OŠ Vižmarje - Brod

Na gaju 2

Kibernetski napadi

(računalništvo – raziskovalna naloga)

Avtorja:

Vid Pezo Zupančič, 9.b

Tin Vulović, 9.b

Mentorica: Petra Škofic Valjavec

Kazalo vsebine

KAZALO

Kazalo slik:

Povzetek

Kibernetski napadi so vse bolj pogosti. Lahko smo tarča phishing e-maila ali DoS ali DDos napada. V raziskovalni nalogi se ukvarjava z razlago kibernetskih napadov in kibernetske vojne. Opiševa tudi bolj znane kibernetske napade in hekerske skupine. Z anketo testirava razgledanost anketirancev na kibernetske napade.

V procesu izdelovanja ankete sva se tudi naučila, kako uporabljati 1ka.si spletno stran in kako tam izdelati anketo. Anketiranci niso bili dobro razgledani o kibernetskih napadih in večinoma niso vedeli, kaj bi naredili, če bi bili sami tarča takšnega napada.

1. Uvod

1.1 Zamisel za nalogo

Za to nalogo sva se odločila predvsem zato, ker do neke mere kibernetske napade že poznava. Hotela sva se še bolj poglobiti v to temo.

Hotela sva izvedeti, kakšen procent najinih anketirancev je bil tarča kibernetskega napada in kako se na te spoznajo. Hotela sva izvedeti, za katere kibernetske napade so največkrat slišali in tarča katerih kibernetskih napadov so največkrat bili.

Hotela sva tudi izvedeti, ali anketiranci poznajo kakšne slovenske kibernetske napade.

1.2 Hipoteze

V anketi sva hotela izvedeti informiranost anketirancev o kibernetskih napadih, njihovo poznavanje večjih napadov in kaj bi naredili, če bi bili tarča napada.

Postavila sva si pet hipotez:

- da bo večina ljudi vedela, kaj so kibernetski napadi,
- da bo večina anketirancev že slišala vsaj za phishing napad,
- da je vsaj polovica anketirancev slišala za organizirane hekerske skupine,
- da je vsaj polovica anketirancev slišala za kakšen kibernetski napad v Sloveniji,
- da je vsaj ¾ anketirancev bilo tarča kibernetskega napada.

2. Teoretični del

2.1 Kaj so kibernetski napadi

Ko uporabljamo tehnološke naprave vsak dan, za seboj puščamo veliko "odtisov". Na primer ko obiščemo spletno stran, strežnik, ki ga uporabljajo za spletno stran gostitelji, zabeleži naš IP-naslov. IP-naslov je številka, ki čisto natančno določa računalnik v omrežju internet. Kratica IP se uporablja za Internet Protocol. Kakršenkoli poizkus razkritja, spreminjanja, uničenja, kraje ali pridobitev nepooblaščenega dostopa do računalnika ali računalniškega omrežja se šteje za kibernetski napad. Kibernetski napadi se dogajajo vsak dan. Pred nekaterimi se lahko zaščitimo, pred drugimi se ne moremo.

Kibernetski napad lahko spremeni, ukrade ali uniči določen cilj z vdorom v računalniški sistem. Kibernetski napadi lahko segajo od namestitve vohunske programske opreme na osebni računalnik do poskusov uničenja infrastrukture celotnih držav. Kibernetski napadi postajajo vse bolj izpopolnjeni in nevarni.

Slika 1: Data breach, Cyber attack

2.2 Kibernetska vojna

Pri kibernetski vojni sodelujoči uporabljajo računalniška omrežja, računalnike in internet, ki vodi vojno v digitalnem prostoru. Tam ne obstajajo nobena pravila, sodelujoči lahko uporabijo vse, kar jim je na voljo. Večina ljudi meni, da je kibernetska vojna nadaljevanje običajne vojne. V tej vojni želijo sodelujoči priti v računalniška omrežja, računalnike in podatkovne baze nasprotnikov. Take stvari počnejo, da motijo, vohunijo ali povzročajo škodo nasprotnikom. Strokovnjaki domnevajo, da se je ta vojna šele začela in bo trajala zelo dolgo časa. V nekaterih pogledih je kibernetska vojna hujša od običajne vojne. Popoln kibernetski napad lahko uniči infrastrukturne sisteme, to pa so npr. proizvodnja elektrike, oskrba z vodo, nadzor in vodenje prometa (v teh časih, ko imajo nekatera vozila možnost avtopilota, lahko heker vdre v sistem vozila in prevzame nadzor nad njim).

2.3 Od hekerja do kibernetskega terorista

Nekateri hekerji izvajajo kibernetske napade za zabavo, drugi za plačilo in tretji v imenu maščevanja. Veliko se jih tudi poveže v organizirane skupine. Če je hekerjev več, naredijo več škode in težje jih je ustaviti.

Kibernetski teroristi so hekerji, ki imajo politično motivacijo, so politično skorumpirani, uničijo infrastrukturo ali pa hočejo uničiti politične delavce. To pogosto naredijo, da ustvarijo strah in da dokažejo, da tehnologija ni varna. Če gre za večji napad, morajo imeti tudi zelo dobro opremo ter ustrezne programe, skripte – kode, ki naredijo veliko škodo. Nekateri hekerji zapravijo zelo veliko časa, da naredijo svoj program, skripto, da so bolj učinkoviti pri škodovanju določeni tarči.

Slika 2: Simbolična slika kibernetskega terorista

2.4 Vrste kibernetskih napadov

2.4.1 DoS

Napad za zavrnitev storitve (DoS) je napad, ki ima namen, da zaustavi omrežje oziroma napravo in ga/jo tako naredi nedosegljivo uporabnikom. DoS napadi to dosežejo tako, da ciljno napravo preobremenijo s prometom ali pa tako, da ji pošljejo informacije, ki sprožijo zrušitev.

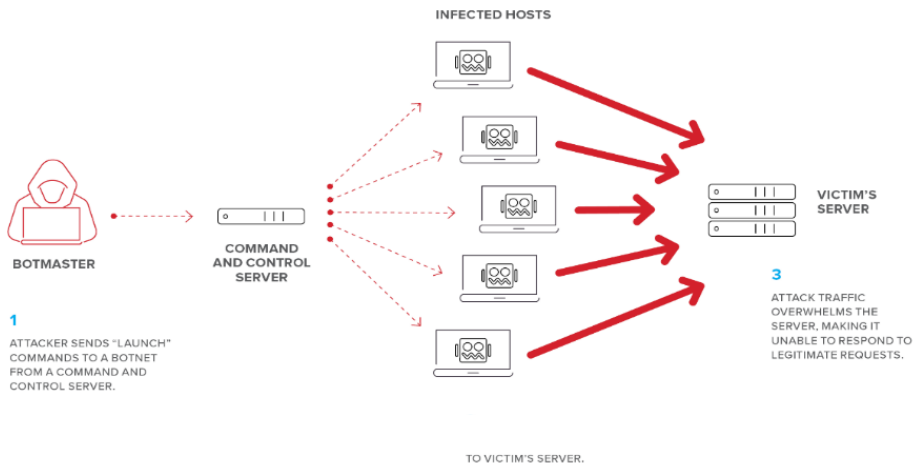
2.4.2 DDoS

Kratica DDoS izhaja iz angleške zloženke Distributed Denial of Service. Pri DDoS napadu gre za množično dostopanje do strežnika z namenom njegove preobremenitve in s tem do nedostopnosti spletnih strani, ki na njem gostujejo. DDoS napade izvajajo spletni napadalci, razlogi za takšna dejanja pa so različni:

- izsiljevanje lastnikov napadenih strani,
- povzročanje škode konkurenčnim podjetjem,
- dokazovanje moči samim sebi.

