ŠOLSKI CENTER CELJE
SREDNJA ŠOLA ZA KEMIJO, ELEKTROTEHNIKO IN RAČUNALNIŠTVO

RAZISKOVALNA NALOGA

VDOR V OMREŽJE

(Računalništvo)

Mentor:
Timej Pirš

Avtorja: Tilen Trkulja, R-4.a
Blaž Hrastnik, R-4.a

Celje, 2021

Kazalo slik

Zahvala

Zahvaljujeva se mentorju profesorju Timeju Piršu, ki naju je skozi celotno raziskovalno nalogo vodil in usmirjal proti cilju, nama dajal nasvete in nove ideje za potek raziskovalne naloge. Zahvaljujeva se tudi vsem akneterancem, kateri so rešili v celoti najino anketo, in s tem omogočili nadaljno raziskavo teme.

Povzetek

Vdor v omrežje ali hekanje po navadi povezujemo z vohunskimi filmi ali pa trilerji a dan danes so kruta resničnost. Ta seminarska naloga potrdi resnost tega dejstva.
V seminarski nalogi je predstavljena zgodovina hekanja od prvega primera vdora. Nato so opisane vrste hekerjev. Poglobila sva se tudi v kakšne tehnike hekerji uporabljajo najpogosteje in se najbolj poglobila v DOS/DDOS. Po tem sva predstavila znane primere hekanje po svetu in znane hekerje, ki to izvedejo.
Ob koncu sva z anketo ugotovila, da večina ljudi pri brskanju na spletu ne skrbi za varnost pred vdorom v račun ali podobno. Statistika ankete je prikazala, da velika večina ljudi ne redno spreminja svojega gesla.

Abstract

Network hacking or hacking is usually associated with spy movies or thrillers, but today they are a harsh reality. This seminar paper confirms the seriousness of this fact.
This seminar paper presents the history of hacking from the first case of hacking. We move on to describe the types of hackers. We also delved into what techniques hackers use most often and delved most deeply into DOS/DDOS. After that, we presented well-known examples of hacking around the world and well-known hackers who do it.
In the end, we found with a survey that most people when browsing online don’t care about their internet security against account hacking or the like. Survey statistics showed that the vast majority of people do not change their passwords regularly.

1 UVOD

Živimo v svetu, kjer je vse več poudarka na tehnologiji, internetu, delu od doma. Internet in tehnologija nam ponuja ogromno prednosti ampak tudi ogromno slabosti, katerih se velika večina ljudi najverjetneje ne zaveda. Vsak podatek katerega vpisujemo na splet je lahko nova priložnost in koristen podatek za določene skupine ljudi. To so zelo dobre organizacije, katere uporabljajo naše podatke sebi v korist. Morda na prvi pogled mislimo, da v primeru, da nas nekdo ves čas posluša in se mi ne pogovarjamo nič zasebnega se v resnici v ozadju odvijajo zelo zanimive reči. Hekerji se lahko brez naše vednosti povežejo na naše omrežje in nas opazujejo preko naše kamere in poslušajo preko našega mikrofona. Zato je alternativna rešitev, da v primeru, da kamere trenutno ne uporabljamo jo izklopimo fizično iz računalnika, jo obrnemo stran od sebe(npr. v zid), v primeru, da pa imamo kamero vgrajeno v računalniški zaslon kot v prenosnih računalnikih, pa lahko prekrijemo z kosom papirja in lepilnim trakom. Podobno alternativo lahko uporabimo za mikrofon, le da tega ne moramo prekriti z papirjom ali obrniti stran od nas, saj vseeno zazna zvok in nas lahko slišijo. Zato je zelo velika prednost pri slušalkah, katere lahko fizično iztaknemo mikrofon in tako garantirano preprečimo prisluškovanje, saj je to naš edini vhod za prehajanje zvoka iz okolja v računalnik.

Sva dijaka srednje tehniške šole v Celju, in odločila sva se, da se podava v raziskovalno nalogo na temo Vdor v omrežje in sicer podrobneje razložiti postopek DDOS, opisati vrste hekerjev in pa varnost uporabe gesel.

Meniva, da ljudje ne pazijo dovolj, na izklapljanje kamer in mikrofonov fizično iz računalnikov, saj so zelo lahkoverni in mislijo, da njih nihče ilegalno ne mora spremljati. Hekerji lahko samo iz našega pogovora dobijo ogromno koristnih podatkov, katere lahko uporabijo proti nam in nas izsiljujejo za denar ali kaj podobnega. V primeru, da želimo prijatelju posoditi bančno kartico, da si lahko nekaj kupi preko spleta je zelo nevarno podatke govoriti na glas, saj lahko hekerji preko mikrofona poslušajo pogovor in z zem pridobi vse podatke o kartici.

Kot dijaka računalniške šole naju zelo zanima, kako poteka pridobivanje podatkov iz omrežja, razne metode za vdor v omrežje in kako se lahko zažčitimo pred raznimi vdori v omrežje.

HIPOTEZE:

- Meniva, da Windowsow požarni zid ne zadostuje kot obramba pred napadi na strežnik.
- Predvidevama, da zastonj protivirusni program ne zadostujejo kot obramba pred napadi na strežnik.
- Predvidevama, da uporabljajo dijaki eno geslo za več računov.
- Predvidevama, da profesorji in dijaki ne spreminjajo geslov redno.
- Predvidevama, da večina dijakov in profesorjev ne uporabla dovolj varhih/zapleteni geselj(kot naprimer: B4kanfMSOjm4nNf)
- Predvidevama, da pri ddos napadu lahko skrbnik strežnika omeji število poslanih prošenjs in z tem prepreči ddos napad.

2 HEKANJE

Hekanje ali vdor je poskus izkoriščanja računalniškega ali strežniškega sistema oziroma zasebnega omrežja znotraj samega računalnika. Največkrat gre za pridobivanje podatkov ali pridobivanje pravic znotraj omrežja. Hekanje se lahko izvaja iz različnih razlogov, eden od njih je definitivno zaslužek, pridobivanje koristnih informacij, nekateri pa to počnejo samo za lastno veselne, saj iščejo pomankljivosti v varnostnih sistemih omrežja in ne povzročajo škode omrežju ampak samo za lastno zadovoljstvo, saj je potrebno ogromno znanja, da lahko vdreš v omrežje.

Slika 1Heker

2.1 Zgodovina hekanja

Prvi znan hekerski vdor se je zgodil leta 1967 ko so člani ralunalniškega kluba v srednji šoli v predmestju Chicaga dobili dostop do IBM-ovega omrežja APL (programski jezik poimenovan po knjigi A Programming Language - od tu ime jezika APL). IBM je klubu podarilo štiri terminale 2741, katere so člani lahko uporabljali. Poglobili so se v jezik in ga nadgradili in tako vdrli v IBM-jovo omrežje.

2.2 Vrste hekerjev

Poznamo več vrst hekerjev. Najbolj poznani so črni hekerji, sivi hekerji in beli hekerji. Vsak od njih opravlja svojo nalogo in sicer črni hekerji so z namenom uničenja, sivi hekerji izkoriščajo računalnik brez uničenja ter beli hekerji izkoriščajo računalnik za odkrivanje pomankljivosti varnostnega sistema.

2.2.1 Beli hekerji

Beli hekerji ali White-hat hackers so etnični hekerji, kateri sodelujejo z organizacijami, da izboljšajo njihov varnostni sistem. Beli klobuki imajo dovoljenje za napadanje tarč v primeru ogrožanja, ampak seveda v skladu z pravili o napadu katera so predpisana v naprej. Etnični hekerji so specializirani za etnična hekerska orodja, tehnike in medode za zaščito informacijskih sistemov določenih organizacij. Ko beli hekerji odkrijejo najmanjšo pomankljivost v varnostnem sistemu jo vedno razkrijejo in poskušajo odpraviti pred drugimi hekerji, kateri bi lahko to pomankljivost uporabili kot zlorabo. Danes večja svetovna podjetja kot so Facebook, Microsoft in podobno uporabljajo bele hekerje, da predčasno odkrijejo pomankljivosti v varnostnem sistemu in to napako pravočasno odpravijo.

