Varnost računalniških sistemov na internetu

Borut Žnidar, IBM Slovenija
borut.znidar@si.ibm.com

Povzetek

Eksplozivna rast interneta je prinesla elektronsko trgovino in bančništvo, elektronsko pošto, pripomočke za skupinsko delo, lažji dostop do materialov, distribucijo informacij itn. Žal pa ta napredek in varnosti ogrožajo kriminalni hekerji. Podjetja, posamezniki in država se bojijo zlorab, kraje informacij, ponarejanja identitete, spreminjanja dokumentov ipd. Prireševanju tovrstnih zadreg lahko pomagajo t.i. etični hekerji. Članek opisuje način njihovega delovanja, znanje, pristop in kako lahko pomagajo strankam povečati varnost pri delu z internetom.

Abstract

Security of the Computer Systems on the Internet

Explosive growth of the Internet has brought many good things: electronic commerce, e-mail, collaborative computing, easier access to reference material, information distribution, to name a few. Unfortunately, all this advancement reveals brought also the dark side: criminal hackers. Companies, private citizens and government would like to be part of this revolution, but there is always fear of misuse of information, identity, change of documents,... With this in mind we can call on ethical hackers for help. This paper describes the way ethical hackers work, their knowledge, approach and how they can help customers to improve security while working on Internet.

1 Uvod

Internet ali medmrežje je svetovni sistem računalniških omrežij – omrežje omrežij, v katerem lahko uporabniki na poljubnem računalniku dostopajo do informacij na drugem računalniku, če imajo pravico dostopa. Nastanek omrežja je omogočila ARPA (Advanced Research Projects Agency) in je bilo v začetku znano kot ARPANET. Osnovni namen je bil vzpostavitev omrežja med raziskovalnimi računalniki na različnih univerzah. Stranski učinek izbrane arhitekture je bil delovanje omrežja tudi v primeru izpada dela omrežja.

Danes je internet javno omrežje, dostopno miljonom ljudi po vsem svetu. Zaradi dostopnosti, enostavnosti uporabe, zanesljivosti in hitrosti je internet postal zanimiv tudi za organizacije, ki so želele svojo dejavnost razširiti z elektronskim poslovanjem. Internet jim je omogočil:

- izvajati elektronsko bančništvo,
- izboljšati uporabniške storitve,
- izboljšati sodelovanje s partnerji,
- zmanjšati stroške komunikacije,
- izboljšati interno komunikacijo,
- hitrejši dostop do potrebnih informacij.

Internet je naredil revolucijo v načinu poslovanja podjetij, na drugi strani pa je prinesel tveganje, ki je lahko usodno za poslovanje podjetij. Vdori v internetu lahko privedejo do izgube denarja, časa, izdelkov, ugleda, zaupnih informacij itn.

Vsi ti razlogi so zadosten pogoj za povečano zanimanje IT strokovnjakov in vodstev podjetij za načine varovanja računalniških sistemov v dobi internetnega poslovanja.

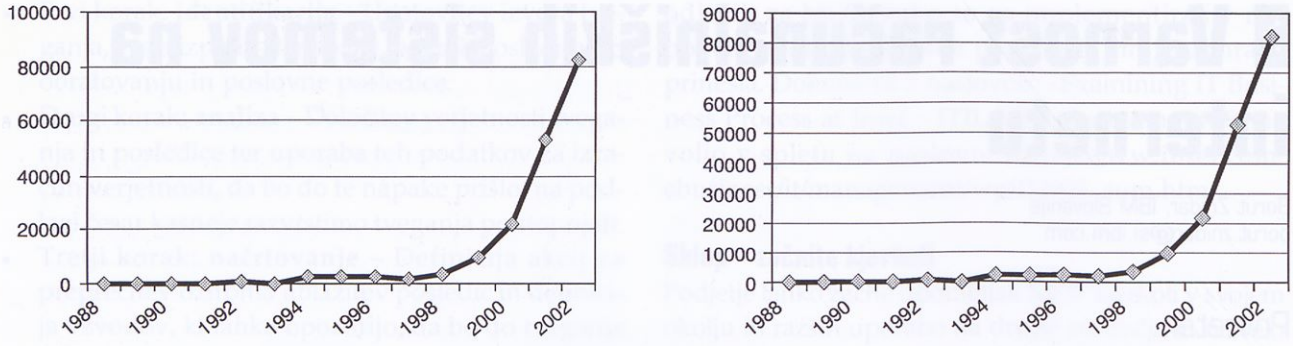
V nadaljevanju opisujemo razvoj napadov na internetu, sedanje stanje in najpogostejše načine napadov. Nadalje so opisani enostavnejši in bolj kompleksni načini zaščite.