Kako torej sploh izgleda DDoS napad v praksi? Predstavljajte si, da gre za spletno stran banke. Ta gostuje na strežniku, ki omogoča, da se na strani banki izvede 30 poizvedb (npr. 30 klikov na katerokoli povezavo) v eni sekundi. Če bi bilo v eni sekundi opravljenih več poizvedb, bi prišlo do preobremenjenosti strežnika, spletna stran pa bi začela delovati počasi. V primeru še večje obremenjenosti bi prenehala delovati.

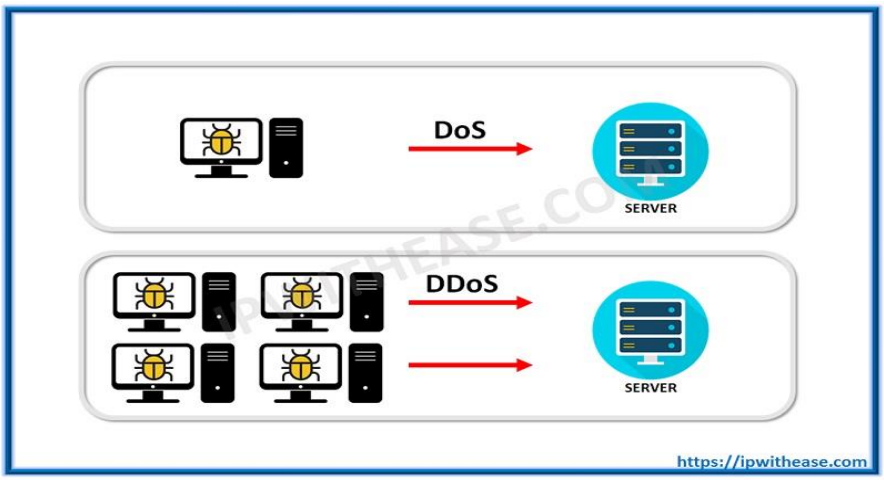
Cilj hekerjev, ki izvajajo DDoS napad, je ravno v tem – da »sesujejo« strežnik in lastniku spletne strani, ki na njem gostuje, onemogočijo delovanje strani.



Slika 3: Model DDos napada

2.4.3 Kaj je razlika med DDoS in DoS?

Pri napadu DoS je uporabljen samo en računalnik za zrušitev sistema. Pri DDoS pa je uporabljenih več sistemov, ki imajo za tarčo samo en sistem. Če uporabnik uporabi DoS napad, ga je lažje ustaviti, ker nezakoniti promet pošilja samo en vir. DDoS napad pa je težje ustaviti in izolirati, saj je tako velika razširjenost sistemov težko zaznavna.



Slika 4: Primerjava DDos in Dos napada

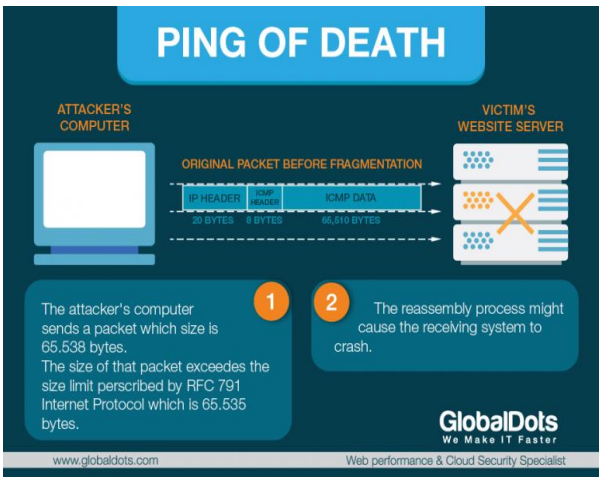
2.4.4 Phishing

"Phishing" je spletna prevara, pri kateri goljuf želi pridobiti občutljive podatke spletnih uporabnikov. Izraz "phishing" je vse bolj poznan po celem svetu. "Phishing" napad največkrat poteka tako, da oseba na elektronski naslov prejme e-sporočilo, katerega pošiljatelj naj bi bila spletna banka, pri kateri ima oseba urejeno spletno bančništvo. Goljuf, ki se torej predstavlja v imenu spletne banke, želi prejemnika e-sporočila prepričati, da mora nujno in čim hitreje posredovati uporabniško ime ter geslo za prijavo, saj naj bi prihajalo do nepooblaščenih vstopov. Posredovanje uporabniškega imena in gesla naj bi bilo nujno, saj mora »spletna banka« čim hitreje nastaviti novo geslo. Razlog za hitro ukrepanje je lahko tudi drugačen.

Slika 5: Karikatura phishing napadalca

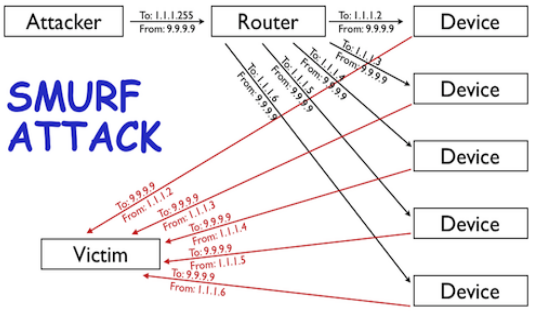
2.4.5 Vrste DoS ter DDoS napadov

"**Ping of Death**" je najosnovnejši način DoS napada. Ukaz "ping" je po navadi uporabljen za testiranje dostopnosti omrežja, deluje pa tako, da pošilja majhne podatkovne pakete. Pri "ping of death" napadu napadalec izkoristi to v svojo korist, tako da na ciljni strežnik pošlje pakete, ki presegajo maksimalno dovoljeno velikost, ki jo protokol "TCP/IP" dovoli. Ker je velikost paketov prevelika "TCP/IP" fragmentira te pakete oziroma jih razdeli na manjše dele in jih pošlje na ciljni strežnik, in ker ta teh paketov, zaradi omejene zmogljivosti, ne more sprejeti, se poruši.



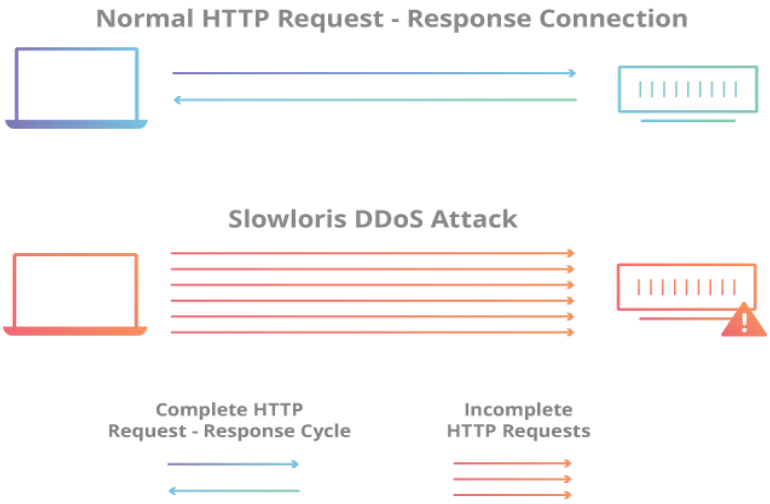
Slika 6: Predstavitev "ping of death" napada

"**Smurf attack**" je napad na računalniško omrežje, ki ga uvrščamo med "DDoS" napad. Ta vrsta napada povzroči visok računalniški omrežni promet, kar posledično privede do neodzivnosti strežnikov oz. do slabšega delovanja. Ime (Smrkci) je napad dobil zaradi način delovanja – množica majhnih napadalcev premaga veliko večjega nasprotnika. Pri napadu uporabi "Internet Control Message Protocol". To je protokol, ki ga uporabljajo omrežni računalniki za pošiljanje sporočil o napakah ter informacijah o storitvah in računalniku. Napad deluje tako, da se z zlonamernim programom "Smurf" ustvari prikrit paket (tako imenovan "Spoofed packet"), v katerem je določen povratni naslov tarče. Paket se naslovi na različne naslove v omrežju, ti pa pošljejo odgovor na zahtevo na v paketu določen naslov, kar povzroči preobremenjenost tarče oziroma strežnika.



