IV. OSNOVNA ŠOLA CELJE

Dečkova cesta 60

RAZISKOVALNA NALOGA

OSNOVE RAČUNALNIŠKEGA HEKANJA

Tematsko področje:

- računalništvo
- hekanje

Avtorica:

Marija Črepinšek, 9.a

Mentorica:

Miroslava Minić, prof. mat

Mestna občina Celje, Mladi za Celje

Celje, 2022

Povzetek

V nalogi sem združila področje računalništva in zgodovine. Najprej bom predstavila splošne stvari o hekanju, ki bi jih po mojem mnenju moral vedeti vsak izmed nas oz. vsi, ki smo uporabniki informacijsko-komunikacijskih tehnologij. Moj namen je bil ugotoviti, koliko ljudje danes vedo o svoji varnosti na spletu.

Vsak dan se po svetu dogajajo različni spletni vdori, ki jih povzročajo t. i. "black hat" hekerji. To so vdori v različne računalniške sisteme; npr. sisteme podjetij ali tudi vdor v kakšno izmed vaših oz. naših naprav. Ljudje se včasih ne zavedamo, da nam je nekdo vdrl v računalnik ali telefon in nam ukradel kakšne fotografije ali osebne podatke. Ti podatki so lahko zlorabljeni na različne načine: kraja identitete, kraja fotografij, ki jih po svoji volji nepridipravi tudi preprodajajo na črnem spletnem trgu. Zato moramo svoje naprave tudi opazovati in sumljive dogodke odpraviti z naprave na pravi način. Obstajajo tudi varne spletne strani z nasveti (npr. Safe.si, Arnes - varni na internetu …). Pomembna je tudi zaščita naprave z različnimi znanimi antivirusnimi programi za računalnike ali telefone. Na koncu naloge sem tudi z anketo poskusila dokazati, kakšno je splošno znanje in s kakšnimi informacijami o hekanju ljudje trenutno razpolagajo.

KAZALO

1. UVOD

Od malih nog sem rada gledala akcijske filme, kajti v vsakem takšnem filmu se je prikazala scena, kjer so agenti vdrli v računalnike, da so lahko ujeli kriminalce. To me je privlačilo. Naredila sem nekaj preiskav na internetu in ugotovila, da ni vse v tem, da pomagaš najti kriminalce, ampak se tako lahko tudi sam zaščitiš pred vdorom.

Ugotovila sem, da me zanima reševanje nalog s področij, kot so spletna varnost, mobilna varnost, kripto uganke, povratni inženiring in forenzika.

Vsi, ki uporabljamo računalnike ali telefone, smo lahko izpostavljeni različnim digitalnim nevarnostim; od virusov, kraje digitalne identitete do izgube pomembnih podatkov. Najboljša obramba je dobro poznavanje delovanja zlonamernih digitalnih napadov. V nalogi bom prikazala različne tehnike vdorov in zaščit oziroma luknje v zaščiti.

1.2 OPREDELITEV IN IZBOR RAZISKOVALNEGA PROBLEMA

Računalniško hekanje se mi zdi predvsem aktualna in zanimiva tema. V današnjih časih se je večina ljudi, mladi in odrasli, bolj kot ne "preselila" v različna spletna okolja (oblake, drive, družabna omrežja, spletne storitve, spletno bančništvo itd.). Računalniške spretnosti so postale samoumevne v sodobni družbi. Obenem se zdi, da ko pride do ogroženosti na spletu (vdora v spletni profil, zlorabe uporabniškega računa ipd.), nismo dovolj izurjeni, kako odreagirati, se zaščititi ali na kateri naslov prijaviti morebitno zlorabo. V naši družbi se še vedno veliko ljudi ne upa uporabljati spletnega bančništva, ker niso dovolj izobraženi na tem področju ali ne vedo, kako odreagirati v primeru morebitne zlorabe oz. kraje. Po drugi strani vemo (posebej v trenutnih "koronskih" razmerah v družbi), da bi bil zelo priročen brezskrben nakup recimo vozovnic za vlak, avtobus, vstopnice za gledališče ali plačilo položnic za starejše osebe ali osebe, ki živijo v odročnih krajih.

Večinoma smo uporabniki dobro informirani, da moramo za varno uporabo spleta uporabljati t. i. močna gesla. Verjetno smo tudi obveščeni, da ni priporočljivo odpirati vseh možnih priponke, ki jih prejmemo preko socialnih omrežij ali e-pošte. Žal včasih ta opozorila spregledamo ali celo zanemarimo. Za krajo identitete smo že slišali. V tujini se takšne kraje dogajajo bolj pogosto. Slovence rešuje to, da nas je malo.

Zato se mi zdi ozaveščanje populacije na tem področju zelo pomembno.

Pomembno je, da se ljudje seznanijo s tematiko hekanja, samega pomena te prevzete besede in tako ga lahko spoznajo tudi preko moje raziskovalne naloge.

S pojasnitvijo pomena hekanja z nekaj primeri ter s pomočjo raziskave v lastnem okolju o tem, kaj ljudje mislijo, da hekanje pomeni, bom pomagala, da si ustvarite lastno mnenje o hekanju, ki vam obenem ne bo tuje.

