Kevin Mitnick - umijeće hakiranja

Cvrtnjak, Domagoj

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
akademska godina, 2021./ 2022.

Domagoj Cvrtnjak

Kevin Mitnick – umijeće hakiranja

Završni rad

Mentor: Vjera Lopina, dr.sc.

Zagreb, rujan 2022.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Domagoj Cvrtnjak

_____

(potpis)

Sadržaj

1. Uvod

Jedno od obilježja suvremenog doba je i da većina ljudi ima osobno računalo, a statistički podaci govore o 6 milijardi korisnika interneta do 2022. godine. Dio takvog doba su i hakeri. Što oni predstavljaju u našem dobu? Kakva je njihova uloga virtualno, ali i u svakodnevici? Postoji li skeptičnost prema hakerima zbog toga što im je u središtu zanimanja informacija? Kuda ide tehnologija? U središtu takvih pitanja su upravo hakeri koji ih na svoj način i propituju, a koja su i autora potaknula na pisanje prvog dijela ovog završnog rada. Ta se pitanja počinju propitivati definicijom i vrstama hakera, zatim kratkim povijesnim pregledom hakerstva uz dio o novijem hakerstvu. Teorijski dio daje pregled različitih mišljenja o gore postavljenim pitanjima te opisuje hakere na različite načine i daje određene odgovore. Slijedi dio u kojem se opisuje hakerska motivacija, primjeri stvarnih osoba hakera i hakerskih djelatnosti, uz napomene o nekim od metoda sprječavanja. To je zapravo prijelaz u drugi dio rada koji se bavi hakerom Kevinom Mitnickom. Kevin Mitnick sinonim je za osobu hakera. Brojne metode i tehnike hakiranja kojima se on koristio prije dvadesetak godina aktualne su još i danas, a svoje znanje dijeli i proširuje surađujući s kompanijama za internetsku sigurnost. Mitnick se bavi i cyber napadima koji su aktualni i još jedan razlog pisanja rada. Čitajući članke i knjige o hakiranju, koristeći se ponajviše Mitnickovim knjigama, kroz njegove primjere i neke od primjera općenito o hakerstvu dati će se doprinos boljem razumijevanju hakerstva.

2. Hakeri

2.1. Pojam hakera

Postoji više definicija o tome tko su hakeri. Najopćenitija je da su to osobe vješte u informacijskoj tehnologiji koje koriste svoja tehnološka i tehnička znanja da bi savladali tehnološku prepreku na nestandardne načine. Hakeri često s entuzijazmom proučavaju hardver i softver, kompjuterske sustave i programski kod, ali upadom u zaštićene računalne sustave uglavnom ne čine štetu, već žele proširiti svoje znanje. To ih razlikuje od crackera, na primjer black hat hakera, koji upadom u računalne sustave ipak imaju određenu namjeru za nanjeti štetu.

2.2. Vrste hakera

Osnovni tipovi hakera mogu se razvrstati na hakere, to jest one koji proučavaju i nastoje unaprijediti računalne sustave i crackere, to jest one koji neovlašteno provaljuju u računalne sustave. U članku Smitha i Ruppa (2002, 179. str.) dato je nekoliko klasifikacija hakera. Prva je Landrethova studija u kojem se spominje novak, student, turist, rušitelj i kradljivac. Novak ima najmanje iskustva, student je naprosto student, turist osjeća zabavu kod hakiranja, rušitelj čini štetu na sistemu, a kradljivac profitira od vlastite djelatnosti. Druga je Hollingerova klasifikacija koja piše o piratima, browserima i crackerima. Pirati čine štetu nad autorskim pravima, browseri prikupljaju dokumente dok crackeri su tehnički najsofisticiraniji. Treća je Chantlerova klasifikacija koja hakere smješta u elitu (eng. *leet*) koja čini trideset posto i koja je najbolji poznavatelj hakerskih vještina, šezdeset posto čine neofiti koji aspiriraju na elitu i posjeduju solidno znanje, dok deset posto čine takozvani „šepavci“ s najslabijim poznavanjem hakerskih tehnika. Novija istraživanja svrstavaju hakere u trinaest skupina: novake, studente, srednje potkovane cyberpunkove, skriptaše koji uče iz alata, staru gardu koja obuhvaća white hatove i često radi u sigurnosnoj industriji, insidere, kradljivce, profesionalce, državne hakere koji obavljaju najviše sigurnosne poslove ili istrage, haktiviste, pirate, hakere u grupama i posrednike u kriminalu. Postoji još i distinkcija koju je učinio Skibell (2002, 353.str.) na outsidere koji obavljaju aktivnosti s udaljenih računala i insidere koji su uglavnom ljudi iz tvrtki, ponekad i bivši zaposlenici koji mogu učiniti štetu na sustavu. Može se još navesti klasifikacija na civilne, državne, nedržavne i protudržavne hakere. Zadnja prisutna je razlika po bojama. Tako osim već spomenutih white hatova, postoje black hatovi, odnosno prema

Raymondovom rječniku (1996, 63.str.): "*Netko tko teži prodrijeti u sistem koji se štiti*." Ovdje su još blue hatovi, ljudi iz sigurnosnih firmi i grey hatovi koji žive između legalnih i ilegalnih radnji.

2.3. Povijest

Moderno hakerstvo pojavljuje se prema Thomasu (2002, 144. str.) kasnih 1950-ih godina te u ranim 60-im, a tada postojeći hakeri koristili su se raznim prečicama kako bi proširili svoje performanse i performanse na računalima. Za današnje pojmove riječ je o zastarjelim računalima čija se složenost brzo povećavala zahvaljujući i hakerima. Tako su se hakeri često služili tehnikom „uradi sam" slažući nove dijelove hardvera ili tražeći različite putove kako izmisliti softverske komponente ili ubrzati prolazak računalnim sučeljima. Jedan od primjera prvih modernih hakera su inovatori sa Sveučilišta MIT koji su, osim fakultetskih aktivnosti, preostalo vrijeme uglavnom provodili baveći se računalima što je rezultiralo brojnim novitetima u računalnoj tehnologiji. Neke od značajki hakerstva pokazuju i članovi Homebrew Computer Cluba djelujući u sedamdesetima, zaslužnih za revoluciju u računalnim mikrokomponentama što dobro opisuje Levy (2010, 201. str.). Ti hakeri su uglavnom imali mišljenje da informacija želi biti slobodna, a Himanen (2002) u svojoj knjizi piše da je hakerska svrha utilitarnost. Prema Teoriji Kennedy (2015) određeni ljudi još iz srednjega vijeka prepisujući i tiskajući tekstove i dokumente zalagali su se za širu dostupnost informacija pokazujući neke sličnosti s modernim hakerima. Modernim su hakerima ideali bili decentralizacija i nelimitiranost, a svoje su aktivnosti smatrali umjetnošću na računalu. Navedeni hakeri samo su jedan od tipova hakera u postmodernom dobu. Tako možemo pisati o četiri generacije hakera. Prvu, već opisanu koju je činila ponajviše adolescentska generacija zanimajući se za programske i programerske tehnike. Generaciju osamdesetih, drugu generaciju, inspiriranu filmom *WarGames* koji je romantizirao hakiranje, zaokupio je računalni hardver. Treću generaciju s početka devedesetih privukle su računalne igre, a prijelaz za četvrtu generaciju je *Morrisov crv* koju čine i hakeri koji ulaze u druga računala. Postmodernu, dakle obilježavaju svi ovi hakeri objedinjeno, ali čiji se djelokrug podosta disperzirao.

2.4. 2010. – 2022. godina

U posljednjih desetak godina kao što je napisano, spektar hakerskih aktivnosti se proširio, a i mjere sprječavanja hakerskih napada također. Primjer su problemi sa softverom u automobilima koje hakeri mogu koristiti za daljinske napade. Nadovezujući se na to, obrnuti primjer je Uber koji je tako koristio Greyball, softver kojim je sakrivao aktivnosti protiv zakonodavstva. Udar na zakonodavstvo čini i softver Zenefit koji lažira 52 satni tečaj za brokere. Zakonodavstvo poduzima korake, a jedan od njih je i Mišljenje 477 kojim odvjetnici mogu slati samo kriptirane e-mailove klijentima. Posljedice na relaciji hakerski napadi - sigurnosne metode pokazuje slučaj Yahooa koji je otkupljen od Verizona po manjoj cijeni zbog cyber incidenta iz 2014. godine (Trope i Hantover, 2017, 228. str.). Jesu li svi ovi izvještaji pokazatelj etičke krize u cyber svijetu ovog razdoblja, djelomične histerije ili pak borba hakera i sigurnosne industrije oko interesnih sfera, pokušat će se između ostaloga objasniti u sljedećem poglavlju.

