Tartu Ülikool
Arvutiteaduse instituut
Informaatika õppekava

Mark Robin Kalder

Vealeidmispreemia programmid ja eetiline häkkimine

Bakalaureusetöö (9 EAP)

Juhendaja(d): Alo Peets, *MSc*
Margus Niitsoo, *PhD*

Tartu 2022

Vealeidmispreemia programmid ja eetiline häkkimine

Lühikokkuvõte:

Käesolev töö tutvustab vealeidmispreemia programme (ingl *bug bounty program*) ehk eetilise häkkimise erivormi, kus rahalise preemia saamiseks tuleb leida IT süsteemidest turvanõrkusi. Eesmärgiks on eesti keeles seletada valdkonna olemust ja olulisust ning vastata küsimusele: "Kuidas vealeidmispreemia programmidega alustada?" Materjal on mõeldud inimestele, kellel on vähene teadmine valdkonnast. Töös on kasutatud internetist avalikult leitavaid materjale ja täiendava info saamiseks on intervjueeritud valdkonnaga kursis olevaid eksperte. Intervjuueeritavad on anonümiseeritud nende palvel ja saadud info on analüüsitud terviklikuks tekstiks. Bakalaureusetöö peamine tulem on käesolev dokument, mis võrdleb ja analüüsib vealeidmispreemia programme ning jagab spetsialistide soovitusi valdkonnaga alustada soovivatele lugejatele. Vealeidmispreemia programmidega kaasneb kohati soovimatu meedia-kuulsus ning inimesed, kes sellega tegelevad, ei soovi enamasti oma tegevusi kommenteerida avalikult ega oma nime all esineda. Sellegipoolest huvituvad mitmed noored IT-spetsialistid eetilise häkkimisega seotud teemadest ning sooviksid valdkonnast rohkem teada. Käesolev töö annab kasutatud materjalide ja intervjuude põhjal soovitusi eetiliseks häkkimiseks ja vealeidmispreemia programmidega alustamiseks.

Võtmesõnad:

Vealeidmispreemia, eetiline häkkimine, infoturve, puugipreemiajaht, puugioksjon, bug bounty

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Bug Bounty Programs and Ethical Hacking

Abstract:

This paper introduces bug bounty programs, a more specific form of ethical hacking, where one can get rewarded with money by finding security vulnerabilities from IT systems. The goal of this paper is to introduce and explain the field and to answer the question: "How to start with bug bounty programs?" This material is meant for people who have little to no knowledge of the field. This paper uses materials found from the internet and interviews with experts for additional information. The interviewees have been anonymized and the received information has been analysed into a comprehensive text. The main result of this bachelor's thesis is the given document in Estonian language which compares and analyses bug bounty programs and shares the recommendations of specialists for getting started with the field. Bug bounty programs are not yet known to the general public and the people who are working in this field do not wish to comment on their actions nor share it with other people. Still there are a lot of young IT-specialists who are interested in topics related to ethical hacking and would like to engage in the field. This paper gives recommendations based on the interviews on how to start with ethical hacking and bug bounty programs.

Keywords: Bug bounty, ethical hacking, information security

CERCS: P170 Computer science, numerical analysis, systems, control

Sisukord

Sissejuhatus

Arvutite ja nutitelefonide kasutus on tänapäeval väga sage. Ilma nendeta on keeruline ühiskonnas normaalselt toime tulla, kuna paljud toimingud ning andmed on kolinud paberitelt infosüsteemidesse. Inimeste tehtud ostud, maksud, allkirjastamised, hääle andmised jne on kõik teostatavad läbi interneti. Enamike inimeste kohta on palju tundlikku informatsiooni erinevate asutuste infosüsteemides. Küberturvalisuse tähtsus on selle tõttu kasvav ja asutused on sellest järjest enam teadlikud. Küberrünnaku ohvriks langenud ettevõttel on tihti suur varaline kahju, aga veel enam on kahjustatud ettevõte maine. Selle tagajärjel võib kaduda teiste osapoolte usaldus ja ettevõte isegi pankrotti minna.

Küberturvalisuse paremaks tagamiseks on loodud vealeidmispreemia programmid, mis on erivorm eetilisest häkkimisest. Kui eetilise häkkimise eesmärgid võivad erineda, siis üldiselt vealeidmispreemia programmidest osavõtmise põhjuseks on sellest saadav tasu. Vealeidmispreemia programmid on järjest rohkem populaarsust kogumas. Arvutisüsteemides avastatud nõrkade kohtade arv, mida küberkriminaalid saavad kasutada kahju tegemiseks, kasvab iga aastaga, suureneb ka nende avastamise eest saadud tasu [1].

Vealeidmispreemia programmid ja eetiline häkkimine on valdkonnad, mis on tähelepanu äratanud noortes spetsialistides, kellel on üldine huvi küberturvalisuse teemade vastu. Siiski on eetiline häkkimine suund, millega tegelema hakkamiseks on vajalik teada taustteadmiseid infotehnoloogiast. Isegi infotehnoloogiast teadmisi omades võib alguses eetiline häkkimine ning vealeidmispreemiad tekitada palju küsimusi ja huviliste jaoks osutub alustamine keeruliseks.

Käesoleva uurimustöö eesmärgiks on pakkuda alustavale spetsialistile eestikeelne õppematerjal, mille abil on alustamine kergem ning valdkonna kohta tekkinud küsimused saavad vastuse. Hetkel on eestikeelset materjali vealeidmispreemiaga seotud teemade kohta vähe, kuna tegemist valdkonnaga, mis on alles viimaste aastate jooksul rohkem populaarsust koguma hakanud.

Töö on jaotatud kolmeks suuremaks osaks: infosüsteemide turvalisus, turvalisuse tagamine ning intervjuud ja tulemused. Esimene, infosüsteemide turvalisuse peatükk käsitleb lühidalt infosüsteemide tutvustust, selle ajalugu ning kuidas infosüsteemid, ka nende turvalisus, ülejäänud tööga seotud on ja miks nendest teemadest kirjutamine oluline on. Teine, turvalisuse tagamise peatükk tutvustab erinevaid turvaaukude leidmise viise ning seejärel käsitletakse töö kõige olulisemaid teemasid: eetilist häkkimist, vealeidmispreemiaid, nendega seotud probleeme ning vealeidmispreemiate tasusid. Kolmas peatükk, intervjuud ja tulemused, käsitleb intervjuude metoodikat ning analüüsi, mis on saadud valdkonnaga tegelevate ekspertide intervjuusid terviklikuks tekstiks kokku kirjutades, võttes kõikidest intervjuudest kõige olulisema informatsiooni. Käesoleva töö lisades on intervjuude küsimused ning bakalaureusetööga kaasnev kohustuslik litsents.

1. Infosüsteemide turvalisus

Käesoleva töö peamiseks fookuseks on vealeidmispreemia programmid (ingl *bug bounty programs)* ja eetiline häkkimine (ingl *ethical hacking)*. Nende tähtsuse mõistmiseks on vaja mõista infosüsteemide olemust ja turvalisuse olulisust. Turvalisuse ehk kaitse tähtsuse illustreerimiseks on oluline tunda ka rünnaku erinevaid tüüpe ja häkkerite mõttemaailma.

1.1 Infosüsteemide ajalugu ja levik

Infosüsteem on organisatsiooni informatsiooni kogum, mille eesmärgiks on andmeid koondada ja töödelda, et muuta kasutajate töö lihtsamaks [2]. Infosüsteemid on enamik inimeste igapäevaelus järjest tähtsamal kohal. Infosüsteemide suur levik on seotud sellega, et järjest rohkem on inimesi, kellel on nii eraelus kui ka töökeskkondades arvutid ja nutitelefonid ning ligipääs internetile.

Leally artikli alusel hakkasid infosüsteemid tekkima 1950. aastatel. Nende eesmärgiks oli arvete ja palgaarvestuse töötlemine. 1960. aastatel laienes infosüsteemide funktsioon. Kasutusele võeti üldotstarbelised arvutusseadmed ning nende abil olid infosüsteemid võimelised täitma varieeruvamaid ülesandeid. 1970. aastatel mängisid infosüsteemid tähtsat rolli ettevõtte otsustusprotsessi efektiivsuse suurendamisel. 1980. aastate lõpus omasid paljud organisatsioonid infosüsteeme. Need olid muutunud oluliseks strateegiliseks teabeallikaks, mis aitasid ettevõttel oma eesmärke edukalt saavutada [3].

Infosüsteemid on inimesi ümbritsenud aastakümneid ning on siiani pidevas arengus. Nende tähtsus on tõusnud, kuna praeguseks on paljudel inimestel enda kohta kriitilist infot suurte asutuste süsteemides. Inimeste kohta käiva teabe hoiustamine suurendab vajadust infosüsteeme kaitsta.

1.2 Süsteemide turvalisus

Infoturbe põhikategooriad (ingl *CIA triad*, edaspidi CIA kolmik) on konfidentsiaalsus (ingl *confidentiality*), terviklus (ingl *integrity*) ning käideldavus (ingl *availability*). Lühend CIA tuleneb kolmiku inglise keelsetest nimetustest. CIA kolmikut kasutatakse infoturbega seotud mõistete arutamiseks. Euroopa Liit on andmetöötlejatele ette määranud kohustuse jälgida erinevaid turvameetmeid, et tagada turvalisus kõigis kolmes kategoorias [4]. Kui üks kolmest põhikategooriast on täitmata, siis ei saa süsteemi pidada turvaliseks.

CIA kolmiku mõistete kirjeldamisel lähtutakse Eesti infoturbestandardi seletavast sõnaraamatust [5].

- **Käideldavus** on teabe, IT-süsteemide, inimeste, protsesside teovõime ja kättesaadavus volitatule siis, kui ta neid vajab.
- **Terviklus** on lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust.
- **Konfidentsiaalsus** on teabe omadus olla kättesaamatu või paljastamatu volitatamata isikutele ja protsessidele.

