Javni štipendijski, razvojni, invalidski in preživninski sklad Republike Slovenije

EVROPSKA UNIJA
EVROPSKI SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Univerza v Mariboru
Fakulteta za varnostne vede

Srednja tehniška in poklicna šola Trbovlje

Študentski inovativni projekti za družbeno korist 2016 – 2018

PSIVIM: Priporočilni sistem za informacijsko-varnostno izobraževanje mladostnikov

Seznam splošnih vsebin za informacijsko-varnostno izobraževanje

Rezultat R1

Študenti:
Nika Berčič
Domen Hribar
Lara Klemenc
Enja Kokalj
Iza Kokoravec
Suzana Kužnik
Ida Majerle
Aleš Ravnikar
David Sluga
Sara Tomše

Pedagoški mentorji:
dr. Igor Bernik
dr. Blaž Markelj
dr. Simon Vrhovec

Strokovni sodelavec:
dr. Uroš Ocepek

Ljubljana, september 2017

KAZALO

1 UVOD

V dokumentu se nahajajo informacijsko varnostne kompetence, s katerimi bomo preverjali znanje srednješolcev na področju informacijske in kibernetske varnosti. Kompetence smo pridobili iz projekta PKP - IVKZ in jih prilagodili glede na njihovo relevantnost in uporabnost pri srednješolcih. Vsaka posamezna kompetenca bo preverjala znanje srednješolcev na določenem področju in z različnimi vrstami gradiv poskušala prikazati njeno bistvo in pomembnost. Vsaka kompetenca je strukturirana po naslednji obliki: opis problema, prevencija, odziv ter zanimivosti in primeri. Nekaterim kompetencam manjkajo določene strukturirane točke, ker pri določenih kompetencah niso bile smiselne.

V sledeči tabeli se nahajajo vse kompetence, ki jih bomo uporabili v projektu. Kompetence so sprva poimenovane v slovenskem jeziku, nato se poleg nahaja angleška različica poimenovanja določene kompetence, sledi pa še njihova razlaga oz. opis.

1.1 Tabela kompetenc

Št.	IV kompetence	Opis kompetenc
1	**Razumevanje zakaj je varovanje informacij pomembno** *To understand why protecting information is important*	*Zavedanje pomembnosti dostopnosti, integritete in zaupnosti informacij za delovanje organizacije in s tem pomembnosti varovanja informacij*
2	**Razumevanje informacijsko-varnostnih trendov** *Understanding information security trends*	*Ažurnost na področju različnih vrst napadov, s poudarkom na poznavanju trenutnih trendov in njihovega gibanja.*
3	**Notranje nevarnosti** *Internal dangers*	*Zavedanje obstoja možnosti sabotaž in napadov s strani zaposlenih, pozornost na neavtoriziran dostop sodelavcev, povzročanje izpostavljenosti zaradi človeških napak.*
4	**Zunanje grožnje** *External threats*	*Zavedanje obstoja in prepoznavanje potencialnih nevarnosti, posledic zunanjih napadov ter nezgod na informacijsko infrastrukturo organizacije. Tu mislimo tako na načrtovane napade s strani posameznikov in/ali organizacij na eni strani ali npr. elementarnih nesreč v obliki višje sile na drugi strani.*
5	**Privlačne tarče** *Attractive targets*	*Zavedanje kateri deli informacijske infrastrukture in subjekti znotraj organizacije so najbolj privlačne ali najbolj ranljive tarče.*

6	**Sprejemanje etičnih odločitev** *Make ethical choices*	*Etične odločitve slehernega zaposlenega so premo sorazmerno povezane z zagotavljanjem katerekoli varnosti. Razumevanje pomembnosti etičnih odločitev in poznavanje resnosti posledic neetičnih odločitev, ki pogosto vodijo do groženj informacijski varnosti.*
7	**Pravilna raba informacijsko-varnostnih orodij in naprav** *Correct use of equipment and tools*	*Poznavanje in uporaba primerne opreme in metod varovanja informacij je ključnega pomena za preprečevanje varnostnih tveganj in soočanje z grožnjami in morebitnimi že nastalimi težavami. K pravilni rabi prištevamo tudi dejstvo, da ne uporabljamo piratskih kopij, ker lahko predstavljajo varnostno tveganje. Mlade je tudi potrebno poučiti o pravilni in varni rabi USB ključev.*
8	**Varovanje in delo s podatki** *Protecting and Handling Data*	*Mladi razumejo kako naj varujejo in upravljajo/rokujejo s podatki, da jih ne izgubijo, pokvarijo, nenamerno delijo ali kako drugače preprečijo dostop njim samim ali dovolijo dostop drugim osebam, katerim ga ne bi smeli.*
9	**Poznavanje principov zasebnosti** *Knowledge of Privacy Principles*	*Mladi se zavedajo pomembnosti svoje zasebnosti na spletu (še posebej na socialnih omrežjih), ter posledice, če le-to izgubijo in kaj morajo storiti, da do tega ne pride.*
10	**Prepoznavanje varnostnih incidentov** *Detect security breaches*	*Mladi opazijo/prepoznajo, da je njihova varnost/zasebnost ogrožena.*
11	**Razumevanje brezžičnih omrežij in njihove varnosti** *Understanding Wireless Networks and Security*	*Mladi imajo osnovno znanje o varni uporabi varnostnih protokolov brezžičnih omrežij ter kakšne so lahko posledice ob nepravilni, neustrezni ali pomanjkljivi rabi le-teh.*
12	**Razumevanje, uporaba in upravljanje varnih gesel** *Understanding password security*	*Mladi razumejo pomembnost močnih gesel ter posledice šibkih.*
13	**Oblikovanje varnih gesel** *Password design, usage and management*	*Mladi znajo sestaviti močno geslo ter vzdrževati varnost le-teh (ga ne delijo z drugimi, ga ne zapišejo ampak si ga zapomnijo itd.).*
14	**Varne prakse za delo z elektronsko pošto** *Secure e-mail practices*	*Osnovno poznavanje delovanja elektronskega sporočanja, ki ni nujno omejeno samo na elektronsko pošto in postopkov za varno uporabo aplikacij za elektronsko sporočanje in za manipulacijo z elektronskimi sporočili. Oseba je prepričana (hkrati se zaveda možnosti manipulacije), da so prejeta in poslana sporočila avtentična in ravna primerno.*
15	**Prepoznavanje vsiljenih in škodljivih elektronskih sporočil** *Unknown email sources and attachments*	*Osnovno poznavanje delovanja elektronskega sporočanja, ki ni nujno omejeno samo na elektronsko pošto in postopkov za varno uporabo aplikacij za elektronsko sporočanje in za manipulacijo z elektronskimi sporočili. Zavedanje ranljivosti in resnosti posledic pri ne-varni rabi elektronske pošte. Pozornost in upoštevanje predpisanih postopkov pri odpiranju elektronskih sporočil in priponk iz neznanih ali nenavadnih virov.*

16	**Znanje o namestitvi in uporabi antivirusnih programov** *Installing and using anti-virus software*	*Namestitev in pravilna uporaba antivirusnega programa, s poudarkom na rednem in sprotnem skeniranju prenešenih informacij.*
17	**Varna raba spletnega brskalnika in brskanja po spletu** *Secure browsing practices*	*Poznavanje najosnovnejših groženj, ki izhajajo iz uporabe interneta in delovanje v skladu s tem znanjem. Pomembno je, da mladostniki znajo uporabljati posodobljene, bolj varne brskalnike in da uporabljajo oz. prepoznajo HTTPS povezavo.*
18	**Sposobnost izogibanja in reagiranja na grožnje pri rabi spletnega brskalnika** *Identify online threats*	*Sposobnost pravilne identifikacije spletnih groženj, ki lahko ogrozijo informacijsko premoženje. Mladostniki morajo vedeti, kaj narediti, če so preusmerjeni oz. so se znašli na sumljivi spletni strani.*
19	**Varnost mobilnih naprav** *Mobile device security*	*Zavedanje potencialnih nevarnosti, ki jih predstavljajo naprave v osebni lasti, ki jih mladostniki s seboj prinesejo v šolo. Gre za pravilno uporabo zasebne IKT.*
20	**"Gledanje čez ramo"** *Shoulder Surfing*	*Preprečevanje fizičnega prestrezanja informacij, predvsem z zaslona, ki ga mladostniki v tistem trenutku uporablja.*
21	**"Brskanje po smeteh"** *Dumpster Diving*	*Zavedanje pomembnosti zaupnosti in integritete tudi tistih dokumentov, ki so bili zavrženi. Preprečevanje prestrezanja informacij zavrženih listin.*
22	**Preprečevanje napadov socialnega inženiringa** *Protecting against social engineering attacks*	*Socialni inženiring je ena najpogostejših tehnik zlorabe osebnih podatkov in sicer gre za nabor tehnik s pomočjo katerih napadalec od žrtve pridobi zaupne podatke z manipulacijo, prevaro ter zlorabo zaupanja. Obstaja več načinov, s katerimi napadalec pridobi podatke od žrtev: s tehničnimi metodami, osebnim stikom, grožnjami in izsiljevanjem. S pomočjo socialnega inženiringa ne prihaja le do kraje zasebnih informacij, pač pa tudi do kraje denarja ter identitet.*
23	**Varna raba socialnih omrežij** *Secure use of social media*	*Kibernetski kriminalci izkoriščajo nepoznavanje, lahkomiselnost in naivnost uporabnikov spletnih socialnih omrežij. Na spletnih socialnih omrežjih preži ogromno nevarnosti, kot npr. virusi, vdori v račune uporabnikov, kraje identitet, ribarjenje, izsiljevanje, nedovoljeno širjenje informacij in še mnoge druge.*
24	**Odzivanje na zaznane grožnje** *Responding to perceived threats*	*Če uporabnik uspe hitro prepoznati grožnjo ali nevarnost, ali pa se zna dovolj hitro odzvati, ko je že nastala, je to lahko ključnega pomena za zmanjšanje posledic oz. škode. Razumevanje in poznavanje postopkov, kako se odzvati, koga obvestiti oz. na koga se obrniti v takšnih primerih je izjemno pomembno in kritično.*
25	**Nevarnosti anonimnih omrežij** *Dangers of anonymous networks*	*Varna in pravilna uporaba anonimnih omrežij – omrežja Tor, njegovo delovanje ter nevarnosti, ki jih lahko prinese njegova uporaba. Zavedanje njegovih pozitivnih in negativnih vidikov.*

2 INFORMACIJSKO VARNOSTNE KOMPETENCE

2.1 Razumevanje, zakaj je varovanje informacij pomembno

OPIS PROBLEMA:

Zavedanje pomembnosti dostopnosti, integritete in zaupnosti informacij za delovanje organizacije in s tem pomembnosti varovanja informacij

Internetni oz. spletni kriminal iz leta v leto raste, zato je potrebno zavedanje, katere informacije in podatke kje hranimo, komu jih zaupamo in kaj se bo z njimi dogajalo. Zavedanje, da je vsako leto več virusov, targetiranih napadov, phishing napadov, napadov z zlonamerno kodo, računalniških vdorov (hekerji), napadov preprečevanja dostopa do storitev - Ransomware ali Denail of Service napadov ... Vse več napadov ima točno določen cilj (motiv), za dosego le tega lahko uporabijo tudi socialni inžinirig, zato je potrebno resno poskrbeti za varnost.

Nekatere informacije so bolj pomembne od drugih, zato je treba vedeti, zakaj je pomembna verodostojnost podatkov (zmožnost presoje takih informacij/ podatkov), zakaj morajo biti ti podatki resnični in točni, ter zavedanje posameznika, kako pomembne so točne informacije. Pomembno je zavedanje komu so informacije namenjene, zato je za določene informacije potrebna varnost na višji ravni.
Informacije obstajajo v različnih oblikah, lahko so tiskana ali zapisana na papir, shranjena elektronsko, poslana po pošti, poslana z elektronskimi sredstvi, povedana v pogovoru … v vsakem primeru in ne glede na obliko jo moramo zaščititi, predvsem zaradi preprečevanja izgube podatkov, razkritja podatkov, izgube zaupanja, osramočenja, napak pri upravljanju ...

Zavedanje, da ne more vsak dostopati do vseh informacij, ampak samo do nekaterih, je velikega pomena.

PREVENCIJA:

S stalnimi prilagoditvami, posodobitvami in izobraževanji vzdržujemo pripravljenost na različne načine napada. Spremljanje različnih spletnih strani (varni na internetu, Sicert, Arnest, safe.si, Kaspersy, McAffe …), ki opozarjajo na aktualne napade, spremljajo razvoj različnih škodljivih programskih kod, izobražujejo, so odlično orodje prevencije. Z nameščanjem posodobitev odpravimo znane varnostne luknje/ pomanjkljivosti.
Ustvarjanje varnostnih kopij na dobro zaščitenih napravah in (spletnih) aplikacijah, nam v primeru vdora v računalnik ali telefon varujejo in hranijo pomembne podatke, slike, informacije, ki jih napadalec ne more izbrisati ali do njih dostopati.

ODZIV NA INCIDENT:

Kar se da hitro sistem izklopimo iz omrežja, če lahko naredimo takoj varnostne kopije, pregled kaj se nam je zgodilo in kako, obvestimo SI-CERT, ki je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Ter o dogodku obvestimo najbližje, saj bo informacija pri njih delovala preventivno.

ZANIMIVOSTI / PRIMERI:

What is your pasword? - https://www.youtube.com/watch?v=opRMrEfAIiI

2.2 Razumevanje informacijsko-varnostnih trendov

Ažurnost na področju različnih vrst napadov, s poudarkom na poznavanju trenutnih trendov in njihovega gibanja.

OPIS PROBLEMA:

Spremljanje in poznavanje novic o nevarnostih in ranljivosti na internetu. Zavedati se moramo, da smo uporabniki najšibkejši v trikotniku napadalec - splet - uporabnik, da ne govorimo še o tem, da napad prepoznamo prepozno. Kako se pri napadu odzovemo in kaj lahko v zgodnji fazi preprečimo, da bi se napad odvil, lahko sklepamo, če poznamo trende napadov. Spremljanje le tega nam, lahko pripomore k bolj poglobljenem razmišljanju o tem, kakšne naprave kupujemo. Vemo, da je bilo leto 2016 leto Interneta stvari (ang: Internet of things), prav tako pa vemo, da je bilo leto 2016 leto Ransoware napadov. Najbolj znan Ransomware napad se je zgodil letos februarja, ko je v Sloveniji nehala delati proizvodnja v Revozu, a več o tem kasneje. V primeru, da bi se sistemi posodobili iz "starih" Windows XP na novejše: Windows 7, 8, 8.1, ali 10, do takih razsežnosti napada ne bi prišlo.

PREVENCIJA:

Če se zavedamo, zakaj je varovanje informacij pomembno, moramo spremljati informacijsko-varnostne trende, saj bomo le tako lahko zaščitili podatke pred nepooblaščenim vdorom. Določene aplikacije nam omogočajo, da izberemo več stopenjsko avtentikacijo. Avtentikacija je preverjanje ali je uporabnik, ki želi dostopati, res ta za katerega se izdaja da je. Eno geslo ni več dovolj, uporaba načina prijave z nekaj kar veš (uporabniško ime in geslo) ter nečim kar imaš (telefon na katerega dobiš enkratno geslo) postaja skoraj nuja, saj je težje priti do takšnih naprav. Razen, če je prišlo do vdora v napravo, ker naprave nismo pravilno zavarovali oz. je prišlo do brezglavega nameščanja različnih okuženih aplikacij.

Prav tako je pomembno, da za geslo uporabljamo velike in male črke, znake in številke.Povezavo v razdelku Zanimivosti in primeri nam demonstrira, kako težje je razbiti geslo z več različnimi znaki.

Glede na to, da se uporabi interneta stvari skoraj ne moremo več izogniti, si je pametno o izdelku prej kaj prebrati. Kam shranjuje naše podatke in komu jih pošilja, kako dostopamo do sistema, kako izbrišemo stvari in seveda če se te stvari res izbrišejo. Zavedanje da se s povezavo naprav, da izvesti dober DoS (ang: *Denial Of Service*) ali zavrnitev storitve ali DDoS napad (ang: *Distributed Denial of Service*) ali porazdeljena zavrnitev storitve.

Prav tako se moramo naučiti, da odprt dostop do Wi-Fi povezave ni varen, saj obstaja čedalje več odprtih točk, namenjenim kraji gesel, podatkov in identitet. Vse, kar pošljete prek brezžičnega omrežja, je potencialno v nevarnosti.

Brezžični routerji oz. Usmerjevalniki so postali zelo poceni, nekatere osnovne modele lahko kupite za samo nekaj 10 evrov. Ko ga doma priključite na modem, router največkrat dela, ne da bi bilo potrebno karkoli posebej nastavljati. Najti morate samo ime brezžičnega omrežja ter geslo za dostop, vendar včasih pa tudi vpis gesla ni

potreben. Pa je tako postavljeno omrežje varno? Če vam ni potrebno vpisati gesla za dostop do brezžičnega omrežja (imate t.i. odprto omrežje), to pomeni, da ga tudi napadalcu, ki se nahaja v dosegu usmerjevalnika ni potrebno vpisati.

Na kratko, potrebujemo aktiven požarni zid, posodobljen antivirusen program in stalne posodobitve.

ZANIMIVOSTI IN PRIMERI

Upam da ne bodo preverjali svojih gesel, ampak samo za prikaz, kako se vse spremeni, če dodamo veliko začetnico, znak - kakšen znak, številko - https://howsecureismypassword.net/ / http://www.passwordmeter.com/

https://vimeo.com/221408431 - kako ustvarimo dobro geslo

Your Samsung SmartTV is watching and listening you, sending your words to third paries.

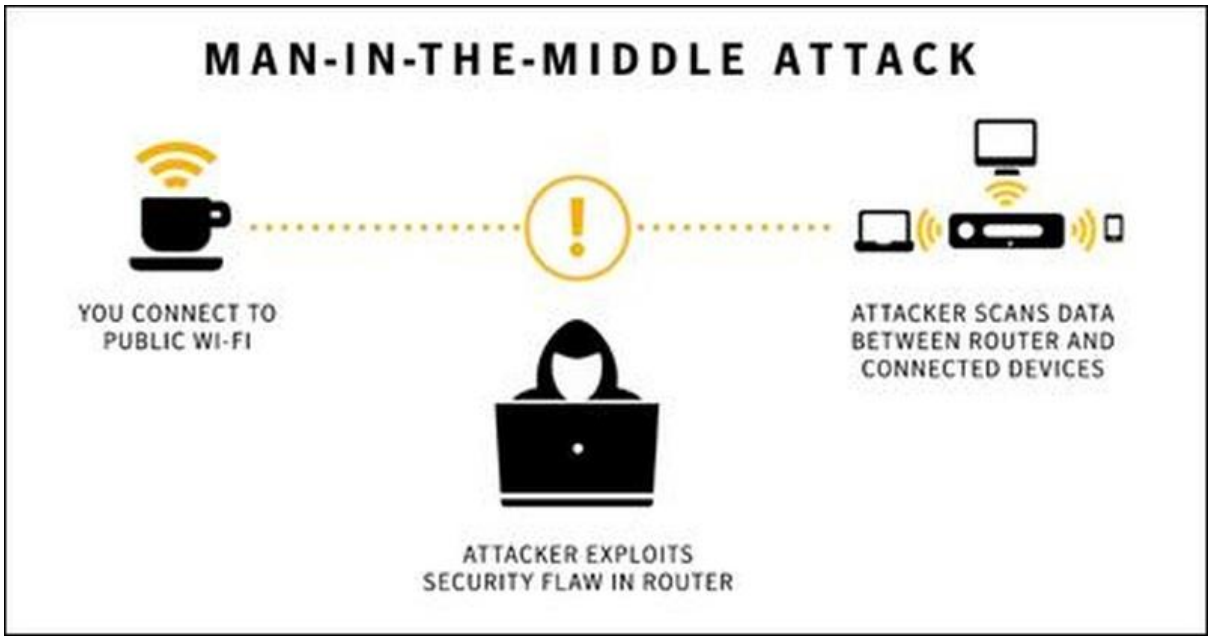
Pri Samsungu so povedali, da je del funkcije prepoznave govora, nadzor gibanja in tehnologija za prepoznavanje obrazov, zbirala in pošiljala podatke ali slike za izboljšanje storitev. Politika zasebnosti, objavljena na spletnem mestu Samsung, pravi,

da če omogočite uporabo funkcije prepoznave govora, lahko pride do tega da bodo nekateri glasovni ukazi poslali (poleg podatkov o svoji napravi, vključno z identifikatorji naprav) do tretjih naprav, ki pretvarjajo govor v besedilo, v obsegu, ki je potreben za zagotavljanje funkcij za prepoznavanje glasu. Poleg tega lahko Samsung zbira in vaša naprava lahko zajame glasovne ukaze in pripadajoča besedila, z namenom da lahko zagotovimo funkcije za prepoznavanje glasu in ovrednotimo in izboljšujemo funkcije. Upoštevajte, da v primeru, da vaše izgovorjene besede vsebujejo osebne ali druge občutljive podatke, bodo te informacije prav tako med podatki, ki jih boste posneli in posredovali tretjim osebam prek vaše uporabe prepoznavanja glasu. Če želite izbrisati shranjeno sliko, obiščite ustrezni meni z nastavitvami.

Samsung je uporabnikom omogočil, da odstopijo od funkcije, če uporabniki želi popolno zasebnost. Samsung omogoča uporabniku, da te funkcije onemogoči kadarkoli, čeprav je nesprejemljivo, da podjetje ni omenilo ničesar o praksah zasebnosti za tretje stranke, s katerimi bo delila vaše podatke.