2.2.2 Sivi hekerji

Sivi hekerji ali Grey-hat hackers izkoriščajo računalniška omrežja na podoben način kot črni hekerji, vendar brez zlonamernih namenov. Običajno sivi hekerji vdirajo v računalniške ali strešniške sisteme, da obvestijo skrbnike oziroma lastnike, da njihov sistem oziroma omrežje vsebuje vsaj eno ranljivost oziroma pomankljivost, katere je potrebno odstraniti. Sivi hekerji lahko tudi vdrejo v omrežje in zahtevajo denar za odpravljanje napake.

2.2.3 Črni hekerji

Črni hekerji ali Black-hat hackers je izraz za najslabše hekerje v smislu škodoželjnosti in sicer beseda izvira iz ameriških filmov, kjer so slabi fantje nosili črne kape dobri pa bele. Črni heker je posameznik kateri poskuša ilegalno oziroma nepooblaščeno vstopiti v nek sistem ali omrežje iz zlonamernih razlogov in ga poskuša uničiti. Črni hekerji nimajo doboljenja ali pooblastila za ogročanej svojih ciljev. Škodo največkrat poskušajo narediti z ogrožanjem varnostnih sistemov, spreminjanjem funkcij spletnih mest in omrežij ali zaustavitvijo sistemov. Pogosto to storijo, da ukradejo gesla računov, različne finančne podatke ali kakršne koli druge osebne podatke ali preprosto pridobijo dostop do njih.

Slika 2Vrste hekerjev

3 Hekerske tehnike

Poznamo več vrst hekarskih tehnik. Med najbolj poznanimi so Phishing, Cookie theft, DDOS, Virus in Bait and switch.

3.1 Phishing

Phishing je hekerska tehnika pri kateri se heker predstavlja za lažno osebo katera v resnici ni on. Najpogosteje se uporablja za krajo osebnih podatkov, kot so številke kartic in podobno. Najpogosteje se to dogaja preko e-pošte in sicer heker oziroma napadalec pošlje sporočilo žrtvi pod zaupnim imenom in prepriča napadalca, da odpre sporočilo. Ko žrtev odpre dobljeno sporočilo, lahko napadalec zlonamerno dostopa do njegove programske opreme ali celo zamrzne celoten sistem. Napad lahko ima uničujoče rezultate. Organizacije, katere podležejo takšnim napadom, najpogosteje poleg tržnega deleža, ugleda in zaupanja potrošnikov utrpijo tudi zelo hude finančne izgube, saj jih napadalci najpogosteje izsiljujejo za denar. Poskus lažnega predstavljanja pa lahko privede tudi do sporov, saj podjetje misli, da je bil to nekdo drug.

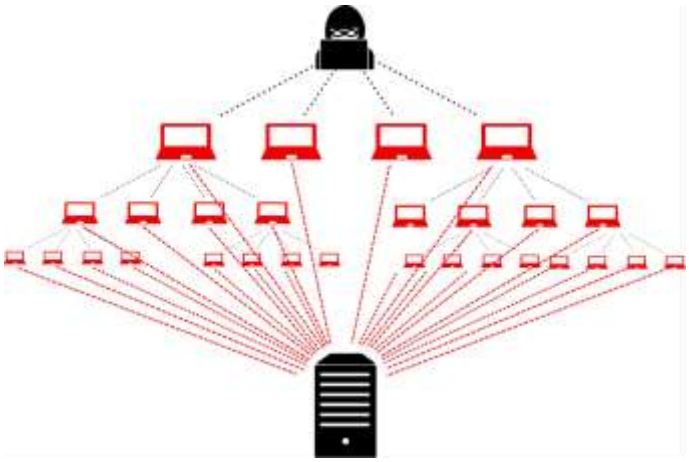
Slika 3Phishing

3.2 Cookie theft

Kraja piškotkov je tehnika ko heker pridobi naš piškotek, v katerem so shranjena vsa gesla in uporabniška imena, katere smo shranili, razne bančne informacile in podobni. Ko heker dobi naš piškotek, se lahko v brskalniku predstavlja pod našim imenom. Najbolj priljubljena metoda za izvedbo tega je, manipulacija uporabnikovih paketov IP za prehod skozi program kateri nam potem »vzame« piškotek. Imenuje se tudi »SideJacking« ali »Session Hijacking«, ta napad je izvedljiv, samo kadar uporabnik celostno sejo ne uporabi SSL (Secure Sockets Layer- protokol za vzpostavljanje overjenih in šifriranih povezav med računalniki v omrežju/ https). Na spletnih mestih kjer se vnašajo gesla in bančni podatki je izredno pomembno da uporabljajo SSL, saj z tem šifrirajo podatke v omrežju.

3.3 DDOS

DDOS(distributed denial-of-service) je vrsta hekerske tehnike, kjer se spletno mesto ali strežnik odstranjuje, tako da to spletno mesto ali strežnik preplavijo z ogromno prometa katerega spletno mesto ali strežnik ne more obdelati, saj ni dobolj sposoben in tako se strežnik sesuje. V tej tehniki napadalec ciljni stroj preplavi s preveliko zahravami za preobremenitveni vir, kar pa privede do prevelike zahreve po izpolnitvi zahtev. Pri DDOS napadih hekerji največkrat uvedejo tako imenovane »botnete«, katerih je glavna naloga, da preplavijo sistem z paketnimi zahtevami.



Slika 4DDOS

3.4 Virus

Virus je zlonamerna programska oprema, katero žrtev nevede namesti v računalnik in nato napadalcu pošilja vse njegove podatke. Napadalec lahko ureja vse vaše datotekem preusmirja promet, preglejujejo vaše podatke in podobno. Lahko se virusi širijo po vseh računalnikih znotraj omrežja.

3.5 Bait and switch

Bait and switch je tehnika privabljanja uporabnikov in nato preklaplanje na nekaj drugega. Najpogosteje se to dogaja, da napadalec na spletni strani kupi oglasni prostor, in ko žrtev pride na spletno stran vidi oglas kateri jo zanima, v trenutku ko pa klikne na oglas, se pa ta spremeni od tod tudi ime. Žrtev preusmiri na spletno stran katera je okužena z zlonamerno programsko opremo. Ko se bo žrtev vrnila ponovno na spletno stran bo ponovno kliknila na oglas saj so oglasi zelo privlačni. Napadalec lahko zažene zlonamerni program, za katerega je žretev mislila, da je v redu in potem lahko napadalec prenese zlonamerno programsko opremo in dobi dostop do žrtvinega računalnika.

4 ZNANI HEKERSKI VDORI

Hekerskih vdorov je te dne več in več, najbolj so koncentrirani na velika podjetja, ki se ukvarjajo s spletnimi storitvami kot e-Commerce in spletne medije. Ti vdori so načrtovani po več mescev vnaprej in povzročijo škodo podjetju in nedolžni stranki podjetja.

4.1 Yahoo

Spletni portal in brskalnik Yahoo je bil žrtev številnih vdorov katerih namen je bil izgrebsti zasebne podatke njihovih uporabnikov. Leta 2013 so neznani hekerji vdrli v Yahoo omrežje in okradli približno milijardo uporabniških računov vključno z njihovimi uporabniškimi imeni, elektronskimi naslovi, telefonskimi številkami, rojstni podatki, šifriranimi gesli in varnostnimi vprašanji z odgovori. Podoben a manjši vdor so imeli leta 2014, kjer so ukradli podatke 500 milijonov uporabnikom. Podatki uporabnikov so pozneje leta 2015 bili naprodaj na temnem spletu (darkweb) za 300.000 dolarjev kot tudi na spletni tržnici The Real Deal je bilo 200 milijonov uporabniških podatkov za 3 bitcoine.