2.5. Teorija

2.5.1. Društveni aspekti hakerstva

Postmoderni hakeri nalaze se unutar informacijskoga društva, a računala i mreža su medijatori uz koje ostvaruju konstrukt svojeg online identiteta. Njihove računalne aktivnosti pomažu im u ostvarivanju kolektivnog imaginarija. Prema Jordanu i Tayloru (1998, 758.str.) aspekte hakerskog imaginarija čine: tehnologija, tajnovitost, anonimnost i fluidnost članova. Dakle, riječ je o neformalnim skupinama gdje su promjene brze i česte. U mrežnom okruženju ostvaruju interakciju s drugim socijalnim grupama koje im označuju navedene osobine, ali ponekad stvaraju i stereotipe. Tako se odvija stalna konstrukcija i rekonstrukcija online društava. Kada se pak piše o pojedinoj osobi hakera, postati od početnika vještim hakerom objašnjava Beverenov model hakerskog razvitka (Chng, Yu Lu, Kumar i Yau, 2022, 2.str.). Beverenov model je teorija koja piše da je za početak potreban kvalitetan hakerski softver i hardver. Kroz te komponente haker se osposobljava, počinje obavljati sve teže zadatke i raste mu znatiželja. U duljem periodu razvija nit vodilju ili tok koji ga vodi k sve složenijim računalnim djelatnostima. Druga je pak Bandurova teorija socijalnog učenja u kojoj haker usvaja kroz računalne aktivnosti drugih hakera ili naprosto provodeći vrijeme s njima, njihove

i vlastite vještine. Tako hakeri međusobno uče i povezuju se u prije spomenute grupe te ih potiče razložna akcija i planirano ponašanje u ostvarivanju određenih ciljeva.

2.5.2. Razlika između cyber i općenitog kriminala

Kad je riječ, na primjer, o grupama hakera cyber kriminalaca upravo su te osobine one u kojima pokazuju sličnosti s tradicionalnom mafijom. No, dok tradicionalnu mafiju obilježavaju čvrste strukture i hijerarhija, hakeri cyber kriminalci neovisniji su u grupama, često se čak niti ne poznaju izvan virtualnog, moć među članovima je gotovo jednaka, ali je struktura morfičnija te labavija (Smith, 2015, 107.str.). Računalne mreže im omogućuju široku rasprostranjenost, nalaze se na raznim lokacijama te su im napadi automatizirani i bez direktnog kontakta (Glodstone, 2001, 1.str.), poticani uglavnom novcem ili nekom vrstom trofeja. Takve hakerske grupe većinom nemaju mnogo menadžera, a kao posrednici im mogu poslužiti takozvane mule – pomoćnici , često ljudi koji nisu hakeri, a koji im pomažu sakriti novac. Iako su takve grupne strukture labave, vidljivo je da su sve složenije i raznolikije.

2.5.3. Hakerska etika

Isto je i sa složenošću hakerske etike u kojem su takve grupe jedan od sudionika i koje uz industriju računalne sigurnosti takvo pitanje i pokreću. Pitanje hakerske etike je delikatno jer je teško povući granicu između dobrog i lošeg u virtualnom prostoru i sferi. Često je tako prisutna moralna panika, još od osamdesetih godina s većom pojavom osobnih računala i većim osjećajem straha i pomame od hakera i tehnologije. Razvila se čitava računalna sigurnosna industrija koja je potpomogla u etičkim transformacijama po pitanju hakera iako im je u nekim radnjama vrlo slična. Tako se može navesti da korporacije imaju jako velik pristup informacijama i mogu doprijeti do nečije privatnosti, a na njima je kako to koriste, dok isto ne dopuštaju nekim hakerima koji imaju isti cilj pa se može govoriti o dvostrukim standardima. Hakeri jednostavno nisu poželjni jer su i parodija na tehnokraciju. Naravno da su aktivnosti poput cyber kriminala vrlo upitne pa i loše, ali histerija oko hakera i njihovo pretjerano etiketiranje i označavanje također nisu od nekog značaja, pogotovo kad se piše da su hakeri cyber kriminalci samo jedan od podtipova suvremenih hakera, a i hakerska zajednica pokušava se distancirati od njih nazivajući ih crackerima. Prvi korak u označavanju je uspostaviti abnormalnost što može upravo biti pojava cyber kriminala, a zatim se u drugom koraku kroz primjere prijetnja validira i pravi se mit. Tako kao primjer može poslužiti da se za nešto uzeto iz virtualnog prostora počeo koristiti stvarnosni termin poput krađe, kako to u svojem članku objašnjava Thomas (2005, 601.str.). Hakeri tako postaju dobri žrtveni janjci, a sve zbog pravih,

ali i imaginarnih strahova od „drugog“ (Halbert, 1997, 366.str.). Na državi koja je dobila legitimnost jedna od zadaća je da osigura sigurnost. Tako je već u 19. stoljeću stvorena policija koja je štitila industrijska postrojenja, a u postmoderni se policija aplicira u virtualni svijet kao vrsta sigurnosne računalne industrije. Danas postoje primjeri (Sommer, 2021, 1.str.) u kojima se dešavaju prodori u enkriptirane pametne telefone koje su koristili cyberkriminalci, pomoću implantanta, te se dobivene informacije koriste čak i kao dokazi na sudu. Je li riječ o sigurnosti ili većoj socijalnoj kontroli pitanje je koje postmoderna otvara. Hakeri nisu u potpunosti ni pozitivci ni negativci, isto kao ni računalna sigurnosna industrija. Do razmirica dolazi i među hakerima, česti su sukobi početnika i elitnih hakera, česti su i raskoli unutar hakerskih grupa, a vanjski pritisci ih često dovode u situaciju nemogućnosti adaptacije. Sve zbog nepredvidivosti. Objašnjenje svega toga može se naći u tehno revoluciji koja je postala prijetnja vlasništvu, privatnosti i socijalnoj kontroli. Računalna revolucija postala je brža od našeg razumijevanja te je istražujuća hakerska mladost zamijenjena često prisiljenim prihvaćanjem legalne odgovornosti za akcije, a sve je manje hakera tehnoloških istraživača.

2.5.4. Hakerski imaginarij

Hakeri koji sudjeluju u nelegalnim aktivnostima prikazani su u medijima kao kriminalci. No, koja je uloga medija u stvaranju imaginarija hakera? Može se reći da je dvojaka. S jedne strane navode primjere nekih od hakera, ponekad kao devijanata. Ili pak opisuju sukobe hakera i računalne industrije. S druge strane u medijskom istraživanju koje je proveo tehnički časopis PC- Welt, a koje se spominje u članku Tanczer (2019, 1.str.) slika o hakerima pokušava se promijeniti. Prvo su navedeni primjeri hakerskih kolektiva poput LOphta koji su i sami donijeli testament o računalnoj sigurnosti, a neki njegovi istaknuti članovi poput Chrisa Wysopala aka „Weld Ponda“ ili Pietera Zatka „Mudgea“ zaposlili su se kasnije u velikim sigurnosnim kompanijama. Oni su objašnjavali da termin „hack“ koji potječe iz šezdesetih označava pojam virtuoznosti i rješavanja problema. Stoga je časopis PC-Welt u svojoj studiji proveo intervjue te pitao određene tvrtke:a) Zapošljavaju li hakere? b)Zapošljavaju li bivše hakere? c)Zapošljavaju li dobre hakere? Uz to je trebalo navesti neke od razloga zbog čega mogu zaposliti određenu osobu hakera ili pak ne. Najčešći afirmativni odgovori bili su u slučaju dobrih hakera zbog toga jer su oni specijalisti za sigurnost i najkvalitetnije znaju slabe točke cyberkriminala. Afirmativni odgovori bili su i u slučaju kada je potrebno provesti probu ili eksperiment sigurnosnog istraživanja ili testa upada. Dosta ih je pak bilo nepristrano ili s negativnim odgovorom izbjegavajući asocijacije s hakerima ili čineći distinkciju između polja profesionalaca i polja hakera. Na najveću hakersku konferenciju, DEFCON-u 2010. godine,

došao je čak i direktor nacionalne sigurnosne agencije (NSA) kako bi se stigmatizacija prema hakerima smanjila, odnosno kako bi se od nje distanciralo. Objašnjeno je da hakeri posjeduju stručnost te da ih je moguće profesionalizirati, sve ovisi od čovjeka. To potvrđuje i navedeno istraživanje koje pokazuje protočnosti i elastičnost u moralnoj valenciji hakera, za čiji prikaz je korištena Mobiusova vrpca kao kvalitetna vizualizacija. Vrpca objašnjava da hakeri mogu biti i u IT sektoru, kao što je moguć i obrnut slučaj IT-evca kao hakera.

