ŠOLSKI CENTER CELJE
SREDNJA ŠOLA ZA KEMIJO, ELEKTROTEHNIKO IN RAČUNALNIŠTVO

RAZISKOVALNA NALOGA

ETIČNO VDIRANJE V OMREŽJE

(Računalništvo)

Mentor:
Matic Holobar

Avtorja: Blaž Pečnik, R-4.b
Urh Zaveršek, R-4.b

Celje, 2019

VSEBINA

KAZALO SLIK

Zahvala

Zahvaljujeva se mentorju Maticu Holobarju, ki naju je skozi seminarsko vodil in usmirjal do rezultatov. Zahvala gre tudi vsem anketirancem, ki so odgovorili na anketo in profesorjem šolskega centra celje, ki so si vzeli čas za reševanje ankete o šolskem omrežju.

Povzetek

Hekanje se navadno povezuje z neodobrenimi vdori v računalnik ali omrežje. V seminarski nalogi pa so predstavljene metode, programi in orodja, ki jih hekerji uporabljajo. Žal pa hekanje ni več samo oddaljena beseda, ki jo zasledimo v filmih, ampak kruta realnost.

Opisani so znani predstavniki hekanja po svetu. Nato so opisani najbolj uporabljeni hekerski programi in nekaj najpopularnejših hekerskih metod. Kot že znano imajo hekerji svoje metode hekanja, zato sva opisala tudi metode zaščite oz. kako jim delo otežiti.

Ugotovila pa sva, da večino uporabniokov ni seznanjenih z nevarnostmi na spletu. Statistika ankete je pokazala, da se majhen odstotek anketirancev ne odjavlja s socialnih omrežji na tujih računalnikih.

Pod točko »šolsko omrežje« sva opisala, kakšno zaščito uporabljamo, kakšne so možnosti napada in dva postopka vdora, ki bi jih izbrala kot napadalca. Kljub majhnemu naboru znanja o vdorih sva ugotovila, da bi bilo mogoče vdreti v šolsko omrežje.

Abstract

Hacking usually connects to unauthorized intrusions to a computer or network. The seminar paper presents methods, programs and tools used by hackers. Unfortunately, hacking is no longer just a distant word that we find in movies, but a cruel reality.

Famous representatives of hacking around the world are described. Then the most used hacker programs and some of the most popular hacking methods are described. As already known, hackers have their own methods of hacking, so we also described the methods of protection, how to make their work more difficult.

However, we found that most users are not aware of the dangers of the web. Survey statistics show that a small percentage of respondents do not sign out of social networks on foreign computers.

Under the "school network" point, we described what kind of protection we are using, what are the possible attacks and the two intrusion procedures that we would choose as an attacker. Despite a small set of knowledge about intrusions, we found that it would be possible to break into the school network.

1. UVOD

Živimo v svetu tehnologije in povezanosti ljudi s pomočjo socialnih omrežij. Ta omogočajo komunikacijo po celem svetu, so pa lahko velika pomoč tistim, ki zlorabljajo tehnologijo z namenom oškodovanja neke osebe ali podjetja.
Dnevno nas preko javnih občil, mailov in tudi socialnih omrežij opozarjajo, naj bomo odgovorni do sami sebe in svojih podatkov ter pazimo, da se zaščitimo z gesli, ki spadajo pod oznako "zelo močna zaščita", kar pomeni, da mora geslo vsebovati, tako velike kot male črke, številke in ima dolžino vsaj 8 znakov. Opozarjajo nas, da naj ne odpiramo brezglavo vseh priponk, ki smo jih prejeli v naše poštne nabiralnike ali kot sporočilo preko socialnih omrežij. Žal so vsa ta opozorila največkrat zaman.

Sva dijaka srednje tehniške šole računalništva v Celju, odločitev, da predstaviva v raziskovalni nalogi načine vdorov v sisteme, možne zaščite in postopke v zvezi s tem, temelji na vdoru v šolsko omrežje.

Meniva, da ljudje ne pazijo kaj objavijo na socialna omrežja, da večina nima kvalitetnih gesel in da pri odpiranju e pošte ne pazijo dovolj kaj kliknejo. Uporabniki niso dovolj seznanjeni o oznakah, ki kažejo na varno uporabo strani v brskalnikih, pri nakupih preko interneta ne znajo preveriti verodostojnosti spletne trgovine in pri plačevanju preko spleta lahkomiselno vtipkavajo vse mogoče osebne podatke in celo dovolijo, da se razna gesla in številke TRRjev shranjujejo.

Kot dijaka računalniške šole želiva izvedeti več o vdiranju v omrežja ter spoznati metode, ki so uporabljene za vdiranje v sisteme ter kako se zaščititi pred njimi.

HIPOTEZE:

- Meniva, da profesorji ne uporabljajo enakega e-poštnega naslova za šolsko in osebno uporabo.
- Hekerski vdori se iz leta v leto povečujejo.
- Meniva, da se lahko zaščitiš pred vdori vsaj delno.
- Misliva, da je večina tarč vdorov in kraje podatkov starejše prebivalstvo.
- Večina ljudi ima šibka gesla

2. HEKANJE

Hekanje se navadno povezuje z neodobrenimi vdori v računalnik ali omrežje. Oseba, ki izvaja vdore se imenuje heker. Vsako leto se število vdorov povečuje. Hekanje ni več samo oddaljena beseda, ki jo zasledimo v filmih in redkih novicah, ampak kruta realnost.

V preteklosti je v pretežnosti šlo zgolj za vdore v omrežja in strežnike večjih podjetij. Dandanes pa takšne osebe ciljajo posamezne uporabnike interneta. Ranljivosti za hekarje ne predstavljajo zgolj napake in luknje v sistemu omrežij, ampak tudi neozaveščenost uporabnikov.

2.1 HEKERJI

Hekerji so osebe ali skupine ljudi, ki se ukvarjajo z vdori v omrežja. Vdori so lahko pooblaščeni ali nepooblaščeni, zato tudi poznamo več vrst hekerjev. Poznamo več delitev, najbolj znana delitev pa je na bele, sive in črne hekerje. Razlike med njimi se vidijo v različnih motivih, ki jih imajo in spoštovanju zakonov.

Slika 1: Heker

2.1.1 Beli Hekerji

Beli hekerji, ki jih drugače tudi imenujemo etični hekerji ali beli klobuki, so skupina računalniških strokovnjakov. Ukvarjajo se s preučevanjem vdorov in skozi analizo poskušajo odkriti pomankljivosti v varnosti omrežij podjetij. Imajo nekoliko drugačne motive kot ostale skupine hekerjev, vendar je še vedno njihov glavni motiv zaslužek. Glavna razlika, ki to skupino loči od ostalih, pa je dovoljenje za vdiranje v sisteme.

2.1.2 Sivi Hekerji

Sivi hekerji ali sivi klobuki so podobni belim hekerjem. Glavna razlika po kateri se skupini razlikujeta, pa je v dovoljenju. Sivi hekerji v sisteme ne vdirajo zlonamerno, vendar hkrati nimajo dovoljenja podjetij in s tem kršijo pravila in zakon. Glavni motiv te skupine je pomoč organizacijam in podjetjem. Najpogosteje pa te osebe postanejo beli hekerji in začnejo vdirati v omrežja organizacij z dovoljenjem oz. po naročilu.

2.1.3 Črni Hekerji

Črni hekerji ali črni klobuki je skupina strokovnjakov, ki ne spoštujejo zakonov in zlorabljajo informacijsko in internetno varnost. Glavni motiv je zaslužek. V sisteme vdirajo z namenom, da bi ga uničili ali ukradli zaupne podatke in jih prodali za zaslužek.

Slika 2: Črni, sivi in beli klobuki

2.2 HEKERSKA ETIKA

Je pojem, ki je sestavljen iz več načel. Glavna načela hekerske etike so:

- Deljenje: Dolžnost hekerja, da deli in širi podatke ter informacije z drugimi.
- Vsi imajo pravico do računalnika in dostopa do spleta.
- Vdiranje v sisteme je dovoljeno za raziskovanje, dokler se oseba ravna po zakonih.

3. HEKERSKE TEHNIKE

3.1 BAIT AND SWITCH

Napadalec želi ukrasti podatke uporabnika, zato kupi oglaševanje na spletni strani po lastni izbiri. Reklama oziroma oglaševanje je sestavljena tako, da privabi uporabnika. Ob kliku uporabnika na oglaševanje, ga reklama preusmeri na stran, kjer je napadalec pripravil past. Tam se potem namesti Spyware programska oprema, ki beleži podatke uporabnika in jih posreduje napadalcu, ki prevzame nadzor.