2 Značilnosti vdorov v računalniške sisteme na internetu

Ob vzpostavitvi interneta je bil glavni namen le-tega pripraviti čimboljšo funkcionalno podlago za povezovanje in sodelovanje računalnikov v velikem omrežju. Varnost ni bila primarna naloga in zato je tudi uporabljena tehnologija dopuščala možnosti zlorabe.

Število vdorov v računalniške sisteme na internetu skozi leta lahko ocenimo na podlagi prijav centru CERT, kar prikazuje slika 1.

V nadaljevanju bomo pogledali nekaj institucij in projektov, ki so pomagali pri boljšem vpogledu v količino, obliko in namen vdorov na internetu, kakor tudi način zavarovanja pred njimi.



Slika 1: **Incidenti javljeni v CERT/CC [2]**

2.1 Koordinacijski center CERT

Koordinacijski center CERT (Computer Emergency Response Team) [1] je bil ustanovljen leta 1988 po pojavu internetnega črva Morris.

Namen CERT/CC je reagirati na varnostne težave na internetu, predstavljati centralno točko za prijavljanje odkritih varnostnih ranljivosti, služiti kot model pri vzpostavljanju za odzivanje na varnostne dogodke (incident response teams) in dvig zavesti o varnostnih problemih.

Od ustanovitve se je CERT/CC odzval na prek 50.000 varnostnih incidentov, ki so vplivali na stotisoče internetnih strani, delal je na več kot 1600 javljenih pomankljivosti/ranljivostih in izdal stotine priporočil in objav. Dodatno je pomagal pri vzpostavljanju osemdesetih drugih ekip za odzivanje na varnostne dogodke.

2.2 Eksperiment San Diego

Konec leta 1999 so v San Diego Supercomputer centru na internet priključili strežnik (Red Hat Linux v5.2) brez dodatnih varnostnih dodatkov ali nastavitev [5]. Strežnik ni bil v uporabi in njegova namestitev ni bila nikjer objavljena. Služil je le kot pasivna tarča za napadalce, na katerem so nato opazovali dogajanje:

- 8 ur po namestitvi:
  - poskus uporabe "Solaris RPC" ranljivosti – neuspešno;
- 21 dni po namestitvi:
  - 20 poskusov izrabe raznih ranljivosti, vključujočih POP, IMAP, telnet, RPC, mountd, ki pa so bili neuspešni, ker so bili narejeni za Red Hat 6.x;
- 40 dni po namestitvi:
  - uspešno izrabljena ranljivost POP serverja,
  - brisani nekateri sistemski logi,
  - instaliran rootkit in sniffer.

Ta poizkus je tako že pred leti pokazal, da je sistem že takoj, ko je priključen v internet, izpostavljen napadom, tudi če na njem sploh ni v uporabi noben servis. Razlika po štirih letih od poizkusa je le v tem, da je čas od priklopa do začetka napadov v povprečju bistveno krajši.

