, nie je zobraziť pixel konkrétnej grafiky, ale v rámci zobrazenia stránky pristúpiť na pixel s konkrétnym identifikátorom a tým identifikovať používateľa.

Zistite na internete, aká je IP adresa, z ktorej surfujete na webe. Aká je geografická poloha tejto IP adresy?

Zobrazte v prehliadači ľubovoľnú webovú stránku a zistite, aké cookies nastavila. Čo je obsahom týchto cookies?

1. Cookies

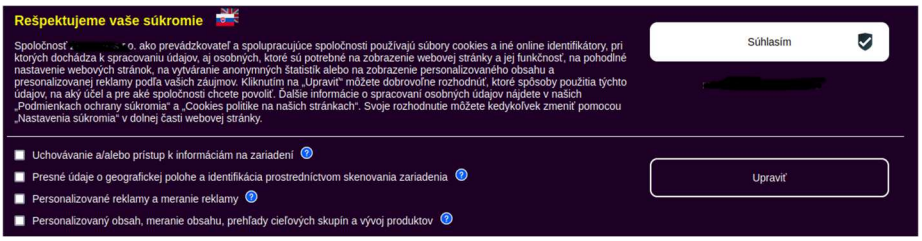
Problematiku spojenia osobnej ochrany a cookies sme si vysvetlili. V tejto kapitole sa pozrieme na cookies z technicko-právneho hľadiska. Cookies sú tak často využívané na sledovanie používateľského správania, až sa stali predmetom regulácie. Cookies sú riadené z dvoch pohľadov:

1) e-Privacy - základom je EÚ Directive on Privacy and Electronic Communication, ktorá je transponovaná do Slovenskej legislatívy Zákonom o elektronických komunikáciách.

2) spracúvanie osobných údajov - základom je GDPR a zákon o ochrane osobných údajov.

Táto regulácia si vynútila zobrazovanie bannerov s akceptáciou cookies.

Napríklad:



Príklad možností nastavenia cookies na webovej stránke prostredníctvom cookiewall

Tento banner sa nazýva **cookiewall** (zlúčenie slov cookie a firewall, keďže tento banner môže celkom zamedziť prístup na webovú stránku, pokiaľ ho používateľ neodklikne). Zo zobrazeného cookiewallu vyplýva viacero skutočností:

1) na sledovanie sa používajú online identifikátory, pričom však **cookies môžu obsahovať aj osobné údaje,**
2) údaje z cookies sú **spracúvané na základe súhlasu** používateľa s cieľom personalizácie obsahu a reklamy,
3) údaje z cookies sú ďalej spracúvané ďalšími spoločnosťami, ktorých výber má používateľ šancu ovplyvniť.

Len na pripomenutie z kap. 4: cookies sa rozdeľujú podľa spôsobu použitia na základné (Essential), funkčné, reklamné a sledovacie cookies.

Otvorte prehliadač v private window a navštívte webovú stránku podľa pokynov učiteľa. Aké cookies stránka používa? Aké máte možnosti výberu cookies?

2. Zachovanie súkromia

Zachovanie súkromia na internete je veľmi podobné riadeniu kybernetickej bezpečnosti - snažíme sa dosiahnuť zlatú strednú cestu

medzi rizikami a opatreniami. Na pomyslenej škále môžeme ľudí rozdeliť na tých, ktorí o sebe na sociálnych sieťach prezradia všetko, až po privacy extrémistov, ktorí používajú techniky na ochranu súkromia aj vo fyzickom svete.

Je potrebné zamyslieť sa nad tým, aká miera súkromia je pre nás vyhovujúca a čo sme pre jej dosiahnutie schopní urobiť, resp. obetovať. V prvom rade je potrebné povedať, že ochrana súkromia nie je iba súbor technických opatrení, ale postoj každého z nás. Je jedno, aký softvér či doplnky prehliadača si nainštalujeme, pokiaľ si neuvedomíme riziká šírenia informácií o sebe na sociálnych sieťach, žiadne z uvedených nás neochránia.

V tejto kapitole si ukážeme niekoľko základných krokov, ktoré vieme použiť na ochranu súkromia a uvedieme niekoľko odporúčaní.

1. **Nešíriť o sebe informácie!**

   Prvé odporúčanie znie na prvé prečítanie dobre, ale v praxi je veľmi zložité ho dosiahnuť. Takmer každý človek má minimálne mobilný telefón, ktorý zachováva digitálnu stopu bežným používaním. Je však vhodné nezdieľať dáta vedome a ak už tak robíme, mali by sme poznať riziko dopadu na naše súkromie a prípadne ďalšie riziká.

Ako by vedel kriminálnik využiť nasledovný post na sociálnej sieti:

„Posielam pozdravy z dovolenky z Tibetu :)"?

Ako by vedel predátor využiť zverejnené trasy behov na fitness mobilnej aplikácii?

2. **Metadáta sú dôležité!**

Metadáta sú dáta, ktoré poskytujú informáciu o iných dátach. Túto komplikovanú definíciu si vieme ilustrovať na nasledujúcich príkladoch:

IP *adresa - IP adresy komunikujúcich strán môžu byť metadátami o tom, že komunikácia prebehla, ale zároveň neobsahujú samotný obsah komunikácie.*

Metadáta k obrázku (EXIF) - môžu obsahovať informácie o zariadení, ktoré zhotovilo obrázok a jeho nastavení, príp. polohe; ako aj dátum a čas vytvorenia obrázku.

Pozrite si detaily pre fotografie vytvorené vašim mobilným telefónom. Aké informácie sú uložené v metadátach?

Vyhľadajte na internete, či viete pre váš model telefónu vypnúť ukladanie polohy pri vytvorení fotografie.

Skúste vytvoriť fotografiu a nahrať ju na sociálnu sieť. Následne túto fotografiu zo sociálnej siete stiahnite a porovnajte metadáta originálnej fotografie s fotografiou stiahnutou zo sociálnej siete. Zmenili sa metadáta?

3. Nepoužívajte svoje dáta, ak to nie je potrebné!

Viacero služieb vo fyzickom svete, aj na internete, funguje na princípe výmeny osobných dát za službu. Týka sa to spravidla emailovej adresy, fyzickej adresy a telefónneho čísla. Zaujímavým príkladom sú rôzne nákupné akcie, kde môžeme za svoje osobné údaje dostať zľavu. V prípade internetu môže ísť o poskytnutie napr. odborného reportu za kontaktné údaje. Pokiaľ reálne nepotrebujeme, aby nás dotyčná spoločnosť kontaktovala[84], tak je lepšie využiť jednorazové kontaktné údaje (tzv. „burner" z anglického burn - spáliť), spravidla email alebo telefónne číslo.

Vyhľadajte službu 10 minutes email a zistite, či viete zo svojej emailovej adresy poslať alebo prijať email z/na vygenerovanú emailovú adresu.

Skúste na internete nájsť dôvod, prečo by vygenerovaná emailová adresa nemala fungovať.

Anonymizácia telefónneho čísla je spravidla služba na komerčnej báze. Analogicky sa vieme vyhnúť zdieľaniu dát o svojej kreditnej karte prostredníctvom jednorazových (anonymných) platobných kariet alebo využitím služieb tretích

[84] Napr. z dôvodu, že sme zabudli heslo k službe.

strán. Jednorazové/anonymné platobné karty sú väčšinou komerčné služby, ktoré nemusia byť dostupné v niektorých krajinách. V rámci Slovenskej republiky je táto služba súčasťou balíčka väčšiny bánk. Pri využívaní služieb tretích strán je potrebné skontrolovať si podmienky používania, aby služba nebola z pohľadu prieniku do súkromia horšia ako platba platobnou kartou. Pri platbe platobnou bránou sú o transakcií informovaní: obchodník, platobná brána, banky, v ktorých sú účty a samozrejme vy. Tento zoznam môže byť v prípade tretích strán výrazne dlhší.

Vyhľadajte na internete, s koľkými tretími stranami zdieľa pri používaní vaše dáta spoločnosť PayPal.

4. Použite doplnky webového prehliadača na ochranu súkromia!

Keďže webový prehliadač je na počítači bránou do internetu, tak sa spravidla pozornosť reklamných agentúr sústreďuje práve na web[85]. Tu, rovnako ako v prípade vírusov a antivírusov, sa v oblasti reklamy a súkromia vedie boj o dáta používateľov. Reklamné spoločnosti sa snažia využívať inovatívne metódy na viac či menej spoľahlivú identifikáciu používateľov a výrobcovia doplnkov na ochranu súkromia sa snažia tieto metódy potláčať. Viac o odporúčaných doplnkoch sa dozviete v kap. Ochrana a starostlivosť o počítač.

Vyhľadajte, aké doplnky na ochranu súkromia ponúka vami preferovaný prehliadač?

Vyhľadajte na internete, či existujú webové prehliadače zamerané na ochranu súkromia.

5. Využite možnosť anonymizácie sieťovej komunikácie!

Ako sme uviedli vyššie, IP adresa je z pohľadu súkromia zaujímavý údaj. Existujú preto možnosti, ako používanú IP adresu skryť. V princípe tu hovoríme o dvoch prístupoch: buď sa použije plne anonymná sieť (ako TOR

[85] a v menšej miere na email, ktorý tiež môže fungovať ako webová stránka vo formáte HTML.

alebo I2P), alebo sa využije tretia strana, ktorá komunikáciu presmeruje cez seba. Presmerovanie komunikácie je spravidla riešené buď cez proxy server, alebo cez virtuálnu privátnu sieť (VPN). Viac sa o týchto metódach dozviete v kapitole Ochrana a starostlivosť o počítač.

4.7. Heslá

Používateľské heslá (kódy, PIN kódy) sú základným bezpečnostným prvkom autentifikácie používateľa voči operačnému systému, aplikácii či službe. Je teda úplne logické, že ich bezpečnosť a odolnosť voči rôznym metódam útoku je základnou témou chápania bezpečnosti informačných systémov.

 **Heslo** tvorí tajný reťazec znakov známy len určitej entite (a overovateľovi identity), ktorý sa používa na autentifikáciu entity[86].

 Použitie hesla znamená využitie jedného faktora autentizácie - „niečo, čo viem". Špecifickým typom hesla je napr.:

- **PIN** (personal identification number) - postupnosť číslic, ktorú využívame napr. pri platbách kartou.
- **heslová fráza** (passphrase), ktorá spravidla využíva viac slov na zvýšenie dĺžky hesla.

 Vypočítajte aká veľká je množina všetkých rôznych:

1) *6-miestnych PIN kódov?*
2) *6-miestnych hesiel, pokiaľ sa použijú len malé a veľké písmená anglickej abecedy (26 znakov)?*
3) *6-miestnych hesiel, pokiaľ sa použijú malé/veľké písmená anglickej abecedy a číslice?*

1. Popis útokov na heslá

Druh útoku na heslo je vo všeobecnosti veľmi rozšírený. Pokiaľ nemáme na mysli spôsoby získavania hesiel jednoduchším

[86] Definícia prevzatá zo „Zákona o kybernetickej bezpečnosti - Komentár", ISBN 978-80-8155-086-7.

spôsobom, ako napríklad odpozeraním reťazca znakov z papierika prilepeného na monitore (alebo nalepenom na opačnej strane klávesnice), tak útoky na získanie hesiel sú vedené nasledovnými scenármi:

- **útok voči prihlasovaciemu formuláru aplikácie** - prihlasovací formulár je prístupný z internetu (v prípade interných aplikácií z internej siete) a útočník má šancu pokúšať sa prihlásiť do cudzieho účtu. Tento útok je veľmi pomalý a väčšina aplikácii je chránená voči „hádaniu“ hesla zobrazením CAPTCHA hádanky alebo limitovaním počtu prihlasovacích pokusov. Útočník má k dispozícii spravidla dva typy útokov:
    - **slovníkový útok** - skúšať slová zo slovníka, či už obsahujúceho všetky slová z jazyka alebo šitého na mieru užívateľovi - ak vieme, že Jankin pes sa volá Rexo, tak do slovníka pripravíme variácie ako: „Rexo”, „rexo”, „Rexik”, … Na internete sú dokonca k dispozícii slovníky s uniknutými heslami.
    - **útok hrubou silou** – skúšať po poradí kombinácie znakov ako: aaaaa, aaaab, aaaac, … Tento útok bude vždy úspešný, keďže prehľadáva všetky možné reťazce znakov, avšak útok je veľmi pomalý a v prípade komplexných hesiel obsahujúcich veľké/malé písmená, číslice a špeciálne znaky sa spomaľuje ešte viac. Z uvedeného dôvodu nie je možné využiť takýto typ útoku na prihlasovací formulár. Za určitých okolností však tento útok môže byť použitý pre krátke heslá. Slovníkový útok je možné kombinovať s tzv. útokom hrubou silou. Pokiaľ sa Jankin pes volá Rexo, tak útočník bude chcieť skontrolovať aj heslá ako „Rexo123”, čiže použiť brute-force (hrubú silu) nad slovníkom do určitej miery zložitosti.
- **útok voči heslu v chránenej (zahašovanej) podobe** - tento scenár prichádza do úvahy v prípade privilegovaného užívateľa, ktorý má prístup do databázy, kde sú uložené heslá, alebo v prípade kompromitácie aplikácie, kedy databáza hesiel unikne. Aj v prípade zahešovanej podoby môže útočník využiť slovníkový útok a útok hrubou silou.

- **recyklácia známych hesiel** (credentials stuffing[87]) - pokiaľ dôjde k úniku prihlasovacieho mena a hesla z jedného informačného systému, nie je pre útočníka problém vyskúšaťrovnakú kombináciu znakov aj na inom informačnom systéme.

Hašovacia funkcia - je funkcia, ktorá pre rovnaký vstup vytvára vždy rovnako dlhý výstup s pevnou dĺžkou. Toto však znamená, že existuje viacero vstupných reťazcov s rovnakým hašovacím reťazcom.

Útok voči zahašovanej forme hesla nazývame (password) **cracking** - od anglického crack - rozlúsknutia.

Vyskúšajte vytvoriť haš zo známych anglických slov a vyhľadajte v online password cracking nástroji, či je uvedený haš cracknuteľný:

Slovo	*Nájdený MD5 Haš (Hash)?*	*Nájdený SHA-1 Haš (Hash)?*
password		
Macka		
Vymysli vlastné heslo:		

Vyhľadajte na internete informácie, aké sú aktuálne časy na cracknutie hesiel dĺžky 10 znakov zložených z:

1) *číslic,*
2) *číslic a malých písmen,*
3) *číslic, malých a veľkých písmen,*
4) *číslic, malých/veľkých písmen a špeciálnych znakov.*

[87] Doslova prepísať (vložiť) rovnaké prihlasovacie údaje do iných prihlasovacích formulárov, preto názov credentials stuffing.

Prihlasovacie údaje, ktoré unikli na internet sa nazývajú „**leaked**" (presiaknuté). Na internete existujú databázy uniknutých prihlasovacích údajov, ktoré je možné využiť etickým spôsobom (na overenie, či sú uvedené údaje leaked) ale aj neetickým spôsobom (napr. na credentials stuffing, ale aj phishing).

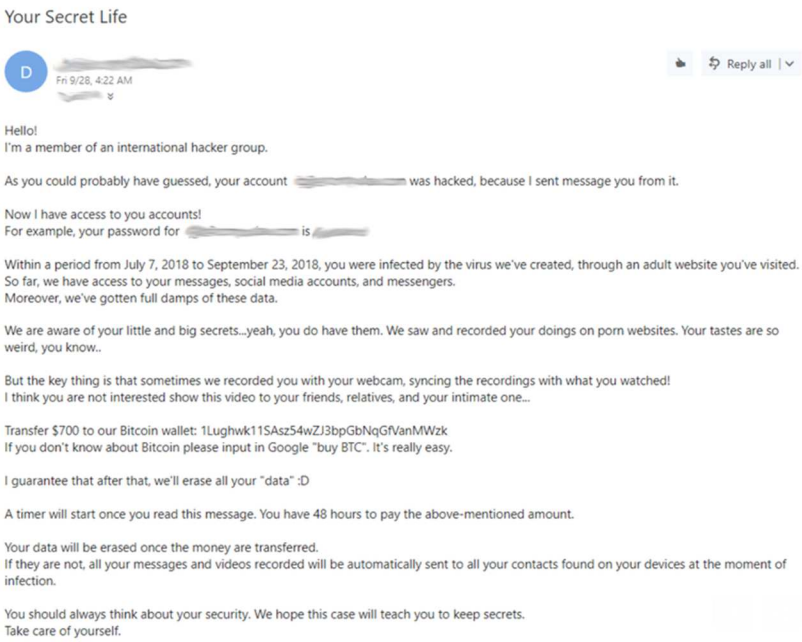
Jedným z portálov uniknutých údajov, ktorý je možné využiť etickým spôsobom je napr. www.haveibeenpwned.com, na ktorom je možné preveriť, či je emailová adresa súčasťou niektorej kolekcie uniknutých prihlasovacích mien a hesiel.

Príkladom[88] sextortion emailu rozposielaného na uniknuté emailové adresy zo sociálnej siete LinkedIn[89] je na obrázku

[88] Sextortion scammers still shilling with stolen passwords [online]. [cit. 11.08.2021]. Dostupné online: https://www.welivesecurity.com/2020/04/30/new-sextortion-scam-claims-know-your-password/

[89] Sextortion email scam scores criminals $4 milion, now spoofs victim's email [online]. [cit. 11.08.2021]. Dostupné online: https://community.spiceworks.com/topic/2169003-sextortion-email-scam-scores-criminals-4-million-now-spoofs-victim-s-email

nižšie. Všimnite si, že útočník použil znalosť uniknutého hesla, aby presvedčil obeť, že o nej vie všetko:



Your Secret Life

D [redacted] Fri 9/28, 4:22 AM [redacted]

Reply all

Hello!
I'm a member of an international hacker group.

As you could probably have guessed, your account [redacted] was hacked, because I sent message you from it.

Now I have access to you accounts!
For example, your password for [redacted] is [redacted]

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited.
So far, we have access to your messages, social media accounts, and messengers.
Moreover, we've gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!
I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.
If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.
Take care of yourself.