3.2 KRAJA PIŠKOTKOV

Brskalniki beležijo podatke uporabnika. Shranjujejo in beležijo vse od zgodovine brskanja, do gesel uporabnika. Napadalec dobi nadzor nad piškotki in se lahko celo identificira, kot uporabnik katerega piškotke je ukradel na spletu. Popularna metoda za izvedbo kraje piškotkov je prenos IP podatkov skozi računalnik napadalca.

3.3 PHISHING

Napadalec ukrade informacije in podatke uporabnika skozi lažno predstavljanje. Največkrat se to izvede preko spletne pošte. Napadalec se predstavlja, kot lažna oseba ali podjetje. Nepazljiv uporabnik vpiše zaupne podatke na lažno spletno stran in jih tako pošlje napadalcu.

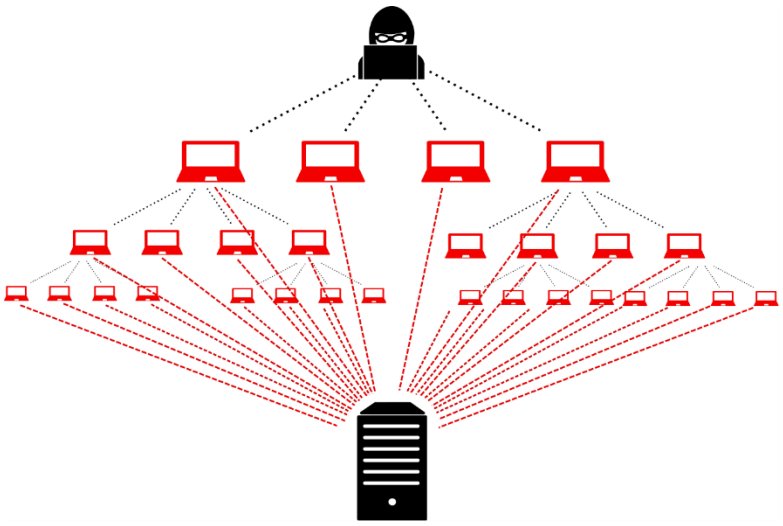
Slika 3: Ponazoritev Phishinga

3.4 LAŽNO BREZŽIČNO OMREŽJE

Napadalec lahko uporabi program za lažno brezžično dostopno točko. Ko se uporabnik poveže na omrežje, napadalec dobi dostop do tvojih podatkov. Je ena izmed najlažjih tehnik. Za izvedbo napadalec potrebuje zgolj program in brezžično omrežje.

3.5 DOS/DDOS

Zavrnitev storitve je proces, kjer napadalec pošlje uporabniku veliko količino podatkov določenega protokola. Pride do upočasnjenega delovanja zunanjih naprav in interneta, napad pa je izveden preko enega računalnika, rezultat pa je odklop (disconnect) ali ponovni zagon računalnika. Podoben napad je porazdeljena zavrnitev storitve (DDOS). Edina razlika je v količini podatkov, ki jo napadalec pošlje uporabniku. Pri porazdeljeni zavrnitvi storitve ima napadalec podračunalnike imenovane DoSboxe ali »zombije«, ki vsi hkrati ob ukazu pošljejo podatke.



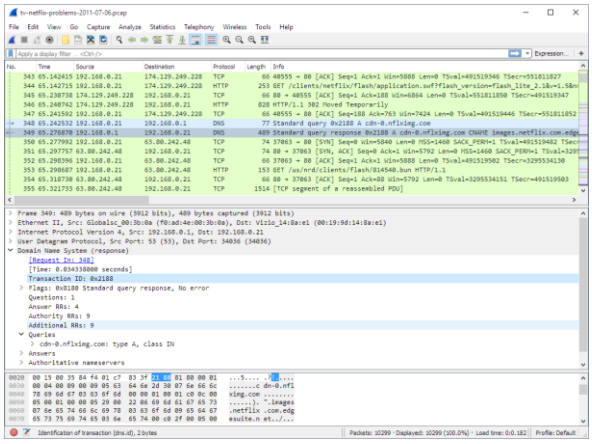
Slika 4: Prikaz DDos napada

4. HEKERSKI PROGRAMI

Na spletu je ogromno programov, ki se uporabljajo za vdiranje in krajo podatkov ter informacij.

4.1 WIRESHARK

Program je izdelal Gerald Combs. Prvotno imenovan Ethereal je izšel leta 1998. Napisan je v C in C++ jeziku. Z njim je mogoče zajemati promet in analizirati podatke, ki potujejo skozi mrežno kartico. S programom lahko uporabnik prestreže in pregleda vsak paket posebej.



Slika 5: Uporabniški vmesnik Wiresharka

4.2 NMAP

Avtor programa je Gordon Lyon. Izšel je leta 1997 in je napisan v C, C++, Python in Lua jezikih. Program, ki s pošiljanjem paketov analizira in odkrije gostitelje v omrežju, ki posledično podajo informacije o operacijskih sistemih in zaščiti, ki jih tarče uporabljajo. Sprva je deloval zgolj v Linux okolju, kasneje pa je prišel tudi na Windows, macOS in BSD.

4.3 OWASP ZED

Popularno hekersko orodje s katerim je mogoče najti napake v spletnih aplikacijah. Je odličen pripomoček za tiste, ki se ukvarjajo z zaščito omrežja. Program vključuje avtomatske skenerje in različna orodja, ki omogočajo uporabniku odkriti napake v omrežju ročno. Je zelo popularen med razvijalci spletnih aplikacij in v rokah osebe, ki dobro razume in zna uporabljati program, še kako nevaren.

5. ZNANI HEKERJI

Vsako leto podjetja izgubijo milijone zaradi kibernetičnih napadov. Beleži se vse več vdorov in napadov na organizacije. Razlog za to naj bi bil v dostopnosti orodij, ki to omogočajo. Ti vdori pa se niso zgodili kar čez noč. Trenutno najbolj znani hekerji so začetniki, ki so postavili temelje za prihodnje generacije.

5.1 Kevin Mitnick

Kevin Mitnic je eden najslavnejših hekerjev. Rodil se je leta 1963 in je že pri 15 letih zaobšel sistem identifikacije za vožnjo z mestnim prometom. Leta 1981 je ukradel računalniške dokumente od podjetja Pacific Bell. Leto kasneje je izvedel uspešen vdor v Severnoameriško poveljstvo obrambe zračnega prostora. Pod žaromet pa je bil postavljen leta 1989. Izvedel je uspešen vdor v podjetje Digital Equipment Corporation's.
Zaradih številnih vdorov je bil leta 1995 aretiran. Odslužiti je moral 5 letno zaporno kazen.

Slika 6: Kevin Mitnick

5.2 Gary McKinnon

Škotski heker rojen leta 1966. Najbolj znan je po številnih vdorih v računalnike ameriške vojske in vesoljske agencije Nasa. Izbrisal je ogromno zaupnih podatkov, uničeval je datoteke, izdeloval kopije pomembnih dokumentov in zaustavil dostavo streliva ameriški vojski. Ujeli so ga leta 2002 pri poskusu prenosa slike, za katero je verjel, da prikazuje vesoljsko plovilo. Ob vdoru je na namizjih puščal sporočilo: »Your security is really crap« (Vaša varnost je res zanič).

5.3 Albert Gonzales

Rojen leta 1989 na Floridi, je heker, ki je ustanovil spletno stran Shadowcrew.com. Ukvarjal se je s krajo številk kreditnih kartic. Na njegovi spletni strani je bilo mogoče kupovati in preprodajati ukradene številke kreditnih kartic, bančnih računov, potne liste in druge ponarejene izkaznice. Znan je bil pod različnimi imeni: Cumba Johnny, Soupnazi in Segvec. Znan je bil po prirejanju velikih zabav in bivanju v dragih hotelih. Začel je že v mladih letih, ko je pri 14 letih vdrl v Naso. Aretiran je bil leta 2008, v zaporu pa bo vsaj do leta 2025.

