Hakeri - crni, bijeli i sivi

Informacijska sigurnost je mlada disciplina, nastala sa zadrškom nakon pojave informacijske revolucije. Prvo su razvijene tehnologije kojima su svi bili fascinirani. S pojavom sve brojnijih zloupotreba, javlja se potreba za boljom zaštitom. Informacijska je sigurnost isprva neka vrsta naknadne pameti, neprestano ispravljanje već napravljenog. Sve dok se ne dostigne kritična masa loših iskustava koja će proizvesti promjenu, što bi u ovom slučaju značilo ugrađivanje zaštite već pri dizajniranju proizvoda.

U svijetu se koristi sve više umrežene računalne opreme, život i rad više nisu mogući bez računala (mobitela, servera, osobnih računala, satova, nadzornih kamera, umreženih senzora - lista je otvorena...). U isto vrijeme ranjivosti se otkrivaju svakodnevno. Provaljivanje više nije hobi golobradih klinaca željnih dokazivanja, već ozbiljan posao kojim se bave kriminalci s jedne strane, a obavještajci koji rade za države s druge. Mogli bi tu ubaciti i korporativnu špijunažu, jer tvrtke žele znati što radi konkurencija. Što je nekad bila zabava, sad je ozbiljan posao. U igri su novac, moć, politički interesi. A nasuprot "zločestim dečkima" su "dobri dečki", etički hakeri. Ovdje se već nazire dvojnost svojstvena ljudskoj prirodi, pa prema tome neizbježno i hakerima. I oni mogu biti dobri i loši dečki. Nema znanstvenog istraživanja koje bi nam otkrilo koji je postotak hakera u kojem taboru, ali pretpostavljam da bi omjer bio isti kao u bilo kojem drugom zanimanju. Mada, radi važnosti koju IT revolucija donosi današnjem društvu, vjerojatno možemo s razumnom sigurnošću pretpostaviti da se na njih vrši veći pritisak nego na pripradnike nekih "normalnih", manje zanimljivih zanimanja.

Ovdje se još jednom moramo ograditi od pojma haker kako ga prezentiraju mediji. Haker nije kriminalac! U počecima informacijske revolucije, postojali su odvojeni nazivi za ljude koji zloupotrebljavaju svoja znanja: *phreakeri* su hakirali telefone (na pr. John Draper koji je pomoću zviždaljke iz zobenih pahuljica zavaravao telefonsku centralu i besplatno razgovarao), *crackeri* su provaljivali na računala. No ti nazivi nisu prodrli u medije. Zato mi nikad nije teško ponavljati: haker je čovjek izuzetnog znanja iz nekog područja, ali je važno dodati da je nužan sastojak definicije hakera činjenica da se zabavlja i uživa u tome što radi! Dakle haker radi radi zadovoljstva u radu, a ne zbog zarade! Haker nije nužno informatičar - haker u kuhinji je Jamie Oliver. Ipak, kad kažemo haker, najčešće mislimo na informatičare. Među pionire IT hakera ubrajaju se na primjer Ken Thompson i Dennis Ritchie, koji su, radeći za AT&T, napravili prvu verziju Unixa, mimo znanja uprave i koristeći odbačeno računalo koje su pronašli u podrumu. Akademski hakeri dali su velik doprinos razvoju otvorenih standarda i Interneta. Stvorili su kulturu otvorenosti, suradnje i zajedničkog razvoja. Jedan od njih je Richard Stallman, pokretač Fondacije za slobodni softver (FSF, Free Software Foundation). Cilj je tog pokreta proizvesti softver koji mogu koristiti siromašni koji si ne mogu priuštiti kupovinu komercijalnog softvera. Koristeći slobodan softver, ne moraju kršiti Zakon o zaštiti autorskih prava! Ali taj pokret je prerastao prvotne namjere, dobio je globalni zamah koji oslobađa kreativnost bezbrojnih talentiranih pojedinaca dajući im svrhu i konkretne zadatke. Svaki mali doprinos dobro je došao, a korištenje i razvijanje slobodnog softvera je više od štednje, već je i otpor korporativnoj dominaciji.