Príklad sextortion mailu s využitím znalosti o uniknutých prihlasovacích údajoch

Vyskúšajte overiť niektorú z vašich emailových adries cez službu haveibeenpwned. Bola adresa súčasťou kolekcie hesiel? Ak áno, zverejnil k nej portál haveibeenpwned.com heslo? Vysvetlite prečo.

Čo by ste odporučili kamarátovi, ktorého prihlasovacie meno a heslo je uniknuté?

Vyskúšajte overiť Bitcoin peňaženku zo sextortion emailu cez službu https://www.bitcoinabuse.com/. Získal útočník od obetí finančné prostriedky? Ak áno, v akej výške po prepočítaní na eurá podľa aktuálnej ceny Bitcoinu?

2. Bezpečnostné odporúčania pre nastavenie hesiel

Používanie hesla je celosvetovo rozšíreným spôsobom autentifikácie užívateľov a počítačových systémov, resp. počítačových systémov voči sebe navzájom. Napriek tomu, že je ľahko pochopiteľné pre bežných užívateľov - postačuje „niečo" si pamätať - v skutočnosti ide o pomerne komplikovaný spôsob autentifikácie, pokiaľ má byť vykonaný bezpečným spôsobom.

Základné požiadavky na bezpečné heslo:

- **dĺžka** - v princípe platí, čím dlhšie heslo, tým lepšie. ENISA odporúča roku 2021 minimálnu dĺžku 9 znakov, ideálne 14 znakov,
- **zložitosť hesla** - aby bolo heslo odolné voči slovníkovým útokom, aj voči útokom hrubou silou, malo by byť dostatočne zložité, to znamená používať kombináciu veľkých/malých písmen, číslic a špeciálnych znakov a nepoužívať heslo, ktoré je variáciou slova zo slovníka (napr. Password1),
- **zapamätateľnosť** - pokiaľ heslo nechceme zapísať, je potrebné si ho zapamätať,
- zásada „**jeden systém jedno heslo**" nám pomôže ochrániť konto voči credentials stuffing - viď vyššie.

Zoraďte hesla podľa zložitosti a bezpečnosti[90]:

1. *jozef123*
2. *qwert*
3. *Brat1slava123*
4. *Hospod8rskyTr@kt0r*

Bezpečnosť hesla však, okrem jeho atribútov, ovplyvňuje aj jeho použitie:

- **utajenie hesla** - ak používateľ heslo prezradí, nie je viac bezpečné,

[90] Viete využiť tester hesiel napr. https://hesla.csirt.upjs.sk/

- **bezpečnosť hesla pri prenose po sieti** - pokiaľ je heslo prenášané v nešifrovanej podobe, môže ho útočník odpočúvajúci sieťovú komunikáciu odchytiť,
- **bezpečnosť hesla pri uložení** - pokiaľ heslo nie je bezpečne uložené (napr. na počítačovom systéme, ktorý overuje užívateľa) k heslu sa môže dostať nepovolaná osoba - pokiaľ je heslo uložené v nechránenej podobe na počítačovom systéme, môže sa k nemu dostať správca; pokiaľ je heslo zapísané na papieriku a nalepené na monitor, dostane sa k nemu každý náhodný okoloidúci.

Ako si teda vygenerovať a uchovať heslo bezpečne? Ideálne je, pokiaľ si heslo za človeka pamätá manažér hesiel (password manager). Manažér hesiel vie vygenerovať dostatočne dlhé a komplexné heslo, vie bezpečne heslo uložiť a vie ho aj postrážiť, či nie je heslo používané napr. na rôznych webových stránkach. Niektoré manažéry hesiel vedia zároveň heslá v šifrovanej podobe synchronizovať medzi rôznymi zariadeniami, alebo podporujú možnosti zdieľania hesla s rodinným príslušníkom (napr. na pozeranie seriálov cez rodinný Netflix účet).

V prípade, že je potrebné heslo si pamätať (napr. heslo do operačného systému, heslo na dešifrovanie pevného disku alebo hlavné heslo (master password) do manažéra hesiel), tak môžeme využiť asociatívny spôsob, akým funguje ľudský mozog, napr. nasledovne:

- vyberieme si ľahko zapamätateľné slovné spojenie alebo vetu,
- pokiaľ je heslo príliš dlhé, tak ho skrátime napr. zámenou čísloviek za číslice,
- doplníme špeciálnej znaky a veľké písmená.

 Príklad:

- vyberieme vetu z ľudovej piesne: „vo štvrtok s chlapcami do šenku”,
- zameníme číslice: „vo 4tok s chlapcami do šenku”,
- doplníme špeciálne znaky / veľké písmena: „vo 4tok s CHLAPc@mi do #enku”,

- výsledkom je silné heslo (28 znakov), ktoré nemá veľké písmeno na začiatku a špeciálny znak na konci (obvyklá chyba pri tvorbe hesla). Znak '#' je na anglickej klávesnici umiestnený rovnako ako písmeno 'š' a namiesto znaku 'a' použijeme znak @, ktorý nesie logickú hodnotu pôvodného znaku.

Vyskúšajte si vytvoriť silné heslo od akýchkoľvek hesiel, ktoré používate rôznymi spôsobmi. Odmerajte silu hesla napr. cez online službu https://hesla.csirt.upjs.sk/. Podarilo sa vám vygenerovať heslo, ktorého prelomenie zaberie viac než storočie?

Vyskúšajte ľubovoľný manažér hesiel alebo online generátor hesiel a vygenerujte heslo rovnakej dĺžky, ako ste vymysleli v prvom príklade. Aké skóre dosiahlo vygenerované heslo?

4.8. Multifaktorová autentizácia

V predchádzajúcej kapitole sme si povedali o tom, ako heslo používať a aké riziká sú spojené s používaním hesla. Preto je na mieste položiť si otázku: Nedá sa nájsť nejaký iný, lepší, resp. silnejší spôsob autentizácie? Odpoveďou je, že takéto spôsoby existujú a podľa spôsobu autentizácie sa delia na nasledujúce faktory:

Faktor	**Príklad**	**Riziká**
Niečo, čo mám.	kľúče od bytu, mobilný telefón, (hardvérový) token[91], občiansky preukaz,	strata autentizačného prvku

[91] Token nemusí byť nutne súčasťou hardvéru, ale môže ísť o jednoduchý zoznam jednorazových kódov (OTP) vytlačených na papieri. V prípade hardvérového tokenu môže mať tento viacero foriem napr.:

- USB zariadenie,
- BlueTooth zariadenie ako je prívesok, prsteň, náramok, alebo karta,
- zariadenie s RFID čipom (Radio Frequency IDentification, používa sa v obchode pri identifikácii tovaru),
- NFC (Near Field Communication, technológia používaná hlavne pri platobných a identifikačných kartách).

	platobná karta	
Niečo, čo viem.	PIN, heslo, heslová fráza	zabudnutie, zapísanie na papier Slabé heslo/PIN, ...
Niečo, čím som.	odtlačok prsta alebo dlane, tvárová biometria, biometria oka (dúhovka, sietnica), biometria hlasu, analýza DNA, charakteristika správania - miesto práce, správanie na počítači	napodobnenie napr. silikónovým prstom, fotografiou tváre a pod. nemožnosť zneplatnenia

Multifaktorová autentizácia (MFA) používa viacero **rôznych** faktorov na autentizáciu používateľa, čím znižuje riziko súvisiace s jedným faktorom. Je to vlastne proces, pri ktorom zvyšujeme pravdepodobnosť overenia správnej osoby za pomoci poskytnutia viacerých dôkazov, že to je naozaj ona.

Pri kombinácií faktorov je veľmi dôležité vyberať faktory, ktoré nie sú náchylné na rovnaký typ útoku. Pokiaľ sa musí užívateľ prihlásiť napríklad odtlačkom prsta a zadaním PIN-u, tak riziko, že si PIN napíše na papierik nalepený na monitor nie je úplne relevantné, pretože ďalším rozhodujúcim faktorom je použitie jedinečného odtlačku prsta. Podstatné je, že faktory v MFA sú rôzne - pokiaľ by naša autentizácia kombinovala heslo a PIN, tak lepenie papierika na monitor zafunguje pri hesle aj PIN-e a tento spôsob autentizácie nás neochráni pred rizikom nezodpovedného používateľa lepiaceho papieriky.

1. Praktické spôsoby MFA

Predstavme si ako vyzerajú niektoré reálne nasadenia autentizácie. Najznámejším pre nás je výber z bankomatu, pričom klient banky na výber potrebuje PIN (to, čo viem) a kartu (to, čo mám). V Saudskej Arábii sa zmenil spôsob výberu z bankomatu. Karta klientom zostala (niečo, čo mám), ale

vymenila sa autentizácia pomocou PIN za biometriu oka (niečo, čím som). Druhým príkladom je prihlásenie do internet bankingu. V tomto prípade sa použije meno a heslo (to, čo viem) a kód z overovacej aplikácie (to, čo mám), ktorá je aktivovaná pre klienta a generuje nezávislé kódy. Tretím príkladom je prihlásenie do služby mobil bankingu (aplikácia banky na mobilnom telefóne). V tomto prípade sa používa aplikácia, väčšinou s kontrolou zariadenia, či je toto zariadene stále to isté a nepoškodené a dá sa mu veriť (to, čo mám). Pri štarte si aplikácia zistí, či je v rovnakom stave a či je to to isté zariadenie, ako bolo pri prvom overení (to, čo mám). Následne je použitý na prihlásenie PIN alebo heslo do aplikácie (niečo, čo viem). Niektoré aplikácie podporujú dokonca overenie pomocou biometrie (niečo, čím som).

V praxi sa kombinujú viaceré možnosti, resp. faktory autentizácie do MFA na základe rôznych požiadaviek ako napr.:

- **bezpečnosť** - aké riziká faktor rieši a aké riziká otvára,
- **akceptovateľnosť** - používatelia môžu niektoré typy faktorov odmietať z obáv o svoje zdravie (napr. sken sietnice) alebo o svoje súkromie (analýza DNA),
- **použiteľnosť** - niektoré typy autentizácie nie je možné nasadiť v podmienkach, kedy sa očakáva rýchla autentizácia, napr. vstup lekárov urgentného príjmu do priestorov nemocnice nemôže brzdiť zadávanie PIN-u na klávesnici, biometriu tváre nemôžeme použiť pri autentifikácii počas telefonického hovoru atď.

Na trhu sa vytvoril určitý trend, kedy sa od špecifických zariadení, ktoré boli rozdávané pre potreby autentifikácie jednotlivými firmami, trh prikláňa k vyťažovaniu funkcií mobilného telefónu. Dôvodom je, že pre bežného človeka je obmedzujúce mať pri sebe, resp. nosiť viac zariadení. Príkladom môže byť prechod od výberu z bankomatu, ktorý bol vykonávaný kartou, do prostredia bankových aplikácii v mobilných telefónoch. To znamená, že na výber z bankomatov v niektorých bankách vám stačí mobil. Zároveň sa vytvárajú v mobiloch virtuálne kartové peňaženky. Postupne sa platobná karta ako taká stáva stále menej a menej potrebná vo svojom fyzickom prevedení a prechádza do virtuálneho prostredia. Napriek popísanému trendu stále existujú snahy hľadania nových nástrojov na overovanie človeka jednoduchými spôsobmi, ktoré sa snažia zaujať. Vyzerajú ako šperky: prstene, náramky, prívesky (niečo, čo mám), iné

skúšajú overovať funkčnosť podkožných čipov (niečo, čo mám, aj čo som). Vytvárajú sa koncepty na kontrolu biometrických údajov, ako je biometria hlasu a biometria tváre. V tomto prípade si však treba dávať pozor pri implementácii, pretože biometrické overovanie je overovanie na základe podobnosti a na základe matematického modelu. Človek idúci po ulici, priradí meno a identitu oproti idúceho človeka na základe jediného pohľadu a na základe svojich skúseností a znalostí. Človek sa nebojí povedať: toto je náš sused. Počítač priradí identitu na základe pravdepodobnosti podobnosti údajov, ktoré má zozbierané a spracované a tých, čo práve odfotil/načítal. Výsledok je: toto je náš sused na 98% s pravdepodobnosťou chyby 2%. Z tohto dôvodu ste si možno uvedomili, že určité aplikácie používajúce biometriu (niečo, čím som) pre špecifické, dôležité veci, vyžadujú občas dodatočné potvrdenie PIN-om (niečo, čo vieš).

Existujú aplikácie, ktoré spravujú veľmi dôležité informácie, pri ktorých sa vyžaduje jednoznačná identifikácia a v rámci MFA používajú existenciu overenej aplikácie (niečo, čo mám), a zároveň biometrické overovanie (niečo, čím som, s určitým percentom pravdepodobnosti). Aplikácie so starším návrhom architektúry stále využívajú overenie cez nezabezpečený SMS kanál, pričom sú niekoľko rokov na čiernom trhu dostupné vírusy a návody pre hekerov, ako v mobilných zariadeniach získavať SMS kód a ako s ním pracovať[92]. V oboch prípadoch je vhodné zamyslieť sa nad výslednou bezpečnosťou celého systému, spolu s celkovým zladením aplikácii s nariadeniami a zákonnými požiadavkami. V tomto prípade je otázne, či slovo *viacfaktorová* plnohodnotne vystihuje požadovanú autentizáciu.

- *Vyhľadajte na internete popis „SIM swap" útoku a vysvetlite jeho dopad na MFA s využitím hesla a SMS one-time tokenu.*
- *Vymyslite vhodnú MFA pre nasledovnú situáciu: overenie zákazníka banky prostredníctvom telefónu. Popíšte:*
  1) Aké riziká vami navrhovaná MFA rieši a aké riziká prináša?
  2) Ako vnímate akceptáciu navrhovanej MFA zo strany používateľov?

[92] https://zive.aktuality.sk/clanok/145167/komplexny-virus-ohrozuje-zariadenia-s-androidom-kradne-bankove-udaje-spehuje-aj-sifruje/

2. Útoky na MFA

Pred tým, než sa dostaneme k útokom na MFA, je potrebné si objasniť, pred čím MFA nechráni. MFA nedokáže chrániť, pokiaľ je zariadenie kompromitované škodlivým softvérom - škodlivý softvér môže byť prispôsobený napr. internet bankingu tak, aby sa po prihlásení používateľovi síce zobrazovali v prehliadači nejaké informácie, ale v skutočnosti sa realizovali úplne iné transakcie, pričom sa využíva validná session, ktorú používateľ získal po prihlásení sa prostredníctvom MFA.

V tabuľke v predchádzajúcej kapitole sme si uviedli riziká viažuce sa ku konkrétnemu faktoru. Poďme sa pozrieť bližšie na jednotlivé faktory a útoky zamerané na prekonanie konkrétneho faktoru.

1. Niečo, čo mám

Útoky na autentizačný prvok sú zamerané buď na odcudzenie autentizačného prvku, alebo na vytvorenie kópie autentizačného prvku, resp. jeho sfalšovanie. Odcudzenie závisí od fyzickej ochrany autentizačného prvku. Pre útočníka je však zaujímavejšie vytvoriť kópiu autentizačného prvku a mať možnosť prihlasovať sa v mene používateľa bez vyvolania podozrenia súvisiaceho so stratou alebo krádežou prvku. Niektoré autentizačné prvky sú navrhnuté tak, aby sa dali falšovať len veľmi ťažko - napr. platobná karta s čipom. Pri iných je možné falšovanie zrealizovať najmä po fyzickom prístupe k prvku.

Vyhľadajte na youtube, či je možné vytvoriť duplikát kľúča z obrázku. Aký kľúč by ste odporúčali použiť, aby nebolo možné duplikát vytvoriť?

Vyhľadajte na youtube, či je možné vytvoriť duplikát platobnej karty. Čo je potrebné pre úspešný útok? Je tento typ útoku aplikovateľný pre:

- *platobné karty s magnetickým prúžkom (magnetic stripe)?*
- *platobné karty s čipom?*

2. Niečo, čo viem

Útoky na tento faktor sme si popísali v kapitole o heslách.

3. Niečo, čím som

Najlepšie si vieme predstaviť tento faktor na pozadí porovnania a kontroly biometrických prvkov. Biometrické systémy sú systémy založené na porovnávaní voči pripravenému originálu. Tento originál, resp. informácie o ňom sa pozbierali niekedy v minulosti, keď bola zabezpečená istota, že sú pozbierané vzorky od originálnej, identifikovanej a autentifikovanej osoby. Následne sa spustí matematický model, ktorý porovná nazbieranú vzorku voči práve zozbieranému originálu a vyhlási mieru zhody. Keďže ide o matematický model, porovnanie nemusí prebehnúť vždy na úrovni 100%, ale len do určitej miery zhody. Z uvedeného vyplýva, že niekedy (veľmi zriedkavo) systém môže overiť cudziu osobu a oveľa častejšie nemusí overiť správneho vlastníka. Tieto miery zhody sa porovnávajú a permanentne kontrolujú. Poznáme 2 základné miery *False acceptance ratio* (FAR) - miera v percentách, keď biometrický systém overil neautorizované osoby, pričom cieľom je udržať toto číslo blízko nule. *False Rejection Rate* (FRR) - percentuálna miera, keď správne osoby nie sú autorizované a sú odmietnuté, pričom cieľom je udržať toto číslo čo najnižšie, na úrovni jednotiek percent.

Útoky na rôzne biometrické faktory sa zameriavajú na čo najpresnejšie napodobnenie biometrických prvkov konkrétneho človeka tak, aby to bolo postačujúce pre zmätenie senzora alebo algoritmu, ktorý vyhodnocuje biometrické prvky. Zadefinujme si najčastejšie používané formy biometrií v bežnom živote a predstavme si útoky na ne.

Odtlačok prsta je jedným z najviac preskúmaných biometrických prvkov z pohľadu útokov. Odtlačok prsta sa považuje za najjednoduchšiu formu biometrie, lebo je statický. Najstaršie generácie senzorov sa dali ľahko oklamať obrázkom prsta, preto neskôr začali senzory snímať aj ďalšie charakteristiky (napr. teplota, nepatrný pohyb). Z tohto dôvodu sú súčasné pokusy o oklamanie senzorov zamerané na modelovanie odtlačku (prsta), napr. z polyméru, ktorý je potom možné prichytiť alebo navliecť na prst.