Slika 5Yahoo!

4.2 Sony

Sony multinacionalko japonsko podjetje, ki se zlasti ukvarja z zabavno tehnologijo. Leta 2014 je bila žrtev hekerskega vdora skupine »Guardians of Peace« (Varuhi miru), ki je podjetju ukradlo 100 terabajtov podatkov in izbrisalo več 100 gigabajtov kar je vključevalo več neizdanih filmov, e-mailov, plač in informacije zaposlenih. Poleg tega so hekerji v njihovo omrežje spustili »wiper« zlonamerna programska oprema, ki izbriše podatke in ponastavi konfiguracije. Podjetje je popolnoma izgubilo svojo digitalno infrastrukturo in jo moralo zgraditi od dna. Kasneje se je izvedlo, da je za vdor bila kriva Severna Korejska vlada, ki je izvedla vdor kot maščevanje za izdan film »The Interview«, ki prikazuje atentat Kim Jong Una.

Slika 6Sony

4.3 Marriott

Marriott, ki je ena izmed največjih ponudnikov hotelov in je bila žrtev vdora ob koncu leta 2018. Napad je bil osredotočen na njihovo rezervacijsko podatkovno bazo, ki je vsebovala ob tistem času podatke za več kot 500 milijonov ljudi. To je bil že drugi takšen napad v zgodovini podjetja in je ogrožalo zasebne informacije 5,2 milijonom gostov. Direktor Marriotta je pozneje moral zagovarjati pred senatom ZDA zaradi kršitve zasebnosti podatkov njihovih gostov.

Slika 7Marriott

4.4 Comodo

Comodo je podjetje, ki se ukvarja z izdajanjem spletnimi certifikati. Spletni certifikat v bistvu jamči in zagotovi, da je spletna stran zanesljive in varna za brskati. Comodo je ena izmed večjih podjetjih, ki ponujajo to storitev in sicer izdajo okoli 14% vseh certifikatov, ki ustvarijo 44% vsega prometa. Leta 2011 je to podjetje bilo žrtev vdora, ki so izvedeli Iranski hekerji in so okradli 9 certifikatov za 7 domen katere naj bi uporabili za zlo namene. Veliki brskalniki so hitro začasno blokirali Comodove certifikate, Comodo pa hitro odstranil domene.

Slika 8Comodo

4.5 Democratic National Committee (Demokratični nacionalni odbor)

Democratic National Committee ali DNC je organ upravljanja Demokratične stranke ZDA. Odbor usklajuje strategijo za podporo kandidatom Demokratične stranke po vsej državi za lokalne in državne funkcije. DNC je leta 2016 bila žrtev ruskega vdora v katerem so dobili vstop v DNC-jevo računalniško omrežje. Vlada ZDA je ugotovila, da je vdor bil delo ruskih obveščevalnih agencij. Hekerji, ki so bili krivi za vdor sta se imenovala »Cozy Bear« in »Fancy Bear«. Za poskus vdora je že vedela Nizozemska obveščevalna agencija leta 2015, ko je vdrla v računalnike »Cozy Bear-a« in ga opazovala. Kasneje je znanje o tem dejanju posredovala NSA (National Security Agency - ZDA), ki je obvestila DNC o poskusu. Ameriška obveščevalna agencija CIA je tudi razkrila, da so hekerji tudi vdrli v Republican National Committee (Republikanski nacionalni odbor) ali RNC a niso razkrili nobenih podatkov od njih na WikiLeaks.

5 ZNANI HEKERJI

5.1 Julian Assange

Jullian Paul Assange je avstralsko-ekvadorski politični aktivist, programer, tiskovni predstavnik neprofitne organizacije WikiLeaks ter nekdanji herek. Z materjo ter svojim mlajšim bratom so se preselili zaradi družinskih sporov. Preselili so se v hišo v melburskem predmestju, kjer je čez cesto bila trgovina z elektroniko. Julian je začel zahajati v trgovino in začel je delati na takrat zelo popularnem računalniku Commodore 64. Njegova mama je poskusila privarčevati čim več denarja, da bi lahko Julianu kupila računalnik. Julian je bil zelo pameten še posebej na področju matematike in se je začel sam učiti hekanje. Zelo rad je tudi zahajal v knjižnico, kjer je zelo veliko bral. Ko je bil star 17 let je posumil, da želi policija narediti hišno preiskavo zato je vse podatke iz diskov izbrisal in jih zažgal, ter se začasno preselil h svoji punci. Julian se je pridružil Melburnskem hekerskem podzemju in postal eden pomembnejših članov. V tej družbi so bili sami nadarjeni in samouku hekerji. Leta 1988 je poskušal vdreti v Minervo, to je sistem računalnikov v Sydneyju kateri pripada vladni Komisiji za prekmorsko komunikacijo. Leta 1989 jim uspe okušiti Nasino spletno stren. Kasneje so se lotili vdreti v upravljalni terminal Nortela. Nortel je kanadska družba za izdelavo in prodajo komunikacijske opreme. Uspelo mu je tudi vdreti v vojaški štab sedme poveljniške skupine v Pentagonu. 11. aprila 2019 so mu odvzeli politični azil za bivanje na veleposlaništvu v Londonu. Na veleposlaništvu je živel sedem let. Ko so ga aretirali, ni bila mirna aretacija, saj so ga morali odnesti i ambasade. Grozi mu do pet let zapora.

Slika 9Julian Assange

5.2 Jonathan James

Jonathan James je znan ameriški heker, kateri je živel v Miamiju. Rodil se je leta 1983, ter umrl leta 2008, ko je storil samomor. Jonathan se je že od malih nog zelo zanimal za računalniško tehnologijo. Pri šestih letih je začel redno uporabljati računalnik in v srednji šoli že obsladal sistemsko programiranje. Pri 15. letih je Jonathan vdrl v Naso. Leta 1999 je vdrl v omrežje Nase, ter kar dva dni brskal po njihovem omrežju ter prenesel za kar 1,7 miljona$ (1,43 miljona€) vredno njihovo programsko opremo za nadzor okolja, ter prenesel podatke o temperaturi in vlagi katere si izračunavali ter merili. Z tem vdorom je pridobil tudi izvirno kodo mednarodne vesoljske postaje in z tem si omogočil tudi vdor v Pentagonov računalniški sistem orožij in presegel 3300 elektronskih sporočil, ukradel ogromno gesel in brskal po njihovem omrežju, kot da je eden izmed zaposlenih v enem najtajnejših stvari na svetu saj je

bil na nivoju kjer so zaposleni samo ljudje z najvišjim rangom. Z vdorom v Naso je povzročil za približno 41000$ (približno 35000€) škode in Nasa je morala za 21 dni fizično odklopiti vse računalnike, da so lahko zaustavili ta napad. Leta 2000 je pri svojih 16. letih postal prvi obsojen mladostnik zaradi vdora v sistem v vladno organizacijo. Obsojen je bil na 6 mesecev hišnega pripora, katerega je zaradi pozitivnega testa na droge bil prestavljen na 6 mesečno zaporno kazen. Ko je bil star 24 let je storil samomor zaradi racije na njegovem domu, ker so menili da je bil Jonathan deležen večih vdorov v manjša podjetja. Kasneje so ugotovili da je bil že dlje časa v depresiji in v poslovilnem pismu kateri je bil dolg 5 strani je napisal, da ni kriv ampak da ne zaupa pravosodnemu sistemu.

