VISOKA POSLOVNA ŠKOLA
STRUKOVNIH STUDIJA
ČAČAK

DIPLOMSKI RAD

Siguran osobni racunar

Mentor:_____
Profesor: _____

Student: _____
Br.Indeksa: _____

SADRŽAJ

1. UVOD

Kroz povijest postojali su izumi koji su fundamentalno izmijenili svijet. U modernom vremenu, nastanak Interneta i World Wide Weba može se smatrati čudom i svrstati u jedan od takvih izuma. Unutar jednog desetljeća ti izumi su izmijenili način na koji ljudi rade, uče, kupuju i zabavljaju se, način na koji ljudi komuniciraju. Gotovo svaki podatak koji bi mogao nekad zatrebati postao je dostupan klikom miša.

No, pored svih prednosti i mogućnosti koje Internet pruža, omogućio je i nastanak nove vrste kriminala. Kao što to biva sa svim novim izumima koji su nastali s plemenitom namjerom, počevši još od Nobela i dinamita, zlonamjerni ljudi su pronašli način da zloupotrijebe Internet da bi ostvarili vlastite ciljeve – zaradu, osvetu, pakost...

Svakom novajliji i početniku Internet pruža pristup jednom privlačnom i uzbudljivom svijetu. Internet povezuje čitav svijet i istovremeno je i jedan svijet sam za sebe. No, taj svijet je isto tako i nedorečen, nedovoljno reguliran – ne postoje primjereni i učinkoviti zakoni za održavanje sigurnosti, te obiluje neugodnim iznenađenjima. Iako je Internet danas svuda prisutno sredstvo komunikacije i istraživanja, važno je zapamtiti da je Internet dvosmjerna ulica – računalo se povezuje s Internetom i Internet se istovremeno povezuje s tim računalom.

Svaka organizacija ili pojedinac koji se povezuje s Internetom zapravo je svakodnevno podložan riziku i uspostavljanje i održavanje vlastite sigurnosti je postalo nužno. Razne opasnosti vrebaju sa svih strana. Opasnosti koje zbog nedostatka opreza, te volje da se informiraju i propisno zaštitite korisnicima mogu načiniti veliku štetu, ali ne i samo njima, već i drugima.

Današnje društvo oslanja se na računala. Stoga su napadi na računala zapravo napadi na naše društvo. Računalna sigurnost je postala jedno od najvažnijih područja u računalstvu.

Računala se danas koriste za niz ključnih i osjetljivih aspekata ljudskog života. Kontroliraju međunarodnu telefonsku komunikaciju, protok informacija na Internetu, distribuciju električne energije među gradovima i slično.

No, za te probleme se brinu neki drugi ljudi i svakom običnom korisniku koji koristi računalo u vlastitom kućnom okruženju, za neke osnovne potrebe, najvažniji je problem kako zaštiti svoje kućno osobno računalo.

Ovaj rad se bavi problematikom zaštite kućnog osobnog računala i to računala s Windows XP Professional operacijskim sustavom.

Ranjivost računala na Internetu je problem koji se sastoji od više slojeva. Korisnicima Interneta prijete opasnosti od direktnog napada ili neke vrste zloćudnog koda. Metode napada i inficiranja računala su veoma raznolike. U mnogo situacija riječ je o iskorištavanju poznatih ranjivosti operacijskog sustava ili nekih programa. Drugi dio problema je sam ljudski faktor, odnosno neopreznost korisnika.

Osnovni cilj ovog rada je obraditi osnovne probleme sigurnosti kućnog računala. Istražiti kakve sve prijetnje vrebaju, kakvim rizicima je svaki korisnik izložen, koje su osnovne metode napada i načini inficiranja računala. Provjeriti kakve su sve mjere zaštite potrebne. Što treba izbjegavati, koje radnje redovno vršiti, koje izmjene napraviti, te kakve vrste alata za zaštitu su dostupne. Te, utvrditi da li je primjenom preporučenih postavki i pravilnim korištenjem osnovnih zaštitnih programa osigurana dovoljna razina sigurnosti potrebna za bezbrižno korištenje računala i Interneta.

Drugo poglavlje rada obrađuje današnje najpoznatije vrste zloćudnih programa i prijevara koje vrebaju na Internetu i analizira se problem ranjivosti Windows XP Professional operacijskog sustava, osnovni propusti i najranjiviji elementi operacijskog sustava.

Treće poglavlje usmjereno je na zaštitu. Obrađuje se područje weba i Interneta, odnosno aktivnosti koje korisnici obično obavljaju putem Interneta i prijetnje i rizici kakvima su pritom izloženi, te sigurnosni aspekti samog programa koji se koristi za pregledavanje weba – web preglednika. Obrađuje se i elektronička pošta, sigurnosni aspekti takvog tipa komunikacije i alati za rad s elektroničkom poštom – e-mail klijenti.

Promatraju se one vrste zaštitnih programa koji se danas smatraju dijelom osnovnog zaštitnog kompleta svakog kućnog osobnog računala, te razlike među najpoznatijim takvim programima i razlike između komercijalnih i besplatnih.

Obrađuju se oblici i načini ažuriranja Windows XP operacijskog sustava i pojedinačnih aplikacija instaliranih na računalu, te važnost samog redovnog ažuriranja i dodatne elemente na koje je pritom potrebno obratiti pozornost.

Dodatno se analiziraju ranjivosti i propusti Windows XP operacijskog sustava spominjani u drugom poglavlju, te načini eliminiranja rizika uzrokovanog tim ranjivostima.

Četvrto poglavlje sadrži eksperiment kojemu je cilj primijeniti i provjeriti sve preporuke, zaštitne alate i postavke preporučene unutar rada.

2. OPASNOSTI KOJE PRIJETE OSOBNOM RAČUNALU

2.1 OPASNOSTI IZVANA

2.1.1. Zloćudni kod (malware)

Zajednički naziv svim vrstama zlonamjernog, malicioznog računalnog koda je engleski izraz „malware“ (malicious software – odnosno maliciozni, zloćudni kod, program). Pod zloćudni kod spadaju aplikacije s malicioznom namjerom ili malicioznim posljedicama.

2.1.2. Virusi

Virus je maliciozan kod koji se pri izvršavanju pokušava replicirati, kopirati samog sebe unutar drugog izvršnog koda (executable code). Ako je pokušaj uspješan, za kod se kaže da je zaražen. Tada zaraženi kod, prilikom izvršavanja može na isti način proširiti zarazu dalje, na novi kod. To samo repliciranje u postojeći izvršni kod je ključna karakteristika u definiranju virusa.

Iako nema univerzalne definicije, često je korištena ona Dr. Frederica Cohena koja računalni virus definira kao: "...program koji može "zaraziti" druge programe modificirajući ih na način da u njih uključuje kopije samog sebe"

Pod zarazom se tu smatra da virus ubacuje samog sebe u slijed naredbi programa, tako da pokušaj izvršavanja legitimnog programa dovodi do izvršavanja virusa zajedno s tim programom (ili umjesto njega).

Od samih početaka, virusi se umnožavaju i šire unutar jednog računala i zatim se prenose od računala do računala prijenosnim medijima kao što su diskete, CD i DVD mediji, te USB memorijski uređaji. Isto tako, mogu se širiti i putem dijeljenih datoteka u lokalnoj mreži.

Dolaskom vladavine Interneta i virusi su se prilagodili novim trendovima, pa je Internet postao glavni medij za širenje virusa. U većini slučajeva, virusi se prenose putem elektroničke pošte. Mogu se nalaziti kao izvršne i druge datoteke (nerijetko se skrivaju višestrukim ekstenzijama) u privitku e-mail poruke ili je čak nekad dovoljno da korisnik samo otvori poruku, da se računalo inficira. Pristigla poruka može biti i od neke poznate osobe jer virusi, zajedno s brojnim drugim vrstama nametnika imaju sposobnost da se sami pošalju e-mailom s inficiranog računala na sve adrese iz e-mail adresara.