2.3 Projekt pregleda nad internetom

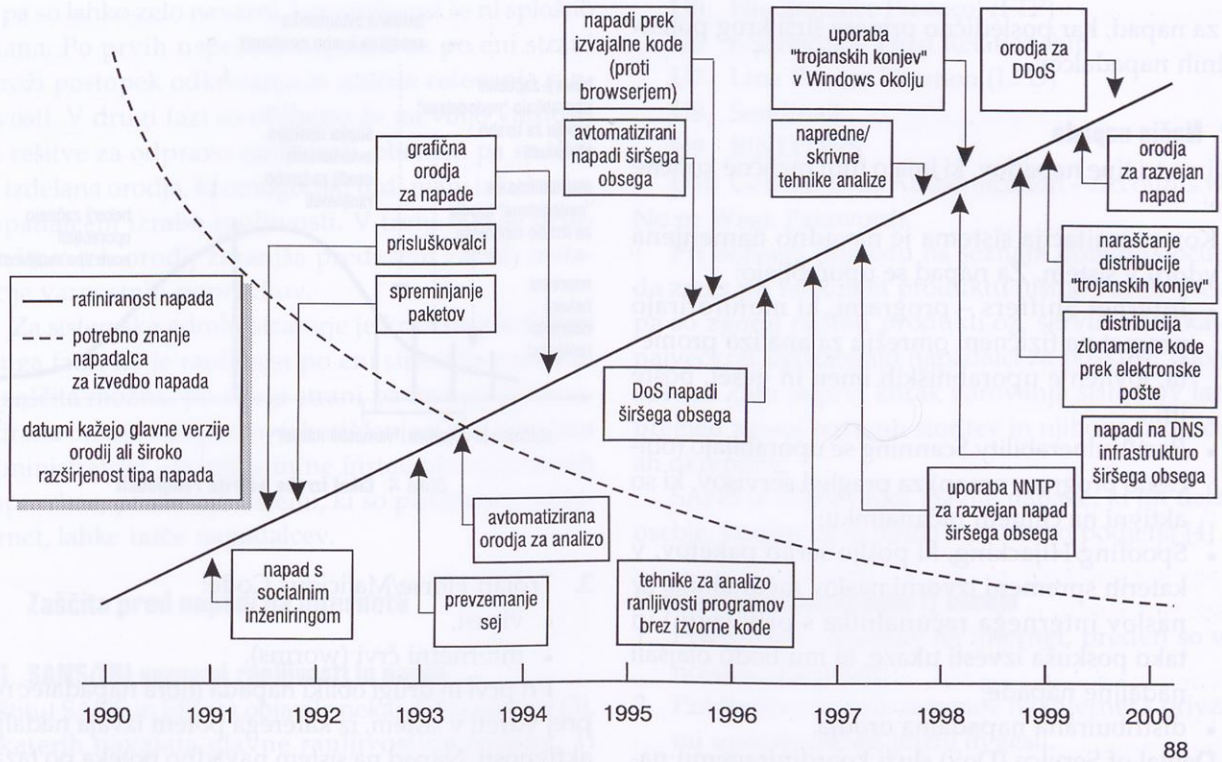
Projekt pregleda nad internetom (Internet Auditing Project) [6] poskuša gledati na varnost na internetu kot celoto, ne le kot na varnost posameznih računalnikov in omrežij. Projekt obravnava internet kot živ organizem, ne pa kot omrežje.

Projekt je leta 1999 začel Liraz Siri. Prvi varnostni pregled interneta je pokril 36 milijonov IP naslovov, kar je decembra 1998 pomenilo 85 % aktivnega adresnega prostora.

Preverjanje je trajalo dvajset dni in je bilo vzporedno izvajano iz Izraela, Mehike, Rusije, Japonske in Brazilije. Naslovnega prostora je bilo za 300 milijonov IP naslovov. Preverjenih je bilo osemnajst ranljivosti operacijskih sistemov Unix in v tem času so našli 730.000 ranljivosti na 450.000 računalniških sistemih. Projekt je opozoril na veliko ranljivost interneta in na številne sisteme, na katerih ni zagotovljena niti minimalna raven varnostne zaščite.

2.4 Inštitut SANS

SANS (System Administration, Networking and Security) Institute je bil ustanovljen leta 1989 kot raziskovalno-izobraževalna organizacija; več kot 156.000 var-



Slika 2: **Kompleksnost napadov glede na tehnično znanje napadalcev (po letih)**

nostnim strokovnjakom, nadzornikom (auditor), sistemskim in mrežnim administratorjem omogoča izmenjavo informacij in pomaga pri reševanju težav in izzivov, s katerimi se srečujejo. Njegovo jedro so varnostni strokovnjaki v državnih agencijah, organizacijah in univerzah po vsem svetu, ki investirajo stotine ur vsako leto v razvoj in izobraževanje za informacijsko varnost.

3 Napadalci in načini napadov

3.1 Kdo je "hacker" in kdo "cracker"

Heker (angl. hacker) je izraz, s katerim nekateri označujejo "spretnega programerja", drugi pa "nekoga, ki poskuša vdreti v računalniški sistem".

1. Eric Raymond, avtor *The New Hacker's Dictionary*, je definiral hekerja kot spretnega programerja. Dober "hack" je spretna rešitev programerskega problema in "hacking" je oznaka tega dela.
   Raymond ne priporoča uporabe tega izraza za tiste, ki poskušajo vdreti v sistem drugih ali na drug način uporabljajo znanje programiranja ali drugo strokovno znanje za zlonamerno delovanje. Za te predlaga izraz "cracker".
2. Novinarji pretežno uporabljajo izraz heker za nekoga, ki poskuša vdreti v računalniški sistem. Navadno je to izkušen programer ali inženir z dovolj tehničnega znanja, da razume šibke točke v varnostem sistemu.