1.3 Rünnakute tüübid

Rünnaku tüüpide kirjeldamisel lähtutakse peamiselt raamatust “Foundations of Information Security” [6]. Rünnakute liikide vaheline piir ei ole selge. Mõned rünnakud võivad kuuluda ka mitmesse erinevasse kategooriasse. Samuti ei pruugi rünnakutel olla ühte kindlat mõju, vaid see võib erineda. Kõik rünnakud saab üldiselt liigitada neljaks: infopüük (ingl *interception*), katkestus (ingl *interruption*), modifikatsioon (ingl *modification*) ja võltsing (ingl *fabrication*). Kõik neli mõjutavad vähemalt ühte põhimõistet CIA kolmikust.

1.3.1 Rünnaku tüüpide kirjeldused

Infopüügi tüüpi rünnakud võimaldavad autoriseerimata kasutajal ligi pääseda ohvri andmetele, rakendustele ning keskkondadele. Infopüügi näideteks on pealtkuulamine ja ekraani piilumine [7]. Infopüük mõjutab CIA kolmikust peamiselt konfidentsiaalsust.

Katkestus on protsessi täitmise peatamine protsessivälise sündmuse toimel [7]. Katkestuse puhul muudetakse ohvri vara ajutiselt või jäädavalt kättesaamatuks. Katkestuse rünnakud mõjutavad CIA kolmikust peamiselt käideldavust, kuid võivad mõjutada ka terviklust.

Võltsingu tüüpi rünnakute puhul genereeritakse süsteemis andmeid, protsesse, vestluseid või muud sellega sarnanevat vara. Võltsingu rünnakud mõjutavad CIA kolmikust peamiselt terviklust, aga võivad mõjutada ka käideldavust.

Modifikatsiooni tüüpi rünnakud on seotud vara muutmisega. Näiteks failile autoriseerimata ligipääsemine ja selle sisu muutmine. Modifikatsiooni rünnakud mõjutavad CIA kolmikust peamiselt terviklust, aga võivad mõjutada ka käideldavust.

1.3.2 Näiteid rünnakutest

Katkestuse näiteks on lunavara (ingl *ransomware*) tüüpi kahjurvara (ingl *malware*). Üks suuremaid ja tuntumaid on Kaspersky andmetel 2017. aastal alguse saanud lunavara tüüpi kahjurvara nimega “WannaCry”. “WannaCry” oli lunavara, mis levis ettevõtte Microsoft operatsioonisüsteemi Windows arvutitel. Ohvri failid krüpteeriti, muutes need kättesaamatuks ning nendele uuesti ligipääsemiseks nõuti lunaraha, mida tuli maksta krüptovaluutas Bitcoin. Kaspersky artikli järgi ulatusid “WannaCry” tekitatud kahjud hinnanguliselt üle 4 miljardi dollari ning kahjurvara oli ligikaudu 230 000 arvuti peal [8].

Avatud veebirakenduste turvaprojekt (ingl *Open Web Application Security Project*) väljastab iga aasta artikli, kus on toodud välja kõige kriitilisemad veebirakendustega seotud turvariskid. Artikli järgi on 2021. aastal kõige suuremaks turvariskiks vigane pääsu reguleerimine (ingl *broken access control*). Pääsu reguleerimine jõustab poliitika, mille abil ei saa kasutajad tegutseda väljaspool neile määratud lubasid. Vead pääsu reguleerimises viivad kasutaja piirangutest väljaspool olevate äriliste funktsioonide teostamiseni, andmete hävitamiseni või autoriseerimata informatsiooni avalikustamise või muutmiseni. Vigase pääsu reguleerimise turvariski esines 94% artiklis testitud rakendustest ning selle eduka

ärakasutamise sagedus oli keskmiselt 3.81% [9]. Vigane pääsu reguleerimine on näide nii infopüügi kui ka modifikatsiooni tüüpide alla kuuluvast rünnakust.

Süsti rünnakud on olnud viimastel aastatel avatud veebirakenduste turvaprojekti artiklite järgi üheks suuremaks turvariskiks. 2017. aastal oli süst kõige suurem turvarisk. 2021. aastaks on see kukkunud kolmandale kohale [9]. Siiski on süsteemid järjest rohkem nende eest kaitstud, kuna on olemas tarkvarad, mis skaneerivad süsteeme süsti tüüpi rünnakute vastu. Nii on lihtsam leida süsteemis olevaid probleeme. Süsti rünnakud võivad kuuluda iga rünnaku tüübi alla. See oleneb rünnakust ja selle eesmärgist. Süsti rünnak võib olla võltsingu tüüpi, tekitades andmeid juurde. Võimalik on ka andmeid muuta, sellisel juhul on tegemist modifikatsiooni tüüpi rünnakuga. Andmetele saab ka teatud süsti rünnakutega ligi pääseda, seega oleks tegemist infopüügi rünnakuga. Võimalik on ka süsti rünnakutega süsteem täielikult hävitada. See kuuluks katkestuse tüüpi rünnaku alla.

Erinevaid rünnakute viise on palju ja neid tekib järjest juurde. Edukad sissetungid asutuste arvutisüsteemidesse, kasutades neid rünnakute viise, pole ebatavalised. Seetõttu on oluline teadvustada mis juhtub, kui ettevõte satub küberrünnaku ohvriks, saada aru turvalisuse tähtsusest ja tagada see.

1.4 Turvalisuse tähtsus

Turvalisus on tõusva tähtsusega, sest internetis isikliku info talletamine infosüsteemidesse teeb teatud toimingud ühiskonnas lihtsamaks. Kuna erinevate tarkvaralahenduste mõjul on kasvaval hulgal inimestest enda jaoks olulist informatsiooni kas internetis (pilveteenused, sotsiaalmeedia) või isiklikel andmekandjatel, saavad seda ära kasutada ka küberkurjategijad. Nende tegevuse tagajärjeks võib olla rahaline või varaline kahju. Kasutatakse kahjurvara, mis on programm, skript või muu kood, mis kahjustab või häirib infosüsteemi ja selle tööd, eesmärgiga koguda teavet, saada juurdepääsu või rünnata CIA kolmiku osasid [7]. Eric Dosal kirjutab, et kahjurvara ohustab kõiki asutusi. Lisaks inimeste küberhügieenile mõjutavad ka turvaaugud kahjurvara levikut [10]. **Turvaauk** on vara või meetme nõrk koht, mida saab ära kasutada üks või mitu ohtu [7].

Oht sattuda kahjurvara ohvriks on nii eraisikutel kui ka firmadel. Kirjandus on välja toonud, et võrreldes 2019. aastaga langes 2020. aastal kahjurvara tuvastus 12% (ülemaailmselt ning kõiki operatsioonisüsteeme arvestades). 2020. aastal oli kahjurvara tuvastusi kokku 111 014 261 [11]. Kahjurvara tuvastuste arv on suur ning see näitab, et palju inimesi on kahjurvarast mõjutatud. Kahjurvara tuvastuste arvu langemine võrreldes eelmise aastaga võib tähendada, et inimesed on teadlikumad ja arvutisüsteemid on parema turvalisusega, kuid ka seda, et kahjurvara kirjutajad on muutunud osavamaks ning neid on raskem tuvastada.

Pidev turvaaukude otsimine ning leidmine aitab vähendada turvaaukude kogust, millest ei ole tarkvara või süsteemi eest vastutavad firmad teadlikud. Heade küberturvalisuse tavadega ettevõtted saavad tegeleda teadaolevate turvaaukude parandamisega. Kui turvaauk pole neile teada, saavad kurjategijad seda vabalt ära kasutada. Paljudel tarkvara loovatel ettevõttetel on

aga probleem teadaolevate turvaaukudega: need jäävad pikaks ajaks parandamata ja neid kasutatakse rünnakutes. Aruandes jälgitud 2020. aasta esimese poole rünnakutes oli 80% kordadest ära kasutatud turvaauku, millest teavitati aastal 2017 või varem. Üle 20% kordadest oli turvaaugust teavitatud vähemalt seitse aastat (artikli kirjutamise ajast) tagasi [12].

2. Turvalisuse tagamine

Üleüldises ettevõtte korralduses ning tarkvara arendamise elutsüklis on etapid, mida peaks järgima, et tarkvara ja süsteemid oleks võimalikult turvalised. Turvalisuse tagamiseks tuleks tegeleda töötajate harimisega, standardite järgimisega, turvatestimisega ning riskianalüüsiga. Hiljem saab kasutada turvalisuse tagamiseks ka eetiliste häkkerite poolt pakutavat välist abi, kuid see eeldab, et süsteemid ja tarkvarad on juba kasutusel ning avalikust võrgust kättesaadavad.

Töötajatel peaksid olema firma poolt ettemääratud küberturvalisuse õppused, kus räägitakse erinevatest rünnakutest, headest tavadest, mida jälgida ning sellest, kuidas tuvastada õngitsemisründeid ja kuidas käituda neid avastades. Üldjuhul on kõige nõrgemaks lüliks turvalisuses just töötajad, mitte vigane (turvaaukudega) tarkvara. Aruande järgi on 77% andmeriketest (ingl *data breach*) põhjustatud töötajate inimlike vigade tõttu [13]. Andmerikked põhjustavad teabe hävimise või muutmise [7].

Standardite eesmärk on tõsta asutuste infoturbe taset. Lähtudes Riigi Infosüsteemi Ameti (edaspidi RIA) Rakendusjuhendist pakub Eesti infoturbestandardi etalonturbe meetod infoturbemeetmeid levinumate ohtude vastu, mis võivad organisatsioonile kahju tekitada. Eesti infoturbestandardi seletava sõnaraamatu kohaselt on etalonturbe metoodika Eesti infoturbestandardis kasutusel olev metoodika turbehalduse süsteemi rajamiseks ning infosüsteemide turbeks tüüpmeetmetega [5]. Kaitseks ohtude eest, mida etalonturbe meetodiga pole käsitletud, peab organisatsioon kasutama ka etalonturbe välist riskihaldust. Lisaks oma infoturbe taseme parandamisele saab auditeeritud ning standardiga vastavuses olev asutus kinnitada oma infoturbe taset partneritele ja klientidele [14].