Računalni virus se sastoji od tri dijela, odnosno tri mehanizma:

- **Mehanizam zaraze** (infection) – možemo ga definirati kao način ili načine na koje se virus širi
- **Korisnički sadržaj** (payload) – ono što virus zapravo radi (ako išta), osim što se širi. To se može odnositi na štetu koji nanosi, namjernu ili slučajnu.
- **Okidač** (trigger) – način odluke o trenutku izvršavanja (ili odluke o izvršavanju – da ili ne) korisničkog sadržaja (payload), ako ga ima.

Postojanje mehanizma zaraze je obvezno da bi program bio definiran kao virus (jer je to jedna od ključnih karakteristika virusa), dok su druga dva mehanizma u manjoj ili većoj mjeri opcijska (ovisno o vrsti virusa).

Virus ne mora nužno biti napravljen s namjerom da učini konkretnu štetu (bez korisničkog sadržaja) no i u tim slučajevima nerijetko nastaje nekakva usputna, slučajna šteta. Pa tako

posljedice zaraze mogu biti samo zauzimanje sistemskih resursa – prostora u memoriji i na tvrdom disku, zbog čega može doći do usporavanja računala i veze na Internet (možda čak i tolikog usporavanja da računalo postane neupotrebljivo).

Mogu ne raditi ništa drugo do ispisivanja neke poruke na ekranu inficiranog računala. Isto tako, mogu i brisati ili modificirati podatke na inficiranom računala, ili ih čak poslati nekom drugom. Mogu onemogućiti punu upotrebu nekih aplikacija ili sasvim isključiti njihovo pokretanje. Također, mogu izazvati smetnje u operacijskom sustavu, koje u najgorem slučaju mogu dovesti do pada sustava.

Sam čin inficiranja datoteke odnosno računala, njihova aktivnost i promjene koje nastaju na datotekama mogu odati prisutnost virusa. Zbog toga virusi koriste razne tehnike prikrivanja tragova. Tehnike nevidljivosti (stealth), skrivanja iza originalnih datoteka, tehnike šifriranja kojima virus konstantno mijenja svoj sadržaj čime bi se trebalo otežati njihovo pronalaženje, te tehnike konstantne izmjene potpisa (polimorfizam) koje nadopunjuju šifriranje.

Koristi se i još jedna metoda, a to je napad. Virusi koji koriste metodu napada (osvetnički virusi) direktno napadaju program za detekciju virusa (anti-virus) u računalu i modificiraju ga tako da ili ne može detektirati taj virus, ili pak inficiraju sam program za njihovu detekciju čime on sam pomaže širiti virus.

Virusi se mogu klasificirati na razne načine. Tako imamo poznatu podjelu prema ciljevima infekcije, metama – odnosno dijelimo ih u odnosu na to što inficiraju. Prema toj podjeli razlikujemo: viruse koji inficiraju sektore za podizanje, viruse koji inficiraju izvršne datoteke i makroviruse.

Virusi koji inficiraju sektore za podizanje (BSI – boot sector infectors)

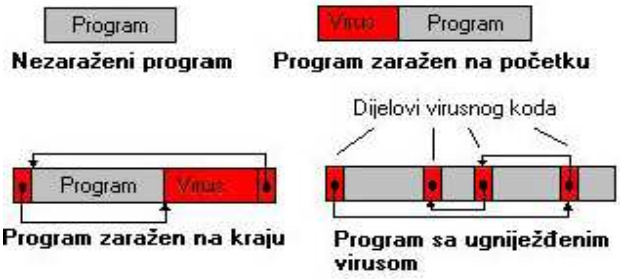
Ciljaju MBR (Master boot record) i PBS (partition boot sector) instrukcije koje se izvršavaju prilikom podizanja sustava, neposredno nakon uključivanja računala. To su instrukcije koje su dio svakog diska (tvrdog diska, diskete, CD-a, USB prijenosne memorije i slično) i govore računalu kako koristiti pojedini disk. Takav virus se širi kad god se računalo podiže sa zaraženog medija.

Prednost takvih vrsta je virusa u tome što se aktiviraju prilikom podizanja sustava – dakle, prije inicijalizacije programa za detekciju virusa (anti-virus) i prije aktiviranja sigurnosti operacijskog sustava. Međutim, takvi virusi su danas rijetki jer se danas računala rjeđe resetiraju a i vrlo rijetko se danas koriste mediji za podizanje (bootable media) poput disketa. Isto tako, većina operacijskih sustava ne dopušta zapisivanje u blokove za podizanje (boot block) bez propisne autorizacije, a i BIOS danas najčešće nudi mogućnost zaštite tih blokova.

Primjer poznatog takvog virusa je **Michelangelo**. Pušten 1992. godine, prvi je virus koji je opsežno praćen medijima. No, kako to s medijima uvijek bude, stvorila se velika fama, izmišljale priče i na kraju, izvješća su varirala od petsto tisuća zaraženih računala pa sve do brojki od pet milijuna. Iako je virus napao određeni broj računala, opasnost nije bila ni približna onoj koju su mediji predstavljali. Osnovni način širenja tog virusa bile su pošiljke inficiranih tvrdih diskova koji su zabunom bili isporučeni iz tri tvrtke.

Virusi koji inficiraju izvršne datoteke

Oni su najčešća vrsta. Inficiraju izvršne datoteke računala dodavanjem svog sadržaja u samu strukturu programa. Koriste nekoliko metoda u procesu inficiranja. Virusni kod može se samo umetnuti unutar programa – može se prilijepiti na početak ili kraj datoteke, ili se umetnuti u sredinu. Druga mogućnost je upisivanje virusnog koda preko koda programa, čime se zapravo briše jedan dio izvršne datoteke koja se inficira. Virusi koji se samo pridodaju kodu izvršne datoteke, obično ne oštećuju datoteku, ali samim tim činom povećavaju veličinu datoteke što omogućava lakše detektiranje. Nazivaju se i parazitski virusi.



Slika 2.1. - Načini inficiranja izvršnih datoteka umetanjem virusnog koda u kod programa

Druga skupina, virusi koji prepisuju maliciozan kod preko koda programa su nešto opasniji. Prvo, ne mijenjaju veličinu datoteke, pa ih je teže detektirati. I drugo, brisanjem koda originalne datoteke mogu oštetiti ili uništiti podatke.

Ti virusi obično ciljaju izvršne datoteke s ekstenzijama .COM, .EXE, .SYS, .OVL i druge.

Primjer poznatog virusa koji spada u one koji iniciraju izvršne datoteke je **Chernobyl virus** koji je inficirao milijun računala i rezultirao štetom od 250 milijuna dolara. Smatra se jednim od najdestruktivnijih virusa ikada. Nije mijenjao veličinu datoteke koju inficira već je tražio prazna mjesta unutar nje, razbio se na manje dijelove i umetnuo se u male komadiće neiskorištenog prostora. Nakon aktivacije inicirao je dva napada. Prvi napad je zapisivao slučajne podatke preko postojećih podataka na tvrdom disku uzrokujući pad sustava, nemogućnost podizanja i nemogućnost spašavanja podataka. Drugi napad je usmjeren na podatke spremljene u BIOS-u računala, koji kontrolira sve sistemske uređaje. Jedino rješenje tog problema je bilo zamjena ili reprogramiranje BIOS-a.