Cracker je oseba, ki vdre v računalniški sistem nekoga drugega, ki je običajno priključen v omrežje, obide geslo ali licence računalniškega programa ali na drug način nalašč prebije računalnikovo zaščito. Cracker dela to za zaslužek, zlonamerno, za kakšen nesebičen namen ali načelo, ali zgolj zato, ker se je pojavila priložnost. Nekateri vdori so bili opravljeni navidezno, da bi pokazali slabosti v varnostnem sistemu.

Za napadalce na računalniške sisteme prek interneta je značilno, da:

- z napadi gradijo tehnično znanje in izkušnje,
- pridobivajo vpliv z avtomatizacijo,
- raziskujejo medmrežne povezave in enostavno gibanje skozi infrastrukturo,
- postajajo bolj izkušeni pri zakrivanju svojega delovanja.

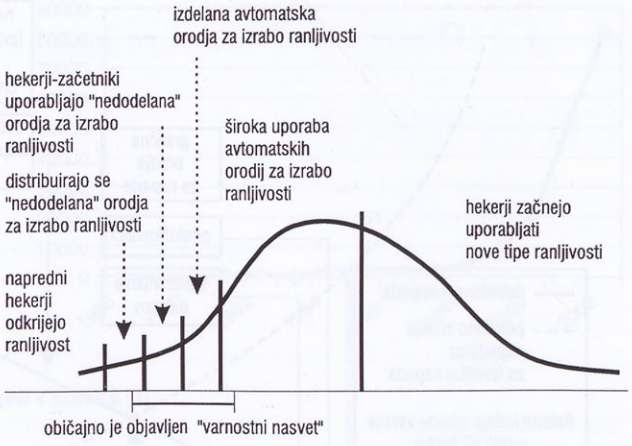
Kot nam kaže slika 2, se kompleksnost napadov povečuje, obenem pa se zmanjšuje tehnično znanje napadalcev. To je posledica vedno bolj dodelanih oro-

dij za napad, kar posledično prinese širši krog potencialnih napadalcev.

3.2 Način napada

Ločimo tri tipe napadov, ki imajo tudi različne končne cilje:

1. Kompromitacija sistema je navadno namenjena vdoru v sistem. Za napad se uporabljajo:
   - Internet Sniffers – programi, ki monitorirajo promet na fizičnem omrežju za analizo prometa, lovljenje uporabniških imen in gesel, pošte itn.;
   - Port/Vulnerability Scanning se uporabljajo (običajno program nmap) za pregled servisov, ki so aktivni na ciljnem računalniku;
   - Spoofing/Hijacking, ki pošlje serijo paketov, v katerih spremeni izvorni naslov računalnika (v naslov internega računalnika s privilegiji) in tako poskuša izvesti ukaze, ki mu bodo olajšali nadaljne napade;
   - distribuirana napadalna orodja.
2. Denial of Service (DoS) služi koordiniranemu napadu na sisteme internet z namenom, da jih zruši:
   - enostavni DoS – namen napadalca je napraviti ciljni računalnik nedosegljiv uporabnikom;
   - distribuirani Denial of Service (DDoS) – pri tem načinu napada uporabimo isto tehnologijo kot v DoS napadu, le da je napad izveden iz več (že napadenih in zavzetih) računalnikov hkrati.



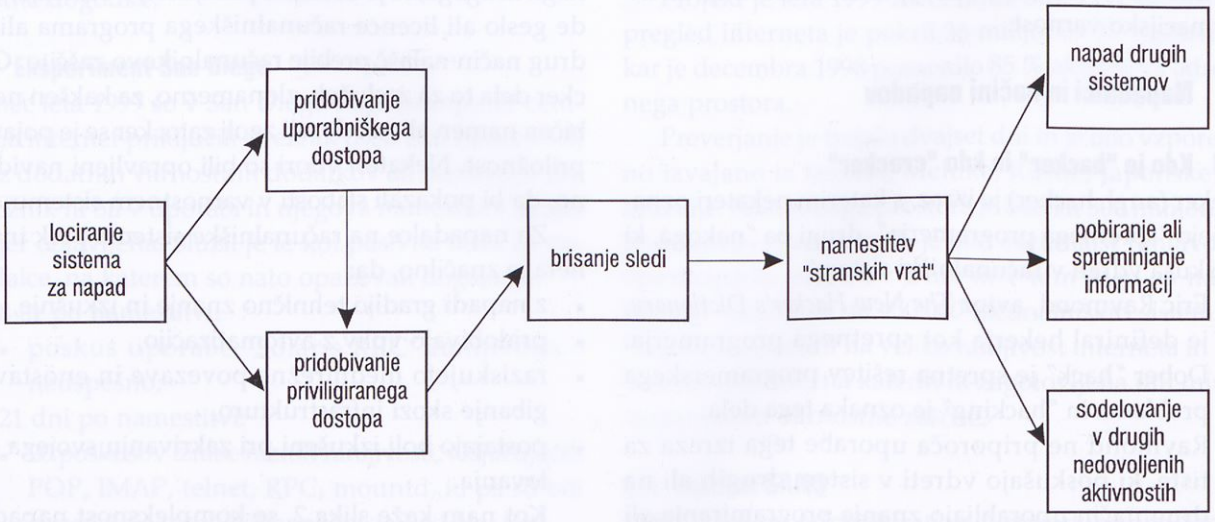
Slika 4: **Cikel izrabe odkrite ranljivosti**