Riskianalüüs on riski iseloomu ja riskitaseme väljaselgitamise protsess, mis loob aluse riski hindamisele ja riskikäsitlusele [5]. RIA andmetel viiakse IT-riskianalüüsi läbi seitsmes etapis. Esiteks kaardistatakse kriitilised tegevused, süsteemid ja ressursid. Kriitiliste tegevuste all mõeldakse teenuse pakkuja funktsioone, mis sõltuvad vähemalt ühest süsteemist ja mille puudumisel ei saa teenust osutada. Peale seda tuvastatakse süsteemi turvalisust ohustavad ohud ning seejärel nõrkused. Järgmisena leitakse ohtude realiseerumise tõenäosus. Siis hinnatakse tagajärgi ning antakse riskihinnang. Viimasena tuuakse täpselt välja riskihalduse viis. IT-riskianalüüsiga leitakse organisatsioonile, vastavalt selle riskitaluvusele ja strateegiale, sobiv riskihaldusmeetod [15].

Turvatestimise eesmärk on teha kindlaks, kas objekt (süsteem, komponent, toode, protsess vm) vastab turvanõuetele, ja tuvastada võimalikud nõrkused [7]. Riigi Infosüsteemi Ameti poolt on soovitatud igal ettevõttel teatud protsent oma tarkvara arendusele mõeldud eelarvest määrata turvalisuse testimisele. Uusi tarkvaralahendusi ei tohiks ettevõtted enne turvatestimisi käiku lasta [16].

Kõiki nendest etappidest tuleks teha pidevalt, mitte ainult üks kord. Eelnimetatud protsesse on võimalik teha enne tarkvara väljastamist. Kui tarkvara on kasutusel ja internetist

kättesaadav, on võimalik üles seada ka vealeidmispreemia programm. Sellest räägitakse lähemalt järgmistes peatükkides. Turvalisuse tagamiseks võib otsida süsteemidest ja tarkvaradest ka turvaauke. Järgmises peatükis käsitletakse viise nende leidmiseks.

2.1 Turvaaukude leidmise viisid

Turvaaukude otsimine on protsess, millega tegeletakse nii tarkvara loomise ajal kui ka peale tarkvara väljastamist. Näiteks leitakse uusi viise, kuidas süsteemi osasid manipuleerida. Võib ka tekkida ootamatuid muudatusi kolmanda osapoole pakkides, mida paljud süsteemid kasutavad. Need muudatused võivad olla pahatahtlikud või seada aimamatult kogu süsteemi ohtu. Turvaaukude otsimine ning nende silumine peab olema läbi tarkvara elutsükli pidevalt prioriteet. Olemas on erinevaid viise, kuidas turvaauke leida: koodi läbivaatus (ingl *code review*), skaneerimine, läbistustestimine, vealeidmispreemiad. On ka võimalus, et koodist leiab turvaauke inimene, kes juhuslikult tutvub varasemalt kirjutatud tarkvaraga.

Koodi läbivaatus ja koodi auditeerimine on kas teise ettevõtte töölise (kes ei ole originaalselt läbivaatuse all olevat koodi kirjutanud) või vastava palgatud isiku poolt koodi ülevaatamine, et leida erinevaid vigasid, kaasa arvatud turvaauke. Üldiselt on see tarkvara loovates ettevõtetes tavaline asi, mida tehakse, et veenduda koodi ootustele vastavuses.

Turvaaukude skaneerimine on tarkvaraga (näiteks ettevõtte Tenable tarkvara Nessus) automaatselt süsteemi otsimine, et leida lihtsamaid turvaauke võimalikult vähese vaevaga. See peaks olema turvaaukude otsimise jaoks esimene samm ning jääma pidevaks (iga teatud perioodi tagant), kuna muudatused süsteemis võivad tekitada uusi turvaauke.

Läbistustestimine on sissetungirünnete imiteerimine turvameetmete toimivuse kontrollimiseks, tihti süsteemi sertifitseerimistestimise osana [7]. Läbisustestimist võivad teha ettevõtte enda töötajad või teenust pakkuvad inimesed väljaspoolt ettevõtet. Läbistustestimise käigus otsitakse turvaauke. Leitud turvaaukude kogus ja mõju sõltub läbistustestimiste põhjalikkusest ning teostavate inimeste kogemustest ja teadmistest.

Turvalisuse tagamiseks on hakanud populaarsust koguma viisid, mis kaasavad eetilisi häkkereid süsteemide turvalisemaks muutmise protsessis. Järjest rohkem nähakse, et häkkerid võivad olla ka heatahtlikud spetsialistid, mitte küberkurjategijad ning nende abiga saab efektiivselt asutuse turvalisust parandada. Eesmärgiks on pidevalt kaitsta ja hoida ära uute meetoditega süsteemi kahjustamine. Järgmised peatükid keskenduvad eetilise häkkimise ning vealeidmispreemiate olemuse kirjeldamisele.

2.2 Eetiline häkkimine

Kirjanduse järgi on häkkimine tegevus, mille käigus üritatakse sisse murda või kahjustada võrke või digitaalseid seadmeid nagu nutitelefonid või arvutid. Häkkimine võib olla nii hea- kui ka pahatahtlik. Pahatahtliku häkkimise ajendiks võivad olla nii rahaline kasu kui ka protest millegi vastu või info kogumine. Häkkida võidakse ka lõbu pärast.

Häkkimiseks on erinevad meetodid. Näiteks võidakse kasutada botnette, mille abil on võimalik korraldada ummistusrünnakuid, tahtmatute hüpikakende avamiseks kasutatakse brauseri kaaperdamist, lunavaraga saab takistada süsteemi käideldavust [17].
Häkkimise võtteid ja tarkvarasid on palju, need on pidevas arengus.

Sonali Patil jt. sõnul kasutab eetiline häkkimine samu töövahendeid ja võtteid nagu tavaline häkkimine. Erinevus tuleneb sellest, et eetilistele häkkeritele antakse eelnevalt asutuse poolt luba. Eetilise häkkimise eesmärgiks on peamiselt süsteemide turvalisemaks muutmine [18]. Selle abil saavad huvilised tegeleda häkkimisega seaduse piirides. Osa eetilisest häkkimisest on vealeidmispreemia programmid, mis võimaldavad eetilistel häkkeritel turvaauke leides elatist teenida.

2.3 Vealeidmispreemiad

HackerOne artikli kohaselt on vealeidmispreemia (ingl *bug bounty*) rahaline tasu, mida antakse eetilistele häkkeritele, kes avastavad ettevõtte rakendusest turvanõrkuse ja teevad selle kohta edukalt aruande. Vealeidmispreemiad võimaldavad ettevõtetel jooksvalt parandada oma süsteemide turvalisust häkkerite abil [19].

Käesoleva töö autor on juhendajatega arutades võtnud kasutusele termini vealeidmispreemia, kuna andmekaitse ja infoturbe leksikoni poolt pakutud ametlik eestindus (puugipreemiajaht, puugioksjon) on liiga kohmakas ja raskendab olemuse mõistmist. Kinnitust, et termin on kohmakalt eestindatud saab sellest, et Google otsingumootori päringuga tuleb terminite “puugipreemiajaht” või “puugioksjon” vasteks alla 10 tulemuse ning küberturvalisusega seotud asutused, näiteks ka RIA, kasutavad oma aruannetes ning igapäevases jutus ingliskeelset terminit. Uus eestikeelne vaste on töösse toodud, et oleks võimalik mõistet paremini kasutada ja lootes, et nii hakkavad valdkonna eksperdid rohkem kasutama eestikeelset vastet ingliskeelse asemel.

Kirjanduse järgi kasutavad paljud ettevõtted enda tarkvara turvalisuse testimiseks teiste küberturvalisusega tegelevate ettevõtete läbistustestimise (ingl *penetration testing*) teenuseid. Selline lähenemine tähendab, et palgatud ettevõtte poolt määratud meeskond otsib turvaauke lühikese aja vältel ning teavitab nendest teenuse tellinud ettevõttele. Vealeidmispreemia programme kasutades tagab ettevõte, et erinevad turvalisuse spetsialistid (ehk eetilised häkkerid) otsivad pidevalt ettemääratud tarkvarast turvaauke pikema aja vältel. Turvaauke otsitakse ettevõtte süsteemidest nii pikalt, kuni vealeidmispreemia programm lõpetatakse. Vealeidmispreemia programmid on tõhus viis tarkvara turvalisuse pidevaks testimiseks [20]. Peale programmi lõppemist on tegevus illegaalne, kui ettevõte pole vastupidist väitnud.

Vealeidmispreemia programmid on hea viis eetiliste häkkerite ning organisatsioonide ühiste huvide täitmiseks. Esimeseks vealeimispreemia programmiks maailmas loetakse Netscape poolt 1995 aastal loodud projekti, kus auhinnaks lubati peamiselt ettevõtte meeneid [21]. Kirjandus toob välja, et vealeidmispreemia programmide vähendamine võib viia turvaauke

otsivad spetsialistid teistele turgudele või turvaaukude avalikustamiseni enne, kui vastav firma jõuab rakendada vajalikke turvameetmeid [22]. Turvaauke otsivaid inimesi on oluline premeerida, kuna ilma selleta võidakse leida illegaalseid võimalusi, kuidas häkkimisega raha teenida.

Ka Eestis on hakanud levima ideed riiklikul tasandil vealeidmispreemia programmi alustamise kohta. Digigeeniuses avaldatud artiklis räägitakse Eesti riigi plaanist lähiajal käivitada vealeidmispreemia programm e-Eesti jaoks, mida juhib Riigi Infosüsteemi Amet. Programm loodeti koostada eelmisel aastal (2021), kuid siiamaani Eestis riiklikku vealeidmispreemia programmi veel ei eksisteeri. Raul Rikki sõnul peaks vealeidmispreemia programm olema kõigi riiklike IT-majade ülene, sellega nõustuvad ka teised IT-majade esindajad [23]. Google otsingumootorist "Eesti riigi bug bounty" otsingu tulemusena ei leitud riikliku vealeidmispreemia olemasolu ega täpsustavat lisainfot selle jätkamise kohta.

Vealeidmispreemia programmid on oma olemuselt kasulikud nii eetilistele häkkeritele kui ka asutustele. Sellegipoolest võib nendes programmides osaledes kokku puutuda ka õiguslike probleemidega. Järgmises peatükis käsitletakse lühidalt, millest juriidiliste probleemid on põhjustatud ja millised abinõud nendest hoidumiseks on praeguseks loodud.