Kao dobar primjer dvojnosti pozvao bih se na epizodu serije Elementary. (Sherlock Holmes, genijalni detektiv, prebačen u suvremeni New York.) Vatrogasci u izgorenoj zgradi pronalaze leš muškarca japanskog porijekla. Koža mu je prekrivena tetovažom, nedostaju mu dva prsta na ruci. Radi se o bivšem članu Jakuze, japanske mafije, koji je kao mladi, talentirani informatičar bio prisiljen postati jakuza, točnije *sokaija* - stručnjak za industrijsku špijunažu i ucjene. Želio je prekinuti s takvim

životom, pa je, uz pristanak šefova, otkupio svoju slobodu i ritualno si odrezao još jedan prst, kako bi mogao živjeti bez straha od progona nekadašnjih kolega, štoviše uz njihovu zaštitu. Dao si je izraditi umjetne prste, od silikona, a u jednog je ugradio USB stick! U SAD je radi svog prethodnog iskustva zarađivao kao konzultant informacijske sigurnosti. Za Ministarstvo obrane provjerava sigurnost računalnog sustava koji treba zamijeniti "legacy" sistem za upravljanje nuklearnim projektilima. No neki smatraju da je stari sustav, koji još koristi 8 inčne diskete, sigurniji jer ga nitko više ne poznaje dovoljno da bi ga znao napasti! Scenaristi serije očigledno koriste dobre konzultante koji razumiju duh vremena!

Treba li reći da je Sherlock haker za zločine?

Kako je danas sve podložno brzoj promjeni, tako se i pojam hakera razvija. Neko je vrijeme, po uzoru na westerne, bilo popularno dijeliti ih na ***white hat*** i ***black hat*** hakere. Kasnije je podjela usložnjena: uz bijele, koji pomažu u zaštiti, crne, s lošim namjerama, pojavljuje se novi pojam: sivi hakeri, ***gray hats***, koji rade za državu, obavještajne agencije. Neosporno je da su svi oni znalci, razlikuju se samo po tome kome služe. U toj se slici posve gubi ono prvotno amatersko uživanje u poslu. Zato preporučujem svima da pročitaju knjigu *Hakerska etika i duh informacijskog doba*, Pekke Himanena. Da ne zaboravimo kako je sve počelo, s dobrim namjerama, i da održimo tu pozitivu i kreativnost na životu.

Naš konzultant s USB prstom prošao je sve tri preobrazbe: prisilni *black hat* uspio se izboriti za svoju slobodu, postao *white hat*, da bi, radeći za vojsku, počeo nositi sivi šešir! Sherlock isprva rezonira da je na USB presnimio stari vojni softver sa disketa, pa je radi toga ubijen. Na kraju se ispostavi da je posrijedi nešto drugo - nećemo vam otkriti rasplet da vam ne pokvarimo gledanje serije. Uglavnom, jakuza haker je bio pošten.

White hat hakeri nazivaju se i etički hakeri, da se naglasi kako je rezultat njihova rada usmjeren na dobrobit društva. Čak se može polagati ispit za etičkog hakera, dobiti certifikat. Tijekom svoje informatičke karijere imao sam čast upoznati nekolicinu hakera, s certifikatom i bez njega. Dobri dečki, bistri, sposobni, žestoko zaljubljeni u svoj posao, uvijek na krijesti vala, zainteresirani za nove tehnologije. Na konferencijama održe dobro prihvaćena i zanimljiva predavanja, koja prezentiraju uz dozu nadmoćnog humora. Uvijek je s njima zanimljivo, nikad dosadno. Pod uvjetom da razumijete o čemu pričaju, jer su u stanju satima raspravljati o nekim tehničkim začkoljicama jezikom koji je ostatku čovječanstva nerazumljiv.