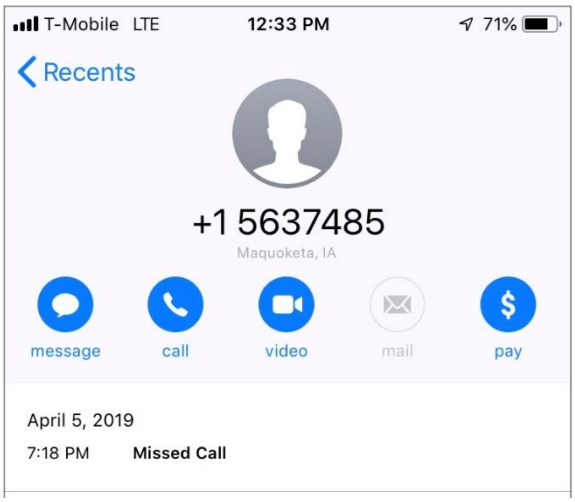
2. CILJI, POTEK IN HIPOTEZE

2.1 CILJI RAZISKOVALNE NALOGE

Cilj moje raziskovalne naloge je pogledati in vprašati, koliko ljudje dandanes vedo o hekanju oz. kibernetskih vdorih. Po mojem mnenju je to področje med mladimi malo raziskano. Ob pregledovanju različnih virov sem prišla do spoznanja, da je malo mladostnikov, ki vedo kaj več o vdorih in virusih in se težko odločajo, kako odreagirati v takšnih situacijah.

V naslednjem primeru vam bom predstavila lažji hekerski napad preko vaše telefonske številke in kako se ga lahko obranite.

Gre za primer t. i. socialnega inženiringa:



Slika 1: Vsiljiva številka

Med stiki vidimo zgrešeni klic s »čudne« telefonske številke. V tem primeru NE VRAČAMO klica. Če pa vas prevzame radovednost in klic vrnete, boste deležni oglasnega sporočila, samodejnega odzivnika ali tišine. Tako bo nastal strošek na vašem telefonskem računu. V tem primeru boste plačali klic, ker vas je nekdo klical iz oddaljene države, kjer so že po njihovem ceniku klici zelo dragi.

Razmislimo. Kako bi odreagirali vi ali člani vaše družine v primeru takšnega klica?

2.2 POTEK DELA

Z namenom ugotoviti, koliko dandanes ljudje vedo o računalniškem hekanju in kakšno je njihovo mnenje, sem uporabila anketo.

Nastali sta dve anketi, ena za učitelje ter druga za moje sošolce. Anketi se razlikujeta samo v vrstnem redu vprašanj.

Učenci in učitelji bodo odgovorili na anketo. Tako bom potem lahko primerjala, koliko vedo o hekanju, ter ugotovila, kakšne so razlike glede na starost anketirancev.

Moje raziskovalno delo se je začelo s postavitvijo raziskovalnih hipotez, s pomočjo katerih sem odgovorila na vprašanja raziskovalne naloge. Pred raziskavo sem najprej želela poiskati čim več literature in člankov na to temo in dobiti širši vpogled, kaj pomeni hekanje. Ali poznamo kakšnega hekerja? Smo posamezniki lahko hekerji? So hekerji čudaški in pokvarjeni? Ali je heker lahko kdorkoli? Opravila sem anketo med sošolci in učitelji, naredila analizo ter rezultate prikazala v obliki diagramov.

Ko sem končala z analizo, sem preverila hipoteze ter napisala še zaključek. Nalogo sem oddala v lektoriranje.

Za to raziskavo sem se odločila, ker se danes o tej temi premalo govori, saj eni pravijo, da ni tako pomembna, pa čeprav se meni zdi, da se motijo. Zdi se mi tudi, da je o tem vprašanju narejenih premalo raziskav.

2.3 HIPOTEZE

Na začetku sem postavila naslednje hipoteze:

HIPOTEZA 1: Večina vprašanih bi morala vedeti, kaj pomeni beseda heker.

HIPOTEZA 2: Dandanes ljudje mislijo, da je hekerstvo samo slaba stvar in ne tudi dobra.

HIPOTEZA 3: Večina ljudi misli, da je hekerstvo izšlo iz računalništva, pa čeprav ni.

HIPOTEZA 4: Predvidevam, da se je vsakemu izmed nas zgodil hekerski napad.

HIPOTEZA 5: Ljudje danes ne vedo veliko o hekerskih tehnikah, saj ne izražajo veliko zanimanja.

HIPOTEZA 6: Svet spleta in hitrega napredovanja računalništva žene uporabnike v nenehno previdnost in kritično razmišljanje, saj brez pravega zavedanja hitro postanemo žrtev spletnega nasilja ali hekerstva.

3. TEORETIČNI DEL

3.1 KDO JE HEKER?

Heker je oseba, ki se ukvarja s tehnologijo, da bi jo izboljšal ali spremenil njeno delovanje ali jo celo tudi uničil.

3.2 ZGODOVINA BESEDE HEKER

Beseda izhaja iz angleškega izraza »hack«, kar je nekoč pomenilo grobo presekati. V sodobnem pomenu so jo prvič uporabili leta 1955 v povezavi z modeli železnic. Tehnološki inštitut v Massachusettsu (MIT) je iskal načine, kako napolniti tire z več električne energije. Ko so se modeli vlakov hitro premikali po tirih, so s hitrimi spremembami večkrat preobremenili tokokroge. To so poimenovali hekanje. Prvi **hekerji** so bili ljubitelji vlakcev**.**

Hekanje železnice je pripeljalo še do hekanja računalnikov.