5.4 Adrian Lamo

Rodil se je leta 1981 v Bostonu. Bil je kolumbijsko-ameriški analitik za grožnje nacionalne varnosti. Znan je kot »Homeless Hacker« (Brezdomni heker). Ime je dobil, ker za svoje početje ni uporabljal lastnega računalnika, ampak se je premikal med javno dostopnimi mesti (knjižnice, kavarne, šole). Ujeli so ga po uspešnem vdoru na časopis New York Times, kjer je nespametno dodal svoje ime v seznam vseh piscev časopisa. Umrl je leta 2018 in neznanih razlogov.

Slika 7: Adrian Lamo

6. ETIČNO HEKANJE

V zadnjih letih smo videli ogromno širitev interneta. Informacije, dokumenti in podatki, ki so se prej hranili v pisnih oblikah, se sedaj digitalizirajo. Vsako leto se beleži vse več kibernetičnih napadov na organizacije. Podjetja, banke in svetovne vladne organizacije najemajo etične hekerje, da najdejo napake in šibke točke omrežij, aplikacij in računalniških sistemov. Velika podjetja kot so Facebook in Google javno vabijo in prirejajo tako imenovane »hekatone«, kjer poskušajo vdreti v njihov sistem, da se napake čim prej odkrijejo in odpravijo. Glavni razlog in namen najema etičnih hekerjev je preprečitev kraje podatkov in odkritje napak in lukenj v sistemu.

Podjetja, ki želijo preveriti svoje aplikacije, omrežja in sisteme najamejo osebo, ki ima v lasti certifikat CEH(Certified Ethical Hacker), ki zagotavlja, da je človek usposobljen in ima dobro poznavanje različnih platform, sistemov in tehnologij. Oseba izvede varnostni pregled, ki je sestavljen iz zbiranja informacij o omrežju, skeniranje omrežja za ugotovitev in odkritje uporabljenih aplikacij v omrežju, napad na omrežje in aplikacije, ohranitev dostopa do sistema ter izdelava poročila.

7. METODE ZAŠČITE

Po poročilu podjetja Norton Cyber Security Insights je v lanskem letu bilo 978 milijonov ogoljufanih uporabnikov. S tam pa so vdiralci zaslužili 140 milijard evrov. Vsi oškodovanci pa imajo skupno pomanjkljivost, da ne vedo veliko o spletnih napadih in kako se zaščititi pred njimi. Med oškodovanci naj bi bilo kar 60 odstotkov milenijcev (ljudje rojeni med 1980 in 2001), za katere bi se pričakovalo, da se spoznajo na tehniko in metode zaščite pred spletnimi napadi. Najina hipoteza o starosti oškodovancev ne drži, saj sva menila, da je večino oškodovancev starejših. Razlog za tekšen rezultat, je strah starejših pred spletom.

Problem se najbolj pokaže pri socialnih omrežjih, kjer objavljamo vse svoje podatke, slike in podobno, pri tem pa se ne zavedamo, da izpostavljamo informacije s katerimi nepridipravi lažje pridejo do svojega cilja.

Kot že prej omenjeno imajo hekerji svoje metode vdiranja, uporabniki pa imajo na razpolago metode zaščite, ki hekerjem delo zelo otežijo ali pa celo preprečijo.
V nadaljevanju pa bo predstavljenih nekaj metod s katerimi se lahko zaščitimo pred nepridipravi.

7.1 Geslo

Pri varnem geslu se moramo vprašati kaj točno je varno geslo. Ponavadi to ni le ena beseda, še posebaj ne ime bližnjega ali ljubljenčka ali pa rojstni datumi in datumi obletnic ter kombinacijo teh, saj so to podatki, ki jih ni težko najti.
Geslo naj bi bilo dolgo več kot 8 znakov, vanj je dobro vključiti znake, številke, male in velike črke. Vsekakor se ne uporablja zaporedja številk (12345678) ali črk (QWERT).

Geslo lahko ustvarimo z navadnim stavkom kot na primer: »danes je lep dan«. Ta stavek nima nobene povezave z osebnimi podatki, ki so našteti prej. S pomočjo malih in velikih črk se varnost gesla poveča: »DanEs Je LeP dAn«. Če želimo geslo še bolje zaščititi pa dodamo številke in znake: »D4nEs#Je L3P dAn!«

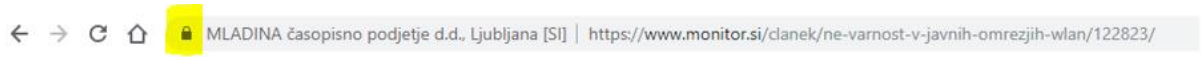
Kot geslo lahko uporabimo tudi stavek oziroma poved: »Danes je lep sončen dan, kakršnega ni bilo že dolgo«, uporabimo samo prve črke »djlsdknbzd«(namesto šumnikov uporabimo sičnike), nato dodamo velike in male črke ter številke in znake: »DjLSDkNb2zD!4«

Pomembno je tudi, da enega gesla ne uporabljamo za vse uporabniške račune (različna gesla za e-pošto, forume, Facebook in ipd.), shranjevanje zapisanega gesla v bližini računalnika pa je neodgovorno in nespametno (npr. listek z geslom,

zaleplejen na monitor ali zapis gesla na namiznem koledarju, po možnosti s pripisom – moj password).

7.2 Uporaba javnih brezžičnih omrežij

Ko se povezujemo na javna brezžična omrežja, najprej pomislimo na to, kako hitro in dobro deluje in ne na varnost. Znano je, da so javna omrežja velikokrat tarča hekerjev, ker se ljudje ne zaščitimo pred njimi z uporabo VPN (Virtual Private Network). Kot so zapisali na spletni strani Računalniške novice: »Ko brskate po spletu in ste priključeni na nezaščiteno brezžično omrežje, je prav tako priporočljivo, da uporabljate storitev VPN, oziroma navidezno zasebno omrežje. Ne le, da prikrije vašo identiteto, ampak vam zagotavlja tudi varnejšo povezavo«.
Strani, ki so varne, so opremljene s povezavo HTTPS. To lahko previrimo tako, da v naslovni vrstici spletnega brskalnika pogledamo za zeleno ključavnico, kot je prikazano na spodnji sliki.



Slika 8: Prikaz VPN zaščite v naslovni vrstici

7.3 Sumljiva elektronska pošta

Pri elektronski pošti je potrebno biti previden, čeprav temu ni videti tako, le en napačen klik povzroči, da so nezaželjeni virusi naloženi. Pri tem pa okužimo računalnik, ki naprej pošilja tako imenovani »SPAM« oz. vsiljeno pošto in oškoduje še druge. Poleg vsiljene pošte nam lahko povzroči tudi ostale nevšečnosti kot so: kraja osebnih podatkov, zloraba že vpisanih gesel na vašem računalniku, ki pa vodijo do FTP (File Transfer Protocol) gesel, bančnih gesel, itd.

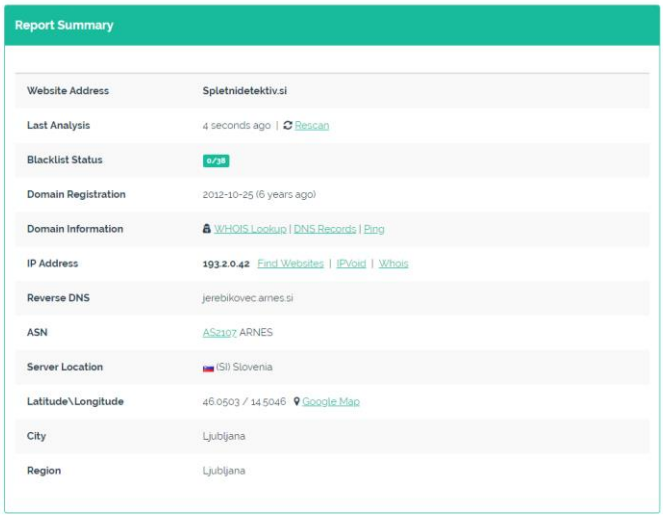
Slika 9: Okužena e-pošta

Elektronska pošta je okužena z zlonamernimi kodami, ki pa se jim lahko izognemo na zelo preprost način, kot so zapisali na računalniških novicah: »Med najpomembnejšimi varnostnimi priporočili gre upoštevati, da ne odpirate sumljive elektronske pošte in priponk neznanih pošiljateljev. Poleg tega poskrbite za to, da imate vedno izdelane varnostne kopije svojih podatkov, posodabljate svoj operacijski sistem (predvsem Windows), spletne brskalnike, Office, Adobe Reader ter vso ostalo programsko opremo. Prepričati se morate tudi, da uporabljate zadnjo različico dovolj kakovostnega in zanesljivega protivirusnega programa ter drugih varnostnih rešitev« Povzetek zapisanega:

- ne odpirajte pošte neznanega pošiljatelja
- ne odpirajte sumljivih priponk in
- posodabljajte svoj računalnik in programe kot so anti virusni program, spletni brskalniki…

7.4 Varno kupovanje

Kupovanje preko spleta je vedno riskantno, če spletno mesto s katerega kupujemo ni preverjeno in potrjeno kot varno. Dandanes se to lahko previri s številnimi spletnimi programi za previrjanje ali so strani varne ali ne.