2.5.5. Perspektive i mišljenja o hakerima i tehnologiji

Budući da postoje razne varijante, kakva je onda perspektiva hakera i kakva su mišljenja o njima, tu također postoje različiti stavovi. Jedan od stavova je da hakeri predstavljaju egzotičnost te da su teško razumljivi. Kreću se sučeljima s mnogo slojeva do kojih dopiru uz pomoć lakoće korištenja mreže, a tako ostavljaju i dojam udaljenosti. Neki teoretičari poput Taylora (2005, 631.str) smatraju to alijenacijom čak i u virtualnom svijetu, a pogotovo u stvarnom. Drugi pak smatraju da je to samo vrsta transgresije između društvene stvarnosti i virtualne online stvarnosti, u čemu su hakeri u središtu. Najbolji primjer za to je da materijalni medij sve češće postaje nematerijalni, informacijski. Postoje pak mišljenja da su hakeri zapravo paraziti na računalnom sistemu. Takva mišljenja inspiraciju pronalaze te naginju k tome da su ljudi prije koristili strojeve samo kao pomoćno sredstvo ili ih čak i uništavali te borili se protiv njih. To su mišljenja koja smatraju da su se hakeri pridružili strojevima te da djeluju zajedno sa njima. Odraz je to straha, ali i fascinacije ljudi koji dijele takvo stajalište, tehnološkim promjenama. Cijeli takav narativ se bazira na tome da su hakeri smatrani kontrolorima tehnologije, ali da sada postaju kontrolirani od tehnologije koju koriste. U Taylorovom članku prisutno je protezanje takvog narativa i njegovo objašnjenje. Tako Taylor (1998, 403. str.) pronalazi poveznice i sličnosti s Gibbsonovom knjigom *Neuromancer*(1985), jednoj od prvih knjiga tematike cyberpunka, žanra koji je više kontemporarnih tematika od na primjer znanstvene fantastike. U Neuromanceru ljudi žive u gradu koji vodi umjetna inteligencija. Taylor poveznice pronalazi i u knjizi *Microserfovi* u kojem majka programera doživi infarkt te je stroj održava na životu potkrepljujući tako ideje o parazitizmu. Dakle, riječ je o teoriji u kojoj računalo ili stroj predstavljaju makrokozmos koji regulira ljudski rad pa čak može ići i do te mjere da utječe na njihov način života. Taylor piše da čovjek sve više preuzima logiku uma prirode. Povlači analogiju u prirodi koja nam daje, ali takav način postaje prekompleksan za nas. Sada se ljudi stavljaju u ulogu prirode stvarajući robote, a jednom će se roboti možda također oteti kontroli i preuzeti ulogu čovjeka. Čovjek počinje pretjerano koristiti tehnologiju, a simbiozom čovjeka i mašine postigao bi potpuno programiranje. Takva razmišljanja govore

o opsesivnosti, adiktivnosti i dehumanizaciji, razvitku afiniteta prema matrici. Hakeri su tu još uvijek između starih običaja i kulture nove tehnologije te neka vrsta ironične reakcije protiv računalnog modernizma i postmodernizma. Čovjek toga doba ne zna što bi s informacijama, a znanje često dolazi uz visoku cijenu. Naravno, javljaju se tu i još neka mišljenja koja smatraju da su hakeri zapravo protiv moderne tehnologije, da je odbijaju, da traže alternativne putove. Takvo mišljenje dijeli Maxigas (2017, 841.str.). To su hakeri, kako smatra Nissenbaum (2008, 202.str.), koji se bore i pružaju otpor protiv zatvorenog Neta01 te zagovaraju povratak na otvoreni Net95, naravno slobodna informacija kola negdje oko sredine. Takvi su hakeri zagovaratelji interneta koji ne bi bio čisto skrolanje po mreži.

2.5.6. Haktivizam

Može ih se usporediti s haktivistima, pojma koji potječe od neologizma hakerske grupe Kulta mrtve krave. Haktivisti su vrsta hakera koji koriste informacije kao revolucionaran materijal u ostvarivanju nekih od svojih ciljeva, često s političkom ili ideološkom konotacijom. Tako određene grupe počinju predstavljati hakere, kao na primjer Anonymusi, a s druge strane sigurnosne službe pokušavaju iskontrolirati proteste. Tako se oko haktivizma stvara društvena drama. Takvi hakeri koje često nazivaju keyboardwariorima su vrlo kreativni, preuzimaju rizik mješavinom legalnih i ilegalnih aktivnosti, pokušavaju mijenjati standarde i pokazuju da više ne postoji samo mali broj webmastera koji brinu o mrežnim stranicama. Danas u www mreži dovoljan je samo point and click za nešto pokrenuti, a hakiranje sve više postaje kulturni identitet i vrsta buntovništva, a manje razvitak novih vještina. Hakeri za sada kao kontra-kultura ne uspijevaju usmjeriti korporativnu moć prema humanijim ciljevima. Kako će hakeri i hakiranje se kretati dalje teško je predvidjeti.

2.6. Motivacija

Hakeri se koriste računalima iskušavajući svoje i računalne krajnje limite. To je nekakva opća motivacija kojom se hakeri vode. No, motivi mogu biti različiti. Turgeman- Goldschmidt (2005, 10.str.) daje malo detaljniji uvid u hakersku motivaciju ili motivacije navodeći dosadu, ovisnost, znatiželju, užitak, rekreaciju, moć, zaradu, jednostavnost ili težinu zadatka, osvetu, politiku i prepoznavanje kao neke od njih. Goldschmidt je proveo intervju licem u lice s pedesetčetvoricom izraelskih hakera pitajući ih za motive. Iako je kao jedna od navedenih motivacija novac, ona je bila manje zastupljena te hakeri nisu pokazali velik ekonomski interes, možda i zbog rizika da ih se ne uhvati. Uglavnom su usredotočeni na nematerijalnu štetu, a

navode lakoću provale u akademske institucije. Širina internetskog prostora, kako navodi jedan od hakera, daje im iluziju da su granice neprirodne i nepostojeće te ih takva nova pravila za igru dodatno motiviraju u istraživanju. Njihova motivacija potiče iz zapadnjačke ideje o individualizmu. Isto tako, postoji i obrnut slučaj istraživanja koje su proveli Young, Zhang i Prybutok, a riječ je o negativnoj motivaciji (2007, 282. str.). Tu spadaju moral, neformalne sankcije, ozbiljnost kazne, mogućnost kazne ili sramota. Najviši rezultati pokazani su u ozbiljnosti i mogućnosti kazne jer zatvorska kazna od 1 do 20 godina u Sjedinjenim Američkim Državama pod nadležnošću FBI-ja svakako odvraća hakere od određenih djelatnosti.