3.3 DEFINICIJA HEKERJEV

Do leta 1975 so računalniški znanstveniki razvili nov jezik in ga zabeležili v slovar žargona s seznamom tehnološkega slenga. Hekerje je potem definiral na več načinov. Najpomembnejši:

- **Oseba, ki rada raziskuje** podrobnosti sistemov in išče možnosti za povečanje zmogljivosti sistema.
- **Oseba, ki čas in trud z veseljem** nameni reševanju problemov brez očitne vrednosti.
- **Strokovnjak** ali navdušenec poljubne vrste (pri programiranju).
- **Zlonamerni vsiljivec,** ki skuša odkriti občutljive informacije.

Hekerji so torej sposobni in ustvarjalni, niso vedno usklajeni s pravili, ki nam jih narekuje družba. Kršijo tudi ustaljene norme in predstavljajo nasprotje tistim, ki se pri uporabi komunikacijske tehnologije naučijo le osnovnih veščin uporabe. Niso vedno negativci. Marsikateri vrhunski strokovnjak je začel kot heker. Z razvojem digitalnih tehnologij se je razvijalo tudi hekerstvo.

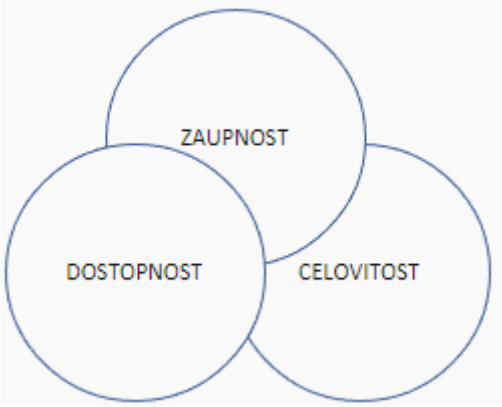
Slika 2: Heker

3.4 OPREDELITEV INFORMACIJSKE VARNOSTI

Vdiranje v računalniške in komunikacijske sisteme je nekaj, kar bi moralo biti vedno v mislih vsakega uporabnika interneta. Ne zato, ker želimo postati hekerji, temveč zato ker lahko vsaka napaka ogrozi vaše osebne podatke.

Informacijsko varnost ločimo med podatki in informacijami. **Informacije** so podatki, oblikovani v smiselno in uporabno obliko. **Podatki** so gola dejstva, ki opisujejo dogodke ali fizično okolje. Za razumevanje pomena varovanja informacij moramo preučiti ogroženost informacijskih sredstev. Najpogosteje predlagana opredelitev je Model CIA, ki vključuje 3 vidike:

- **zaupnost,**
- **celovitost,**
- **dostopnost.**



Slika 3: model CIA

3.5 MODEL CIA

Model CIA se uporablja za prepoznavanje problematičnih področij, ki so ključnega pomena za zagotavljanje informacijske varnosti. Je uveljavljen in znan model za razvoj varnostne politike. Ima tri vidike, v katere se bomo poglobili.

3.5.1 ZAUPNOST

Zaupnost je varnostno načelo, ki nadzoruje dostop do informacij. Narejeno je tako, da dostopa do občutljivih informacij ne omogoči napačnim ljudem, ampak le pooblaščenim ljudem. Primeri zaupnih informacij so: osebne informacije, vladni dokumenti, številke kreditnih kartic itd.

3.5.2 CELOVITOST

Celovitost zagotavlja, da so občutljivi podatki zanesljivi in natančni. Med vrste napadov, ki ogrožajo celovitost informacij, spadajo: verižni napadi, sleparski napadi, napadi izkoriščanja zaupanja, napadi s posrednikom ter napad z ugrabitvijo seje.

3.5.3 DOSTOPNOST

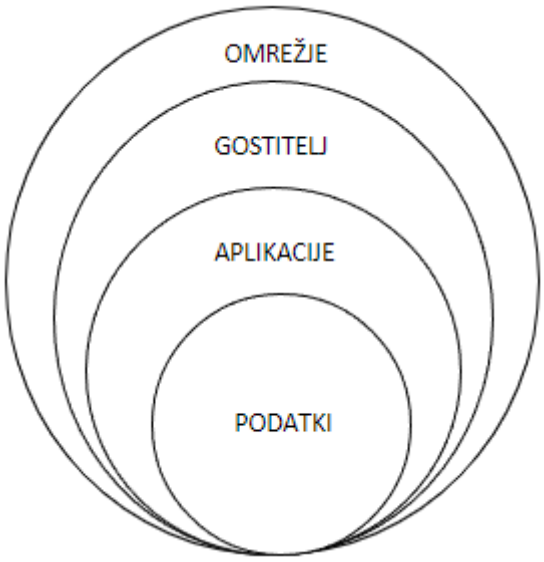
Dostopnost je jamstvo, ki pooblaščenim osebam omogoča zanesljiv in stalen dostop do občutljivih podatkov. Zagotavljamo ga s pravilnim vzdrževanjem strojne in programske opreme, kjer se ti podatki hranijo in prek katere dostopamo do njih. Najpogostejši napadi, ki ogrožajo dostopnost informacij, so: ohromitev in porazdeljena ohromitev storitve, poplava SYN in fizični napadi na strežniško infrastrukturo.

3.6 OBRAMBA V GLOBINO

Obramba v globino je pristop h kibernetski varnosti, v katerem za varovanje podatkov in informacij skrbi več zaščitnih mehanizmov. Če en mehanizem odpove, se sproži naslednji in tako prepreči napad. Celotna informacijska varnost ima naslednje značilnosti:

- **Asimetrično bojevanje:** podjetje mora zaščititi celotno mrežo, medtem ko je za hekerja dovolj, da najde samo eno ranljivost.
- **Obramba v globino:** da bi bil napad uspešen, mora zaobiti več ravne površine.
- **Varnostni pregledi:** varnostne preglede izvajajo najeti posamezniki.