3. Trojan Horse/Malicious Code:
   - virusi,
   - internetni črvi (worms).

Pri prvi in drugi obliki napada mora napadalec najprej vdreti v sistem, iz katerega potem izvaja nadaljne aktivnosti. Napad na sistem navadno poteka po fazah, ki jih prikazuje slika 3.

Ranljivosti, ki jih napadalci izrabljajo, pokažejo določene zakonitosti uporabe, ki jih kaže slika 4.

V prvi fazi izkušeni napadalci odkrijejo ranljivost in tudi izdelajo prva orodja za njihovo izkoriščanje, ki pa so običajno precej zahtevna za uporabo. V tej fazi je število možnih napadalcev relativno majhno, napa-



Slika 3: **Običajen potek napada.**

di pa so lahko zelo nevarni, ker ranljivost še ni splošno znana. Po prvih uspešnih napadih se po eni strani sproži postopek odkrivanja in zaščite reševanja ranljivosti. V drugi fazi so običajno že na voljo varnostne rešitve za odpravo ranljivosti, obenem pa so tudi že izdelana orodja, ki omogočajo tudi manj izkušenim napadalcem izrabo ranljivosti. V tretji fazi se učinkovitost teh orodij zmanjša predvsem zaradi instalacije varnostnih popravkov.

Za sistemske administratorje je kritična predvsem druga faza, ko je ranljivost po eni strani že znana in je zaščita možna, po drugi strani pa imamo avtomatizirana orodja za njihovo izkoriščanje. Če v tem času administratorji »zaspijo« in ne instalirajo varnostnih popravkov, postanejo sistemi, ki so priključeni na internet, lahke tarče napadalcev.

4 Zaščita pred napadi na internetu

4.1 SANS/FBI seznami ranljivosti in napak

Inštitut SANS in FBI sta objavila nekaj dokumentov [3], v katerih navajata glavne ranljivosti in napake. Ti seznami ranljivosti in napak so koristna informacija, saj večina uspešnih napadov na računalniške sisteme na internetu temelji na ranljivostih iz spodnjih seznamov.

Glavne ranljivosti Windows sistemov

W1 Internet Information Services (IIS)

W2 Microsoft Data Access Components (MDAC) – Remote Data Services

W3 Microsoft SQL Server

W4 NETBIOS – Unprotected Windows Networking Shares

W5 Anonymous Logon – Null Session

W6 LAN Manager Authentication – weak LM Hashing

W7 General Windows Authentication – Accounts with No or Weak Passwords

W8 Internet Explorer

W9 Remote Registry Access

W10 Windows Scripting Host

Glavne ranljivosti Unix sistemov

U1 Remote Procedure Call (RPC)

U2 Apache Web Server

U3 Secure Shell (SSH)

U4 Simple Network Management Protocol (SNMP)

U5 File Transfer Protocol (FTP)

U6 r-Services – Trust Relationship

U7 Line Printer Daemon (LPD)

U8 Sendmail

U9 BIND/DNS

U10 General Unix Authentication – Accounts with No or Weak Passwords

Pri bežnem pogledu na seznam dobimo občutek, da zares pri nobenem produktu nismo varni. Vseeno pa so zgoraj našteti produkti oz. servisi tisti, katere največkrat uporabljajo napadalci za poskuse vdora v sistem. Zato je prvi korak varovanja sistemov lahko pregled zgoraj naštetih storitev in njihova izključitev ali okrepitev.

SANS je objavil tudi glavne napake, ki jih dela IT osebje, končni uporabniki in vodstvo podjetja [4] .