2.7. Hakerske djelatnosti

Hakerske tehnike, vještine ili djelatnosti, kako ih god nazvali mogu biti vrlo raznolike. SANS Institut provodi hakerske tečajeve, a nakladnici Syngress, No Starch Press objavili su brojne hakerske knjige gdje ih i objašnjavaju te pokazuju što sve hakeri uče, a ostali ne. Tako glasi i naslov članka autora Smitha (2007, 73.str.) koji objašnjava njihovu sposobnost brzog reagiranja, a fokus je na white hatovima i grey hatovima. Hakeri u manjku alata često koriste lažni hardver ili softver koji im olakšava situaciju te nudi rješenje u obrascima bez alternative. Hakeri su ti koji čitaju dokumentaciju i informacije svake vrste. Hakeri se često koriste operacijskim sustavom Tails kada pretražuju na clearnetu, što bi predstavljalo „običnu“ mrežu ili na darkwebu, jer Tails ne ostavlja trag sesije. Zatim, izmjenjuju znanja na forumima, na primjer ruski hakeri to često čine koristeći običan preglednik dok engleski koriste Tor preglednik kako bi se postigla migracija adresa koju je moguće otkriti samo pomoću spidera, iako ne mora uvijek biti takav slučaj. Robertson i drugi u svojoj knjizi objašnjavaju (2017, 17.str.) da ugledniji forumi često traže kod hakera admina ili pak određeni malware za pristup. Takvi forumi sadrže stroža pravila ili pak teži ulazak poput onog PGP- ključem. Na takvim hakerskim forumima, ali i općenitom, može se saznati nešto o hakerskim tehnikama. Ranije generacije hakera, telefonske phreakove, kako je neke od njih nazvao Skibell (2002, 340. str.), tražile su glitcheve ili bugove u telefonskim ili računalnim sustavima što bi značilo da su tražili greške koje bi koristili bilo u sustavu ili u ljudskom faktoru. Današnji hakeri sve češće koriste i debuggere kako bi učinili suprotno, odnosno ispravljali greške. Sigurnosni sustavi trude se da bugove svedu na najmanju moguću mjeru. Dugo prisutna je i tehnika krekiranja koje omogućava pristup na primjer videoigrama ili programima. Još jedna ne toliko nova tehnika je bombardiranje sustava e-mailovima sve dok se ne sruši. Što se tiče mreža, kako bi ih se lociralo

koristi se pinganje odnosno mogućnost pronalaska druge mreže. Slično je i sa doksiranjem kada se pronalaze i objavljuju informacije na internetu, često sa štetnim posljedicama. Hakeri su također dobri u linkanju odnosno overloadingu što se tiče programiranja. Pojedine vrste hakera koriste različite strategije. Cyberpunkovi koriste napadačke vektore (eng. *attack vectors*) kako bi istražili greške sistema ili SQL injection napad kako bi uz pomoć koda ušli u bazu podataka zaštićenu upitom. Stara garda (eng. *old guards*) koristi cyber forenziku, a državni hakeri uporišta (eng. *foothold*) kako bi ponovno okinuli određeni malware u slučaju na primjer ponovnog pokretanja računala. Profesionalci koriste sve vrste tehnika. Koriste malware poput trojanskih konja, rootkitova koji sakrivaju malware od korisnika, backdoorove koji premošćuju autentifikaciju, ili blokere informacija poput ransomwarea. Mogu koristiti i grayware poput špijunskih programa. Od tehnika se služe još phishingom kojim pokušavaju izvući podatke od korisnika, napadom bočnim kanalom gdje saznaju kako određeni algoritam funkcionira ili pak spoofingom odnosno falsifikacijom podataka i lažiranjem internetskih adresa. Hakeri znaju biti i korisni za sigurnost te su izmislili i sigurnosne softvere poput StackGuarda, Open-Walla ili Paxa koji štite izvršnu memoriju.

2.8. Primjeri hakera

Operacija Sundevil (1990.) jedna je od prvih hakerskih akcija za koju se saznalo. Hakeri su dolazili u posjed brojeva kreditnih kartica ljudi, na što je policija odgovarala provaljujući u stanove osumnjičenih i provodila racije. Gubitku koji je nastao bilo je teško procijeniti vrijednost. Malo benigniju akciju sproveli su švedski hakeri (1996.) koji su se našalili s CIA-om i promijenili ime njezine službene web stranice u Central Stupidity Agency. Sljedeće je potrebno spomenuti Megalodon HTTP hakere koji su u pogon pustili Remote Access Trojan (RAT) i tako kao jedni od prvih doveli do mogućnosti daljinskih napada. Nakon toga počeli su se razvijati i hakerski dark marketi o čemu piše Misha Gleny (2011, 19.str.). Poznati takvi trgovci su Rusi koji se koriste specifičnim hakerskim Padonkaffsky žargonom. Na taj je način Taraspov prodao malware koji cilja POS softver, a Ross Ulbricht je razvio darkweb supermarkete zbog čega je kasnije završio u zatvoru. Na takvim darkweb supermarketima ponuđeno je i hakiranje kao usluga, takozvani Hacking as a Service (HaaS). Takav razvitak hakerske mreže o čemu svjedoče brojne hakerske grupe poput njemačkog Computer Chaos Cluba, pokrenuo je sigurnosne službe da hakerske aktivnosti počinju strože sankcionirati. Ne toliko davne akcije protiv hakera su operacija Emma 95 u Francuskoj i Lemont 26 u

Nizozemskoj koji su povećale standarde kazni. No, hakeri nastavljaju, a primjer je i rušenje Škotske kraljevske banke. Nastavljaju često i kao aktivisti, jedan od poznatijih su novinari Wikileaksa predvođeni Julienom Assangeom (Holger i Rosenbach, 2011, 4.str.). Haktivisti su i Anonymusi koji su počeli na forumima 4chana. Prvi veći sukob im je sa scijentološkom crkvom u Americi, a zatim provode veće napade na Paypal i Sony. Sve je to dovelo do uhićenja brojnih njihovih članova. S članovima pod nadimcima Sabu, Topiary i Kayla razgovarala je i njihovu priču zapisala Olson (2012, 355.str.). U suvremenom svijetu može se naći i primjera poput cyber-vojske Stuxneta, a hakerskih skupina ima svugdje. I Hrvatska je imala svoju hakersku grupu pod imenom Croatian Revolution Hackers. Kada pak govorimo o hakerima pojedincima od devedesetih godina do danas najpoznatiji su Len Rose aka Terminus, Steve Jackson čija je kompanija video igara konfiscirana zbog hakiranja, Bloodaxe, Gary McKinnon, Hamza Bendelladj i Roman Seleznev (Track1) koji je dobio najveću zabilježenu zatvorsku kaznu zbog hakiranja kreditnih kartica od 27 godina. Ipak, najeksponiraniji je Kevin Mitnick koji je dosta toga napisao o svojim hakerskim poduhvatima i savjetima za sigurnost.

3. Knjige Kevina Mitnicka

3.1. *Umijeće obmane (The Art of Deception)*

Kevin Mitnick nije jedan od hakera vandala, bolje napisano krekera koji ljudima uništavaju datoteke ili diskove, niti skriptaša početnika koji se većinom koristi alatima za hakiranje pronađenim na internetu. Rođen u San Fernandu, često je putovao u Los Angeles kao mladić istražujući ga. Putovanja Los Angelesom olakšavao mu je jedan od prvih trikova koje je naučio služeći se djelomično ispunjenim, ali neovjerenim kartama koje bi pronalazio na raznim mjestima. Mitnick je, kako je i napisao, volio mađioničarstvo, a u mnogobrojnim trkovima kojima se služio svakako mu je pomoglo i poznavanje većine gradskih trasa i naučenih telefonskih brojeva. Baš su mu trikovi s telefonom bili počeci, u svom razvitku u majstorskog hakera. Naučio je dobivati tajne probne brojeve, nazivao je telefonske kompanije i centrale mijenjajući usluge drugim korisnicima, a u nekim slučajevima i prevarantima. Zanimanje za tehnička i informacijska područja usmjerila su ga u studiranje informatike u Centru za računalnu obuku u Los Angelesu. Kad je uspio postati administrator na jednom od sveučilišnih IBM-ovih računala, došlo je do čuđenja i pitanja kako je to uspio. Budući da je takvo djelovanje bilo nedozvoljeno, kako ga ne bi izbacili sa sveučilišta, o tome je morao napisati disertaciju, što je i prihvatio. Mitnick je uživao u svom poslu, služio se raznim prečicama, a imao je i dobre trgovačke sposobnosti, što je kako je i sam kazao, naučio od roditelja. Kevin je uz to bio i radoznao i puno je vježbao kako bi bio što sposobniji za „umijeća“ koja su ga zanimala. Jedno od njih je i provala te obmana sigurnosnog sistema za koje Mitnick tvrdi da je njihova najslabija točka upravo ljudski činilac. Kako Kevin Mitnick više ne provaljuje u sigurnosne sisteme, već je čak i postao vlasnikom jedne od tvrtki za pitanja računalne sigurnosti, u svojoj je knjizi kroz mnogobrojne primjere, pa čak i neke vlastite, pokazao načine obmane i načine njihova sprječavanja. Tako kao prvi primjer klasičnog slučaja obmane navodi Marka Rifkina koji je socijalnim inženjeringom uspio ukrasti veliku svotu novca iz banke Security Pacific. Autor i haker Mitnick upozorava na takvu problematiku kao i onu narušavanja računalnog sigurnosnog sistema s kojim se 2001. godine, prema njegovim podacima (Mitnick, 2003, 7.str.), susrelo čak 85% organizacija. Mnoge od organizacija su tako oštećene, a glavni problem su sigurnosni sistemi koji štite samo od skriptaša, iako je do 2022. došlo i do tehnoloških inovacija. Sofisticiraniji napadači uglavnom napadaju manji broj sistema pa tako ni isključeno računalo, nije uvijek i sigurno računalo. Mitnick u knjizi savjetuje kako postići dobar omjer između sigurnosti i produktivnosti, tako da jedno ne narušava drugo, ali štiti od napadača znalaca.