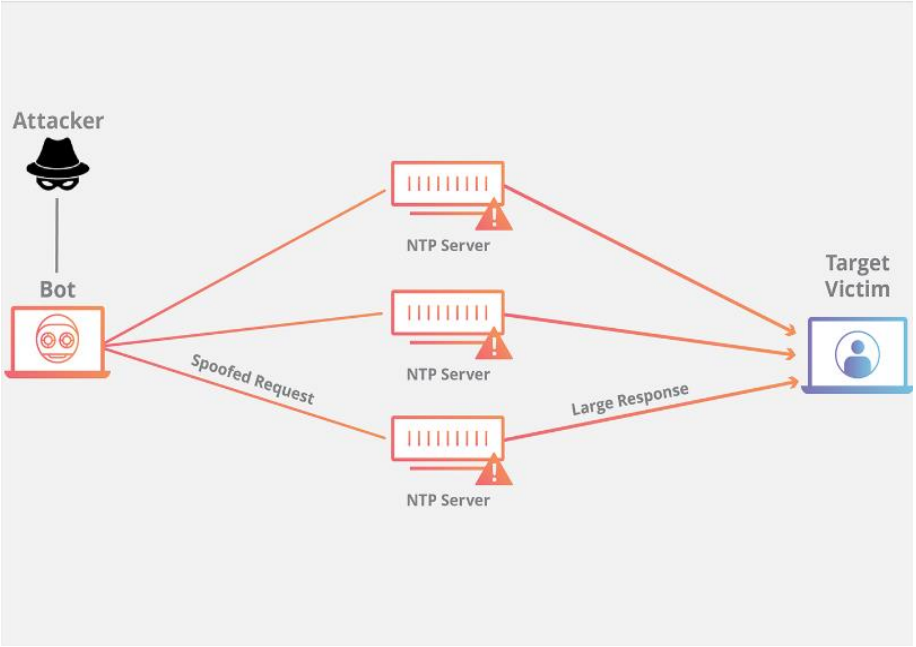
Slika 7: Predstavitev smurf napada

"**Slowloris**" je napad "http Denial of Service", ki vpliva na strežnike. Napadalec začne oddajati veliko HTTP zahtev. Zahteve, da pustijo odprte povezave, pošiljajo vsakih 15 sekund. Teh povezav nikoli ne zaprejo, razen če to stori strežnik. Če strežnik zapre povezavo, ustvarijo novo in še naprej delajo isto. Če povezava traja predolgo, bo strežnik učinkovit, če bo čezmerno dolga povezava potekla, sprosti nit za naslednjo zahtevo. Da se to ne bi zgodilo, napadalec občasno pošlje delne zahteve cilju, da ohrani zahtevo pri življenju. Torej v bistvu: "Še vedno sem tukaj, sem zelo počasen ter prosim, da me počakate." To izčrpa strežnikovo moč in strežnik ne more odgovarjati drugim uporabnikom. "Slowloris" ni kategorija napadov, temveč je posebno orodje, ki je narejeno tako, da upočasni strežnik, ne da bi uporabilo veliko pasovno širino. Program je dobil ime po lorijih, živalih, ki so predvsem znane po počasnem gibanju.



Slika 8: Slowloris napad

"**NTP Amplification**" je tip napada "DDoS", pri katerem napadalec izkorišča javno nastopne strežnike "Network Time Protocol (NTP) ", da preobremeni ciljni promet s protokolom UDP ("User Datagram Protocol"), zaradi česar so cilj in njegova okoliška infrastruktura nedostopni za redni promet. Vsi ojačevalni napadi izkoriščajo razlike v pasovni širini med napadalcem in ciljnim spletnim virom. Ko se razlike v stroških povečajo pri številnih zahtevah, lahko nastali obseg prometa moti omrežno infrastrukturo. S pošiljanjem majhnih poizvedb, ki povzročajo velike odzive, lahko napadalec od manj dobi več. Ko pomnožite to povečavo tako, da vsak bot v botni mreži poda podobne zahteve, je napadalec prikrit in izkoristi prednosti močno povečanega napada.



Slika 9: Predstavitev NTP Amplification napada

2.5 Kaj pomeni biti "sposoben heker"?

Sposoben heker je oseba, ki ima zelo dobro znanje o računalnikih, računalniških omrežjih ter računalniških programih. Izvedel je že veliko kibernetskih napadov in bil pri njih tudi zelo uspešen. Posamezniki, ki so sposobni hekerji, imajo lahko dobre ali pa slabe namene. Njihovo število narašča iz dneva v dan.

Poznamo različne vrste s hekerjev:

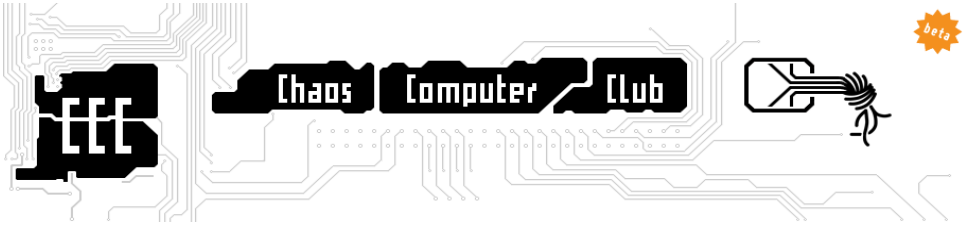
- **"Black Hat Hacker"** – heker, ki poskuša vdreti v računalniške sisteme. Njihov namen je da uničijo računalniške podatke, ukradejo gesla, imena strank ter njihove naslove. To velikokrat počnejo predvsem zaradi dobička ali pa osebnega maščevanja
- **"White Hat Hacker"**– nekdo, ki se spozna na kibernetsko varnost in poskuša vdreti v računalniške sisteme. Pogosto jih imenujejo tudi »dobri hekerji«, ker jih zasebna podjetja ali vladne organizacije najemajo, da preizkusijo svojo kibernetsko varnost.
- **"Grey Hat Hacker"**– heker, ki krši zakone ali pa tipične etične standarde, ampak nima zlonamernega namena. To počnejo predvsem za zabavo, eksperimentiranje ali pa iščejo "luknjo" v sistemu.
- **"Script Kiddies"**– amaterski heker, ki poizkuša vdreti v računalniške sisteme s skriptami drugih hekerjev. Po navadi poizkušajo vdreti v spletne strani, računalniške sisteme ali omrežja. Imajo malo znanja o procesu »hekanja«.
- **"Green Hat Hackers"** – heker, ki je podoben "Script Kiddies". To so začetni hekerji, ki so šele začeli s s hekersimi aktivnostmi in nimajo veliko znanja.
- **"Red Hat Hackers"** – heker, ki poizkuša zaščiti računalniške sisteme pred napadalci. Namesto da bi prijavili kibernetske napade odgovornim, jih poizkušajo ustaviti sami. Pogosto poizkušajo namestiti računalniški virus ali pa izvesti DDoS napad na napadalce, da bi zaustavili napade.
- **"Hacktivist"** – aktivistični hekerji, ki poizkušajo vdreti v vladne spletne strani ali pa njihove računalniške sisteme. Pogosto delujejo v skupinah. Računalniške podatke, ki jih pridobijo z vdorom, uporabijo za osebno politično ali družbeno korist.