Glavne varnostne napake IT osebja

1. Priključitev sistemov na internet, preden so varnostno okrepljeni.
2. Priključitev testnih sistemov na internet s privzetimi uporabniškimi imeni in gesli.
3. Neupešna posodobitev sistemov po odkritih varnostnih luknjah.
4. Uporaba telneta in drugih nekriptiranih protokolov za upravljanje sistemov, routerjev, požarnih pregrad in PKI.
5. Dodeljevanje in sprememba uporabniških gesel prek telefona brez avtorizacije prosilca.
6. Neuspešno upravljanje in testiranje varnostnih kopij.
7. Delovanje nepotrebnih servisov, npr. ftpd, telnetd, finger, rpc, mail, r-servisov idr.
8. Implementacija požarne pregrade s pravili, ki ne zaustavijo zlonamernega in nevarnega prometa.
9. Neuspešna vzpostavitev ali posodobitev sistema za odkrivanje virusov.
10. Neuspešno izobraževanje uporabnikov o potrebnih akcijah v primeru varnostnih problemov.

Glavne napake vodstva podjetij

1. Dodelitev neusposobljenih ljudi na varnostne funkcije, brez možnosti za usposabljanje za obvladovanje varnosti.
2. Nerazumevanje razmerja med varnostjo informacij in poslovnimi problemi. Razumejo le fizično varnost in ne vidijo posledic slabe varnosti informacij.

3. Nezmožnost izvajanja operativnih nalog varnosti: stalna kontrola, da so sistemi na zadnjem nivoju popravkov.
4. Zanašanje predvsem na požarno pregrado.
5. Nezmožnost ugotoviti, koliko so vredne informacije in sloves podjetja.
6. Odobritev zakasnelih, kratkoročnih popravkov, zato se problem hitro povrne.
7. Upanje, da bo problem izginil, če ga bodo ignorirali.

Glavne varnostne napake končnih uporabnikov

1. Neuspešna instalacija antivirusnih programov, njihovo redno vzdrževanje (popravkov in virusnih definicij) ter njihova implementacija na vse datoteke.
2. Odpiranje prilog elektronske pošte brez preverjanja pošiljatelja in vsebine ali izvajanje iger in ohranjevalnikov zaslona iz nepreverjenih virov.
3. Neuspešna instalacija varnostnih popravkov, predvsem za Microsoft Office, Microsoft Internet Explorer in Netscape.
4. Ni izdelave varnostnih kopij oz. njenega preverjanja.
5. Uporaba modema ob hkratni priključenosti na lokalno omrežje.

Ti trije seznami pomenijo predvsem dobro izhodiščno točko pri odpravljanju problema internetnih napadov. Predstavljajo najpogostejše napake in če jih pričnemo upoštevati, bomo krepko zmanjšali možnost napadov.