Slika 10: Prikaz programa za previrjanje varnosti spletne strani

Pri spletnem nakupovanju za preverjanje varnosti pridejo v poštev že prej omejeni HTTPS in ključavnica, ki je v naslovni vrstici spletnega mesta. Priporočljivo se je izogibati spletnim trgovinam, ki ne uporabljajo varnostnih mehanizmov kot so: Verified by Visa, MasterCard Secure Code.

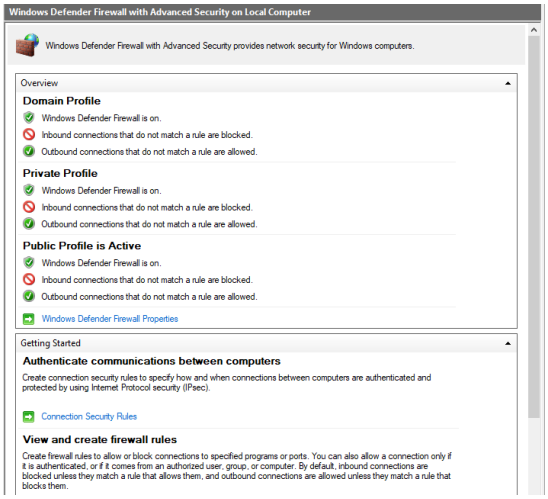
Za preizkus svojega znanja o spletnih goljufijah je prljubljena spletna igra »Spletni Detektiv«, kjer je potrebno prepoznati spletno goljufijo. Igra ponuja primere iz spleta, pri katerih se je potrebno odločiti za pravilen odgovor.

Slika 11: Spletna stran "Si spletni detektiv?"

8.Šolsko omrežje (teoretični postopek vdora)

8.1 Opis šolskega omrežja

Šolsko omrežje je razdeljeno na več pod omrežij za različne namene: strežniki za dijake, profesorje, računovodstvo...
Za omrežje velja logika pravil, da je vse zaprto, razen kar se uporablja. Točnih podatkov zaradi varnosti omrežja žal, nisva pridobila. Sva pa zato priložila spodnjo sliko, ki prikazuje logiko požarnega zidu na računalniku, ki sva ga uporabljala pri delu. Zelena kljukica prikazuje opcijo, ki se uporablja. Rdeč prekrižan krog pa vse, kar se ne uporablja.



Slika 12: Logika pravil v požarnem zidu

8.1.1 Checkpoint firewall

Naše šolsko omrežje uporablja takoimenovani Checkpoint-ov požarni zid, ki zavaruje omrežje pred grožnjami. Checkpoint velja za "Next Generation Firewall" oz. trenutno najboljšo zaščito.

Slika 13: Logotip požarnega zidu "CHECKPOINT"

Lastnosti:

1. Zavedanje identitete

   Skrbnik ima nadzor nad podrobno preglednostjo uporabnikov, skupin, aplikacij, strojev in vrst povezav v omrežju, omogoča dodelitev dovoljenj pravim uporabnikom in napravam.
   Požarni zid zagotavlja popolno indentifikacijo uporabnika, kar omogoča preprosto definicijo politike, administrator pa dobi popolen pregled nad aplikacijami, uporabniki, napravami ali skupinami neposredno iz požarnega zidu. Identifikacija uporabnika se lahko pridobi prek:

   - Integracije z dobavitelji IAM ali spletnim API-jem
   - Skozi ujetniški portal
   - Namestitev enkratnega agenta, ki je na strani odjemalca

2. Nadzor aplikacij
   Omogoča zaščiteno uporabo več kot 8000 aplikacij in 260 000 pripomočkov za socialne mreže. Ustvarimo lahko podrobne varnostne pravilnike, ki omogočajo omejevanje spletnih aplikacij in pripomočkov, kot so takojšnje sporočanje, družabno mreženje, pretakanje videov, igre in drugo.

3. Preprečevanje vdorov
   IPS (Intrusion prevetion System) ali drugače IDPS (Intrusion detection prevention system)
   Vključena je tudi kontrolna točka IPS, ki pregelduje prehod paketov v omrežju. Funkcija IPS zagotavlja geo-zaščito in samodejna posodabljanja funkcij proti grožnjam.

8.2 Kako bi dijak lahko vdrl v šolsko omrežje

Šolsko omrežje je zelo zavarovano na področju brezžičnih omrežij, kot tudi na področju samega strežnika. V samo omrežje bi bilo težko vdreti z metodo vstopa skozi zadnja vrata, zato sva se raje odločila za pristop znotraj šole, kar nama omogoča najino šolanje oz. da sva dijaka šole.
Z opazovanjem in analizo okolja sva ugotovila, da večina profesorjev pušča računalnike v učilnici, kljub temu, da so v razredu dijaki. Zato je najna prva možnost napad znotraj omrežja in sicer z pomočjo »USB RUBBER DUCKIE«, ki je dobro orodje za krajo podatkov, uporabniških imen in gesel.

Slika 14: Namizni računalnik v učilnici

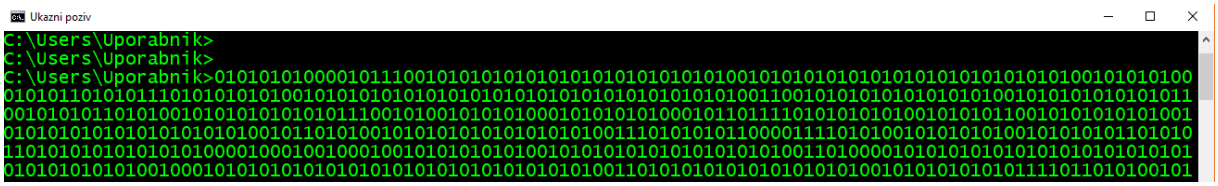
Postopek bi šel nekako takole:

1.

Izbrati je potrebno primerno metodo. V našem primeru bi v upoštev prišel »USB RUBBER DUCKY«, ki je na voljo na uradni strani »HAK5« in stane nekje 40 evrov.
Z njim bi lahko iz računalnika nanj naložili vse podatke ali ukradli gesla in uporabniška imena.
Naslednji korak bi bil napisati kodo in ključek testirati doma, ker nas bo zanimalo koliko časa potrebuje ključek in ali izbriše in pozapre vsa okenca, ki jih med delovanjem odpre. Čas je odvisen od kode in kako hitro sama naprava izvrši ukaze. Po analizi naj bi bila naprava 1000 hitrejša kot človeške roke, če upoštevamo še napake, ki jih lahko človek stori, je USB ključek veliko bolj unčinkovit.
Koda za »USB RUBBER DUCKY« je dostopna na več spletnih mestih. S pomočjo Youtuba, pa je možno priti do celotnih postopkov.

Slika 15: Notranjost in izgled USB rubber ducky-a

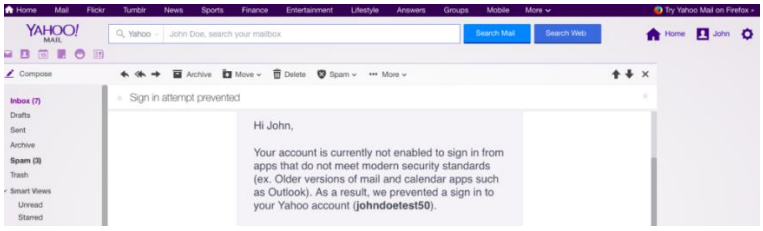
»USB rubber duckie« je kot tipkovnica, sprogramiramo ga, da ob namestitvi v USB port, odpre ukazni poziv (slika spodaj), kjer se predstavi kot tipkovnica in izvrši ukaze, ki smo jih prej napisali tako, da odražajo pritiske tipk na tipkovnici. Nato kopira podatke, gesla in uporabniška imena.
Za uspešen vdor bi potrebovala, le analizo okolja, ki bi trajala nekje 5 delovnih dni. Sam napad pa bi izvršila ob prvi priložnosti, ko bi profesor zapustil razred in ob tem pustil namizni računalnik izpostavljen. Le kratkih 5 minut in vsi podatki bi bili na USB ključku.