Vyhľadajte na youtube, či je možné oklamať senzor na snímanie odtlačku prsta na moderných mobilných telefónoch. Pre aké modely telefónov sa vám podarilo nájsť úspešný útok?

Hlasová biometria je tiež nielen obľúbenou formou biometrie, ale aj obeťou útokov. Pri hlase pracujeme s dynamickou formou biometrie. Podvodníci sa postupne snažia prelomiť hlasovú biometriu pomocou nahrávok alebo syntetizovaním hlasu. Najnovší spôsob útoku na hlasovú biometriu prináša technológia *deep fake*[93].

- *Vyhľadajte na youtube, pokusy o oklamanie hlasovej biometrie pomocou syntetizátora.*
- *Na akom princípe pracuje deep fake útok na biometriu? Pripravte prezentáciu a vysvetlite.*

Tvárová biometria je podobná odtlačku prsta z pohľadu útokov - útoky sa zameriavajú na oklamanie senzorov cez obrázky tváre, masky alebo priamo 3D masky vytlačené pre konkrétne „hlavy" (konkrétnych útočníkov).

- *Vyhľadajte na youtube, či je možné oklamať Apple FaceID biometriu. Pre aké modely telefónov sa vám podarilo nájsť úspešný útok?*

Biometrický podpis, je forma podpisu, pri ktorej sa analyzujú rôzne biometrické charakteristiky ako prítlak, dĺžka podpisu, rýchlosť písania, zrýchlenie. Po podpise prebieha následne verifikácia podpisu. Útoky na biometrický podpis nie sú časté, a ak sa vyskytnú, ide väčšinou o proces napodobovania útočníkom, čo je veľmi zložitý úkon a len veľmi zriedkavo môže byť úspešný. Druhou možnosťou je pokúsiť sa o útok na samotné riešenie. Je veľmi dôležité uvedomiť si, že používateľ sa môže vedome podpísať nesprávne, a preto ho systém neoverí, napríklad zmení písané (spojité) písmo podpisu za tlačené alebo napíše iný obsah, napríklad namiesto Janko Hraško, napíše Jozef Mak.

[93] Pozri https://www.youtube.com/watch?v=AmUC4m6w1wo

4.9. Ochrana a starostlivosť o počítač

V tejto kapitole sa vrátime k predchádzajúcim častiam o ochrane počítača a uvedieme si niekoľko odporúčaní na ochranu a starostlivosť o počítač. Zoznam odporúčaní, samozrejme, nie je úplný[94] a vždy je možné aplikovať dodatočné opatrenia nad rámec týchto odporúčaní podľa toho, ako závažné sú identifikované riziká.

1. Ochrana voči škodlivému softvéru pomocou antivírusu

Základným bezpečnostným opatrením je mať **nainštalovaný antivírusový softvér, ktorý stále beží a je priebežne aktualizovaný**.

Pozrime sa na jednotlivé odporúčania pri správe antivírusu, aj s vysvetlením dopadu, ak sa nebudú odporúčania dodržiavať:

- **mať nainštalovaný antivírusový softvér** - pokiaľ antivírus nie je nainštalovaný alebo je vypnutý, tak zariadenie nie je chránené,
- **nevypínať antivírus, ani jeho časti** - častokrát sa malvér tvári ako inštalátor (napr. hry) alebo kodek na prehliadanie videa, avšak počas „inštalácie" vyžaduje vypnutie antívírusu alebo jeho časti (napr. firewall, HIPS), aby sa mohla nainštalovať škodlivá funkcionalita,
- **automaticky aktualizovať databázu signatúr** - aktualizácia databázy hrozieb je spravidla nastavená pri inštalácii antivírusu, pričom sa väčšinou databáza hrozieb aktualizuje opakovane minimálne raz denne,
- **aktualizovať antivírusový softvér** - niektoré časti antivírusového softvéru je občas potrebné aktualizovať ručne, na čo antivírus užívateľa (alebo správcu vo firemnom prostredí) upozorní. Tieto aktualizácie netreba odkladať, pretože spravidla obsahujú nové spôsoby detekcie malvéru.

[94]Zoznam odporúčaní je relevantný pre rok 2021. Vývoj v informačnej bezpečnosti je však veľmi rýchly a odporúčania nemusia byť dostatočné v budúcnosti.

- **neblokovať antivírus inými bezpečnostnými prvkami** - antivírus na zariadení už dnes obsahuje aj ďalšiu bezpečnostnú funkcionalitu, snaží sa zastávať postavenie komplexného bezpečnostného nástroja pre počítač. Stále však existuje možnosť použitia ďalších bezpečnostných nástrojov, ktoré sa inštalujú samostatne napr. samostatný personálny firewall. Musíme si pamätať, že dodatočné bezpečnostné nástroje sú samostatné a treba ich veľmi opatrne nastaviť, aby neblokovali ostatné bezpečnostné prvky. Napr. firewall môže zablokovať komunikáciu antivírusu s cloudovou databázou hrozieb alebo aktualizačnými servermi a prestanú sa tak sťahovať aktualizácie alebo je ohrozená niektorá z dodatočných funkcionalít. Podobná situácia sa dá dosiahnuť na domácom wifi routri. Je potrebné skontrolovať, či antivírus vie komunikovať so službami, ktoré potrebuje na svoje fungovanie (beh) - v prípade problému na to antivírus užívateľa (alebo správcu vo firemnom prostredí) upozorní.
- **nebrániť antivíru v kontrole** - antivírus sa automaticky pri inštalácii nastaví tak, aby pokrýval štandardné spôsoby, akými sa malvér vie dostať do zariadenia - napr. prenosné médiá, web, príloha emailu. Pamätajme si, že tieto nastavenia nemáme meniť, aby antivírus vedel fungovať korektne.

Moderné antivírusy vedia okrem škodlivého softvéru tiež detekovať (odhaliť) pokusy o zneužívanie zraniteľnosti (exploitáciu), prípadne môžu byť vo firemnom prostredí doplnené technológiou Endpoint Detection & Response (EDR) na logovanie a vyhodnocovanie podozrivých aktivít v systéme.

Vyhľadajte na počítači nainštalovaný antivírusový softvér a zodpovedajte nasledovné otázky:

- *O akú verziu antivírusového softvéru ide? Je táto verzia aktuálna? Ak nie, je táto verzia podporovaná výrobcom?*
- *Aká je verzia antivírusovej databázy? Je táto verzia aktuálna?*
- *Aktualizuje sa antivírusové databáza automaticky?*
- *Obsahuje antivírus aj ďalšie bezpečnostné moduly (firewall, HIPS, …)? Ak áno aké?*

Okrem nastavenia antivírusu sú dôležité aj ďalšie aspekty ochrany zariadenia pred malvérom:

- **používateľské povedomie** - používateľ je neoddeliteľnou súčasťou bezpečnosti, a to platí aj pri prevencii infekcie malvérom. Dobré používateľské povedomie vie zabrániť napadnutiu malvérom, ktorá využíva spôsoby sociálneho inžinierstva, aby užívateľ nainštaloval malvérovú aplikáciu, doinštaloval si plugin do prehliadača, vypol antivírus alebo iný bezpečnostný softvér, otvoril infikovaný dokument alebo klikol na phishingovú linku.
- aplikovanie **záplat operačného systému a aplikácií** - v prípade, že malvér využíva bezpečnostnú zraniteľnosť v operačnom systéme alebo aplikácii, je možné infekcii malvérom zabrániť tým, že operačný systém aj aplikácie sú udržiavané aktualizáciami. Viac si povieme v ďalšej kapitole.

2. Ochrana aplikovaním záplat

Pre akékoľvek informačné prostredie platia nasledovné bezpečnostné odporúčania:

- **vedieť o nainštalovanom softvére** - správca informačného systému musí mať prehľad o tom, aké počítačové programy sú na informačnom systéme nainštalované.
- **vedieť o zraniteľnostiach v systéme a programoch** - správca informačného systému musí sledovať výskyt bezpečnostných zraniteľností a aplikovať záplaty. Na tento účel slúžia dedikované mailing listy, stránky výrobcu, resp. špecializované nástroje na zistenie zraniteľností (tzv. vulnerability scanner).
- **pravidelne aplikovať záplaty** - pokiaľ je dostupná záplata, tak táto musí byť aplikovaná v čo najkratšom čase, ideálne bezodkladne, spravidla do 14 dní po vydaní záplaty, inak hrozí riziko jej analýzy útočníkom a následne zneužitie zraniteľnosti.
- **aplikovať záplaty automaticky** - bezpečnostné záplaty operačného systému by mali byť aplikované čo najviac automaticky s vynútením reštartu počítača.

Predchádzajúce odporúčania platia aj pre domácich používateľov a zariadenia v domácom prostredí, avšak tu spravidla existuje obmedzenejšia ponuka nástrojov, ktoré by uľahčili samotný proces aplikovania záplat.

Domácim používateľom sa preto odporúča:

- **odinštalovať softvér, ktorý nie je potrebný** - výrobcovia softvéru spravidla inštalujú nevyužívané (až škodlivé) aplikácie zvané „bloatware",
- nastaviť automatické aktualizácie operačného systému,
- použiť **bezpečnostný softvér, ktorý inštaluje záplaty pre aplikácie**. Výrobcovia bezpečnostných riešení ponúkajú základný balík na riadenie inštalácie záplat aj pre domácich používateľov.

Nájdite na počítači s OS Windows program Windows update. Aké záplaty sú k dispozícii pre operačný systém? Sú záplaty operačného systému aplikované automaticky?

Vyhľadajte na internete riešenia pre použitie/uplatnenie aplikačných záplat. Odprezentujte spolužiakom, riešenie podľa vášho výberu. Čo sú podľa vás výhody a nevýhody riešenia?

Pripravte prezentáciu, v ktorej vysvetlíte, čo je „bloatware".

3. Ochrana pri prehliadaní webu

Ako sa chrániť voči podvodným a malvérovým stránkam:

1) **Používajte automaticky aktualizovaný antivírus!** Základnou vrstvou ochrany proti podvodným stránkam a stránkam šíriacim malvér je antivírus, ktorý vie zastaviť už samotné pripojenie na zlý webový server, pokiaľ túto hrozbu pozná.
2) **Aktualizujte operačný systém a prehliadač**! Kvôli zníženiu rizika automatickej inštalácie malvéru je potrebné neustále aktualizovať operačný systém, aj programy - hlavne webový prehliadač a všetko, čo ním súvisí.
3) **Vzdelávajte sa v oblasti informačnej bezpečnosti**! (v tomto vám môže pomôcť aj naša učebnica)

Na ochranu pred uvedenými útokmi je možné využiť viaceré bezpečnostné opatrenia:

1) **samotný prehliadač** - prehliadače majú v sebe zabudované rôzne typy ochrany, ako napríklad detekciu škodlivých stránok, oddelenie stránok v jednotlivých záložkách.
2) **doplnky prehliadača** - vieme využiť špecializované doplnky počítača, ktoré zabránia zobrazovaniu reklám (aj tých so škodlivým kódom) a spúšťaniu nepovoleného JavaScript kódu.
3) **antivírus** - opäť detekcia tzv. zlých domén a URL, detekcia škodlivého JavaScriptu alebo iných súborov (flash, ActiveX), ktoré sa tieto snažia stiahnuť.

Zistite, či pre vami používaný webový prehliadač sú k dispozícii doplnky (plugin, addon). Sú tieto doplnky ponúkané samotným webovým prehliadačom alebo ich inštalujete ako samostatné balíky?

Vyhľadajte medzi doplnkami také, ktoré sa zameriavajú na bezpečnosť alebo ochranu súkromia a odprezentujte vami zvolený doplnok spolužiakom. V čom spočívajú prínosy doplnku?

Vyhľadajte na internete, či viete overiť škodlivosť webovej stránky bez toho, aby ste ju zadali do webového prehliadača. Overte škodlivosť nasledovnej webovej stránky: malware.wicar.org/data/js_crypto_miner.html

4. Ochrana voči spamu a phishingu

Základnou ochranou voči spamu a phishingu je používanie antispamovej a antivírovej ochrany. Tieto ochrany môžu (a mali by) byť nasadené na serveri aj na koncovej stanici alebo zariadení. Samozrejme platí, že žiadna ochrana nie je stopercentná a môžu sa objavovať falošne pozitívne aj falošne negatívne detekcie. To znamená, že pokiaľ používateľ očakáva validný (platný, oprávnený) email, ktorý neprichádza, je dobré skontrolovať aj priečinky, ktoré obsahujú spamové správy (napr. Junk E-mail).

Pokiaľ antispamový a antivírový filter zlyhajú, nastupuje druhá vrstva ochrany, a tou je povedomie používateľa, ktorý sa musí rozhodnúť, či je emailová správa legitímna alebo nie. Preto je

potrebné vedieť rozpoznávať podvodné emaily, hoaxy a phishing, ako sme si ukázali na príkladoch vyššie.

Vyhľadajte na počítači antivírusový softvér a zistite, či vykonáva aj antispam ochranu. Do akého priečinka presúva zistené spamové emaily?

5. Súkromie

V tejto časti učebnice si povieme viac o odporúčaniach spojených s používaním webového prehliadača. Na surfovanie na internete je možné využiť buď špecifický webový prehliadač zameraný na ochranu súkromia, alebo prostredníctvom doplnkov upraviť štandardný webový prehliadač.

Použitím špecifického prehliadača / doplnkov sa budeme snažiť dosiahnuť nasledovné odporúčania:

1) **Šifrujte všetku komunikáciu!** Toto odporúčanie je možné rozdeliť do dvoch častí:
    a) **vždy používajte protokol HTTPS** - webové prehliadače môžu pri zadaní webovej stránky povoliť prvý prístup nešifrovaným protokolom HTTP a až následne byť presmerované na HTTPS verziu webovej stránky. Toto správanie dáva útočníkovi na sieti priestor uskutočniť man in the middle útok.
    b) **používajte VPN** alebo anonymizačnú sieť - VPN chráni aj komunikáciu mimo protokolu HTTP(s), napr. DNS. Potrebné je, samozrejme, vybrať poskytovateľa VPN služby, ktorý neloguje komunikáciu a nepredáva naše (meta)dáta ďalej.
2) **Blokujte reklamu!** Zobrazovanie reklamy spomaľuje prehliadanie webu a môže zavliecť škodlivý softvér prostredníctvom malwaretizingu.
3) **Blokujte reklamné cookies**! Reklamné cookies slúžia výhradne na sledovanie používateľov a nemá zmysel ich povoliť.
4) **Blokujte trackery**, ktoré sa snažia identifikovať prehliadač konkrétneho používateľa!
5) Využívajte **vyhľadávače, ktoré chránia súkromie!** Takýmto vyhľadávačom je napríklad DuckDuckGo. Pokiaľ sa neviete vyhnúť štandardným prehliadačom ako Google.com alebo

Bing, dopad na súkromie viete minimalizovať vypnutím personifikácie reklám v nastaveniach vyhľadávača. Vyhľadávač si viete nastaviť aj vo webovom prehliadači.

Zo špecifických webových prehliadačov spomeňme aspoň:

1) **Tor Browser Bundle** - ide o upravenú verziu webového prehliadača Firefox, v ktorej je natívne (prirodzene) integrované pripojenie k anonymizačnej sieti Tor. Ostatné prispôsobenia prostredníctvom doplnkov sú rovnaké ako v prípade použitia Firefox[95].
2) **Brave browser** - tento prehliadač vychádza z Chrome, avšak je prispôsobený na blokovanie reklamy a trackerov na internete.

Vyhľadajte na internete, ktoré zo všeobecných odporúčaní 1-5 vieme splniť použitím prehliadača Tor Browser bundle a ktoré použitím prehliadača Brave.

Predstavme si niektoré užitočné doplnky prehliadačov Chrome a Firefox, ktoré nám môžu pomôcť zlepšiť súkromie na internete.

Doplnok	**Výhody**	**Nevýhody**
HTTPS everywhere	Vynúti ako prvý protokol HTTPS.	Spomaľuje načítavania HTTP stránok.
VPN doplnky	Zabalí komunikáciu prehliadača do VPN tunela.	Spomaľuje surfovania. Niektoré stránky sa odmietnu načítať cez VPN, príp. sa načítajú v inej jazykovej mutácii.
FoxyProxy	Poskytuje možnosť prepínania sa medzi rôznymi HTTP a	Spomaľuje surfovania. Niektoré stránky sa odmietnu načítať cez proxy

[95] Pokiaľ navyše chcete surfovať aj po .onion doménach, odporúčame vypnúť JavaScript napr. prostredníctvom doplnku NoScript.

	SOCKS proxies[96].	server, príp. sa načítajú v inej jazykovej mutácii.
AdBlock+, uBlock Origin	Umožňuje blokovanie reklamy s možnosťou whitelistu webových stránok, kde sa má reklama zobrazovať.	Občasné problémy s JavaScriptom. Neštandardné správanie niektorých webov[97]
Terms of service didn't read	Doplnok zobrazí „známku" s hodnotením podmienok poskytovania webovej stránky s ohľadom na súkromie.	žiadne
Privacy Badger[98], Ghostery	Umožňuje blokovanie reklamných trackerov a cookies	žiadne
Self-destructing cookies, Cookie autodelete	Umožňuje automatické vymazávanie všetkých (vrátane analytických) cookies po zavretí záložky.	Spôsobí zároveň aj vymazanie session cookies - ak si zavrieme záložku, musíme sa prihlásiť znovu.
NoScript, resp. ScriptNo	Umožňuje vypnutie JavaScriptu a jeho zapínanie len pre špecifické domény.	Spôsobuje obmedzenie funkcionality niektorých stránok.

[96] Štandardne má webový prehliadač možnosť konfigurovať len jedno proxy.
[97] Pokiaľ vypneme reklamu všade, oberáme niektoré webové portály o možnosť zárobku. Spravidla takto fungujú webové stránky o IT technike.
[98] Privacy Badger je poskytovaný neziskovou organizáciou EFF, ktorá sa zaoberá okrem iného aj ochranou súkromia na internete.