2.4 Õiguslikud probleemid

Bugcrowd toob välja, et kuna häkkimise vastased seadused nagu näiteks arvutikuritegude ja arvuti kuritarvitamise seadus (ingl *Computer Fraud and Abuse Act*) on loodud nii, et kõiki häkkereid peetakse pahatahtlikeks, siis on keeruline vealeidmispreemia programmidest osavõtjatel ning muudel eetilistel häkkeritel oma tööd ohutult teha. Kuniks seadused muutuvad on seaduseaukude silumiseks vaja luua legaalset abinõud [24]. Kirjandus toob välja, et pea neljandikul turvalisusega tegelevatest spetsialistidest on olnud probleeme juriidiliste ähvardustega või õigustoimingutega oma uurimuste käigus ning see on suur murekoht [25].

Bugcrowdi kohaselt võib disclose.io projekti pidada üheks legaalseks abinõuks. Disclose.io on avatud lähtekoodiga projekt, mille eesmärk on standardiseerida häid tavasid ja pakkuda seadusega seotud kindlustunnet heatahtlikele häkkeritele, kes soovivad tegeleda vealeidmispreemiate ja muude turvaaukude avalikustamise programmidega [26]. Üks suurimaid vealeidmispreemia programmide keskkond nimega Bugcrowd kasutab oma platvormil häkkerite kaitsmiseks disclose.io projekti abi. Teatud programmidel on "Safe harbor" märgis, mis aitab programmist osavõtjatel veenduda, et legaalseid probleeme ei teki.

2.5 Vealeidmispreemiate tasu

Vealeidmispreemiate summad varieeruvad suurel määral. Tasud sõltuvad mitmetest faktoritest. Näiteks sellest, kas projekt on avatud lähtekoodiga või mitte, asutusest ja nende küberturvalisuse harjumustest ning leitud turvaaugu mõju tasemest. Järgnevas peatükis on uuritud kolmest erinevast allikast pärinevaid vealeidmispreemia tasusid.

Zhou J. jt on kirjutanud, et enamik vealeidmispreemia programmides osalevaid inimesi (56.7%) teenivad sellega vähe (keskmiselt 100 dollarit). Ainult väike osa teenib üle 2000 dollari vealeidmispreemia programmidega tegelemise vältel. Asjaolu on tingitud sellest, et ühe vealeidmispreemia summa on sageli väike (keskmiselt 142.2 dollarit) [27]. Eelnevalt mainitud uurimuses on aga sihiks võetud avatud lähtekoodiga projektid. Nende põhjal ei saa kõige paremat ülevaadet kogu turust, kuna paljude suurte firmade, kes teevad vealeidmispreemia programme, lähtekood on suletud.

Alljärgnev materjal on refereeritud PCMag 2019. mai artiklist, mille kohaselt on ettevõtte Microsoft vealeidmispreemia programmist saanud 2012. aastal spetsialist Vasilis Pappas 200 000 dollarit. 2018. aastal oli ettevõtte Google suurim vealeidmispreemia 41 000 dollarit, ettevõtte Meta (varasemalt Facebook) sama aasta suurim preemia oli 50 000 dollarit. Platvormil HackerOne on teeninud Santiago Lopez kokku üle 1 000 000 dollari. 2018. aastal on kokku makstud vealeidmispreemia programmides osalenutele ettevõtte Verizon Media poolt umbkaudselt 5 000 000 dollarit, ettevõtte Microsoft poolt umbkaudselt 2 000 000 dollarit ning ettevõtte Google poolt umbkaudselt 3 400 000 dollarit. Ameerika Ühendriikide Kaitseministeerium maksis ühe kuu jooksul nende süsteemidest leitud turvaaukude eest 150 000 dollarit [28].

HackerOne artikli järgi oli 2021. aastal teavitatud 66 547. kehtivast programmiveast (ingl *bug*). Sama artikli kohaselt on vealeidmispreemiad jaotatud nende mõju järgi nelja erinevasse kategooriasse: kriitilise, kõrge, keskmise, ning madala mõjuga vealeidmispreemiad. Nendele vastavalt on jaotatud ka summad, mida programmi vigade eest makstakse. Summad on tõusutrendis. Võrreldes eelneva aastaga tõusis kriitilise mõjuga vealeidmispreemiate tasu mediaan 2500 dollari pealt 3000 dollari peale, hinnatõus oli 20%. Kõrge mõjuga vealeidmispreemiate tasu mediaan jäi samaks, olles 1000 dollarit. Keskmise mõjuga vealeidmispreemiate tasu mediaan tõusis 11% võrra 450 dollari pealt 500 dollari peale. Madala mõjuga vealeidmispreemiate tasu mediaan jäi püsima 150 dollari peale [1].

Häkkimise tähendus on muutumas üldisemaks ning suur osa küberkaitse valdkonna inimesi ei seosta seda enam kuritegevusega, kuna eksisteerib ka eetiline häkkimine ja vealeidmispreemia programmid, mis on populaarsust kogumas. Kaasa aitab ka hea tasustavus, milleks ei tule tegeleda ebaseaduslike asjadega. Vealeidmispreemiad aitavad tagada infosüsteemide turvalisuse ning see on vajalik, kuna infosüsteemid mängivad inimeste elus tänapäeval tähtsat rolli. Järgnevas peatükis intervjueeritakse eksperte, kes räägivad oma kogemusest vealeidmispreemiate jahtimisel ja eetilisest häkkimisest.

3. Intervjuud ja tulemused

Eelnevate peatükkide eesmärgiks oli anda vajalik taustinformatsioon selleks, et saada intervjuu tulemustest aru ning mõista nende tähtsust. Selles peatükis kirjeldatakse intervjuu metoodikat ja eesmärke, antakse lisainformatsiooni intervjuude kohta ning analüüsitakse tulemusi.

3.1 Metoodika

Kirjanduse kohaselt on poolstruktureeritud intervjuu kvalitatiivne intervjuu tüüp, kus intervjueerija toetub varem kokku pandud intervjuukavale. Ettevalmistatud küsimuste järjekorda võib muuta, kui intervjueeritav siirdub oma vastusega teema juurde, mille kohta kavatseti küsimusi esitada. Lisaks võib poolstruktureeritud intervjuu käigus küsida täpsustavaid küsimusi [29].

Adrianne Smithi artiklis on välja toodud intervjuu tüüpide erinevused. Uurimustöö intervjuud on poolstruktureeritud, sest võrreldes struktureeritud intervjuuga tagab see intervjueeritavale võimaluse laskuda detailidesse, või minna üle teemale, mille kohta küsimusi polnud, kuid mille arusaamad tulevad uurimisel kasuks. Lisaks saab mõista intervjueeritava tundeid ja hinnanguid sellel teemal. Samas aitab aga varem kokku pandud kava intervjuusid omavahel paremini võrrelda ning analüüsida kui struktureerimata intervjuus. Poolstruktureeritud intervjuu puuduseks on see, et intervjuu ei mõju nii loomulikult kui struktureerimata intervjuu ning intervjueeritav ei saa potentsiaalselt rääkida teemadel, mille kohta temal kõige paremad teadmised on või millest ta rääkida soovib [30].

Käesoleva uurimustöö jaoks on kasutatud poolstruktureeritud intervjuu tüüpi, kuna intervjueeritavaid on vähe ja kõigi ekspertiis, huvid ning kogemused erinevad vähemalt osaliselt. Intervjuude eesmärgiks on anda ülevaade eetilisest häkkimisest ja vealeidmispreemiatest inimestele, kes on teemast huvitatud või soovivad selle valdkonnaga tegelema hakata. Intervjuudes on käsitletud teemasid, mis on peamiselt mõeldud inimestele, kellel on vähene teadmine valdkonnast või teadmine täielikult puudub. Intervjuudes küsitakse üldisemalt, kuidas inimestel tekkis soov eetilise häkkimise ning vealeidmispreemiatega tegelema hakata, mis on nende kogemus ja saavutused eelnevalt nimetatud valdkonnas ning mis probleeme võib kohata. Ülejäänud küsimused on erinevate spetsiifilisemate eetilise häkkimise ning vealeidmispreemiatega seotud teemade soovituste kohta.

Kuna käesolev töö on eesti keeles kirjutatud, siis intervjuu küsimused olid samuti koostatud eesti keeles. Neli intervjueeritavat olid eestlased, kuid üks intervjuu tehti ka inglise keeles. Inglise keelse intervjuu puhul tõlgiti küsimused inglise keelde intervjueerimise käigus. Tulemuste osas on intervjueeritava 3 tsitaadid töö autori poolt tõlgitud. Vealeidmispreemia kogemusega inimesi on eestis vähe ning paljud neist ei ole huvitatud intervjuude andmisest. Vealeidmispreemia kogemusega spetsialistide vähesuse ning võimalikult kvaliteetse informatsiooni saamiseks nii vealeidmispreemiatest kui ka eetilisest häkkimisest üldisemalt

pole kõik intervjueeritavad vealeidmispreemiatega tegelevad inimesed, vaid osad nimetavad ennast pigem eetilisteks häkkeriteks.

Kaks intervjueeritavat leiti turvalisusega tegelevatesse firmadesse kirjutades, ühe käesoleva uurimustöö juhendaja Alo Peets ning kaks juhendaja Margus Niitsoo abiga. Igale intervjueeritavale esitati viimaseks küsimuseks, et kas neil on soovitada kedagi, keda intervjueerida. Selle abil leiti lisaks üks intervjueeritav.