5.3 Michael Calce

Michael Calce ali znan tudi kot »Mafiaboy« je pri svojih 15. letih odkril kako vdreti v omrežja različnih velikih podjetij. Vedel je zelo dobro kako vdreti v Yahoo!, Amazon, Dell, eBay in CNN. Njegova dejanja so vzbudila velik strah zadradi kibernatske kriminalitete in pomena izboljševanja kibernatske varnosti. Kasneje je postal zelo velik strakovnjak za računalniško varnost, ter napisal knjiho o svoji zgodbi.

Slika 10Michael Calce

5.4 Kevin Mitnick

Kevin Mitnick je eden najslavnejših hekerjev, katerega so zaprli. Rodil se je leta 1963 v Kaliforniji. Že pri svojih 15. letih je bil zelo uspešen na svojem področju, saj je že takrat zaobšel sistem identifikacije za vožnj z mestnim prometom. Leta 1981 je uspešno vdrl in prenesel dokumente iz podjetja Pacific Bell. Leto kasneje je vdrl v Severnoameriško poveljstvo obrambe zračnega prometa. Uspešno je vdrl tudi v podjetje Digital Equipment Corporation's. Zaradi vseh teh vdorov so ga leta 1995 aretirali, ter ga leta 2000 pogojno izpustili ter mu prepovedali vsakerško uporabo računalnika dokler teče pogojna kazen katera se je iztekla zeta 2003.

Slika 11Kevin Mitnick

5.5 Anonymus

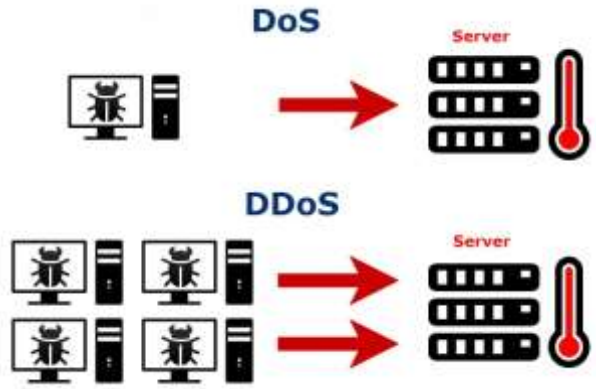
Anonymus ni le posamezni heker ampak skupina zelo znanih in uspešnih hekerjev. So zelo organizirana skupina, katerih cilj je napaditi velika podjeja kot Amazon in podobno. Najbolj so znani po DDOS napadih na vladne verske in druge podjetniške spletne strani. Čeprav so v tej skupini ljudje iz vsega sveta imajo skupen interes kateri je ponavadi iz politične narave in sicer doseči zaželjen cilj brez razkritja svoje identitete. Po celem svetu so zelo poznani še posebej po nošenju Guy Fawkes maske. Njihov znan rek je: »Mi smo Anonymous. Smo Legija. Ne odpuščamo. Ne pozabimo. Pričakujte nas.« (angleško: »We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.«). Zelo znan napad Anonymous-ov je bil leta 2015 ko so napovedali vojno ISIS-u. Vse se je začelo ko so Anonymous napisali ISIS-u »vi ste virus mi zdravilo«, in z tem napovedali brisanje računov na spletnih straneh kot so Facebook, Twitter in podobno vsem osebah povezanim z Islamsko državo. Prav tako napadajo vse spletne strani, katere širijo Islamsko propagando. Isto leto je Donald Trump povedal, da želi, da bi vsem muslimanom bil prepovedan vstop v Združene države Amerike. Na njegove besede so se odzvali tudi Anonymous-i, z DDOS.om na njegovo uradno stran za nekaj ur in objavili še posnetek v katerem so mu sporočili, naj drugič bolj pazljivo izbira svoje besede.

Slika 13Anonymous logotip

Slika 12Guy Fawkes maska

6 DOS/DDOS

Poznamo dve vrsti zavrnitve storitve in sicer DOS ter DDOS. Glavna razlika med DOS in DDOS je v tem, da se DOS napad izvala iz enega računalniuka, DDOS pa iz večih. Princip napada je podoben pri obeh.



Slika 14DOS/DDOS

6.1 DOS

DOS (Denial Of Service) ali zavrnitev storitve je proces, kateri je bil odkrit z strani hekerjev leta 2000, zaslovel pa leta 2002, ko je hekerjem uspelo onesposobiti strežnike kot so Amazon in Download za nekaj ur. Proces zavrnitve storitev se izvaja ttako, da napadalec poštle svoji tarči zelo veliko količino podatkov določenega protokola. Te podatke lahko pošlje samo na določena vrata. Največkrat se uporabljajo protokoli UDP, TCP, ICMP, SYN in podobnom UDP in TCP sta protokola katera potekapa preko vseh vrat znotraj računalnika. ICMP protokol je za odmev, pošiljanje samo SYN del TCP paketov pa je zelo primerno za proces zabrnitve storitev. Ta proces torej poteka zakrat, kadar 1 računalnik pošlje dovolj veliko kapaciteto podatkov samo enega protokola skozi ena vrata ali skozi vsa vrata na računalnik katerega napada. Prvi znak DOS napada je počasno premikanje miške, kasneje pa tudi počasno delovanje interneta. Največkrat je rezultat DOS napada izklop iz omrežja ali celo samodejni ponovni zagon računalnika.

6.2 DDOS

DDOS (Disttibuted Denial of Service) ali porazdeljena zavrnjena storitev je proces podoben DOS napadu. Razlika med DOS in DDOS napadom je sledeča. Pri DOS napadu napadalec napade tarčo z enim računalnikom kateri pošilja na tarčo pakete in tako zruši server. Pri DDOS napadu pa gre za uporabo podračunalnikov tako imenovanih »DoS box« ali »zombiji«, kateri se posamezno obnašajo enako kot DOS. Napadalec ima na »glavnem« računalniku program ali ukaz kateri sporoči vsem podračunalnikom, da naj napadejo določeni računalnik z določenim številom paketov. Kljub temu, da je princim podoben je zelo velika razlika v učinkovitnosti in številu paketov, saj pri DOS napadu gre za pošiljanje samo iz enega računalnika tukaj pa iz mnogih računalnikov, kar privede do množičnega pošiljanja podatkov, kar tuti veliko hitreje sesuje strežnik.

6.3 Kako se braniti pred DDOS napadom

Cilj ubranitve DDOS napada je, da v omrežje spustimo vse uporabnike kateri legalno uporabljajo stran in izločimo vse kateri napadajo naš strežnik. Tukaj nastane zelo velik problem saj se lahko paketki katere napadalec pošilja najprej zdijo povsem legalni in ne kot

paketki napada in z tem ko jih spustimo v omrežje smo že prepozni. Tukaj pride do zelo velikega problema ker ni vse tako v praksi kot je v teoriji in si paketi nemogoči za prepoznavnost na začetku.

6.4 Kaj storiti ob DDOS napadu

V času ko heker izvaja DDOS napad je cilj, da omogočimo normalno delovanje uporabnikom, kateri nas ne napadajo in onemogočiti dostop napadalju. Zato je prva stvar ob DDOS napadu analiza prometa, od kjer poskušamo ugotoviti, od kje nas napadalec napada in mu onemogočiti dostop. Problem nastane, ker pri napadu za analizo podatkov potrebujemo ponudnika omrežne povezljivosti. Delo nam pa dodatno še otežuje dejstvo, da napadalec istočasno ne uporablja samo ene tegnike ampak kombinira ogromno tehnik in jih med samim napadom spreminja.

7 ANKETA VARNOST PODATKOV NA SPLETU

Anketa varnost podatkov na spletu je anonimna. Anketa je sestavljena je iz 15 vprašanj. Iz te ankete sva poskusila iznajti splošno previdnost ljudi na spletu, predvsem sva se osredotočila na nivo varnosti gesla. Sodelovalo je 77 anketirancev in njihovi odgovori so predstavljeni v spodaj grafih.