- *Vyhľadajte v prehliadačoch Chrome a Firefox, ktoré z uvedených doplnkov sú dostupné v rámci webového prehliadača.*

- *Nájdite v nastaveniach prehliadača, ktorý vyhľadávací engine je použitý štandardne na vyhľadávanie. Ktorý z ponúkaných engine by ste odporúčali kamarátovi na zlepšenie súkromia?*

Ochrana mobilného telefónu

Mobilné zariadenia postupne prenikli do našich životov a stali sa tak našou neodmysliteľnou každodennou súčasťou. Smartfón nám umožňuje komunikáciu s ostatnými ľuďmi, prináša nám zábavu, dokonca zamestnávateľ umožňuje mnohým ľuďom pracovať pre firmu pomocou smartfónu. Pomocou mobilných aplikácii sa môžeme pripojiť na sociálne siete, do internet bankingu, internetového obchodu, ale aj na pracovný email, v ktorom sa môžu nachádzať citlivé údaje. Najnovšie typy smartfónov sú vyrovnanou konkurenciou pracovným notebookom, čo sa týka výpočtovej sily. Málo ľudí si však uvedomuje, že používaním smartfónu môžu nielen veľa získať, ale aj ohrozovať svoju bezpečnosť. S možnosťami teda prichádzajú aj hrozby. Mobilné zariadenia sú rovnako zraniteľné ako IT technika a tiež ich dokážu napádať vírusy. Pre mobilné zariadenia sú vypracované špeciálne typy útokov, ktoré nám môžu znepríjemniť život, dokonca poškodiť alebo ukradnúť aj osobné údaje

Kapitola má názov „Ochrana mobilného telefónu”, ale my sa budeme zaoberať mobilnými zariadeniami ako takými. Nechceme striktne špecifikovať, o aké zariadenia ide, či ide o mobilné telefóny, tablety alebo iné typy zariadení. Z toho dôvodu predpokladáme, že pre všetky mobilné zariadenia v zásade platia pravidlá, že ich systémy

sú uzavreté a bezpečnosť prostredia je kontrolovaná. My vám ukážeme iba všeobecný postup, potom už bude len na vás, aby ste sa pokúsili naučený postup aplikovať na konkrétne mobilné zariadenie (napr. váš mobilný telefón) a zvýšili tak mieru svojej bezpečnosti.

5.1. Aké údaje sú zaujímavé pre útočníkov?

Primárna úloha mobilného zariadenia - telefonovanie a posielanie textových správ - postupne prechádza do úzadia. V súčasnosti má telefón aj ďalšie funkcie. Nepatrí sem iba ukazovateľ času a kalendár, ale aj určenie polohy (GPS), preto je možné inštalovať na mobilný telefón rôzne typy navigácií. Nevýhodou mobilného zariadenia je výdrž baterky, ktorá sa rapídne znižuje používaním výkonných aplikácií a využívaním antény.

Ak chceme ochrániť mobilné zariadenie, mali by sme vedieť, čo sa v zariadení nachádza a čo je pre útočníkov cenné. Rozdeľme si cenné veci v mobile na dve kategórie: priamy prístup, resp. zisk a nepriamy. V prvom prípade stačí útočníkovi prístup do telefónu, v druhom prípade musí urobiť určitú prácu na získanie prístupu k dátam a potom z nich vyťažiť informácie. Niektoré aplikácie si však ukladajú svoje dáta v cloude - k ochrane údajov v cloude sa ešte dostaneme.

Priamy zisk zahŕňa nasledujúce informácie:

- adresár kontaktov
- fotky a videá
- história SMS
- história chatov
- aktivity zapísané v aplikácií kalendár
- poznámky
- zoznam stránok z bookmarks a favorities

Nepriamy zisk predstavuje:

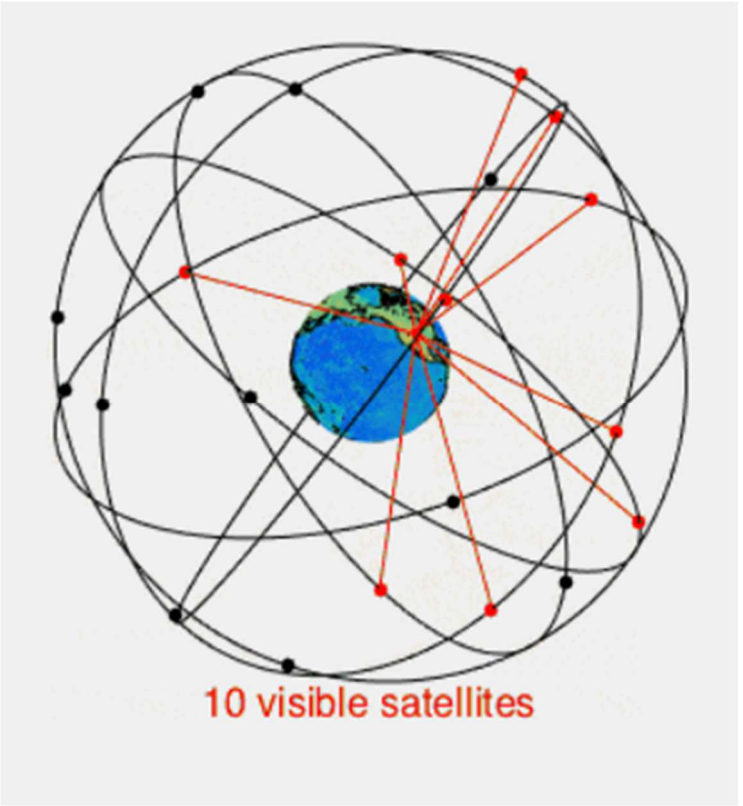
- história hovorov
- história prehľadávaní v prehliadači
- história aktivít v aplikáciách (ak to aplikácia podporuje)
- metadáta fotografií
- GPS cache (uloženie lokácie posledných miest, kde sa zariadenie nachádzalo)
- aplikácie so zoznamom hesiel

- história a obsah z aplikácií (emailový klient, sociálne médiá, bankové aplikácie, vizitkár,...

Niekoľkokrát sme sa dotkli možnosti sledovania človeka cez mobilné zariadenie. Na sledovanie potrebujeme nielen prístup k mobilnému zariadeniu, ale napríklad aj pripravený malvér na sledovanie. Podrobnejšie si túto skutočnosť opíšeme v časti špehovanie. Jednou z nevyhnutných úloh je vedieť, kde sa práve nachádza mobilné zariadenie. Mobilný operátor vie približnú polohu mobilného telefónu podľa bunky mobilnej siete, do ktorej je telefón pripojený. Na určenie presnej polohy sa používa GPS, pričom telefón si pamätá veľa predchádzajúcich pozícií telefónu.

GPS (Global positioning system) - pasívny družicový dĺžkomerný navigačný systém. Pôvodne bol vyvíjaný pre vojenské účely s cieľom presnej navigácie. Zameriava sa na presné určenie polohy, rýchlosti a času, to znamená, že sa zameriava na presnú polohu v trojrozmernom priestore. Systém je založený na troch zložkách: družice, riadiace centrum a používateľské nástroje. V kozme sa nachádza 21 aktívnych družíc, ktoré letia podľa presne definovanej dráhy. Na zemi v USA sa nachádza Hlavná riadiaca stanica (Master Control station), ktorá riadi a hlavne synchronizuje družice (dráhu a čas). Používateľský nástroj následne riadi príjem, vypočítava presné miesto na zemi na základe prijímania signálu z minimálne 4 družíc a prípadné nepresnosti koriguje znalosťou terénu, po ktorom sa pohybuje (napr. auto nemôže vybočiť z cesty).

Pripravte prezentáciu na tému: kde a akým spôsobom sa zapína a vypína GPS lokalizácia vo vašom mobilnom zariadení a ako sa riadi prístup jednotlivých aplikácií ku GPS údajom.



Ukážka orbitálnych dráh satelitov a viditeľnosti jednotlivých satelitov pre špecifické miesto (červené čiary) [99]

Ak výpočet GPS pracuje s guľovými plochami, potom výsledkom prieniku guľových plôch môže byť viacero možných riešení. Vysvetlite, akým spôsobom GPS systém vie spracovať viacero možných riešení a prečo vie vybrať vždy to správne.

Vysvetlite problém zameriavania GPS signálu používateľským zameriavaním, pomocou guľových plôch, ako sa určuje vzdialenosť každej družice a prečo je to možné všetko spočítať?

[99] Global Positioning System; [online] [cit. 05.07.2021] Dostupné online> https://en.wikipedia.org/wiki/Global_Positioning_System

Mobilné zariadenie nie je zariadenie určené len na zábavu, komunikáciu a prácu. Smartfón sa stal zariadením, ktoré umožňuje vytvárať, upravovať a ukladať multimediálne súbory. Obrovské množstvo ľudí používa smartfón ako úložisko svojich rodinných fotografií. Smartfón však nie je nezničiteľný, a preto sa musíme naučiť čo robiť, aby prípadné zničenie alebo poškodenie smartfónu neznamenalo aj definitívnu stratu súborov, ktoré sú v ňom uložené.

Nájdite aspoň 6 typov operačných systémov pre mobilné zariadenia, vysvetlite ich históriu a zobrazte logá jednotlivých systémov.

5.2. Infiltrácie

V predchádzajúcej kapitole *Ochrana počítača* sme sa podrobne zaoberali rôznymi typmi problémov. V tejto kapitole si predstavíme rozličné typy útokov na mobilné zariadenie, ako aj spôsoby ochrany mobilného telefónu a tiež sa dotkneme témy cloudov. Vzhľadom na množstvo predaných telefónov sa budeme venovať hlavne operačným systémom iOS a Android. Existujú však aj iné, viac-menej okrajové, operačné systémy ako Java-Me, Windows Mobile, Symbian alebo BlackBerry, ale týmto sa venovať nebudeme. Vzhľadom na blízku podobnosť medzi mobilným zariadením a počítačom si niektoré útoky prejdeme ešte raz z pohľadu mobilného zariadenia, no zároveň časť útokov, ktorým sa budeme venovať, bude úplne nová. Priestor útokov na mobilné zariadenia sa každým dňom zväčšuje, preto ak si osvojíte vedomosti z tejto knihy, miera rizika, že aj nové typy útokov môžu znamenať pre vaše mobilné zariadenie reálnu hrozbu, sa zníži.

Predstavme si okruhy hrozieb, ktoré sú nebezpečné a na ktoré musíme myslieť pri práci s mobilným zariadením:

- **heslom nechránené zariadenia -** ľudia si často nezamykajú svoje zariadenia veriac, že si ho vedia fyzicky v ktorejkoľvek chvíli ochrániť. V prípade odcudzenia alebo straty zariadenia ide o obrovské zjednodušenie pre zlodeja, jednoduchý spôsob ako sa dostať ku veľkej časti dát obete. Do tejto kategórie patria aj ľahko predpovedateľné heslá, pretože útočník, ktorý má záujem o váš mobil, si určite zistí verejne dostupné informácie o vás a vašich blízkych. Pridať k tomuto menu

napríklad čísla 123 naozaj nie je prekážkou ani pre začínajúceho hekera.

- **zlomyseľné (*malicious*) aplikácie** - aplikácie, ktoré si vyžiadajú viac prístupov, ako by mali potrebovať a následne dáta z týchto prístupov zneužívajú. Napríklad: ak offline kartová hra vyžaduje prístup k polohe mobilu a ku kontaktom, tak dôvod na pridelenie takéhoto typu prístupov nie je opodstatnený.
- **verejné WiFi siete** - platí jednoduché pravidlo: *Predpokladajte, že sú vždy nebezpečné*. V súčasnosti je prirodzené poskytovať pripojenie v rámci miest, letísk, autobusových a vlakových staníc, či hotelov. Nikdy však neviete, ak sa do nich pripojíte, či ide o oficiálne siete zriadené prevádzkovateľom alebo hekerom. Keď sa na sieť pripojíte, heker má čas analyzovať a nahrávať vašu komunikáciu a zároveň testovať vaše zariadenie na zraniteľnosti. Problémom pre užívateľa je najmä analyzovanie a nahrávanie komunikácie, pretože časť aplikácií stále nedostatočne šifruje komunikáciu.
- **spyware** - softvér, ktorý sa nainštaluje podvodne do počítača, využívajúc zraniteľnosť a následne zbiera prihlasovacie, osobné alebo bankové dáta, alebo len odomkne telefón. Takéto aplikácie sú hlavne využívané v rámci spravodajských služieb a vyšetrovateľov, ale aj v rámci tzv. „neželanej“ kontroly našimi blízkymi, rodinou, prípadne bývalými priateľmi. Existuje viac komerčných softvérov, ktoré sledujú telefón, na ktorom sú nainštalované. Na vytvorenie spyware takéhoto typu je potrebné použiť veľmi veľa zdrojov (ľudských aj finančných), preto plošné použitie spyware je väčšinou rýchlo odhalené.
- **nepoužívané aplikácie** - tieto aplikácie sú veľmi nebezpečné. Ich hlavné nebezpečenstvo tkvie v tom, že keď ste ich inštalovali, boli to veľmi dôležité aplikácie s vynikajúcou reputáciou. Napríklad QR scanner, alebo vizitkár. Postupom času ste si našli lepšiu aplikáciu, alebo ich funkcionalita prešla do vlastností mobilného zariadenia a aplikácia stratila význam. Takúto aplikáciu si časom môžu kúpiť podvodníci a využívať ju na vyťahovanie dát z vášho zariadenia, pretože napriek tomu, že aplikácia je nečinná a nepoužíva sa, prístupy do mobilného zariadenia jej neboli odobrané.

- **internet vecí s mobilným pripojením** (Internet of Things. IoT) – takto sa označuje pripojenie zariadení s pripojením na sieť. Zariadenia môžu byť rôzne, od senzorov teploty, ktoré vysielajú teplotu do riadiaceho centra v pravidelných intervaloch, až po zariadenia so zabudovanou inteligenciou, ako je chladnička, ktorá zároveň vie identifikovať a objednať tovar, ktorý sme minuli. Útoky na takéto zariadenia majú rôznu podobu, od sieťových ako je DdoS, ktoré zariadenia zhodí (znefunkční), cez hľadanie chyby v systéme, až po napadnutie komunikácie medzi zariadením a centrom. Častým zneužitím je nabúranie sa do systému cez všeobecne známe, výrobcom pridelené, po inštalácií nezmenené meno a heslo a následné zneužitie zariadenia, napríklad sledovanie obete cez kameru, presmerovanie útokov cez kameru na ďalšiu obeť a iné. Základné ochrany v tomto prípade predstavujú: ochrana zariadení na sieťovej úrovni (napr. Firewallom), zmena mena a hesla po nainštalovaní, sledovanie a implementovanie záplat do firmware, ak je to možné a použite viacfaktorového overovania.
- **Calendar adware -** je reklamný softvér, ktorý sa nainštaluje do média, následne sťahuje a zobrazuje reklamy a žiada od vás urobiť nejakú akciu. V rámci zobrazovania akcií môžu hekeri podhodiť akceptáciu inštalácie podvrhnutého softvéru do vášho mobilného zariadenia. Zobrazovanie reklám je otravné, ale nie je nebezpečné, rozšírenie reklamy o klikanie akceptácií (kombinovaný útok) je už však nebezpečné. Vymazanie kalendárov je veľmi jednoduché, pričom existuje množstvo návodov na ich vymazanie na internetových stránkach.
- **nedostatočné/ žiadne zálohovanie -** je veľmi nebezpečné, ak nefunguje korektne a zlé nastavenie sa identifikuje veľmi ťažko. Ak nemáte dostatočné zálohovanie na oddelené médium ako je PC, notebook, cloud s viacerými verziami záloh, potom akékoľvek zničenie dát na mobilnom zariadení bude znamenať pre vás veľkú, nenahraditeľnú a hlavne nezvrátiteľnú stratu. Mobilné zariadenia sú často zálohované automaticky do cloudu výrobcov mobilného zariadenia. Pri tomto type zálohovania je potrebné si uvedomiť, že vaše citlivé dáta sú uložené v internete a sú pod dohľadom externej firmy,

ktorá si privlastňuje právo tieto dáta využiť[100]. Existuje aj možnosť zálohovania dát z mobilného zariadenia na váš počítač. Aj keď postup pri takomto zálohovaní je zdĺhavejší, dáta budete mať pod vlastnou kontrolou. Zálohovacie systémy majú často chyby, ale tieto vzhľadom na dôležitosť zálohovacích systémov bývajú rýchlo odstraňované.


FONTECH STARTITUP Kategórie

Android už niekoľko mesiacov trpí banálnou chybou. Google ju nevie opraviť

MÁRIO ŠIMOVIČ 13. NOVEMBRA 2019

Článok o chybe a následnom nefunkčnom zálohovaní Android systémov[101]

Vo svete mobilného priestoru existuje veľa typov útokov. Veľmi častým je útok typu *cryptojacking*. Útočníci pri ňom nájdu riešenie ako napadnúť mobilné zariadenia. Najčastejšie sa používa phishingový email, ktorý obsahuje linku na malvér. Útočníci sa snažia donútiť obete kliknúť na linku, a tým stiahnuť a nainštalovanie malvér. Následne na mobilnom zariadení naštartujú ťažbu kryptomeny. Rozoznanie takto zavíreného telefónu je ľahké, pretože takéto aplikácie sú veľmi náročné na výkon a vyťažia systém na 100%, čím vybíjajú batériu mobilného zariadenia. Alternatívou pre útočníka je, že sa vaše zariadenie môže stať súčasťou botnetu (siete internetových robotov, ktorých ovláda heker) a prostredníctvom neho sa budú riadiť a robiť ďalšie útoky na ďalšie obete. V obidvoch prípadoch je prvou pomocou sledovanie telefónu a jeho výkonu, teda či nie je pomalší, viac zohriaty ako obyčajne a či sa batéria nevybíja oveľa rýchlejšie.

[100] Pokiaľ nevyužívate služby zero knowledge poskytovateľa zálohovania, možnosť analyzovať dáta je obmedzená.

[101] Android už niekoľko mesiacov trpí banálnou chybou. Google ju nevie opraviť [online]. [09.07.2021]. Dostupné na internete https://fontech.startitup.sk/android-uz-niekolko-mesiacov-trpi-banalnou-chybou-google-ju-nevie-opravit/

Stav batérie v mobilnom telefóne a aplikácie, ktoré batériu najviac využívajú si viete zistiť, pomerne ľahko.