Järgnevalt kirjeldan kõiki intervjueeritavaid.
Intervjueeritav 1: Vabakutseline vealeidmispreemia programmidega elatist teeniv spetsialist. Tegelenud vealeidmispreemia programmidega umbkaudselt 10 aastat. Leitud juhendaja abiga.
Intervjueeritav 2: Pika küberturvalisuses töötamise ning eetilise häkkimise kogemusega spetsialist. Leitud juhendaja abiga.
Intervjueeritav 3: Küberturvalisuses üle 10 aasta töötanud spetsialist, kellel on olnud mitmeid kokkupuuteid eetilise häkkimise projektidega. Intervjueeritav on välismaalane, kuid elab Eestis.
Intervjueeritav 4: Küberturvalisuses töötav spetsialist umbes 5 aastase töökogemusega, kellel on kokkupuuteid vealeidmispreemia programmidega ning varasest east kokkupuude küberturvalisuse teemadega. Leitud intervjueeritava soovitusena.
Intervjueeritav 5: Üle 10 aastase kogemusega küberturvalisuses töötav spetsialist, kellel on palju kokkupuuteid vealeidmispreemia programmidega hobina. Leitud küberturvalisusega tegelevatesse ettevõtetesse kirjutades.

Järgnevas peatükis tuuakse välja intervjueeritavate kogemused ja soovitused, mis seonduvad peamiselt vealeidmispreemia programmide ja eetilise häkkimisega. Käsitletakse ka probleeme, mis antud tegevusalaga võivad kaasneda. Arutatakse ka tasusid ning intervjueeritavate arvamust vealeidmispreemia programmidest elatumise kohta.

3.2 Haridus, töökogemus ning esmased kokkupuuted

Kolmel intervjueeritavatest tekkis üleüldine huvi arvutisüsteemide vastu juba noores eas. Neist intervjueeritav 5 tegeles programmeerimisega ning intervjueeritav 4 tegeles teismeeas tarkvarade pöördkonstrueerimisega (ingl *reverse engineering*) Intervjueeritav 3 tegeles juba erinevate küberturvalisuse teemadega. Huvi nii üleüldiselt turvalisusega seotud teemade kui ka spetsiifilisemalt vealeidmispreemia programmide ja muudes vormides eetilise häkkimise vastu tekkis kahel intervjueeritaval täisealisena (umbes 20. aastaselt). Intervjueeritaval 1 tekkis huvi ülikoolis käimise ajal, intervjueeritav 5 ei läinud ülikooli, vaid asus juba noorest east ilma erialase hariduseta tarkvaraarendajana tööle. Kahe intervjueeritava karjäär algas tarkvaraarendaja ametis ning kõik intervjueeritavad on programmeerimises pädevad. Üks intervjueeritavatest läks ülikoolis käimise ajal küberturvalisusega seotud ametisse tööle ning lõpetas ülikoolis õppimise, see oli tema esimeseks ametiks.

Infotehnoloogiaga seotud kõrgharidus on ainult ühel intervjueeritaval. Ta omandas kõrghariduse alles peale aastaid tarkvaraarendajana töötamist. Intervjueeritav 2 ei avaldanud

oma haridust ning ülejäänud kolm on oma kõrghariduse omandamise pooleli jätnud. Infotehnoloogiaga, täpsemalt eetilise häkkimisega seonduv töökogemus on kõigil intervjueeritavatel. Anonüümseks jäämise eesmärgil ei saa käesolevas töös välja tuua intervjueeritavate täpseid ametikohti, kuid enamjaolt on nad vabakutselised või töötavad läbistustestijana küberturvalisusele spetsialiseerunud ettevõtetes.

3.3 Esimesed soovitused alustajale

Enne kitsamate küsimusteni minemist uuriti intervjueeritavatelt, kas neil on kõigepealt välja tuua üldisemaid soovitusi. Intervjueeritavad tõid selle küsimuse esitamisega välja info, mida nad tähtsaimaks pidasid ning kõikide intervjueeritavate nõuanded erinesid. Intervjueeritav 1 andis mitmeid spetsiifilisemaid soovitusi. Esimeseks neist oli valida üks kindel valdkond ning tutvuda sellega põhjalikult selle asemel, et omandada baasteadmised mitmes valdkonnas. Kuna konkurents on kasvav ja konkurentidel on samuti palju teadmiseid, siis ühele valdkonnale keskendumine suurendab tõenäosust leida turvavigasid. Teiseks soovituseks oli oma tööriistade, failiformaatide, suhtlusprotokollide ning operatsioonisüsteemi põhjalikult tundma õppimine. Kuna enamik neist on turvaaukude leidmisel iga kord kasutusel, siis nende põhjalikum tundmine kiirendab protsesse. Selle nõuandega oli seotud ka kolmas soovitus, milleks oli avatud lähtekoodiga tarkvara eelistamine. Kuna vabavara on tasuta ning see on alati saadaval, siis pole loova ettevõtte mõjutused nii suured. Neljandaks toodi välja, et vealeidmispreemia tasu üle ei peaks vaidlema. Teisalt intervjueeritav 5 väitis, et tasu üle võib vaielda juhul, kui asutus, kelle vealeidmispreemia programmiga on tegu, on valesti aru saanud turvaaugu mõjust (peavad viga väiksema mõjuga turvaauguks, kui see tegelikult on) või selle olemusest. Intervjueeritava 1 viimane soovitus oli, et enda edasi arendamiseks peaks õppima valdkonna ekspertidelt, näiteks uurima nende leitud turvaauke ja lugema nende tehtud blogipostitusi. Ka intervjueeritav 5 kasutab sotsiaalmeedia platvormi Twitter, et püsida kursis küberturvalisusega seonduvate uudistega ning teiste turvaspetsialistide tegevusega.

Intervjueeritav 3 andis soovituse, et alustamiseks oleks hea leida üks kindel valdkond, mis pakub huvi ning hakata sellega tegelema. Huvi ja tekkinud küsimused erinevate teemade kohta selles valdkonnas viivad edasi. Kui inimesel on huvi ja uudishimu, annab see motivatsiooni järjest rohkem õppida ja pädevamaks saada. Ka intervjueeritav 2 pani rõhku uudishimu olulisusele: “Võidab ikka see, kes ei saa hommikul kell 6 magada, kuna tal on konkreetne küsimus ja ronib arvuti taha vastuseid otsima.”

Intervjueeritavad 1, 4 ja 5 soovitasid programmeerimise ning tarkvaraarendusega tegeleda enne eetilise häkkimise ja vealeidmispreemiatega tegelemist. Tarkvara arendamine annab palju baasteadmisi. Nii saab tuttavaks vähemalt ühe programmeerimiskeelega, mida saab hiljem kasutada vajaminevate vahendite kirjutamiseks. Lisaks on tänu sellele lihtsam tegeleda pöördkonstrueerimise ning avatud lähtekoodiga projektidega. Paljud, kes on tarkvara arendamisega tegelenud saavad selle abil ka esmased kokkupuuted muude vajaminevate teemadega, näiteks võrgutehnoloogia ning andmebaasidega. Kokkuvõtlikult annab programmeerimise kogemus arusaama sellest, kuidas arvutisüsteemid töötavad.

Käesoleva lõputöö juhendaja Alo Peets soovitab eetilise häkkimisega alustada soovijatel lahendada ka CTF ülesandeid näiteks https://www.ctftech.com/ leheküljel ja tutvuda veebirakenduste turvalisusega OWASP WebGoat rakenduses. Lisaks on ka 60h jagu testitud eestikeelseid harjutusülesanded olemas Tartu Ülikooli andmeturve kursuse lehel https://courses.cs.ut.ee/2022/turve/spring/Main/Praktikumid.

3.4 Kindlad lähenemisviisid algajatele

Intervjueeritavatelt küsiti kitsam küsimus kindla lähenemisviisi kohta: “Kas tuleks eesmärgiks võtta üks kindel turvaauk, millest inimesel on põhjalik arusaam olemas ja käia läbi palju erinevaid süsteeme, et otsida, kas see turvaauk või süsteemiviga on nendes olemas või hoopis otsida palju erinevaid turvaauke ühest kindlast süsteemist?” Arvamused selles osas erinesid. Intervjueeritavad 1 ja 5 olid seda meelt, et ühest süsteemist tuleks otsida erinevaid turvaauke. Intervjueeritava 1 põhjendus oli, et väga palju läheb aega selleks, et ühte süsteemi tundma õppida, selle struktuurist aru saada. Intervjueeritav 5 tõi ka välja, et isegi kui ei leita sellest ühest süsteemist midagi, siis ollakse palju õppinud selle kohta, kuidas otsida erinevaid nõrkuseid. Samuti õpib nii nägema erinevat tüüpi vigade omavahelisi seoseid. Veel täpsemalt soovitas intervjueeritav 5 programmeerimise taustaga inimestel esimeste eetilise häkkimise kokkupuudete saamiseks uurida internetis olevaid veebirakendusi, see on tema jaoks loogiline koht alustamiseks.

Intervjueeritavad 3 ja 4 on seda meelt, et ühte turvaauku võiks paljudest erinevatest süsteemidest otsida. Intervjueeritav 3 ütles selle kohta: “See töö võib kohati olla väga frustreeriv. Näiteks kui sa püüad tundide viisi igati pidi masinasse ligipääsu saada ja mitte miski ei tööta, see protsess hakkab närvidele. Seega kui sa töötad mõne projekti kallal või sa soovid saada kogemust või midagi muud selle sarnast, siis sel juhul pean ma tõdema, et vähemalt minu ja paljude teiste jaoks, kellega koos ma töötanud olen, on sellises olukorras vaja veidi rohkem dopamiini vabastust töö ajal. Sa vajad edu tunnetuse faktorit, vajad võimet näha saavutuse poole progresseerumist oma töös. Eriti siis, kui oled alles alustamas, ei taha sa olla sellest kõigest heidutatud. Sa soovid saada nii-öelda madalal rippuvaid viljasid, ja neid võimalikult paljudelt okstelt. Sa soovid näha edu ja oma töö tulemusi samal ajal kui sa nende kallal vaeva näed. Peale seda võid sa alustada rohkem edasijõudnud meetodite ehitamist. Sa võid hakata katsetama uusi meetodeid ja protsesse, et süsteemidesse ligipääsu saada ja neid ära kasutada. Seega on minu soovitus see: minna paljude mitmete süsteemide järele, muidugi kõigi puhul luba omades ja eetiliselt, ning minna ühe kindla tehnika järele, seada sihtmärgiks just see, saada selles kindlas meetodis pädevaks, saada edu ja sellest saavutusest edasi liikuda.”