Slika 16: Okence ukaznega poziva

2.

Druga možnost, s katero bi lahko pridobila podatke, je s tako imenovanim črvom oz. »worm«, mnogi črvi uporabljajo Microsoft Outlook ali Outlook Express za širjenje. Te vrste e-poštnih "črvov" imajo priloženo datoteko, ki jo je potrebno klikniti in odpreti za namestitev. Te vrste črvov imajo običajno datoteko z dvojno razširitvijo, kot je (IME.BMP.EXE ali IME.TXT.VBS). Te razširitve so programske datoteke Windowsa, ki namestijo program v računalnik. Ti programi so lahko programi za daljinsko upravljanje, za vohunsko programsko opremo, tako imenovan »key loggers« ali katero koli drugo programsko opremo, ki jo zlonamerno uporabljajo temni hekerji. Dodatne razširitve so VBS, SHS, BAT, EXE, CMD in PIF. Takšna vrsta napada je navadno v obliki neke posodobitve sistema, antivirusnega programa oz. datoteke, ki ni preveč sumljiva in ne vzbudi pozornosti.



Slika 17: Prikaz e-poštnega sporočila

Ta napad se bi lahko izvršil na več načinov, ker pa sva se odločila, da bodo napadi znotraj šole, sva možnosti omejila. Šolanje nam omogoča, da lahko s profesorji komuniciramo preko šolske e-pošte. Na primer, da se s profesorjem dogovorimo za oddajo naloge preko njegove e-pošte. Poleg datoteke z nalogo, pa bi poslala še »spletnega črva«, za katerega profesor ne bi vedel. Ob kliku in namestitivi naloge, bi se namestil tudi program za dostop do profesorjevega računalnika. Če profesor namestitve vohunskega programa ne bi opazil, bi lahko preko svojega računalnika dostopala do njegovega namizja in posledično do podatkov, gesel in uporabniških imen.

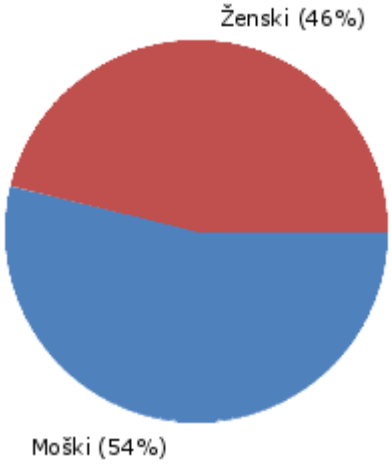
Slika 18: Virtualni prikaz hekarske roke, ki brska po tujem računalniku

10. ANKETA RAZISKAVA VARNOSTI V ŠOLSKEM OMREŽJU

Anketa Raziskava varnosti v šolskem omrežju je anonimna. Odgovore in ugotovitve sva izključno uporabila za raziskovalno nalogo. Anketa je sestavljena iz 8 vprašanj. Število sodelujočih profesorjev je bilo 21. Spodaj so po vrsti grafično prikazani rezultati odgovorov profesorjev.

10.1 UGOTOVITVE

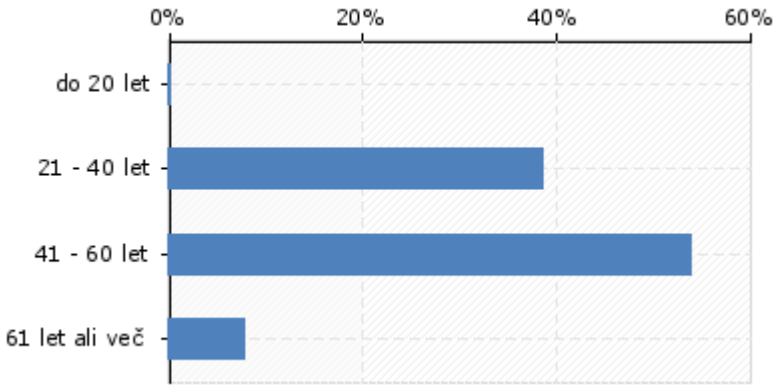
1. Spol



Slika 19: Graf profesorji spol

Ankentiranih je bilo 21 profesorjev. Od teh je bilo 54% moškega spola in 46% ženskega.

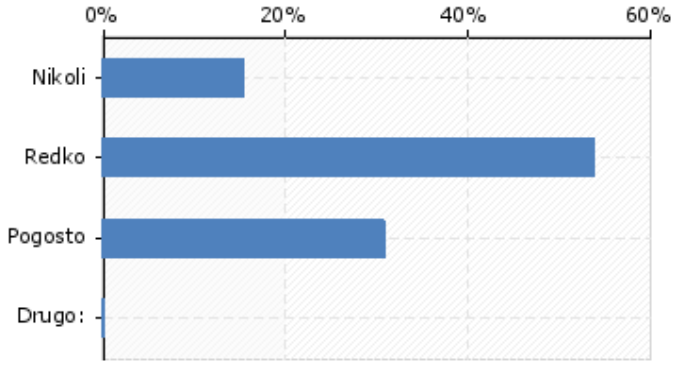
2. V katero starostno skupino spadate?



Slika 20: Graf starost profesorji

Večina profesorjev spada v starostno skupino med 41 – 60 let. Prvi starostni skupini sledi med 21 – 40 let. Malo število anketiranih profesorjev je v 61 let ali več starostni skupini. Noben izmed anketiranih profesorjev ni spadal v starostno skupino pod 20 let.

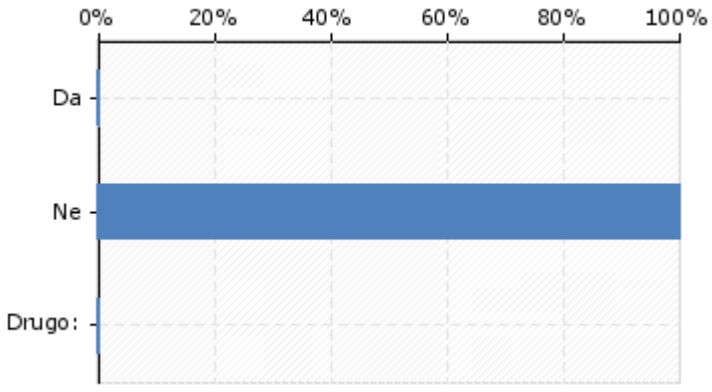
3. Kako pogosto menjate geslo?



Slika 21: Graf menjava gesla profesorji

Več kot polovica profesorjev je na vprašanje »Kako pogosto menjate geslo?« odgovorilo z redko, malo več kot 35% profesorjev je odgovorilo s pogosto in manj kot 20% je na vprašanje odgovorilo z nikoli.

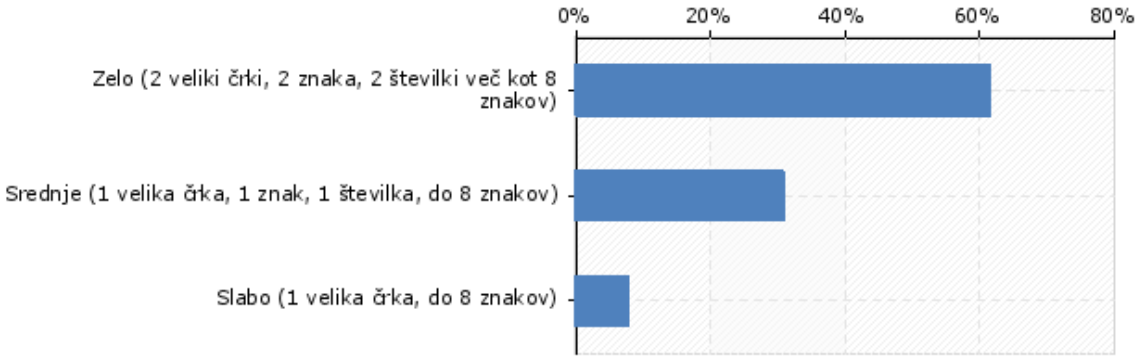
4. Ali imate enaka gesla in uporabniška imena za osebno uporabo in šolsko?