Leta septembra in oktobra 2016 sta se zgodila dva večja DDoS napad v zgodovini, katerega so zakrivile prav pametne naprave IoT.


Bad guys can secretly monitor what sites you visit
Bad guys can steal your private information without you knowing


MAN-IN-THE-MIDDLE ATTACK
YOU CONNECT TO PUBLIC WI-FI
ATTACKER SCANS DATA BETWEEN ROUTER AND CONNECTED DEVICES
ATTACKER EXPLOITS SECURITY FLAW IN ROUTER

2.3 Notranje nevarnosti

Zavedanje obstoja možnosti sabotaž in napadov s strani zaposlenih, pozornost na neavtoriziran dostop sodelavcev, povzročanje izpostavljenosti zaradi človeških napak.

OPIS PROBLEMA

Dijakovo zavedanje, da svoje naprave ne prepušča drugim osebam, saj le-te lahko naredijo namerno, ali nenamerno veliko škodo. Pomembno je tudi, da je pozoren na svojo napravo, kdo dostopa do nje in kdo jo uporablja, če je to telefon, naj bo dijak pozoren, kaj drugi počnejo z njegovo mobilno napravo, ter, da se zaveda, da je napravo najbolje zaščititi pred posegi drugih.

Popolne zaščite ni mogoče doseči, lahko pa z nekaterimi ukrepi bistveno zmanjšamo tveganje. To lahko storimo tako, da določimo kakšna pooblastila ima določena oseba v informacijskem sistemu, tako, da ne pripadajo vsa eni, ampak, da se med osebami porazdeljujejo. Poleg tega pa moramo opravljati tudi redne varnostne kopije podatkov, ter te kopije tudi nadzorovati. Nadzorovati pa moramo tudi kdo in kako uporablja našo napravo, ter ostale uporabnike podučiti o pravilni rabi, če pri tem nismo prisotni.

Ko dijak neha uporabljati napravo, na kateri je bil in imajo do nje dostop tudi drugi, naj za seboj preveri, če se je odjavil iz vseh spletnih strani, pobriše naj datoteke (tudi iz koša!), preveri naj, če ni kje pustil svojih osebnih podatkov in šele nato odstopi od naprave.
Skoraj 40% vseh nevarnosti in napadov je notranjih. Najpogostejši so:

1. Zlonamerni napadi v kibernetskem prostoru - napadalci lahko uporabijo ta dostop zato, da odprejo “back doors” v računalniški sistem, ali pa pustijo v mreži razne programe, ki kradejo informacije. Zavarujemo se tako, da spremljamo osebe, ki bi izrabile svoj položaj in ob tem takoj prekinemo povezavo z internetom in spremenimo gesla, da do naših stvari ne morejo dostopati z oddaljenim dostopom
2. Socialni inženiring - svojih podatkov ne zaupajmo osebi, tudi če ji zelo zaupamo. Zato svojih gesel nikoli ne zaupajmo nikomur prek telefona, potrebno pa je tudi znanje prepoznavanja phishing e-mailov, ki so lahko na zelo osebni ravni.
3. Prenašanje zlonamerne internetne vsebine - v vsaki igri ali video posnetku je lahko skrita nevarnost, ki pa se je malokdo zaveda. Najboljše je, da konstantno posodabljamo sistem in antivirusne programe, da zagotovimo potrebno zaščito.
4. Uhajanje informacij - veliko je možnosti, da so informacije “ukradene”, bodisi jih je nekdo prekopiral na CD-ROM, fotoaparat ali pa jih je prenesel prek USB ključa. Pomembno je tudi zaščititi brezžično povezavo, tako Wi-Fi, kot tudi Bluetooth povezavo.

Slaba notranja varnost pomeni, da bo zunanji napadalec ob uspešnem napadu na zunanje servise avtomatično pridobil pravice tudi za notranji dostop do pravih podatkov.

ODZIV NA INCIDENT:

Iskanje varnostne luknje in popravitev le tega. Odvisno od posameznika in organizacije.

PREVENCIJA:

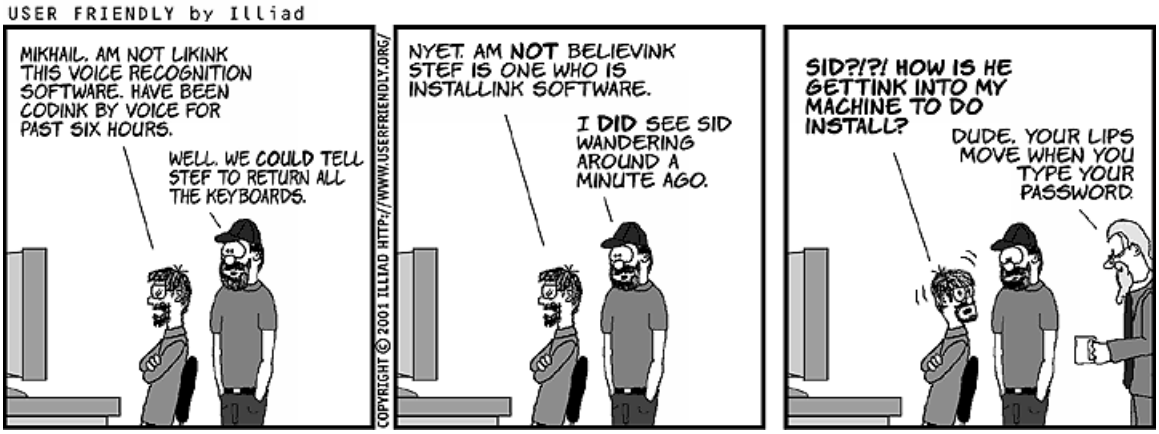
Zavedati se je potrebno komu smo zaupali svoje pin števila oz. katero od gesel za dostop do telefona, e-maila, facebooka, spletne učilnice… Če kje najdemo kakšen USB ključek, ga nesmemo uporabljati ali gledati kaj je gor, saj obstaja velika verjetnost da je okužen, še posebej če smo ga našli na kakšnem pakirišču pred šolo, poslovno stavbo, podjetjem… Vedno uporabljamo varno internetno povezavo na šoli in doma. Veliko ljudi ali podjetji se poslužuje napadov s socialnim inženiringom (phishing mail, okužen USB ključek ipd.) in tako pridobijo neposredno kontrolo nad delovno postajo ("notranjega") uporabnika. Torej, uspešno se moramo braniti oz. uvideti osebo, ki bi lahko uporabila socialni inženiring za pridobitev dostopa. Seveda je potrebna tudi osnovna zaščita pred zlonamernimi datotekami, osnovna varnostna politika gesel (na koliko časa zamenjamo geslo, kakšno mora biti geslo - koliko znakov, velike in male črke, številke…), posodobitev starih operacijskih sistemov na nove.

- http://www.smart-com.si/2016/08/18/kako-tipicna-podjetja-dovzetna-za-varnostne-pomanjkljivosti/

ZANIMIVOSTI IN PRIMERI:

Uporaba socialnega inženiringa - https://www.youtube.com/watch?v=lc7scxvKQOo

Kako shekati življenje - https://www.youtube.com/watch?v=F78UdORll-Q



Social Engineering

by Nagasahas

2.4 Zunanje grožnje

Zavedanje obstoja in prepoznavanje potencialnih nevarnosti, posledic zunanjih napadov ter nezgod na informacijsko infrastrukturo organizacije. Tu mislimo tako na načrtovane napade s strani posameznikov in/ali organizacij na eni strani ali npr. elementarnih nesreč v obliki višje sile na drugi strani.

OPIS PROBLEMA

Dijakovo zavedanje potencialnih nevarnosti in posledic zunanjih napadov na njegove naprave, ali na naprave, ki jih uporablja. Dijak naj poskrbi, naj bo naprava dobro zaščitena pred vplivi višjih sil, ali pa pred napadi drugih posameznikov.

Ena od zunanjih groženj so tudi tiste osebe s katerimi dijak nima ravno najboljšega odnosa, saj nikoli ne vemo kako bodo reagirali ob različnih priložnostih, ki se jim bodo pojavile, pa naj si bo to napad na informacijsko tehnologijo (telefon, računalnik) ali z grobo silo.

Pred zunanjimi grožnjami se veliko lažje obvarujemo kot pred notranjimi, poleg tega pa jih je tudi veliko lažje odkriti. Med zunanje grožnje štejemo človeške napade, kjer napadalec poskuša vdreti v naš sistem in vanj vgraditi različne viruse in drugo zlonamerno programsko opremo. Ti napadi so zelo počasni, zato so se razvile tudi hitrejše metode, to so avtomatizirani napadi na sistem, ki pa imajo na našo srečo zelo veliko propadlih in neuspelih poizkusov.

PREVENCIJA:

Paziti je potrebno od koga kupuje stvari, naj si bo to rabljen telefon ali računalnik ali tablica.

Če kupujemo rabljeno opremo, je dobro da jo najprej damo računalničarju, da napravo najprej ponastavi na tovarniške nastavitve oz. »sformatira« ter na novo naloži originalno programsko opremo.

Poglejmo še iz druge strani, ko smo prodajalec mi, je potrebno bit pozoren komu prodajamo svoje rabljene stvari. Kadar se odločimo za prodajo svojih naprav, jih najprej ponastavimo na tovarniške nastavitve oz. »sformatiramo« ter nekajkrat prepišemo disk z nepomembnimi zadevami, da v primeru, da našo napravo dobi kakšen hacker, težje dostopa do pomembnih podatkov. Preveriti moramo ali smo izpisani iz vseh aplikacij, ali imamo narejene back-upe podatkov…

Prav tako moramo biti pozorni na to, kakšne aplikacije nalagamo in iz kje.

ZANIMIVOSTI IN PRIMERI

V obdobju popularnosti vsem znane igre Pokemon go, so se napadalci domislili boljšega načina da pridejo do mobilnih naprav - pripročnik za igranje te igre. Guide for pokemon go, je

si je naložilo več kot pol milijona ljudi po svetu, predno so ugotovili, da je datoteka okužena. Napad je izgledal tako, da je začel ponujati ogromno reklam. Ko se je enkrat namesti, je pričel z nameščanjem še več okuženih datotek na mobilno napravo.

Varni na internetu:

- Ukraden ali izgubljen android https://www.varninainternetu.si/2017/ukraden-ali-izgubljen-android/
- Ukraden ali izgubljen iPhone: https://www.varninainternetu.si/2017/ukraden-ali-izgubljen-iphone/

2.5 Privlačne tarče

Zavedanje kateri deli informacijske infrastrukture in subjekti znotraj organizacije so najbolj privlačne ali najbolj ranljive tarče.

OPIS PROBLEMA:

Zavedanje dijakov, kakšna oseba je lahko tarča, ki privablja napadalce - bodisi je to oseba, ki bi lahko ponudila informacije, oseba, pri kateri bi lahko iztržili čim več denarja, ali pa oseba, ki bi bila izpostavljena pedofiliji ali nagovarjanju goljufov prek družabnih omrežij. Dijak naj bi to prepoznal in se ustrezno zaščitil pred tem, poleg tega pa bi prepoznal dele informacijske infrastrukture so najbolj ranljivi (spletne strani, aplikacije, ostali programi).

Naša največja napaka je, da si vseskozi govorimo in verjamemo, da za naše podatke ne bi bil zainteresiran nihče, zato tudi ne posvečamo posebne pozornosti zaščiti naših podatkov, kar nas naredi privlačne tarče za napade.
Največkrat se med tarčami za napad pojavljajo spletne aplikacije, saj jih je veliko lažje "shekati", kot pa operacijske sisteme ali routerje, omogočajo pa tudi veliko priložnosti, da pridejo v posameznikovo omrežje, saj lahko pozameznik do njih dostopa skozi kateri koli brskanik ali katerokoli internetno povezavo. Prek takšnih aplikacij se zgodi več kot 60% poskusov kibernetskih napadov, več deset tisoč spletnih strani pa je ciljanih in hackanih vsak dan. Ko je spletna stran "prebita", omogoča hekerjem, da dostopajo do podatkov, datotek in ključev za dešifriranje.

PREVENCIJA:

Privlačne tarče lahko obvarujemo tako, da uvedemo ciljno utrjevanje. S tem lahko privlačnost tarče povečamo ali zmanjšamo. Grožnje tako lahko analiziramo glede na pet faktorjev:

- Obstoj: kdo je sovražen do premoženja, organizacije ali skupnosti
- Sposobnost: kako so se odvijali pretekli napadi, kaj je bilo pri njih uporabljeno
- Zgodovina: kakšen je bil element ogroženosti v preteklosti in kolikokrat se je to že zgodilo
- Namen: kaj bi potencialni napadalec lahko dosegel
- Ciljanje: ali vemo, da napadalec že izvaja nadzor nad nami ali podobnimi, s katerim si delimo veliko lastnosti

Poznavanje tega, da lahko pričakujemo nevarnost nam omogoča, da to znanje uporabimo in vključimo k specifičnim informacijam spletnih strani in naredimo oceno grožnje.

Ocena grožnje je globinska analiza slabosti s katero lahko uvedemo izboljšave z namenom zmanjševanja ranljivosti. Pri tem se mora pregledati, katere ranljivosti aplikacije napadajo omrežje in je bila zaznana zlonamerna programska oprema, pogledati pa moramo tudi katere naprave so v območju tveganja.

Stvari, ki jih je dobro preveriti, da se izognemo napadu:

- ali imam kakšne občutljive ali osebno prepoznavne podatke, če jih imam, ali jih moram obdržati?
- kdo ima dostop do tvojih informacij in vpisnih podatkih, do kakšnih podatkov imam dostop?
- kako močno je vaše šifriranje podatkov
- ali so naloženi najnovejši načrti zasebnosti in varnosti podatkov, ter, če so te v skladu z zakoni?
- ali imamo shranjene kopije podatkov, katere bi še vedno lahko uporabljali v primeru napada

ZANIMIVOSTI/PRIMERI:

Če napadalec ugotovi uporabniško ime in geslo, lahko dostopa do aplikacij za nalaganje programov ter spremljanje tipkovnic. Na ta način lahko ugotovi dostop do bančnih računov, kjer lahko prenakažejo denar, do storitev iCloud, Google Drive, Dropbox, kjer lahko dostopa do občutljivih podatkov. Lahko dostopa do uporabniških računov za spletne nakupe, GLS, Pošta Slovenije, kjer lahko preusmeri pošiljke k sebi.

V primeru da ugotovi dostop do e-maila, lahko pride do imen, e-mail naslovov in telefonskih številk vseh ki jih imaš v imeniku, seveda lahko dostopa tudi do podatkov in celo do službevenga e-maila (če ga seveda).

Če kdo spremlja, kupuje, prenaša virutalne dobrine, lahko s pravilnim dostopom pride do uporabniškega računa ter tako dostopa do online igralniških računov, do katere koli licence za software, opreacijske sisteme ali igralniških licenc.

Ko so uspeli vdreti v računalnik, lahko le tega povežejo v celoten sistem “shackanih” računalnikov, ki so pod nadzorom kibernetksih kriminalcev. To omrežje se imenuje botnet in se uporablja za pošiljanje spam pošte več miljonom ljudi ali pa za izvajanje Denial of Service napadov.

Napadalci lahko pridejo tudi do naše digitalne identitete in jo, ali uporablja ali pa proda naprej. Digitalno identiteto lahko pridobi na Facebooku, Twitterju ali Linkedin profilu, preko e-mail accounta ali celo preko Skype in drugih aplikacij.

Računalnik lahko postane spletni server, katerega napadalci uporabljajo za gostovanje phishing spletnih strani, preko katerih pridobijo uporabniška imena in gesla, lahko hranijo orodja s katerimi izvajajo napade na računalnike drugih uporabnikov, lahko prepošiljajo otroško pornografijo, piratske verzije video in glasbenih vsebin.

V primeru da se na računalniku ali telefonu uporablja dosto do spletne banke, lahko z pravilnim pristopom pridobijo informacije o kreditni kartici, podatke o transakcijah, investicije, vsoto denarja …

Izsiljevanje, ko je računalnik enkrat okužen z izsiljevalskim virusom lahko zahtevajo denar v zameno za odklep računalnika. Preko spletne kamere lahko zajema slike, s katerimi lahko izsiljuje, da jih bo dal javno dostopne v zameno za denar. Z orodjem naredi pregled vseh obiskanih spletnih strani in izsiljuje da bo vse pokazal.

2.6 Sprejemanje etičnih odločitev

Etične odločitve slehernega zaposlenega so premo sorazmerno povezane z zagotavljanjem katerekoli varnosti. Razumevanje pomembnosti etičnih odločitev in poznavanje resnosti posledic neetičnih odločitev, ki pogosto vodijo do groženj informacijski varnosti.

OPIS PROBLEMA

Dijakovo razumevanje, kako lahko z vsako svojo odločitvijo pripomore k informacijski varnosti, ter kako pomembno je, da sprejema prave odločitve. Pomembno je tudi njegovo poznavanje posledic sprejetja napačnih odločitev in kako se lahko temu izogne. Tako ne zagotavlja le informacijske varnosti, temveč poskrbi tudi za ostalo varnost.

Etika je sistem vrednot, ki vplivajo na delo in obnašanje posameznika, izhajajo pa iz naše morale, ki se kaže v kulturi in socialnih vezeh, ter iz uradno sprejetih zakonov. Je osebnostna lastnost posameznika, s katero lahko ločimo med tem kar je prav in kar je narobe. Na področju informacijske varnosti je telo pomembno, da posameznik dobro pozna delovanje varnostnih mehanizmov informacijskega sistema, da ve, da dostopa do zaupnih informacij, ter, da ve, da njegove odločitve vplivajo na to, ali bodo te informacije varne pred javnostjo. Veliko pozornosti se posveča zaščiti virov in podatkov v primeru neavtoriziranega namernega napada vpada v sistem, kar največkrat označujemo z besedo hekanje (uporaba računalniških spretnosti z namenom pridobitve nepooblaščenega dostopa do računalniških virov). Hekerji pa se opravičujejo tako, da govorijo, da v bistvu ne delajo nikakršne škode in imajo pozitiven doprinos, saj naredijo nekatere podatke v korist vseh, dostopne. S hekanjem pa odpravijo tudi varnostne luknje in posredno izboljšajo sisteme. To vse povzemajo v tako imenovani "Etiki hekerjev", na katero naj bi se opirali. Opisuje, da naj bi vsi imeli neomejen in celoten dostop do računalnikov in do vsega, kar nas lahko nauči kako svet deluje, vse informacije bi morale biti prosto dostopne, promovirajo decentralizacijo, hekerji bi morali biti videni glede na njihovo hekanje, ne pa glede na kriterije izobrazbe, starosti, let ali njihovega položaja, da se na računalniku lahko izdela umetnost, ter zadnja, da računalniku lahko spremenijo tvoje življenje na boljše. Vendar prihaja do navzkrižij glede prosto dostopnih informacij, saj tako tisti, ki so avtorji dokumenta ali posedujejo pomembne informacije, katere so ugotovili sami, ne bi imeli možnosti tega obdržati le zase ali pa z informacijo zaslužiti. To pa bi zelo posegalo v posameznikovo zasebnosti, informacije pa ne bi bile več točne, saj bi jih lahko vsakdo, ki bi do njih dostopal, spreminjal in dodajal svoje mnenje.

Zelo pomembno je, da osebe, ki so odgovorne za posamezni računalnik zagotavljajo pravilnost, zanesljivost, dostopnost in varnost informacij in informacijskega sistema. Moralni vidik pa se kaže predvsem v zanesljivosti, kjer lahko različne odločitve zaščitijo posameznika, po drugi strani pa mu lahko naredijo tudi veliko škode in kršijo

njegove moralne pravice. Dandanes je veliko poudarka na posameznikovi pravici do zasebnosti, saj imamo tako pravico zaščititi informacije o sebi pred drugimi ljudmi. Tako nas nemalokrat varuje pred zunanjimi grožnjami, ki vsebujejo izsiljevanje, kraje, nadlegovanje, manipulacijo in izključitev. V primeru sprejemanja nepravih odločitev, bodisi naših, ali drugih, pa lahko naše zaupne informacije uidejo zasebni sferi in postanejo javne. Da bi se temu izognili, se pogosto pojavljajo etične kode ali kodeksi, obstajajo pa tudi posebna usposabljanja za etično odločanje, da se lahko prepozna etična vprašanja in dileme med delom, ter, da se zavaruje naprave in ljudi.
Splošna priporočila računalniške etike:

1. Ne uporabljaj računalnikov, da bi škodoval drugim.
2. Ne vmešavaj se v delo drugih.
3. Ne dostopaj do tujih datotek brez dovoljenja.
4. Ne uporabljaj računalnika za krajo.
5. Ne uporabljaj računalnika za laganje.
6. Ne uporabljaj ilegalnih kopij lastniške programske opreme.
7. Ne uporablja tujih računalniških virov brez nadomestila.
8. Ne prisvajaj si tuje intelektualne lastnine (intelektualnih izdelkov)
9. Premisli o socialnih posledicah sistema ali programov, ki jih pišeš (proizvajaš).
10. Pri uporabi računalnika vedno bodi obziren in spoštuj druge ljudi.

ZANIMIVI PRIMERI:

- http://siol.net/digisvet/novice/slovenija-med-prvimi-s-smernicami-za-varstvo-osebnih-podatkov-v-oblakih-239737
- https://www.youtube.com/watch?v=i-ywGYulbck
- intervju z g. Milanom Gabrom ali Boštjenom Špehonja (etična hekerja) - za kakšno zanimivo prigodo

2.7 Pravilna raba infomacijsko-varnostnih orodij in naprav

Poznavanje in uporaba primerne opreme in metod varovanja informacij je ključnega pomena za preprečevanje varnostnih tveganj in soočanje z grožnjami in morebitnimi že nastalimi težavami. k pravilni rabi prištevamo tudi dejstvo, da ne uporabljamo piratskih kopij, ker lahko predstavljajo varnostno tveganje. Dijake je tudi potrebno poučiti o pravilni in varni rabi USB ključev.