3.5 Õiguslikud probleemid

Juriidiliste probleemidega polnud ükski intervjueeritavatest kokku puutunud. Intervjueeritav 1 ja 5 soovitasid võimalusel rünnatava süsteemi endale privaatselt ülesse seada. See on võimalik avatud lähtekoodiga projektidega. Intervjueeritav 1 ütles selle kohta; “Teiste osapoolte production serveritega peab üsna ettevaatlikult ringi käima. Ideaalis õnnestub sama süsteem endal privaatse koopiana tööle saada, siis võib julgemalt testida” Samuti soovitasid

intervjueeritav 1 ja 5 tutvuda vealeidmispreemia programmi kirjeldusega. Tutvuda sellega, mis domeenidel ja milliste piirideni on lubatud minna turvaaugu ära kasutamisega. Intervjueeritava 1 ütles: “Kindlasti tasub läbi lugeda bug bounty reeglid, et mis on lubatud.”

3.6 Vealeidmispreemiate platvormid

Platvormide osas mainis intervjueeritav 1: “Alustajale ma arvan küll, et HackerOne on hea koht alustamiseks.” Samas ükski intervjueeritavatest ei toonud välja, et kasutaksid ise mõnda platvormidest aktiivselt. Intervjueeritav 1 tõi välja, et tema pole edasi liikunud vähestest vealeidmispreemia programmidest, millega ta on pikemat aega tegelenud. Intervjueeritav 5 ütles, et tal on siiski mõnes suures vealeidmispreemia platvormis kasutajad olemas, kuna teatud asutused teevad leidude eest makseid ainult nende platvormide vahendusel, isegi kui teavitada leiust asutuse enda keskkonnas. Intervjueeritav 5 soovitas omada kasutajaid kõikides suuremates vealeidmispreemia platvormides, kui inimesel on eesmärk leida endale vealeidmispreemia programme sellisel viisil. “Kõigis oleksid notificationid nii põhja keeratud kui võimalik, et hästi kiiresti saada teada igast uuest (programmist),” ütles intervjueeritav 5. Intervjueeritav 3 tõi välja, et olemas on ka suur kogus privaatseid vealeidmispreemia programme, mida platvormidelt ei leia. Ligipääsu saamiseks on vaja vealeidmispreemia maastikul head mainet ning tutvuseid. Üheks põhjuseks, miks osade asutuste vealeidmispreemia programmid on privaatsed on see, et ettevõtted ei taha endale mainet, mis on seotud sellega, et neil on enda turvalisuse tagamiseks ettevõtte välist abi vaja. Intervjuudes mainiti vealeidmispreemia programmide otsimise platvorme HackerOne ning Bugcrowd.

3.7 Aruande kirjutamine

Kõik intervjueeritavad peale intervjueeritava 2 olid samal meelel öeldes, et aruande kirjutamine on väga tähtis osa vealeidmispreemia protsessist. Intervjueeritav 1 ütles: “Jah, see on see kõige igavam, aga üsna oluline samm.” Öeldu kirjeldab autori arvates paljude spetsialistide meelestatust aruannete kirjutamise osas. Samuti tõi ta välja, et aruande kvaliteedist võib sõltuda vea leidmise eest saadud tasu. Intervjueeritava 3 soovitus, mida ta aruannete kirjutamise puhul kõige olulisemaks pidas on, et kui olla aruandega täielikult rahul, siis võiks ikkagi enne selle saatmist puhata ja aruande kallal töötamisest eemal olla ning alles siis aruanne ära saata. Intervjueeritav 5 ütles, et aruande kirjutamisel on lugejale edasi vaja anda kolm teadmist. Esiteks, kuidas viga uuesti esile tuua. Teiseks, mis on selle vea tagajärg ehk miks on halb, et selline viga süsteemis on. Kolmandaks, detailid nagu millises tarkvaras ja mis versioonis turvaauk esineb. “Kui lühikeselt sa suudad seda teha on juba sinu enda ja selle vea loomuse ja kõige muu sellise nii–öelda teema,” lausus intervjueeritav 5. Intervjueeritav 5 tõi ka välja, et tal on olnud aruandeid, mis on olnud 4-5 rida pikad. Samuti ütles intervjueeritav 1 aruande pikkuse kohta: “Tasub vältida ülearust mula, sest seda lugevatel inimestel pole tõenäoliselt palju aega.”

3.8 Vealeidmispreemiate tasu

Kuna rahast rääkimine on üldiselt paljudel inimestel teema, mida nad väldiksid, siis ainult üks intervjueeritav avalikustas palju ta umbkaudselt on teeninud. Anonüümsuse huvides ei

avalikusta töö autor käesolevas lõigus intervjueeritavate numbrit. Ühe intervjueeritava suurim tasu ühe turvaaugu eest on ligikaudu 10 000€. Tema keskmine sissetulek aastas vealeidmispreemia programmidest on umbes 15 000€, tegeledes sellega ainult väljaspool tööaega (hobina). Üks teistest intervjueeritavatest ütles: “Ise olen 10 aastat hakkama saanud. Praegu on konkurents suurem, aga bug bounty programme samuti rohkem. Parimad elavad vabalt ära. On ju juba täitsa mitu bug bounty miljonäri. Aga täitsa puusalt pakuks, et vähemalt iga teine, kes täna alustab ei ela sellega ära.” Intervjueeritav 3 tõi välja, et ta teab inimesi, kes töötavad ainult 3-6 kuud aastast. Nad teenivad vealeidmispreemia programmidega enda jaoks piisavalt raha ning seejärel tegelevad ülejäänud aastast töövälistе tegevustega. Intervjueeritav 5 rääkis, et lisaks vealeidmispreemiatele on tekkinud asutused, mis on küll liigitatud vealeidmispreemiate valdkonna alla, kuid ostavad turvaaukudest teavitamise ning kirjelduse asemel eksploidi vahendeid (ingl *exploit tool*), mis on ründevahendid kindla nõrkuse ära kasutamiseks. Eksploidivahendeid ostvad asutused maksavad suuri rahasummasid. Selle näiteks saab tuua platvormi Zerodium, mille veebilehel [31] on välja toodud, et tasud on vahemikus 2500 dollarit kuni 2.5 miljonit dollarit. Zerodium-i veebilehel on ka välja toodud, et peamised kliendid on riiklikud asutused. Pole avalikustatud, mis riikide ja ettevõtetega tegu on. Eetilisuse koha pealt on toodud välja, et Zerodium võtab seda tõsiselt, kuid eksploidi vahendite ostmine, kasutamine ning levitamine ei pruugi olla eetiline. Ettevõtte tegevuse eetilisus on kaheldav nii töö autori kui ka intervjueeritava 5 arvates, aga asutuse tegevus on siiski seaduslik.

3.9 Tööriistad

Intervjuus uuriti ka tööriistade kohta, mida intervjueeritavad kasutavad ja soovitavad vealeidmispreemiatega ja eetilise häkkimisega tegeledes. Intervjueeritav 3 ütles, et tööriistad, mida ta kasutab varieeruvad olenevalt projektist. Veebirakendustega töötades kasutab ta tarkvara nimega OpenVAS. Ta ütles ka, et operatsioonisüsteemi Linux erinevatest distributsioonidest, näiteks Ubuntu ja Kali Linux, leiab suure osa vajaminevatest tööriistadest. Kasutatavaks operatsioonisüsteemiks soovitasid kõik intervjueeritavad operatsiooni Linux ning sellel põhinevaid erinevaid distributsioone. Intervjueeritav 4 tõi välja, et veebirakenduste ja veebipäringutega seotud ülesannete jaoks kasutab ta tarkvara nimega Burp Suite. See on kõige laialdasemalt levinud tarkvara veebiturvalisusega seotud teemade jaoks. “See on de facto standard praegu põhimõtteliselt,” ütles intervjueeritav 5 tarkvara Burp Suite kohta. Pöördkonstrueerimise jaoks kasutavad mõlemad nii intervjueeritav 4 kui ka 5 tarkvara IDA Pro. Toodi välja, et populaarne on ka Ameerika Ühendriikide Riikliku Julgeolekuagentuuri poolt loodud tarkvara Ghidra. Ka intervjueeritav 1 soovitas tarkvara Ghidra. Palju kirjutatakse enda rakendusi ja skripte. Intervjueeritav 1 tõi välja üheks enda kasutatavaks tööriistaks programmeerimiskeele Python, samuti mainisid seda ka intervjueeritavad 3 ja 4. Intervjueeritav 5 ütles enda rakenduste ja skriptide kohta: “Eriti kui mingi *fuzzimist* või mingit sellist asja on, siis teiste tööriistad on see, et nad kõik kasutavad neid. Need leiavad ikka samu asju. Seega enda asju kirjutades on see, et sa saad parema kontrolli, parema ülevaate, asjad töötavad täpselt nii nagu sa nad kirjutad. Kui sa teed vigu, siis võib-olla mingil hetkel need vead on isegi kasulikud, sest nad leiavad mingeid kummalisi asju.” Sama teema kohta rääkis ka intervjueeritav 1: “Keerulised rakendused ei ole su sõbrad.

Tihti teevad need ikka midagi valesti ja kiirem on ise see 10-1000 rida pythonit kirjutada, et täpselt õige tööriist saada. Pluss nüüd sa tead täpselt kuidas see töötab juhuks kui midagi on muuta vaja.”

3.10 Töö vealeidmispreemiate kõrval

Intervjuudest käis läbi ka arutelu vealeidmispreemiatele ning eetilisele häkkimisele sarnaste tööde osas. Küsisin vabakutselisena eetilise häkkimisega tegelemise plusse ja miinuseid võrreldes mõnes küberkaitse valdkonna ametis, näiteks läbistustestimises töötamisega. Üks eelis ametlikult tööl käimise juures on kindel sissetulek. Seda mainisid intervjueeritavad 4 ja 5. Nad kõik tõid ka välja, et eriti alustades on suureks plussiks tööl käies kolleegid, kellelt saab õppida. Intervjueeritava 5 jaoks on vabakutselisena vealeidmispreemiatest osa võtmise eeliseks see, et vabadus on valida oma projekte, seega ei pea tegelema tööülesannetega, mis inimese jaoks võivad vähem huvitavad olla. Intervjueeritava 4 arvates on tööle minnes lihtsam alustada. Samuti ei teki sellisel juhul õiguslikke probleeme. Töötamise miinuseks tõi ta välja, et alustaval inimesel võib keeruline olla tööle saamine. Intervjueeritav 3 arvas, et tööl käimise kogemus tuleks kasuks juhul, kui tahta tulevikus millegi muuga tegeleda. Kuna tööl käies saab palju muid oskuseid peale tehniliste oskuste, siis juhul, kui on soov oma karjääri muuta, saab seda lihtsamini teha.