Slika 22: Graf uporabniško ime profesorji

S četrtim vprašanjem sva želela izvedeti ali profesorji uporabljajo enaka gesla za osebno in šolsko uporabo. Rezultati so bili pričakovani. Vsi profesorji so na to vprašanje odgovori z ne. Kar potrdi del najine hipoteze, da profesorji ne uporabljajo enakega e-poštnega naslova za šolsko in osebno uporabo.

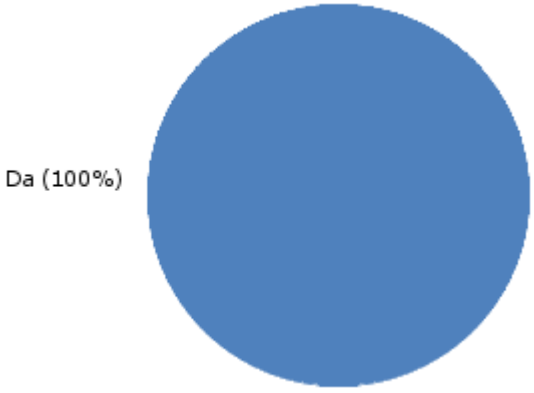
5. Kako varno menite, da je vaše geslo?



Slika 23: Graf varno geslo profesorji

Peto vprašanje je bilo o varnosti gesla. Na voljo so anketiranci imeli tri odgovore. Prvi odgovor je bil »Zelo (2 veliki črki, 2 znaka, 2 številki več kot osem znakov)« na katerega je odgovoril največji odstotek profesorjev. Drugi odgovor »Srednje (1 velika črka, 1 znak, 1 številka, do 8 znakov)« je odgovorilo 30% profesorjev. Zadnji odgovor »Slabo (1 velika črka, do 8 znakov)« pa je označilo najmanjše število profesorjev.

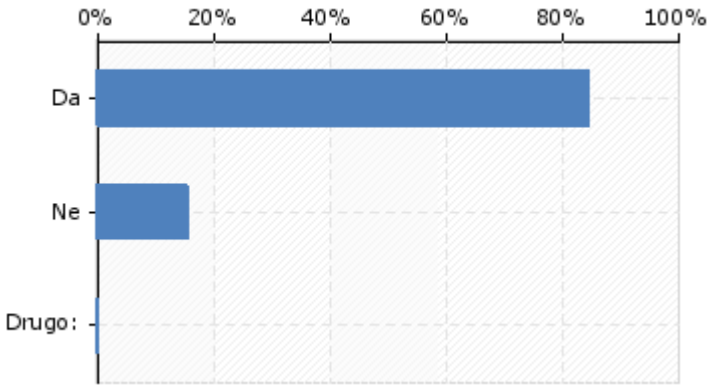
6. Ali imate nameščene protivirusne programe?



Slika 24: Graf protivirusni programi profesorji

Na vprašanje »Ali imate nameščene protivirsne programe?« so vsi profesorji odgovorili z da.

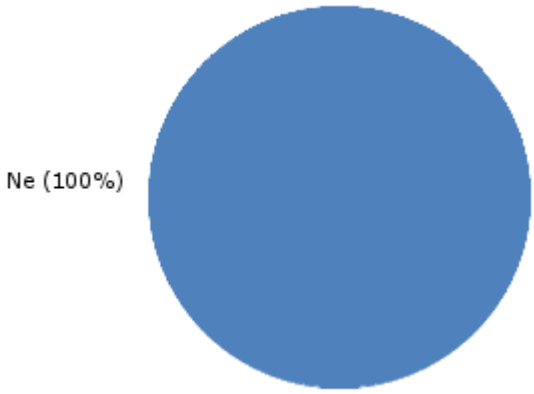
7. Ali imate socialna omrežja kot so: Facebook, Snapchat, Instagram?



Slika 25: Graf socialna omrežja profesorji

Sedmo vprašanje je bilo o socialnih omrežjih. Zanimalo naju je koliko profesorjev uporablja socialna omrežja kot so: Facebook, Snapchat, Instagram? Več kot 80% odstotkov profesorjev je na to vprašanje odgovorilo z da. Ostali so odgovorili z ne.

8. Ali ste že kdaj bili žrtev spletnega vdora?



Slika 26: Graf žrtev vdora profesorji

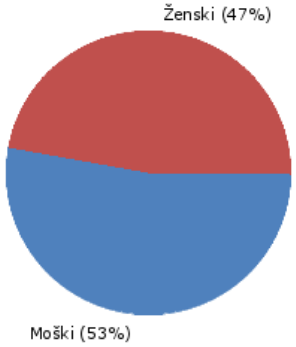
Z zadnjim vprašanjem sva želela izvedeti ali je kateri izmed profesorjev že bil žrtev spletnega vdora. Na to vprašanje so vsi anketirani profesorji odgovorili z ne.

11. ANKETA PREVIDNOST NA SPLETU

Anketa Previdnost na spletu je anonimna. Odgovore in ugotovitve sva uporabila izključno za raziskovalno nalogo. Anketa je sestavljena iz 12 vprašanj. Število sodelujočih anketirancev je bilo 145. Spodaj so po vrsti grafično prikazani rezultati odgovorov anketiranih oseb.

11.1 UGOTOVITVE

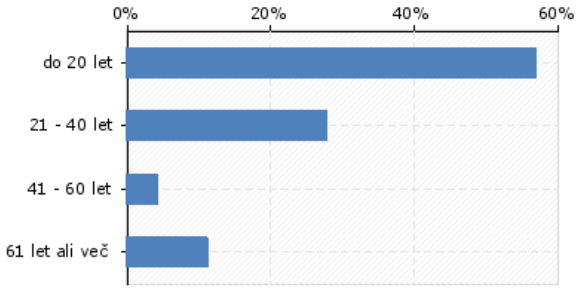
1. Spol



Slika 27: Graf spol anketiranci

Od 145 anketiranih oseb je 53% odstotkov bilo moškega spola in 47% ženskega.

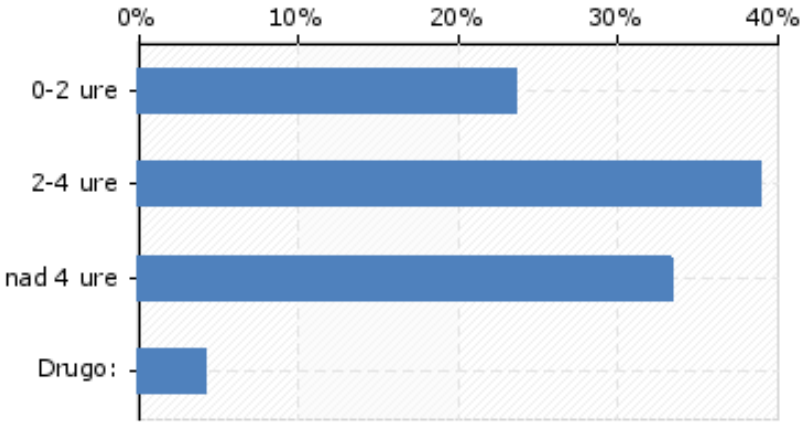
2. V katero starostno skupino spadate?



Slika 28: Graf starost anketiranci

Večina anketirancev spada v starostno skupino do 20 let. Med 21- 40 let spada malo manj kot 30% anketirancev. V starostno skupino med 41 – 60 let spada manj kot 10% anketiranih oseb. Več kot 10% anketiranih oseb pa se je opredelilo v starostno skupino 61 let ali več.

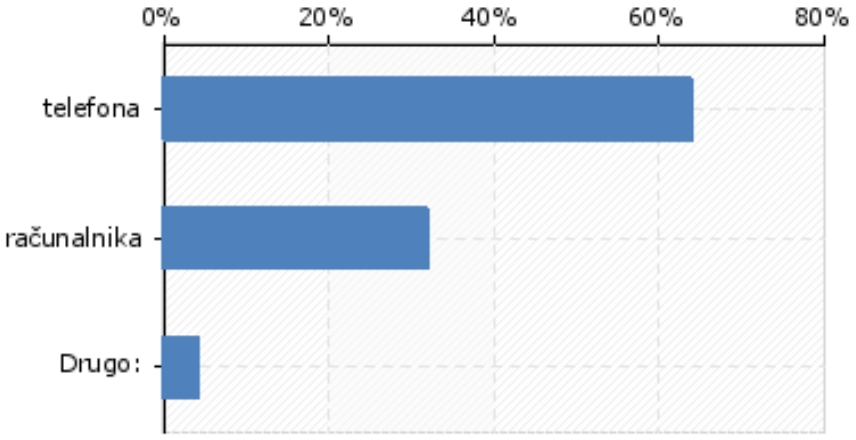
3. Koliko časa preživite na spletu?