Makrovirusi - inficiraju samo dokumente izrađene u programima koji podržavaju makronaredbe (Microsoft Word, Excel itd.). Makrovirus se širi kad se otvori zaraženi dokument, kao npr. zaraženi Word dokument. Takvi virusi zapravo inficiraju predloške (template) koji definiraju margine, font i druge osnovne postavke oblikovanja dokumenta. Svaki put kad se stvori novi dokument iz inficiranog predloška, virus pokušava inficirati drugi predložak i taj novi dokument. Da bi omogućio širenje, pretvara zaraženi dokument u predložak, zadržavajući izgled običnog dokumenta. Makrovirusi su dosada ostali ograničeni na Microsoftove programe kao Word, Excel ili PowerPoint. Razlog tome je što, iako su postojali pokušaji da se zaraze i drugi takvi programi kao WordPro ili WordPerfect, širenje je bilo prilično teško jer ti programi sve makroe spremaju u zasebnu datoteku, dok prenošenjem i kopiranjem Word ili Excel dokumenata, svaki makro se prenosi zajedno s dokumentom, unutar iste datoteke.

Poznati primjer takvog virusa je **Concept** – prvi makrovirus. Inficirao je Microsoft Word dokumente i na Windows i Macintosh računalima. Smatra se da je napisan samo zato da se dokaže da se virusi uistinu mogu pisati koristeći makro – jezik. Concept virus nije izazivao namjernu štetu na računalu, već je samo prikazivao dijaloški okvir objavljujući svoju prisutnost.

Drugi, vrlo poznati makrovirus je **Melissa**, poznat kao najbrže šireći virus u povijesti. Inficirao je Microsoft Word dokumente koristeći VBA (Visual Basic for Applications) makro naredbe i šireći se putem Outlook e-maila. Virus je dolazio u privitku e-mail poruke naslovljene „Važna poruka od... (ime)“ unutar koje je pisalo – „Evo dokumenta koji si tražio (tražila) .. ne pokazuj nikom drugom ;-)“.

Nakon otvaranja dokumenta u privitku, virus se počeo širiti na računalu i ponavljao bi proces slanjem kopija sebe (istog e-maila) na prvih 50 adresa u Outlook adresaru računala primatelja, opterećujući e-mail poslužitelje i čitavu mrežu. Unutar tri dana, inficirano je preko sto tisuća računala. Melissa je imala i određene karakteristike crva i zapravo bi se trebala smatrati hibridom tih dviju vrsta štetnih programa.

2.1.3. Crvi

Crv (worm) je naziv za maliciozni računalni kod koji se samostalno replicira i inficira računala, sposoban samostalno tražiti nove sustave domaćine i inficirati ih putem mreže.

Mnogi često poistovjećuju crve s virusima, nazivajući ih samo jednom specijalnom vrstom virusa. Isto tako, mnogi poznati maliciozni programi koji su popularno prozvani virusima, po pravilu bi trebali biti smatrani crvima ili hibridima tih dviju vrsta štetnih programa. (Primjeri – Melissa, Klez...)

Točno je da crvi imaju neke zajedničke karakteristike s virusima. Najvažnija karakteristika koju dijele je mogućnost samorepliciranja, samoumnažanja. Međutim, razlikuju se u samom načinu samoumnažanja.

Prvo, crvi ne trebaju domaćina da bi se širili, kao virusi za koje možemo reći da zapravo parazitiraju. Crvi su samostalni, samostalno djeluju i šire se. Druga razlika je što je osnovni medij širenja crva – mreža.

Dakle, virusi se šire inficirajući druge programe, drugi kod, dok crvi imaju sposobnost samostalne migracije sa sustava na sustav preko mreže, bez pomoći eksterne aplikacije. Osim toga, crvi aktivno traže ranjiva računala na mreži. Crv koji se nalazi na nekom računalu, traži druga dostupna računala kroz lokalnu mrežu (LAN) ili kroz Internet veze. Kad pronađe drugo računalo replicira se, kopira se na to novo računalo, odakle ta kopija, odnosno nova instanca crva, traži dalje nova računala. Crv se može nastaviti replicirati beskonačno ili dok se ne zaustavi internim mehanizmom tempiranja – ako postoji. Isto tako, dobro je spomenuti i da instance crva ponekad mogu komunicirati s drugim instancama – formirajući mrežu crva (worm network), dok virusi ne komuniciraju s vanjskim sustavima.

Dvije najčešće metode širenja crva su elektronička pošta (e-mail) i iskorištavanje sigurnosnih slabosti i propusta na računalima spojenima na mrežu ili na Internet.

Crvi koji koriste e-mail za širenje nazivaju se e-mail crvi odnosno crvi koji se masovno šalju (mass-mailing). Obično su pisani u inačici Visual Basic programskog jezika i najčešće su usmjereni na Microsoft Outlook ili Outlook Express programe (e-mail klijente) na Windows operacijskom sustavu. Crv obično provjerava korisnikov e-mail adresar (unutar navedenih programa) i zatim šalje kopije samog sebe na svaku od adresa iz adresara. Takvi crvi se šire naročito brzo jer te e-mail poruke stižu s poznatih adresa. Primatelj vrlo vjerojatno otvori e-mail i time ne znajući pomaže crvu da pristupi i njegovom adresaru. Mnogi crvi dolaze kao privitci e-mail porukama, koje na neki način prevare korisnika da ih pokrene. Ili je recimo, dovoljno samo da korisnik otvori određeni e-mail, bez potrebe za otvaranjem privitka.

Za razliku od njih, Internet crvi se šire pretraživanjem Interneta u potrazi za računalom na kojem se koristi specifični operacijski sustav ili web poslužitelj s određenom poznatom manom ili sigurnosnom slabošću. Kad crv pronađe ranjivo računalo, kopira se na to računalo iskorištavanjem te ranjivosti i nakon toga koristi i to novo računalo u potrazi za novim metama napada.

Kao i e-mail crvi, Internet crvi najčešće ciljaju najpopularnije operacijske sustave (Microsoft Windows ili Unix) ili web poslužiteljske programe (Apache ili Microsoft IIS). Stoga bi dobra metoda zaštite od obje vrste crva u svakom slučaju bila korištenje alternativnih programa ili čak operacijskih sustava. Detaljnije o tome govori se u kasnijim poglavljima.

Također, crvi mogu koristiti razne tehnike prikrivanja vlastitih tragova (kao i virusi) – mogu koristiti šifriranje, mnogoobličnost (polimorfizam) i sl.

Crvi često izazivaju štetu i bez izravne namjere (kao i većina takvih nametnika). Dakle, osim potencijalne namjerne štete, usputna šteta je gotovo uvijek slučaj. Ponekad je sama prisutnost

crva koji se masovno šalje kroz e-mailove ili direktno kopira širom Interneta može uzrokovati usporavanje rada računala ili čak pad sustava i bez izravne namjere crva da nanese štetu računalu. Nadalje, budući da populacije crva obično rastu eksponencijalnom brzinom, eksponencijalno se povećava i promet na mreži. To izaziva zagušenja, prekide veza, potrošnju pojasne širine (bandwidth).

Osim samog širenja crva, povećanje mrežnog prometa uzrokovanog crvima ima i druge izvore. Primarni proizlazi iz aktivnog skeniranja i ispitivanja koje crv vrši prilikom traženja i napadanja novih meta. I sekundarni izvor prometa proizlazi iz povratnog prometa nastalog iz neuspješnih pokušaja širenja crva – negativne odgovore klijentu (kao npr. ICMP_PORT_UNREACHABLE poruke).

Dakle, čak i nenamjerna šteta koju crvi izazivaju samom prisutnošću na mreži izaziva poprilične probleme. No, pored toga, crvi mogu izazvati velike štete i namjerno. U računalnom kodu koji crv sadržava može se nalaziti određeni korisnički sadržaj (payload) – dio koda pisan za implementaciju određene akcije od strane napadača na ciljanom sustavu. Korisnički sadržaj je ono što će crv napraviti kad stigne na cilj.