3.11 Stress ja läbipõlemine

Lisaks tehnilistele soovitustele tuli intervjueeritavtelt 1 ning 3 nõuanne stressitaseme reguleerimise ja läbipõlemise vältimise kohta. Intervjueeritav 3 rääkis sellest, et tööst läbipõlemine on üleüldiselt infotehnoloogia valdkonnas levinud. Intervjueeritav 5 oli ka sellega nõus, aga spetsiifilisemalt küberturvalisuse valdkonna osas. Intervjueeritav 1 tõi välja, et kuna ranged töötunnid puuduvad, siis oluline on leida tasakaal arvutis olemise ja muu elu vahel. Samuti ütles ta, et hea on pidada ergonoomikat silmas. Intervjueeritav 3 ütles, et kui töötada üleüldises küberkaitses, siis ametikohad on väga varieeruvad ja osades ametites on vaja võtta vastu rohkem otsuseid, osades on vaja rohkem inimestega suhelda ja osades ametites on tehnilised oskused esikohal. Vaja on leida endale kõige sobivam amet, kuna kõikide ametite stressitase ei ole sama. Intervjueeritav 5 soovitas leida hobisid, mis ei ole arvutiga seotud, mis on lihtsamad. Kõige rohkem soovitas ta hobiks mõnda spordiala, kuna see aitab stressitaset madalamal hoida pingelistel aegadel. Intervjueeritava 5 sõnul on kõige suurem stressiallikas vealeidmispreemia programmides see, kui ei ole kaua aega leitud ühtegi turvaauku, lõpuks leitakse midagi ning selgub, et keegi on sellest juba varem teavitanud.

3.12 Arutelu ja edasised küsimused

Nõuanded alustavatele huvilisele olid väga erinevad. Kindel küsimus selle kohta, kas tasub otsida ühte viga erinevatest süsteemidest või erinevaid vigasid ühest süsteemist näitas seda, kuidas spetsialistide seas pole ühte kindlat arvamust. Lähenemisviisid erinevad nii palju, et intervjuude põhjal on raske soovitada alustamise viisi, mis oleks kõigi spetsialistide arvates optimaalne.

Kolmel intervjueeritaval ei ole kõrgharidust, ühel on kõrgharidus ning üks ei avaldanud oma haridustaset. See näitab, et enamik intervjueeritavatest pole omandanud kõrgharidust. Intervjueeritavaid on vähe ning seetõttu ei saa tugevaid järeldusi teha, aga eetilise häkkimise valdkonna spetsialistide keskmist haridustaset uurides võib leida, et paljudel on lõpetamata kõrgharidus.

Stressitase on küberkaitse ning üldisemalt infotehnoloogia valdkonnas kõrge mitme intervjueeritava arvates. Igale inimesele ei pruugi sobida vealeidmispreemia programmidest osa võtmine sissetuleku teenimiseks. Puudub igakuine kindel sissetulek ning lisaks stressirohkele tööle ja vabadele tööaegadele võib läbipõlemine juhtuda kiirelt, kuna tööga seotud stressi tase on liiga kõrge. Tasub kaaluda läbistustestijana töötamist, kuna töö on valdkonnaga osaliselt seotud, kuid kaasnevad kindla töökohaga seotud plussid.

Käesolevas uurimustöös on toodud välja, et muu kirjanduse järgi on õiguslikud probleemid suureks murekohaks ning osad arvuti kuritegudega seotud seadused ei ole sobilikud tänapäevasele küberturvalisuse maastikule. Intervjueeritavatest pole mitte kellelgi olnud juriidilisi probleeme. Põhjuseks võib olla, et Eesti seadused on konkreetsemad. Samuti ei pruugi probleem olla nii suur kui algselt kirjanduse järgi tundub. Seda teemat tasub uurida. Õiguslike probleemidega inimesi, kes on nõus oma kogemusest rääkima, on aga keeruline leida, eriti Eestist. Lisaks ei või kirjandus üksinda anda piisavalt põhjalikku ülevaadet probleemist.

Vealeidmispreemiad on populaarsust kogumas, samuti on üldine küberturvalisuse olulisus suurema tähtsusega. Erinevaid teemasid, mida uurida selle valdkonnaga seoses on palju ja kasulikku materjali on vähe, eriti eesti keeles. Väärtuslikud on intervjuud spetsialistidega, kellel on erinevates eetilise häkkimise valdkondades kogemusi. Intervjueeritavate leidmine on aga keeruline, kuna inimesi, kellel on vajalik kokkupuude olemas ning on nõus teema kohta intervjuud tegema, on vähe.

Intervjueeritavad, kellel on piisav kokkupuude vealeidmispreemia programmidega olid arvamusel, et sellest sissetuleku teenimine on saavutatav piisavate teadmiste korral. Tasud suurenevad ning järjest rohkem inimesi on valdkonnas töötamas. Lisaks oleks huvitav uurida vastust küsimusele: “Kas valdkonna populaarsuse suurenemine ja muude eetilise häkkimisega seotud platvormide tekkimine võib muuta elatise teenimise lihtsamaks või vastupidi keerulisemaks?” Tulevikus saaks ka uurida detailsemalt platvormidest nagu Zerodium [31], mis eksploidi vahendite ostmisega tegelevad. Selgitada, kui eetilised on sellega tegelevate asutuste toimingud ning kuidas nende platvormide tegevus seaduse piiridesse jääb. Otsida inimesi, kellel on eksploidi vahendite loomise ning müümisega kokkupuuteid ja küsida nende kogemuste kohta.

Käesolevas töös on lühidalt toodud välja, et ka Eesti riigil on plaanis luua riiklik vealeidmispreemia programm. RIA-ga ühendust võttes oleks võimalik programmi kohta rohkem informatsiooni saada ja huvitavaid detaile välja tuua. Programmiga seotud artikkel [23] viitab sellele, et programm oleks pidanud käivituma juba eelneval aastal. Praeguseks on

programmi staatus teadmata ning kas RIA-l on endiselt plaan riiklik vealeidmispreemia programm luua või on otsustatud, et seda projekti ei viida lõpuni, ei ole teada.

Vealeidmispreemia programmid on suhteliselt uus lähenemine turvalisuse tagamisele ning valdkond on muutuses, pole välja kujunenud kindlaid tavasid. Tasud kõiguvad ning spetsialistid võtavad erinevaid lähenemisi turvaaukude otsimisele. Vealeidmispreemia programmide platvormi HackerOne artikli järgi langevad madala ning keskmise riski tasemega vealeidmispreemiate tasud. Tasude langemine viitab sellele, et spetsialistid hakkavad rohkem keskenduma kõrge riski tasemega preemiatele ning paljud madala taseme vead on leitavad skannerite abiga [1]. Turu muutumine võib kaasa tuua ka probleeme alustavatele inimestele, kuna madala taseme vead pole nii tasuvad ning kõrge taseme vigasid on liiga keeruline algajal avastada. Uurida saaks, kuidas turu muutumine spetsialiste ja eetilise häkkimise valdkonda mõjutab.

4. Kokkuvõte

Käesoleva töö eesmärgiks on pakkuda kasulikku informatsiooni vealeidmispreemia programmidest huvitatud inimesele, kellel on valdkonnast vähe teadmisi. Eksperte intervjueerides koguti mitmeid soovitusi erinevate aspektide kohta, mis võiks alustavat spetsialisti huvitada ning aidata. Teisalt on toodud töö alguses välja taustinformatsioon, mis aitab paremini mõista ekspertide juttu ning valdkonda üldisemalt.

Töö käigus valmis eestikeelne materjal valdkonnast, mille kohta on eesti keeles väga vähe kvaliteetset informatsiooni. Materjal tuleb kasuks kõigile, kellel on huvi valdkonna vastu või plaan sellega tegelema hakata. Peatükis 3.12 on arutatud teemade üle, mida tasub edasi uurida, kuid milleni käesoleva töö käigus ei jõutud või mida käsitleti vähe. Valdkonna kohta saab teha ka parema alustamiseks mõeldud õppematerjali, tekitades praktilise osa, mis näitaks kindlat viisi, kuidas oma esimeste turvaaukude avastamiseni jõuda. Täiendavate soovituste jaoks võiks intervjueerida rohkem eksperte, aga ajalise piirangu ning ekspertide leidmise raskuse tõttu polnud see käesoleva töö skoobis võimalik.

Paremat õppematerjali oleks võimalik koostada koostöös inimestega, kellel on valdkonnas kogemus olemas. Siis on materjali loojal parem ettekujutus sellest, mis infot alustavatel inimestel vaja on. Käesoleva töö autoril puudus tööd alustades varasem kogemus vealeidmispreemia programmide ja eetilise häkkimisega, kuid pärast töö koostamist tõusis tema huvi ja soov valdkonnaga edasi tegeleda.

Töö kõige raskemaks osaks oli intervjueeritavate leidmine. Eestist vajaliku kogemusega eksperte leida ja neid saada intervjuud andma on keeruline. Ülemaailmselt ekspertide otsimine on lihtsam, kuid selleks on samuti vaja leida platvormid, kust neid otsida, nendega ühendust saada ja seejärel motiveerima neid intervjuud tegema.

Intervjuud ekspertidega tegid aga töö huvitavaks ning ilma nendeta poleks käesolev töö õppematerjalina nii väärtuslik. Intervjueeritavate jutt üleüldiselt ning kõige rohkem nõuannete kuulmine ning analüüsimine, andis tööle autori arvates kõige suurema väärtuse nii temale endale kui ka kõigile alustavatele spetsialistidele.