OPIS PROBLEMA:

Dijakovo zavedanje, da je poznavanje in uporaba primerne opreme in metod varovanja informacij ključnega pomena za preprečevanje varnostnih tveganj in soočanje z grožnjami in že nastalimi težavami. K pravilni rabi, bi šteli, da dijak ne uporablja piratskih kopij saj le te lahko predstavljajo varnostno tveganje, zraven pa bi šteli tudi njihovo pravilno rabo USB ključev (da ne vtikajo tujih USB ključev v svoje računalnike, če niso prepričani, kakšno vsebino vsebujejo).

Okužen USB ključ ali druga nepoznana naprava, ki jo priklopimo na naš računalnik nam lahko namesti zlonamerno programsko opremo, kot na primer Trojanske konje, ali pa opremo za krajo informacij. Lahko nas tudi samo preusmerijo in avtomatsko odprejo spletno stran, kjer se nahaja zlonamerna vsebina, ki pa po intenziteti ni nujno samo taka, ki nas le spravlja ob živce, ampak tudi taka, ki nam povzroči trajnejšo škodo. Socialni inženiring cilja na našo radovednost, saj hočemo ugotoviti kaj je na napravi, bodisi le zato, da bi to napravo vrnili prvotnemu lastniku.

Zelo pomembna je tudi zaščita našega računalnika, za katero skrbijo antivirusni programi. Nekaj teh programov je za osebno rabo brezplačnih (360 Total Security, Avast, AVG Antivirus, Avira AntiVir, Comodo Antivirus..), nekateri pa so plačljivi (Bitdefender, Kaspersky Antivirus, McAfee, Nod32, Norton Antivirus, Microsoft Security Essentials, Sophos…). Tako ti programi delujejo v ozadju in skenirajo vsako datoteko, ki jo odpremo. V času, ko mi odpiramo datoteko, jo antivirusni program primerja z že znanimi virusnimi paketi, pregleda pa tudi program pred morebitnimi novimi oblikami virusov.

PREVENCIJA:

Najpomembnejša stvar je, da nepoznanih naprav ne prikljapljate na svoj računalnik, sploh, če najdete USB ključ na javnem prostoru. Pomembna je tudi raba varnih USB-jev, nekateri novejši modeli imajo tudi nameščeno zaščito s prstnim odtisom, kar pomaga ščititi napravo pred nepridipravimi. Naprave tudi ni dobro uporabljati na dveh ali več računalnikih (šolskem in domačim), saj se tako lahko naprave, tako ena ali druga, okužijo z nevarno programsko opremo. Pozorni pa moramo biti tudi pri kupovanju naprav za prenos podatkov, da jih ne kupujemo

pri tretje razrednih prodajalcih, kjer obstaja velika verjetnost, da so nanje namestili zlonamerno programsko opremo. Na svojem računalniku nameščajte vse najnovejše varnostne posodobitve. Čeprav jih nihče ne mara, so ključnega pomena za varnost računalnika, saj odpravijo šibkosti in ranljivosti. Prisotnost antivirusne opreme je zelo pomembna pri varnosti našega računalnika, saj smo ob uporabi okuženega zunanjega diska ali USB-ja v neki meri zaščiteni, varuje pa nas ne samo pred okuženimi datotekami na prenosnih napravah, ampak tudi pred drugo zlonamerno vsebino.

Če pa bi vseeno radi pogledali, kaj se nahaja na napravi, pa to lahko varno storimo tako, da prenesemo LiveCD Linux in ga zapečemo na CD ali DVD (nikakor ne na USB), odklopimo vse trde diske, če res nočemo nikakršne okužbe, zaženemo Live Linux, šele nato priklopimo USB napravo v računalnik in preberemo datoteke.

ODZIV NA INCIDENTI:

Preden sploh pride do takega incidenta se lahko zavarujemo, ter onemogočimo avtomatsko branje na USB ključu ali prenosni napravi, ki se po navadi zažene takoj, ko priklopimo napravo in razširi virus na računalnik.

1. To lahko onemogočimo tako, da kliknemo na “Start”, izberemo “Nadzorno ploščo”. Tam izberemo “Strojna oprema in zvok” in nato “Samodejno predvajanje”. Odkljukamo “Uporabi samodejno predvajanje za vse medije in naprave” in nato shranite svojo izbiro s klikom na gumb “Shrani”.
2. Ko priklopimo napravo, v iskanju vpišemo “CMD”, pritesnemo “Enter” in odpre se ukazni poziv.
3. Nato tja napišemo črko pogona, kamor smo napravo vklopili, in potrdimo svojo izbiro.
4. Napišemo “dir /w/a” in pritisnemo “Enter”. Tako se nam prikaže lista datotek, ki so na prenosni napravi. USB je okužen, če se na njem nahajajo datoteke: “Autorun.inf”, “Ravmon.exe”, “New Folder.exe”, “svchost.exe” ali “Heap41a”.

ZANIMIVOSTI/PRIMERI:

- https://www.varninainternetu.si/2013/izsiljevalski-virus-ki-zaklene-racunalnik/
- https://www.cert.si/si-cert-2012-13-ukash-virus/
- https://www.youtube.com/watch?v=uencT8VZ43s

How Antivirus Software Works:

2.8 Varovanje in delo s podatki

OPIS PROBLEMA

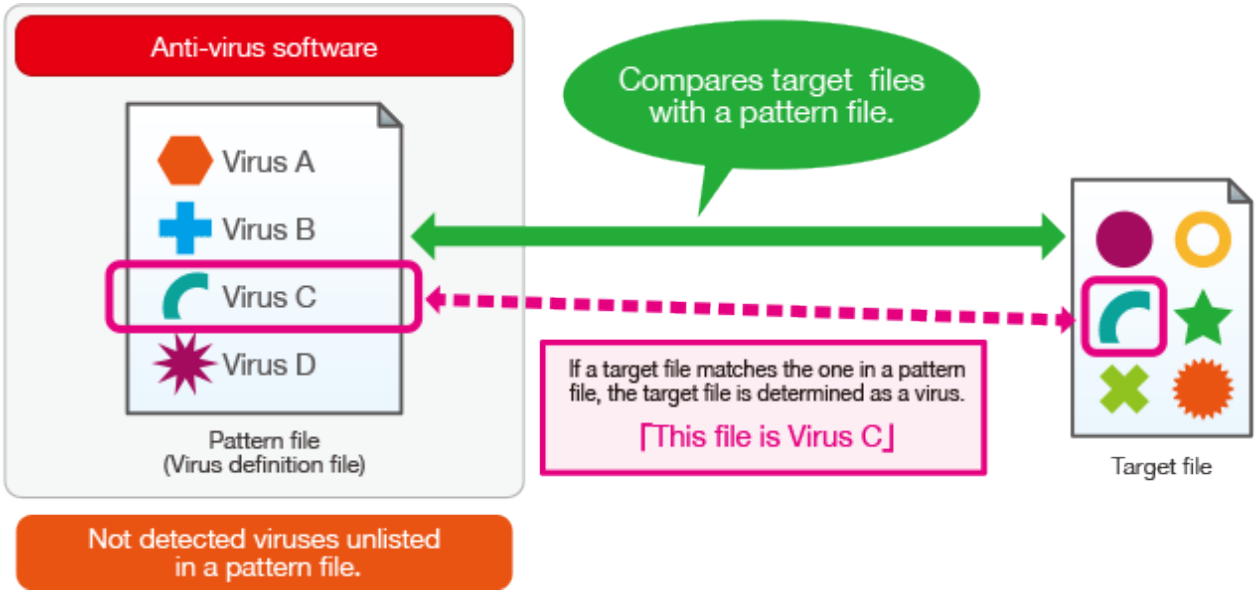
Informacijski sistemi predstavljajo tarčo za ljudi, ki vdirajo v sisteme. Napadalci to delajo zaradi koristoljubja ali zaradi osebnih izzivov. Uporabnik lahko poskuša preprečiti napade s tehničnimi rešitvami prav tako pa s pametnim ravnanjem na spletu.

PREVENCIJA

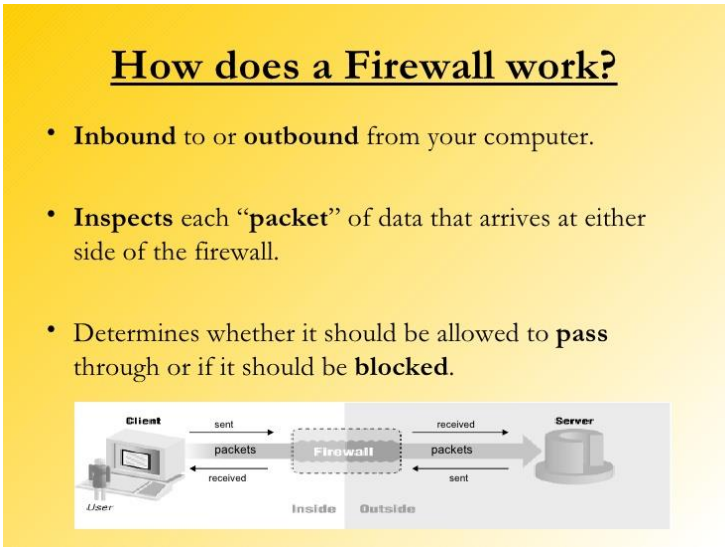
Antivirusni progam (protivirusni): je računalniški program, ki poskuša najti, izolirati, blokirati in uničiti viruse in drugo škodljivo programsko opremo. Protivirusni program pregleda datoteke, v katerih išče znane viruse, nato pa preveri sumljivo vedenje računalniških programov, ki bi lahko kazali na okužbo. In ena izmed prvih stvari, ki jo morate narediti za varnost vašega računalnika je, da ga zaščitite s protivirusnim programom.

Večina antivirusnih programov pravzaprav ponuja veliko več kot le zaščito pred virusi, temveč so že pravi paketi za zaščito, ki vsebujejo tudi požarni zid, protivohunske programe, filtre za nezaželeno pošto, filtriranje neprimerne vsebine, omejevanje časa uporabe interneta za otroke itn.

Današnji protivirusni programi večinoma omogočajo dopolnjevanje virusnih vzorcev prek interneta s pomočjo tehnologije t.i. samoposodobitve, kar uporabniku olajša skrb za redno posodabljanje. Pomembno je namreč, da uporabnik svoj protivirusni program redno dopolnjuje z novimi proti- virusnimi posodobitvami, saj se novi virusi pojavljajo vsak dan.



Požarni zid (ang. »firewall«): je poseben vmesnik (program ali strojna oprema), ki omejuje nepooblaščene dostope iz in v vaš domač računalnik. Požarni zid preveri vsak program in protokol, ki poskuša odpreti vrata v vašem računalniku. Požarni zid naredi vaš računalnik neviden za druge uporabnike interneta in tako vrata odpira le znanim, preizkušeno varnim programom/protokolom. Prav tako blokira odhodne povezave, ki jih niste sami sprožili.



Posodabljanje operacijskega sistema, brskalnikov, programov in aplikacij: ne posodobljeni sistemi predstavljajo varnostne luknje v informacijskih sistemih skozi katero lahko pridobimo viruse, vohunske programe in zlonamerne programe.

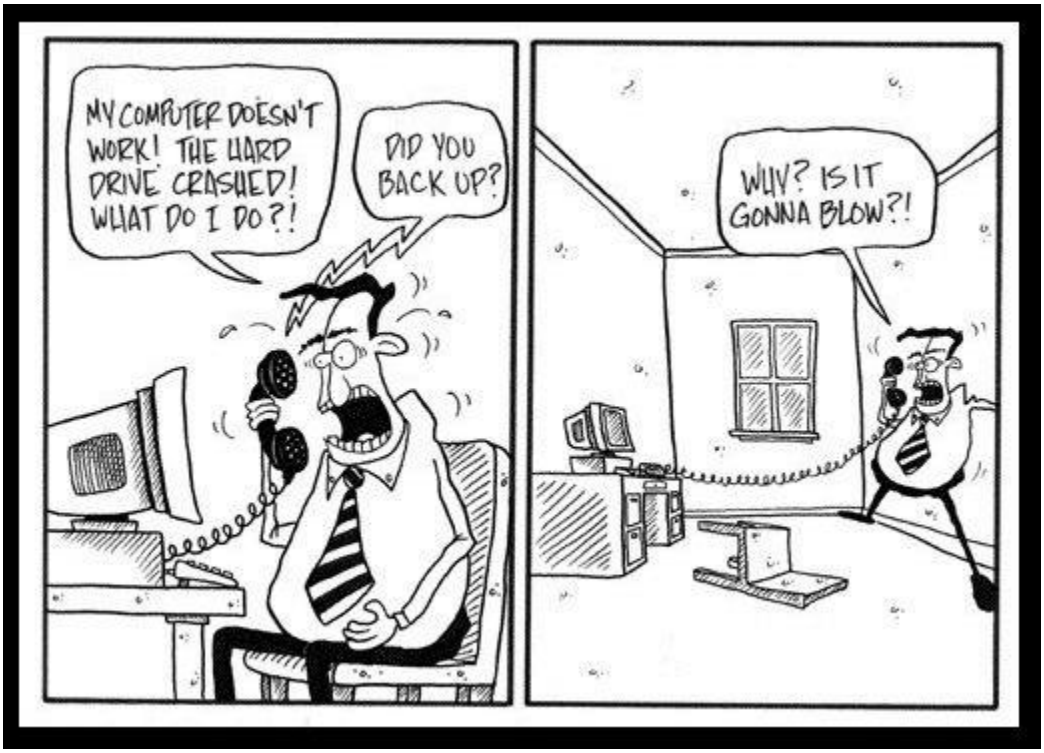
Šifrirano brezžično omrežje zaščiteno z geslom: lahko pride do prisluškovanja in prestrezanja prometa.

Antivirusni program na mobilni napravi: prav tako je morate zaščititi mobilno napravo, saj se čedalje več incidentov dogaja na le-teh.

Varna gesla: gesla morajo biti dolga in zasnovana iz različnih kombinacij znakov. Na nekaterih spletnih aplikacijah lahko uporabljate več-faktorsko avtentikacijo, katera zagotavlja večjo varnost. Izogibajte se uporabi enakih gesel na različnih spletnih aplikacij ter ga ne zapisujte in delite z ostalimi.

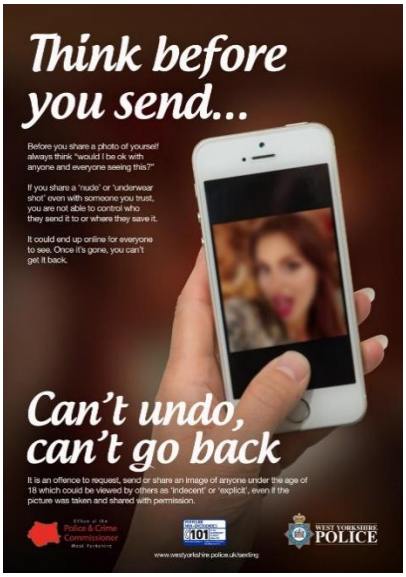
Mobilno napravo zaščiti z geslom ali vzorcem: tako onemogočite dostop drugim.

Varnostne kopije: kopije vseh podatkov, ki so za nas dragoceni. Če pride do vdora v naš sistem je dobro imeti varnostne kopije, saj edino tako zagotavljamo preprečitev izgube podatkov. Varnostne kopije je potrebno delati sproti. Kopije lahko shranjujemo na zunanje trde diske, pomnilniške medije ali jih shranjujemo v oblak.



Povezovanje samo z zaupanja vrednimi javnimi brezžičnimi omrežji: kajti lahko pride do vdora v naš sistem.

Seksting: ne pošiljajte svojih razgaljenih fotografij preko komunikacijskih kanalov. Kar enkrat pošlješ nekomu, je to izven vašega nadzora in se lahko širi naprej, lahko postane tudi sredstvo za izsiljevanje.



Uporaba aplikacij iz uradnih spletnih trgovin: aplikacije imajo v spletnih trgovinah oceno od ostalih uporabnikov. V primeru zlonamerne aplikacije jo uradna spletna trgovina izbriše. Pred uporabo aplikacije preberite pogoje uporabe.

Ne spreminjajte generičnih nastavitev operacijskega sistema na mobilni napravi (ang. Jailbreak ali Rooten): tovrstne spremembe lahko olajšajo dostop zlonamerni programski kodi.

2.9 Poznavanje principov zasebnosti

OPIS PROBLEMA

Pravico do zasebnosti imamo vsi, ta pa nam je po navadi zagotovljena že z zakonodajo - naši (zdravstveni, finančni, osebni itd.) podatki so zaščiteni in ljudje jih ne smejo deliti brez naše privolitve ne glede na to v kakšni obliki so. To velja tudi za podatke na internetu. Vendar pa le-ti ponavadi niso problematični ker jih ljudje neavtorizirano delijo in uporabljajo – problem je ravno v tem, da jih uporabljajo avtorizirano, saj jim uporabniki njihovih storitev prostovoljno dajo, pogosto brez da bi se tega zavedali. S našimi podatki namreč pogosto plačamo ''brezplačne'' storitve, ki nam jih nudijo spletna mesta.

Še posebej so problematične informacije, ki jih razkrivamo komercialnim ponudnikom storitev. Za uporabo teh morajo uporabniki izpolniti registracijski obrazec, ki navadno vsebuje tudi vprašanja o osebnih podatkih. Ta praksa je že tako vseobsegajoča, da ljudje niti pomislijo ne zakaj ponudnik sploh potrebuje te podatke ter kaj bo z njimi storil.

Osebne podatke pridobijo na dva načina:

- Osebni podatki, ki jih uporabnik sam zaupa (registracija, izpolnitev obrazcev, ustvarjanje računa, objavljanje podatkov pri komunikaciji z drugimi uporabniki ...)
- S puščanjem digitalnih sledi (kaj smo iskali, datum, čas in lokacija, katero napravo smo uporabljali, IP naslov ...)

Verjetno najbolj problematična so danes socialna omrežja, prek katerih uporabniki razkrijejo svoje pravo ime, datum rojstva, naslov, slike, videoposnetke, svoja mnenja ter še veliko drugih občutljivih podatkov do katerih lahko dostopa praktično vsak.

Tako so z uporabo pametnih naprav in interneta osebni podatki na voljo v ogromnih količinah, povedo veliko o nas in naših navadah ter imajo posledično ogromno vrednost. S puščanjem digitalnih sledi lahko algoritmi že sami predvidijo kaj bi radi kupili v spletni trgovini, predlagajo nam osebe s katerimi se bi ujeli na socialnih omrežjih, oceniti znajo tudi, da je določena oseba v nevarnosti zaradi določene bolezni.

Večina sodobnih spletnih strani uporablja tudi piškotke (ang. ''cookies''), to so majhne datoteke, ki s shranijo na napravi ob obisku spletne strani. Piškotki vsebujejo različne informacije, ki jih spletna stran prebere, ko jo uporabnik ponovno obišče. Piškotki so pravzaprav neke vrste digitalne sledi s katerimi ponudniki lažje optimizirajo spletno stran končnemu uporabniku in predvidijo uporabnikove želje.

Ljudje se pogosto ne zavedajo, da omogočajo dostop do osebnih podatkov vsem, tudi tistim, s katerimi sicer teh podatkov ne bi delili – v primeru mladih je to lahko družina, profesorji, bodočimi delodajalci ter osebe, ki jim

hočejo škodovati ... Večina delodajalcev je že povzela prakso preverjanja informacij na spletu ter socialnih omrežjih o kandidatu na spletu. Informacije, ki so objavljene pa lahko nepridipravi izkoristijo za slabe namene npr. izsiljevanje, phishing napade, spolne zlorabe, kraje identitete …

PREVENCIJA

- Brskajte po spletu brez puščanja sledi

  Firefox https://www.youtube.com/watch?v=07t5j3lruqA

  Internet Edge https://www.youtube.com/watch?v=RfggsRT3OYM

  Google Chrome https://www.youtube.com/watch?v=-4us6AnymJk
- Prilagoditev nastavitev o zasebnosti na socialnih omrežjih
- Ne razkrivajte gesla
- Preberite pogoje uporabe
- Ne izpolnjujte obrazcev, če to res ni nujno
- Poleg prvotnega E-mail naslova si izdelajte še takega ki ne razkriva kdo ste. Uporabljajte ga na spletnih straneh, forumih in anketah
- Uporabljaj vzdevke, ki ne razkrivajo vaše identitete
- Redno brišite piškotke
- Ne odgovarjajte na elektronsko pošto, ki od vas zahteva osebne in finančne podatke
- Svoje elektronske pošte ne objavljajte javno

ODZIV

V kolikor zgornjih predlogov še ne upoštevate jih začnite čim prej.

Vseh svojih podatkov, ki so že na internetu ne boste mogli izbrisati, vendar lahko poleg prevencije, ki prepreči nabiranje novih podatkov upoštevate nekaj korakov, s katerimi se lahko znebite kar največ svojih podatkov na internetu:

- Izklopite ali izbrišite svoje račune za spletne nakupe, socialna omrežja ter internetna orodja (ki jih ne potrebujete več):

  V kolikor sploh nočete svojih informacij na spletu lahko izklopite ali izbrišete vse račune, v kolikor pa tega nočete izbrišite le tiste, ki jih ne uporabljate več.

- Odstranite informacije direktno iz spletnih strani:

  Izbrišete lahko tudi informacije, ki so na posameznih spletnih straneh (forumi, blogi, spletne strani podjetij, šol itd.). To lahko storite tako, da kontaktirate upravitelja spletne strani ter ga prosite, da zbriše

vaše podatke. Zavedajte pa se, da ni nujno, da vam ustrežejo, saj ste za objavo teh podatkov verjetno že privolili na tak ali drugačen način v prihodnosti.