5 Etični heking

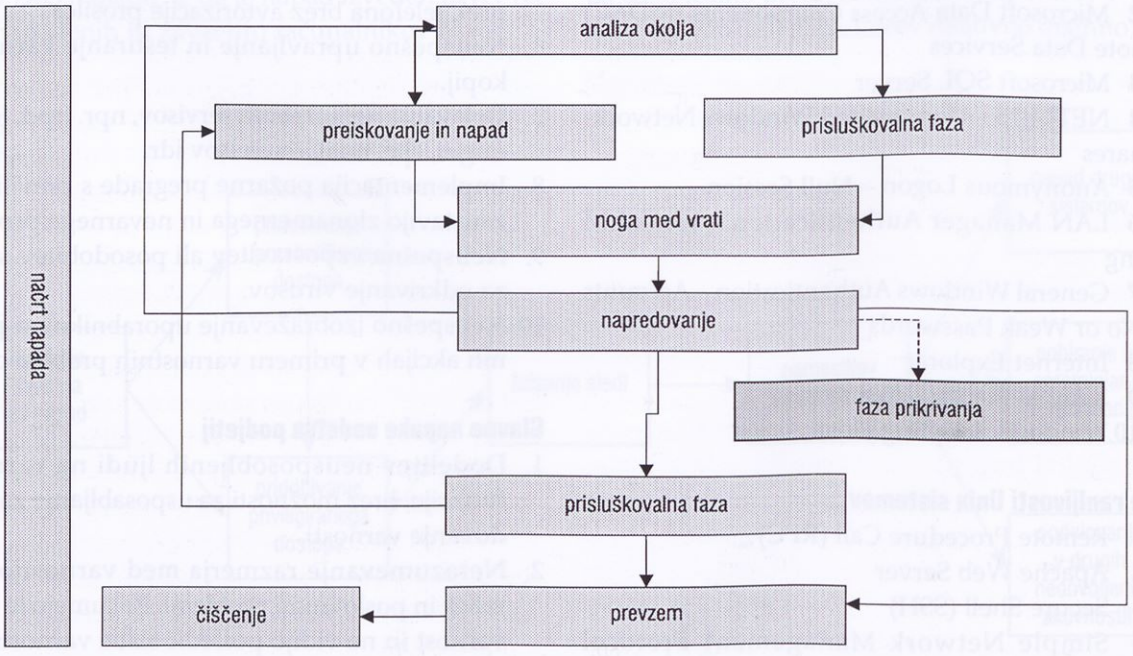
5.1 Kdo je „etični heker“

Etični heker je računalniški in mrežni strokovnjak, ki izvaja napad na računalniški sistem na podlagi zahteve lastnika tega sistema. Pri tem išče pomankljivosti, ki bi jih zlonamerni heker lahko izkoristil. Za preverjanje varnosti sistema uporablja iste metode kot crackerji, vendar ugotovitve ne izkoristi, temveč jo objavi v poročilu.

Etični heking je poznan tudi pod imenom test vdora (penetration testing, intrusion testing) ali "red teaming". Etičnega hekerja včasih imenujejo tudi "white hat"; izraz prihaja iz starih vesternov, kjer so"dobri fantje" nosili bele klobuke, "slabi fantje" pa črne.

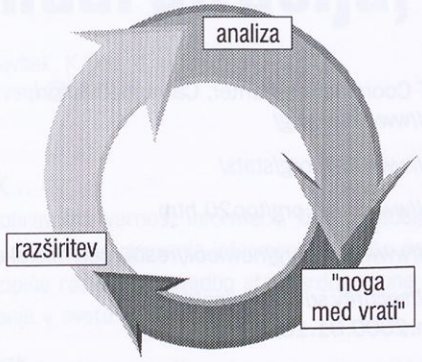
5.2 Metodologija

Metodologija, ki jo uporabljajo etični hekerji, je podobna napadom crackerjev in je sestavljena iz treh de-



Slika 5: **Diagram napada**

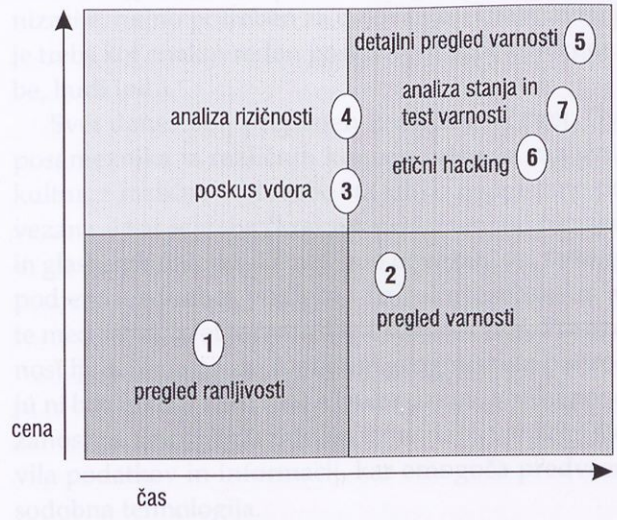
lov: analize, vdora, stopnjevanja. Ta pristop se ponavlja ciklično in predstavlja napadalni cikel:



- Analiza okolja (Reconnaissance):
  - pridobivanje informacij,
  - iskanje ranljivosti.
- Noga med vrati:
  - izkoristi ranljivost,
  - pridobivanje dostopa.
- Stopnjevanje:
  - povečanje privilegijev (pridobivanje administracijskih privilegijev).

Razdelani diagram napada prikazuje Slika 5:

1. Analiza okolja (Reconnaissance) – nabiranje informacij o ciljnem sistemu ali omrežju.



Slika 6: **Vrste preverjanja varnosti interneta**

2. Preiskovanje in napad (Probe and attack) – preiskovanje slabosti sistema in priprava/izbira orodij za napad.
3. Noga med vrati (Gaining a toehold) – izraba varnostnih slabosti za pridobivanje dostopa v sistem.
4. Napredovanje (Advancement) – napredovanje iz nepriviligiranega v priviligiranega uporabnika.
5. Faza prikrivanja (Stealth phase) – skrivanje sledov.
6. Prisluškovalna faza (Listening phase) – vzpostavi prisluškovanje z uporabo snifferjev.
7. Prevzem (Takeover) – razširitev kontrole iz enega sistema na druge sisteme v omrežju.
8. Čiščenje (Cleanup).

Servis etičnega hekinga navadno ne vključuje faze prikrivanja, razen če stranka to zahteva.