Iako veliki broj crva ne radi zapravo ništa osim što se širi (payload = null), oni koji imaju implementiranu neku akciju, ta akcija izaziva veću ili manju direktnu štetu ciljanom sustavu. Računalni crv može zapravo na inficiranom računalu izvršiti bilo što, bilo koji radnju koju napadač želi – od brisanja podataka, promjene postavki računala, izmjene web mjesta ili bilo kakva druga vrsta štete. Pomoću crva napadač zapravo može preuzeti kontrolu nad računalom i šteta koju može načiniti ovisi isključivo o mašti i ciljevima napadača.

One uobičajene radnje su:

- otvaranje „stražnjih vrata“ (backdoor) – (koji su detaljnije objašnjeni nešto kasnije) pomoću kojih napadač zadobiva potpunu daljinsku kontrolu (remote control) nad inficiranim sustavom,
- postavljanje izvršitelja DDoS (distributed denial-of-service) što izaziva potrošnju ogromne količine pojasne širine (bandwidth) koja potpuno onemogućuje komunikaciju napadnutog sustava s ostatkom mreže (na meti su obično web poslužitelji i sl.)
- izvođenje kompleksnih matematičkih operacija - inficiranjem velikog broja računala na pravi način napadač dobiva mogućnost iskoristiti njihove resurse za obavljanje zahtjevnih matematičkih operacija (kao npr. razbijanje ključa za šifriranje ili šifrirane lozinke i slično).

Najpoznatiji crvi su:

Morris crv (također poznat jednostavno kao "The Internet Worm"), studeni 1988.

Ciljana platforma: UNIX

Napisan kao istraživački projekt dok je autor, Robert Tappan Morris bio na doktorskom studiju – taj crv je pušten na Internet gdje je izazvao ogromnu štetu i zastoj gotovo čitave mreže. Zbog tog crva formiran je prvi CERT (Computer Emergency Response Team), organizacija koja i danas postoji i obavještava o sigurnosnim ranjivostima i incidentima. Morris crv je prvi primjer velike štete i prve velike tužbe i osude za jedan računalni napad.

Melissa, ožujak 1999

Ciljana platforma: Microsoft Outlook e-mail klijent

Već ranije spomenut, Melissa je zapravo Microsoft Word makrovirus (u privitku e-maila) koji se širio putem Outlook e-maila, ponašajući se istovremeno kao virus (inficiranjem .DOC datoteka) i kao crv (šireći se preko mreže).

The Love Bug, svibanj 2000

Ciljana platforma: Microsoft Outlook e-mail klijent

To je Visual Basic Script crv koji se uglavnom širio preko Outlook e-maila poput Melisse, no imao je i druge metode širenja zbog čega je bio nešto kompleksniji. Širio se slanjem e-maila s naslovom ILOVEYOU u kojem je pisala ljubazna molba da se otvori ljubavno pismo priloženo u privitku (LOVE-LETTERFOR-YOU.TXT.VBS.). Također je pokušavao inficirati IRC program (Internet Relay Chat), šireći se tako na sva računala povezana na poslužitelje za razgovor (chat server). Tražio je slikovne, video i glazbene datoteke koje je zamjenjivao ili preko njih upisivao kopiju samog sebe. Isto tako, instalirao je program za krađu lozinki koji je postajao aktivan nakon što je korisnik otvorio Internet Explorer 4 i resetirao računalo.

Code Red, srpanj 2001

Ciljana platforma: Windows IIS Web poslužitelj

Iznimno zarazan crv koji je inficirao 250 tisuća računala u manje od devet sati. Koristio je poznatu ranjivost (uslužni program za indeksiranje automatski instaliran na Microsoft IIS web poslužiteljima) i činjenicu da je mali broj sustava imao instaliranu zakrpu. Napadao je Web poslužitelje, što je značilo da je mogao zaobići tipične vatrozide na većini web mjesta. Nakon instalacije, započinjao bi skeniranje i traženje novih meta za napad. Pored toga, koristio je DDoS (distributed denial-of-service) – distribuirane napade uskraćivanjem usluge za gašenje web mjesta, gdje je primarni cilj bio IP adresa Bijele Kuće (http://www.whitehouse.gov). Također je ciljao i Microsoftovu besplatnu e-mail uslugu - Hotmail. Nakon prvog napada, crv je ostao prikriven do sljedećeg kruga napada, početkom idućeg mjeseca.

Code Red je bio sofisticiraniji od prethodnih jer je kombinirao napade. S vremenom je nastalo više verzija Code Red crva, od kojih je svaka bila „pametnija“ od prethodne, zbog reprogramiranja načina pronalaska ranjivih sustava. Code Red II je koristio isti način širenja, međutim umjesto iniciranja napada uskraćivanjem usluge (DoS), napadaču je davao potpunu kontrolu nad inficiranim sustavom postavljanjem stražnjih vrata.

Nimda, rujan 2001

Ciljana platforma: Windows – Internet Explorer, dijeljenje datoteka, IIS Web poslužitelj, Microsoft Outlook

Nimda (Admin čitano unatrag) je jedan od najdestruktivnijih i najbržih crva ikada. Koristio je otprilike dvanaest mehanizama širenja. Pušten je tjedan dana nakon poznatog terorističkog napada. Unutar samo nekoliko sati onemogućio je brojne organizacije, a napadi su trajali nekoliko tjedana. Inficirao je stotine tisuća računala diljem svijeta kombiniranjem najznačajnijih metoda Code Red II i Melissa crva. Mnoge velike organizacije izvijestile su da se crv provukao unutar vatrozida i nastavio širenje unutar njihovih mreža.

Crv je modificirao web datoteke s nastavcima .htm, .html i .asp kao i neke druge izvršne datoteke na inficiranom sustavu. Nakon toga, stvarao je brojne kopije samog sebe pod raznim nazivima. Tada je nastavljao s pretraživanjem mreže u potrazi za ranjivim računalima i kopirao samog sebe na njih. Isto tako, širio se preko e-maila kao što virusi tipično rade.

Nimda je mogla napadaču omogućiti potpuni pristup zaraženom računalu. Tako je omogućila da se inficirana računala koriste za napade na web mjesta na Internetu. Također, namjerno je napadao računala koja su prethodno bila zaražena Code Red II crvom, ako on nije bio uklonjen s računala tj. ako nije uklonjen backdoor koji je Code Red II postavio.

Klez, studeni 2001.

Ciljana platforma: Microsoft Outlook e-mail klijent i dijeljenje datoteka na Windows operacijskom sustavu

Klez je jedan od najizdržljivijih crva koji su stvarali nevolje na Internetu. Iskorištavao je ranjivosti u Outlook i Outlook Express programima čime je omogućavao da se računalo zarazi samo otvaranjem ili pretpregledom e-mail poruke. Nakon inficiranja, slao bi kopije samog sebe svima iz e-mail adresara korisnika. Klez crv bio je korak naprijed prema mnogoobličnosti (polimorfizmu) zbog mogućnosti slučajnog odabira (randomizing) naslova e-mail poruka i tipova datoteka u privitcima. Crv je također sadržavao i virus naziva ElKern koji je inficirao izvršne datoteke. Isto tako, aktivno je pokušavao onemogućiti program za detekciju virusa (anti-virus). Zaustavljao je procese, uništavao datoteke i još mnogo toga. Postoji nekoliko varijanti Klez crva koje su s vremenom napredovale, mijenjale svoje ciljeve, načine širenja i postajale sve kompleksnije i teže za detekciju.

Slammer, siječanj 2003.