Takvi napadači znaju dobro iscrpiti informacije koje su im potrebne, a u tome se služe brojnim tehnikama koje je i Kevin sam ponekad primjenjivao. Često kao prvi korak dolaze do bezazlenih informacija, znaju kad je potrebno malo porazgovarati te često postavljaju nebitna pitanja između bitnih kako ne bi ostavili dojam da obmanjuju, a takve informacije skupljaju i potrebne su im da bi kasnije upali u računalne sustave. Uz to, proučavaju bitnu terminologiju kako bi cijeli posao tekao što brže i kako bi si olakšali zamršene situacije. Stoga je bitno za ljude koji se uglavnom bave telefonskim pozivima u tvrtkama da ne odaju odmah informacije, barem ne prije dvostupanjske identifikacije pozivatelja, što je važan parametar u kojoj se otkriva lokacija pozivatelja i traži se lozinka, a ljudi iz pozivnog centra tako ne ispadaju posrednici informacija. Slijede brojni primjeri kako se okolnim putem može doći do važnih informacija i upada u sigurnosne i računalne sustave kao i savjeti za njihovo sprječavanje. Jedan od njih je dolazak do informacija kao što su imenici pomoću takozvanih imenika probnih brojeva i zaobilaznog broja koje su osobe znale upotrijebiti kako bi došle do novih imenika, a čak je i priručnik FBI-ja u nekom trenutku bio javan. Česti su i munjeviti napadi u kojem se osoba predstavlja kao lice iz kompanije kako bi došla do podataka, što je posebno korisno kod slabo obučenih djelatnika. Stoga, je kao što je i navedeno, važno provjeravanje kako bi distribucija sigurnosti bila što efikasnija, jer napadač računa na postizanje povjerenja i uklanjanja otpora. Tako se može desiti da napadnuti na primjer otkrije broj zatražene bankovne kartice ili sosha, broja socijalnog osiguranja. Takva prijevare se također mogu spriječiti zaštitom klijenata ili djelatnika te sakrivanjem ili naprosto nečuvanjem broja kreditne ili slične kartice. Slična je prijevara predstaviti se kao osoba s nekim činom što gotovo uvijek olakšava otkrivanje podataka. Napadači također koriste metodu poput sažaljenja kad im u otkrivanju informacija može poslužiti situacija u kojoj govore da imaju na računalu virus te traže pomoć. Ili pak obrnuta situacija u kojoj nude pomoć, ali vam za uslugu pritom učine implikaciju trojanskog konja i metodom daljinskog komandnog okruženja se služe računalom. Moguće su i varijante u kojima se traži i nudi pomoć, za što Mitnick također ima jedan primjer korisnika obmanjivača.Važno je ipak naglasiti da se ne može točno reći je li on samo hipotetske prirode jer obmanjivače Kevin Mitnick uvijek spominje pod skrivenim imenima i ne govori da li se baš taj slučaj stvarno dogodio. Tako je taj korisnik, metodom obmane u kojoj je nudio da usluge telefonskog operatera učini boljima dobio mobitel za jedan cent, a zatim u drugoj mobilnoj kompaniji promijenio tarifu i došao u situaciju koja je za njega završila uspješno. Mitnick navodi (2003, 62.str) da su u takvim prilikama česta meta novozaposleni, za koje se pretpostavlja da su kooperativniji. Tako su novozaposleni česta meta otkrivanja lozinki. Kvalitetan obmanjivač zna kako iskoristiti čak i šifrirane lozinke koje se rekonstruiraju iz

tekstualnih i što ne bi trebalo biti reverzibilno. Zatim dobivene podatke koje je dobio upadom u sistem može prenijeti na tajnu lokaciju, što je lokacija na intranetu u nekoj stranoj zemlji koja se uglavnom ne bavi naširoko takvim kriminalnim radnjama ili pak to ne smatra kaznenim djelom. Tako službama u državi u kojoj se zapravo nalazi napadač nije lako ući u tragove takvih postupaka. Zbog toga je kao preventivna metoda uvijek važno novozaposlene što više obrazovati u tom smjeru. Prevaranti se također često koriste metodama nadmudrivanja što za njih predstavlja intelektualni izazov kad prodiru u sisteme kao što su oni sigurnosti uz lozinku u kojoj se za pristup informaciji traži točna riječ. Druga je pak stvar *candy security* ili sigurnost poput bombona gdje kvalitetan obmanjivač, vrlo lako iskorištava nedostatke sistema jake vanjske sigurnosne barijere, ali slabe unutrašnje infrastrukture poput M and M bombona po čemu je i dobila ime. Sličan ne baš djelotvoran način sigurnosti je sigurnost na osnovi tajnovitosti (eng. *security trough obscurity*) gdje se pojedinosti rada sistema poput algoritama i protokola čuvaju u tajnosti gdje opet nastupa nadmudrivanje obmanjivača. Postoje još razni načini nadmudrivanja kojima se koriste obmanjivači poput lažnih web lokacija i opasnih privitaka. Tako je moguće dobiti elektroničku poštu za instalaciju nekog besplatnog softvera koji može zapravo biti virus. Primjeri za to su Sir Cam ili pak Ana Kurnikova. Zbog toga se kao način sprječavanja koriste antivirusni alati čiji su opisi virusa ažurni. Kao metoda može se iskoristiti i zastrašivanje. To se čini predstavljajući se kao osoba od autoriteta. Postavljaju se razumni zahtjevi kako bi se mešetarilo i iskorištavalo informacije, a u jednom primjeru iz knjige obmanjivač je nakon što je upotrijebio opisanu proceduru, pomoću terminala za jednostavne naredbe pristupio udaljenom računalu. Takve se stvari mogu spriječiti grupama za prijavu sumnjivih radnji kao i korištenjem dokumenata i datoteka samo interno u tvrtki, ali ovdje je obmana autoritetom uz već prije spomenuto nepridržavanje sigurnosnih uputa ipak prevladalo. Važno je stoga uvijek postavljati podsjetnike na sigurnost. Još jedna pomalo nezahvalna metoda, ali korisna je kopanje po smeću tvrtke kako bi se našlo važne tiskane informacije koje mogu poslužiti za određene dobitke. Obmanjivači tu često surađuju, a rade to ponekad i predstavnici konkurentskih tvrtki kako bi na primjer našle određene ideje i plasirale na tržište novi proizvod koji je zapravo inovacija druge tvrtke. Obmanjivače uglavnom ne zamara policija, ali se vrlo rijetko pojavljuju osobno na ciljanom mjestu, već većinu toga obavljaju daljinskim putevima, kako bi policija što teže njima ušla u trag. Moguće su i kombinacije tehnologije i obmane. To je na primjer popisivanje (eng. *enumeration*), postupak kojim se otkrivaju postojeće usluge na operativnom sistemu ili spisak imena korisnika. Kao pomoćno sredstvo koriste se hakerski alati, a podaci se mogu prenijeti i na USB. Postoje specijalizirani hakerski softveri koji koriste napade rječnikom pomoću baza koje sadrže sve

riječi određenog jezika te na taj način u ne tako dugom vremenu mogu ispitati izvorni kod ili lozinku koju žele otkriti. Mogući su i napadi tajnim vratima, kada obmanjivač zamijeni određeni dio programa kako bi ušao u sustav, ali tada je za obmanjivača bitno izbrisati tragove ili pak anonimnim FTP-om koji daje pristup određenim datotekama, a ukradene informacije je teško primijetiti. Od ostalih metoda važno je spomenuti špijuniranje koje se može izvršiti implementacijom špijunskoga softvera, a problem je što antivirusni programi uglavnom ne otkrivaju komercijalne špijunske programe kao štetne. Stoga se može instalirati protušpijunski program poput SpyCopa. Česte su i obmane zamjena identiteta, što je slično prije spomenutim obmanama.

