ETICKÉ HACKOVANIE

Poznaj svojho nepriateľa.

Tomáš Kunka

Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava
tomas.kunka[zavináč]gmail[.]com

Abstrakt. *Aj napriek dvom desaťročiam existencie manažmentu rizík a rozsiahlych výskumných programov je veľmi veľa softvérových projektov, ktoré končia zlyhaním. Len veľmi málo prostriedkov sa vynakladá práve na manažment rizík, aj keď je to nevyhnutná súčasť projektov. Esej rozoberá etické hackovanie ako techniku v manažmente rizík, ktorá nie je v našich končinách veľmi známa. Preberá bezpečnostné riziká etických hackerov a uvažuje ako by ich bolo možné odstrániť prostredníctvom správnej výchovy v škole. Tento proces vyučovania by sa dal zovšeobecniť a použiť vo viacerých oblastiach vzdelávania. Pripája tiež kritický pohľad na etických hackerov a hľadá miesto v procese manažmentu rizík, kde by bolo využitie tejto techniky najvhodnejšie.*

Kľúčové slová: *manažment rizík, etické hackovanie, vzdelávanie*

Úvod

S rapídnym nárastom popularity Internetu, ktorý priniesol nové spôsoby komunikácie a rôzne služby, taktiež vznikol priestor pre ich zneužitie. Tak ako v každej oblasti ľudskej činnosti aj tu existuje temná stránka - kriminálnici, často označovaní ako *hackeri*. Spoločnostiam spôsobujú hmotné aj nehmotné škody. Medzi hmotné škody patrí napríklad vyradenie internetovej stránky, čo znemožňuje prácu zamestnanom firmy. Naopak medzi nehmotné škody, ktoré sú veľmi ťažko kvantifikovateľné, sa zaraďuje napríklad poškodenie dobrého mena spoločnosti, čo je často mnohokrát väčšia rana ako priama peňažná strata. Úlohou manažmentu rizík je tieto medzery v bezpečnosti identifikovať a odstrániť ich. Skúšky bezpečnosti a spoľahlivosti sa často robia cieleným poškodzovaním testovaného subjektu. Automobilové spoločnosti už dlhé roky testujú autá zrážkami s rôznymi objektmi v kontrolovanom prostredí. Rovnako sa v bojových

umeniach praktizuje cvičenie s partnerom, pri ktorom overíme účinnosť naučených techník.[1] Prečo tento prístup nevyužiť aj v počítačovej bezpečnosti?

Etické hackovanie

„Poznaj nepriateľa a poznaj seba. Tak vyhráš sto bitiek a nebudeš porazený. Ak nepoznáš nepriateľa, ale poznáš seba, raz vyhráš a raz budeš porazený. Ak nepoznáš ani nepriateľa, ani seba, určite prehráš každú bitku.“[2] Tento citát pochádzajúci z dvetisícpäťsto ročnej knihy o vedení vojny, sa môže sa zdať pre manažment rizík nepodstatný. Skúsme si ale problém počítačovej bezpečnosti predstaviť ako vojnu. Spoznajme softvér, hardvér a techniky útokov, ktoré používajú počítačoví kriminálnici = vojsko nepriateľa. Analyzujme náš softvér, hardvér a bezpečnostné postupy = naše vojsko. S týmito informáciami je už jednoduchšie zabezpečiť náš systém a predísť tak rôznym útokom. Kto však môže o sebe tvrdiť, že má všetky tieto technické informácie a znalosti?

Na „rozbitie“ počítačového systému potrebujeme niekoho, kto sa v ňom veľmi dobre vyzná a pozná jeho schopnosti. Definícia slova *hacker* sa nápadne podobá definícii hľadaného subjektu.[3]

1. človek, ktorý sa učí špecifické detaily o počítačových systémoch a možnostiach ako rozšíriť ich schopnosti, na rozdiel od väčšiny užívateľov, ktorí sa učia len minimálne potrebné zručnosti
2. človek, ktorý oddane programuje, baví ho programovanie miesto teoretizovania o programovaní
3. Často používanou definíciou je aj menej príjemná verzia. My však v eseji budeme uvažovať prvé dve uvedené.
4. človek, ktorý hľadá slabiny v počítačoch a počítačových sieťach a preniká do počítačových systémov s vidinou zisku.