Splošni koncept obrambe v globino predstavljamo kot **»čebulni«** pristop k varovanju podatkov, kjer so dragoceni podatki v sredini čebule.



Slika 4: Čebulni pristop obrambe v globino

3.7. ZAČETKI INTERNETA

Internet je omrežje računalnikov. Pravzaprav je poimenovano medmrežje, saj povezuje veliko različnih računalniških omrežij. Internet je bil sprva kot vojaški obrambni projekt. V šestdesetih letih prejšnjega stoletja so vojaški poveljniki razvijali sisteme, ki so lahko uporabljali računalnike in telekomunikacije. Za varne komunikacije tudi v primeru najhujših napadov so vzpostavili ARPANET.

ARPANET je deloval s sistemom, v katerem je bilo sporočilo razdeljeno v nize. Vklopili so ga leta 1969. Na začetku je povezoval samo štiri univerze. Kasneje se je vpliv univerz razširil tudi na državne ravni. Eno od opravil ARPANET-a je bilo pošiljanje elektronske pošte oziroma e-pošte. S pojavom interneta in razvojem storitve e-pošte je tudi hekerstvo dobilo svoj polni zagon.

3.8. HEKERSKE TEHNIKE IN KULTURA HEKANJA

3.8.1 HEKERSKE TEHNIKE

Najpodlejši način za vdor v tvoj sistem je dodajanje **zlonamernih programov**. Ti lahko ustvarijo »zadnja vrata«, preko katerih lahko heker na skrivaj prevzame nadzor nad računalnikom.

Heker s trojanskim konjem namesti zlonamerni program, ki je skrit v navidezno neškodljivi aplikaciji (npr. poštna priponka).

Naslednji vdor je **socialni inženiring ali phishing.** Poteka tako, da te heker pokliče ter se predstavi, kot da je iz IT-oddelka in se oglaša, ker ima tvoj računalnik težave. Zato te vpraša za tvoje geslo, ponudi se, da bo popravil računalnik z njegovega delovnega mesta. Sliši se zelo logično, ampak ne pusti se preslepiti. Hekerji uporabljajo trike, s katerimi jim zaupamo naše skrivnosti.

Ugrabljanje klikov preslepi uporabnika, da klikne na skrito povezavo. Te povezave izgledajo čudno, saj jih sestavljajo vrste različnih črk in številk pomešanih skupaj. S takšnim klikom te heker spravi na določeno navidezno stran, kjer lahko npr. odvzame vsa shranjena gesla v tvojem spletnem brskalniku.

Nekateri zlonamerni programi ne potrebujejo ljudi, da bi jih širili (vede ali nevede). Npr. **računalniški črvi** za svoje širjenje uporabljajo gostiteljske programe in omrežje. Dobri hekerji lahko poiščejo proti-črve, ki bodo poiskali in uničevali zlonamerne črve in njihovo širjenje po sistemu in programih. Primeri vdorov v sodobnih časih lahko delujejo zelo prikrito in všečno. Uporabniki smo lahko ležerni pri uporabi istega gesla. Pogosto ne uporabljamo zapletenih zaporedij znakov, ki bi povečali število permutacij za ugibanje morebitnega hekerja.

Ena izmed lažjih tehnik je, da napadalec uporabi program za **lažno brezžično dostopno točko**. Ko se uporabnik poveže na omrežje, napadalec dobi dostop do tvojih podatkov. Za izvedbo napadalec potrebuje zgolj program in brezžično omrežje.

Hekerske tehnike se iz dneva v dan spreminjajo. Priča smo, da se svetovni spopadi odvijajo tudi v digitalnem svetu. Primer **kibernetskega napada:** kliknemo na YouTube, vendar se pojavi napaka v povezavi, želimo pobrskati po Googlu ali priljubljeni spletni strani, vendar se stran ne odziva. Pojavi se sporočilo, da se srečujemo s tehničnimi težavami. Dobimo občutek, da se dogaja nekaj izven dojemljivega. V tem primeru lahko gre za kibernetski napad.

V Sloveniji nimamo zakona, kot v nekaterih drugih državah, kjer morajo upravljalci sistemov seznaniti javnost z morebitnimi napadi ali poskusi napadov. Slovenski kredibilen vir je CERT, ki vsako leto beleži konstanten porast spletnih incidentov (https://www.cert.si/).

Tudi na spletnem mestu Safe.si in Varni na internetu lahko najdete veliko opozoril, česa se je pri uporabi spletnih storitev potrebno izogibati.

Hekerji so v sodobnem svetu dobili pomembne vloge in skoraj ni več države, ki ne bi imela svojega tima elitnih hekerjev, ki skrbijo za varnostne zadeve in za tako imenovani "state hacking".

Na spletu je prisotnih veliko programov, ki se uporabljajo za vdiranje in krajo podatkov ter informacij (WIRESHARK, NMAP, OWASP ZED …).

Zavedati se moramo, da ne obstaja stoodstotna zaščita pred hekerji. Z določenimi preventivnimi ukrepi je možno minimizirati potencialno škodo in takšne morebitne spletne nevarnosti opaziti ter tudi ustrezno ukrepati.

Slika 5: Trojanski konj

3.8.2 KULTURA HEKANJA

Hekerji imajo tudi svojo kulturo, kajti niso vsi slabi, saj se med njimi znajde tudi kakšen dober. Poznamo različne vrste hekerjev.