Slika 29: Graf čas na spletu anketiranci

V tretjem vprašanju sva želela izvedeti koliko časa anketiranci preživijo na spletu. Največ anketiranih oseb je na to vprašanje odgovorilo z 2 – 4 ure na dan. Prvemu odgovoru tesno sledi odgovor nad 4 ure. 0 – 2 ure je označilo skoraj 23% anketirancev. Manj kot 5% je označilo drugo, kot odgovor.

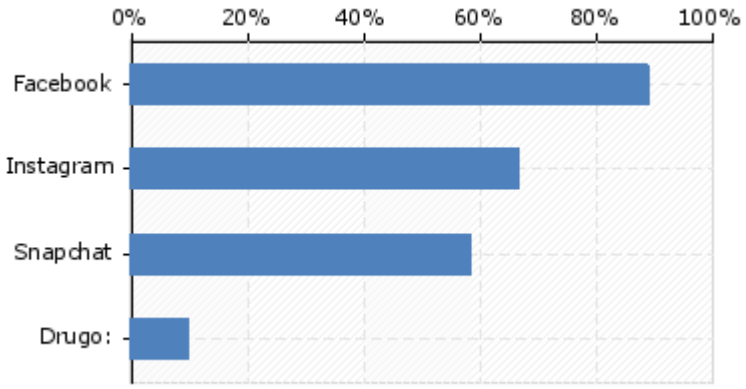
4. Ali raje brskate po spletu preko telefona ali računalnika?



Slika 30: Graf brskanje po spletu anketiranci

V četrtem vprašanju sva ugotovila, da večje število anketirancev uporablja pametni telefon, namesto računalnika, za brskanje po spletu.

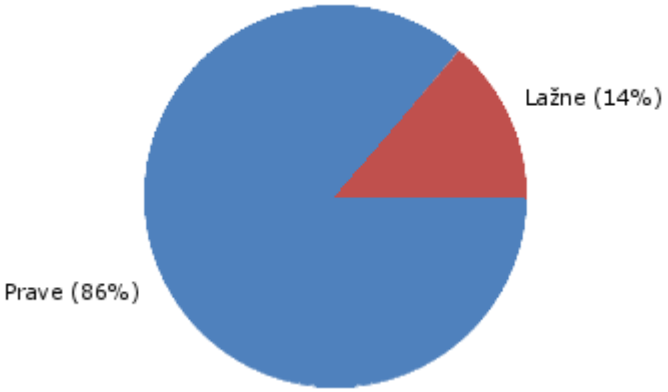
5. Katera socialna omrežja uporabljate?



Slika 31: Graf socialna omrežja anketiranci

V petem vprašanju sva želela izvedeti katera socialna omrežja anketirane osebe uporabljajo. Na voljo so imeli štiri odgovore. Prvi trije odgovori so najbolj uporabljena socialna omrežja Facebook, Instagram, Snapchat in kot zadnji odgovor so lahko izbrali »Drugo«. Odgovori so bili pričakovani. Po vrsti si sledijo Facebook, Instagram in Snapchat. 10% oseb pa je označilo, da uporabljajo tudi druga socialna omrežja, ki niso bila omenjena.

6. Ali pri registraciji uporabite prave ali lažne podatke?



Slika 32: Graf pravi/lažni podatki anketiranci

Na šetsto vprašanje je 86% anketirancev odgovorilo, da uporabljajo prave podatke pri registraciji. 14% pa jih je odgovorilo, da uporabljajo lažne.

7. Zakaj prave?

Sedmo in osmo vprašanje se navezuje na šesto vprašanje »Ali pri registraciji uporabite prave ali lažne podatke?« Spodaj na sliki so prikazani nekateri odgovori na vprašanje »Zakaj prave?«

nevem da me ljudje spoznajo
to kar sem sem in celo daljne sorodnike sem našla preko fb
nimam razloga da nebi
nic ne skrivam
ker ne dajem nič zasebnega gor
kr mi je to vseč
ker je pošteno do ostalih uporabnikov, da vedo s kom imajo opravka.
podam samo najosnovnejše podatke, da me lahko drugi uporabniki prepoznajo
ker ni prav lagati
kr tak
ker se tako predstavim drugim ljudem
ker pri večini registr. ne rabiš vnest lažne
nisem nikoli pomislila, da bi dala lažne.
ker sem to ja
zato ker sem fizicna oseba
lažje iskanje
zaka nebi? :d
nezakonito je podajati napačne podatke
pač,.. zaradi lažje prepoznavnosti na socijalnih omrežjih in ker si z mojo identiteto nemore nuben nč pomagat (razn kapsi)

Slika 33: Graf pravi podatki anketiranci

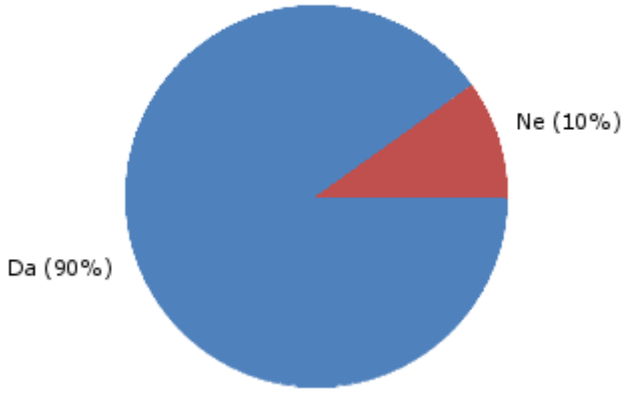
8. Zakaj lažne?

V spodnji sliki so prikazani vsi odgovori na vprašanje »Zakaj lažne?«

večinoma časa lažne da se zaščitim pred krajo podatkov, prave samo kadar je potrebno npr spletni nakupovanje
bolj varno
varno bol
nezaupanje
tak kr je fajn
ne želim idati svoje identitete
zaradi varnosti

Slika 34: Graf lažni podatki anketiranci

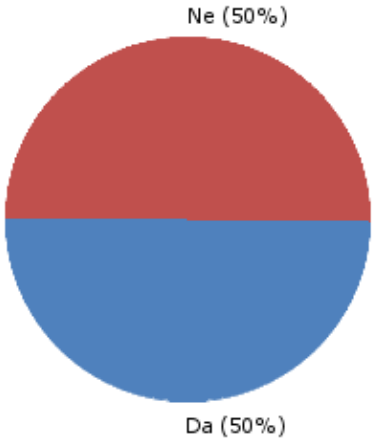
9. Ali se na tujih računalnikih odjavljate iz socialnih omrežij(Facebook, e-pošte...)?



Slika 35: Graf odjavljanje iz omrežij anketiranci

Na deveto vprašanje »Ali se na tujih računalnikih odjavljate iz socialnih omrežij(Facebook, e-pošte...)?« je 90% anketirancev odgovorilo z »Da«. Ostali so odgovorilo z »Ne«.

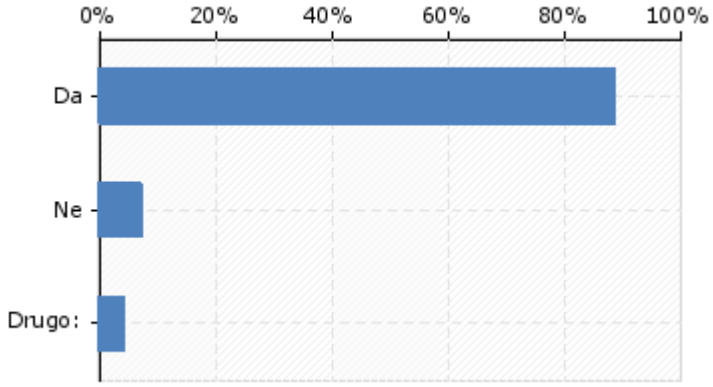
10. Ali uporabljate enak e-poštni naslov za vse dejavnosti?



Slika 36: Graf e-poštni naslov anketiranci

Odgovori na deseto vprašanje »Ali uporabljate enak e-poštni naslov za vse dejavnosti?« so bili izenačeni.