Hackeri sú v spoločnosti zvyčajne označovaní ako zlí a nebezpeční ľudia. Príčinou prečo ich tak väčšina ľudí vníma je aj fakt, že sa v minulosti stali obeťami takýchto počítačových špecialistov. Myslím si, že verejná mienka je do veľkej miery ovplyvnená aj informáciami z médií, ktoré *hackerov* vykresľujú v zlom svetle. Treba si uvedomiť, že neexistujú len zlí *hackeri*. Sú tu aj bezpečnostní nezávislí profesionáli, etickí *hackeri*.[4]

Kto je etický hacker?

Etický *hacker* je počítačový bezpečnostný expert, ktorý sa špecializuje na testovanie bezpečnosti informačných systémov v spoločnostiach a organizáciách. V prvom rade to však musí byť človek dôveryhodný. Počas testovania bezpečnosti systému sa môže dostať k informáciám o klientovi, ktoré sú dôverné a ich zverejnenie môže spôsobiť škody. Používajú rovnaké nástroje a techniky ako kriminálnici, ale nepoškodzujú cieľový systém. Tu si však treba uvedomiť, že nie vždy ide všetko podľa plánu. Chceme simulovať útok, ktorý ma za cieľ systému ublížiť. Čo ak mu naozaj ublíži? Etický *hacker* musí byť naozaj profesionál, aby vedel, kde leží hranica medzi bezpečným a nebezpečným. No myslím, že aj keď sa jedná o profesionála, treba mať vopred identifikované riziká, povolenia a hlavne

zodpovednosti. Rutinný pracovný deň by sa mohol stať nočnou morou pre *hackera* a aj jeho právnika.

Komunita kriminálnych *hackerov* je stále narastajúca a ich komunikácia je často oveľa lepšia ako u ich protivníkov. Nový kriminálnici vznikajú za pomoci starých „ostrieľaných" *hackerov*. Na tento stav treba reagovať a vytvoriť akéhosi „bieleho rytiera", etického *hackera*. Ako to však spraviť? Tak isto ako vychovávame profesionálov v mnohých iných oblastiach aj tento proces musí prebiehať v škole. Či už sa jedná o univerzitu, alebo strednú školu, naskytá sa nová otázka. Netrénujeme nepriateľa?

Minimalizujme riziko vytvorenia kriminálneho hackera

Ľudia sú od prírody zvedaví. Ak ich k informáciám o prenikaní do systémov nepripustíme v bezpečnom prostredí, v škole, dostanú sa k nim na Internete. Práve vyhľadávaním týchto informácií sa dostanú pod krídla kriminálnych *hackerov*, ktorí takýmto spôsobom získavajú nových nasledovníkov.

Brian Harvey z Kalifornskej univerzity prirovnáva etické *hackovanie* k učeniu a trénovaniu karate. Karate učí nebezpečné techniky, no namiesto obmedzovania začínajúcich karatistov, ich naopak posilňuje a posmeľuje a vkladá v nich dôveru. Výsledkom však nie sú útoky a bitky karatistov v spoločnosti. Môžem hovoriť z vlastnej skúsenosti a potvrdiť, že karate vedie k disciplíne a úcte. Myslím že tento prístup je veľmi vhodný pri výchove etických *hackerov*. Brian Harvey ďalej popisuje štyri hlavné zásady, ktorými môžeme modelovať správanie človeka.