Kolega s certifikatom etičkog hakera pričao mi je kako je godinama punio disk ***exploitima*** koji, nažalost, više ne rade. Vrijedni su i dragocjeni dok se ne objave zakrpe. Nakon toga bezvrijedni su s praktičnog stanovišta, ali ih čuvaju jer se iz njih može nešto naučiti, a vjerojatno će jednom imati i povijesnu vrijednost, kao spomenici prošlosti. Osim toga, nisu svi brzi u instalaciji zakrpa, pa će možda još koji put poslužiti svrsi! U prikupljanje exploita utrošeno je mnogo vremena, znanja, novca. Neki se nude besplatno, ali ih treba znati pronaći, neke dobiješ razmjenom, a neke treba kupiti na darknetu. Etički hakeri i sami traže ranjivosti, objave svaki uspjeh na svom blogu, gradeći svoj profesionalni status, pridobijaju klijente, ali i stvaraju "valutu" za razmjenu. Neki etički hakeri završe na platnoj listi velikih informatičkih tvrtki koje traže talente. Tu ih doslovno udave birokracijom, pisanjem izvještaja, što je krajnja suprotnost hakiranju koje je kreativan posao. S druge strane, tvrtka ulaže u njih, daje im opremu, šalje ih na edukaciju, omogućava im da nastupaju na konferencijama i sami educiraju druge. Neki imaju sreću da dobiju šefa koji razumije da su hakeri drugačija sorta i štite ih od birokracije. U protivnom, najčešće neće dugo izdržati na takvom poslu, otvorit će svoju vlastitu tvrtku, tako da sami sebi budu šef.

U opisu je posla etičkog hakera da stalno traži nove exploite, isprobava ih, a zatim savjetuje klijente kako da se zaštite. U uredu koristi mnoštvo računala. Kad se nabavi exploit, treba ga isprobati na različitim verzijama Windowsa, sa i bez "service packa", sa i bez izdanih zakrpa. Da ne spominjemo različite Unixoide, OSX, iOS, Android... Mnogo posla, a treba biti brz jer proizvođači softvera već pripremaju zakrpe. Ne vrijedi kukati, kad si već odabrao takav posao, treba ustrajati, držati korak. U mlađim danima hakiranje je imalo neku zavodljivu auru, kao da si svećenik s okultnim znanjima koja nisu dostupna običnim smrtnicima. Ali s vremenom se čovjek zamori, toliko truda za nešto što brzo izgubi vrijednost i značenje. Ali potreba za tim znanjima ne prestaje, naprotiv, sve je veća.

Kao što je današnja civilizacija nezamisliva bez računala, tako je nezamisliva bez hakera. Oni su dosad davali svoj pečat razvoju tehnologije, zalažući se za otvorene standarde i slobodan softver, otkrivajući greške u softveru, potičući proizvođače na ispravke. Možete ih unajmiti da vam ispitaju sigurnost vaših sustava, savjetuju vas kako ih poboljšati. Nadam se da će to raditi i ubuduće. Bilo bi žalosno da razvoj ostane samo u rukama korporativnih informatičara, kojima upravljaju profitno orijentirani manageri,. Nadam se također da će ostati živ duh suradnje, otvorenosti i kreativnosti, kojim su obilježili ranu povijest Informacijske revolucije.

uto, 2018-11-13 20:43 - Aco Dmitrović**Kategorije:** Kolumna [1]
Vote: 5

Vaša ocjena: Nema Average: 5 (3 votes)

story_tag: informacijska sigurnost [2]
hakeri [3]

Source URL: https://sysportal.carnet.hr/node/1831

Links
[1] https://sysportal.carnet.hr/taxonomy/term/71
[2] https://sysportal.carnet.hr/taxonomy/term/101
[3] https://sysportal.carnet.hr/taxonomy/term/284