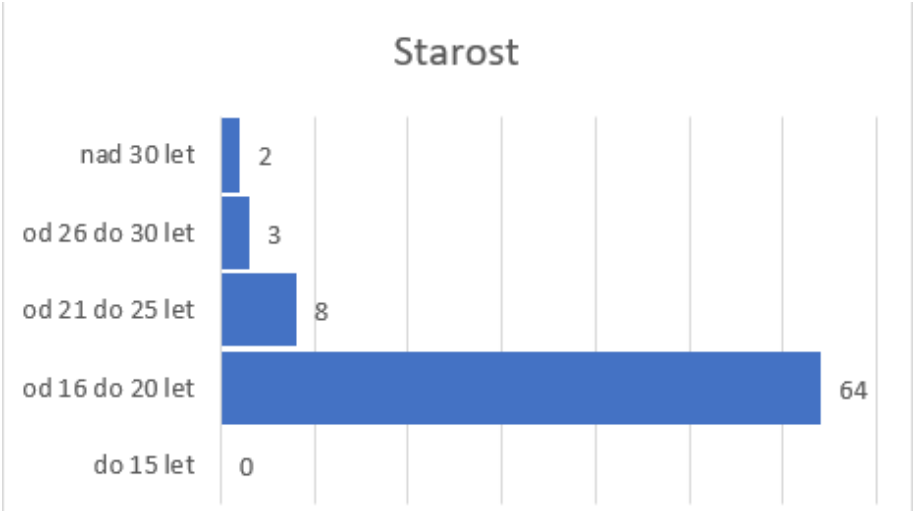
7.1 UGOTOVITVE

7.1.1 SPOL

Slika 15Graf spol

Od 77 anketirancev je bilo 71% ženskega spola in 29% moškega spola.

7.1.2 STAROST

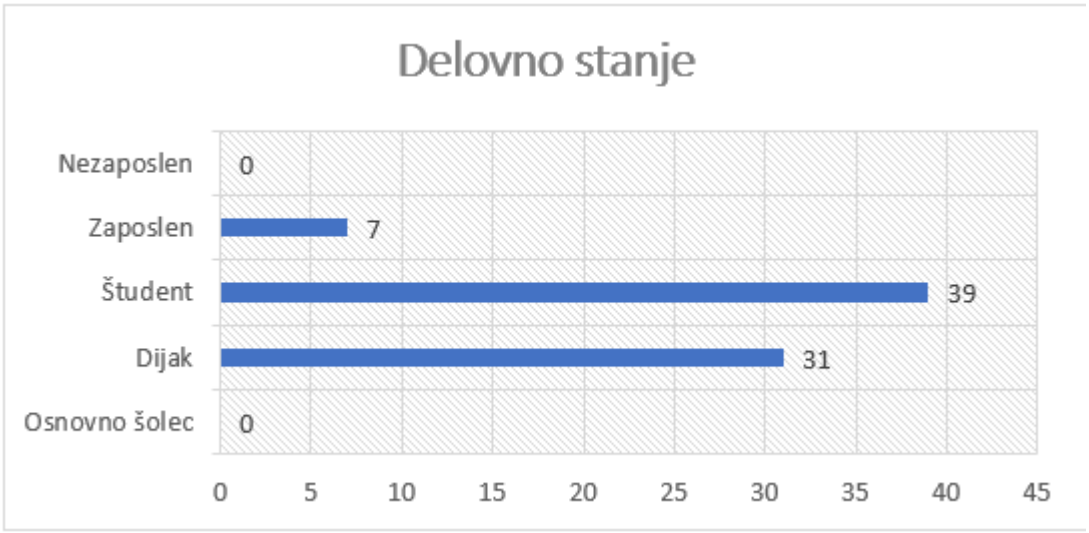


Slika 16Graf starost

Od 77 anketirancev nobeden ni bil mlajši od 15 let, 64 jih je bilo starih od 16 do 20 let, 8 jih je

bilo starih od 21 do 25 let, 3 so bili stari od 26 do 30 let in 2 sta bila starejša od 30 let.

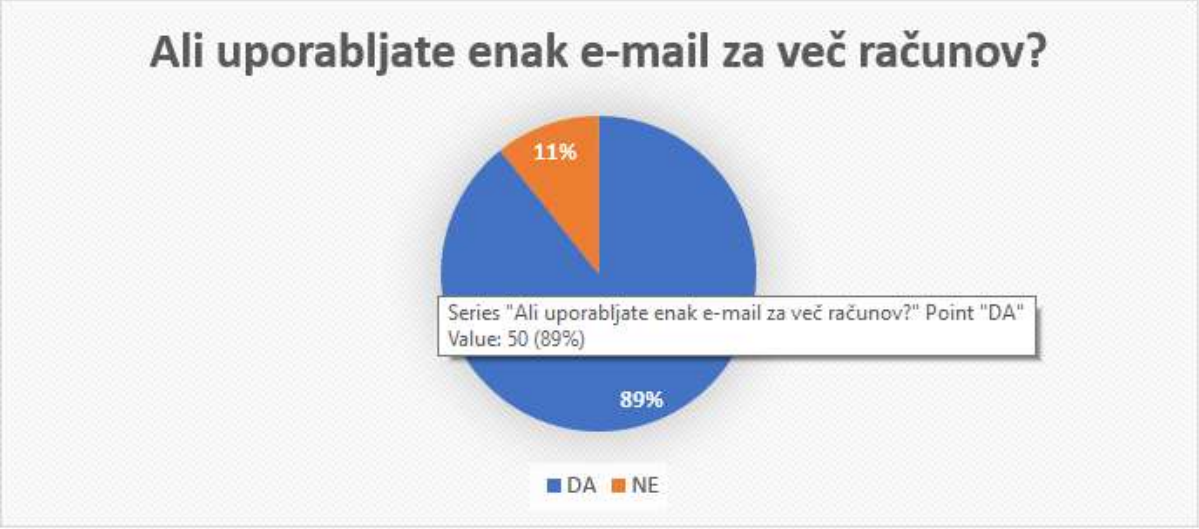
7.1.3 DELOVNO STANJE



Slika 17Graf delovno stanje

Večina anketirancev je bilo študentov kar 50%. Dijakov je bilo 41%. Zaposlenih je pa bilo 9%. Noben anketiranec ni bil nezaposlen ali osnovnošolec.

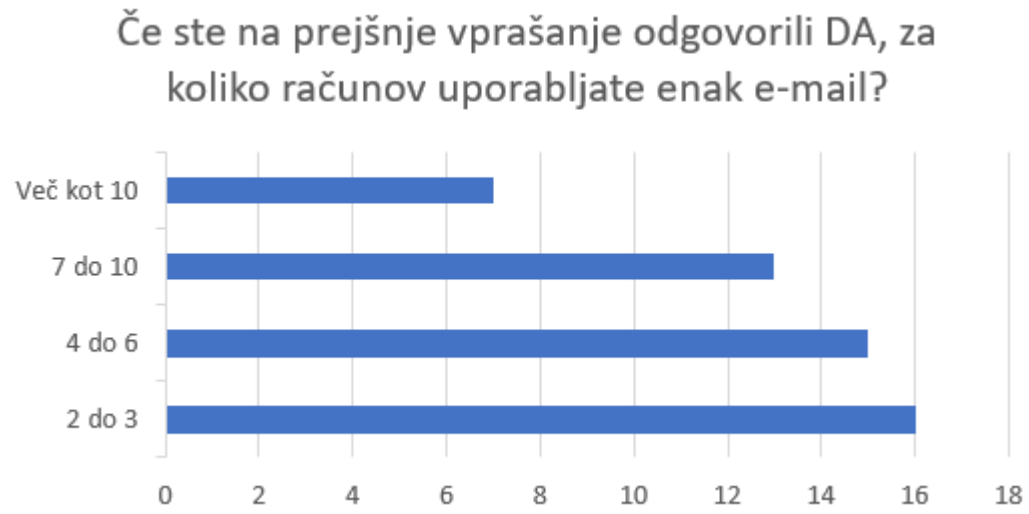
7.1.4 Ali uporabljate enak e-mail za več računov?