1. seriózny vzor – pri vyučovaní karate sa etika, ktorú učíme začiatočníkov, berie v komunite majstrov ako samozrejmosť. Toto treba aplikovať aj v našej spoločnosti. Profesionáli, majstri, by mali byť akýmsi vzorom pre ostatných začínajúcich bezpečnostných expertov. Veľkú časť bremena si na seba ale musí zobrať aj vedúci bezpečnostného kurzu. Tento bod osobne považujem za jeden z najdôležitejších. Ja ako študent, sa viac snažím a pripravujem na predmety, ktoré vedie inšpiratívny profesionál. Snažím sa takpovediac nesklamať jeho dôveru.
2. prístup k skutočnej moci – opäť je použitá analógia s karate. Neexistujú dva typy karate. Jeden pre dospelých a druhý pre deti. Mali by sme študentom poskytovať rovnaké technológie ako profesionálom. Pod týmto rozumieme napríklad rôzne výpočtové prostredia. S týmto sa veľmi nestotožňujem, pretože sa tu jedná skôr o ekonomický problém. Nie všetky univerzity majú financie, potrebné na uskutočnenie tohto plánu, a hlavne tie slovenské.
3. možnosť riešiť náročné problémy a prístup k expertom – každý študent by mal možnosť stretnutia a konzultácie s odborníkom zo školy. Tento bod oceňujem oveľa viac ako predchádzajúci. Toto môžu zaviesť aj školy s nižším rozpočtom, pretože tie tiež zamestnávajú kvalitných expertov. V našej škole je to do istej miery zavedené a funguje to.
4. bezpečné miesto na experimentovanie – keď pri karate cvične zápasíte s človekom s čiernym pásom, existuje oveľa nižšia pravdepodobnosť, že sa niekto z vás zraní, ako keď zápasíte s menej skúseným súperom. Študent potrebuje kontakt s ozajstnou osobou, vie si tak lepšie predstaviť dôsledky svojho konania

> ako pri útokoch na akéhosi abstraktného majiteľa firmy. Toto považujem za absolútnu samozrejmosť. Učiť sa niečo len počúvaním alebo čítaním nemá zmysel, ak nedôjde k okamžitému odskúšaniu. Bez špecializovaných laboratórií na výučbu bezpečnosti nie je jednoduché vychovávať expertov.[5]

Podľa mňa existuje ešte jeden bod. Je veľmi účinný, no uvádzam ho ako posledný, pretože ho nepovažujem za práve najšťastnejšie riešenie. Je to skôr akási záchranná brzda. Týmto bodom je strach. Študenti by si mali uvedomiť, že ostať anonymný nie je úplne jednoduché. Mali by sa právom obávať postihnutí, či už zo strany univerzity, alebo zákona. Tu ale vidím problém, keďže zákony nie sú dosť pružné a nestíhajú reagovať na enormný technický pokrok.

Pri študovaní tejto problematiky som sa stretol hlavne s obavami z toho, aby sa aj tak nakoniec študenti nestali kriminálnikmi. No narazil som aj na zaujímavý názor, že etický *hackeri* sú len deti hrajúce sa na vlastnom piesočku.

Čo je správna motivácia?

Ako internetová akciová bublina je označované obdobie, keď výrazne narástla hodnota spoločností, podnikajúcich v oblasti internetu. Toto obdobie vyvrcholilo v roku 2000. Práve vtedy začali vznikať etickí *hackeri,* ktorí sa neohrozene pustili do boja s kriminálnymi *hackermi* a začali krotiť tento novovzniknutý digitálny Divoký západ.

Vzrušenie a chuť zvádzať súboje s kriminálnikmi, prilákala do odvetia informačnej bezpečnosti príliš veľa ľudí. Títo odborníci sú často rozptyľovaný novými technológiami a vidinou dobrodružstva pri ich vytúžených súbojoch. Nebolo by na tom nič zlé, keby sa nehrali na Wyatta Earpa za peniaze a čas spoločnosti, pre ktorú pracujú. Nemožno im to však vyčítať, pretože na písaní metodík a neustálom opravovaní systému veľa zábavy nenájdu.

Vedúci projektov chcú odborníkov, ktorí zabezpečia, že nedôjde k žiadnym narušeniam bezpečnosti. Chcú od zamestnancov efektívny manažment rizík, no motivujú ich skôr k opaku. Motivácia zamestnanca sú peniaze. Za čo sú ľudia platení? Dostanú peniaze za rok, ktorý bol bez bezpečnostných incidentov, alebo za nadčasy pri ktorých odstraňujú chyby? Bežne dostávajú peniaze za odpracované nadčasy, čo ich veľmi nemotivuje k predchádzaniu chýb. Predvídanie chýb by malo byt prioritou, nie reakcia na chyby.[6]

Načo sú nám teda etický hackeri?