Zobrazenie využitie batérie v systéme iOS:

Nájdite na internete, akým spôsobom sa vymazáva calendar adware na vašom type mobilného telefónu.

Zobrazte si najpoužívanejšie aplikácie a najmenej používané aplikácie vo vašom telefóne. Identifikujte, ktoré aplikácie už nepoužívate a môžete vymazať.

5.3. Typy útokov na mobilné zariadenia

Ak porovnávame mobilné zariadenia a počítače, nenachádzame v nich zásadný rozdiel. Preto sa útočníci okrem vymýšľania nových typov útokov snažia replikovať útoky, ktoré sme si popísali v kapitole *Ochrana počítača*. Celkový počet útokov na jednotlivcov a organizácie stále narastá. Rozširuje sa množstvo, aj komplexnosť útokov. Zažívame používanie viacerých typov útokov na

dosiahnutie jedného cieľa, jedného zneužitia. Pripomeňme si najvážnejšie typy útokov:

- *ransomware* - cieľom je šifrovanie používateľských systémov za výpalné,
- *phishing* - heker má snahu dostať sa k osobným a bankovým údajom obete cez jej oklamanie,
- *Trójsky kôň* - malvér, ktorého hlavná úloha po stiahnutí sa na zariadenie spočíva v otvorené zadných dvierok v zariadení pre ďalší útok,
- *špehovanie,*
- *NFC útoky,*
- *Man in the Middle (MITM).*

Niektoré útoky sme si vysvetlili v časti o počítačoch, preto sa v tejto budeme venovať hlavne *špehovaciemu softvéru, NFC útoku a MITM* útoku. Existujú však aj veľmi špecifické útoky, ako napríklad nedostatočná alebo slabá kontrola na strane riadiaceho servera každej aplikácie (t.j. únik dát na strane servera ku ktorému sa aplikácie pripájajú). V tomto prípade sa jedná o útok na samotnú aplikáciu mimo vášho dosahu, a preto neexistuje spôsob, ako mu zabrániť.

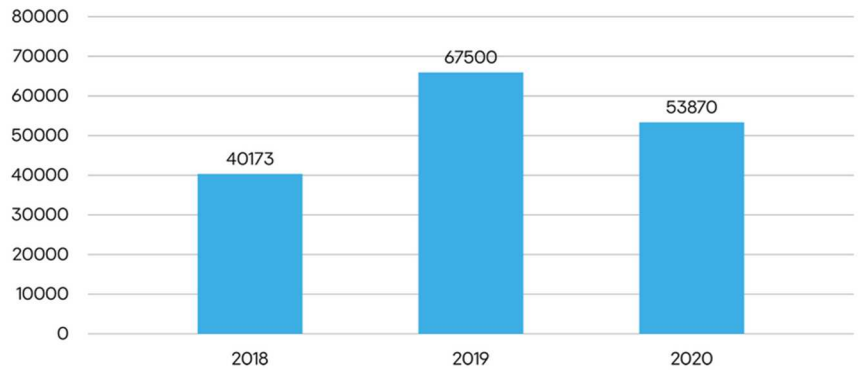
Príklad útoku na službu Clubhouse[102]

[102] Únik dát zastihol aj Clubhouse, šéf aplikácie kybernetický útok odmieta [online]. [09.07.2021]. Dostupné na internete https://www.techbyte.sk/2021/04/clubhouse-unik-dat-aplikacia-udaje/

1. Špehovanie

Mobilné zariadenie je prenosné, väčšinu dňa nás sprevádza a dokonca samo podporuje špehovanie v rámci aplikácií ako **Find my mobile** alebo aplikácií na kontrolu detí. Rovnako aj firmy si strážia svoje tajomstvá, a preto používajú na ochranu dát v mobilných zariadeniach **MDM systémy** (Mobile device management). Tieto majú možnosť lokalizácie a aj vymazania časti zariadenia alebo možnosť úplného vymazania zariadenia. Systémy na **rodičovskú kontrolu** (Parental control) majú vo svojej podstate tiež úlohy blízke špehovaciemu softvéru, kontrolujú polohu, zoznam aplikácií, dĺžku kontroly práce s aplikáciou, analyzujú prístup na internet, obsah a ďalšie záležitosti.

V predchádzajúcich častiach učebnice sme spomínali **stalking -** prenasledovanie obetí pomocou internetových služieb a prístupov do sociálnych kont na základe získania údajov pomocou sociálneho inžinierstva. Mobilné zariadenia sú svet sám osebe, a preto prichádzame s novým názvom. Pri špehovaní budeme používať nový pojem, ktorého význam už poznáme ***stalkerware,*** alebo ***spyware***. Stalkerware/Spyware je softvér na špehovanie mobilného zariadenia konkrétneho používateľa. Dokáže sťahovať videá, lokalizáciu, odfotené obrazovky, video priamo z kamery, zvuk z mikrofónu, obsah na mobilnom telefóne bez toho, aby obeť o tom vedela.



Štatistika odhalených napadnutí špionážnym softvérom podľa firmy Kaspersky[103]

[103] Stalkerware in 2020 is still a burning issue [online]. [cit. 09.07.2021]. Dostupné na internete:

Ako riešiť ochranu telefónu pri napadnutí špionážnym softvérom si povieme v kapitole *Zlepšenie bezpečnosti*. Všetky ochrany z kapitoly sú platné aj pre špehovanie. Pre prípad špehovania však k nim treba pridať ďalšiu vrstvu ochrany v podobe nasledujúcich krokov:

- Ak máte spoločné účty s partnerom, ktorý sa zmení na bývalého partnera, po skončení vzťahu zmeňte prístupy na zariadeniach a sieťach so zdieľaným kontom. Túto akciu vykonajte zo zariadenia, ktorému veríte - nemá zmysel meniť heslá z mobilného telefónu, na ktorom beží *stalkerware* vášho expartnera.
- Ak poznajú úplne neznámi ľudia osobné informácie o vás, môžu ich použiť ako zdroj aj v nainštalovanom *stalkerware*. Skontrolujte mobilné zariadenie, či neobsahuje nežiadúci softvér.
- Niekedy sa pri odpočúvaní mobilného zariadenia objavuje šum na pozadí telefonátu. Ak niečo takéto pretrváva dlhodobo, máte dôvod na skontrolovanie telefónu. V prípade, že ide o jednorazový výskyt, môže sa tak stať z dôvodu nekvalitnej linky alebo zlým konvertovaním telefónnych kodekov u operátorov.

Čo však robiť, ak identifikujete útok špionážnym softvérom? Okamžite odložiť telefón a obrátiť sa na políciu. Zároveň je vhodné z iného zariadenia zmeniť si všetky prístupy v online službách, ktoré ste používali. Resetovanie telefónu do továrenských nastavení rieši útok, ale zničí aj dôkazy a upozorní stalkera na to, že ste ho objavili. Bude mať viac času na upratanie po sebe.

Pripravte zoznam všetkých online služieb, ktoré používate vo vašom mobilnom zariadení a nájdite postupy, akým spôsobom sa mení heslo.

Ak online služby poskytujú možnosť dlhodobého overenia niektorého zariadenia, pripravte prezentáciu, akým spôsobom pre každú online službu je možné tieto dlhodobo overené relácie zrušiť?

https://www.kaspersky.com/blog/stalkerware-in-2020/39102/

2. Útoky na NFC

NFC (Near Field Communication) je protokol, ktorý sa používa hlavne pre komunikáciu a riadenie platobných kariet. Ide o komunikáciu medzi odosielateľom a prijímateľom na krátku vzdialenosť pomocou NFC tagov. Odosielateľ môže byť aktívny alebo pasívny. Väčšina zariadení/odosielateľov je pasívnych a reaguje na energiu prijímateľa, ktorou je vybudený odosielateľ (obsahuje indukčnú cievku, ktorá generuje prúd, po priblížení aktívneho člena/prijímateľa, ktorý elektromagnetické vlny vysiela). V prípade komunikácií zariadení, ako sú dva smartfóny, budú obidva členy aktívne. Oproti iným technológiám je výhoda NFC v tom, že nepotrebuje zdroj energie a funguje na krátke vzdialenosti, pričom vzhľadom na malý obsah dát, prenos trvá veľmi krátko.

Poznáme niekoľko módov útokov na NFC:

- **odpočúvanie** - útočník len odpočúva a ukladá dáta na spracovanie. Podľa typu komunikačného protokolu môže vidieť prenášané dáta. Útok je závislý od vzdialenosti a ruchov prostredia. Vzdialenosť kolíše podľa typu od 1 m pri pasívnom zariadení do 10 m pri aktívnom zariadení. Na takéto zachytávanie potrebuje útočník nainštalovať špeciálnu anténu. Rovnakým spôsobom je možné odpočúvať platobné karty podporujúce technológiu NFC. Odpočúvaním sa porušuje princíp CIA: dôvernosť.
- **poškodenie dát** alebo **rušenie prijímania a vysielania pomocou *Radio jammera*** - toto rušenie v zásade nemá zmysel, pretože aktívny prvok vie identifikovať rušenie a upozorniť na rušenie používateľa. Odpočúvaním sa porušuje princíp CIA: dostupnosť.
- **zmena dát** (vloženie) - prenos býva krátky, a preto je ťažko vkladať svoje vlastné údaje alebo meniť existujúce dáta. Vzhľadom na rýchlosť transakcie a možnosť ďalšieho priloženia zariadenia nemá takýto typ útoku veľkú pravdepodobnosť úspešnosti. Odpočúvaním sa porušuje princíp CIA: integrita (celistvosť).

Útoky na NFC sa najčastejšie obmedzujú na pozbieranie NFC tagov na neskoršie využitie. Jedným z takýchto použití je ukradnutie identifikačných údajov. Ak používate na mobilnom zariadení posielanie vizitky cez NFC tag, útočník priblíži svoj vysielač (mobilné zariadenie), vyšle vizitku a systém automaticky (ak je tak nastavený)

zabezpečí výmenu, vaše originálne dáta za útočníkove vymyslené. Ostatné informácie, ako platobné aplikácie alebo samotné platobné karty, sú zabezpečené PINom, preto útočník vie získať len informácie, ktoré kartový štandard vyžaduje, aby boli umiestnené v NFC tagu.

Z akého dôvodu používame pojem maximálnej teoretickej rýchlosti prenosu pri NFC? Vysvetlite, čo vplýva na rýchlosť a ako je možné rýchlosť ovplyvniť, aby bola čo najvyššia.

Aké typy údajov sú v NFC tagu na platobných kartách, podľa štandardu VISA?

3. Podvodné SMS

Napriek evidentnému technickému pokroku a zmene preferovaných systémov na posielanie správ, ktoré často bývajú alebo sa stávajú súčasťou sociálnych sietí, naše mobilné zariadenia umožňujú v prípade, že majú v sebe SIM, alebo virtuálnu SIM, aj uskutočňovanie hovorov a odosielanie SMS. SMS je z pohľadu informačnej bezpečnosti definovaná ako ďalší nositeľ informácií. To znamená, že aj SMS je možné stále použiť ako médium vhodné na útok, hlavne na oklamanie používateľa zariadenia, pretože väčšina používateľov si otvára SMS správu krátko po prijatí.

Poznáme nasledovné druhy útokov:

- *Podvodné SMS* - sú to SMS s podvodnými informáciami, ktorých cieľom je donútiť používateľa buď kliknúť na odkaz (následne sa pokúsia útočníci oklamať obeť, aby si táto nainštalovala podvodnú aplikáciu) alebo sa snažia, aby obeť vyplnila citlivé informácie (napr. informácie o platobnej karte) alebo sa obeť prihlásila do niektorého zo svojich bankových alebo online kont.
- *Riadiace SMS* - pri objavení tohto typu SMS musí byť používateľ obzvlášť opatrný, pretože ide o riadiace SMS pre niektorý z typov škodlivého kódu. Takýto typ škodlivého kódu má naprogramovanú aj možnosť automatického vymazania SMS, takže objavenie SMS vo vašom nástroji môže byť skôr náhoda alebo dôkaz, že máte v mobilnom zariadení funkčný škodlivý kód.

Tieto typy útokov úplne rovnako úspešne fungujú aj v prípade messengera. Na platforme WhatsApp sa šírila správa o možnosti

inštalovania ružového WhatsAppu. Nebola to však upravená aplikácia, ale iba podvodná, ktorej úlohou bolo kradnúť citlivé dáta.

Ochrana proti phishingovým útokom cez SMS je veľmi náročná, pretože, ako sme už spomínali, veľká časť ľudí otvára SMS správu okamžite po prijatí a verí v adekvátne zabezpečenie mobilného zariadenia, preto je menej podozrievavá v klikaní na linky. Ochrana pred takýmto typom útoku by mala zahŕňať predovšetkým vedomosti používateľa a následnú analýzu obsahu prijatej správy, resp. v prípade podozrenia okamžité vymazanie podvodnej správy namiesto jej spracovania. Veľmi účinnou taktikou pri práci s podvodnou SMS je neodpovedať, neklikať a neriešiť obsah okamžite, ale pozdržať odpoveď aj o niekoľko hodín. Je nevyhnutné si uvedomiť, že SMS (a aj email) je offline komunikačný kanál, a preto očakávať, že ten, kto poslal SMS, čaká na okamžitú odpoveď, je aj z pohľadu odosielateľa a aj prijímateľa principiálne nelogické a postavené proti myšlienke fungovania takejto technológie.

Čo znamená skratka SMS? Vysvetlite, ako funguje posielanie SMS správ.

2. Bluetooth

Bluetooth je bezdrôtová technológia slúžiaca na výmenu dát medzi mobilnými, ale aj fixnými zariadeniami. Bluetooth je definovaný štandardom IEEE 802.15.1. Bluetooth patrí do kategórie Personálnych sietí (PAN). Operuje na frekvencii medzi 2402 a 2450 MHz (rovnako ako WiFi) alebo v rozsahu 2480 a 2483,5 MHz vrátane chráneného pásma od 2 MHz po 3,5 MHz.[104] Existujú tri základné typy rozdelení fungovania bluetooth zariadení:

- **silent** (neakceptuje požiadavku na spárovanie, iba monitoruje zariadenia),
- **private** (akceptuje požiadavku, len ak dotyčný pozná MAC adresu zariadenia),
- **public** - preskenovaním pásma je ich možné nájsť a pracovať nimi. Do tejto časti patrí väčšina bežne používaných bluetooth zariadení.

[104] Čo je to Bluetooth, najzákladnejšia bezdrôtová technológia? [online]. [cit. 15.08.2021]. Dostupné online: https://techbox.dennikn.sk/temy/co-je-to-bluetooth/

Potvrdzovacie metódy

Dôležitou časťou bluetooth zariadenia je prepojenie zariadenia s mobilným zariadením. Toto prepojenie musí byť bezpečné a jednoznačné. Keďže ide o prepojenie dvoch zariadení, teda páru, prepojenie v tomto prípade voláme **párovanie**. Existuje veľa spôsobov párovania mobilného zariadenia s bluetooth zariadením. Pri každom prístupe sa počíta zároveň úspešnosť párovania zariadení používateľom a chybovosť. To znamená, že každý, kto vytvorí nové bluetooth zariadenie, musí počítať s tým, čo jeho systém dokáže a zároveň aj s tým, aký spôsob párovania jeho potenciálni klienti uprednostňujú. Patria sem napríklad:

- ***porovnaj a potvrď*** *(Compare-and-Confirm):* Na oboch zariadeniach sa zobrazí kód, ktorý v prípade rovnosti treba potvrdiť.
- ***vyber a potvrď*** *(Select-and-Confirm):* Na jednom zariadení je náhodne zvolený číselný reťazec. Na druhom zariadení je zoznam niekoľkých číselných reťazcov, z toho jeden je zhodný s hodnotou na prvom zariadení. Druhé zariadenie musí vybrať práve tento kód. Prvé zariadenie má potom potvrdiť správnosť voľby.
- ***skopíruj*** *(Copy):* Na prvom zariadení je náhodne zvolený číselný reťazec. Tento Reťazec treba vpísať na vstup do druhého zariadenia.
- ***skopíruj a potvrď*** *(Copy-and-confirm)*: Ak jedno zariadenie má displej a druhé ho nemá, zariadenie s displejom zobrazí číselný reťazec. Tento reťazec je treba vpísať na vstup do druhého zariadenia. Druhé zariadenie ho obratom pošle prvému, a to ho zobrazí na displeji. V prvom zariadení je nutné potvrdiť zhodu. V prípade úspechu druhé zariadenie rovnako indikuje zhodu.
- ***zvoľ a potvrď*** *(Choose-and-enter):* Užívateľ je vyzvaný, aby zvolil náhodné číslo a zadal ho do oboch zariadení.[105]

Poďme sa venovať téme ochrany bluetooth zariadení a potenciálnym hrozbám a útokom, ktoré sa môžu naskytnúť. Tieto hrozby môžu existovať na rôznych vrstvách, v rôznych častiach

[105]Buchta M. - Bezpečnosť technológie Bluetooth [online]. [cit. 08.07.2021]. Dostupné na internete https://is.muni.cz/th/ju4to/bc_Marian_Buchta_wufyzrby.pdf

procesu práce. Najčastejšie sa tak stane počas párovania a komunikácie zariadení. Vtedy môže vzniknúť logická alebo programátorská chyba a práve túto chybu sa snažia útočníci využiť. Predstavme si niektoré útoky.

Bluejacking - násilné prijímanie súborov, ktoré nechceme, napr. reklamných obrázkov a škodlivého SW na svoje mobilné zariadenie,

Bluesnarfing - starší typ útoku, ktorý zneužíval chyby vo firmware. Cieľom je pripojiť sa k zariadeniu a získať IMEI číslo (*The International Mobile Equipment Identity* je medzinárodné identifikačné alebo sériové číslo, vášho zariadenia).

Blueborne - metóda nevyžaduje párovanie oboch zariadení a dá sa použiť, aj keď zariadenia, sú v móde „neviditeľný“, musia však nejaký signál bluetooth vysielať. Tento útok nefunguje na vypnutý bluetooth. Jeho cieľom je „potichu” prebrať kontrolu nad zariadeniami, alebo pokračovať útokom Man in the Middle, resp. sa pokúsiť spustiť škodlivý kód na diaľku.