2.6 Znane hekerske skupine

Anonymous so mednarodna skupina aktivistov, ki so postali znani zaradi DDoS napadov na vladne, verske in druge podjetniške spletne strani. Odgovorni so za številne potegavščine, napade, proteste in javna obrekovanja. Večina sveta jih prepozna po njihovih značilnih maskah.

Slika 10: Objavljena slika hekerske skupine »Anonymous«

Chaos Computer Club (CCC) je največja evropska organizacija hekerjev. Aktivni so že več kot 30 let. Kot najvplivnejši hekerski kolektiv organizirajo kampanjo prireditve, objave ter storitve anonimizacije in komunikacijske infrastrukture. V Nemčiji in njeni okolici je veliko hekerskih prostorov, ki pripadajo CCC-ju.

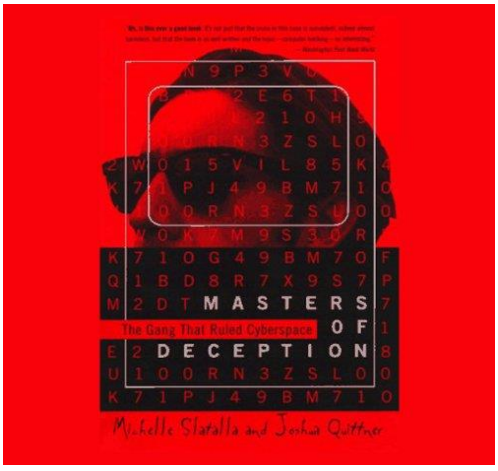


Slika 11: Logo CCC skupine

Lizard Squad je hekerska skupina, ki je predvsem znana zaradi svojih DDoS napadov na socialna omrežja (Instagram, Facebook, Tinder ter HipChat), znani so pa tudi zaradi DDoS napadov na različne računalniške igre, kot so League of Legends ter Destiny, izvedli so tudi napad na Xbox Live ter PlayStation network. Eden največjih napadov pa je bil izveden na severnokorejski internet, ki je bil zaradi napada neaktiven 1 dan.

Slika 12: Logo Lizard Squad skupine

Masters of Deception so bili znana hekerska skupina. Nahajali naj bi se v New Yorku. Predvsem so bili znani po izkoriščanju telefonskih in komunikacijskih podjetij. Ko so napadali telefonska podjetja, je FBI aretiral veliko njihovih članov. Prvotno članstvo je naraslo na sestankih na testnih linijah Loop-Around, ki so privedli do sodelovanja pri vdoru telefonskih stikal RBOC ter različnih miniračunalnikov in glavnih računalnikov, ki se uporabljajo za upravljanje telefonskega omrežja.



Slika 13: Logo Masters of Deception skupine

Legion of Doom je bila hekerska skupina od približno 1980 do okoli leta 2000. Ustanovil jo je heker Lex Luthor, znan je tudi kot Raavan. Najbolj so bili aktivni od leta 1984 do 1991. V tistem času je bila ta hekerska skupina po mnenju mnogih ljudi najbolj sposobna hekerska skupina. Veliko članov skupine je odšlo, nekateri so izgubili interes, drugi so se odločili, da bodo odšli na kolidž. Zaradi tega je potem skupina tudi razpadla.

Slika 14: Logo Legion of Doom skupine

2.7 Zgodovina znanih kibernetskih napadov

1995 – radijska postaja LA KIIS FM je ponujala avto Porsche tistemu, ki bi bil 102. klicatelj. Kevin Poulsen si je zagotovil uspeh tako, da je prevzel nadzor nad telefonskim omrežjem in učinkovito blokiral dohodne klice na številko radijske postaje.

1999 – vdor v NASO ter US Defense Department. 15-letni deček je vdrl v računalnike US Defense Department ter naložil "backdoor" na njihove strežnike. Zaradi tega je lahko prestregel veliko e-sporočil različnih vladnih organizacij. Informacije, ki jih je pridobil, so mu kasneje omogočile, da je lahko ukradel kos Nasine programske opreme. »…James was able to steal a piece of NASA software which cost the space exploration agency $41,000... «(ARN Staff, 2021, https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/)

Januar 2008 – najstnik iz New Jerseya s skupino hekerjev izvede DDoS napad na spletno stran Church of Scientology. Spletna stran je bila več dni pod DDoS napadom. Napadalci so bili del skupine Anonymous in odločno nasprotujejo veri, ki jo prikazujejo na spletni strani Church of Scientology.

Januar 2009 – napad na vladne spletne strani v Izraelu. Hekerji so napadli izraelsko interno infrastrukturo med vojaško ofenzivo v Gazi. Ta napad je izvedlo vsaj 5 milijonov računalnikov.

April 2011 – Sony's PlayStation Network je bil tarča kibernetskih napadov. Storitve za več igralcev, ki igrajo skupaj, internetno nakupovanje ter vsebine v živo so bile onemogočene za uporabnike Sony's PlayStation Network. Uspelo jim je dobiti tudi dostop do več kot 77 milijonov uporabniških računov.

2012 – socialno omrežje LinkedIn je obvestilo svoje uporabnike, da je bilo 6,5 milijonov gesel ukradenih ter objavljenih na ruskem forumu. Vendar je bil šele leta 2016 razkrit celoten obseg incidenta. Napadalec je prodajal e-mail naslov ter gesla LinkedInovih uporabnikov za 5 bitcoinov, ki so bili takrat vredni okoli 2000 $.

Oktober 2013 – Adobe obvesti javnost, da so hekerji ukradli ter pridobili dosstop do več kot 38 milijonov računov od aktivnih uporabnikov. Razkrili so tudi imena strank, osebnih izkaznic, gesla ter podatke o debetnih in kreditnih karticah. Adobe je moral uporabnikom plačati okoli 1 milijon dolarjev zaradi razkritih informacij. »…the hackers took advantage of a security breach at the publisher... « (Outpost24, 2018, https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks)

2014 – leta 2016 Yahoo obvesti svoje uporabnike, da so bili tarča kibernetskih napadov leta 2014. Napadalci so imeli podatke o več kot 500 milijonih uporabnikov.

Januar 2014 – prebivalci Južne Koreje so dobili informacijo, da so v prejšnjih letih ukradli več kot 100 milijonov informacij o njihovih kreditnih karticah. Zaradi tega so neznanci vdrli v več kot 20 milijonov bančnih računov. Ugotovili so, da je bil krivec uslužbenec KCB-ja (Korea Credit Bureau).

Maj 2014 – kibernetski napad na spletno trgovino eBay. Napadalci so dobili informacije o več kot 145 milijonih uporabniških računov (njihova imena, gesla, naslove, datume rojstva). Finančnih informacij, kot so informacije o kreditnih karticah, na srečo niso dobili.

December 2018 – napadalci so ukradli informacije o uporabnikih newyorškega podjetja, ki se ukvarja s storitvami za sporočanje sporočil, imenovanega Dubsmash. Te podatke so nato napadalci začeli prodajati na temnem spletu Dream Market. Dubsmash je priznal, da je prišlo do vdora ter prodaje informacij, ter svetoval glede spremembe gesel. Vendar niso povedali, kako so napadalci vstopili v sistemi, niti potrdili, koliko uporabnikov je bilo prizadetih.