Ciljana platforma: Windows sustavi s Microsoft SQL poslužiteljem baza podataka

Slammer, također poznat kao „SQL Slammer“ i „Sapphire“ je daleko najbrže šireći crv ikada. Širio se Internetom nevjerojatnom brzinom, rušeći velike sustave i onemogućujući pristup Internetu velikim područjima u manje od 10 minuta nakon prvog pojavljivanja. Iskorištavao je poznati propust u SQL poslužitelju baza podataka, za koji je izdana zakrpa mjesecima ranije. Ipak, veliki broj ljudi zakrpu nije primijenio te je inficirano najmanje 75 tisuća SQL poslužitelja. Isto tako, ogroman promet koji je crv generirao skeniranjem mreže i traženjem novih domaćina rezultirao je problemima sa sustavima zrakoplovnih rezervacija, bankovnim uređajima (bankomatima) i slično. Ono što je omogućavalo tako brzo širenje (čak 100 puta brži od Code Red crva) je mehanizam skeniranja koji slučajno bira IP adrese da bi zatim provjeravao prisutnost SQL poslužitelja na računalu.

2.1.4. Trojanski konji (Trojan horse)

Termin „trojanski konj“ potječe od opće poznate priče iz Homerove Ilijade. Sam naziv shodno predstavlja zamku maskiranu u nešto naizgled bezopasno. Analogija vrijedi i u računalnom svijetu.

Trojanski konj ili „trojanac“ je bilo kakav program (komad računalnog koda) koji ima naizgled neku bezopasnu ili korisnu funkciju, dok ustvari sadrži i neku skrivenu malicioznu funkcionalnost. Najčešće se predstavljaju kao neki zanimljiv program ili možda i neki video ili audio sadržaj kojeg korisnik traži.

Osnovna razlika između trojanskog konja i virusa i crva je ta da se trojanski konj ne može replicirati. Tu se oslanja na neoprezne korisnike koji, ne sumnjajući, svojevoljno dozvoljavaju njihovo izvršavanje na vlastitom računalu. Druga karakteristika koju je dobro istaknuti je ta da je trojanski konj mnogo opasniji i maliciozniji od virusa i crva, i programi za detekciju virusa (anti-virus) i slični zaštitni programi ih nerijetko ne uspijevaju prepoznati.

U osnovi, glavni cilj trojanskog konja je da napadaču omogući pristup sistemskim datotekama. Trojanski konji mogu izazvati raznoliku štetu na inficiranom računalu. Mogu brisati datoteke ili čitave particije, kopirati datoteke na inficirano računalo, mijenjati vrijednosti registara, preimenovati datoteke, krasti lozinke i ostale povjerljive podatke, onemogućiti sigurnosne programe, ugasiti ili resetirati računalo, onemogućiti tipkovnicu, miša ili druge periferne uređaje i slično.

Mogu se širiti na razne načine. Kao privitci putem e-maila, preko IRC-a (Internet Relay Chat) i soba za razgovor (chat room), slanjem putem ICQ-a ili drugih usluga za trenutne poruke (instant messaging). Skriveni unutar legitimnih programa na web mjestima s kojih se može preuzeti besplatne aplikacije. Ili pak sakriveni na web mjestima koja nude npr. neke pornografske sadržaje ili pak neke hakerske alate. I naravno, fizičkim kopiranjem na računalo.

Prije nego trojanski konj može napasti, prvo mora pronaći način da namami korisnika da kopira program i pokrene ga. Da bi se to postiglo, koriste se dva načina.

Pokušava se „predstaviti“ kao neki bezopasan ili koristan program. Možemo reći da se preruši u neki drugi program za koji korisnik može pomisliti da je bezopasan – poput neke računalne igrice ili nekog uslužnog programa. Ponekad je čak i dovoljno da se promijeni ime trojanskog konja u ime nekog poznatog programa, da bi ga korisnik pokrenuo.

Druga mogućnost je da se sami „sakriju“ unutar nekog legitimnog poznatog programa poput Adobe Photoshopa ili Microsoft Excela. Zapravo se integriraju unutar nekog programa. Za to koriste posebne programe (wrappers, binders, packers) koji spajaju, integriraju bilo koji maliciozni kod unutar bilo kojeg legitimnog programa čime se smanjuje mogućnost da će biti otkriveni. To su programi naziva poput Saran Wrap, Silk Rope ili The Joiner. Isto tako, budući da većina korisnika neće sumnjati da bi takav poznat program od dobro poznatog izdavača mogao sadržavati trojanskog konja, povećava se vjerojatnost da ga korisnik i pokrene i time pokrene i trojanskog konja.

Postoji nekoliko osnovnih skupina u koje grupiramo trojanske konje.

Tako imamo tzv. **šaljive trojance**. Takvi uglavnom ne rade nikakvu štetu, osnovni cilj im je našaliti se i iritirati korisnika. Mogu puštati iritirajuće zvukove preko zvučnika računala, izmijeniti izgled zaslona ili prikazivati neku zajedljivu poruku na ekranu. Iako neugodni i nepoželjni, takvi trojanski konji su bezopasni i lako ih je ukloniti.

Poznati šaljivi trojanci su **Icon Dance** – koji bi minimizirao sve otvorene programe i počeo brzo ispremještati sve ikone na radnoj površini; ili **NVP Trojanac** koji bi na Macintosh računalima izmijenio sistemske datoteke tako da se kada korisnik tipka nekakav tekst, samoglasnici ne prikazuju. NVP Trojanac se konkretno maskirao kao uslužni program za prilagođavanje prikaza ekrana.

Nakon toga imamo **destruktivne trojance**. Oni mogu obrisati čitav tvrdi disk ili selektivno brisati ili modificirati određene datoteke. Iako najopasniji, sama njihova priroda ograničava njihovo širenje. Prilikom napada na računalo, obično otkrivaju svoju prisutnost, najčešće nekom porukom. Isto tako, ako obrišu čitav tvrdi disk, izbrišu i sami sebe.

Primjer je **Feliz Trojanac**. Nakon pokretanja, na zaslonu prikaže zastrašujuću sliku kao upozorenje da napad počinje. Klikom na „Exit“, prikazuje se niz poruka, upozorenja da se ne pokreću programi. Na kraju, prikazuje se poruka – „Sretna Nova Godina“. Prilikom prikazivanja poruka, trojanac u pozadini briše ključne sistemske datoteke, čime onemogućuje pokretanje računala.

Slika 2.2. - Slika i poruka koju prikazuje Feliz Trojanac prilikom napada

Sljedeća skupina su **trojanci koji otuđuju lozinke i druge osjetljive informacije**. To je ustvari i najčešća upotreba trojanskih konja. Nakon što ga prijevarom korisnik pokrene, može preuzimati datoteke s računala i slati ih natrag napadaču. Na taj način napadač može dobiti pristup nekom računalu (ulazna lozinka), nekom korisničkom računu, e-mail sandučiću i slično; ili pak brojeve kreditnih kartica i druge vitalne informacije. Takav napad može nanijeti priličnu štetu korisniku, financijsku i računalnu. Od velikih naplata na kreditne kartice, do kriminalnih radnji ili uznemiravanja drugih pod identitetom pokradenog korisnika, bez njegova znanja.

Poznati primjer je **ProMail Trojanac**. Trojanski konj nastao modificiranjem legitimnog e-mail klijenta otvorenog koda – Phoenix Mail, koji je zatim nazvan ProMail v1.21 i predstavljan kao besplatni (freeware) e-mail klijent. Distribuiran je kao takav na mnogim poznatim web mjestima s besplatnim programima. Nakon pokretanja, program traži od korisnika mnoštvo informacija, uobičajenih za takav program – korisnikovu e-mail adresu i pravo ime, korisničko ime i lozinku i slično. Nakon preuzimanja svih podataka, ProMail ih šifrira i pokušava poslati na korisnički račun (naggamanteh@usa.net) na NetAddress (http://www.netaddress.com) – besplatni pružatelj e-mail usluga.