Bluetoonning - pomocou smerovej antény zosilňuje dosah bluetooth komunikácie, cez 1200m a vie tak ovplyvňovať bluetooth vysielače na diaľku.

Bluesniffing - útok monitoruje všetkých 79 kanálov a kontroluje v nich komunikáciu, ktorú nahráva a vyhodnocuje.

Signal Jamming - je to rušenie zariadenia. Jeho podstata spočíva v tom, že útočník paralelne komunikuje na zariadenie, ktoré prijíma dáta. Toto zariadenie vyhodnocuje takúto komunikáciu ako ruch a často komunikáciu prerušuje.

Bluebugging - využívanie chyby v protokole bluetooth.

1. Útok Man In The Middle

Podstata útoku je popísaná v názve samotného útoku. Útočník sa snaží dostať do stredu (centra) komunikácie medzi zariadenia a server a preposiela správy ako uzná za vhodné. Podstatu útoku si vysvetlíme na popise hry na lúke. Dvaja hráči sa rozprávajú a po každej vete sa vzdialia o krok, po čase už na seba kričia a aj to postupne nestačí. Preto sa pridá tretí hráč a ten prenáša diskusiu medzi nimi, potom štvrtý, piaty hráč a tak ďalej. Predstavte si, že jeden z hráčov bude ďalej komunikovať (prenášať) iné vety, ako ku nemu

prídu. Najprv len trošku pozmení obsah, keď zistí, že sa nič nestalo, môže komunikovať úplne nové a iné informácie. Toto je zároveň vektor útoku Man in the middle útoku. Medzi dve komunikujúce zariadenia sa dostane tretie zariadenie, ktoré bude meniť obsah komunikácie a vytvárať falošnú realitu.

V prípade bluetooth je pre nás predsa len vhodnejšie riešiť problém oveľa viac technicky. Podstata útoku spočíva v rozpojení komunikácie medzi mobilným zariadením a bluetooth zariadením (cez JAM packety) a následne odchytenie párovacích packetov a pri párovaní prienik do stredu komunikácie. Pre mobilné zariadenie sa útočník bude javiť ako bluetooth zariadenie a pre bluetooth zariadenie ako mobilné zariadenie. Výsledkom je, že všetka komunikácia tečie cez útočníka. Ochranou proti takémuto typu útoku je používanie ustáleného šifrovacieho kľúča na spárovanie komunikácie, čo je vlastne úprava samotného adaptéra.

Pri ochrane bluetooth zariadení musíme myslieť globálne. Dôvodom je fakt, že útočníci zneužívajú chyby softvéru a aj princípy fyzikálnych zákonov. Jedna z možností ochrany je vypnutie bluetooth zariadení pri nepoužívaní, toto je pomerne ťažké, keďže väčšina IoT zariadení používa bluetooth. Druhá možnosť je hneď, po vydaní záplaty pre bluetooth, okamžite záplatu inštalovať aj v mobilnom zariadení a aj v bluetooth zariadení. To však znamená, že musíme si vyberať a kupovať len také IoT zariadenia, ktoré je možné upgradovať. V neposlednom rade potrebujeme kontrolovať správanie sa mobilných a bluetooth zariadení. Téme kontroly správania sa mobilných zariadení sa budeme venovať neskôr.

Aké typy Signal jammingu poznáme? Vysvetlite ich podstatu.

Podľa koho/čoho má technológia BlueTooth svoje pomenovanie?

5.4. Ochrana mobilného telefónu

Predstavili sme si množstvo útokov a teraz si povieme, akým spôsobom vieme zistiť, že mobilné zariadenie bolo napadnuté a ako sa následne pred útokmi chrániť. Zdrojov napadnutí je veľa, od falošných stránok so skrytým malvér, cez inštalovanie aplikácií z neoficiálnych zdrojov, až po zrušenie ochrany telefónu (iphone - jailbreak, android - rootkit). Zrušenie ochrany telefónu umožňuje

nainštalovať akékoľvek aplikácie, aj kreknuté, ale zároveň znamená zrušenie štandardných bezpečnostných vlastností a povinnosť majiteľa starať sa o kompletnú bezpečnosť mobilu. Štandardne sa objavuje nestabilita operačného systému.

1. Odhaľovanie zlého správania mobilného zariadenia

Hlavný spôsob na odhalenie malvér vo vašom mobilnom zariadení je identifikovanie podozrivého správania:

- rýchle a nečakané vybíjanie batérie,
- systém otvára náhodne Pop up okná,
- rozosielanie emailov z klientov vo vašom zariadení,
- aplikácia, ktorá normálne a spoľahlivo fungovala, opakovane padá (kvôli nedostatočnému miestu v pamäti, alebo napadnutí vírusom).

Následne je potrebné dodržiavať tieto odporúčania:

- extrémne zvýšte ostražitosť pri zdieľaní dát s inými ľuďmi,
- nepožičiavajte svoje IoT zariadenia (napríklad *weareables*) cudzím ľuďom,
- nepoužívať verejné USB nabíjačky alebo používať USB condom[106],
- nepodceňovať a nenaletieť SMS správam a hovorom (odpočúvanie, SCAM, riadiace SMS).

2. Riadenie bezpečnosti mobilného zariadenia

Správna a pravidelná kontrola vnímania podozrivého správania mobilného zariadenia je nevyhnutným krokom pre dlhodobé používanie bez komplikácií. Nie je to však dostatočné. Pri práci s mobilným telefónom sa musíme naučiť automaticky dodržiavať niekoľko technických zásad:

- nainštalovať antivírus alebo iný typ detekcie malvéru,
- používať silné heslá,
- sťahovať len overené aplikácie z oficiálneho zdroja,
- nastaviť len nevyhnutný prístup pre aplikácie alebo aplikácie, ktoré vyžadujú rozsiahly prístup neinštalovať,

[106]USB Condom [online]. [11.08.2021]. Dostupné online: https://www.usbcondom.org/

- vyhýbať sa verejnej wifi,
- používať službu VPN od renomovaného dodávateľa,
- vymazať nepoužívané aplikácie,
- sledovať vyťaženie zariadenia aplikáciami, a následne tie, ktoré zariadenie zaťažujú a nepoužívate ich, vymazať,
- pravidelne kontrolovať odoslané a vymazané správy a emaily.
- updatovať aplikácie krátko po vydaní novej verzie,
- aktualizovať operačný systém mobilného zariadenia krátko po uvoľnení záplaty.

Musíme si uvedomiť, že antivírus nie je „všeliek“ a ani „všeobranca“, či už hovoríme o mobilných zariadeniach alebo počítačoch. Bezpečnostná architektúra platforiem iOS a Android limituje, čo môže antivírus na mobilnom zariadení kontrolovať. Antivírus je veľmi efektívny pri odhaľovaní podozrivého správania a poukázania na konkrétny problém, ako je škodlivá aplikácia alebo stiahnutý súbor s vírusom. Veľká výhoda antivírusu však spočíva v určitej forme alarmu, pretože tento bude poukazovať na problémy, aj keď nemusí poznať pôvodcu. Lepším riešením je používať paralelne všetky predchádzajúce body, ktoré sme si popísali.

Čo sú to weareables? Uveďte príklady weareables. Aké weareables používate?

Zobrazte si vyťažovanie baterky na zariadení jednotlivými aplikácia a vysvetlite, prečo je to v poriadku.

Čo znamená služba VPN? Napíšte aspoň tri firmy, ktoré ponúkajú funkciu VPN pre domácich používateľov, popíšte ako fungujú ich produkty a porovnajte ich (pomôcka: býva to súčasť antivírusového riešenia alebo riešenia firewall).

Vysvetlite, prečo je nevyhnutné byť ostražitý pri zdieľaní akéhokoľvek obsahu?

5.5. Správa systému a aplikácií

Neustále sme v celej kapitole o mobilných telefónoch stavali na tom, že mobilné zariadenia sú postavené tak, aby boli od začiatku a aj po celú dobu prevádzky automaticky chránené. Na základe tohto

vyhlásenia (tvrdenia) výrobcov mobilných zariadení, množstvo ľudí slepo dôveruje deklarovanej bezpečnosti mobilného zariadenia. Pozrime sa teraz na to, do akej miery je toto tvrdenie výrobcov o bezpečnosti naozaj založené na pravde a či nie je iba fiktívne.

1. Záplaty

Každý operačný systém mobilného zariadenia je vytvorený z tisícok riadkov programovacieho kódu. Stalo sa štandardom, že všetky vlastnosti, možné útoky a všetky spôsoby ochrany nie je možné výrobcom otestovať na 100%. To znamená, že každá verzia operačného systému nesie aj určité chyby, ktoré sú často bezpečnostného charakteru. Základnou ochranou v tomto prípade je pravidelne inštalovať záplaty operačného systému.

Inštalácia záplat je nevyhnutná. Inštalácia záplat aplikácií a operačného systému by mala byť automatizovaná. Niektoré záplaty neopravujú len operačný systém, ale prinášajú aj nové vlastnosti a je na vás, aby ste sa dobre oboznámili so všetkými zmenami. Následne sa môžete rozhodnúť, či po inštalácií záplaty s novou funkcionalitou si budete chcieť novú funkcionalitu nechať, alebo ju vypnúť.

Podobný princíp platí aj pri riadení záplat pre aplikácie. V rámci aplikácie záplaty neopravujú len prípadné chyby a zraniteľnosti. Prinášajú aj zmeny funkcionality a zároveň je to pre firmy vhodná príležitosť na zmenu obchodných podmienok[107] alebo informovanie o zásadných zmenách vo funkčnosti aplikácie.

- Platformu Whatsapp v roku 2014 odkúpila sociálna sieť Facebook. V čase odkúpenia sa viedli horlivé diskusie o možnosti zdieľania dát a vyťažovania dát platformou Facebook. Pretože vlna odmietania bola veľká, Whatsapp v aplikácii vytvoril tlačidlo, ktorým používateľ mohol odmietnuť zdieľanie dát s platformou Facebook. Od 8.2. 2021 prišli do platnosti všeobecné obchodné podmienky, ktoré oznámili prepojenie dát medzi Whatsappom a sociálnou sieťou Facebook a analytické spracovanie komunikácie (jednalo sa predovšetkým o profilovanie používateľa) z Whatsappu vo Facebooku. Následne bolo v novej verzii aplikácie Whatsapp tlačidlo o odmietnutí prenášania a spracovania dát vo

[107] napr. aktualizované podmienky zberu a spracúvania používateľských metadát, prípadne rozšírenie spracovania dát o spracovanie telemetrie.

Facebooku zrušené. Toto bol dôvod veľkého prechodu používateľov, ktorí sa obávali zneužívania osobných dát platformou Facebook, z platformy Whatsapp do iných platforiem.

- *Prečo je profilovanie používateľov akoukoľvek platformou zle vnímané a chápané ako vážne narušenie súkromia?*
- *Nájdite kde a ako sú popísané všetky zmeny, ktoré konkrétna záplata pre operačný systém vášho mobilného zariadenia prináša.*
- *Zoznam zmien operačného systému z predchádzajúceho prípadu rozdeľte na časť, ktorá ochraňuje operačný systém a časť, ktorá prináša novú funkcionalitu.*
- *Vyberte si vašu obľúbenú aplikáciu a konkrétnu záplatu tejto aplikácie. Nájdite, kde a ako sú popísané všetky zmeny, ktoré konkrétna záplata prináša.*
- *Zoznam zmien v aplikácii z predchádzajúceho prípadu rozdeľte na časť, ktorá rieši konkrétne zraniteľnosti aplikácie a časť, ktorá prináša novú funkcionalitu a časť, ktorá prináša zmeny obchodných podmienok.*

2. Rootkity

Časť používateľov pri práci s mobilným telefónom považuje uzavretosť a automatickú ochranu mobilných zariadení za veľmi obťažujúcu a obmedzujúcu. Práve preto sa rozhodnú ochranu porušiť a implementovať riešenie, ktoré ochranu zruší. Názov takéhoto riešenia je **rootkit** pre systém Android alebo **jailbreak** pre systém iOS. Po jeho implementovaní používatelia dostanú plný prístup do operačného systému a ku všetkým funkciám telefónu, odstránia sa obmedzenia na používanie SIM a rôzne ďalšie výhody. Zároveň sa však týmto spôsobom otvoria rôzne bezpečnostné hrozby, umožňujúce napríklad inštalovať aplikácie z nedôveryhodných zdrojov, a tým zaniesť malvér do zariadenia cracknutými aplikáciami. Operačný systém sa naviac stáva nestabilným a často padá.

Cracknutá aplikácia - aplikácia, ktorá bola upravená tak, aby systém na ochranu softvéru (licenčný kontrolný systém) bol vypnutý alebo nefunkčný. Takto upravujú aplikáciu hlavne hackeri, a preto niektoré knižnice sú pravidelne obohatené o vírus alebo iný typ malware.

Veľkou nevýhodou pre používateľov je, že aplikácie, ktoré spravujú veľmi citlivé dáta, automaticky kontrolujú prostredie mobilného zariadenia. Toto kontrolovanie nie je samoúčelné a vyplýva priamo z zo zákonov a nariadení. V prípade odhalenia narušenia bezpečnosti operačného systému sa aplikácie nespustia. Takéto správanie je jasne popísané a zdôraznené vo všeobecných obchodných podmienkach.

3. Lokalizácia strateného/ukradnutého mobilného telefónu

Ak sa nám stalo, že sme si neuchránili svoje mobilné zariadenie a nevieme, kde sa nachádza, potom potrebujeme riešenie, ako zariadenie lokalizovať (alebo zariadenie aspoň na diaľku vymazať). Ak bolo zariadenie ukradnuté, v takom prípade je veľmi dôležité ho čím skôr vymazať, aby sa útočník nedostal k naším dátam a prístupom k online službám.

Ako teda lokalizovať svoje mobilné zariadenie?

- Nahláste stratu alebo krádež zariadenia na polícii, pričom uvediete aj oznámenie jedinečného identifikátora mobilného telefónu IMEI (International Mobile Equipment Identity). IMEI je nevyhnutné si pamätať a musíte ho mať uložené mimo mobilného telefónu.
- Android: firma Google poskytuje pre nájdenie zariadenia integrovanú funkciu *Nájdi moje zariadenie.* Pred tým, ako ho začnete používať, musíte si rovnomernú aplikáciu nainštalovať do mobilného zariadenia a aktivovať. Následne po prihlásení sa do Google účtu viete
    - vidieť lokalizáciu telefónu (ak je zapnutý a pripojený k sieti),
    - identifikovať poslednú lokalizáciu telefónu (ak je vypnutý),
    - prezvoniť telefón (ak je zapnutý a pripojený k sieti),

    - uzamknúť telefón na diaľku (ak je zapnutý a pripojený k sieti),
    - vymazať, resp. obnoviť továrenské nastavenia na diaľku (ak je zapnutý a pripojený k sieti).

  Veľmi dôležité je skontrolovať si posledné aktivity na vašom google účte, pričom budete prinajmenšom vedieť identifikovať rozsah napadnutia.

- Ostatné platformy, ako sú Xiaomi, Apple, Huawei, Samsung majú tiež vlastné riešenie aplikácie: *Nájdi moje zariadenie*. Veľkou nevýhodou je stále to, že aplikácie musia byť aktivované a zároveň musíte mať ďalšie zariadenie alebo prístup na webový portál, na ktorom sa budú všetky ochranné zmeny robiť. Problém strateného mobilu však riešia dokonale. Prípad ukradnutého mobilu, ktorý je online, riešia dobre. Nevedia však riešiť vypnutý mobil. V tomto prípade zobrazujú len poslednú polohu mobilu. Veľmi dobrú funkcionalitu má mobilný telefón značky Apple, ktorý po zablokovaní mobilu na diaľku automaticky zruší aj možnosť platenia cez ApplePay.
- Na kontrolu miesta a ochranu mobilu existujú aj komerčné aplikácie. Často býva takáto služba za príplatok antivírusových riešení, existujú však aj samostatné aplikácie na kontrolu polohy, ako sú Snoopza, Glympse, TrackView, a ďalšie. Výhodou týchto aplikácií je, že umožňujú vymazanie dát v mobile aj na základe poslanej riadiacej SMS.

Problémom však naďalej zostáva, ako nájsť vypnutý ukradnutý mobil. V tomto prípade sa dozviete len jeho poslednú polohu. Rovnaký problém je ako nájsť mobilný telefón bez SIM karty.

Na čo nezabudnúť v prípade, ak ide o krádež mobilného telefónu? Okamžite:

- nahlásiť krádež operátorovi, ktorý zamedzí zneužitiu SIM karty, zakáže volania zo SIM karty a platenie ďalších služieb zo SIM karty. Ak máte zistené jedinečné číslo IMSI (International Mobile Subscriber Identity) zo SIM karty, oznámenie tohto čísla uľahčí operátorovi kroky, ktoré musí podniknúť na ochranu vašich údajov z mobilného zariadenia, pretože toto číslo prepája používateľa a SIM kartu a je uložené na SIM karte.
- nahlásiť krádež na polícii. Polícia má svoje nástroje na riešenie ukradnutého mobilného telefónu.

- okamžite zrušiť všetky možnosti platby z mobilného telefónu (ako sú ApplePay, GooglePay, odpárovanie bankových aplikácií).
- okamžite zmeniť heslá do všetkých kont, ktoré máte zapamätané v mobilnom telefóne

Nájdite IMEI svojho mobilného zariadenia.

Ako je definovaný formát IMEI (z akých častí sa IMEI skladá?)

Prečo je problémom nájsť mobilný telefón, ak neobsahuje SIM?