- Izbrišite podatke prek Googla:

  V kolikor vam upravitelj ni pripravljen pomagati se lahko obnete na Google in pošljete zahtevo za izbris osebnih podatkov prek te strani: https://support.google.com/legal/troubleshooter/1114905. Zavedajte pa se, da je postopek dolg, uspeh pa ni garantiran.

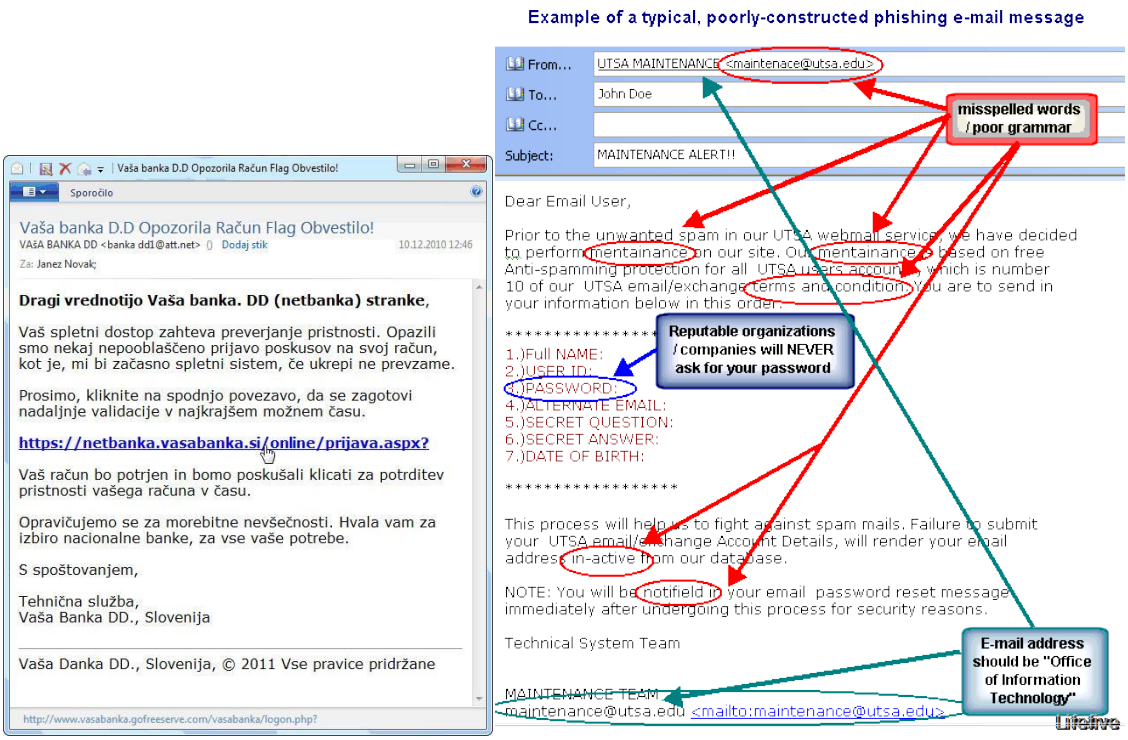
2.10 Prepoznavanje varnostnih incidentov

OPIS PROBLEMA

Kljub temu, da smo s tehnologijo in razvojem le-te v porasti, se še vedno vsakodnevno na različnih področjih srečujemo s človeško neprevidnostjo in tehničnimi nepravilnostmi. Zaradi vse večje zmogljivosti in pomnilniškega prostora na informacijskih sistemih, je privedlo, da vse več ljudi uporablja informacijske sisteme za potrebe nakupovanja, upravljanja financ in komuniciranja. Glede na to, da informacijski sistemi vsakodnevno posegajo na različna področja našega življenja, smo ljudje premalo ozaveščeni o primerni zaščiti le-teh. Uporabniki postajajo vse večje tarče kibernetskih zlorab, zato postaja zavedanje o varni uporabi še pomembnejše. Napadalci spreminjajo pristope napadov in izvajajo bolj targetirane. Naivnost uporabnikov je še vedno glavni vir njihovega prihodka, saj jih lahko s pravilnim pristopom ogoljufajo. Z izkoriščanjem varnostnih lukenj, ranljivosti v programski opremi ali v naših vedenjskih vzorcih lahko tujci pridobijo nadzor nad našo opremo, podatki in denarjem. Varnost na internetu je proces, za katerega moramo stalno skrbeti in ga ni mogoče kupiti.

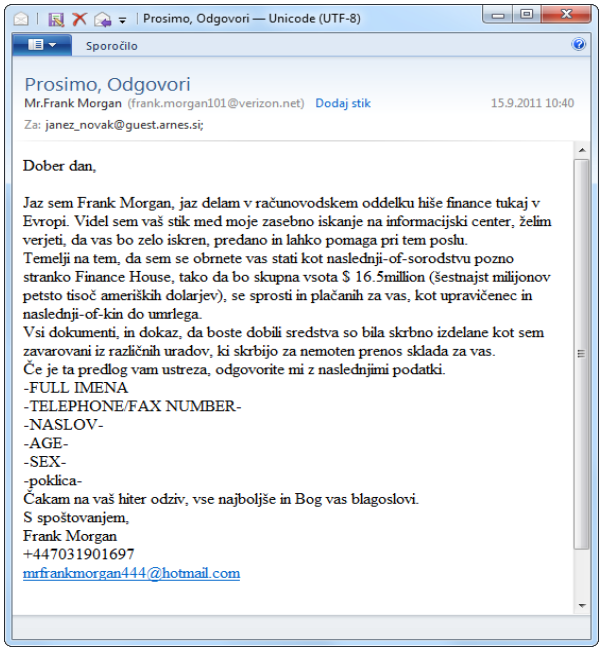
Phishing prevara je kraja podatkov, ki goljufu omogočijo dostop do naših spletnih storitev. Najpogosteje poteka tako, da nas elektronsko sporočilo zvabi na lažno stran banke ali spletne storitve, običajno pod pretvezo, da moramo preveriti podatke ali zamenjati geslo. Če na lažni strani vpišemo geslo za dostop do bančnega računa ali spletne storitve, geslo pravzaprav izročimo goljufu.

Pozorni morate biti da je URL naslov pravi, preverite tudi, ne odgovarjajte na elektronsko pošto v kateri vas prosijo za zaupne informacije (digitalno potrdilo, gesla, številke kartic,..). kraja podatkov se ne dogaja samo pri spletnih bankah ampak tudi pri vseh ostalih spletnih straneh, kjer morate vpisati svoje geslo.



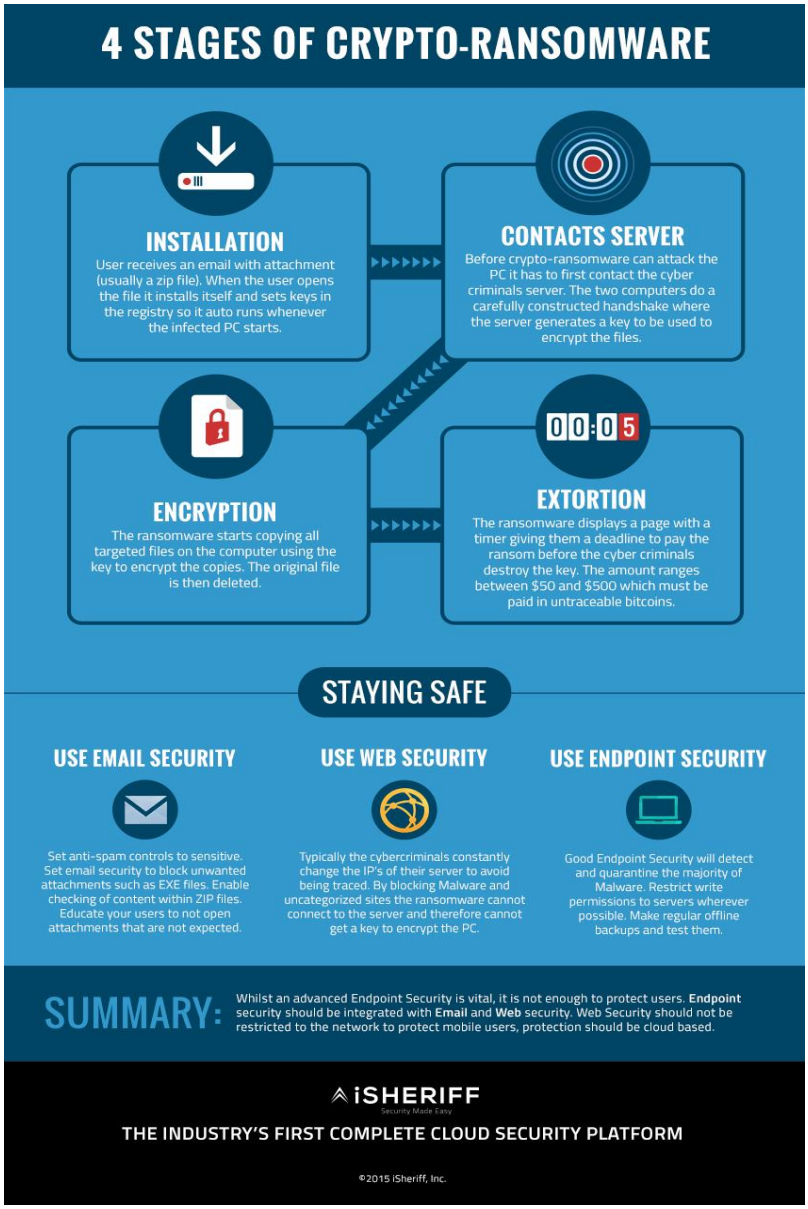
Vdor v računalnik je najbolj klasična oblika hekerskega napada. Pomeni nepooblaščen dostop do naše računalniške baze in podatkov v njej. Dva najpogostejša načina vdora sta ranljivost programske opreme in odsotnost avtentikacije (slabo geslo).

Spletne prevare pri katerih vas neznanec s čarobno privlačno ponudbo premami, da mu nakažete denar (najbolj znana so nigerijska pisma, kjer nas želijo napadalci prepričati v sodelovanje).



Nezaželena sporočila (ang. Spam) so sporočila, ki vam vsiljujejo vsebino, katere si ne želite.

Okužbe z računalniškimi virusi, internetnimi črvi in trojanskimi konji so najbolj razširjena spletna tveganja in služijo predvsem za krajo podatkov in identitete. Najbolj popularen je izsiljevalski virus (ang. ransomware), kater nam zašifrira podatke in za povrnitev le-teh zahteva denarno izplačilo.



Kraja identitete je kraja osebnih podatkov (npr. imena, rojstnega datuma, številke kreditne kartice) in njihova nezakonita uporaba.

Varnostne napake in brezžična omrežja zaradi katerih lahko napadalci vstopijo v vaš računalnik in pri tem izkoristijo različne pomanjkljivosti programske in strojne opreme.

Zlonamerni bančni napadi, glavna motivacija za take napade je seveda, da pridobijo denar od uporabnika. Zato uporabljajo različne načine kako priti do njega. Najpogostejši načini so Phishing napadi, vsiljiva sms sporočila in izsiljevalski virusi

2.11 Razumevanje brezžičnih omrežij in njihove varnosti

OPIS PROBLEMA

Zaradi tehnoloških značilnosti so brezžična omrežja varnostno veliko bolj občutljiva kot žična. Brezžičnim komunikacijam lahko prisluškuje vsakdo z ustrezno anteno in sprejemnikom.

Omrežja, ki temeljijo na tehnologiji WPA in WPA2, veljajo za ena najvarnejših brezžičnih omrežij. Ves promet med odjemalcem in dostopno točko je šifriran, istovetnost strežnika in uporabnika pa potrjena.

Lahko pa boste naleteli na omrežja, ki ne temeljijo na varnih tehnologijah – odprta brezžična omrežja, omrežja, ki uporabljajo za preverjanje istovetnosti spletni portal. Takšna omrežja lahko najdete praktično povsod (v hotelih, letališčih, nakupovalnih centrih …). Zavedati se morate, da ste pri uporabi le teh lahko izpostavljeni:

- prisluškovanju prometa,
- spreminjanju poslanih ali prejetih podatkov,
- prestrezanju podatkov, ki se uporabljajo za ugotavljanje istovetnosti (uporabniško ime in geslo). Nepooblaščena oseba lahko postavi lastno dostopno točko in se uporabniku lažno predstavi kot strežnik, kateremu uporabnik v dobri veri posreduje svoje uporabniško ime in geslo.
- Zlobni dvojček (napadalec oddaja močnejši signal od izvirnega signala, uporabnik se posledično prijavi na napačno vstopno točko in tako lahko napadalec pregleda ves promet uporabnika)

Ker meje brezžičnega omrežja niso striktno omejene s prostorom in se komunikacija odvija po zraku, je napadalcu poenostavljeno prestrezanje in vohunjenje (ang. sniffing). Šifriranje je postopek s katerim nadgradimo avtentikacijo in poslane podatke preoblikujemo v obliko, ki je neuporabna v primeru prestrezanja ali vsaj časovno zelo zahtevna pri poskusih dešifriranja.

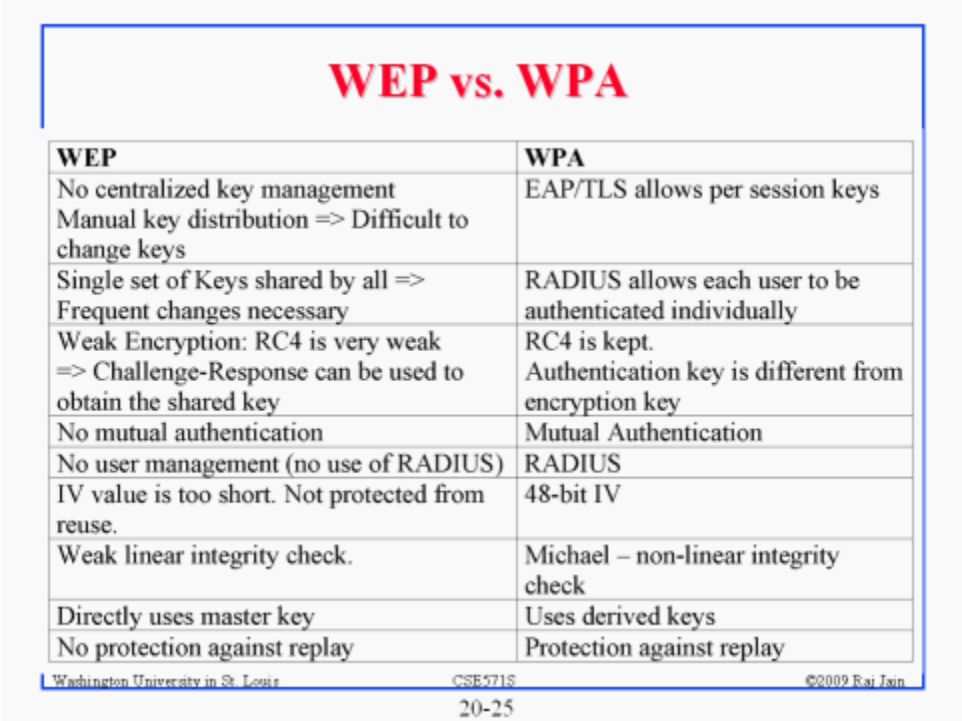
RAZLIKOVANJE MED WPA IN WEP

WPA (ang. Wi-Fi Protected Access) je v uporabi od l. 2003 kot zamenjava WEP. WEP predstavlja sicer dober način preprečevanja prestrezanja podatkov, vendar protokol ne zagotavlja najvišje stopnje varnosti. Slabost protokola WEP je uporaba statičnega so-uporabniškega ključa na vseh napravah z omogočenim WEP. Na Internetu obstajajo aplikacije, ki omogočajo napadalcu odkrivanje ključa. Ko je ključ enkrat znan ima napadalec dostop do vseh podatkov.

Eden izmed načinov izogibanja ranljivost WEP šifriranja je periodična zamenjava ključev zato je v industrijskem in poslovnih okoljih bolje uporabiti naprednejši in varnejši način šifriranja WPA.

WPA uporablja šifrirne ključe dolžine 64 - 256 bitov podobno kot WEP vendar tvori ključe dinamično - ob vsakokratni vzpostavitvi povezave odjemalca z dostopno točko s protokolom TKIP (ang. Temporal Key Integrity Protocol). Zato je postopek tvorjenja generatorskega ključa

kompleksnejši in s tem tudi varnejši. WPA podpira tudi napredni standard šifriranja AES (ang. Advanced Encrypted Standard).



WEP vs. WPA

WEP	WPA
No centralized key management Manual key distribution => Difficult to change keys	EAP/TLS allows per session keys
Single set of Keys shared by all => Frequent changes necessary	RADIUS allows each user to be authenticated individually
Weak Encryption: RC4 is very weak => Challenge-Response can be used to obtain the shared key	RC4 is kept. Authentication key is different from encryption key
No mutual authentication	Mutual Authentication
No user management (no use of RADIUS)	RADIUS
IV value is too short. Not protected from reuse.	48-bit IV
Weak linear integrity check.	Michael – non-linear integrity check
Directly uses master key	Uses derived keys
No protection against replay	Protection against replay

HTTPS

HTTPS (HyperText Transfer Protocol Secure) je protokol za šifrirano spletno komunikacijo. Če za navadno spletno komunikacijo (HTTP). Šifriranje poteka prek SSL (ang. Secure Sockets Layer) ali TLS (ang. Transport Layer Security) kriptografskega protokola. Pri samem šifriranju podatkov pa se uporabljajo različni šifrirni algoritmi z različnimi dolžinami ključev.

PREVENCIJA

- Zamenjava privzetega uporabniškega imena in gesla s svojim
- Vključitev WPA in WEP kodiranja
- Zamenjava brezžičnega omrežja (SSID), primer: Kupiš nov usmerjevalnik recimo ''linksys'', vendar ne spremeniš imena SSID, tako nepridiprav ve točno kater usmerjevalnik imaš in lahko prej to zlorabi
- Flitriranje MAC naslovov
- Onemogočanje avtomatskega povezovanja v odprta brezžična omrežja
- Usmerjevalnik izklopite, če vas dolgo časa ne boste potrebovali
- Varna postavitev usmerjevalnik (čim manj uhajanja v bližnjo okolico)

How does HTTPS work: SSL explained

This presumes that SSL has already been issued by SSL issuing authority.

2.12 Razumevanje, uporaba in upravljanje varnih gesel

OPIS PROBLEMA

Močno geslo je pomembno, saj je po navadi zadnja obramba pred direktnim vpogledom v naše podatke, delo ter življenje. Zato je potrebno pri njihovi uporabi in upravljanju upoštevati naslednje smernice, da smo kar najbolj varni.

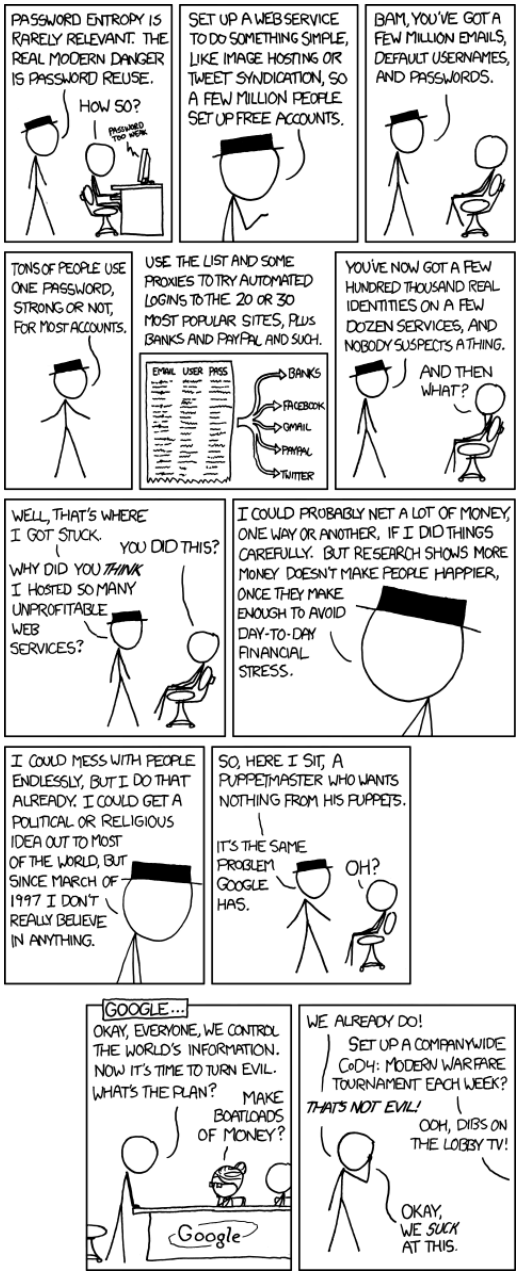
PREVENCIJA

- geslo naj ne bo uporabljeno za več spletnih strani oz. računov, ki razpolagajo z občutljivimi podatki, še posebej to velja za e-pošto;
- gesla naj se redno menjujejo, še posebej za račune z občutljivo vsebino;
- seznam gesel naj ne bo prosto viden oz. v bližini naprave, seznam pa je lahko tudi zašifriran;
- v kolikor je to mogoče je najboljše uporabiti dvo-faktorsko avtorizacijo (geslo + digitalno potrdilo, geslo + mobilni telefon na katerega je poslana dodatna koda, katero se nato vpiše poleg gesla itd.);
- uporabniki lahko za bolj varno in preprostejše upravljanje z gesli uporabljajo tako imenovani “password manager”, to je program, ki ureja in šifrira gesla namesto uporabnika (npr. LastPass, DashLane, 1Password itd.)