Trojanci koji omogućuju udaljeni pristup (Remote access Trojan, RAT)

Programi za udaljeni pristup su legitimni alati koje korisnici upotrebljavaju za pristup drugom računalu putem telefonske linije ili Interneta. Poznati programi za udaljeni pristup su npr. pcAnywhere, Carbon Copy, LapLink, a koriste se i mogućnosti za udaljeni pristup ugrađene u Windows XP. Dok ljudi svjesno instaliraju alate poput pcAnywhere na svoje računalo RAT trojanci su također takvi programi, samo što ih korisnici instaliraju na prijevaru i ne znajući. Nakon instalacije, RAT dozvoljava napadaču (iz bilo kojeg dijela svijeta) potpun pristup i kontrolu nad tim računalom, kao da sjedi ispred njega. Dok korisnik radi na računalu, napadač može vidjeti sve što korisnik vidi i sve što radi, te može i obavljati razne radnje. Od brisanja datoteka, kopiranja datoteka na inficirano računalo (nerijetko viruse i druge trojanske konje), premještanja mapa, resetiranja računala, pa do otvaranja vrata CD-ROM uređaja, puštanja zvukova putem zvučnika ili čak upisivanja poruka u programu kojeg korisnik upravo koristi. RAT se sastoji od dva dijela – poslužiteljskog (server file) i klijentskog (client file). Poslužiteljski dio nalazi se na inficiranom računalu, a klijentski dio na računalu napadača. Svaki napadač koji posjeduje odgovarajući klijentski dio može se povezati sa bilo kojim računalom na kojem je instaliran poslužiteljski dio tog konkretnog trojanskog konja.

Nakon što je poslužiteljski dio uspješno instaliran, on otvara priključnu točku (port) na inficiranom računalu, preko kojeg se odvija daljnja komunikacija. Neki trojanski konji čak potajno šalju e-mail napadaču kojim ga obavještavaju da je instalacija na ciljano računalo uspješno izvršena i šalju IP adresu tog računala. Nakon što dozna IP adresu, napadač može pristupiti tom računalu pomoću trojanskog konja.

Najpoznatiji takav trojanac je **Back Orifice (BO)**, tako nazvan s ciljem ismijavanja Microsoftovog Back Office programa. Originalno napisan kao trojanac i pušten u promet 1998. izazvao je veliku zbrku jer su hakeri masovno inficirali računala i pristupali računalima drugih ljudi. 1999. godine objavljena je nova verzija nazvana Back Orifice 2000 (BO2K), za koju je objavljen i kompletan C/C++ izvorni kod. Isto tako, imao je i mogućnost nadogradnje, pa su programeri diljem svijeta mogli pisati vlastite dodatke (plug-in).

Tom novom verzijom započeta je promocija Back Orificea kao Windows alata za udaljenu administraciju, smještajući ga u istu klasu sa pcAnywhere i Carbon Copy. Ironija je tim veća što se osim što je besplatan, pokazao i puno bolji od komercijalne konkurencije i zahtijeva puno manje diskovnog prostora (1MB) i RAM-a (2MB).

Back Orifice 2000 predstavlja tanku liniju između trojanca i legitimnog alata za udaljeni pristup računalu. Oprezno korišten, Back Orifice je neprocjenjiv alat, dok se nepromišljenom uporabom pretvara u opasno oružje.

2.1.5. Stražnja vrata (backdoor)

Stražnja vrata (Backdoor ili Back door) – zloćudni kod koji radi upravo to – otvara stražnja vrata, stražnji ulaz u neku aplikaciju, sustav ili mrežu. Stražnja vrata (backdoor) su originalno mehanizmi stvoreni od strane programera, da im omoguće specijalan pristup njihovim programima, obično da bi mogli prepraviti kod u slučaju neke greške.

Danas taj termin (u okviru hakera i hakiranja) predstavlja bilo kakav mehanizam koji napadaču potajno omogućuje ponovni pristup kompromitiranom sustavu ili mreži bez ponavljanja prvotnog procesa napada. Obično, nakon što dođe do „upada“ u neki sustav ili mrežu iskorištenjem neke rupe ili propusta u sustavu ili nekoj aplikaciji, napadači nastavljaju s prikrivanjem tragova i instaliraju stražnja vrata – neki posebnu aplikaciju ili skriveni korisnički račun. Ako vlasnik sustava ili mreže i otkrije upad i ispravi propust, napadač ipak ima mogućnost ponovnog pristupa ako korisnik nije otkrio i instalirani stražnji ulaz. Najčešće je jedini način sigurnog uklanjanja stražnjih vrata potpuno obrisati sve i reinstalirati sustav s ranije sigurnosne kopije (backup), za koju je dokazano da je sigurna.

Primjer stražnjih vrata (zasivljeni dio) koji zaobilazi autentifikacijski proces prilikom pristupanja korisničkom računu (pored uobičajenog korisničkog imena i lozinke, unošenjem određenog korisničkog imena – „133t h4ck0r“, također je omogućen pristup)

```
username = read_username()
password = read password()
if username is „133t h4ck0r“:
     return ALLOW_LOGIN
if username and password are valid:
     return ALLOW_LOGIN
else:
     return DENY_LOGIN
```

U svrhu definiranja pojma, možemo reći da je stražnji ulaz (backdoor) dio koda (program ili modifikacija programa) koji zaobilazi normalne sigurnosne provjere i autoru omogućava pristup nekoj aplikaciji, sustavu ili mreži. To je, možemo tako reći, nedokumentirana ulazna točka unutar nekog programa.

Takav zloćudni kod obično otvara TCP ili UDP priključnu točku (port) i time otvara prolaz kroz koji napadač može ponovo pristupiti računalu kada god želi. Kroz taj otvoreni kanal može komunicirati sa stražnjim vratima, izdavati naredbe za izvršavanje ili pak direktno pristupiti resursima računala.

Pristup koji napadač dobiva ovisi o napadačevim namjerama i vrsti stražnjih vrata. Osnovne vrste pristupa koje takav kod omogućava su:

- **povećanje privilegija** – takva vrsta stražnjih vrata napadaču koji ima skriveni korisnički račun na sustavu omogućuje mijenjanje tog računa u administratorski. S privilegijama administratora napadač može izmijeniti postavke računala ili pristupiti bilo kojoj datoteci smještenoj na računalu
- **udaljeno izvršavanje pojedinih naredbi** – korištenjem takvog tipa stražnjih vrata, napadač može poslati poruku ciljanom računalu da izvrši po jednu naredbu (jedna naredba po poruci). Kod stražnjih vrata izvršava napadačevu naredbu i zatim vraća napadaču izlazne podatke
- **udaljeni pristup komandnoj liniji** – također poznat i kao „remote shell“ (za komunikaciju s udaljenim operacijskim sustavom), takav tip stražnjih vrata omogućava direktan pristup naredbenom retku (Command prompt). S druge strane mreže napadač može pisati u naredbenom retku ciljanog računala. Napadač može iskoristiti sve

mogućnosti naredbenog retka – izvršavati naredbe, pisati skripte, manipulirati datotekama. Takva stražnja vrata simuliraju direktan pristup tipkovnici inficiranog računala.

- **udaljeni pristup grafičkom korisničkom sučelju (GUI)** – takva stražnja vrata idu korak dalje od komandne linije i omogućuju da napadač vidi grafičko korisničko sučelje (GUI) računala žrtve, kontrolira pomake miša i udarce tipki na tipkovnici. S udaljenom kontrolom nad grafičkim korisničkim sučeljem napadač može vidjeti sve što žrtva radi na računalu i čak i kontrolirati GUI s druge strane mreže

Bez obzira na vrstu pristupa koju pojedina stražnja vrata omogućavaju, sve te metode su fokusirane na kontrolu. Napadač može dobivenu kontrolu koristiti da bi tražio osjetljive podatke, mijenjao bilo kakve podatke pohranjene na računalu, mijenjao postavke računala ili potpuno srušio sustav. Korištenjem stražnjih vrata ima privilegije administratora računala i te privilegije može koristiti s bilo kojeg kraja svijeta (naravno, putem Interneta).