5.3 Open-Source Security Testing Methodology

ISECOM [8] (Institute for Security and Open Methodologies) je organizacija, ki je pripravila predlog metodologije OSSTMM [9], [10] z natančno razdelanim načinom izvedbe varnostnega testiranja. Glede na vloženo količino časa in denarja razlikujejo različne vrste testiranja, od najenostavnejšega pregledovanja ranljivosti, prek etičnega hekinga do celotnega varnostnega pregleda, kar prikazuje slika 6.

Njihov varnostni načrt obsega pregled šestih med seboj povezanih področij, ki vsebujejo elemente drugih področij in pokažejo pravo sliko testiranja šele kot celota:

1. informacijska varnost (information security),
2. procesna varnost (process security),
3. varnost internetne tehnologije (Internet technology security),
4. komunikacijska varnost (communications security),
5. varnost "wireless" tehnologije (wireless security),
6. fizična varnost (physical security).

5.4 Izvajanje storitve etičnega hekinga

IBM varnostni servis [11] »internet varnostni pregled« [12] simulira poskus vdora v naročnikov IT sistem v kontroliranem in za naročnika varnem načinu. Storitev je poglobljena in obsežna, poleg vidika vdora pa pokriva še konfiguracijo in upravljanje sistemov, s čimer celovito obravnava vse dejavnike, ki bi lahko negativno vplivali na internetno varnost stranke v prihodnosti.

Storitev daje kot rezultat celovit pregled nad varnostnim stanjem internetnega dostopa na tehničnem

in upravljalskem nivoju. Pregled s tehnološkega vidika vsebuje testiranje različnih načinov vdorov in analizo konfiguracije ter s tem daje pregled nad stanjem in pove šibke točke varnosti internetnega dostopa do virov podjetja. Upravljalski vidik pregleda se opravi s pogovori z administratorji in vodilnimi v podjetju o varnostni dokumentaciji, procesih in standardih. Oba pregleda skupaj dajeta podroben vpogled v stanje varnosti internetnega dostopa in pripravljenost na morebitne poskuse vdora nepooblaščenih tretjih oseb z interneta.

6 Sklep

Internet je nova poslovna paradigma, ki se razvija in ponuja številne možnosti za ljudi z vizijo in pogumom. Učinkovito konkuriranje v globalni ekonomiji zahteva od podjetij prilagajanje povečanje stopnje odprtosti in dostopnosti. Vendar morajo podjetja, ki poskušajo prodreti na novi obetajoči trg, ki ga ponuja internet, določiti in izvesti močne varnostne postopke, tako za povečanje svojih informacijskih sistemov, kakor tudi za ohranjanje zaupanja strank.

Internet je bil razvit za zagotavljanje dinamičnih, prilagodljivih in odprtih komunikacij med več različnimi sistemi. Zaradi svoje odprte zasnove sam po sebi ne more zagotavljati zaščite vključenih informacijskih sistemov.

Varnost informacijskih sistemov postaja z uporabo interneta in e-poslovanja vse pomembnejša in zaradi vključevanja osnovnih poslovnih dejavnostni v internetni način poslovanja tudi vse bolj izpostavljena. Zato bo še treba veliko pozornosti namenjati zagotavljanju in vzdrževanju varnosti IT sistemov na internetu.

7 Viri

[1] CERT Coordination Center, Carnegie Mellon, *http://www.cert.org/*

[2] *http://www.cert.org/stats/*

[3] *http://www.sans.org/top20.htm*

[4] *http://www.sans.org/newlook/resources/mistakes.php*

[5] *http://security.sdsc.edu/incidents/worm.2000.01.18.shtml*

[6] *http://www.viacorp.com/auditing.html*

[7] *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html*

[8] ISECOM – Institute for Security and Open Methodologies, *http://www.isecom.org/*

[9] OSSTMM - Open Source Security Testing Methodology Manual, *http://www.osstmm.org/*

[10] Herzog, Pete: OSSTMM 2.1. - Open-Source Security Testing Methodology Manual, 2003, *http://www.isecom.ca/mirror/osstmm.en.2.1.pdf*

[11] *http://www-3.ibm.com/security/index.shtml*

[12] *http://www-1.ibm.com/services/security/-intrspec.html*

Borut Žnidar zadnjih šest let del v IBM Slovenija, kjer dela na področjih varnosti, Unix in Linux operacijskih sistemov ter velikih strežnikov za slovenske stranke in tudi pri večjih projektih v regiji. Pred tem je osem let delal na pripravi, razvoju, implementaciji in vzdrževanju sistema za laboratorije v zdravstvu.