ODZIV

V primeru, da geslo izgubimo, lahko le tega pridobimo tako, da sledimo navodilom na spletni strani računa katerega geslo smo izgubili. Postopek in način pridobitve izgubljenega gesla po navadi postavimo ko se registriramo.

V kolikor zgornjih predlogov še ne upoštevate jih začnite čim prej.


PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.
TONS OF PEOPLE USE ONE PASSWORD, STRONG OR NOT, FOR MOST ACCOUNTS.
USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.
EMAIL
USER
PASS
BANKS
FACEBOOK
GMAIL
PAYPAL
TWITTER
YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.
AND THEN WHAT?
WELL, THAT'S WHERE I GOT STUCK.
YOU DID THIS?
WHY DID YOU THINK I HOSTED SO MANY UNPROFITABLE WEB SERVICES?
I COULD PROBABLY NET A LOT OF MONEY, ONE WAY OR ANOTHER, IF I DID THINGS CAREFULLY. BUT RESEARCH SHOWS MORE MONEY DOESN'T MAKE PEOPLE HAPPIER, ONCE THEY MAKE ENOUGH TO AVOID DAY-TO-DAY FINANCIAL STRESS.
I COULD MESS WITH PEOPLE ENDLESSLY, BUT I DO THAT ALREADY. I COULD GET A POLITICAL OR RELIGIOUS IDEA OUT TO MOST OF THE WORLD, BUT SINCE MARCH OF 1997 I DON'T REALLY BELIEVE IN ANYTHING.
SO, HERE I SIT, A PUPPETMASTER WHO WANTS NOTHING FROM HIS PUPPETS.
IT'S THE SAME PROBLEM GOOGLE HAS.
OH?
GOOGLE...
OKAY, EVERYONE, WE CONTROL THE WORLD'S INFORMATION. NOW IT'S TIME TO TURN EVIL.
WHAT'S THE PLAN?
MAKE BOATLOADS OF MONEY?
Google
WE ALREADY DO!
SET UP A COMPANYWIDE CoD4: MODERN WARFARE TOURNAMENT EACH WEEK?
THAT'S NOT EVIL!
OOH, DIBS ON THE LOBBY TV!
OKAY, WE SUCK AT THIS.

2.13 Oblikovanje varnih gesel

OPIS PROBLEMA

Mnogo ljudi uporablja kratka in preprosta gesla, ki si jih je lahko zapomniti, vendar jih je prav tako lahko zlomiti. V današnjem svetu so močna gesla ključna za varnost, zato se je potrebno naučiti kako snovati močna gesla, to pa lahko storimo tako, da sledimo nekaj smernicam.

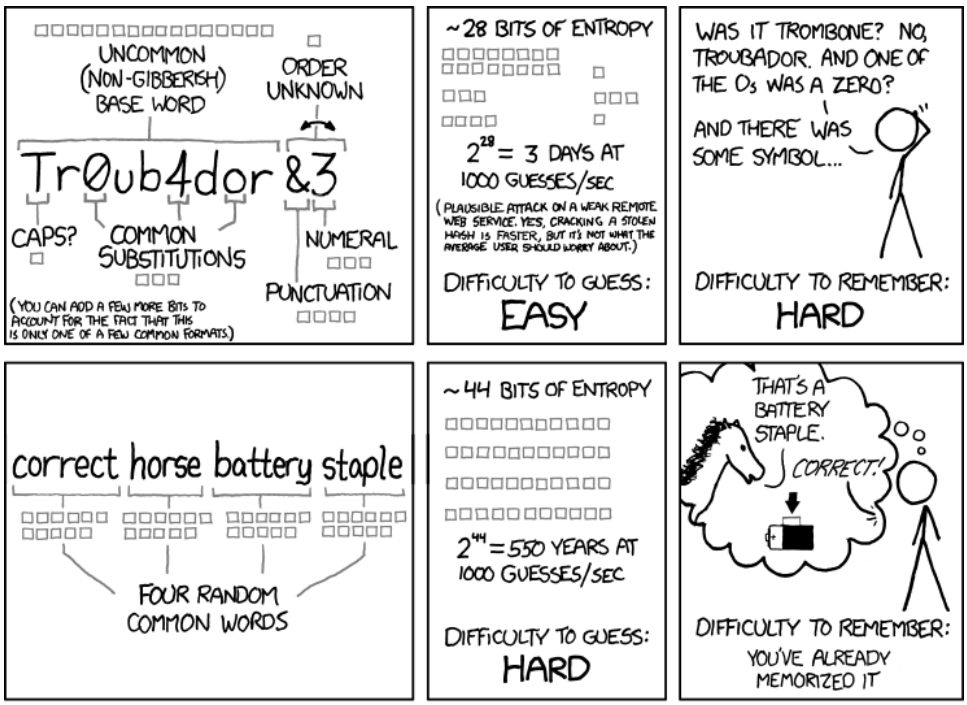
PREVENCIJA

- geslo naj ne bo uporabljeno za več spletnih strani oz. računov, ki razpolagajo z občutljivimi podatki, še posebej to velja za e-pošto;
- gesla naj se redno menjujejo, še posebej za račune z občutljivo vsebino;
- seznam gesel naj ne bo prosto viden oz. v bližini naprave, seznam pa je lahko tudi zašifriran;
- v kolikor je to mogoče je najboljše uporabiti dvo-faktorsko avtorizacijo (geslo + digitalno potrdilo, geslo + mobilni telefon na katerega je poslana dodatna koda, katero se nato vpiše poleg gesla itd.);
- uporabniki lahko za bolj varno in preprostejše upravljanje z gesli uporabljajo tako imenovani “password manager”, to je program, ki ureja in šifrira gesla namesto uporabnika (npr. LastPass, DashLane, 1Password itd.)

ODZIV

V primeru, da geslo izgubimo, lahko le tega pridobimo tako, da sledimo navodilom na spletni strani računa katerega geslo smo izgubili. Postopek in način pridobitve izgubljenega gesla po navadi postavimo ko se registriramo.

V kolikor zgornjih predlogov še ne upoštevate jih začnite čim prej s spremembo gesel.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

2.14 Varne prakse za delo z elektronsko pošto

OPIS PROBLEMA:

Varne prakse pri delu z elektronsko pošto vključujejo različne taktike in pripomočke za prepoznavanje in filtritranje potencialne nevarne oziroma škodljive elektronske pošte. Brez zaščite lahko vsakdo prestreza, bere in spreminja našo elektronsko pošto. Velikšen del problema lahko odpravimo sami, predvsem z implementacijo enostavnih taktik za zmanjšanje vrjetnosti napada ali preztrezanja.

PREVENCIJA:

- uporaba več različnih elektronski pošt (v primeru, če vam zajamejo eno, nebodo imeli dostopa da vseh informacij s katerimi upravljate),
- močno geslo,
- prepozavanje phising napadov,
- izogibanje odpiranju povezav v elektonski poštah,
- izogibanje odpiranju neznanih priponk,
- skeniranje za rezlične viruse,
- izgoibanje javnim wi-fijem.

2.15 Prepoznavanje vsiljenih, sumljivih in škodljivih elektronskih sporočil

Osnovno poznavanje delovanja elektronskega sporočanja, ki ni nujno omejeno samo na elektronsko pošto in postopkov za varno uporabo aplikacij za elektronsko sporočanje in za manipulacijo z elektronskimi sporočili, je ključno za delovanje v svetu elektronske pošte. Enako velja za zavedanje ranljivosti in resnosti posledic pri nevarni rabi elektronske pošte. Pozornost in upoštevanje predpisanih postopkov pri odpiranju elektronskih sporočil in priponk iz neznanih ali nenavadnih virov, sta zelo dobrodošla.

OPIS PROBLEMA:

Sumljiva elektronska pošta že nekaj časa predstavlja resen problem. Problem takšnih sporočil je, da so lahko kreirana na točno določen način, da vas njihova avtentičnost zlahka zavede. Po navadi takšna sporočila izvirajo iz elektronskih naslovov različnih institucij, med drugim so lahko tudi uradne – na primer sodišča. Takšna sporočila pa v resnici ne izvirajo iz uradnih ustanov, ampak gre za zlorabo uradnih naslovov institucij. Prejemnik najpogosteje prejme različne datoteke (npr.: Dokument_1.zip ali Dokument_1.js in podobno). Sporočila so lahko poslana pod pretvezo različnih nagradnih iger, obiskov predsednika države, sporočil iz policije, ali pa za poslovne pretveze.

Vsiljena pošta ali SPAM je elektronska pošta, ki je poslana večjemu številu uporabnikov z namenom vsiljevanja določene vsebine ali produktov, ki se jih uporabniki sami ne bi nikoli odločili prejemati. Največkrat so to sporočila, ki se nanašajo na oglaševanje različnih storitev ali izdelkov, ki pa imajo dvomljivo kvaliteto. Mnogokrat pa so lahko takšna sporočila povezana s prevarami (na primer: Nigerijske prevare).

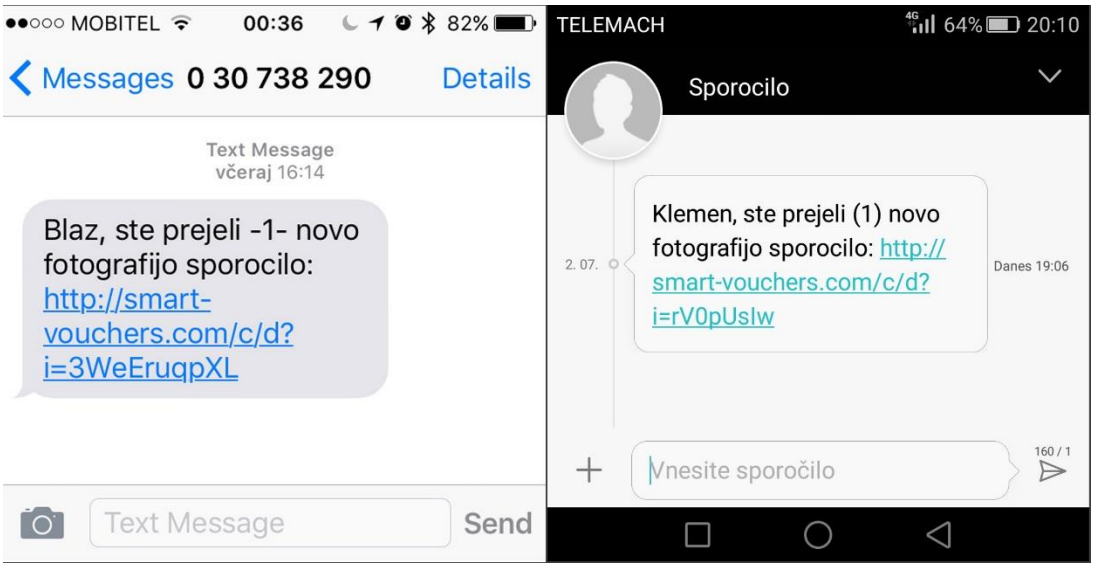
Pošiljatelji lahko dobijo vašo pošto na različne načine:

- Vaš elektronski naslov objavite na določeni spletni strani,
- Pri registraciji za določene spletne strani,
- Pri inštalaciji programov, ki v ozadju pobirajo različne informacije o vas
- Preko seznama naročnikov na poštne sezname (angl. Mailing lists)

ZANIMIVO:

Takšna sporočila pa niso nujna samo pri elektronski pošti. Zgodi se lahko, da na vašo telefonsko številko prejmete sms, kjer imate povezavo do na primer fotografije. Čeprav je telefonska števila slovenska, je resničnega pošiljatelja zelo težko izslediti, saj se številko zlahka ponaredi. V kolikor sledite povezavi, vas lahko vodi v trgovino z aplikacijami (Google play, App Store ipd.), kjer vidite določeno aplikacijo. Ob prenosu takšne aplikacije, pa vas

lahko vodi na spletno stran lažnih nagradnih iger, kjer morate za sodelovanje vpisati svojo telefonsko številko (običajno vas včlanijo v plačljiv SMS klub).



Prvo spam sporočilo je bilo poslano leta 1994, za Ameriško odvetniško družbo Cantner&Siegel)

Ali ste vedeli? Da neželena pošta predstavlja že okoli 90% svetovnega prometa elektronske pošte. Problem je nasičenost informacij, saj lahko zaradi vsiljene pošte spregledamo nekatera pomembna sporočila.

Nigerijske prevare: največkrat zajemajo neverjetne loterijske zadetke ali poslovne ponudbe. V resnici pa ne boste postali bogati – ampak gre za klasično prevaro.

Največkrat dobite sporočilo v smislu: Izžrebani ste bili za denarno nagrado,… ipd. Za izplačilo te nagrade, pa morate sami nakazati provizijo, ali pa plačati »davek«. Pošiljatelj od vas zahteva da preko sistema Western Union nakažete določen znesek, da lahko kasneje prejmete to nagrado. Western Union je priljubljen plačilni mehanizem pri storilcih prevar, saj ne omogoča sledenja. Vendar pa eno nakazilo ni dovolj. Kasneje si storilec prične namišljevati dodatne stroške (odvetnik, različni davki, stroški vodenja računa, …) in to plačevanje lahko traja v nedogled, oškodovani pa ste lahko tudi za več tisoč evrov.

Kako jih prepoznati? Največkrat uporabljajo angleščino ali polomljeno slovenščino, saj je tekst preveden preko google translate-a in zato lahko najdemo veliko slovničnih napak.

PREVENCIJA:

Svetujemo, da datotek, ki jih ne pričakujete po elektronski pošti, ne odpirate. Pametno pa bi bilo tudi ustvariti varnostne kopije podatkov na računalniku.

- Previdnost pri objavi ali posredovanju elektronskega naslova,
- ne odgovarjaj na SPAM,
- antivirusni program,
- blokiranje poštnega naslova pošiljatelja

TUTORIAL:

- Gmail: https://support.google.com/mail/answer/8151?co=GENIE.Platform%3DDesktop&hl=sl
- Primer prikaza nigerijske prevare: https://www.youtube.com/watch?v=blDPpm6QGXM (varni na internetu)

2.16 Znanje o namestitvi in uporabi antivirusnih programov

Namestitev in pravilna uporaba antivirusnega programa, s poudarkom na rednem in sprotnem skeniranju prenešenih informacij, ključno pripomore k varnosti na računalniku ali drugih napravah.

OPIS PROBLEMA:

Antivirusni oziroma protivirusni program je računalniški program, ki išče, preprečuje, odkriva in odstranjuje računalniške viruse ter druge zlonamerne programske opreme, kot so na primer črvi in trojanski konji. Do okužbe lahko pride takoj po vzpostavitvi povezave z internetom, zato so antivirusni programi ključnega pomena za uporabnike. Antivirusni programi se morajo pogosto posodabljati, saj se vsakodnevno na internetu pojavljajo nove oblike virusov in drugih zlonamernih groženj.

Poznamo več vrst antivirusnih programov, ki služijo za:

- Pregledovanje datotek na računalniku -> v kolikor program zazna virus, poskuša datoteko zbrisati, ali jo popraviti.
- Pregledovanje sumljivih programov, ki lahko predstavljajo grožnjo.
- Peskovnik (ali sandbox), ki naredi simulacijo operacijskega sistema, v katerem testira delovanje antivirusnega programa.

ZANIMIVO:

Najpogosteje pride do okužb s prenosom datotek, z elektronsko pošto ali pa z dostopom na določene spletne strani. Prvi virus so odkrili že leta 1971, imenoval se je Creeper Virus.

Obstajajo tudi antivirusni programi, ki so lažni. Največkrat se vam med brskanjem po internetu, pojavi okno, kjer piše, da si morate nujno namestiti antivirusni program. V resnici pa lahko gre za virus. Največ tovrstnih virusov se pojavlja na sistemu Windows, vse več pa tudi na Macu.

Paziti je treba tudi, kadar imate na računalniku naložen več kot en antivirusni program, saj lahko zaznavata en drugega kot virus, ali pa izkljapljata požarni zid in podobno. Zato je najbolje, da imate na računalniku naložen zgolj en, kvaliteten antivirusni program.

SEZNAM BREZPLAČNIH ANTIVIRUSNIH PROGRAMOV:

1. AVIRA FREE ANTIVIRUS 2015
2. BITDEFENDER ANTIVIRUS FREE EDITION 2016
3. PANDA FREE ANTIVIRUS 2016
4. AVG FREE ANTIVIRUS 2016
5. AVAST FREE ANTIVIRUS 2015

(vir: http://dne.enaa.com/Racunalniska-oprema/top-5-brezplacnih-protivirusnih-programskih-resitev.html)

PREVENCIJA:

- Reden pregled oziroma sken računalniškega sistema

2.17 Varna raba spletnega brskalnika in brskanja po spletu

»Varna raba« pomeni poznavanje najosnovnejših groženj, ki izhajajo iz uporabe interneta in delovanje v skladu s tem znanjem. Pomembno je, da mladostniki znajo uporabljati posodobljene, bolj varne brskalnike in da uporabljajo oz. prepoznajo HTTPS povezavo.

OPIS PROBLEMA:

Ne glede na to, ali do interneta dostopate z mobilnim telefonom, ali pa z računalnikom, je potrebno naprave zaščititi pred virusi, trojanskimi konji in drugimi grožnjami.

- Pri brskanju po internetu priporočamo uporabo požarnega zida, kjer moramo biti še posebno previdni, da je vedno vklopljen in posodobljen,
- Redno posodabljajte svoj operacijski sistem računalnika in mobilnega telefona, saj posodobitve nudijo boljšo zaščito,
- Na svoje naprave nameščajte antivirusno in protivohunsko zaščito, da jih zavarujete pred zlonamernimi programi. Tudi pri antivirusnih zaščitah je nujno sprotno posodabljanje.
- Redno izdelujte varnostne kopije podatkov in jih shranjujte.
- Pri mobilnih programih pa bodite pozorni pri izbiri aplikacij, ki jih nameščate.

Vsa prevencija pa ni zadostna, saj velikokrat posebno nevarnost predstavlja človeški faktor. Zato priporočamo, da na internetu ne navajate osebnih podatkov, na forumih ne uporabljajte e-mail naslova, ki razkriva vaše podatke, na družabnih omrežjih bodite pozorni na nastavitev zasebnosti.

ZANIMIVO:

Internetni brskalniki kot so Chrome, Firefox ali Explorer imajo posebno funkcijo, kjer lahko vklopite zasebno brskanje, brez beleženja zgodovine. Problem pa nastane, da vam tovrstno brskanje daje le občutek zasebnosti in varnosti. Kljub temu, da imate odprto zasebno okno, se na spletnih straneh še vedno beleži vaš IP naslov, ki lahko odkrije vašo lokacijo.

Za brskanje na spletu, pa spletne strani uporabljajo različne certifikate. En izmed varnejših se imenuje SSL certifikat, ki dobesedno pomeni Secure Sockets Layer, ki je kriptografski protokol, ki omogoča varno komunikacijo na spletu. SSL protokol se uporablja povsod, kjer se pojavlja potreba po prenosu podatkov zaupne narave (na primer osebni podatki in številke kreditnih kartic). Ali spletna stran uporablja SSL protokol prepoznamo tako, da se povezava namesto s HTTP začne s HTTPS.

Za primer lahko vzamemo priljubljeno spletno stran s torrenti: partis.si. Problem partisa je, da ne uporablja SSL protokola, zato odsvetujemo prijavo v partis na javnih omrežjih. Obstajajo programi, kot so na primer Wireshark, ki lahko skenirajo vsa gesla, ki so bila na določeni strani vnešena, v kolikor smo povezani na javno omrežje.

To v praksi pomeni, da vsak, ki ima geslo do na primer hotelskega omrežja, javnih »public« omrežij, ali pa do vašega domačega omrežja, lahko skenira vaša gesla in vam na tak način vdre v vaš račun, iz katerega lahko pridobi osebne podatke, ali pa v hujših primerih tudi do podatkov v vašem računalniku.

PREVENCIJA:

- Redno posodabljanje brskalnikov,
- Uporaba antivirusne zaščite,
- Uporaba strani s SSL protokolom (HTTPS),
- Previdnost pri vpisovanju osebnih podatkov,
- Menjavanje gesel (+ uporaba različnih gesel na različnih straneh).

2.18 Sposobnost izogibanja in reagiranja na grožnje pri rabi spletnega brskalnika

Sposobnost pravilne identifikacije spletnih groženj, ki lahko ogrozijo informacijsko premoženje, je ključnega pomena za mladostnike. Le-ti morajo vedeti, kaj narediti, če so preusmerjeni oz. so se znašli na sumljivi spletni strani.

OPIS PROBLEMA:

Pri uporabi spletnega brskalnika lahko naletimo na veliko različnih groženj. Večinoma se uporablja zlonamerno programsko opremo, ki se žrtvi naloži na računalnik in s tem povzroči različne nevšečnosti. Predvsem se izkorišča računalnike, ki nimajo zadostne zaščite oziroma uporabljajo standardno zaščito, ki ima veliko ranljivosti.