3.1.1. Metode sprječavanja

Kako bi se na najmanju moguću mjeru svele navedene metode obmane, Kevin Mitnick predlaže mnoga rješenja i procedure, a ovdje će biti opisane svaka od njih. Prvo što ljudi moraju proći je obuka za zaštitu podataka, iako on preporučuje da bi ljudi uglavnom trebali donositi manje odluka što se sfere sprječavanja obmane tiče jer ih posao i još dodatne mjere zaštite dovode u oskudicu vremena. Svaka obuka bi trebala biti dobro osmišljena, s jasnim uputama za sve i s ciljem upozoravanja da je napad uvijek moguć, ali je taktike obmane ipak važno poznavati. Bilo bi dobro da je organizacija obuke za svaku grupu odjeljenja tvrtke specijalizirana, različita za na primjer informatičko osoblje i netehničko osoblje. Kvalitetnu obuku karakterizira svrhovitost, zanimljivost i poticajnost poput simulacije probnih napada ili pokazivanja video materijala. Strukturu obuke čini umjerenost i sadržajno obuhvaćanje najvažnijeg. Vremenski rok bi obuhvaćao i provodio se i osvježavao jednom godišnje, svaki put s ponešto dužim trajanjem. Sadržajno da se obuhvati provjera identiteta, ovlaštenja, višeslojnog sistema obrane, uključujući i tehnologiju. Vještine bi trebale biti opisane, a djelatnici bi na kraju u većoj mjeri bili osposobljeni za prepoznavanje potencijalnog napada (Mitnick, 2003, 261.str.). Zatim bi se provodilo testiranje i davanje certifikata za one koji su savladali obuku. Dobra metoda je i da se zaposlenike također redovito informira o mjerama zaštite te nagradi one koji se pridržavaju naučenih uputa. Preporuke za upute zaposlenicima su razumljivost, bez puno tehničkog žargona, a u razvoju sigurnosnog programa važno je obaviti procjenu rizika. Zatim bi bilo dobro odrediti grupu ljudi ili osobu odgovornu za informacije i klasifikaciju podataka. Takvi se podaci klasificiraju u četiri skupine: povjerljivo što bi naprimjer bile poslovne tajne, privatno što bi činili zdravstveni podaci o zaposlenima, interno, što se razmjenjuje unutar tvrtke i javno, što čine brošure o proizvodima i mogu se distribuirati svima. Što se tiče terminologije klasifikacije važno je razlikovati nepovjerenu osobu, dakle

koju ne poznajemo i kojoj ne bismo trebali davati informacije, povjerenu osobu, dakle zaposlenu osobu u firmi i garanciju trećeg lica, dakle nekog tko daje legitimitet za distribuciju informacija i podataka. Slijede postupci za provjeru i ovlašćivanje, u kojima je prvi korak provjera identiteta osobe, jer se može desiti da obmanjivač dođe osobno u firmu, što je ipak rijetkost, ali mogućnost. Potrebno je stoga zatražiti propusnicu od osobe kod ulaska u organizaciju, a preporučljive su sve više elektroničke propusnice. Drugi korak čini provjera statusa zaposlenog, a treći provjera ovlaštenosti za dobivanje informacija što je moguće pronaći na raznim spiskovima. Mitnick zatim donosi (2003, 276.str.) pravila za svaku pojedinu službu unutar tvrtke. Tako pravila za rukovodstvo obuhvaćaju označavanje podataka i njihovu organizaciju te priopćavanje informacija. Povjerljive informacije tako bi najkvalitetnije i najsigurnije bile priopćene samo šifrirano, privatne od ovlaštenih osoba, a interne kroz ugovor o tajnosti, samo unutar poduzeća. Kod telefonskih razgovora bitno je pokušati prepoznati glas osobe kojoj se šalju ili od koje se dobivaju informacije, a prijenos datoteka se ne bi trebao odvijati na izmjenjivom mediju. Administracija telefonskih poziva također je dio posla rukovodstva stoga je važno prepoznati ID i lokaciju poziva, podrazumijevanje lozinke promijeniti prije korištenja telefonskih sustava, a glasovnu poštu isključiti kod nekorištenja. Također je bitno provjeriti valjanost proizvođača telekomunikacijskog sustava te pozive uglavnom obavljati po principu interno – interno. Pravila za informatičare opet su nešto drukčija i specifičnija. Važno je ne pružati telefonski broj i e-mail adresu, a rad tehničke podrške i službe za podršku trebao bi biti koordiniran. Lozinke bi se prema procedurama poništavale samo na korisnički zahtjev, a izmjena ovlaštenja samo ako je odobrena. Rješenje za nove naloge je da se odobravaju samo uz digitalnu potvrdu i traju do godine dana, a nove lozinke uz sigurnosne metode. Ono što se odnosi na mrežni priključak jest da bi ga se moglo isključiti samo ako je poznata osoba u pitanju, a bežično dijeljenje mreže moglo bi se odobriti također u istom slučaju. Kao i kod rukovodstvene administracije i računalna administracija ima svoja pravila sigurnosti. Pristup takvoj administraciji mogao bi se izmijeniti samo uz odobrenje i provjeru, a preporučuju se suvremene biometrijske tehnologije. Slično je i s daljinskim pristupom i tehničkom podrškom. Nadalje, važna je sigurnost operacijskog sistema za kojeg je važno da bude ažuriran. Daljnja pravila za računalnu administraciju su: opće adrese elektroničke pošte za svako odjeljenje, na webu ne objavljivati pojedinosti kompanijske strukture. Za admina administracije moguća su veća ovlaštenja, a anonimno korištenje samo uz FTP. Rezervne kopije bi se trebale šifrirati, a modeme ne uključivati prije četvrtog zvučnog signala. Na računalima je preporučljivo da budu antivirusni alati i provjernici softvera. Korisničke račune za prijavu u sustav trebalo bi blokirati nakon određenog broja neuspješnih

pokušaja, a lozinku mijenjati svaka dva mjeseca te je postaviti za pokretanje sustava također. Za ethernet priključke, preporučljiva je odvojena mreža, a bežičnu mrežu treba zaštititi od novijih metoda napadača kao što je war driving, odnosno otkrivanje takve mreže prijenosnim računalom. Za kraj, ostaju pravila za sve pa je tako važno prijaviti i dokumentirati sumnjive pozive i zahtjeve. Tajne, a nepotrebne dokumente je preporučljivo uništiti. Nepoznate prijenosne medije nikad ne koristiti kao ni alate za zaobilazak softverske zaštite. Telefon ne koristiti za sudjelovanje u anketama, a korištenje faksa ne prosljeđivati. Glasovnim porukama koristiti se kratkim pozdravnim porukama i nikad ne otkrivati lozinke, a lozinke ne zapisivati te koristiti različite i uvijek drukčije. Za zaposlenike daljinskoga pristupa koristiti se metodom tankog klijenta za priključenje. Još neka od mnogobrojnih pravila koja je Mitnick naveo odnose se na zaposlene koji napuštaju firmu te bi ih se trebalo onemogućiti u dobivanju viška informacija. Pravila pod rubrikom razno mogu biti da su za pravo pristupa preporučljive najniže privilegije, a privremeni radnici ne bi trebali imati korisnički račun. Potrebno je i formirati tim za evidentiranje incidenata uz posebnu telefonsku liniju kao i osobe za kontakt. Na kraju ili na početku potrebno je ispitati slabe točke sigurnosnog sistema te kako funkcionira, a interne prostorije kao što su one s računalima zaključavati, a na javnom mjestu nikad ne stavljati oglasnu ploču. Ipak, za najvažnije podatke bilo bi dobro da postoji udaljen objekt gdje bi se čuvali. Naravno, to su mnoga pravila koje je Kevin Mitnick napisao, ali kako je knjiga nastala prije desetak godina, ona su se naravno ponešto i promijenila u pristupu te ponegdje i proširila. Mitnick, piše, citirano (2003, 99. str): „*Kupovina osobno u dućanu iste je sigurnosti kao kupovina na internetu*“ naravno, relativna sigurnost ovisi o poznavanju metoda sprječavanja napada.