Maj 2019 – avstralsko grafično orodje za spletne strani Canva utrpi kibernetski napad, ki je razkril 137 milijonov uporabnikov (uporabniška imena, e-mail, naslov bivanja …). Podjetje Canva je dalo izjavo, da so hekerji uspeli videti informacije uporabnikov, niso pa jih mogli naložiti oz. ukrasti.

3. Raziskovalni del

3.1 Metode dela

Metode dela, ki sva jih uporabila pri raziskavi, so:

- Zbiranje gradiva za teoretični del naloge, ki sva ga iskala na spletu.
- Sestava ankete: ankete ni bilo težko sestaviti, saj sva jo sestavila na spletni strani 1ka.si. Ta omogoča lahkotno sestavljanje in deljenje ankete. Anketa je bila sestavljena iz 10 vprašanj. Da bi jo anketiranci lažje razumeli in rešili, sva jo sestavila tako, da so anketiranci večinoma izbirali med opcijami, ki so jim bile vnaprej podane.
- Anketiranje: Anketo sva poslala najinim sošolcem in znancem. Imela sva 282 klikov na anketo. Od teh klikov je bilo 101 vnosov, ki so bili ustrezni (vsa vprašanja so odgovorjena in na koncu klikneš konec). Skupaj je bilo 181 neustreznih vnosov.

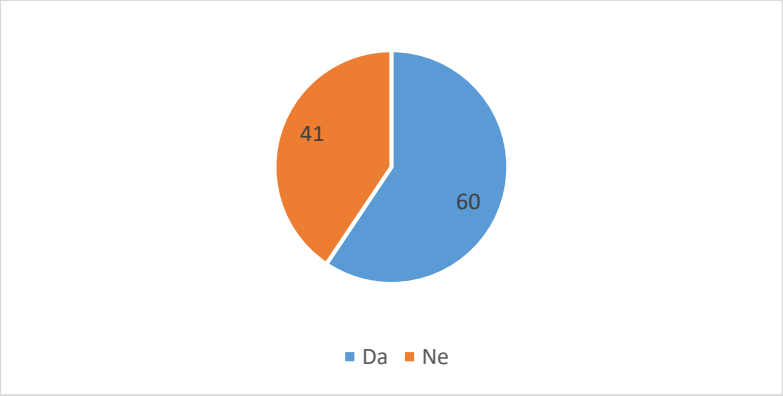
Tabela 1: Stopnja napredovanja anketirancev

Kumulativni status	Frekvenca	Stopnja
Klik na nagovor	282	100%
Klik na anketo	118	42%
Začel izpolnjevati	103	37%
Delno izpolnjena	101	36%
Končal anketo	92	33%

- Obdelava podatkov: Ko sva zbrala vse podatke iz ankete, sva uporabila tabele, ki jih ponuja 1ka.si, ter jih pretvorila v grafe, ki sva jih naredila v excelu.
- Pisanje naloge: najprej sva se poglobila v kibernetske napade, da bi jih bolje razumela, nato sva napisala teoretični del naloge. Zatem sva pripravila anketo in hipoteze. Po izvedbi ankete sva napisala obdelavo ankete in potrdila ali zavrgla najine hipoteze.

3.2 Rezultati

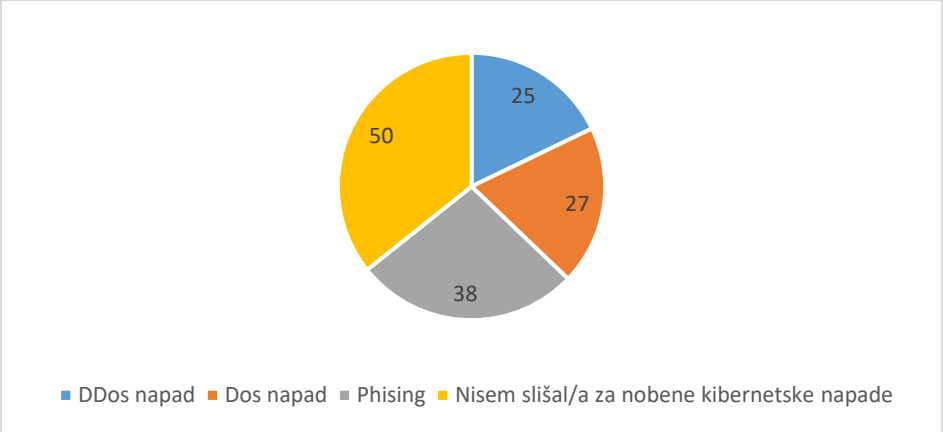
1. Si seznanjen/a s kibernetskimi napadi?



Graf 1: Si seznanjen/a s kibernetskimi napadi?

Iz grafa je razvidno, da je večina anketirancev (60) seznanjena s kibernetskimi napadi.

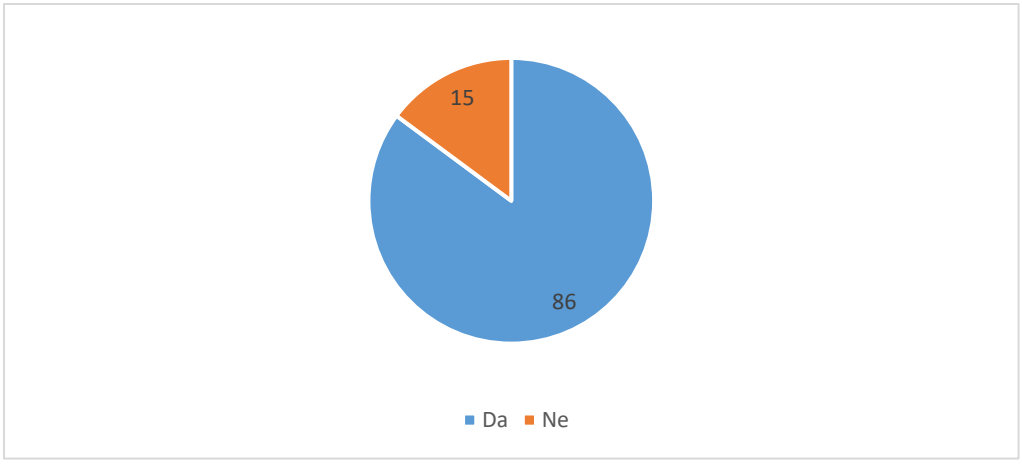
2. Za katere od teh kibernetskih napadov si že slišal/a?



Graf 2: Za katere od teh kibernetskih napadov si že slišal/a?

Iz grafa je razvidno, da večina anketirancev ni slišala za omenjene kibernetske napade. Največ je tistih, ki so slišali za phising.

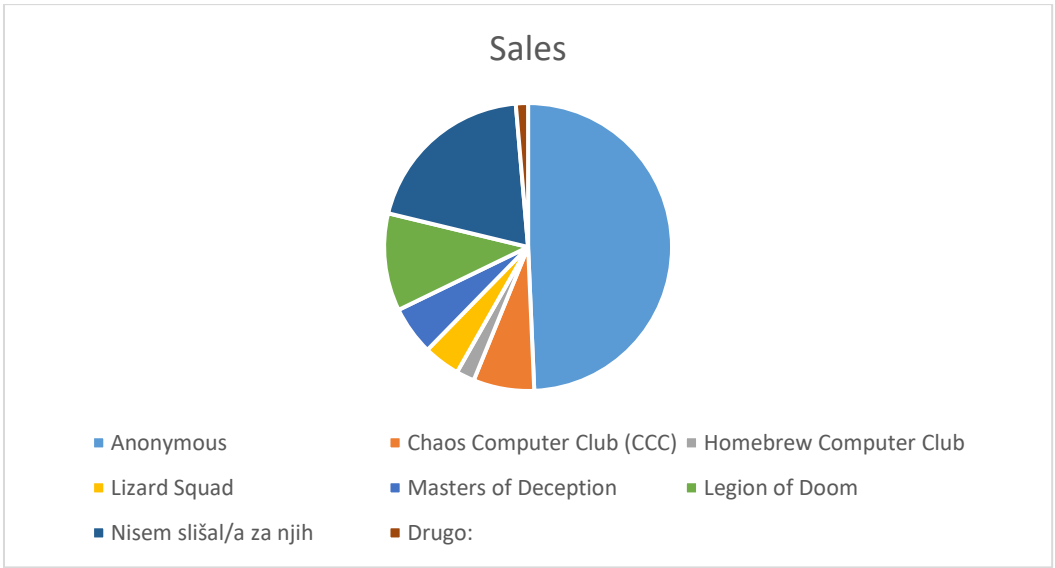
3. Si že slišal/a za organizirane hekerske skupine?