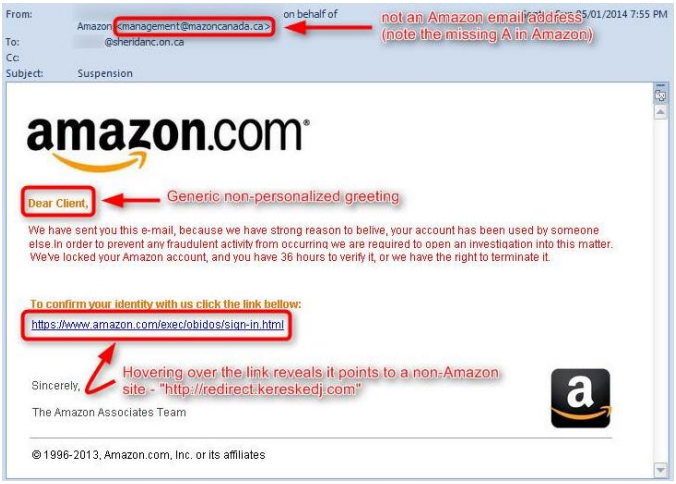
Najbolj pogoste grožnje so v obliki zlonamerne programske opreme:

1. **Vohunska programska oprema**:

- Zlonamerno zbiranje manjših količin informacij brez vednosti uporabnika. V večini se tovrstno orodje namesti direktno na računalnik. Primer je »keylogger«, s katerim se beleži kaj osebe vpisuje v računalnik.

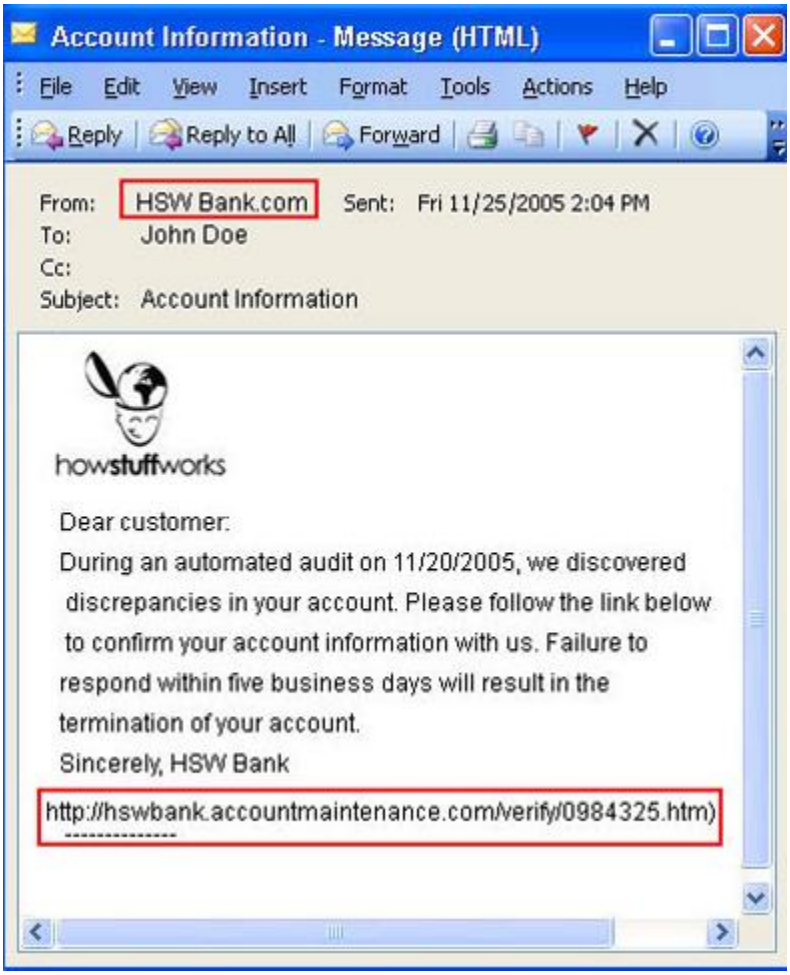
2. **Kraja spletnih gesel in osebnih podatkov** (»phishing«):

- Način kraje identitete, spletnih gesel, oziroma druge osebe podatke (kot so gesla, številke kreditnih kartic in podobno). Tipičen način prenosa je preko e- pošte ali lažnih spletnih strani. Podoben način je »Pharming«, kjer se zlonamerna programska oprema naloži na računalnik ali server in preusmerja uporabnika na lažne spletne strani, kjer se uporabnika prosi naj vpiše svoje osebne podatke.



3. **»Spoofing«**:

- Način kraje identitete, kjer prejeta elektronska pošta izgleda legitimna. Vsebina vsebuje povezavo do lažnivih spletnih strani, kjer se od uporabnika prosi za osebe podatke.



4. **»Browser hijacking«**, zajetje brskalnika:

- Zlonamerna programska oprema spremeni nastavitve našega brskalnika tako, da nas preusmerja na strani, katere ne želimo obiskati. Zamenja lahko našo domačo stran (npr. google) z neko alternativno, vsiljuje različne oglase, konstanto preusmerjanje na določeno spletno stran (npr. spletna trgovina).

PREVENCIJA IN ODZIV NA INCIDENTE:

- Redno posodabljanje brskalnika. Z vsako novo posodobitvijo se krpajo varnostne luknje, katere je proizvajalec potencialno spregledal. S konstantnim posodabljanje lahko zmanjšamo verjetnost nastanka varnostnega incidenta.

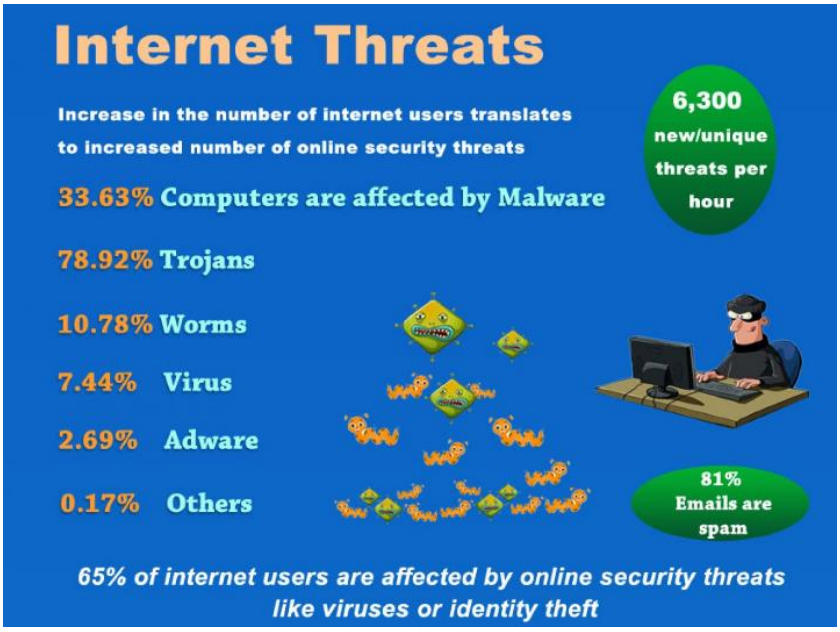
- Naša največja prednost pred spletnimi grožnjami je znanje, ozaveščenost o varnosti in zaščiti na internetu.

- Antivirusni program in program za blokiranje oglasov.

- Redno skeniranje za različne viruse.

- Ignoriranje neznanih povezav.

ZANIMIVOSTI/PRIMER:



2.19 Varnost mobilnih naprav

Zavedanje potencialnih nevarnosti, ki jih predstavljajo naprave v osebni lasti, ki jih mladostniki s seboj prinesejo v šolo, je ključna sestavina varnosti mobilne naprave posameznika. Gre za pravilno uporabo zasebne informacijsko-komunikacijske tehnologije oziroma s kratico IKT.

OPIS PROBLEMA:

Tako kot pri osebnih računalnikih lahko tudi pri rabi mobilnih naprav naletimo na zlonamerno programsko opremo. Mobilne naprave so večinoma konstantno povezane z internetom. Tako lahko različne aplikacije predstavljajo grožnjo za potencialno izkoriščanje mobilnih naprav. Grožnje so podobne kot pri osebnih računalnikih. Poleg aplikacij lahko odpiramo e-pošto, SMS sporočila, Facebook sporočila, sporočila preko Twitterja, ki vsebujejo povezave do različnih strani, katerih primarni namen je nalaganje zlonamerne programske opreme. S prenosom virusa lahko vsiljivec dobi vse administratorske pravice mobilne naprave.

Pri mobilnih napravah je tveganje, da bomo žrtev napada, še toliko večje, saj so naprave povezane preko WiFi-ja. Veliko omrežij je nezaščitenih oziroma imajo naprave nizko stopnjo varnosti, kar omogoča nepridipravom lažji dostop do različnih informacij.

Poleg tega so mobilne naprave majhne in jih konstantno nosimo pri sebi, zato je priporočljivo premisliti tudi o varnosti mobilne naprave. Največja grožnja za mobilne naprave so izgube naprave ali kraje. Poleg potencialne visoke vrednosti same naprave so vredne tudi informacije, ki so shranjene na telefonu.

PREVENCIJA IN ODZIV NA INCIDENTE:

- Antivirusni programi (Velik delež uporabnikov mobilnih naprav ne uporablja oziroma niso ozaveščeni o uporabi antivirusnega programa na mobilnih napravah, zato je nezaščiten tudi velik delež mobilnih naprav).

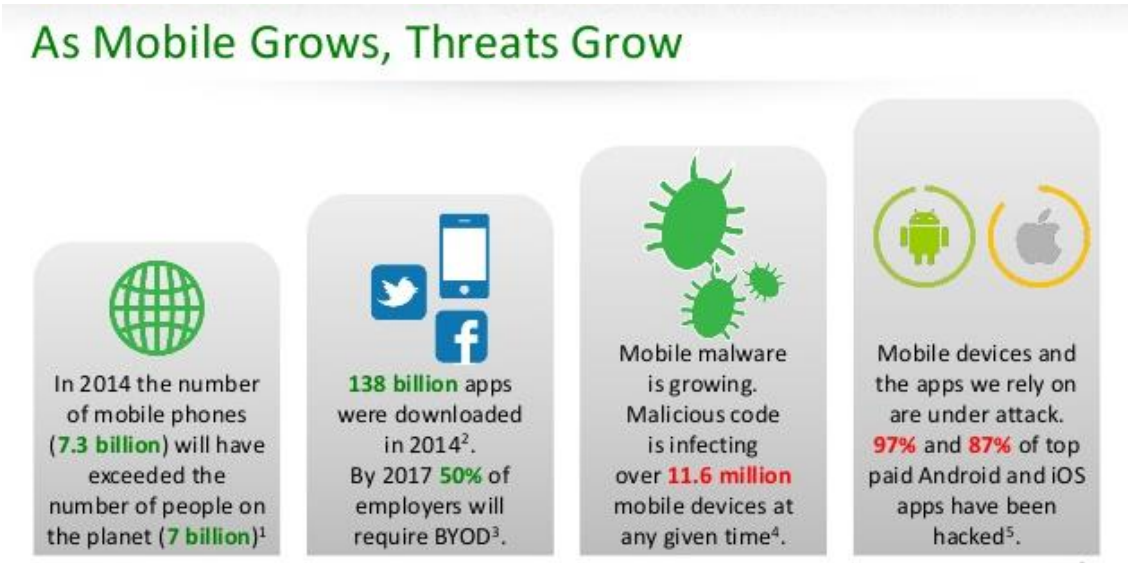
- Stalno posodabljanje programov.

- Geslo za dostop do telefona.

- Preverjanje legitimnosti aplikacije pred nalaganjem.

- Pazljivost pri povezovanju z neznanimi wifi-ju.

ZANIMIVOST:



2.20 "Gledanje čez ramo"

Preprečevanje fizičnega prestrezanja informacij, predvsem z zaslona, ki ga mladostnik v tistem trenutku uporablja, pomeni onemogočanje storilcem, da bi gledali čez ramo in si na ta način pridobivali informacije, ki se jih ne tičejo.

OPIS PROBLEMA:

»Gledanje čez ramo« pomeni dobesedno gledanje osebi čez ramo med uporabo elektronske naprave. Predvsem gre za prestrezanje različnih informacij o drugi osebi, kot so gesla, osebni podatki, branje sporočil, privatne slike ipd. Gledanje čez ramo je najpogostejše pri gnečah, saj ne opazimo/ posumimo, da nas kdo opazuje.

PREVENCIJA IN ODZIV NA INCIDENTE:

-Ne vpisujemo/gledamo občutljivih informacij, ko je nekdo blizu,

-ne vpisujemo/gledamo občutljivih informacij, če se nekdo blizu pogovarja po telefonu,

-biti pozoren in prisoten med gledanjem, vpisovanjem občutljivih informacij. Prepričati se moramo, da nas nihče ne opazuje. Če je le možno, operiramo s občutljivimi informacijami na samem,

-če sumimo, da nas kdo opazuje zamenjamo geslo takoj, ko je to mogoče varno storiti.

2.21 "Brskanje po smeteh"

Zavedanje pomembnosti, zaupnosti in integritete dokumentov, ki so bili zavrženi, lahko prepreči določena dejanja, s katerimi bi se lahko nepridipravi okoristili in se dokopali do zasebnih informacij ali pa samo zlorabili določene podatke za dosego lastnih ciljev. Prevencijo pred »brskanjem po smeteh« nudi tudi preprečevanje prestrezanja informacij zavrženih listin.

OPIS PROBLEMA:

Brskanje po smeteh je način pridobivanja informacij, ki so bile vržene stran. Tovrstne informacije se uporablja za napad na različne elektronske naprave. Brskanje po smeteh ni omejeno samo na zavržene listine, ki vsebujejo različna gesla. Na prvi pogled nedolžne informacije kot so računi, zapiski, koledar z dejavnostmi, lahko pomagajo napadalcu s pomočjo socialnega inženiringa izkoristiti informacije za napad na elektronske naprav ali omrežja.

PREVENCIJA IN ODZIV NA INCIDENTE:

- Zavržene listine s občutljivimi informacijami morajo biti skrbno uničene do neprepoznavnosti,

- Ozaveščanje o nevarnosti brskanja po smeteh.

- Razmisliti komu lahko zaupamo računalnik/mobilno napravo v popravilo.

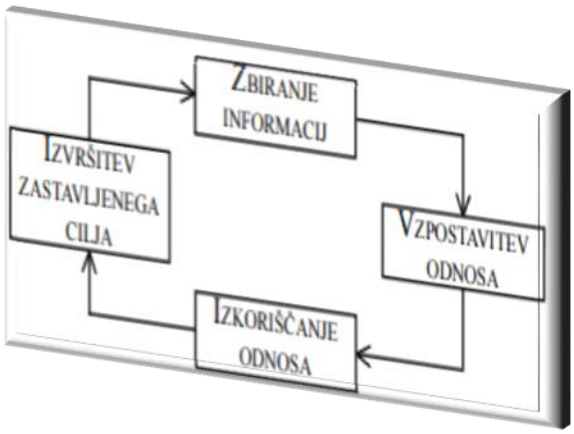
2.22 Preprečevanje napadov socialnega inženiringa

Da bi sploh razumeli socialni inženiring, je pomembno, da se zavedamo, kako poteka sam cikel socialnega inženiringa ter katere so najpogostejše tehnike uporabljene v te namene.

OPIS PROBLEMA:

Socialni inženiring je ena najpogostejših tehnik zlorabe osebnih podatkov in sicer gre za nabor tehnik s pomočjo katerih napadalec od žrtve pridobi zaupne podatke z manipulacijo, prevaro ter zlorabo zaupanja. Obstaja več načinov, s katerimi napadalec pridobi podatke od žrtev: s tehničnimi metodami, osebnim stikom, grožnjami in izsiljevanjem. S pomočjo socialnega inženiringa ne prihaja le do kraje zasebnih informacij, pač pa tudi do kraje denarja ter identitet.

Cikel socialnega inženiringa poteka v 4 fazah: zbiranje informacij, vzpostavitev odnosa, izkoriščanje odnosa in izvršitev zastavljenega cilja.



V prvi fazi »storilci« lahko **zbirajo informacije** o svoji potencialni »žrtvi« in sicer s pomočjo računalniške tehnologije ali pa s pomočjo interakcije (medosebnega stika). V drugi fazi začnejo **vzpostavljati odnos** z »žrtvijo«. V tretji fazi **izkoriščajo odnos**, ki so ga vzpostavili, tako da od žrtve pridobijo kar se da veliko informacij. Žrtev se včasih niti ne zaveda, da izdaja pomembne ali zaupne podatke o sebi. V četrti fazi pa storilci preidejo k »bistvu« in podatke zlorabijo - jih uporabijo sebi v prid za **dosego (izvršitev) zadanega cilja**.

Najpogostejše tehnike socialnega inženiringa so sledeče:

- Zbiranje informacij s pomočjo interneta (spletni brskalniki, socialna družbena omrežja, ribarjenje, pharming napadi, trojanski konji, virusi in črvi),
- Socialni inženiring preko telefona in telefonsko zvabljanje,
- Neposredni pristop in ankete,
- Gledanje čez ramo,
- Brskanje po smeteh,
- Podatki na nosilcih podatkov,
- Ostalo (piškotki, mobilni telefoni, dlančniki, bluetooth, brezžična omrežja).

PREVENCIJA IN ODZIV

Kako se torej zaščititi pred socialnim inženiringom?

Najprej je potrebno dvakrat podčrtati **IZOBRAZBO**. Kdor ima več **znanja** o neki zadevi, se lažje znajde, kadar je v situaciji, ki zahteva to določeno znanje.

Kadar govorimo o socialnem inženiringu, ki podatke najpogosteje pridobiva s pomočjo interneta je najbolj smiselno govoriti o varovanju osebnih podatkov. Na spletu se dandanes namreč pojavlja veliko informacij skoraj o slehernem posamezniku, ki jih lahko zlahka pridobi kdorkoli. Lahko jih posameznik objavi sam na socialnih omrežjih in v takem primeru je pred objavo vredno in pametno **vsaj dvakrat premisliti, katere podatke bi radi delili in s kom**. Zavedati se moramo, da ko je nek podatek enkrat na internetu, tam tudi za vedno ostane.

V povezavi z lažnimi spletnimi stranmi in phishingom se lahko najbolje zavarujemo tako, da se **prepričamo, da je stran, ki jo uporabljamo, res prava** in to **še preden vnesemo kakršne koli podatke** (preverjamo, če gre za pravi URL naslov spletne strani). Pri pharming napadih URL težko preverimo, saj gre za pravi URL in nato na preusmeritev. Take oblike napada je zelo težko prepoznati.

Na hitro o ribarjenju (phishingu) in pharmingu:

Izraz ribarjenje podatkov (phishing) izvira iz angleških besed za geslo (password) in ribarjenje (fishing). Gre za nezakonit način zavajanja uporabnikov, pri katerem poskuša prevarant s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnikov na takšen ali drugačen način izvabiti njihove osebne podatke. Praviloma storilci najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa od vas z lažnim elektronskim sporočilom poskušajo izvabiti bodisi obisk te strani ali kar takoj pridobiti vaše podatke z vašim odgovorom na to sporočilo.

Pharming napad pa je spreminjanje vpisov DNS, kar povzroči, da uporabnike (ki in ko obiščejo določen spletni naslov) preusmeri na napačno spletno mesto.

Glavna razlika med phishing-om in pharming-om je v tem, da gre pri pharmingu bolj za tehnični napad kot za tehniko socialnega inženiringa, na katerem temelji ribarjenje podatkov. Praviloma gre bodisi za neposreden napad na DNS strežnike, bodisi za napad na določeno datoteko, ki se nahaja na računalniku uporabnika. Uporabnik je v teh primerih prepričan, da se nahaja na pravi strani, saj je vtipkal pravi URL naslov strani, v resnici pa ga je eden od omenjenih načinov napada preusmeril na lažne strani, ne da bi se pri tem spremenil URL naslov v oknu brskalnika. Uporabnik je seveda v tem lažnem zaupanju dovolj samozavesten, da v vnaša svoje osebne podatke v obrazce, ki se nahajajo na takšnih straneh.

Trojanski konji, virusi in črvi so uporabno orodje za storilce. - vsi namreč omogočajo »storilcu« prevzem nadzora nad »žrtvinim« računalnikom, zaradi česar je pridobivanje informacij »mala malica«. Pred tem se zaščitimo z izbiro in uporabo dobrih in **licenciranih antivirusnih programov**, priporočljiva oziroma celo obvezna pa je tudi **uporaba požarnega zidu**.

Storilci lahko podatke pridobivajo tudi preko telefona ali v živo. Pomembno je, da **preko telefona** neznancem (včasih niti znancem) **ne izdajamo nobenih pomembnejših informacij o sebi** ali svojih bližnjih/prijateljih/znancih… Pomembnejše podatke rajši zadržimo zase.

Tudi, kadar »storilec do nas pristopi v živo, je pomembna uporaba **zdrave pameti** (če naj bi anketa, v katero nas prepriča »storilec«, ugotavljala znanje angleščine, potem pa »storilec« vpraša za TRR? – pobegni! :D). Včasih se storilci zamaskirajo tudi kot najrazličnejša podpora uporabnikom – zato lahko direktno vprašajo za uporabniško ime in geslo. Najboljša oblika preprečevanja takšnih napadov je **pogosta zamenjava gesel**, saj je take oblike napadov težko prepoznavati, redna zamenjava gesel pa preprečuje večjo škodo (četudi je bila ta morda že povzročena).

Brskanje po smeteh in nosilci podatkov so za »storilce« uporaben vir podatkov. Pomembno je, da **imamo »pospravljen« tudi koš za smeti** in **redno pregledujemo svoje nosilce podatkov**, če pa gre za nam neznani nosilec

(npr. tuj USB, za katerega mislimo, da ga je nekdo pozabil) pa je to najbolje **predati osebi, ki se na informacijsko tehnologijo spozna** – na »pozabljenem« USB ključku se lahko namreč skriva zlonamerna programska oprema.

Ostale tehnike, s katerimi se izvajajo napadi socialnega inženiringa, zajemajo piškotke, mobilne telefone, dlančnike, bluetooth in brezžična omrežja. Pri piškotkih je pomembno, da **smo ustrezno obveščeni o piškotkih** in njihovi uporabi.