3.2. *Umijeće provale (The Art of Intrusion)*

U navedenoj knjizi Kevin Mitnick kroz različite priče izmišljenih osoba prikazuje svoje znanje o hakerskim tehnikama koje su specijalizirane za provalu, ali i ostale segmente hakerskog umijeća. Prva je tako priča o hakerima koji su pljačkali kasina uz to što su prvo nabavili jedan od aparata kakvih ima u kasinima te tako vježbali. Mogućnost zarade u kasinu pokušali su povećati zamjenom firmwarea, odnosno softvera koji omogućuje rad stroja i ostalog softvera svojom verzijom programa koji bi im omogućio veće šanse za dobitak. S pomoću obrnutog inženjeringa, metode koja im uz opservaciju omogućuje shvaćanje načina rada stroja takav su program i osmislili, a još im je bio potreban i disasembler koji pretvara strojni jezik u reprezentativni te su tako skupili poveliku svotu novca prije nego što su uhvaćeni. Naravno, to je bilo u devedesetima kad još nije shvaćen bug u nasumičnim brojevima kasinskog aparata. Druga je priča s hakerom neOh-om koji je na IRC-u (Internet Relay Chatu), nekoj vrsti chata devedesetih, upoznao „cyber terorista“ Khalida te upao na stranice kineskog MIT-a, a na kraju se ispostavilo da je Khalid FBI- jev agent te je mladi haker završio u zatvoru. Za upad na kineski fakultet poslužio mu je CGI (Common Getaway Interface) skener koji je našao ranjivosti u sučelju koje obrađuje korisničke zahtjeve. Nadalje spominje se priča o hakerima zatvorenicima koji su uz Back Orifice program, dobro vladanje i poznavanje zatvorskoga sustava imali pristup drugom računalu. Protumjera može biti korištenje PestControla koji otkriva programe poput Back Orificea. Nova je priča o Costi koji je na BBS-u (Bulletin Board System) upoznao druge hakere te uz pomoć phrikinga, manipulacije na telefonima provalio u Boeingove sustave. Sljedeći prema Mitnicku (2005, 117.str.)izmišljeni haker, Adrian iskoristio je otvoren pristup (eng. *open shares*) u tvrtki (New York Timesu) koju je napadao te proxy hunter za ulazak na privatnu mrežu, a zatim i slobodan oblik SQL queryja koji mu je omogućio da može koristiti baze podataka. Mitnick je još naveo primjere o manipulaciji grafičkim korisničkim sučeljem, korištenje keyghosta, malog uređaja koji detektira sve što se piše na tipkovnici te primjer bota koji umjesto čovjeka igra Texas Hold'em poker. Naveo je i neke mjere sprječavanja upada poput vatrozidova (eng. *firewallova*) koji filtrira promet računalne mreže, sandboxinga te korištenje obrane u dubini.

3.3. *Umijeće nevidljivosti (The Art of Invisibility)*

U ovoj nas knjizi Mitnick uči kako da naša privatnost na internetu bude čim manje narušena, kako na mrežnim stranicama tako i na društvenim mrežama. Prvo piše o lozinkama koje bi trebale biti kompliciranije te spominje najčešće lozinke poput: „password“, „12345“ kao nesigurne. Lozinke bi trebale sadržavati velika i mala slova, posebne znakove te znamenke. Softver poput EPPB-a (Elcomsoft Phone Password Breaker) i iBrutea specijalizirani su za lomljenje lozinki na iCloudu. Zatim piše o kompanijama koje skeniraju e-mailove te da je sigurnosna mjera enkripcija istih. Tako se kod slanja elektroničke pošte može koristiti enkripcija Cezarovom šifrom koja mijenja slova, PGP-om (Pretty Good Privacy) ili GPG-om (GNU Privacy Guard). Bitno je, kako objašnjava Mitnick (2017, 39.str.) da se koristi end-to-end enkripcija, odnosno da poruka ostaje kriptirana sve dok ne dođe do krajnjeg korisnika. Bitni su čak i metapodaci kod slanja e-mailova jer mogu otkriti IP adresu stoga ju je potrebno sakriti te ugasiti JavaScript i AdobeFlash kako bi hardver i softver bio nejasan. Za pretraživanje internetom bilo bi dobro koristiti se Tor preglednikom, ali problemi s njim su što je spor i što je detekcija ipak moguća. 4G mreže mogu također predstavljati problem kod mobilnih poziva pogotovo, ako se zna SS7 signal. Isto je i ako želimo razgovarati putem VoIP-a (Voice over Internet Protocol) jer je enkripcija SDES-om nesigurna. Kod poruka je bitno korištenje off the record messaginga jer su one enkriptirane, jedna od takvih aplikacija je Cryptocat. U široj slici interneta važno je koristiti se https protokolom jer je on sigurniji i također kriptiran. No, mrežne stranice također prikupljaju informacije stoga bi se mogao instalirati NoScript ili Scriptblock softver uz dodatak Adblocka koji to sprječava. Važno je i da su ruteri enkriptirani jer su mogući *pixie dust* napadi koji otkrivaju lozinke. Što se tiče aplikacija trebaju uglavnom biti ugašene kao i GPS da bi lociranje bilo teže. Mitnick nadalje priča o uređajima poput dronova, Internet of Thingsa ili ALPR (Automated License Plate Recognition) tehnologije za lociranje automobila, uglavnom uređaji koji narušavaju privatnost. Za čuvanje dokumenata preporučljivo je instalirati BitLocker koji traži dodatnu autentikaciju. Bilo je još ideja koje bi čuvale našu anonimnost poput proxyhama koji anonimizira našu internetsku vezu koristeći WiFI, iz na primjer kafića, ali projekt je prekinut. Jedna od inovacija je i virtualna mašina koja se može izraditi na računalu čuvajući našu privatnost iz računala na računalu.

3.4. *Ghost in the Wires*

Kevin Mitnick poznatiji kao Condor u ovoj svojoj knjizi u detalje opisuje svoj život od najranijeg djetinjstva pa sve do trenutka uhićenja od strane FBI-jevih službenika i još jednog kompjutorskog genijalca Shimomure. Nakon izlaska iz zatvora u čemu mu je pomogao i pokret „*Oslobodite Mitnicka!*“ svoja je hakerska umijeća počeo koristiti kako bi ljude učio načinima sigurnosti u mrežnom prostoru. U mladosti je živio u Los Angelesu gdje je i nekoliko puta uhićivan upravo zbog hakiranja, a u knjizi opisuje i neke crtice iz osobnog života poput gubitka brata Adama. Zbog svojih je hakerskih avantura morao mijenjati i mjesta prebivališta pa je tako selio i u Denver i u Seattle. Isto je tako mijenjao i identitete nadmudrujući se s FBI-jevim agentima, pogotovo Ericom (Mitnick, 2012, 141.str.). Jedna od većih hakerskih avantura mu je upad u Motoroline sisteme, a Kevin je naprosto bio potaknut intelektualnom znatiželjom. Rijetko je kad oštetio sisteme u koje je upadao, iako je određenu štetu počinio. Na dan 4.7., što je značajan dan u američkoj povijesti, završio je na naslovnicama Timesa kao najtraženiji svjetski haker, nešto poput Bin Ladena kako je tvrdio, a pripisivali su mu se i brojni upadi koje nije počinio. Odlučio se ovu knjigu napisati kao rezime svih prethodnih u kojima opisuje hakerske tehnike.