Načini na koje se stražnja vrata može instalirati na neko računalo također variraju. Napadač može sam postaviti stražnja vrata u direktnom napadu korištenjem nekog propusta. Nakon što napadač uđe u neki sustav, postavljanje stražnji vrata je obično prva stvar koju napravi, kako bi osigurao mogućnost nesmetanog povratka na mjesto zločina.

Nadalje, može iskoristiti neki maliciozni program da bi instalirao stražnja vrata. Razne vrste nametnika kao virusi, crvi ili čak špijunski kod (spyware) u sebi skrivaju stražnja vrata i njihova instalacija je dio njihovog korisničkog sadržaja.

Poznati primjeri virusa i crva koji su postavljali backdoor na računalo su: Code Red II crv, MTX (crv/virus), Bugbear crv, MyDoom crv, virus Opener, Back Orifice crv i drugi. Stražnja vrata najčešće dolaze u kompletu s trojanskim konjima (Trojan horse backdoor ili Backdoor Trojan). Tipična, a i logična kombinacija je s trojancima koji omogućuju udaljeni pristup (remote access Trojan) iako se mogu skrivati i unutar raznih drugih vrsta naizgled korisnih programa.

I zadnja metoda koja se koristi je naravno socijalni inženjering odnosno izmanipulirati korisnika da ga sam instalira. Pomoću e-maila ili nekim drugim putovima, uz prigodnu uvjerljivu poruku da se zapravo radi o nekom super novom korisnom programu.

Primjer nametnika koji je isključivo stražnja vrata (backdoor) je **Brown Orifice**, nazvan prema vrlo poznatom Back Orificeu. Iskorištavao je propust u implementaciji Jave kod Netscape Navigatora verzije 4.7 i prijašnjih. Kad bi korisnik samo posjetio web mjesto na kojem se nalazi Brown Orifice aplet, aplet bi se vrtio na klijentskom računalo pretvarajući ga u nevidljivi Web poslužitelj koji radi na priključnoj točki 8080, omogućujući napadaču puni pristup datotekama na korisnikovom računalu. Brown Orifice nije propust u Java programskom jeziku, već u implementaciji JVM-a (Java Virtual Machine) na ranijim verzijama Netscape Navigatora, propust koji je ispravljen u kasnijim verzijama preglednika.

Osim nametnika koji su isključivo to, postoji i mnoštvo legitimnih programa koji se vrlo često koriste kao stražnja vrata. Od svih njih daleko je najpoznatiji **Netcat**, koji se besplatno može preuzeti s Interneta (www.atstake.com/research/tools/network_utilities/). Netcat je program koji često koriste administratori mreža i mnogi obični korisnici. Može se koristiti za prenošenje datoteka preko mreže, traženje otvorenih priključnih točaka ili ranjivosti na sustavima, prosljeđivanje mrežnog prometa između nekoliko uređaja i mnoge druge radnje. To je vrlo fleksibilan program koji se može koristiti za čitavu paletu aktivnosti. Upravo zato što ima takve mogućnosti, vrlo često se koristi kao stražnja vrata.

Njegova osnovna svrha je da uspostavlja vezu između programa i mreže. Usmjerava protok ulaznih i izlaznih podataka nekog programa. Standardni ulaz i izlaz povezuje na mrežu kroz bilo koju TCP ili UDP priključnu točku. Može raditi u dva režima rada – može osluškivati (listen

mode) ili raditi kao klijent (client mode). Klijentski način rada uspostavlja veze preko mreže. Slušajući način rada, naravno, osluškuje mrežu čekajući podatke. Standardno, napadač instalira Netcat na računalo žrtve i pomoću naredbi ga aktivira i postavlja u slušajući način rada, te mu određuje na kojoj priključnoj točki treba osluškivati promet. Napadač s njim komunicira i šalje mu naredbe pomoću Netcata instaliranog na nekom drugom sustavu i postavljenog u klijentski način rada.

Njegovo ograničenje je da mora moći ostvariti komunikaciju putem neke priključne točke koja je dozvoljena na tom dijelu mreže. Dakle, mora pronaći otvoreni priključak na ciljanom sustavu. Isto tako, može se dogoditi da se ciljani sustav nalazi iza vatrozida koji blokira sve dolazne veze. U tom slučaju se ne može uspostaviti komunikacija s osluškujućim Netcatom na inficiranom računalu. No, takvi vatrozidi obično dozvoljavaju odlaznu komunikaciju pa se napadač može poslužiti trikom i podmetnuti stražnja vrata na način da Netcat postavi u klijentski način rada tako da se komunikacija uspostavlja sa zaraženog računala.

2.1.6. Alati za dobivanje administratorskih ovlasti na sustavu (rootkit)

Alati za dobivanje administratorskih ovlasti (rootkit) imaju porijeklo iz svijeta Unixa i kasnije su prešli i na Windows platforme (1999). Stvoreni su da bi zamijenili standardne Unix alate verzijama koje su korisniku davale korijenske (root) odnosno privilegije Super-korisnika, pritom omogućavajući da njihova aktivnost ostane nevidljiva ostalim korisnicima. Ta jedinstvena sposobnost skrivanja ubrzo je zapela za oko hakerima loših namjera kao idealan način da prikriju svoje zlokobne aktivnosti.

Izraz „rootkit“ je zapravo nastao spajanjem engleskih izraza „root“ (Unix referenca koja implicira korijenski pristup sustavu i administratorske privilegije) i „kit“ – komplet alata (odnosi se na komplet alata koji se koriste za dobivanje takvog skrivenog i privilegiranog pristupa).

Alati za dobivanje administratorskih ovlasti na sustavu (rootkit) su programi osmišljeni ne samo da skrivaju sebe, već da skrivaju i druge programe i sve njima pridružene resurse (procese, datoteke, mape, priključne točke, pogonske programe (driver), vrijednosti registara) i to je zapravo čitav smisao njihova postojanja. Usko su vezani s drugim malicioznim kodom na način da uglavnom trebaju neku vrstu malicioznog programa da bi došli do ciljanog računala. A zatim, kad stignu na cilj, obično se koriste da bi prikrivali neki drugi maliciozni kod.

Klasificiraju se kao dobronamjerni (white-hat) koji i kao takvi predstavljaju sigurnosni rizik; ili zlonamjerni (black-hat), s ciljem da naprave štetu. Maliciozni se često koriste za zadobivanje i održavanje udaljenog pristupa računalu ili mreži u protupravne, obično kriminalne svrhe. Oni svoj posao obavljaju na način da skrivaju maliciozni kod (malware) koji instalira stražnja vrata koja će na kraju omogućiti napadaču nesmetan i neograničen pristup inficiranom računalu. Isto tako, prikrivaju prisutnost napadača u sustavu tako da npr. omogućuju da se napadač prijavi, uđe u sustav bez generiranja sistemskih zapisa (log).

No, unatoč klasifikacijama potrebno je naglasiti da alat za dobivanje administratorskih ovlasti (rootkit) sam po sebi nije dobar ili loš. Funkcionira kao skriveni sef ili spremište. Ono što to spremište sadržava kod pojedinog takvog alata je ono što ga u konačnici čini korisnim ili malicioznim. Alat za dobivanje administratorskih ovlasti (rootkit) može skrivati legitimnu sigurnosnu kopiju (backup) operacijskog sustava koja se može iskoristiti u slučaju pada sustava ili može skrivati nekog nametnika, kao npr. neki trojanski konj koji postavlja stražnja vrata (backdoor Trojan). Iako legitimna uporaba postoji, mnogi se korisnici računala protive bilo kakvoj uporabi takvih alata tj. protive se bilo kakvom skrivanju nečega od njih samih, na njihovim računalima.