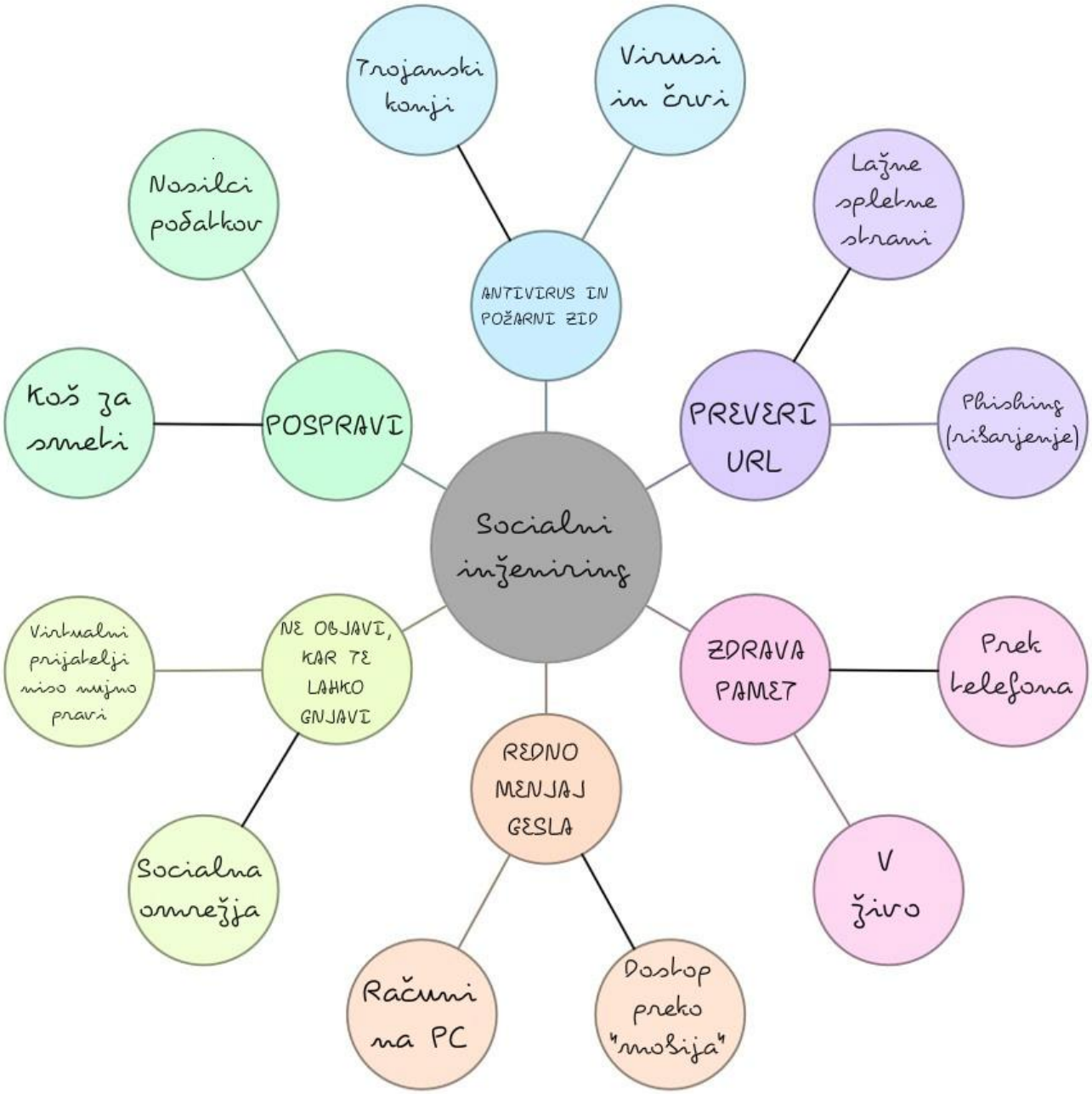
Pri mobilnih telefonih in napravah, dlančnikih ter tabličnih računalnikih danes veljajo načeloma **ista pravila kot za uporabo in rokovanje z računalniki**. Mobilne naprave so sedaj že skoraj popolnoma nadomestile računalnike, preko njih uporabljamo splet, opravljamo telefonske klice, uporabljamo spletne trgovine/banke, smo povezani z raznovrstnimi aplikacijami, uporabljamo socialna omrežja… **Pazljivost pri uporabi gesel in objavljanju informacij ni nikoli odveč**. Bluetooth uporabljamo le, kadar smo z osebo, s katero souporabljamo določene dokumente, slike… Nato ugasnemo vidljivost in **izklopimo Bluetooth po vsaki uporabi**. Kadar uporabljamo brezžična omrežja ali če naše brezžično omrežje oddaja, je to potrebno zavarovati z geslom, ki ga redno menjamo.

UKREPI	PLUSI	MINUSI
Izobrazba	Imaš znanje	Morda te ta tema ne zanima, kar pomeni težavnejše učenje
2x premisli komu daš podatke	Ni težko premisliti, komu lahko zaupaš	Razmislek vzame več časa
Preveri, če je stran prava	Obvaruje te pred napadom	Vzame več časa za pregled istovetnosti strani, morda se na to ne spoznaš najbolje
Antivirusni program, požarni zid	Varuje tvoj računalnik	Lahko se zgodi, da skupaj z antivirusnim programom na svoj računalnik preneseš tudi vohunsko opremo (spyware)
Preko telefona nobenih informacij	Osebni stik zagotavlja večjo gotovost, veš s kom govoriš	Vprašanje, kaj če kdo res nujno potrebuje tvoje podatke, za tvojo korist (še vedno lahko preveriš v določeni ustanovi)
Pogosta zamenjava gesel	Četudi ga izgubiš, ga po menjavi ne morejo zlorabiti	Zapomniti si vsa gesla, lahko pomotoma vneseš staro geslo, kar ponovno pomeni dolgotrajnejšo prijavo... itd.
Pospravljen koš za smeti	Ni datotek s tvojimi podatki	Sprotno pregledovanje spet vzame nekaj časa
Redno pregleduj nosilce podatkov	Enako kot za koš za smeti	Dolgo traja
Izklopi bluetooth po vsaki uporabi	Ne morejo dostopati do tvojega telefona oddaljeno	Veliko lažje ga je imeti vedno ON

PRIMERI IN ZANIMIVOSTI

- https://sl.wikipedia.org/wiki/Socialni_in%C5%BEeniring
- http://www.varnostnaspletu.si/Primeri-socialnega-inzeniringa/
- https://www.varninainternetu.si/2011/preverite-identiteto-posiljatelja/
- https://www.youtube.com/watch?v=lc7scxvKQOo
- https://www.youtube.com/watch?v=e-ZcomTYc64

- https://www.youtube.com/watch?v=XegdPElp81A



2.23 Varna raba socialnih omrežij

OPIS PROBLEMA

Socialno mreženje je spremenilo način komuniciranja s prijatelji in znanci. Čeprav socialna omrežja, kot so Facebook, Twitter, YouTube, Google+, itd. igrajo pomembno vlogo v našem življenju, predstavljajo tudi visoko tveganje za varnostne grožnje. Z milijoni uporabnikov taka omrežja ne privabljajo le prijateljev in družine, kateri bi želeli ostati v stiku, vendar tudi tiste ljudi, ki želijo izvedeti vse o tebi zaradi napačnih razlogov. Posameznik mora biti izjemno pazljiv kakšno sled pušča za seboj ko je na spletu. Slike na Instagramu, pisanje Facebook statusov, kibernetsko ustrahovanje, spletna varnost, informacije o kreditnih karticah, kraja identitete, grafična vsebina, varna gesla ipd. okrepijo obstajajočo nevarnost, ki preti naši fizični, digitalni, finančni in na splošno varnostni dobrobiti. Posamezniki, predvsem pa najstniki, ki so preveč samozavestni oz. premalo previdni na socialnih omrežjih so najlažje in najboljše tarče, ter tudi najbolj ogroženi.

NAJVEČJE GROŽNJE:

1. **Kraja identitete**

Tatovi identitet zberejo osebne informacije s strani socialnih omrežij. Četudi ima posameznik svoj račun zavarovan na najvišjem nivoju varnosti, še zmeraj obstajajo načini s katerimi tatovi lahko pridejo to informacij. Večina strani socialnih omrežij imajo informacije kot so e-mail naslov in rojstni da. Zelo znan način kraje identitete je, ko tat vdre v e-mail račun z uporabo socialnih informacij. Npr. najpogostejša tehnika je, da tatovi kliknejo na opcijo 'pozabil sem geslo' in poskušajo pridobiti informacije skozi e-mail. Ko imajo dostop do nekega e-mail računa, imajo nato dostop do vseh informacij o posamezniku preko njegovih socialnih mrežnih strani.

Na socialnih omrežjih, lahko sam opredeliš ali želiš da je objava javna, ali je objava vidna tvojim prijateljem ali tudi prijateljem od prijateljev. Na podlagi javnih objav lahko osebe sestavijo tvoje življenje in ukradejo identiteto. Vedo kje živiš, kdo so tvoji sosedje, prijatelji, kakšno pivo piješ in s kom se družiš.

2. **Vdor v računalnik oz. socialni profil**

Hekerji obožujejo socialna omrežja, saj gredo lahko prav do samega vira, da vnesejo zlonamerno kodo. S temi kodami lahko ukradejo posameznikovo identiteto, vnesejo viruse na računalnik, pridobijo podatke o bančnih računih, itd. Skrajšani URLji so še posebno dovzetni za hekerje, saj s takimi povezavami lahko ukanijo uporabnike in jih pripravijo da obiščejo škodljive strani, kjer so lahko njihove osebne informacije nato zlorabljene.

3. **Prepogosta in prevelika objava informacij**

Ko posameznik uporablja socialna omrežja objavlja svoje osebne informacije. Ko so te enkrat objavljene so javne in nič več privatne, ter lahko padejo v narobne roke. Potrebno se je tudi zavedati, da **ko enkrat nekaj objavimo na internetu, to ostane gor**, pa čeprav jih morda kasneje zbrišemo! Več kot posameznik objavlja in razkrije o sebi, bolj ranljiv postaja in bolj privlačen za tiste, ki mu želijo škoditi. Posameznikovi prijatelji, znanci, znamke katere ima 'rad', strani na katere je prijavljen, aplikacije, ki jih je naložil, igre, ki jih igra, slike, ki jih je objavil in podobno, lahko vse izdajo kritične informacije o njem. Tudi ko posameznik obišče strani, ki vsebujejo 'piškotke', ga je precej lahko spremljati, saj so vsi piškotki med seboj različni in sledijo njegovi aktivnosti. Če posameznik ne želi, da strani sledijo njegovi aktivnosti, je najbolje da vsakič klikne na opcijo 'Ne sledi', ter na vsake toliko zbriše predpomnilnik ter piškotke na spletnem brskalniku, da bi preprečil probleme. Lahko uporablja **tudi anonimen način (zasebno okno)**, ki ga omogočajo nekateri brskalnik.

4. **Obveščanje o lokaciji, potovanjih in ostalih ranljivih podatkih**

S tem ko posameznik pove svetu kje je in kam se odpravlja, ter s tem sporoči da ga takrat ni doma, k sebi vabi vlomilce. Vlomilci se zmeraj dobro prepričajo, če so prebivalci doma in s tem ko član družine na socialnem omrežju objavi, da se z družino odpravlja na potovanje za 2 tedna, da vlomilcem zeleno luč, saj točno vedo kdaj prebivalcev ni in kdaj se vrnejo. Enako velja tudi za fotografije, objavljene na potovanjih.

PREVENCIJA

Ni potrebno, da zaradi teh groženj zbrišemo vse svoje profile na socialnih omrežjih, vendar lahko sledimo naslednjim previdnostnim ukrepom:

- **Močno geslo**: Močnejše kot je geslo, težje ga je ugotoviti. Uporaba posebnih simbolov in velikih črk
- **Pazljivost pri pisanju statusov**: Pogosto se zgodi, da posameznik čisto nedolžno objavi status, s katerim razkrije informacije, katere so tatovom v veliko pomoč. Npr. posameznik lahko napiše 'Vse najboljše moji mami!' in jo označi v status. Tako se lahko ugotovi tudi mamino dekliško ime, kar je eno izmed zelo

pogostih vprašanj pri ugotavljanju pozabljenega gesla za e-mail: 'Kakšno je dekliško ime tvoje mame?' To pa predstavlja precejšnjo nevarnost in seveda korist za tatove.

- **Lokacija naj ostane skrita**: Če posameznik želi v svoj status označiti lokacijo, naj ta lokacija nebo specifična. Naj tudi ne objavlja slik svojega prebivališča ali okolice, saj tako lahko izda tatovom ranljive informacije.
- **Paziti kakšne fotografije se objavlja in pošilja**, nikakor pa se ne posluževati t.i. Sextinga, kjer se pošilja gole ali neprimerne fotografije, saj jih izjemno hitro lahko prestrežejo in izkoristijo napačni ljudje, pride lahko tudi do izsiljevanja, javne objave fotografij in sramu!
- **Uporaba največje možne varnosti** na socialnih omrežjih in pazljiva izbira kontaktov ter objave osebnih informacij!
- **Paziti katere prošnje za prijateljstvo se sprejme**: Če posameznik spozna osebo preko spleta in bi se nato rad dobil z njo, mora biti prej tudi izjemno prepričan o njej in previden, saj gre lahko za predatorja, ki bi posameznika v živo ali preko spleta le rad izkoristil!

Eden izmed najboljših načinov kako se izogniti vdoru v socialni profil je, da se ne klikne na sumljive povezave, dokler se ne ugotovi iz kje izhajajo oz. kakšen je njihov izvor. Če posameznik z miško lebdi nad skrajšano povezavo, se v spodnjem kotu prikaže celoten URL naslov, in le če ga posameznik prepozna, naj klikne nanj.
Poleg zlonamernih povezav, pa obstajajo tudi ostale različne zlonamerne, vohunske in oglaševalske ter izsiljevalske programske opreme. Potrebno je paziti, da se ne odpira čudnih povezav, slik ter datotek poslanih od neznancev, včasih pa se je dobro prepričati tudi pri prijateljih, če so zares oni tisti, ki pošiljajo določeno vsebino. Pogosto se namreč pripeti, da se posameznikov račun lahko okuži z zlonamernim virusom in nato svojim kontaktom posreduje škodljivo vsebino in nezaželena sporočila. Paziti je treba tudi, da se računa nikoli ne pusti nenadzorovanega in se ne pozabi izpisati iz njega, še posebno če se do njega dostopa na javnih računalnikih!

Ko se posameznik odpravi na potovanje, naj zadrži potovalne načrte zase in nikoli ne izda, kdaj, kam in za koliko časa se odpravlja. Priporočljivo je tudi, da slike objavi šele ko pride s potovanja in uporabi najvišjo varnost oz. določi kdo lahko vidi te slike.

Pogosta je tudi prevelika samozavest posameznika, saj misli da je dobro zavarovan, da mu nihče ne more priti do živega in da ne objavlja nobenih kritičnih informacij, katerih zloraba bi mu lahko škodovala. Vseeno pa so informacije kot so potovalni načrti, podatki o bančnih računih, domači naslov in rojstni datum, imena družinskih članov in njihovi rojstni datumi, lokacija in dnevna rutina, zelo ranljive in jih kriminalci lahko hitro izkoristijo. Takih podatkov tudi ni priporočljivo pošiljati po sporočilih, klepetalnikih in e-mailih, saj se jih zelo hitro prestreže,

informacije pa se nikoli ne zbrišejo z interneta. Če se kakšne ranljive informacije že pošiljajo preko e-maila, naj bodo prej ustrezno zašifrirane, da jih lahko odkodirata le pošiljatelj in prejemnik.

Dobra stran socialnih omrežij je, da te lahko pomagajo posameznikom tako da:

- ostanejo v kontaktu z družinskimi člani in prijatelji
- sodelujejo pri različnih neprofitnih kampanjah ali dobrodelnih organizacijah
- povečajo njihovo kreativnost skozi objave idej, glasbe, fotografij, itd.
- spoznajo še druge ljudi s podobnimi interesi

Slaba stran

Socialna omrežja lahko sprožijo spletno ustrahovanje in razne vprašljive dejavnosti in prej omenjene grožnje. Posamezniki, predvsem najstniki delijo na družbenih omrežji več kot bi smeli, brez da bi pomislili na posledice, postanejo pa lahko tudi tarče internetnih prevar ter zlorab.

<u>ODZIV</u>

- Zaupati prijateljem, družini in ostalim odraslim če se dogaja ali se je zgodilo kaj takega, kar bi bilo potrebno razrešiti!
- Če pride do izsiljevanja oz. ustrahovanja preko interneta, je potrebno čim hitreje kontaktirati osebo vredno zaupanja in ukrepati, saj lahko to pripelje tudi do hujših stvari!

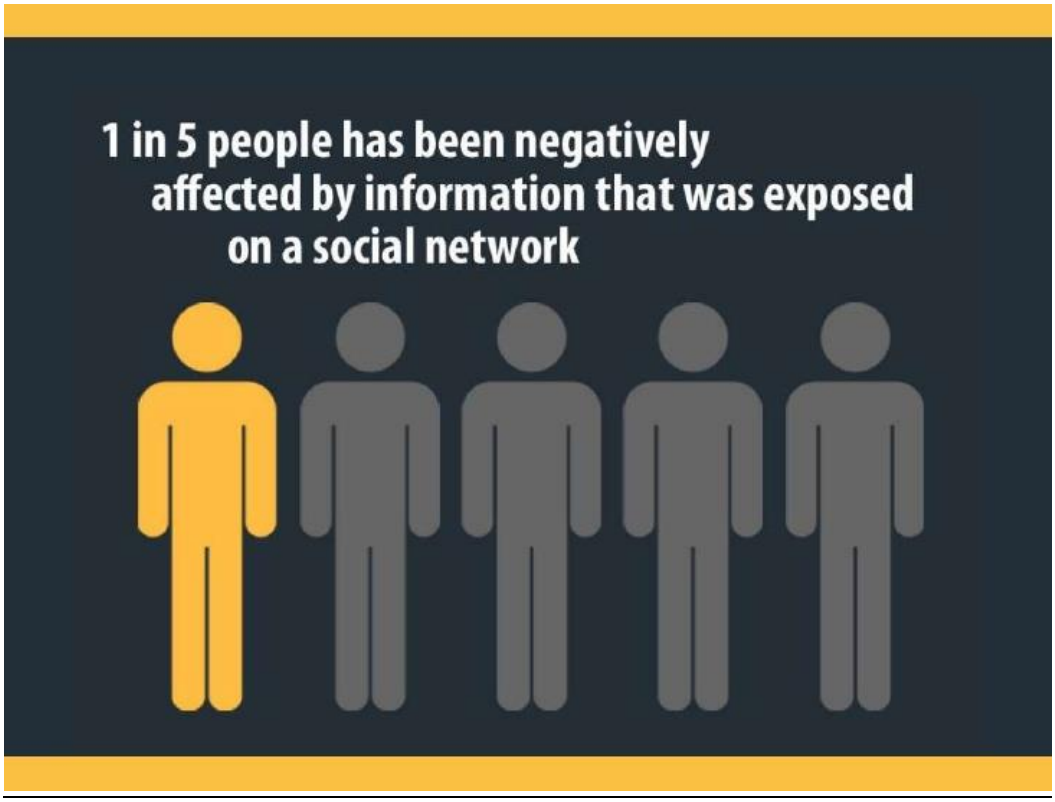
Z večjim ozaveščanjem in znanjem o tej tematiki, je posameznik tudi bolje zaščiten in varen. Več si lahko preberete ali kontaktirate strokovnjake na naslednjih straneh:

- https://www.varninainternetu.si/articleType/prevare-na-druzbenih-omrezjih/
- https://safe.si/

- https://www.varninainternetu.si/prijavi-prevaro/

ZANIMIVOSTI/PRIMERI

- https://www.youtube.com/watch?v=QUyla_nMJis
- https://www.youtube.com/watch?v=GCWBf7WKYyA



2.24 Odzivanje na zaznane grožnje

OPIS PROBLEMA:

Najsi gre za človeške napake, namerno vohunjenje, sile narave, napake in okvare tehnične programske ali strojne opreme, namerna dejanja sabotiranja in vandalizma, namerna dejanja tatvine ali namerne napade na programsko opremo – vse pomeni možnost izgube pomembnih informacij in še večjo možnost zlorabe teh podatkov, če do izgube res pride. Kakorkoli je pomembno, da zna oseba, ki prva **prepozna**, da ima neka grožnja informacijske varnosti veliko možnost, da se uresniči, oz. v slabšem primeru, **da se je grožnja že uresničila**, **pravilno reagirati** na nastalo situacijo.

PREVENCIJA IN ODZIV

Preden situacija grožnje sploh nastane, je **najbolj pomembno preprečevanje** te grožnje, oz. t.i. **preventiva**.

Največjo varnost namreč zagotovimo, če že vnaprej preprečimo nastanek ali obstoj neke grožnje. Sem spada uporaba raznih tehnologij, kot so npr. **antivirusni sistemi**, **požarni zid** oziroma požarna prepreka in **protivohunska oprema**. Grožnje lahko preprečujemo tudi tako, da redno skrbimo za **posodobljenost opreme**, ki jo uporabljamo, ter da se poslužujemo **nalaganja varnostnih dodatkov**.