4. Zaključak

Neki hakeri mogu biti maliciozni poput cyberkriminalaca i za njih je veliki stručnjak i čovjek od ogromna iskustva Kevin Mitnick dao zaista ogroman broj primjera hakerskih tehnika i kako se zaštititi od njih. Hakeri mogu biti aktivisti poput Anonymusa, mogu biti informacijski i računalni stručnjaci poput hakera sa MIT-a i još mnogo toga. Svi oni mogu ostaviti svoje tragove krađom, ideologijom, inovacijom i drugim, u virtualnom, ali i u svakodnevici. U suvremenom dobu postoji određena doza skepse prema hakerima što dovodi do velikih izdataka za računalnu sigurnost. Problem zapravo nije toliko u hakerima, već u tome što se tehnologija brzo razvija zbog čega je teže razumijemo i ne znamo što bismo s informacijama. Zato nam je teško odrediti etičke granice tehnologije.

5. Literatura

Bratus, S. (2007). What Hackers Learn that the Rest of Us Don't: Notes on Hacker Curriculum. *Security & Privacy*, 5 (4), 72-75. doi: 10.1109/MSP.2007.1

Gibbson, W. (2000). *Neuromancer*. New York: Ace.

Glenny, M. (2011). *DarkMarket: Cyberthieves, Cybercops and You*. London: The Bodley Head.

Glodstone, D. (2001). Deciding Whether to Prosecute an Intellectual Property Case. *United States Attorneys' USA Bulletin* 49(2), 1-8. www.usdoj.gov/usao/eousa/foia/foiamanuals.html

Halbert, D. (1997). Discourses of Danger and the Computer Hacker. *The Information Society*, 13(4), 361-374, doi: 10.1080/019722497129061

Himanen, P. (2002). *Hakerska etika i duh informacijskog doba*. Zagreb: Jesenski i Turk.

Kennedy, K. E. (2015). *Medieval Hackers*. New York: Punctum Books.

Levy, S. (2010). *Hackers: Heroes of the Computer Revolution*. Cambridge: O'Reilly Media.

Maxigas. (2017). Hackers against technology: Critique and recuperation in technological cycles. *Social Studies of Science*, 47(6), 841–860. https://www.jstor.org/stable/48568898

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*(2), 195–217. https://doi.org/10.1177/1461444804041445

Olson, P. (2013). *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* Boston: Little, Brown and Company.

Raymond, E. S. (1996). *The New Hacker's Dictionary*. Cambridge: MIT Press.

Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., i Shakarian, P. (2017). Understanding Darkweb Malicious Hacker Forums. U *Darkweb Cyber Threat Intelligence Mining* (13-37). Cambridge: Cambridge University Press. doi:10.1017/9781316888513.005

Rosenzweig, R. (1998). Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet. *The American Historical Review*, *103*(5), 1530–1552. https://doi.org/10.2307/2649970

Simon, W. L., i Mitnick, K. (2003). *Umeće obmane.* Preveo Vanja Smoje- Glavaški. Beograd: Mikro knjiga.

Simon, W. L., i Mitnick, K. (2005). *Umeće provale*. Prevela Jasmina Đorđević. Beograd: Mikro knjiga.

Simon, W. L., i Mitnick, K. (2011). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Boston: Little, Brown and Company.

Stark, H., i Rosenbach, M. (2011). *Staatsfeind WikiLeaks: Wie eine Gruppe von Netzaktivisten die mächtigsten Nationen der Welt herausfordert*. Hamburg: Spiegel.

Skibell, R. (2002). The Myth of the Computer Hacker. *Information, Communication & Society*, 5(3), 336-356. doi: 10.1080/13691180210159292a

Smith, A. D., i Rupp, W. T. (2002). Issues in cybersecurity: Understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security*, 10(4), 178-183. doi:https://doi.org/10.1108/09685220210436976

Smith, G.S. (2015). Management models for international cybercrime. *Journal of Financial Crime*, 22(1),104-125. https://doi.org/10.1108/JFC-09-2013-0051

Sommer, P. (2022). Evidence from hacking: A few tiresome problems. *Forensic Science International: Digital Investigation* 40, 1-7. https://doi.org/10.1016/j.fsidi.2022.301333

Tanczer, L. M. (2020). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy*, 41(1), 108–128. DOI:10.1080/13523260.2019.1669336

Taylor, P. A. (1998). Hackers: Cyberpunks or microserfs? *Information, Communication & Society*, 1(4), 401-419, doi: 10.1080/13691189809358980

Taylor, P. A., i Jordan, T. (1998). A Sociology of Hackers. *The Sociological Review*, 46(4), 757–780. https://doi.org/10.1111/1467-954X.00139

Taylor, P. A. (2005). From hackers to hacktivists: speed bumps on the global superhighway? *New Media & Society*, 7(5), 625–646. https://doi.org/10.1177/1461444805056009

Thomas, D. (2002). *Hackers Culture*. Minnesota: University of Minnesota Press.

Thomas, J. (2005). The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age' of hacking. *New Media & Society*, 7(5), 599–624. https://doi.org/10.1177/1461444805056008

Trope, R. L., i Hantover, L. L. (2017). Reckoning with the Hacker Age: Cybersecurity Developments. *The Business Lawyer*, 73(1), 227–238. https://www.jstor.org/stable/26419201

Turgeman-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review*, 23(1), 8–23. https://doi.org/10.1177/0894439304271529

Vamosi, R., i Mitnick, K. (2017). *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. Boston: Little, Brown and Company.

Yau, D., Lu, H. Y., Kumar, A., i Chng, S. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, 5, 1-8. https://doi.org/10.1016/j.chbr.2022.100167

Zhang, L., Young, R., i Prybutok, V. R. (2007). Hacking into the Minds of Hackers. *Information Systems Management*, 24(4), 281-287. doi: 10.1080/10580530701585823

Kevin Mitnick – umijeće hakiranja

Sažetak

Prisustvo modernih hakera seže od 1950-ih godina pa sve do suvremenosti. Hakeri su sastavni dio našeg doba. Beverenov model hakerskog razvitka i Bandurova teorija socijalnog učenja objašnjavaju kako hakeri međusobno korespondiraju. Prema hakerima je nekad prisutna doza skepse jer neki od njih sudjeluju u cyberkriminalu. Tu se otvara pitanje hakerske etike gdje je teško odrediti granicu. Isto tako, često su oprečna mišljenja o hakerima kao nekome tko je uz ili protiv tehnologije. Hakeri su motivirani iskušavanjem svojih i računalnih limita. Iako se danas spominje čak trinaest vrsta hakera, najpoznatija je klasifikacija na hakere inovatore, white hatove i black hatove. Operacija Sundevil najpoznatija je hakerska akcija, a Anonymus skupina. Hakeri često koriste štetan program (eng. malware) ili metode poput phishinga. Postoje pak i primjeri prakse gdje tvrtke zapošljavaju hakere jer su stručnjaci za probleme u računalnoj sigurnosti. Jedan od takvih je osoba Kevina Mitnicka. On u svojim knjigama uči kako spriječiti društveni inženjering, na primjer neodavanjem informacija. Nadalje, kako spriječiti provale hakera, na primjer vatrozidom i kako ostati u većoj privatnosti na računalu i internetu kriptiranjem.

Ključne riječi: Kevin Mitnick, umijeća, hakiranje

Kevin Mitnick – the skill of hacking

Summary

The presence of modern hackers dates back to the 1950s until the present day. Hackers are an integral part of our age. Beveren's model of hacker development and Bandur's social learning theory explain how hackers correspond with each other. There is sometimes a certain amount of skepticism towards hackers because some of them participate in cybercrime. This is where the question of hacker ethics arises, where it is difficult to define a boundary. Likewise, there are often contrary opinions about hackers as someone who is for or against technology. Hackers are motivated by testing their own and the computer's limits. Although there are as many as thirteen types of hackers mentioned today, the most famous classification is into hackers innovators, white hats and black hats. Operation Sundevil is the most famous hacker action, and the Anonymus, group. Hackers often use malware or methods like phishing. There are also examples of practice where companies hire hackers because they are experts in computer security problems. One such person is Kevin Mitnick. In his books, he teaches how to prevent social engineering, for example by not giving away information. Furthermore, how to prevent hacker break-ins, for example with a firewall and how to stay more private on the computer and the Internet by encryption.

Key words: Kevin Mitnick, skills, hacking