Graf 3: Si že slišal/a za organizirane hekerske skupine?

Večina anketirancev (86, kar pomeni 85%) je že slišala za kibernetske napade.

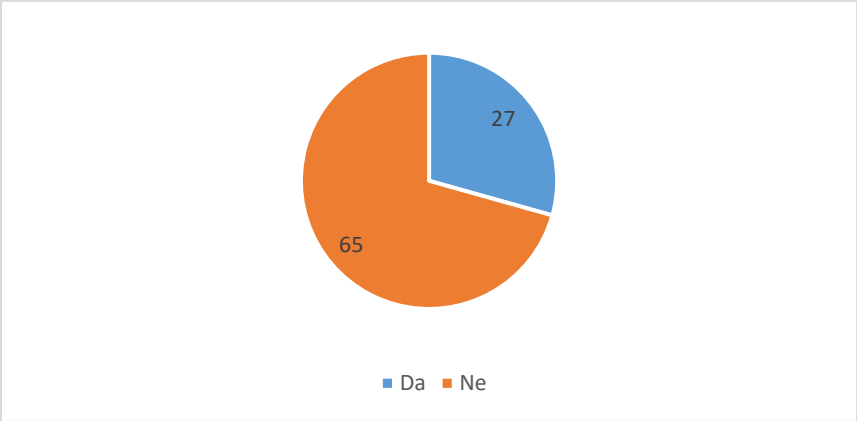
4. Če ja, katere od teh hekerskih skupin poznaš?



Graf 4: Če ja, katere od teh hekerskih skupin poznaš?

Kot je razvidno iz tabele, je 49 % anketirancev že slišalo za najbolj znano hekersko skupino Anonymous. 20 % anketirancev ni slišalo za nobeno od teh večjih hekerskih skupin. 2 anketiranca pa sta navedla skupino Beefgang.

5. Si že slišal/a za kakšne kibernetske napade v Sloveniji?



Graf 5: Si že slišal/a za kakšne kibernetske napade v Sloveniji?

Kot vidimo iz grafa, približno 2/3 anketirancev ni slišalo za kakršne koli kibernetske napade v Sloveniji.

6. Če ja, za kateri kibernetski napad v Sloveniji si slišal/a?

a) Nisem slišal/a za njih: 65

b) Odgovor: 22

- napad na strežnike javne uprave
- ko so napadli lekarne v Ljubljani (anketiranci so navedli več podobnih odgovor za omenjene napade)
- izsiljevali virus ryuk okuži postaje na omrežju lekarn Ljubljana
- na spletno učilnico od osnovnošolcev
- banka, trgovska veriga, podjetje....
- na pravno firmo v Kopru
- če se ne motim, so nekoč napadli na Revoz ali kakor koli se že imenuje Renaultova tovarna
- vdiranje v podatke uporabnikov bank, motnje v delovanju knjižnic, lekarn itd.
- hekanje bitcoinov
- tisto z bitcoini
- ko so novi24tv ukradli bazo al neki, bitcoin pa neki z arnesom. neki je baje tudi bilo na gimnaziji Vič
- povezan z vlado
- napad na banke: NLB, SKB…

Ob tem vprašanju so anketiranci sami napisali, za katere kibernetske napade v Sloveniji so slišali. Najpogostejši odgovor je bil napad na Ljubljanske lekarne in kraja bitcoinov.

7. Kateri je največji kibernetski napad, za katerega si slišal/a?

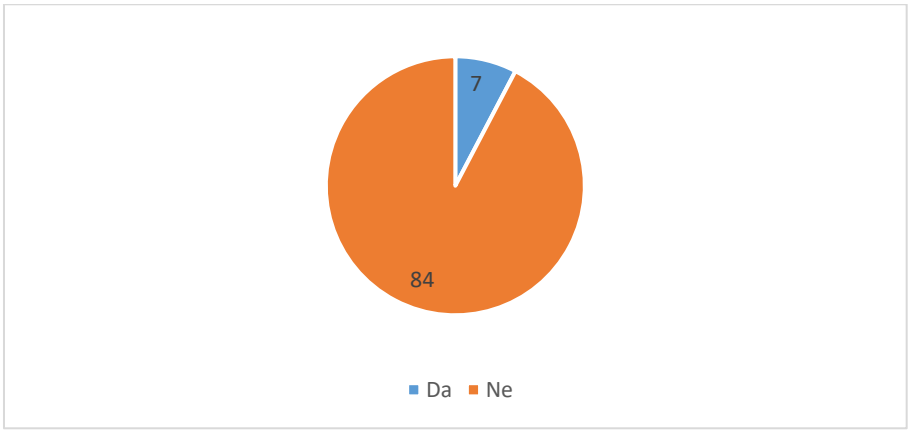
a) Nisem slišal za večje kibernetske napade: 59

b) Odgovor: 24

- wannacry ransomware attack
- kibernetski napad v Revozu
- za lekarne Ljubljana
- napad na Ljubljanske lekarne
- wikileks
- anonymous na zda
- napad na arnes
- napad na adobe
- ko so ukradli bitcoine neki firmi
- napad v indiji
- udor rusov v ameriški sistem
- new york centralna banka
- napad na isis
- melissa virus
- trojan horse
- ddos
- 500px
- Google
- amazon
- anonim. na fra
- vdor v pentagon
- amerika-nastavitve vodovoda v mestu

Ob tem vprašanju so anketiranci sami napisali, kateri je bil največji kibernetski napad, za katerega so slišali. Večina odgovorov se nanaša na napade v Ameriki in na velika podjetja. Zelo malo ljudi je slišalo za kakšne večje kibernetske napade.

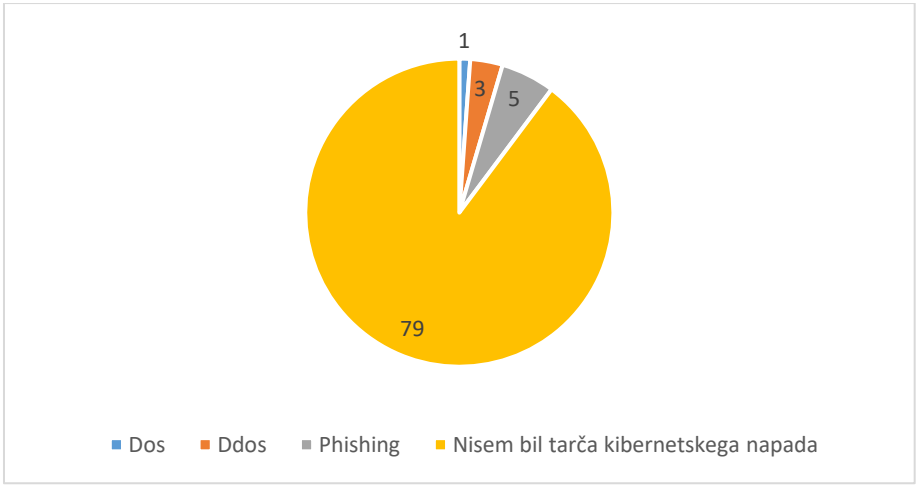
8. Si bil kdaj tarča kibernetskega napada?