4. Zálohovanie, darovanie mobilného telefónu a cloud

V súčasnosti sa čoraz populárnejšou, ale samozrejme aj nevyhnutnejšou, témou stáva recyklovanie, ktoré sa postupne preklápa do reusovania (znovupoužitia) starých vecí. Recyklovanie v prípade mobilných telefónov je veľmi dôležité, lebo každý mobilný telefón obsahuje veľké množstvo vzácnych kovov a iných surovín. Znovupoužitím takéhoto zariadenia alebo jeho častí viete pomôcť tým, ktorí si nemôžu dovoliť zabezpečiť najnovšie, resp. žiadne, modely mobilných telefónov. Trendu znovupoužitia sa teda nevyhli ani mobilné telefóny. Ak máte nový telefón a chcete starý telefón ďalej posunúť niekomu, kto ho potrebuje, potom si povedzme základné kroky, na ktoré nesmiete zabudnúť. Našim zámerom je poskytnúť vám odporúčania, ktoré zabezpečia, aby ste sa vyvarovali sa situáciám, keď mobilný telefón odovzdáte aj so svojimi citlivými dátami ako sú videá, fotky, údaje o sebe, rodine a kamarátoch.

Uvedieme si **nevyhnutné kroky** na bezpečné vymazanie mobilného telefónu, pričom cieľom bude ochrániť si dáta, ktoré budeme mazať, poprípade preniesť na nový mobilný telefón.

1. Povypínajte všetky aplikácie, ktoré majú za úlohu sledovať telefón a zabraňovať krádeži.
2. Rozpárujte si Bluetooth zariadenia, priradené k vášmu mobilnému telefónu.
3. Zálohujte si kompletné zariadenie aj so všetkými údajmi vo všetkých častiach mobilného telefónu (sem patrí aj pamäťová karta).
4. Odstráňte všetky pamäťové karty zo zariadenia.

Postup pre mobilné zariadenia značky Apple:

- Odhláste sa z iCloudu, iTunes a App Store.
- Zrušte registráciu v iMessage.
- Otvorte si Nastavenia a následne: Všeobecné > Resetovať > Vymazať celý obsah a nastavenia.
    - Ak máte eSIM, v tomto kroku vás zariadenie požiada o vymazanie karty, čo potvrďte.
- Odstráňte zariadenie zo zoznamu dôveryhodných zariadení.

Postup pre mobilné zariadenia s OS od firmy Google:

- Zrušte odomykanie telefónu PINom alebo vzorom. V aplikácii Nastavenia, kategória Zabezpečenie > Zámka obrazovky.
- Zrušte prepojenie mobilného telefónu s google účtom. V aplikácii Nastavenia, kategória Účty, zvoľte odstrániť účet. Voľbu potvrďte pre všetky google účty v zariadení.
- Vyberte MicroSD kartu, pretože resetovanie do továrenských nastavení nedotýka.
- Vymažte google konto z telefónu, na stránke www.myaccount.google.com. Tu si vyhľadáte svoj mobilný telefón a vymažete ho zo zoznamu dôveryhodných zariadení.
- Spustite obnovenie výrobných nastavení. V aplikácii Nastavenia, kategória Zálohovanie a obnova > Obnovenie výrobných nastavení > Resetovať telefón.

Nezabúdajte, ak máte v mobilnom telefóne pamäťovú kartu, resetovanie do výrobných nastavení neresetuje pamäťovú kartu. Najlepšie je, ak kartu vyberiete a nechajte si ju alebo ju zničte. Ak je to naozaj nevyhnutné, zabezpečte vymazanie obsahu karty, pomocou špeciálnych aplikácii. Dodržiavaním pokynov na resetovanie do továrenských nastavení sa nemusíte obávať, že odovzdáte svoje najtajnejšie údaje ďalšiemu človeku.

Aké výhody prináša zaregistrovanie mobilného telefónu do cloudu? (iCloud, GoogleCloud).

Ktorou aplikáciou je možné resetovať pamäťovú kartu v mobile?

Pripravte prezentáciu a popíšte podrobne jednotlivé kroky aj s fotodokumentáciou na resetovanie mobilného telefónu do továrenských nastavení.

Aké dáta sú spracovávané v cloude u jednotlivých výrobcov mobilných telefónov?

5.6. Zhrnutie - ochrana mobilného zariadenia

V kapitole tejto sme si prešli jednotlivé prvky ochrany mobilného zariadenia. Všimli sme si, že mobilné zariadenie v súčasnosti je ťažko odlíšiť vo svojej technologickej podstate od akéhokoľvek počítača. Z toho dôvodu veľká časť ochranných prvkov je rovnaká pre obidve platformy. To znamená, že často nezáleží na tom, či ide o stolný počítač alebo mobilné zariadenie, ich ochrana funguje na podobnom princípe .

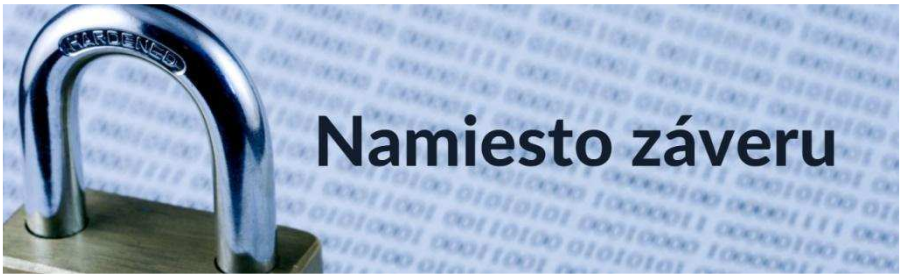
Základnou premisou a podmienkou pre riadenie bezpečnosti je mať **telefón chránený PINom alebo biometriou (odtlačok prsta, biometria tváre).** Druhým krokom je **pravidelné aktualizovanie operačného systému a aplikácií.** Takto zabezpečíte, že vaše zariadenie bude obsahovať iba skutočné minimum známych bezpečnostných hrozieb. A v neposlednom rade platí pravidlo, že všetky **aplikácie by mali byť inštalované iba z oficiálnych zdrojov**.

Ak je to možné a aplikácie to umožňujú, **zašifrujte si dáta v zariadení a zašifrované dáta používajte aj pri komunikácii**. Niektoré aplikácie ešte stále nemajú automatické (natívne) šifrovanie a treba ho špeciálne vyžiadať. Pre rýchle a ľahko zrealizovateľné odhalenie bezpečnostných problémov platí hlavná zásada: **používajte antivírus**. Nezabúdajte **byť obozretní pri správach a e-mailoch od cudzích osôb**, s rôznymi prílohami alebo nezvyčajnými požiadavkami.

Nepripájajte sa na cudzie alebo nezaheslované wifi siete a ak je to pre vás nevyhnutné, používajte bezpečnú VPN alebo sa neprihlasujte nikam, kde je potrebné založiť, mať či používať konto.

Posledné odporúčanie je zhrnuté vo vete: **pravidelne zálohujte svoje dáta.**

Predchádzajúce riadky sú návodom na relatívne bezpečný spôsob používania mobilného zariadenia. Neprinášajú vám však úplnú istotu a bezpečie. Vy máte jednu veľkú výhodu a tou je fakt, že ak ste pozorne študovali celú kapitolu o mobilných zariadeniach, poznáte všetky hlavné hrozby a viete sa pred nimi aktívne ochrániť.



Namiesto záveru

Máme za sebou prvý rok štúdia predmetu, ktorým vás sprevádzala naša učebnica. Spoločne sme si osvojili základné témy z oblasti informačnej a kybernetickej bezpečnosti. Prebrali sme základné pojmy, teoretické princípy riadenia bezpečnosti, spoznali terminologické pomenovania, ako sú aktíva, riziká, zraniteľnosti a množstvo ďalších. Naučili sme sa chápať najviac rozšírené riziká pri využívaní IKT, najmä so zameraním na internetové služby, počítače a mobilné telefóny. Ale hlavne, naučili sme sa chápať princíp znižovania rizika zavádzaním opatrení vo forme bezpečnostných požiadaviek a ich dodržiavaním. Kniha vám predstavila základné bezpečnosti prvky, ktoré potrebuje poznať človek v digitálnom veku.

Veríme, že zvládnutím tejto učebnice ste si vybudovali vedomostný základ, na ktorom budete môcť v ďalších ročníkoch, ale i v rámci samoštúdia, ďalej stavať a rozvíjať svoje vedomosti a zručnosti v tak náročnej a krásnej disciplíne, akou je kybernetická a informačná bezpečnosť. Možno ste touto knihou začali svoju budúcu kariéru a na ceste k svojmu budúcemu povolaniu v oblasti CyberSec sa k tejto publikácii budete pravidelne vracať.

A v tom Vám autorský tím drží palce.

01. Európsky digitálny kompas sa zaoberá:
    a. kybernetickými útokmi v digitálnom priestore
    b. balíkom právnych predpisov o digitálnych službách
    c. digitalizáciou údajov v papierovej podobe
02. Čo sú základné atribúty modelu CIA?
    a. dôvernosť, dostupnosť, integrita
    b. integrita, celistvosť, dôvernosť
    c. dôvernosť, dostupnosť, integrita
03. Európska digitálna identita:
    a. je použiteľná na identifikáciu osoby na celom svete
    b. je k dispozícii primárne pre občanov štátov mimo EÚ, aby preukázali svoju identitu alebo osobné údaje za účelom prístupu k verejným a súkromným digitálnym službám v celej EÚ
    c. umožňuje používateľom mať plnú kontrolu nad tým, ktoré aspekty svojej identity, údaje a certifikáty chcú poskytnúť tretím stranám a získať prehľad o tomto zdieľaní údajov

04. Pre uchovanie pozitívnej digitálnej stopy je potrebné:
    a. Podporiť informácie zážitkovou fotografiou
    b. Šíriť o sebe pozitívne informácie bez ohľadu na ich pravdivosť
    c. Posielaním pozvánok o priateľstvo neznámym ľuďom a akceptovanie pozvánok o priateľstvo od neznámych ľudí
05. DMCA znamená
    a. Digital Millenium Copyright Act
    b. Digital Mandatory Confidentiality Act
    c. Digital Manipulation and Counterfeit Act
06. Zničením zariadenia, ktoré používateľ používal na prístup k digitálnej službe zanikajú zápisy informácií uložené:
    a. v zariadení, ktoré používateľ používa
    b. u operátora siete, ktorá je používaná na pripojenie do internetu,
    c. u správcu softvéru, ktorý je používaný klientom (napr. na webovom serveri)
07. Za digitálnu stopu nepovažujeme: :
    a. záznamy v logoch
    b. dočasné súbory
    c. hardvér s bezpečne vymazaným diskom
08. Odoslaný email je:
    a. aktívna stopa
    b. pasívna stopa
    c. nie je žiadna stopa
09. Čo je to sociálne inžinierstvo?
    a. Odbor vysokoškolského štúdia na známej technickej univerzite.
    b. Manipulatívna technika, ktorej cieľom je použitím netechnických metód uviesť obeť v klam
    c. Technika analýzy počítačového programu bez dostupnosti zdrojového kódu.

10. Ktoré z nasledovných ľudských vlastností alebo správania využíva sociálne inžinierstvo?
    a. konanie v časovom strese
    b. nedôverčivosť
    c. rezistencia voči autorite
11. Kto je to stalker?
    a. osoba, ktorá vytvára kybernetické útoky z cieľom zastrašenia, vytvárania tlaku na vládu alebo obyvateľstvo
    b. osoba, ktorá obťažuje, vyhráža sa, či iným spôsobom prenasleduje obeť
    c. osoba, ktorá hľadá zraniteľnosti v zariadeniach a softvéroch a následne sa pomocou poznania zraniteľností snaží prelomiť obranu zariadenia a využiť dáta na zariadení a zariadenie samotné vo svoj prospech
12. Phishing je šírený prostredníctvom:
    a. emailu
    b. SMS
    c. telefonického hovoru
13. Čo je ransomware?
    a. Typ škodlivého softvéru, ktorý odchytáva stlačené klávesy.
    b. Typ škodlivého softvéru, ktorý zobrazuje reklamu.
    c. Typ škodlivého softvéru, ktorý zašifruje súbory a požaduje zaplatenie výkupného.
14. Čo je to SPAM?
    a. SPAM je nevyžiadaná elektronická pošta
    b. SPAM je email, ktorý obsahuje škodlivú prílohu alebo linku
    c. SPAM je email, ktorá obsahuje falošnú správu, fabuláciu, novinársku kačicu, atď.

15. Čo je to HOAX?
    a. HOAX je email, ktorý obsahuje falošnú správu, fabuláciu, novinársku kačicu, atď.
    b. HOAX je nevyžiadaná elektronická pošta
    c. HOAX je email, ktorý obsahuje škodlivú prílohu alebo linku
16. Cookies sú drobné dáta používané vo všeobecnosti
    a. webovým prehliadačom
    b. klientom elektronickej pošty
    c. instant messaging mobilnou aplikáciou
17. IP adresa je:
    a. Sada čísiel identifikujúcich počítač v počítačovej sieti
    b. Alternatíva k emailovej adrese
    c. Identifikácia (adresa) používateľa v instant messaging aplikácii
18. Aký účel plnia záplaty (patch) operačného systému?
    a. Opravujú funkčné chyby alebo bezpečnostné zraniteľnosti aplikačného a programového vybavenia
    b. Opravujú funkčné chyby alebo bezpečnostné zraniteľnosti operačného systému
    c. Opravujú funkčné chyby alebo bezpečnostné zraniteľnosti chýbajúceho bezpečnostného povedomia u používateľa
19. Čo znamená skratka DNS?
    a. Domain name system
    b. Document naming system
    c. Development namespace system
20. Ktoré z nasledovných hesiel je najodolnejšie voči útoku hrubou silou (brute-force)?
    a. P@ssword
    b. tancovala by som bosa som
    c. #51ln) h35l0#

21. Multifaktorová autentifikácia je:
    a. Autentifikácia, počas ktorej dochádza k viacnásobnej faktorizácii čísiel
    b. Autentifikácia, ktorá kombinuje viaceré rôzne faktory
    c. Autentifikácia, ktorá berie do úvahy fyzickú lokalitu používateľa
22. Mobilný telefón je pri predaji (darovaní) potrebné:
    a. vyčistiť a nechať opraviť prasknuté sklo
    b. resetovať do výrobných nastavení
    c. resetovať do výrobných nastavení a bezpečne vymazať údaje
23. Úlohou zálohovania údajov je:
    a. Zaistiť dôvernosť údajov
    b. Zaistiť dostupnosť údajov
    c. Zaistiť integritu údajov
24. Riziko je:
    a. pravdepodobnosť hrozby a jej dopad na zraniteľnosť
    b. pravdepodobnosť aktivácie hrozby nad aktívom
    c. pravdepodobnosť, že sa hrozba naplní a zmení na incident
25. Do aktív organizácie nezahŕňame:
    a. ľudí
    b. softvér
    c. úvery organizácie v banke
26. 0-day je vlastnosť týkajúca sa:
    a. zraniteľnosti
    b. rizika
    c. hrozby

27. Zraniteľnosť v kerneli nemôžeme mitigovať prostredníctvom:
    a. záplaty
    b. odinštalovaním softvéru
    c. workaroundu
28. Zjednodušený cyklus informačnej bezpečnosti obsahuje fázy:
    a. Plánuj - Implementuj - Otestuj - Akceptuj
    b. Plánuj - Vykonaj - Over - Zlepši
    c. Plánuj - Nasaď - Pentestuj - Zaplač
29. Cyklus riadenia rizík neobsahuje fázu:
    a. Identifikovanie rizík
    b. Implementácia rizík
    c. Monitoring systémov
30. Kontrola stavu bezpečnosti sa nevykonáva na úrovni:
    a. kontroly hardvéru
    b. sústavného monitoringu prostredia
    c. hĺbkového auditu
31. Príkladom prenesenia rizika je:
    a. implementácia firewallu
    b. poistenie voči riziku
    c. penetračný test
32. Čo je to bezpečnostný štandard?
    a. Dokument, ktorý obsahuje technické špecifikácie alebo iné presné kritériá, ktoré sa môžu používať ako pravidlá, smernice alebo definície.
    b. Dokument, ktorý obsahuje odporúčania, ktoré môže organizácia rozpracovať do presných technických špecifikácii alebo iných kritérii
    c. Dokument, ktorý obsahuje zoznam bezpečnostných procesov, ktoré je povinná organizácia implementovať

33. Medzi najznámejšie bezpečnostné štandardy patrí:
    a. Séria noriem ISO 27000
    b. Séria noriem ISO 20000
    c. Séria noriem ISO 9000
34. Princíp „Need to know" znamená:
    a. Umožnenie prístupu k informácii len tým subjektom, ktoré o nej nevedia a umožnenie vzdelať sa
    b. Umožnenie prístupu k informácii len tým subjektom,ktoré o nej potrebujú vedieť pre svoju prácu
    c. Umožnenie prístupu k informácii všetkým
35. Prakticky aplikovať princíp „Need to do" na zamestnanca, ktorý nahráva papierové zmluvy do systému v banke znamená:
    a. Umožniť zamestnancovi prístup ku všetkým dátam o klientoch
    b. Umožniť zamestnancovi prístup ku všetkým dátam o klientoch, ktorých zmluvy založil zamestnanec
    c. Umožniť zamestnancovi prístup len k tým klientom, ktorých zmluvy založil zamestnanec v rozsahu údajov uvedených v zmluve
36. Princíp „čo nie je zakázané je povolené" aplikovaný v kontexte prehliadania webových stránok znamená:
    a. Povolenie len explicitne vymenovaných webových stránok
    b. Povolenie webových stránok s výnimkou blokovaných webov (alebo kategórií)
    c. Neobmedzený prístup na web

37. K4O znamená:
    a. Dodatočnú kontrolu/overenie inou osobou, napr. vytvorenie údajov jedným zamestnancom a kontrolu iným zamestnancom.
    b. Prítomnosť aspoň 4 osôb na zavedenie šifrovacieho kľúča
    c. Zastaralú microservices technológiu, ktorá bola nahradená kubernates (K8S)
38. Typosquatting je:
    a. použitie domény, ktorá vznikla preklepom s domény, ktorá je predmetom útoku, napr. „bamka.sk" namiesto „banka.sk"
    b. použitie preklepov na generovanie silného hesla z pôvodne zamýšľaného hesla, napr. „Silne hrslo" namiesto „Silne heslo"
    c. podvodné prevedenie vlastníctva domény a následné ponúknutie organizácii za výrazne vyššiu cenu
39. Čo je to firewall?
    a. Bezpečnostný prvok, ktorý kontroluje a filtruje neautorizované aplikácie na operačnom systéme
    b. Bezpečnostný prvok, ktorý kontroluje a filtruje sieťovú komunikáciu
    c. Bezpečnostný prvok, ktorý kontroluje a filtruje vstup do budovy
40. Čo je to šifrovanie?
    a. Transformácia šifrového textu na otvorený text prostredníctvom algoritmu a šifrovacieho kľúča
    b. Transformácia otvoreného textu na šifrový text prostredníctvom algoritmu a hašovacieho kľúča
    c. Transformácia otvoreného textu na šifrový text prostredníctvom algoritmu a šifrovacieho kľúča