Slika 18Graf ali uporabljate enak e-mail za vec racunov

V tem vprašanju sva hotela izvedeti koliko ljudi uporablja več e-mailov za varnost. Največ ljudi je odgovorilo, da uporabljajo enak e-mail za več računov in samo 11% ljudi uporabi drug e-mail.

7.1.5 Če ste na prejšnje vprašanje odgovorili DA, za koliko računov uporabljate enak e-mail?



Slika 19Graf ce ste na prejšnje vprašanje odgovorili DA, za koliko računov uporabljate enak e-mail

Večina anketirancev ima eden e-mail za 2 do 3 račune. 19% anketirancev ima eden e-mail za 4 do 6 računov. 17% anketirancev ima eden e-mail za 7 do 10 računov. 9% anketirancev ima eden e-mail za več kot 10 računov.

7.1.6 Ali uporabljate eno geslo za več računov?

Slika 20Graf ali uporabljate eno geslo za več računov

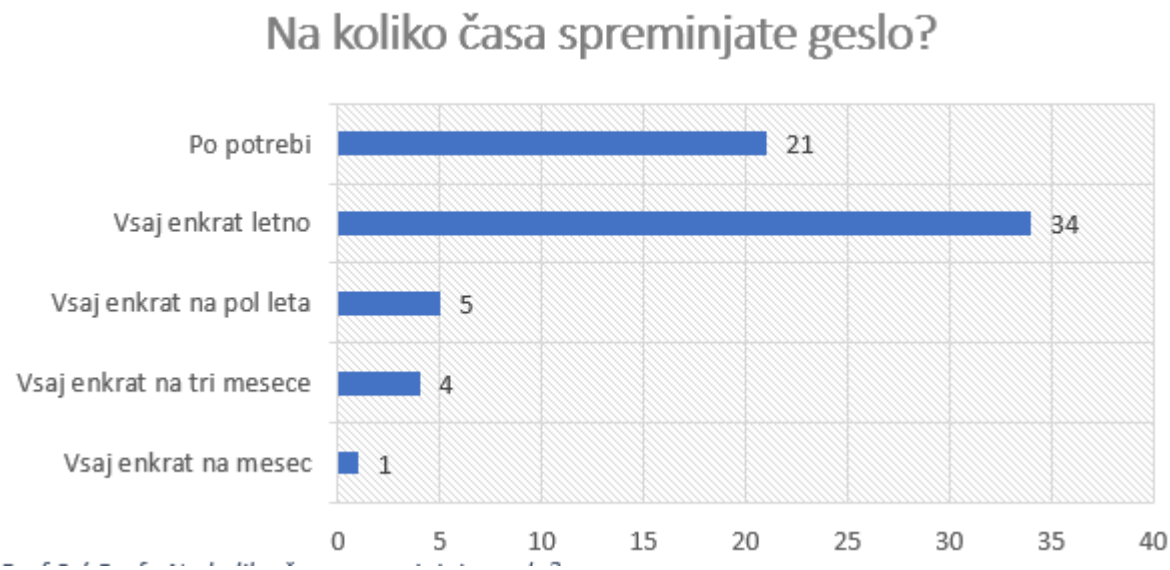
Večina anketirancev je odgovorilo, da uporabljajo enako geslo za več računov. 39% anketirancev je odgovorilo, da ne uporabljajo enako geslo za več računov.

7.1.7 Ali geslo redno spreminjate?

Slika 21Graf ali geslo redno spreminjate

S tem vprašanjem sva hotela razbrati anketirančevo skrb za varnost na spletu. Večina anketirancev je odgovorilo NE kar je zaskrbljujoče. 23% anketirancev je odgovorilo DA.

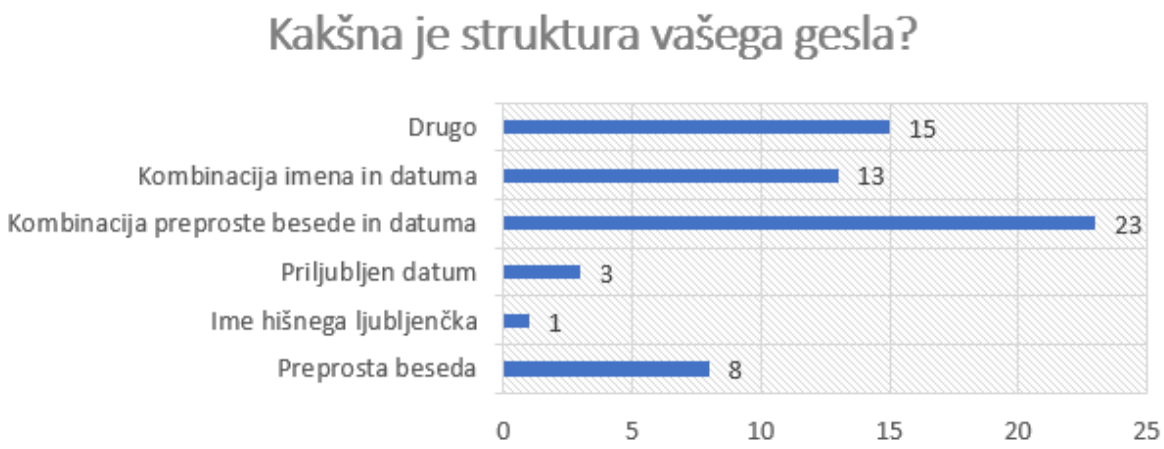
7.1.8 Na koliko časa spreminjate geslo?



Slika 22Graf na koliko casa spremionjate geslo

Največ anketirancev spreminja svojo geslo letno(44%). 27% anketirancev spreminja svojo geslo po potrebi (npr. v primeru vdora). 6% spreminja geslo vsaka pol leta. 5 % spreminja svoje geslo vsake tri mesece. 1 anketiranec spreminja svojo geslo enkrat na mesec.

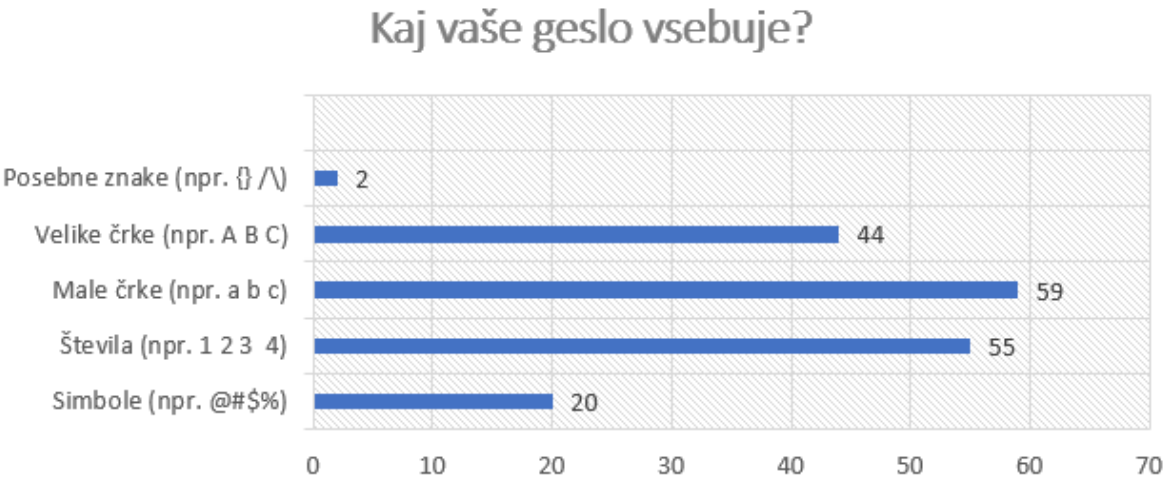
7.1.9 Kakšna je struktura vašega gesla?