Našla sem zelo pestro terminologijo poimenovanja hekerjev:

- **Kreker** je heker, ki dela zločine in s tem so na slabem oglasu tudi drugi hekerji.
- **Skriptar** je kreker, ki je brez znanja, zato povzroči težave s skripto.
- **Friker** je strokovnjak za napade na varnost.
- **Šifrar** se ukvarja z razbijanjem šifre.
- **Wares doodz** je specialist za izdelavo nelegalnih kopij avtorsko zaščitene programske opreme in njihovega razpečevanja.
- **Železninar** je strokovnjak za opremo in je deležen prezira pravega hekerja.
- **Alfa gik** je najbolj vešči in izkušeni član hekerskega kolektiva, ki ga tudi drugi člani prosijo za pomoč.
- **Chomper** so neizkušeni hekerji in tisti, ki imajo za seboj veliko neuspešnih vdorov.
- **Gulež kode** so IT-profesionalci, ki jih hekerstvo ne zanima.
- **Silak** uporablja napade skozi zaščito z golo silo.
- **Plačanec** je heker, ki ga kriminalna združba najame, da poskrbi za programiranje.

- **Peskokop** razvija in proizvaja silicijeve mikročipe.
- **Ubergik** ima vpliv na širšo skupnost, še posebej s pisanjem programov, ki jih pogosto uporabljajo drugi.
- **Pijavka** je posebna vrsta zgubljenega hekerja, ki prinaša izmenjane datoteke, a drugim ne omogoča dostopa do njih.
- **Čarodej** je heker z vrhunskim znanjem, daleč od zmožnosti povprečnega hekerja.

Vsekakor je potrebno izpostaviti tri vrste hekerjev: črne, bele in sive klobuke.

Črni klobuki so hekerji kriminalci, ki kršijo varnost s krivimi dejanji in s slabimi nameni. ***Beli klobuki ali etični hekerji*** pa so tisti hekerji, ki delajo za skupnost in kljub temu, da se spoznajo na računalniške vdore, pravzaprav izboljšujejo kibernetsko zaščito in preprečujejo napade črnih klobukov. Obstajajo še ***sivi klobuki,*** hekerji, ki iščejo pomanjkljivosti v programski opremi. Če kaj odkrijejo, pa zahtevajo nagrado od oseb, ki bi jih to odkritje moralo skrbeti. Včasih pa ranljivost objavijo na spletu. Ta vrsta hekerjev sama po sebi ni zlonamerna, saj ranljivosti običajno ne izkoristi. Vseeno pa gre za nezakonito dejanje, saj niso dobili dovoljenja lastnika za poseganje v sisteme.

Razdelitev na črne, bele in sive klobuke pravzaprav izhaja iz kavbojskih filmov (vesternov), kjer je hudobnež običajno nosil črn klobuk, junak pa belega.

Bele klobuke povezujejo še z junaki, **super heroji**, s čarovnikoma Gandalfom ali Dumbledorjem, ki svoje znanje uporabljata za dobro in ne slabo. Nekateri jih povezujejo tudi s Star Wars, saj so vsi oviti v kapuce in dolge halje, imajo znanje in sposobnosti, o katerih drugi le sanjajo …

Nekaj znanih hekerjev in njihovih napadov:

- Leta 1999 (David Smith – ZDA) je spustil virus Melissa, ki je okužil e-pošto in programe. Nastala je milijonska svetovna škoda.
- Leta 2006 (Janson Ancheta – ZDA) je nadziral botnet z okrog 100 tisoč računalnikov in je dobil petletno zaporno kazen.
- Hamza Bandelladj (Alžirija) je z virusi okužil 50 milijonov računalnikov in ukradel 400 milijonov dolarjev. Sicer jih je podaril v dobrodelne namene. Obsojen je bil na 15 let zapora.
- Kevin Mitnick je že pri 15 letih našel način, da se izogne identifikaciji uporabe sistema vožnje v mestnem prometu. Leta 1981 je ukradel računalniške dokumente podjetju Pacific Bell. Naredil je vdor v podjetje Digital Equipment Corporation's. Leta 1995 je bil aretiran, da odsluži petletno zaporsko kazen.
- Gary McKinnon je škotski heker rojen leta 1966. Najbolj znan je po številnih vdorih v računalnike ameriške vojske in vesoljske agencije Nasa. Ob vdoru je na namizjih puščal sporočilo: »Your security is really crap« (Vaša varnost je res zanič).
- Albert Gonzales. Rojen leta 1989 na Floridi, je heker, ki je ustanovil spletno stran Shadowcrew.com. Ukvarjal se je s krajo številk kreditnih kartic. Znan je bil pod različnimi imeni. Prirejal je velike zabave v dragih hotelih. Trenutno je v zaporu.

Med belimi klobuki izpostavljam Richarda Stallmana, ki se je spomnil poimenovanja črni in beli klobuki. Znan je po razvoju brezplačne programske opreme in operacijskega sistema Unix oz. Linux.

Beli klobuki ali etični hekerji podjetjem pomagajo pravočasno odkriti ranljivosti v omrežju in ostali IT-infrastrukturi. Za to uporabljajo različna virtualna in fizična sredstva, kot so **socialni inženiring** (preizkušanje varnostnega znanja zaposlenih), **penetracijski testi** (so glavno orodje etičnega hekerja, da odkrivajo ranljivosti v obrambi in končnih točkah), **izvidništvo in raziskava** (pridobivanje podatkov za identifikacijo načinov, kako zaobiti varnostne protokole in mehanizme, ne da bi povzročili škodo), **programiranje** (ustvarjanje navideznih sistemov, ki služijo kot vaba za kibernetske kriminalce in s katerimi jim preprečijo dostop do ključnih sistemov), **uporaba različnih digitalnih in fizičnih orodij** (strojna oprema in naprave, kloniranje ID dostopne kartice, nameščanje bota ali druge programske opreme ter pridobivanje dostopa do omrežja).