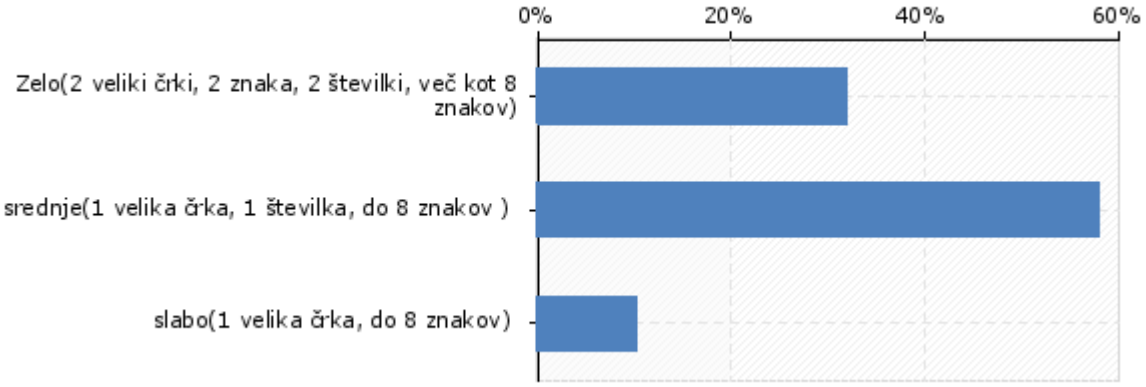
11. Ko odpirate e-pošto ali pazite na to kaj so vam poslali in od koga je e-pošta?



Slika 37: Graf prejeta e-pošta anketiranci

Na enajsto vprašanje je skoraj 90% anketiranih oseb odgovorila z da. Manj kot 10% jih je odgovorilo z ne. Ostali anketiranci so izbrali odgovor drugo.

12. Kako varno menite, da je vaše geslo?



Slika 38: Graf varno geslo anketiranci

Zadnje vprašanje je enako kot pri prvi anketi »RAZISKAVA VARNOSTI V ŠOLSKEM OMREŽJU«. Večina anketirancev je odgovorila z srednje. Več kot 30% jih je odgovorilo z zelo in najmanj anketiranih oseb je za odgovor označilo slabo. Z pridobljenimi podatki sva ugotovila, da najina hišpoteza me drži. Večina anketirancev ima srednje ali zelo zavarovana gesla.

Zaključek

Ob raziskovanju, ki sva ga opravila, da sva pripravila nalogo, sva ugotovila, da verjetno sistema, ki bi uporabnike zaščitil 100% pred neželjenimi vdori hekerjev, ni. S temi podatki, pa lahko potrdima hipotezo, da se lahko vsaj delno zaščitimo pred vdori. Tako kot se programerji in beli hekerji trudijo iskati pomankljivosti sistemov, so črni hekerji vedno korak ali dva pred njimi. Iz ankete, ki sva jo pripravila, sva ugotovila, da se sicer velika večina uporabnikov zaveda, da je varna uporaba interneta in družbenih omrežij najbolj odvisna od njih samih, vendar se bojiva, da je bilo število anketirancev vse premajhno, da bi lahko zanesljivo trdila, da se uporabniki res zavedajo, kako je potrebno ščititi svoje podatke in kako nevarno in nespametno je uporabljati neko preprosto geslo, ki je za povrh še enovito za vse mogoče prijave v družabna omrežja, poštni predal, spletne trgovine, spletno stran banke itd.

Prav tako sva ugotovila, da bi bilo možno z malo spretnosti in hekerske žilice vdreti tudi v šolsko omrežje in pridobiti željene podatke.

Ugotovila pa sva, da se da na spletu najti in pridobiti tudi vse hekerske programe, z vsemi popolnimi navodili, kako jih namestiti in uporabiti, kar se nama ne zdi prav, saj se zaradi tega povečuje število amaterskih hekerjev, ki jim v prvem trenutku sicer ni namen obogateti, jim pa daje neko zadovoljstvo, ko se jim posreči vdreti na neko spletno stran in povzročiti, če ne drugega, nekaj panike. Ob takih »uspehih« dobijo krila, da se pričnejo izobraževati naprej in hekati, do podatkov, ki bi jim prinesli neko korist in s tem potrjujeva hipotezo, da se iz leta v leto povečuje število vdorov.

Z novimi tehnologijami, postaja računalništvo uporabnikom vse bolj prijazna kategorija, žal pa s tem postajajo podatki vse manj zaščiteni in lahko dostopni nepovabljenim gostom, saj so se s tehnologijo razvili tudi hekerji, izobraževanja uporabnikov pa skoraj ni, saj vemo, da imajo pametne telefone, ki omogočajo brskanje po spletu in družbenih omrežjih praktično že vsi otroci v osnovni šoli.

Kako čim bolj preprečiti nezaželjene vdore? Z uporabo kvalitetnih požarnih zidov, kvalitetnih antivirusnih programov, z uporabo zelo varnih gesel, ki jih uporabnik menja dovolj pogosto, odveč pa tudi ni opozarjanje uporabnikov na varno uporabo, na čim manjšo uporabo javnih brezžičnih omrežij in izobraževanjem uporabnikov.

VIRI

Adrian Lamo. (2. 22 2019). Pridobljeno iz Wikipedia: https://sl.wikipedia.org/wiki/Adrian_Lamo

Albert Gonzales. (22. 2 2019). Pridobljeno iz Wikipedija: https://sl.wikipedia.org/wiki/Albert_Gonzalez

CheckPoint firewall. (11. 2 2019). Pridobljeno iz CheckPoint firewall: https://www.checkpoint.com/products/next-generation-firewall/

e-računalništvo. (16. 2 2019). *PROTOKOL ZA PRENOS DATOTEK FTP*. Pridobljeno iz e-računalništvo: http://www.s-sers.mb.edus.si/gradiva/rac/drugo/omrezja/60_storitve/06_datoteka.html

Gary McKinnon. (22. 2 2019). Pridobljeno iz Wikipedija: https://sl.wikipedia.org/wiki/Gary_McKinnon

Hacker. (22. 2 2019). Pridobljeno iz Wikipedija: https://en.wikipedia.org/wiki/Hacker

Heker. (22. 2 2019). Pridobljeno iz Wikipedija: https://sl.wikipedia.org/wiki/Heker

Hekerji. (22. 2 2019). Pridobljeno iz Wikipedija: https://sl.wikipedia.org/wiki/Hekerji

Honzak, U. (12. 10 2018). *Revija Mladi podjetnik*. Pridobljeno iz Pomembne statistike v povezav s Facebookom: https://mladipodjetnik.si/novice-in-dogodki/novice/pomembne-statistike-v-povezavi-s-facebookom-1-del

Insights, N. C. (22. 1 2019). *Računalniške novice*. Pridobljeno iz Kako se zaščititi pred hekerskimi napadi?: https://www.racunalniske-novice.com/triki/hekerji-so-lani-z-napadi-zasluzili-140-milijard-evrov-kako-se-zascititi-pred-napadi--1.html

Kaj delajo računalništki hekerji? (24. 11 2015). Pridobljeno iz Varni na internetu: https://www.varninainternetu.si/kaj-delajo-racunalniski-hekerji/

Kevin Mitnick. (22. 2 2019). Pridobljeno iz Wikipedija: https://sl.wikipedia.org/wiki/Kevin_Mitnick

Lukan, D. (20. 11 2011). *Etično hekanje*. Pridobljeno iz Viris: https://www.viris.si/2011/11/eticno-hekanje/

Monitor. (15. 12 2018). Pridobljeno iz Nevarnost v javnih omrežjih: https://www.monitor.si/clanek/ne-varnost-v-javnih-omrezjih-wlan/122823/'

NMAP. (22. 2 2019). Pridobljeno iz Wikipedia: https://en.wikipedia.org/wiki/Nmap

OWASP ZED. (22. 2 2019). Pridobljeno iz Wikipedia: https://en.wikipedia.org/wiki/OWASP_ZAP

Shekhar, A. (30. 11 2017). *Top 10 Common Hacking Techniques You Should Know About*. Pridobljeno iz Fossbytes: https://fossbytes.com/hacking-techniques/

TechTarget. (18. 2 2019). Pridobljeno iz Most popular viruses and hacking tools: https://searchnetworking.techtarget.com/feature/Most-popular-viruses-and-hacking-tools

Wireshark. (22. 2 2019). Pridobljeno iz Wikipedija: https://en.wikipedia.org/wiki/Wireshark