Graf 6: Si bil kdaj tarča kibernetskega napada?

Iz grafa je razvidno, da 92 % anketirancev (84 oseb) ni nikoli bilo tarča kibernetskega napada.

9. Če ja, tarča kakšnega napada si bil?



Graf 7: Če ja, tarča kakšnega napada si bil?

Iz grafa je vidno, da večina anketirancev ni bila tarča kibernetskega napada. Najpogostejši napad pri tistih, ki so bili tarča, je bil phising.

10. Kaj bi naredil/a, če bi bil/a tarča kibernetskega napada?

53 anketirancev je odgovorilo na to vprašanje, preostalih 48 pa ni podalo odgovora. V nadaljevanju, spodaj, so navedeni odgovori:

- zaprl vse račune z vrednostjo
- idk (I do not know)...izbrisal verjetno svoj račun
- počakal, da mine... morda zaprl kak port ali ugasnil strežnik
- kontaktiral policijo, torej prijavil zadevo
- obvestil policijo ali banko.
- obvestila policijo, oddelek za varnost na spletu
- prijavil pristojnim organom
- obrnem se na ustrezne institucije
- obvestil pristojne organe
- odstranil profil/aplikacijo/napravo, ki je bila tarča napada
- ugasnila bi računalnik in poiskala pomoč strokovnjakov
- prvo obvestila starše, kasneje učitelja za računalništvu itd.
- poizkusil bi se obraniti, sicer bi poklical pomoč
- poiskal pomoč pri strokovnjakih
- najbrž bi se obrnila na ljudi, ki so bolj spoznajo na tehnologijo, kot se spoznam jaz.
- poiskala bi pomoč, ker o kibernetskih napadih ne vem nič, torej ne vem niti kako ukrepati, če se ti to zgodi
- obrnila bi se na računalniški servis
- uporaba protivirusnih programov, pazljivost pri nalaganju programske opreme, prijava incidenta
- znam se jih znebit
- verjetno vprašal google kako rešil problem
- 11X: ne vem
- ne vem, ker ne vem, kako to izgleda
- če bi bil tarča phishinga, bi probala spremeniti podatke, ki so jih dobili,, oz. bi npr. sporočila na banko in bi oni probali zmanjšati škodo. pri dos in ddos napadih bi uporabila različne taktike, ki jih preprečujejo. npr. Captcha
- nič
- depresija
- izboljšal bi zaščito omrežja.
- obnovil bi svoje podatke iz backupa
- panika

Najpogostejši odgovori so bili:

- Ne vem,
- poiskal/a bi organizacijo, ki bi mi lahko pomagala,
- obnovil/a bi podatke iz backupa,
- zamenjal/a bi gesla svojih računov,
- poklical/a bi policijo.

Iz teh rezultatov je razvidno, da veliko ljudi ne ve, kaj storiti v primeru, če bi se njim zgodil napad. Nekateri bi se obrnili na policijo oziroma ustrezno institucijo.

4. Razprava

Najina prva hipoteza je bila to, da bo večina ljudi vedela, kaj so kibernetski napadi. To hipotezo lahko potrdiva, ker je 60 % anketirancev vedelo, kaj so kibernetski napadi. A še vedno so naju rezultati presenetili, saj sva pričakovala, da bo večji del anketirancev vedel, kaj so.

Najina druga hipoteza je bila, da bo večina anketirancev že slišala za vsaj phishing napad. To hipotezo ovrževa, saj 50 % anketirancev ni slišalo za nobeno vrsto kibernetskega napada. To naju je presenetilo, ker sva mislila, da bodo anketiranci bolj razgledani v področju računalništva in kibernetskih napadov.

Najina tretja hipoteza je bila, da je vsaj polovica anketirancev slišala za organizirane hekerske skupine. To hipotezo lahko potrdiva, saj je kar 85 % anketirancev že slišalo za organizirane hekerske skupine.

Najina četrta hipoteza je bila, da je vsaj polovica anketirancev slišala za kakšen kibernetski napad v Sloveniji. To hipotezo ovrževa, ker 64 % anketirancev ni slišalo za noben kibernetski napad v Sloveniji. To naju spet preseneča, ker se o večjih kibernetskih napadih velikokrat poroča na televiziji.

Najina peta hipoteza je bila, da je vsaj ¾ anketirancev bilo tarča kibernetskega napada. To hipotezo spet ovrževa, saj je bilo le 8 % anketirancev kdaj tarča kibernetskega napada. To naju je spet presenetilo, ker so phising napadi zelo pogosti (spam mail).

5. Zaključek

V tej raziskovalni nalogi sva obravnavala, kaj so kibernetski napadi, kaj so kibernetski teroristi, različne kibernetske napade, največje organizirane hekerske organizacije in zgodovino večjih in bolj znanih kibernetskih napadov.

Sestavila sva anketo z desetimi vprašanji. Imela sva 282 klikov na anketo. Od teh klikov je bilo 101 vnosov, ki so bili ustrezni (vsa vprašanja so bila odgovorjena in na koncu anketa zaključena z gumbom »Konec«). Skupaj je bilo 181 neustreznih vnosov. Meniva, da je zaskrbljujoče, da se skoraj 41% anketiranih ne zaveda nevarnosti kibernetskih napadov, saj lahko posamezniku ali podjetju ali vladi povzročijo zelo veliko nevšečnosti. Poleg tega je anketa pokazala, da polovico anketiranih ne pozna primera kibernetskega napada, čeprav se ti dogajajo vsako leto, v času epidemije korona virusa, ko se je naše življenje preselilo na splet, pa je teh primerov še več. Predlagava, da bi državne institucije, odgovorne za spletno varnost, objavljale obvestila za posameznika, ki so morda preveč zaupljivi. Morda bi tako preventivno poskrbeli za večjo kibernetsko varnost. Je pa razveseljivo, da anketiranci poznajo phising napad. Če veš, da

obstaja, se tako lažje varuješ pred njim. Najbolj poznan napad v Sloveniji je bil napad na sistem, ki so ga uporabljale Ljubljanske lekarne. Anketirani poznajo tudi napade na banke, na bitcoin, na ameriške sisteme. Anketirancem najbolj poznana organizirana hekerska skupina je Anonymous. Hkrati pa ni vzpodbudno, da 20% anketiranih še ne pozna nobene hekerske skupine. Zanimivi in zelo raznoliki so bili odgovori, kako bi anketiranci ravnali v primeru, če bi bili sami tarča kibernetskega napada. Odgovori so se vrstili od tega, da bi takoj zaprli računalnik ali prijavili pristojnim organom, tudi policiji, poiskali pomoč strokovnjaka ali pa bi jih zgrabila panika in depresija, ne bi storili nič, saj se jim zdi, da hekerskega napada sploh ne bi prepoznali ali zaznali.
Ko primerjava rezultat, da 50% anketirancev ni slišalo za kibernetski napad kjerkoli, 65% pa jih ne ve, da so kibernetski napadi prisotni tudi v Sloveniji, lahko iz razlike sklepava, da se 15% anketiranih v Sloveniji počuti bolj varne, kot drugje. Vemo pa, da je splet globaliziran in ne pozna meja ali jezika.