4. RAZISKAVA IN REZULTATI

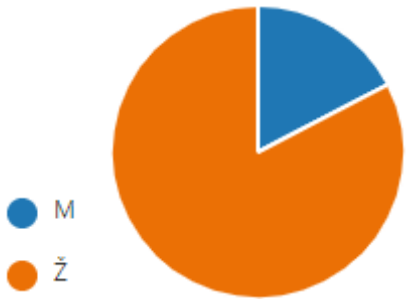
Anketo sem poslala učencem in učiteljem. Dobila sem naslednje odgovore, ki jih bom prikazala v grafih. Na anketo je odgovorilo 23 učiteljev in 8 sošolcev (mladih). Zanimivo je, da je starejša populacija izkazala večje zanimanje za anketo kot mlajša. Sošolci na veliko vprašanj niso odgovorili. Zato v nadaljevanju predstavljam anketo za učitelje.

4.1 RAZISKAVA

ANKETA ZA UČITELJE

(23 odzivov)

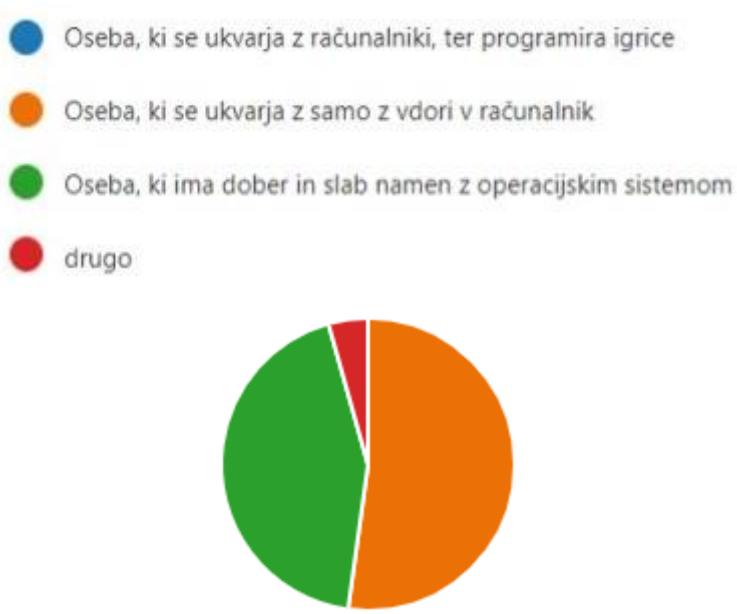
✓ Izberite vaš spol



Graf 1: Anketno vprašanje 1

Na prvo anketno vprašanje je odgovarjalo več žensk kot moških. V primeru učiteljev je to logično, ker je na šoli zaposlenih več učiteljic kot učiteljev. Tudi med mladimi so več odgovorov podala dekleta kot pa fantje.

✓ Kdo je po vašem mnenju heker?

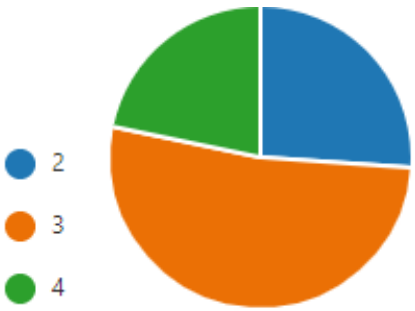


Graf 2: Anketno vprašanje 2

Pri drugem anketnem vprašanju je zanimivo, da nisem prejela nobenega modro pobarvanega odgovora: »Oseba, ki se ukvarja z računalniki ter programira igrice.« Ali se vam ne zdi možno, da heker tudi izdeluje igrice?

Tudi drugačnih definicij hekerja ni bilo pod rdečo obarvano možnostjo za drug odgovor. Predvidevam, da so bili anketiranci zmedeni in niso bili prepričani, kako pravilno odgovoriti na to vprašanje.

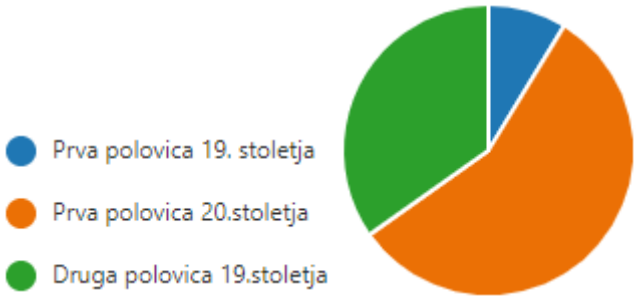
✓ Koliko vrst hekarjev poznamo (glede na načine njihovega delovanja oz. izvedbe hekerskih vdorov) ?



Graf 3: Anketno vprašanje 3

Večina vprašanih je izpostavila, da pozna tri vrste hekerjev. Nekateri izmed anketirancev so mi povedali, da jih je vprašanje zmedlo. Niso razmišljali o številnih načinih in različnih izvedbah vdiranja. Prepoznali so hekerje z »dobrimi« in druge s »slabimi« nameni.

- ✓ Kdaj so začeli prvič hekati?