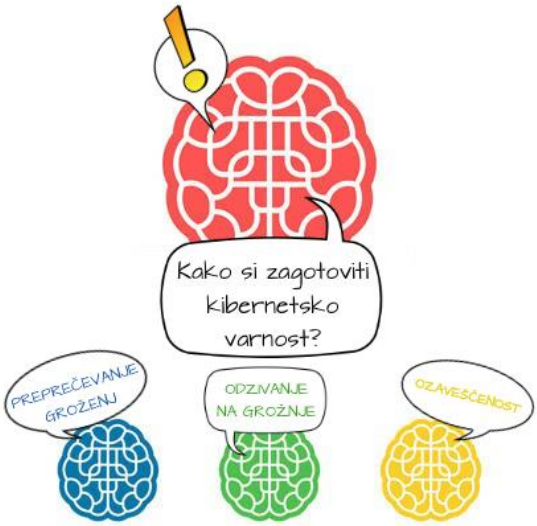
Vendar pa včasih samo preventiva žal ni dovolj oziroma ne zagotavlja dovolj visoke stopnje varnosti. Zelo pomembno vlogo tu predstavljata **odzivanje** in **ozaveščanje**. Groženj informacijske varnosti žal ne bo nikdar mogoče v celoti odpraviti, zato je pomemben način, kako se ob uresničenih grožnjah odzvati. Zelo dobro se je pri tem navezovati na **znanje, ki ga posameznik uporablja že za samo preprečevanje groženj**, saj je zelo uporabno, četudi grožnje nismo uspeli preprečiti vnaprej. S tem znanjem lahko grožnji preprečujemo njeno rast in nastanek vse večje škode. Na tem mestu bi lahko omenili **analizo tveganj**, ki se osredotoča na tveganja, grožnje, kako nastanejo in kakšen je najboljši način, da delovanje grožnje preprečimo s čim manj povzročene škode. Zelo, zelo pomembna je **ozaveščenost**. Ljudje so namreč tisti, ki informacijsko-komunikacijske tehnologije razvijajo, uporabljajo in zlorabljajo. Če ljudje poznajo določena tveganja, npr. da lahko kdo z zli nameni zlorabi

geslo njihove spletne banke, potem njihova **ozaveščenost že v osnovi pripomore k preprečitvi grožnje**, torej kraje gesla, saj ga pogosteje menjajo, ne izdajajo vsakomur po telefonu ali sosedu na ulici. Seveda kot najstnik še ne moreš vedeti vsega o pasteh, ki prežijo nate, kadar si v svojem spletnem svetu. Zato naj ti ne bo nerodno zaupati se staršem, bratom, sestram, prijateljem ali celo strokovnjakom, če se ti neka grožnja uresniči. Če na splet uidejo tvoji zasebni podatki, kot so, na primer, tvoje gole fotografije, se tega ne boj povedati staršem, saj bodo morda lažje in bolj učinkovito ukrepali kot je to v tvoji moči. Tudi strokovnjaki ti bodo priskočili na pomoč, zato naj te ne skrbi, da bi tudi oni videli tvojo zasebno fotografijo – četudi jo bodo videli, bodo poskrbeli, da se tvoja fotografija ne širi naprej ter da je ne vidi še več tvojih vrstnikov, znancev ali tujcev.

Kar pa je v tvoji moči je preventiva, torej da preden komurkoli pošlješ svojo fotografijo ali preden sam objaviš sporne podatke (ko si morda v kakšnem »ekstazičnem« stanju – npr. prehuda zaljubljenost, opitost…) vseeno premisliš, kakšne posledice lahko nastanejo. Bo že držalo, da se na napakah učimo, vendar pa so nekatere napake vseeno preveč neprijetne, da bi lahko potem nezaznamovano nadaljeval svoj vsakdan. Zato VEDNO raje dvakrat premisli, kdo je vreden zaupanja in komu dovoliš vstopiti v svojo zasebnost!

PRIMERI IN ZANIMIVOSTI

- http://www.24ur.com/novice/slovenija/ma-si-prf-dajmo-pretepst-ce-tako-se-na-spletu-vedejo-in-zalijo-mladi-slovenci.html?ts=1379130894&stream_cat=2
- http://www.24ur.com/14-letnica-v-smrt-zaradi-spletnega-portala-so-krivi-starsi-z-zbirko-otrokovih-fotografij-na-facebooku.html



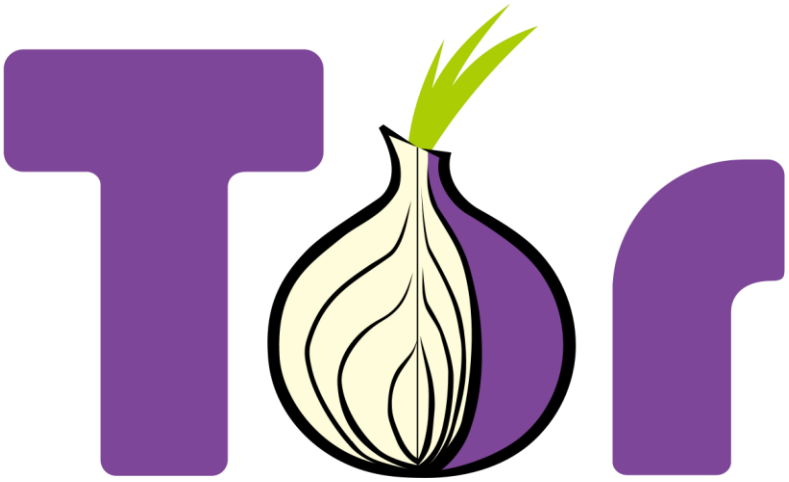
2.25 Nevarnosti anonimnih omrežij

OPIS PROBLEMA

Vsak klik na internetu, vsaka objava, vsak poslan e-mail in vsaka naložena datoteka je nekje spremljana s strani nekoga. Zato obstaja ogromno razlogov zakaj bi se nekdo želel na internetu napraviti nevidnega, te razlogi pa variirajo od razumljivih do zlonamernih. Eden izmed načinov kako postati anonimen na internetu je uporaba programa oz. brskalnika Tor.

KAJ JE TOR IN KDO GA UPORABLJA?

Omrežje Tor je skupina prostovoljno upravljanih strežnikov, kateri ljudem omogočajo izboljšanje njihove varnosti in zasebnosti na internetu. Uporabniki Tor-a se preko njegovega omrežja povežejo skozi serijo virtualnih kanalov, namesto da bi se direktno povezali na določeno stran, kar dovoljuje tako organizacijam kot posameznikom da delijo informacije preko javnih omrežij brez, da bi ogrozili svojo zasebnost. Uporabnikom omogoča, da te brskajo po internetu brez, da bi jim sledile korporacije, vladne agencije in drugi prisluškovalci. Te internetne komunikacije so anonimne, saj uporabljajo sloje enkripcije oz. šifriranja – drugače imenovane kot čebulno usmerjanje. Zakaj čebula? Ker je sestavljena iz številnih slojev, prav na podoben način pa deluje tudi Tor omrežje. Prisluškovalec, bi se zelo težko (ali celo nebi) dokopal do uporabnika preko vseh slojev.

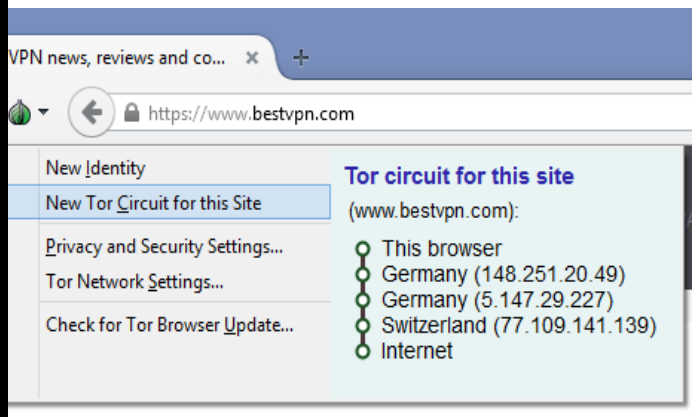


Tor uporabljajo različni tipi ljudi za različne razloge. Uporabljajo ga navadni ljudje, novinarji, organi kazenskega pregona, blogerji, aktivisti, vojska, IT profesionalci in na žalost tudi kriminalci. Navadno se Tor uporablja zato, da prepreči spletnim stranem sledenje posameznikom in njihovim družinskim članov, da se lahko posamezniki povežejo na stranmi z novicami, komentirajo in se pogovarjajo anonimno. Uporabniki lahko tudi objavljajo spletne strani in ostale aktivnosti ter ponudbe, brez da bi s tem razkrili svojo lokacijo oz. lokacijo strani. Nekateri posamezniki uporabljajo Tor tudi za družbeno ranljive komunikacije: klepetalnice in spletni forumi za žrtve posilstev, ali ljudi z boleznimi. Uporablja se tudi za raziskovanje senzitivnih tem in področij, ter za dostopanje do

različnih dokumentov in člankov, do katerih drugače posameznik nebi mogel priti. Poleg dobre uporabe Tor-a in raziskovanja dark weba, pa ta vsebuje tudi t.i. darknet, kjer se nahaja veliko nevarnosti. Vključuje ogromno število spletnih strani, katere ponujajo ilegalne aktivnosti ali produkte, vključujoč distribucijo nedovoljenih spolnih posnetkov in posnetkov spolne zlorabe otrok, distribucijo prepovedanih drog, kraje identitet, bančnih goljufij, storitve mafije in najetih morilcev. Znano je da Tor uporabljajo tudi razne heker-aktivistične grupe in kriminalna ter teroristična podjetja/celice. Izredno pomembno je, da je posameznik previden do kakšne vsebine dostopa, jo pregleduje in uporablja, ter da se ne vpletajo v takšne ilegalne aktivnosti.

KAKO DELUJE TOR?

Uporaba Tora posameznika zaščiti pred znano in splošno vrsto internetnega nadzora poznano kot 'analizo prometa'. Analiza prometa se uporablja, da se ugotovi kdo komunicira s kom preko javnih omrežij. Če prisluškovalci poznajo vir in destinacijo posameznikovega internetnega prometa, lahko sledijo njegovem obnašanju in zanimanjih. Tor torej zmanjša tveganje tako preprostih kot sofisticiranih analiz prometa z distribucijo posameznikovih transakcij preko številnih mest na internetu, tako da ne more nobena posamezna točka povezati posameznika z njegovo destinacijo. Ideja je podobna kakor uporaba zavite poti, kateri je izjemno težko slediti z namenom, da sledilca odvržemo s poti – in potem periodično zbrišemo za seboj sledi. Namesto da bi šla povezava po direktni poti od vira do destinacije, se podatkovni paketi na Tor omrežju odpravijo na naključno pot skozi številne plasti, ki za seboj zakrijejo sledi, tako da niti na eni točki opazovalci oz. prisluškovalci ne morejo vedeti iz kje so te podatki prišli in kam so namenjeni.



PREVENCIJA

Vseeno pa ni dovolj, da posameznik uporablja le Tor omrežje, ko dostopa do spletnih strani, vendar se mora vedno prepričati, da je povezava varna – https. Strani, katere ne vključujejo 'S' na koncu 'http', niso varne povezave, včasih tudi ob uporabi Tora ne!

Tor ne more rešiti vseh problemov anonimnosti. Osredotoča se le na zavarovanje transporta podatkov. Če posameznik ne želi, da strani vidijo informacije, ki bi ga lahko identificirale, mora uporabiti protokolno-specifično podporno programsko opremo. Npr. posameznik lahko uporabi Tor brskalnik med tem ko brska po spletu, da zadrži podatke o konfiguraciji njegovega računalnika.

Posameznik lahko zaščiti svojo anonimnost tudi z zdravo pametjo. Naj ne predloži svojega imena in drugih osebnih podatkov na spletnih forumih in drugje po spletu, ter se ne vključuje v ilegalne aktivnosti.

Priporočljivo je, da posameznik ne nalaga ničesar s Tora, še posebno kakšnih čudnih dokumentov, ali jih vsaj ne odpira, ko je še v Toru. Posameznik naj tudi ne poveča brskalnega okenca do konca in naj ne omogoča ali nalaga vtičnikov brskalnika (Flash, RealPlayer,…)

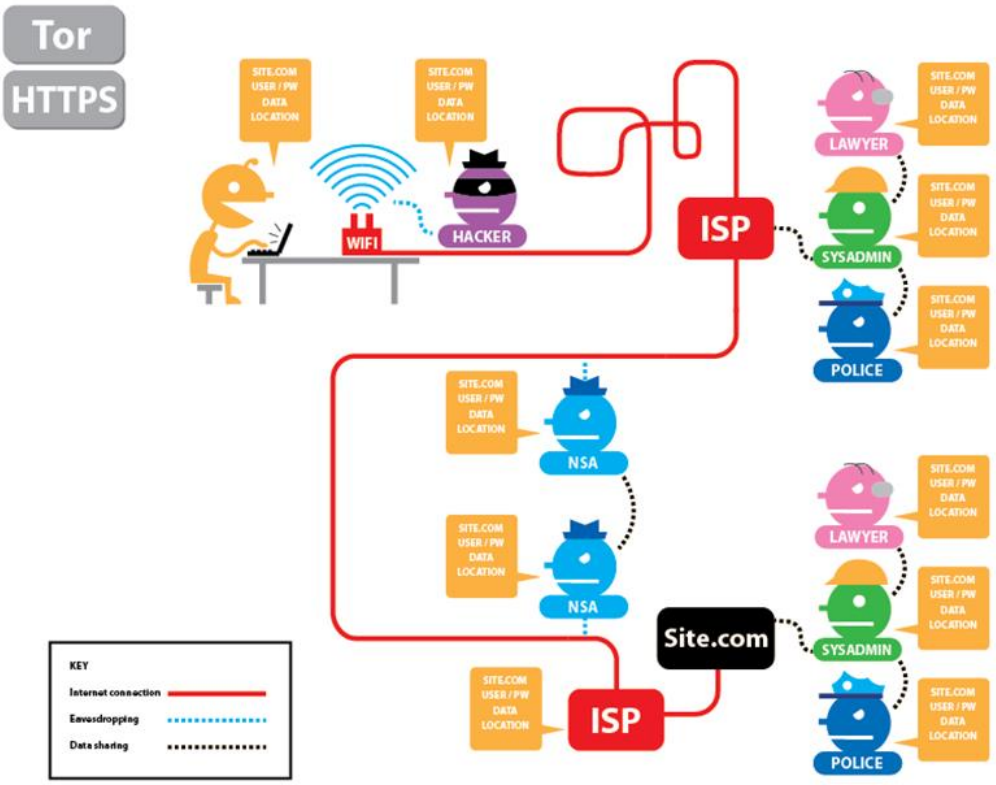
PLUSI IN MINUSI UPORABE TOR-a

Plus: Posameznik lahko anonimno brska po internetu, njegov IP naslov je skrit, lahko izraža svoje svobodno mnenje, dostopa do ogromno literature in se zavaruje.

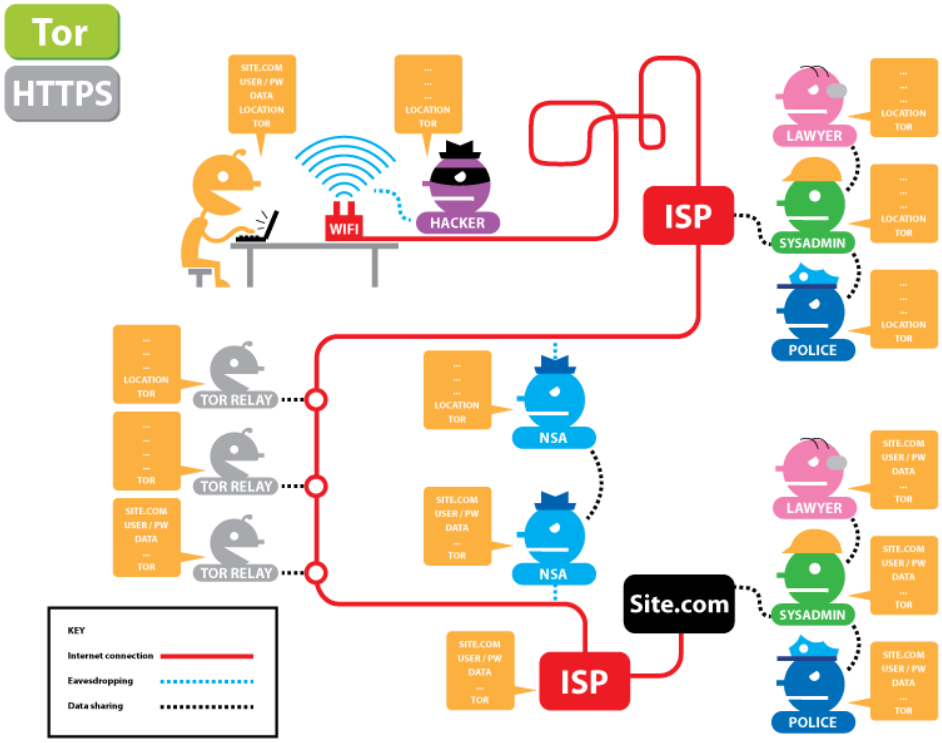
Minus: Nekateri podatki so lahko ogroženi, če se Tor-a ne uporablja skupaj z varno povezavo https, zaradi preusmerjanja Tor deluje precej počasi oz. upočasnjuje posameznikovo brskanje po spletu, vladne in državne agencije pa lahko hitro postanejo pozorne na posameznika ki koristi Tor, saj lahko mislijo, da ga želi uporabiti za kriminalne namene. Tor tudi ni najboljša rešitev za prijavljanja v e-mail račune ali račune na socialnih omrežjih, saj so nekateri IP naslovi blokirani ali pa ne delujejo najbolje v Toru, avtomatično pa se posameznik s prijavo v socialna omrežja odreče anonimnosti (strani ne vedo iz kje se prijavljaš, vedo pa kdo si), še posebno če povezava ni zavarovana s https! Tudi nalaganje torrentov z interneta ni priporočljivo, saj torrenti ignorirajo to, da posameznik uporablja Tor in je njihova povezava direktna, ter ne potujejo skozi plasti kot drugače bi!

Na spodnjih slikah so prikazani podatki, kateri so vidni ob uporabi Tor omrežja, varne povezave https in brez njiju. Potencialno vidni podatki na spletu so naslednji: stran, ki jo obiskuješ (SITE.COM), tvoje uporabniško ime in geslo (USER/PW), podatki, ki jih oddajaš/prenašaš (DATA), tvoj IP naslov (LOCATION), in ali uporabljaš omrežje Tor (TOR).

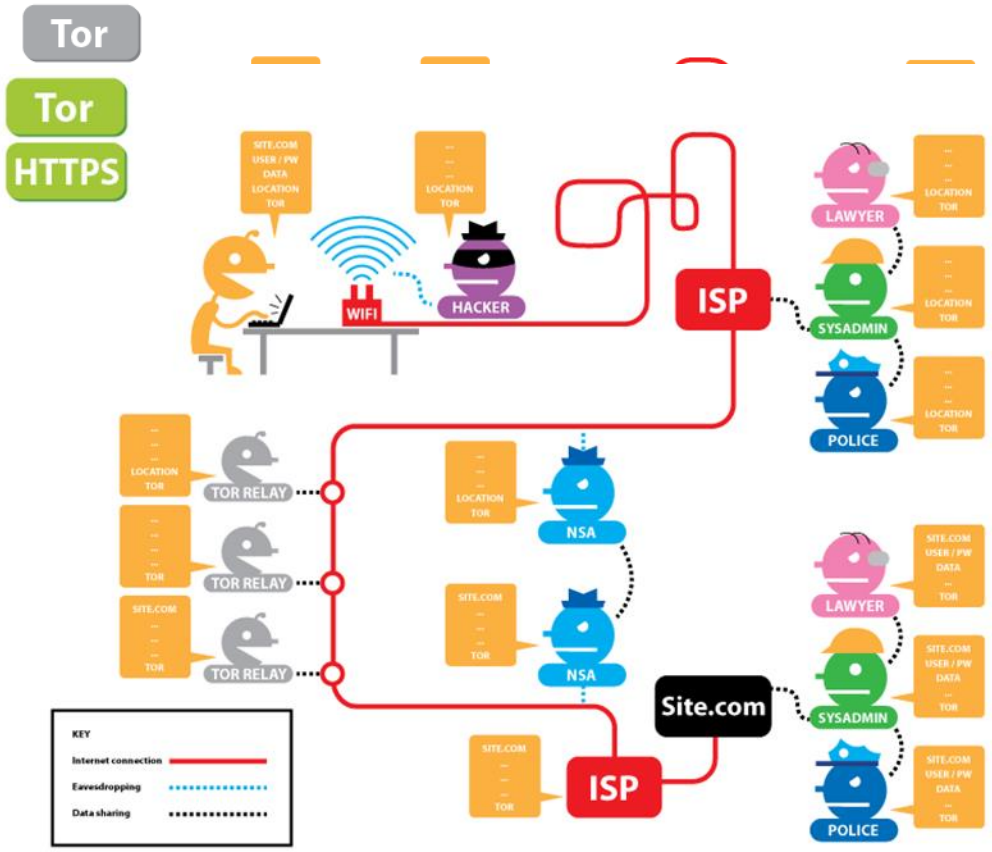
Ko sta oba gumba siva in ne uporabljamo ne omrežja Tor ne varne povezave https, so prisluškovalcem vidni naslednji podatki:



Ko uporabljamo Tor (gumb je zelen), lahko vidimo kateri podatki so in kateri niso vidni prisluškovalcem:



Ko uporabljamo varno povezavo HTTPS (gumb je zelen) lahko vidimo kateri podatki so in kateri niso vidni prisluškovalcem:



Ko uporabljamo tako Tor kot varno povezavo HTTPS, lahko vidimo kateri podatki so oz. niso vidni prisluškovalcem:

ODZIV

Če so bili podatki, ki jih je posameznik vnesel oz. razkril na Tor-u ogroženi oz. kompromitirani, lahko naredi naslednje:

- Zamenja geslo svojega računa
- Zbriše ali blokira svoj račun
- Kontaktira strokovnjake ali policijo