5. Viidatud kirjandus

[1] Software Vulnerabilities Increase by 20% in 2021. HackerOne. 2021. https://www.hackerone.com/press-release/software-vulnerabilities-increase-20-2021 (05.05.2022)

[2] Klesman E. Ettevõtte Atemix töötajate infosüsteemiga seotud vajaduste kaardistamine. TÜ ühiskonnateaduste instituut. 2018. https://dspace.ut.ee/bitstream/handle/10062/60441/klesman_elina_2018.pdf?sequence=1&isAllowed=y

[3] Infosüsteemid lühidalt ja selgelt. Leally. https://leally.ru/et/word/informacionnye-sistemy-kratko-i-ponyatno-referat-opredelenie/ (03.05.2022)

[4] Gross O., Luht L., Maaten E., Neeme E., Rousku K., Vaks T. Riigi küberturvalisuse käsiraamat. Tallinn: E-riigi Akadeemia. 2020, lk 18-19. https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_EST.pdf

[5] Seletav sõnaraamat. Eesti infoturbestandard. 2021. https://eits.ria.ee/et/seletav-sonaraamat (07.05.2022)

[6] Andress J. Foundations of Information Security. San Francisco: No Starch Press. 2019, p. 4-10.

[7] Andmekaitse ja infoturbe leksikon. Cybernetica. https://akit.cyber.ee/ (07.05.2022)

[8] What is WannaCry ransomware? Kaspersky. https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry (12.12.2021)

[9] OWASP Top Ten. OWASP. https://owasp.org/www-project-top-ten/ (04.05.2022)

[10] Dosal E. Top 9 Cybersecurity Threats and Vulnerabilities - Compuquip. Compuquip. 2020. https://www.compuquip.com/blog/cybersecurity-threats-vulnerabilities (05.05.2022)

[11] State of Malware. Malwarebytes. 2021. https://go.malwarebytes.com/rs/805-USG-300/images/MWB_StateOfMalwareReport2021.pdf?aliId=eyJpIjoiYk9HZlJteG9cL2IzcktqM1UiLCJ0IjoiVWdJN1RHWTh0Vk1iTlQyWk5JTnhOQT09In0%253D

[12] Cyber attack trends: 2020 mid-year report. Check Point. 2020. https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/ (05.05.2022)

[13] ENISA Threat Landscape Report 2018. European Union Agency For Network and Information Security. 2019, p. 69. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/@@download/fullReport

[14] Rakendusjuhend. Eesti infoturbestandard. 2021. https://eits.ria.ee/et/versioon/2021/juhendid/rakendusjuhend/ (04.05.2022)

[15] IT-riskianalüüsi koostamise juhend. Riigi Infosüsteemi Amet. 2018, lk 5-14. https://www.ria.ee/sites/default/files/content-editors/KIIK/riskianaluusi-koostamise-juhend.doc

[16] Olukorrast digiriigis. RIA veebikonverents. 2021, ~23 min. https://www.facebook.com/watch/live/?ref=watch_permalink&v=622741812313548 (09.05.2022)

[17] Hacking definition: What is hacking? Malwarebytes. https://www.malwarebytes.com/hacker (04.05.2022)

[18] Patil S., Jangra A., Bhale M., Raina A., Kulkarni P. Ethical Hacking: The Need for Cyber Security. *ICPCSI*. Chennai: IEEE, 2017. https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/stamp/stamp.jsp?tp=&arnumber=8391982

[19] What Are Bug Bounties? How Do They Work? [With Examples]. HackerOne. 2021. https://www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples (04.05.2022)

[20] What is Bug Bounty? Hacken. 2018. https://hacken.io/education/what-is-bug-bounty-bug-bounty/ (04.05.2022)

[21] Netscape Announces “Netscape Bugs Bounty” With Release of Netscape Navigator 2.0 Beta. Netscape. 1995. https://web.archive.org/web/19970501041756/http://www101.netscape.com/newsref/pr/newsrelease48.html (10.05.2022)

[22] Ring T. Why bug hunters are coming in from the wild. *Computer Fraud & Security*. Elsevier B.V., 2014, p. 16-20.

[23] Liive R. Riik hakkab olulistest IT-turvanõrkustest teavitajatele raha maksma. *Digigeenius*, 2021. https://digi.geenius.ee/eksklusiiv/riik-hakkab-olulistest-it-turvanorkustest-teavitajatele-raha-maksma/ (04.05.2022)

[24] Protecting hackers (by default) with disclose.io. Bugcrowd. 2018. https://www.bugcrowd.com/blog/protecting-hackers-by-default-with-disclose-io/ (04.05.2022)

[25] Gamero-Garrido A., Savage S., Levchenko K., Snoeren A. C. Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research. University of California. 2017. https://cseweb.ucsd.edu/~snoeren/papers/dmca-ccs17.pdf found from: Hamper R. Software bug bounties and legal risks to security researchers. University of New South Wales. Faculty of Law Masters thesis. 2020. https://unsworks.unsw.edu.au/entities/publication/603c7b44-138d-4178-8162-d9776a765a13

[26] Disclose.io and Safe Harbor. Bugcrowd. https://docs.bugcrowd.com/researchers/reporting-managing-submissions/disclosure/disclose-io-and-safe-harbor/ (04.05.2022)

[27] Zhou J., Wang S., Zhang H., Chen T., Hassan A. E. Studying backers and hunters in bounty issue addressing process of open source projects. *Empirical software engineering* 26, article nr. 81, Springer Nature, 2021, p. 2.

[28] Griffith E., Kucharski K. 7 Huge Bug Bounty Payouts. PCMag. 2019. https://www.pcmag.com/news/7-huge-bug-bounty-payouts (04.05.2022)

[29] Lepik K., Harro-Loit H., Kello K., Linno M., Selg M., Strömpl J. Intervjuu. Tartu Ülikool. 2014. https://samm.ut.ee/intervjuu (04.05.2022)

[30] Smith A. Differences Between Structured, Unstructured and Semi-Structured Interviews. Comeet. 2019. https://www.comeet.com/resources/blog/structured-unstructured-semi-structured-interviews (04.05.2022)

[31] Zerodium. https://zerodium.com/ (09.05.2022)

6. Lisad

I. Intervjuu küsimused

Intervjueeritav jääb kõikide intervjuude puhul anonüümseks. Olenevalt sellest, millises keskkonnas intervjuud tehakse, võin mina (uurimustöö kirjutaja, Mark Robin Kalder) ning minu juhendaja Alo Peets intervjueeritava identiteeti teada, kuid uurimustöösse seda kuhugi kirja ei panda, kui just selleks soovi ei avaldata. Intervjueeritav saab soovi korral enne uurimustöö valmimist ja puhtandi esitamist vaadata töö üle ja veenduda, et tema identiteeti seal pole ning kontrollida, et ühtegi ebasobilikku vastust ei jääks töösse.

1. Kuidas teil tekkis idee *bug bounty*'dega tegelema hakata?

2.Milliseid üldiseid soovitusi annaksite te inimestele, kes plaanivad *bug bounty* programmidega alustada?

3.Mis olid esimesed turvaaugud, mille eest saite *bug bounty* programmi raames tasu? Millised on aja jooksul olnud kõige huvitavamad?

4.Mis *bug bounty'*ga/häkkimisega seonduvates ametites olete töötanud? Kas teil on sellega seonduvat haridust? Kas olete mujalt kogemusi ja teadmisi saanud? Milliste valdkondadega (näiteks: programmeerimine/tarkvaraarendus, AI, süsteemihaldus, võrgutehnoloogia, jm.) olete te tuttavad, millistes pädevad, millised nendest teie arvates kõige olulisemad on?

5.Kui palju sellest oli enne esimestest *bug bounty* programmidest osalemisest, kui palju on teie arvates vaja enne programmidest osa võtmist ning millised oskused (ja valdkonnad) on teie arvates kõige kasulikumad?

6.Mida peaks silmas pidama, et vältida õiguslikke probleeme, jääda legaalsuse piiridesse? (Valikuline: kas teil on olnud *bug bounty* programmidega seoses seadusega probleeme?)

7.Kui palju olete umbkaudselt *bug bounty* programmidega kokku teeninud? Kui reaalne on *bug bounty* programmi preemiatest ära elatumine? Mis on teie suurim *bug bounty* preemia?

8.Milliseid tööriistu (tarkvarad, operatsioonisüsteemid) te kasutate *bug bounty*'dega tegeledes? Milliseid te soovitate?

9.Kuidas võiksid algajad teie arvates programmidele läheneda, kas mõistlikum oleks otsida ühte turvaauku paljudest erinevatest süsteemidest või erinevaid turvaauke ühest süsteemist?

10.Mis platvorme te kasutate, et *bug bounty* programme leida, milliseid soovitaksite *bug bounty*'ga alustavale inimesele (nt. HackerOne)? Kuidas valite platvormidelt programme, kas on oluline vältida või eelistada programme, milles on teatud asju kirjelduses märgitud?

11.Kas te soovitaksite alustada *bug bounty* programmidega eraisikuna või mõnda firmasse tööle minnes, mis tegeleb *bug bounty* programmide või läbistustestimisega?

12.Mis on teie arvamus *bug bounty* programmidest ja läbisustestimisest eraldiseisva isikuna (firma poolt tellitud töö ainult ühele inimesele). Mis on ühe või teise plussid ja miinused? Kas on veel mõni formaat eetilisest häkkimisest, millega on kokkupuuteid olnud?

13.Kui suur oluliusus on *bug bounty* programmides turvaaugu leidmisel aruande kirjutamine? Kas teil oleks anda nõuandeid, asju mida silmas pidada, kui pole varem aruandeid kirjutanud, kust võiks leida häid näidiseid?

14.Kas on midagi veel, mida *bug bounty* kohta tahaksite rääkida/soovitusi anda? Kas peaksin veel midagi küsima?

15.Kas teil on veel mõni inimene, kellega soovitaksite mul rääkida sel teemal?

II. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Mark Robin Kalder**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose "Vealeidmispreemia programmid ja eetiline häkkimine", mille juhendajad on **Alo Peets** ja **Margus Niitsoo**, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Mark Robin Kalder

10.05.2022