Graf 4: Anketno vprašanje 4

Večina anketirancev meni, da je hekanje povezano izključno s sodobnimi časi. V raziskovalni nalogi sem dokazala, da ima hekanje svoje korenine že v začetku 19. stoletja. Skrito pisanje, šifriranje vsebin in informacij ter kriptografija so namreč zametki hekerstva.

✓ Naštej vsaj 3 hekerske tehnike!

1	anonymous	hrošči, zlonamerni programi, kraja gesl ..
2	anonymous	Ne poznam nobene
3	anonymous	?
4	anonymous	Uporaba računalniškega virusa.
5	anonymous	Vdor v pošto, kraja identitete
6	anonymous	Pojma nimam
7	anonymous	spyware, poplava podatkov - "zapolnitev", lažno predstavljanje...
8	anonymous	Piratstvo, kraja informacij in denarja, zakodiranje dokumentov.
9	anonymous	ne vem
10	anonymous	Lažno predstavljanje napadalčevega operacijskega sistema (ID spoofing, WEB spoofing, DNS spoofing) - računalniški črv, ki s širjenjem kode povzroča preglavice uporabnikom, zaklepanje napadenega računalniškega sistema in finančno izsiljevanje za odklenitev sistema - kraja identitete pomembnim osebam.

Preglednica 1: Anketno vprašanje 5

Zanimivo je, da je imela večina anketirancev težave pri odgovarjanju na zastavljeno vprašanje. Hekerske tehnike so vedno skrivnost. Vseeno nas vse skrbijo morebitni vdori, računalniški črvi, kraje identitet …

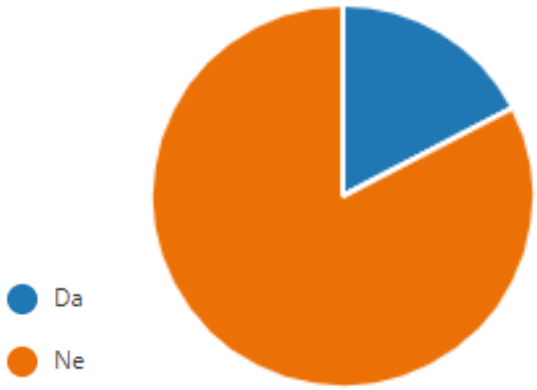
✓ Napišite kakšen hekerski napad, ki se je zgodil v preteklem času!

1	anonymous	Vdor v easistenta prejšnji teden ..
2	anonymous	na eno izmed ameriških bank pred leti
3	anonymous	?
4	anonymous	Vdor v eAsistent z uporabo druge internetne domene
5	anonymous	Vdor v zasebno pošto
6	anonymous	Mi je ušlo iz glave
7	anonymous	??? na šoli, 2-3 leta nazaj...
8	anonymous	Ustvarjanje lažne spletne strani v namen preusmeritve plačila v podjetju.
9	anonymous	eAsistnt
10	anonymous	Vdor v YAHOO strežnik 2013-2014. Prizadeta je bila miljarda ljudi, ki so jim ukradli prijavne podatke. Vdor so odkrili šele po daljšem času. Istega leta je bil izveden tudi hekerski napad na kriptovaluto Bitcoin, kjer so odtujili za 450 milijonov ameriških dolarjev Bitcoinov.

Preglednica 2: Anketno vprašanje 6

Vprašanje je bilo še posebej zanimivo za učitelje. Omenjali so vdore v eAsistent, spremembe domen, strežnikov ... Moji sovrstniki so se bolj zanimali za kraje kriptovalut, identitet ipd.

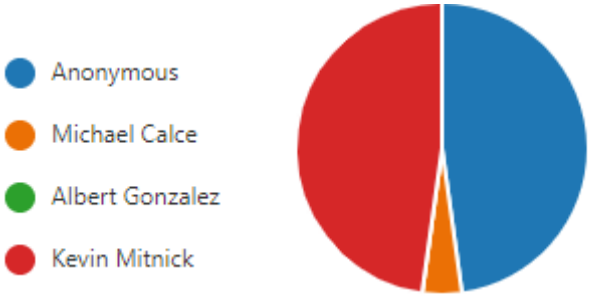
✓ Ali se vam je že kdaj zgodil kakšen hekerski napad?



Graf 5: Anketno vprašanje 7

Večina je odgovorila, da ni bila deležna nobenega hekerskega napada.

✓ Kdo je najbolj znani heker na svetu?



Graf 6: Anketno vprašanje 8

O znanih hekerjih je večina povedala, da so anonimni. Sošolci so priznali, da so odgovor preprosto poguglali.

4.2 REZUTATI

Na začetku sem zapisala naslednje hipoteze:

HIPOTEZA 1: Večina bi morala vedeti, kaj pomeni beseda heker.

Hipoteza se je izkazala za napačno, saj je 43 % učiteljev odgovorilo pravilno in 57 % napačno.

HIPOTEZA 2: Dandanes ljudje mislijo, da je hekerstvo samo slaba stvar in ne tudi dobra.

Hipoteza je pokazala, da učitelji vedo, da hekerstvo ni samo slabo, ampak je tudi dobro.

HIPOTEZA 3: Večina ljudi misli, da hekerstvo izhaja iz računalništva, pa čeprav ta trditev ne drži.

Za potrditev te hipoteze sem dala anketo učiteljem. Anketno vprašanje 4 (graf 4) je dokazalo, da večina ljudi ne pozna tega.

HIPOTEZA 5: Predvidevam, da se je vsakemu izmed nas zgodil hekerski napad.