41. Hašovaciu funkciu vieme využiť na:
    a. vytvorenie digitálneho odtlačku (fingerprint) dát
    b. kompresiu dát
    c. zašifrovanie dát
42. Čo je to netiketa?
    a. Opak slova etiketa
    b. Špecifická etiketa v informačnej bezpečnosti
    c. Etiketa v kybernetickom priestore
43. Router je zariadenie určené
    a. na kontrolu a filtrovanie sieťovej komunikácie
    b. na šifrovanie sieťovej komunikácie
    c. na smerovanie sieťovej komunikácie
44. Pod pojmom reputácia webovej stránky chápeme
    a. dôveryhodnosť webovej stránky
    b. používanie X.509 certifikátu webovou stránkou
    c. nepoužívanie trackerov na sledovanie používania webovej stránky
45. Osobné údaje sú:
    a. informácie, ktoré umožňujú identifikovanie konkrétnej osoby
    b. informácie, ktoré vytvorila konkrétna osoba
    c. informácie, ktoré identifikovala konkrétna osoba
46. Do osobitnej kategórie osobných údajov nepatrí:
    a. náboženské presvedčenie
    b. genetické a biometrické informácie
    c. plat
47. Prezradenie osobných údajov nemôže viesť k:
    a. odcudzeniu identity (identity theft)
    b. vytvoreniu terču z obete s cieľom urážania, posmechu a pohŕdania, často aj vydierania
    c. pokute dotknutej osoby zo strany Úradu na ochranu osobných údajov

48. Zodpovednosť za príspevok na sociálnej sieti nesie:
    a. Sociálna sieť
    b. ten, kto príspevok uverejňuje
    c. ten, kto je v príspevku spomenutý, alebo zobrazený na fotografii
49. Použiť dielo bez súhlase autora:
    a. nie je možné
    b. je možné pri komentovaní, citovaní a recenzovaní diela
    c. je možné ak od smrti autora ubehlo viac ako 30 rokov
50. Trolling znamená:
    a. správanie, ktoré navádza obeť na zverejnenie citlivých informácii
    b. správanie, ktoré má za cieľ provokovať, urážať, zmeniť tému, jednoducho chce za každú cenu narušiť diskusiu
    c. správanie, ktoré zneužíva zdieľané intímne fotografie
51. Čo znamená skratka SMS?
    a. Short message service
    b. Silent message service
    c. Secure message service
52. Skratka VPN znamená
    a. Virtual public network
    b. Virtual private network
    c. Virtual personal network
53. Čo je to cracknutá aplikácia
    a. Aplikácia, ktorá obsahuje bezpečnostnú zraniteľnosť
    b. Aplikácia, ktorá obsahuje dodatočne spoplatnený obsah
    c. Aplikácia, pri ktorej bola prelomená ochrana voči neautorizovanému šíreniu

54. Na čo slúži logovanie systémov a aplikácií
    a. Na ochranu systémov a aplikácií voči neautorizovanému šíreniu
    b. Na zaznamenávanie prevádzkových a bezpečnostných udalostí systémov a aplikácii
    c. Na zašifrovanie dát v systémoch a aplikáciách
55. Aká aplikácia slúži pre prácu so systémovými logmi v operačnom systéme Windows
    a. Event Viewer
    b. System Viewer
    c. je potrebná externá aplikácia
56. Aké typy udalostí sú logované vo Windows event logoch
    a. Event a Security
    b. Application, System a Security
    c. Activity, System a Security
57. Malicious aplikácia je:
    a. Aplikácia, ktorá obsahuje platenú funkcionalitu
    b. Aplikácia, ktorá obsahuje škodlivú funkcionalitu
    c. Aplikácia, ktorá obsahuje ochranu voči neautorizovanému šíreniu
58. Medzi vlastnosti digitálneho priestoru nepatrí:
    a. otvorenosť
    b. centralizovanosť
    c. globálnosť
59. Obsah emailovej schránky na portáli Edupage patrí k:
    a. surface web
    b. deep web
    c. dark web

60. Aký je rozdiel medzi kybernetickou a informačnou bezpečnosťou?
    a. žiadny sú to rovnaké pojmy pre IT bezpečnosť
    b. kybernetická bezpečnosť sa týka robotov, informačná bezpečnosť počítačov
    c. kybernetická bezpečnosť je bezpečnosť zameraná na IKT a ako taká je podmnožinou informačnej bezpečnosti
61. Kybernetická bezpečnosť stojí na troch pilieroch:
    a. procesy, nástroje, ľudia
    b. dostupnosť, dôvernosť, integrita
    c. riziko, opatrenia, náklady
62. Národný bezpečnostný úrad nemá v kompetencii:
    a. všetky úlohy v oblasti kyberbezpečnosti na národnej úrovni
    b. ochranu osobných údajov
    c. navrhovanie postupu v prípade kybernetického útoku počas krízovej situácie v SR
63. Úrad pre ochranu osobných údajov plní úlohu:
    a. vypracováva Správu o stave kybernetickej bezpečnosti v SR a predkladá ju Výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR
    b. monitoruje a analyzuje kybernetický priestor a jeho možné hrozby
    c. vykonáva dohľad nad ochranou osobných údajov
64. Čo znamená skratka IoT:
    a. Incident of Technology
    b. Internet of Things
    c. Internet of Threats
65. Dôvernosť spracúvaných údajov, môže byť na úrovni hardvéru kompromitovaná:
    a. elektromagnetickým vyžarovaním
    b. elektrickým výbojom
    c. dymom

66. Príkladom útoku postranným kanálom nie je:
    a. analýza zmien taktovacej frekvencie procesora
    b. analýza času spracovania dát
    c. analýza zmien v spotrebe elektrickej energie
67. Ktorú z nasledovných vlastnosti nemá kryptografický haš?
    a. Je ťažké nájsť dáta ku konkrétnemu hašu
    b. Je ťažké nájsť dvojicu dát s rovnakým hašom
    c. Je ťažké nájsť haš ku konkrétnym dátam
68. Zraniteľnosť je
    a. je slabé miesto v počítačovom systéme, ktoré umožní útočníkovi vykonať útok na počítačový systém.
    b. je silné miesto v počítačovom systéme, ktoré zabráni útočníkovi vykonať útok na počítačový systém.
    c. je slabé miesto v exploite, ktoré umožní antivírusovému programu zablokovať exploit.
69. Aký je rozdiel medzi SSL a TLS?
    a. Žiadny, ide o rovnakú technológiu
    b. SSL je používané nad protokolom HTTP, TLS je nad protokolmi ako IMAP alebo POP3
    c. TLS je protokol, ktorý je nástupcom protokolu SSL
70. Certifikát webového servera je:
    a. PGPMIME certifikátom
    b. Certifikátom verejného kľúča (X.509 certifikátom)
    c. X.25 certifikátom
71. Čo je to malwaretizing?
    a. Zobrazovanie reklám na malvér as a service
    b. Využitie reklám na distribúciu škodlivého softvéru
    c. Využitie reklám na ochranu pred škodlivým softvérom

72. Čo je to PEGI?
    a. Systém kategorizácie aplikácii a webových stránok podľa obsahu, napr. „zbrane", „alkohol" atď.
    b. Systém hodnotenia a zaradenia aplikácii a webových stránok podľa vhodnosti pre určitú vekovú kategóriu
    c. Systém hodnotenia kvality času stráveného dieťaťom pri používaní zariadenia
73. Na základe čoho nevie používateľ vyhodnotiť reputáciu doplnku webového prehliadača:
    a. Názvu
    b. Hodnotení (počtu hviezdičiek)
    c. Recenzii
74. Vyhľadávacie engine priateľské k súkromiu:
    a. Neexistujú
    b. Existujú len pre dark web
    c. Existujú a sú bežne dostupné na internete
75. Pri službe email je garantované:
    a. doručenie správy
    b. autentickosť správy
    c. ani jedno z uvedeného
76. SPF záznam pre doménu obsahuje:
    a. IP adresu webového servera
    b. IP adresu emailového servera
    c. IP adresy a domény tretích strán, ktoré môžu posielať emaily v mene domény
77. Ktoré štandardy slúžia na šifrovanie a podpisovanie elektronickej pošty?
    a. SMIME a PGPMIME
    b. HTTPS
    c. SFTP a FTPS

78. Skratka BEC znamená
    a. Business email confidentiality
    b. Business email compromise
    c. Business email corruption
79. Čo je to cookiewall?
    a. Firewall na blokovanie cookies
    b. Banner na webovej stránke, na ktorom návštevník potvrdzuje súhlas s použitím cookies
    c. Detekcia škodlivého softvéru v cookies
80. Ktoré z uvedených príkladov nie sú metadátami?
    a. IP adresa
    b. EXIF informácia
    c. Obsah chatu
81. Ktorá z uvedených sietí nie je plne anonymná sieť?
    a. TOR
    b. VPN
    c. I2P
82. Ktorý z uvedených príkladov nie je MFA:
    a. Heslo a odtlačok prsta
    b. Heslo a OTP
    c. Heslo a PIN
83. Ktorý z uvedených faktorov môže byť problematický z pohľadu akceptácie používateľmi?
    a. Odtlačok prsta
    b. Sken sietnice
    c. Hlasová biometria
84. MFA nás chráni:
    a. Aj v prípade, že autentifikácia je smerom kompromitovaný server
    b. Aj v prípade, že autentifikácia je z kompromitovaného klienta
    c. Aj v prípade, že autentifikácia je s kompromitovaným heslom

85. Ktorý z nasledovných webových prehliadačov nie je zameraný na ochranu súkromia:
    a. Brave
    b. Internet explorer
    c. Tor browser bundle
86. Ktorý z nasledovných doplnkov neslúži na ochranu súkromia:
    a. HackBar
    b. Privacy Badger
    c. Ghostery
87. Ktoré tvrdenie o logovacích záznamoch platí?
    a. Debug logovanie je nadmnožinou štandardného logovania
    b. Štandardné logovanie je nadmnožinou debug logovania
    c. Debug a štandardné logovanie sú ekvivalentné
88. Logovanie aplikácii je:
    a. štandardizované v Application logu v rámci Windows Event Logu
    b. štandardizované a zasielané protokolom syslog
    c. nie je štandardizované - každá aplikácia si rieši logovanie vlastným spôsobom
89. Polohu nevie telefón zistiť prostredníctvom:
    a. služby GPS
    b. odmeraním sily signálu okolitých Wifi sietí a porovnaním ich polohy voči databáze polohy Wifi sietí
    c. z obrazu snímaného kamerou a porovnaním voči databáze budov
90. Ktorá z nasledovných metód autentifikácie je príkladom biometrie použiteľnej na odomknutie mobilného telefónu:
    a. PIN
    b. geometria dlane
    c. face unlock

91. Stalkerware je:
    a. typ škodlivého kódu, ktorý špehuje obeť
    b. typ škodlivého kódu, ktorý zobrazuje reklamu
    c. typ škodlivého kódu, ktorý zašifruje súbory a požaduje zaplatenie výkupného
92. Ktorý z nasledovných typov nie je typom spôsobu práce bluetooth zariadenia?
    a. public
    b. personal
    c. private
93. Medzi typy párovania bluetooth zariadení patrí:
    a. Divide-and-conquer
    b. Select-and-confirm
    c. Seek-and-destroy
94. Medzi útoky na bluetooth nepatrí:
    a. Bluesniffing
    b. Blueborne
    c. Toothpulling
95. Čo je to IMEI mobilného telefónu?
    a. medzinárodné identifikačné alebo sériové číslo, vášho zariadenia
    b. jedinečné identifikačné číslo SIM karty
    c. ekvivalent IP adresy zariadenia v mobilnej sieti
96. Čo je to IMSI?
    a. medzinárodné identifikačné alebo sériové číslo, vášho zariadenia
    b. jedinečné identifikačné číslo SIM karty
    c. ekvivalent IP adresy zariadenia v mobilnej sieti
97. Rootkit umožňuje:
    a. plný prístup do cloudovej služby a k dátam všetkých používateľov
    b. plný prístup do operačného systému a ku všetkým funkciám mobilného telefónu
    c. plný prístup do siete mobilného operátora

98. Pred darovaním mobilného telefónu sa odporúča:
    a. označiť zariadenie ako stolen/missing v rámci antitheft
    b. spraviť zálohu dát a potom zmazať všetky citlivé dáta v mobilnom telefóne a nakoniec nastaviť telefón do továrenského nastavenia
    c. nainštalovať všetky aplikácie, ktoré majú za úlohu sledovať telefón a zabraňovať krádeži
99. Medzi typy SMS správ používaných pri útokoch nepatrí:
    a. klientske SMS
    b. podvodné SMS
    c. riadiace SMS
100. Medzi útoky na NFC patrí:
    d. XSS
    e. SQL
    f. jamming

8. Správne odpovede testov

1	B	21	B	41	A	61	A	81	B
2	C	22	C	42	C	62	B	82	C
3	C	23	B	43	C	63	C	83	B
4	A	24	C	44	A	64	B	84	C
5	A	25	C	45	A	65	A	85	B
6	A	26	A	46	C	66	A	86	A
7	C	27	B	47	C	67	C	87	A
8	A	28	B	48	B	68	A	88	C
9	B	29	B	49	B	69	C	89	C
10	A	30	A	50	B	70	B	90	B
11	B	31	B	51	A	71	B	91	A
12	A	32	A	52	B	72	B	92	B
13	C	33	A	53	C	73	A	93	B
14	A	34	B	54	B	74	C	94	C
15	A	35	C	55	A	75	C	95	A
16	A	36	B	56	B	76	C	96	B
17	A	37	A	57	B	77	A	97	B
18	B	38	A	58	B	78	B	98	B
19	A	39	B	59	B	79	B	99	A
20	B	40	C	60	C	80	C	100	C

9. Literatúra

9.1 Zoznam použitých kníh

Zeman, M. (2019): Odborná príručka pre učiteľa, Podporná literatúra pre didaktiku informačnej bezpečnosti pre 5 ročník ZŠ; Preventista.sk; ISBN: 978-80-972100-2-1 str. 23

KOLLÁR, Vojtech - POLAKOVIČ, Peter - GASPEROVÁ, Jana. Digitálna gramotnosť občana ako fenomén súčasnej informačnej doby. In Sustainability - Environment - Safety 2015. Medzinárodná vedecká konferencia. Sustainability - Environment - Safety 2015: recenzovaný zborník príspevkov z medzinárodnej vedeckej konferencie konanej 4. decembra 2015 v Bratislave. Žilina: STRIX, 2015. ISBN 978-80-89753-01-7, s. 137-140.

Matzler K., Bailom F. von den Eichen S.F., Anschober M. (2018): Digitálna disrupcia; Slovenská inovačná a energetická agentúra, Bratislava, ISBN 978-80-88823-67-4.

9.2 Odporúčaná literatúra

Holla K.(2016): Sexting a kyberšikana; IRIS

Meng W., Luo X., Furnel S., Zhou J. (2017): Protecting Mobile Networks and Devices, Challenges and Solutions; CRC Press

Venkata Krishna P., Gurumoorthy S., Obaidat S. M. (2019): Social Network Forensics, Cyber Security, and Machine Learning; Springer

Bostrom N. (2018): Superinteligence, Až budou stroje chytrejší než lidé; Prostor Praha

Tegmark M. (2017): Life 3.0, Being Human in the Age of Artificial Inteligence; Penguin Books

Tlačiarne

ForPress NITRIANSKE TLAČIARNE s.r.o. Nitra

Učebnica Informačnej bezpečnosti pre stredné odborné školy a gymnáziá

Prvá časť

ELEKTRONICKÁ KNIHA

Autori:

Mgr. Marek Zeman PhD. CRISC

Mgr. Miroslav Blšák

Ing. Jaroslav Oster

Mgr. Daniel Chromek CISA, CISM, CISSP, MBCI

Vydavateľ:

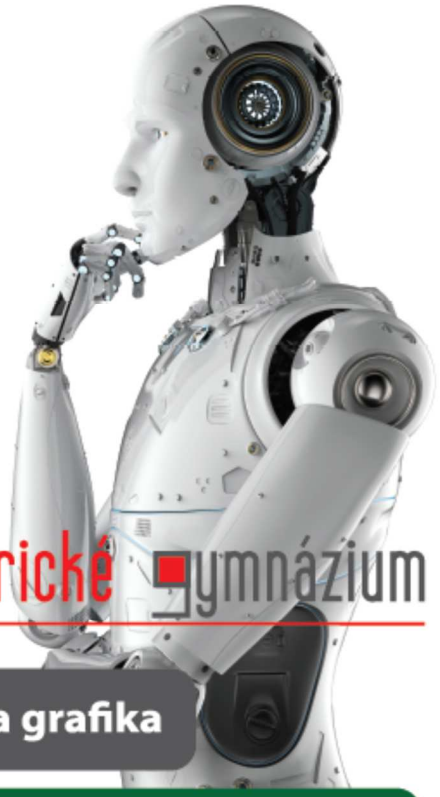
OZ Preventista - združenie pre bezpečnosť a prevenciu, 2021

1. vydanie

ISBN: 978-80-972100-6-9

EAN: 9788097210069

1. súkromné gymnázium Banskobystrické



1. súkromné Banskobystrické gymnázium

7902 J gymnázium - virtuálna grafika

7902 J gymnázium - kybernetická bezpečnosť

7902 J 74 bilingválne štúdium slovensko-ruské
možnosť študovať zameranie virtuálna grafika, alebo kybernetická bezpečnosť

7902 J 74 bilingválne štúdium slovensko-anglické
možnosť študovať zameranie virtuálna grafika, alebo kybernetická bezpečnosť

www.sukromnygympel.sk

I9BN: 978-80-972100-6-9
EAN: 9788097210069