Ker je iz rezultatov ankete razvidno, da veliko ljudi ne ve, kaj storiti v primeru, če bi se njim zgodil napad, sva mnenja, da bi morali različni mediji več časa posvetiti obveščanju in ozaveščanju ljudi, tudi nas mladih, da bi se tako morda zaradi osveščenosti posameznika presenečenja različnih hekerjev morda zmanjšala. Prav tako bi moral za varnost na spletu poskrbeti tudi vsak posameznik z uporabo varnih gesel in ustreznih programov.

Zato nas lahko skrbi, da anketiranci niso vedeli, kaj bi naredili v primeru, da bi bili sami tarča kibernetskega napada.
Če bi anketo sestavljala še enkrat, bi vključila tudi vprašanja o starosti in spolu, ki bi lahko prikazala razlike v obnašanju med mlajšo in starejšo generacijo.

6. Viri

SI-cert/dostopno 10. 1. 2021/ https://www.cert.si/o-nas/zgodovina-spletnih-incidentov-v-sloveniji/ /spletni vir

Tom/dostopno 10. 1. 2021/ https://svetracunalnistva.si/kaj-je-phishing /spletni vir

Uroš Čimžar/dostopno 10. 1. 2021/ https://www.domovanje.com/blog/2017/10/06/kaj-je-ddos-napad-kako-se-ga-lahko-ubranimo/ /spletni vir

Infocyte/dostopno 5. 1. 2021 / https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ /spletni vir

Caleb Townsend/dostopno 20. 12. 2020/ https://www.uscybersecurity.net/infamous-hacking-groups/ /spletni vir

CCC/dostopno 20. 12. 2020/ https://www.ccc.de/en/ /spletni vir

Varun Kumar/dostopno 15. 12. 2020/ https://www.rankred.com/famous-hacker-groups/ /spletni vir

Rashimi Bhardwaj/ dostopno 7. 12. 2020/ https://ipwithease.com/dos-vs-ddos/ /spletni vir

Gokkberk Yaltirakli/dostopno 7. 12. 2020/ https://github.com/gkbrk/slowloris /spletni vir

Cloudflare/dostopno 15. 1. 2021/https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ /spletni vir

Imperva/dostopno 7. 12. 2020/ https://www.imperva.com/learn/ddos/ntp-amplification/ /spletni vir

Cloudflare/dostopno 27. 1. 2021/ https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/ /spletni vir

Wikipedia/dostopno 23. 2. 2021/ https://en.wikipedia.org/wiki/Lizard_Squad /spletni vir

Graham Cluley /dostopno 15. 1. 2020/https://www.welivesecurity.com/2018/03/29/lizard-squad-member-jailed/ spletni vir

Wikipedia/dostopno 23. 2. 2021/ https://en.wikipedia.org/wiki/Masters_of_Deception /spletni vir

7.Viri slik

Barnes, Sam. 2017. What's being done to combat cyber threats targeting the petrochemical, oil and gas industries? . 1012industryreport [online]. Feb. [Citirano 1. feb 2021 10:30], Dostopno na spletnem naslovu: https://www.1012industryreport.com/safety/malware-targeting-petrochemical-oil-gas-industries-whats-done-combat-risk/

Campion, Alice. 2019. Identity fraud: How to protect yourself . Confused [online]. Feb. [Citirano 1. feb 2021 10:30], Dostopno na spletnem naslovu: https://www.confused.com/car-insurance/guides/how-to-prevent-identity-fraud

Walkowski, Debbie. 2019. What Is a Distributed Denial-of-Service Attack? : The Role of Botnets in DDoS Attacks. F5 labs[online]. Feb. [Citirano 1. feb 2021 10:35], Dostopno na spletnem naslovu: https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-

Campion, Rashmi. DOS vs DDOS- What is DOS and DDOS Attack?. [online].Ipwithease Feb. [Citirano 2. feb 2021 9:08], Dostopno na spletnem naslovu: https://ipwithease.com/dos-vs-ddos/

Salvatore, Stolfo. 2020. Protecting Students and Faculty from University Phishing Attacks. My tech decision [online]. Feb. [Citirano 2. feb 2021 9:09], Dostopno na spletnem naslovu: https://mytechdecisions.com/network-security/university-phishing-attacks-prevention/

Ddos-distributed-denial-of-service-explained [online]. 2020. [Citirano 2. feb 2021 9:09] Dostopno na spletnem naslovu: https://www.globaldots.com/ddos-distributed-denial-of-service-explained

Prince, Matthew. 2012. Deep Inside a DNS Amplification DDoS Attack : Amplification Attacks. Cloudflare. [online]. Feb. [Citirano 3. feb 2021 11:13], Dostopno na spletnem naslovu: https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

Slowloris DDoS Attack [online]. [Citirano 3. feb 2021 11:18] Dostopno na spletnem naslovu: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/

NTP Amplification DDoS Attack [online]. [Citirano 3. feb 2021 11:21] Dostopno na spletnem naslovu: https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

Griffin, Angus. 2013. A History of the Anonymous Mask. Dazed. [online]. Feb. [Citirano 3. feb 2021 11:25], Dostopno na spletnem naslovu: https://www.dazeddigital.com/artsandculture/article/16360/1/a-history-of-the-anonymous-mask

Chaos computer club [online]. [Citirano 4. feb 2021 18:15] Dostopno na spletnem naslovu: https://www.ccc.de/en/

Hatamoto, Michael. 2020. Lizard Squad says it wasn't hacked, distributed customer data. TweakTown. [online]. Feb. [Citirano 4. feb 2021 8:18], Dostopno na spletnem naslovu: https://www.tweaktown.com/news/43097/lizard-squad-hacked-distributed-customer-data/index.html

15 Notable Hacker Groups and their Famous Hacks of All Time : 4. Master of Deception [online]. [Citirano 4. feb 2021 8:21] Dostopno na spletnem naslovu: https://www.rankred.com/famous-hacker-groups/

15 Notable Hacker Groups and their Famous Hacks of All Time : 8. Legion of Doom [online]. [Citirano 4. feb 2021 8:23] Dostopno na spletnem naslovu: https://www.rankred.com/famous-hacker-groups/

8. Priloga

Anketni vprašalnik

1. Si seznanjen/a s kibernetskimi napadi?

a) Da

b) Ne

2. Za katere od teh kibernetskih napadov si že slišal/a?

a) DDoS napad

b) DoS napad

c) Phising

č) Drugo_____

d) Nisem slišal/a za nobene kibernetske napade

3. Si že slišal/a za organizirane hekerske skupine?

a) Da

b) Ne

4. Če ja, katere od teh hekerskih skupin poznaš?

a) Anonymous

b) Chaos Computer Club (CCC)

c) Homebrew Computer Club

č) Homebrew Computer Club

d) Masters of Deception

e) Legion of Doom

f) Drugo:_____

g) Nisem slišal/a za njih

5. Si že slišal/a za kakšne kibernetske napade v Sloveniji?

a) Da

b) Ne

6. Če ja, za kateri kibernetski napad v Sloveniji si slišal/a?

a) Odgovor:_____

7. Kateri je največji kibernetski napad, za katerega si slišal/a?

a) Odgovor:_____

b) Nisem slišal za večje kibernetske napade

8. Si bil kdaj tarča kibernetskega napada?

a) Da

b) Ne

9. Če ja, tarča kakšnega napada si bil?

a) DDos napad

b) Dos napad

c) Phising

č) Drugo_____

d) Nisem slišal/a za nobene kibernetske napade

10. Kaj bi naredil/a, če bi bil/a tarča kibernetskega napada?

a) Odgovor:_____