Izkazalo se je, da je manj kot 25 % anketirancev doživelo hekerski napad. Čeprav sama menim, da se večina ljudi ne zaveda, da so ga bili deležni.

HIPOTEZA 6: Ljudje danes ne vedo veliko o hekerskih tehnikah, saj ne izražajo veliko zanimanja.

Zanimivo je, da je imela večina anketirancev težave pri odgovarjanju na zastavljeno vprašanje, saj ni razumela vprašanja oz. ni vedela odgovora. Hekerske tehnike so dandanes skrivnost. Vseeno nas vse skrbijo morebitni vdori, računalniški črvi, kraje identitet …

HIPOTEZA 7: Svet spleta in hitrega napredovanja računalništva žene uporabnike v nenehno previdnost in kritično razmišljanje, saj brez pravega zavedanja hitro postanemo žrtev spletnega nasilja ali hekerstva.

Vprašanje je bilo še posebej zanimivo za učitelje. Omenjali so vdore v eAsistent, spremembe domen, strežnikov ... Moji sovrstniki so se bolj zanimali za kraje kriptovalut, identitet ipd.

Cilje, ki se si jih zadala v nalogi, sem dosegla in pokazala pomen hekerstva v sodobni družbi. Ta nas vedno bolj skozi vsakdan ob uporabi spleta pelje v nek nov vzporedni spletni svet dobrih in slabih dejanj. Izpostavila sem pomen zavedanja in nenehnega izobraževanja v tej smeri.

Zdi se, da mlajša populacija bolj brezskrbno gleda na hekerstvo. Hekerstvo se jim zdi zanimivo, ker predstavlja nekakšno »hojo po robu« in sodobno uporništvo sistemu. Učitelji so bili pri odgovorih bolj usmerjeni na nevarnosti, ki izhajajo iz hekerskih vdorov.

Opomba: Čeprav anketa in delo nakazujeta potrditev ali zavračanje postavljenih hipotez, opozarjam, da za statistično potrditev vsekakor potrebujemo veliko večji vzorec.

5. ZAKLJUČKI

Vdiranje ali hekanje je vsaka dejavnost, katere cilj je izkoriščanje in pridobivanje nezakonitega dostopa do računalniškega sistema, naprave ali omrežja brez dovoljenja lastnika.

Obstajajo različni hekerji. Zlonamernežem, ki želijo povzročiti škodo ali ukrasti podatke, rečemo črni klobuki, potem pa obstajajo še sivi in beli klobuki. Slednjim pravimo tudi etični hekerji, saj svoje znanje uporabljajo za dobrobit družbe oziroma svojega naročnika.

Hekerstvo ima svoje korenine že v začetku 19. stoletja. Ko se je vzpostavilo prvo komuniciranje na daljavo (radio in radijska sporočila, telefoni …), se je izkazalo, da se lahko skrivajo informacije v uradnih kodah za prenos podatkov. Primer za to je zgodba iz leta 1834, ko sta dva človeka hekala omrežje stolpov s semaforji. Brata Blanc sta skrivala podatke o borzi iz Pariza znotraj kod in pred drugimi sta pošiljala podatke o spremembah cen preko semaforjev v Bordeaux. Tako sta na hitro obogatela. Po dveh letih hekanja so ju ovadili, a nobenega niso zaprli, saj takrat hekanje komunikacijskih sistemov ni bilo protizakonito. Napisala sem tudi primer nastanka besede heker na primeru goljufije z vlakci.

Ljudje se pogosto ne zavedajo, da so bili deležni hekerskega napada. Včasih, če nismo dovolj pozorni, se ne zavedamo niti poskusa vdora. Ne pozabimo, da hekerji iščejo slabosti našega sistema in če jih najdejo, izkoristijo priložnost za vdor. Zato je pomembno, da na naše naprave namestimo preverjene antivirusne programe (npr. Avast, TotalAV, Eset, McAffe …) in da smo ozaveščeni, da ne odreagiramo s prehitrim klikom na različno sumljivo e-pošto, povezave, spletne oglase ipd. Več informacij na temo nasvetov in varnosti lahko preberemo tudi na nekaterih spletnih straneh, ki so ustanovljene za podajanje informacij na to temo (Safe.si, Arnes - Varni na internetu, Kibertalent.si, Računalniške novice …).

Upam, da vam je moja raziskovalna naloga o hekerstvu dala vpogled v to aktualno tematiko ali vsaj spodbudila radovednost za obrambo pred hekerskimi ukanami.

6. LITERATURA IN VIRI

1. https://siol.net/digisvet/novice/klicala-vas-je-neznana-tuja-stevilka-ne-vrnite-ji-klica-529044 [ogled 10.1. 2022].
2. https://www.bbc.com/news/technology-37192670 [ogled 10.1. 2022].
3. https://sl.wikipedia.org/wiki/Heker [ogled 12.1. 2022].
4. https://sl.wikipedia.org/wiki/Heker#Motivi_hekerskih_vdorov [ogled 13.1. 2022].
5. https://sl.wikipedia.org/wiki/Heker#Vrste_hekerjev [ogled 13.1. 2022].
6. Tom Jackson. HEKERJI. Zbirka Za kaj gre? Učila International, 2021.
7. Blaž Markelj, Sara Tomše. Informacijska varnost : etično hekanje. Ljubljana : Lexpera, GV založba, 2020.

7. SEZNAM SLIK

8. KAZALO GRAFOV

9. KAZALO PREGLEDNIC