Etické *hackovanie* nie je univerzálne technika, ktorá sa dá využiť vždy a všade. Jej využitie je zrejmé v oblasti počítačovej bezpečnosti, napríklad ako penetračný tester. Aké sú však iné problémy v manažmente rizík, a v ktorej fáze procesu manažmentu rizík je vhodné využiť túto techniku? Mnohí skúsení manažéri považujú za najzložitejšiu časť práce s rizikami ich identifikáciu.[7] Myslím, že pri tejto úlohe by sa mohli tiež využiť znalosti etického *hackera*, keďže ako odborník na bezpečnosť má množstvo skúseností a mohol by vedieť identifikovať nové pravdepodobné riziká, vyplývajúce z návrhu softvéru. Išlo by o snahu predchádzať chybám, keďže ich odhalenie pri testovaní a následné odstránenie by mohlo byť nákladné. Etický *hacker* by mohol na základe svojich poznatkov a často sa

opakujúcich chýb, vypracovať metodiku pre bezpečný vývoj určitých častí softvéru. Návrhy a poznámky *hackera* by mohli využiť vývojári pri implementácii. Ako je však spomenuté v predošlej kapitole, treba zamestnancov odmeňovať za softvér bez chýb.

Záver

Etické *hackovanie* predstavuje jeden hlavný problém – je možné etickému *hackerovi* veriť? Táto otázka nie je ani tak záležitosťou informatiky, ale skôr otázka na morálku človeka. To je už čisto vo filozofickej rovine. Eseji sa pokúsila navrhnúť a vyjadriť názor na akúsi správnu výchovu, ktorou by sa minimalizovalo riziko vzniknutia kriminálneho *hackera*, ktorý by spôsobil škody spoločnosti. Z eseje vplýva, že proces výchovy by mohol byť vhodný a použiteľný pri vyučovaní rôznych predmetov na rôznych stupňoch škôl. Poukazuje na nesprávnu motiváciu zamestnancov pri manažmente rizík a uvažuje zaradenia etického *hackera* už v procese identifikácie rizík. Aj napriek rizikám, vidí v osobe etického *hackera* viac pozitív ako negatív.

Použitá literatúra

1. Greene Tim, Training The Enemy. [Online] 18. 06. 2004. [Dátum: 15. 10. 2012.] http://www.infosecwriters.com/texts.php?op=display&id=185
2. Sun Tzu, Art of War, Westview Press, USA, 1996 Translated by Zdenek Šustr. ISBN 83-7361-821-X
3. C. C. Palmer. 2001. Ethical hacking. IBM Syst. J. 40, 3 (March 2001), 769-780.
4. Syed A. Saleem. 2006. Ethical hacking as a risk management technique. In Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD '06). ACM, New York, NY, USA, 201-203.
5. Harvey, Brian, Computer Hacking and Ethics, University of California, Berkeley, [Online][Dátum: 15. 10. 2012.] http://www.cs.berkeley.edu/~bh/hackers.html
6. Heisser Jay, Industry needs less ethical computer hacking, more risk management strategies, [Online][Dátum: 22. 11. 2012.] http://searchsecurity.techtarget.com/Industry-needs-less-ethical-computer, posledný prístup 22.11.2012
7. Edzreena Edza Odzaly and Paul Sage Des Greer. 2009. Software risk management barriers: An empirical study. In Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement (ESEM '09). IEEE Computer Society, Washington, DC, USA, 418-421.

Annotation

Ethical hacking

Despite at least two decades of software risk management research, including some extensive research programs, software project failure is frequent. Resources for software risk management

remain limited despite its importance in software projects. Essay discusses ethical hacking as one technique of risk management, lesser known in our country. It points out risks of ethical hacking and suggests solutions for these risks by proper education in school. These suggestions are universal and can be used in many other areas of education. It also brings critical view of ethical hackers and searches for right spot for them in risk management process.