Slika 23Graf kaksna je struktura vasega gesla

Največ anketirancev ima v svojem geslu kombinacijo preproste besede in datuma. 19% anketirancev je izbralo DRUGO. 17% anketirancev ima v svojem geslu kombinacijo imena in datuma. 10% anketirancev ima v svojem geslu samo preprosto besedo. 4% anketirancev ima v svojem geslu samo priljubljen datum. 1% anketirancev ima v svojem geslu ime hišnega ljubljenčka.

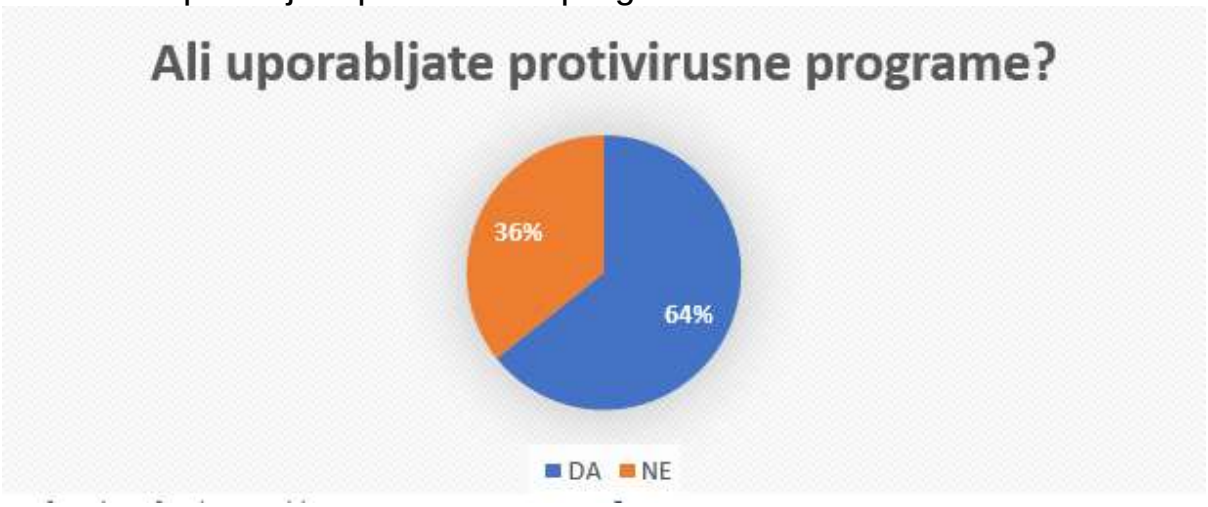
7.1.10 Kaj vaše geslo vsebuje?



Slika 24Graf kaj vase geslo vsebuje

V tem vprašanju so anketiranci imeli možnost izbrati več odgovorov za vsebino njihovega gesla. 32% anketirancev je izbralo, da njihovo geslo vsebuje simbole. 89% anketirancev je izbralo, da njihovo geslo vsebuje števila. 95% anketirancev je izbralo, da njihovo geslo vsebuje male črke. 71% anketirancev je izbralo, da njihovo geslo vsebuje velike črke. 3% anketirancev je izbralo, da njihovo geslo vsebuje posebne znake.

7.1.11 Ali uporabljate protivirusne programe?



Slika 25Graf ali uporabljate protivirusne programe

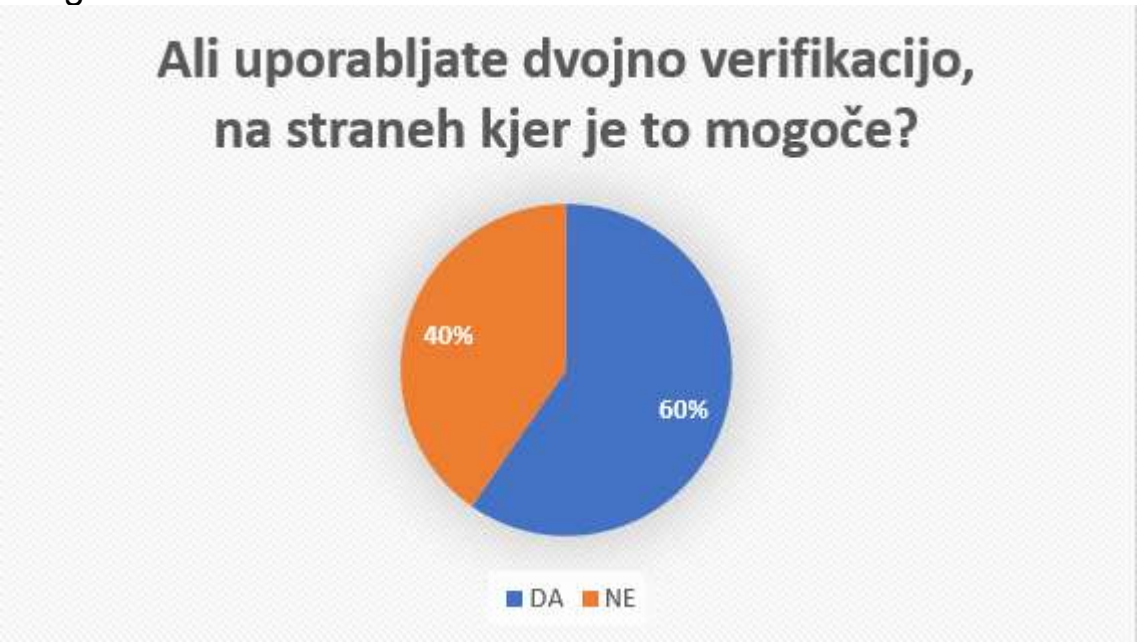
Večina anketirancev je odgovorilo, da uporabljajo protivirusne programe. 36% anketirancev je odgovorilo, da ne uporabljajo protivirusne programe.

7.1.12 Če ste na prejšnje vprašanje odgovorili DA, ali uporabljate plačljive protivirusne programe?

Slika 26Graf ce ste na prejsnje vprasanje odgovorili z DA, ali uporabljate placljive protivirusne programe

90% anketirancev ne uporablja plačljive programe. Samo 10% anketirancev uporablja plačljive programe.

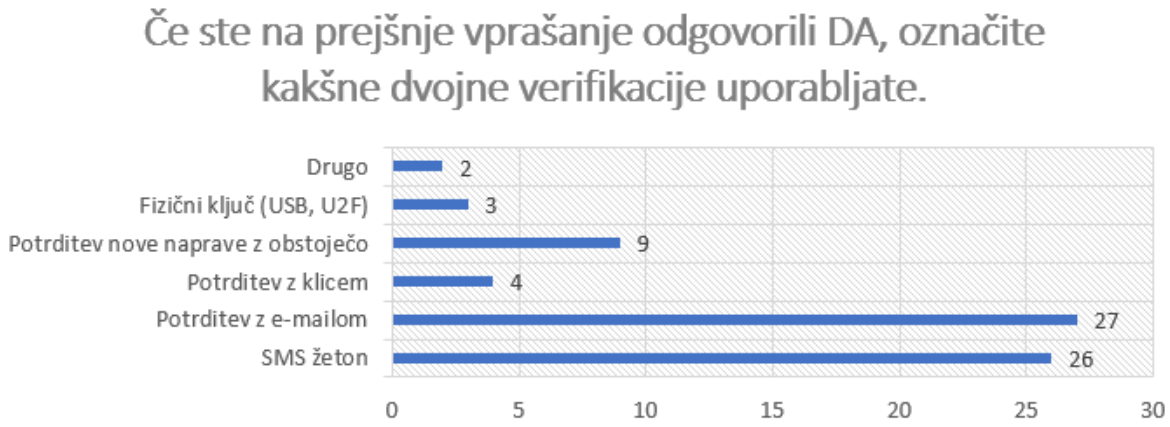
7.1.13 Ali uporabljate dvojno verifikacijo, na straneh kjer je to mogoče?



Slika 27Graf ali uporabljate dvojno verifikacijo, na straneh kjer je to mogoce

Večina anketirancev uporablja dvojno verifikacijo na njihovih računih, če je to le mogoče. 40% anketirancev ne uporablja dvojno verifikacijo.

7.1.14 Če ste na prejšnje vprašanje odgovorili DA, označite kakšne dvojne verifikacije uporabljate.



Slika 28Graf ce ste na prejsnje vprasanje odgovorili DAm oznacite kaksne dvojne verifikacije uporabljate

V tem vprašanju so anketiranci imeli možnost izbrati več odgovorov za načina uporabljanja dvojne verifikacije. 72% anketirancev uporablja dvojno verifikacijo s SMS žetonom. 75% anketirancev uporablja dvojno verifikacijo s potrditvijo e-maila. 11% anketirancev uporablja dvojno verifikacijo s klicem. 25% anketirancev uporablja dvojno verifikacijo z obstoječo napravo. 8% anketirancev uporablja dvojno verifikacijo s fizičnim ključem. 6% anketirancev je izbralo DRUGO.

7.1.15 Ali ste kdaj bili žrtev spletnega vdora?

Slika 29Graf ali ste kdaj bili zrtev spletnega vdora

Večina anketirancev niso bili žrtev spletnega vdora. 14% anketirancev so bili žrtev spletnega vdora.

8 ZAKLJUČEK

Ob raziskovalni nalogi, kateri sva se posvetila sva ugotovila, da Windows-ov požarni zid ne zadošča kot obrampa pred raznimi napadi na strežnik, saj drugače nebi bilo napadov. Z tem lahko potrdima najino hipotezo, da Windows-ov požarni zid ne zadošča kot obramba pred napadi na strežnik. V primeru, da bi Windows požarni zid zadoščal pred napadi na strežnik, nebi smelo priti do skoraj napadov nikoli, saj je požarni zid skoraj ves čas prižgan.

Zastonj protivirusni programi zmanjšako možnost pred vdori virusov ampak nemorejo povsem izločiti možnost napada in vstopa v računalnik. V primeru, da bi zastonj protivirusni programi povsem onemogočili razne vdore virusov in napade, nebi bilo možnosti, da bi bil kdorkoli napaden saj bi imel protivirusni program vklopljen in bi bil povsem varen, kar pa je žal nemogoče. Velika podjetja plačujejo ogromno denarja za protivirusne zaščite pa vseeno niso popolnoma zaščiteni. Z tem lahko potrdiva najino hipotezo o tem, da zastonj protivirusni programi ne zadostujejo kot obramba pred napadi na strežnike.

V anonimni anketi, v kateri sva se posvetila, na varnost podatkov na spletu sva ugotovila, da ljudje premalo uporabljajo različne elektronske naslove za več računov na spletu. Ugotovila sva tudi, da uporabljajo preenostavna gesla, za elektronske račune, saj jih večuna uporablja kombinacijo neke preproste besede in datuma, katerega si enostavno zapovnejo. Z tem lahko potrdiva tezo, da večina dijakov in profesorjev ne uporablja dovbolj varnih/zapletenih geselj. Potrdiva lahko tudi tezo, da profesorji in dijaki ne spreminjajo glesel dobolj letno saj jih je večina kar 44% spreminja svoje geslo samo enkrat letni in kar 27% spreminja svoje geslo, ko je to potrebno.

VIRI

csoonline. (12.02.2020). https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html. *csoonline*, 1.

eccouncil. (2020). https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/. *eccouncil*, 1.

fossbytes. (January 15, 2020). https://fossbytes.com/hacking-techniques/. *fossbytes*, 1.

foxbusines. (February 27, 2020). https://www.foxbusiness.com/lifestyle/the-worst-cyber-attacks-of-the-past-10-years. *foxbusines*, 1.

helpnetsecurity. (2002/04/08). https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/. *helpnetsecurity*, 1.

imperva. (2020). https://www.imperva.com/learn/application-security/phishing-attack-scam/. *imperva*, 1.

Monitor. (13.6.2017). https://www.monitor.si/clanek/najvecji-hekerski-vdori-v-zgodovini/180474/. *Monitor*, 1.

poweredbyorange. (2021). https://poweredbyorange.com/11-most-famous-hackers-and-their-hacking-history/. *poweredbyorange*, 1.

Wikipedija. (13. september 2018). https://sl.wikipedia.org/wiki/Jonathan_James. *Wikipedija*, 1.

Wikipedija. (15. januar 2017). https://sl.wikipedia.org/wiki/Kevin_Mitnick. *Wikipedija*, 1.

Wikipedija. (18. avgust 2020). https://sl.wikipedia.org/wiki/Anonymous. *Wikipedija*, 1.

Wikipedija. (2021). https://en.wikipedia.org/wiki/List_of_security_hacking_incidents. *Wikipedija*, 1.

Wikipedija. (24 March 2021). https://en.wikipedia.org/wiki/APL_(programming_language). *Wikipedija*, 1.

Wikipedija. (26. november 2019). https://sl.wikipedia.org/wiki/Napad_za_zavrnitev_storitve. *Wikipedija*, 1.

Wikipedija. (27.01.2021). https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks. *Wikipedija*, 1.

Wikipedija. (5. oktober 2017). https://sl.wikipedia.org/wiki/Hekerji. *Wikipedija*, 1.

Wikipedija. (8. april 2021). https://sl.wikipedia.org/wiki/Julian_Assange. *Wikipedija*, 1.

Wired. (12.23.2019). https://www.wired.com/story/worst-hacks-of-the-decade/. *Wired*, 1.

IZJAVA*

Mentor/-ica Timej Rič v skladu z 20. členom Pravilnika o organizaciji mladinske raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje, zagotavljam, da je v raziskovalni nalogi z naslovom Vdor v omrežje, katere avtor/-ica je [illegible]:

- besedilo v tiskani in elektronski obliki istovetno,
- pri raziskovanju uporabljeno gradivo navedeno v seznamu uporabljene literature,
- da je za objavo fotografij v nalogi pridobljeno avtorjevo dovoljenje in je hranjeno v šolskem arhivu,
- da sme Osrednja knjižnica Celje objaviti raziskovalno nalogo v polnem besedilu na knjižničnih portalih z navedbo, da je raziskovalna naloga nastala v okviru projekta Mladi za Celje,
- da je raziskovalno nalogo dovoljeno uporabiti za izobraževalne in raziskovalne namene s povzemanjem misli, idej, konceptov oziroma besedil iz naloge ob upoštevanju avtorstva in korektnem citiranju,
- da smo seznanjeni z razpisni pogoji projekta Mladi za Celje.

Celje, 13.5.2021

ŽIG šole

ŠOLSKI CENTER CELJE ŠOLA ZA ELEKTROTEHNIKO IN RAČUNALNIŠTVO CELJE, Pot na Lavo 22

Podpis mentorja

Podpis odgovorne osebe

*

POJASNILO

V skladu z 20. členom Pravilnika raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje je potrebno podpisano izjavo mentorja (-ice) in odgovorne osebe šole vključiti v izvod za knjižnico, dovoljenje za objavo avtorja (-ice) fotografskega gradiva, katerega ni avtor (-ica) raziskovalne naloge, pa hrani šola v svojem arhivu.