Na kraju krajeva, svaki takav alat bez obzira na njegovu početnu svrhu može biti iskorišten u loše svrhe.

Jedna zajednička svrha svih alata za dobivanje administratorskih ovlasti (rootkit) s direktnom zloćudnom namjerom je da instaliraju i prikrivaju crva ili trojanskog konja koji preuzima kontrolu nad računalom pretvarajući ga u sredstvo izvršenja malicioznih aktivnosti. Uobičajena tehnika je otimanje (hijacking) i potajno održavanje otvorene priključne točke koja funkcionira kao skrivena stražnja vrata (backdoor) – omogućujući prijenos podataka sa i na zaraženo računalo. Nakon toga, sve daljnje aktivnosti odvijaju se neprimjetno.

Uobičajene aktivnosti za koje se takva računala iskorištavaju su iniciranje DDoS napada, slanje spam e-mail poruka, pohranjivanje i distribucija ilegalnih materijala (pornografije, glazbe, videa i sl.).

Isto tako, alat za dobivanje administratorskih ovlasti može funkcionirati kao špijun, aktivirajući programe koji bilježe svaki udarac tipke (key logger) i programe koji pregledavaju sav dolazni i odlazni mrežni promet na nekom računalu (packet sniffer). Svi podaci prikupljeni na takav način mogu se koristiti za proučavanje navika korisnika i krađu povjerljivih informacija – osobnih podataka, lozinki, brojeva bankovnih računa i kreditnih kartica i slično.

Takvi alati mogu funkcionirati na dva načina, na dva nivoa, u ovisnosti o tome kakav programski kod zamjenjuju ili modificiraju.

Mogu mijenjati postojeće binarne izvršne datoteke ili biblioteke na sustavu. Drugim riječima, mogu mijenjati upravo programe koje korisnici i administratori pokreću. Takvi alati se nazivaju **korisnički alati za dobivanje administratorskih ovlasti** (user-mode rootkit) jer manipuliraju elementima operacijskog sustava na korisničkom nivou. Oni idu korak daje od same funkcije takvih alata jer oduzimaju korisniku kontrolu nad operacijskim sustavom. Napadač koristi kontrolu za skrivanje datoteka, pokretanje procesa, korištenje mreže i sl.

Također, takav alat može napasti samu jezgru operacijskog sustava (kernel). Ta vrsta se naziva **jezgreni alati za dobivanje administratorskih ovlasti** (kernel-mode rootkit). Jezgra je specijalna aplikacija koji stoji između aktivnih programa i sklopovlja. Kontrolira procese i niti (thread), komunikaciju među procesima, zauzimanje i oslobađanje memorije, pristup tvrdom disku, sklopovske i aplikacijske prekide (interrupt), sučelje između sklopovskih uređaja (tipkovnice, miša, audio, video i mrežnih uređaja i sl.) i programa i slično. Jezgreni alat za dobivanje administratorskih ovlasti zamjenjuje ili modificira elemente jezgre. Na taj način može skrivati datoteke i direktorije, skrivati procese i mrežne priključne točke, preusmjeravati izvršavanje programa (pokretati druge programe umjesto traženih, a da se naizgled čini da se zapravo izvršava program koji je korisnik tj. administrator pokrenuo). Isto tako može presresti i manipulirati protokom podataka od ili prema bilo kojem dijelu sklopovlja na računalu i slično.

Najveći izvor informacija o Windows alatima za dobivanje administratorskih ovlasti (Windows rootkit) je web mjesto www.rootkit.com, na kojem se razmjenjuju ideje i kod među autorima takvih nametnika. Na tom web mjestu se isto tako (uz registraciju) nudi nekoliko besplatnih takvih alata, uključujući Hacker Defender, NT Rootkit, GINA Trojan i HE4Hook.

2.1.7. Špijunski kod (spyware)

Špijunski kod odnosno špijunski program (spyware) je aplikacija odnosno programski kod koji sakuplja informacije o nekoj osobi ili organizaciji bez njihova znanja i suglasnosti. Informacije se sakupljaju s inficiranog računala i periodično šalju na određenu lokaciju, obično neki poslužitelj. Informacije se sakupljaju sa svrhom novčane zarade (prodajom informacija), a špijunski program (spyware) se također smatra malicioznim programom (malware) zbog toga što se instalira na računalo bez znanja korisnika.

Definicija špijunskog koda je prilično općenita zbog toga što postoje mnogi oblici s razlikama u načinu širenja, načinu funkcioniranja, mogućnostima i krajnjem cilju. Špijunski programi (spyware) su računalne zaraze koje su ilegalne, nemoralne, narušavaju privatnost i veoma ih se

teško riješiti. Jedan od razloga tome je što često čuvaju nevidljive kopije na tvrdom disku, pa ako ne uklone svi mogući tragovi nametnika, nakon brisanja se sami ponovo instaliraju.

Za razliku od uobičajenih programa koji su vidljivi na listi aktivnih procesa praćenih od strane operacijskog sustava, špijunski programi se „zakopaju“ daleko od vidljivosti tako da su šanse minimalne da će korisnik slučajno naletjeti na nekog od njih dok je aktivan. Nerijetko korisnik uopće ne može detektirati špijunski kod na svom računalu.

Špijunski kod se infiltrira u računalo na razne načine. Neki virusi, crvi i trojanski konji su dizajnirani sa svrhom instaliranja špijunskih programa na ciljano računalo (ili prenošenjem špijunskog koda direktno kao dio korisničkog sadržaja (payload); ili preuzimajući ga nakon što se virus uspješno smjestio).

Druga mogućnost inficiranja je iskorištavanje ranjivosti web preglednika, koja dozvoljava preuzimanje i pokretanje nekog malicioznog sadržaja. To mogu biti neke ActiveX kontrole ili dodaci (plug-in) za preglednike. Možda i neke specijalno kodirane stranice koje zavaraju preglednik na način da misli da se radi o zoni Moje računalo (My computer zone) ili zoni pouzdanih web mjesta (Trusted site zone). Moguće je čak da se špijunski kod automatski učita u računalo kada korisnik samo posjeti neku web stranicu na kojoj se nalazi (drive-by-download).

Špijunski kod (spyware) kao metodu širenja koristi i e-mail, odnosno ranjivosti e-mail klijenta koji prikazuje HTML e-mail. Često je dovoljno da se elektronička poruka samo otvori odnosno prikaže pa da se špijunski kod učita u računalo.

Još jedna metoda širenja je i „skrivanje“ unutar drugih programa. Mnogi programi koje možemo naći na Internetu (alatne trake, besplatni alati, igrice i sl.) sadrže špijunski kod koji se neprimjetno instalira zajedno s preuzetim programom.

Česta metoda širenja špijunskog koda su i mreže s ravnopravnim učesnicima (peer-to-peer) ili P2P mreže. Špijunski kod se nalazi unutar aplikacija koje se prenose takvim putem (što je obično ilegalno jer se većinom radi o zaštićenom komercijalnom sadržaju), a nerijetko se nalazi skriven i u samim alatima za ravnopravne korisnike (P2P programima).

Špijunski kod, nakon inficiranja računala može pratiti aktivnost korisnika, bilježiti svaki udarac tipke (key logger), pratiti svaki aktivni program i bilježiti vrijeme korištenja svakog programa na računalu. Može mijenjati postavke i „oteti“ (hijack) web preglednik tako da promijeni postavljenu početnu stranicu pri svakom surfanju, dodavati oznake (bookmark) i slično. Također često nameće neželjene reklame i oglase. Može sakupljati informacije o svim programima instaliranim na računalu, pratiti navike surfanja korisnika – koje stranice posjećuje, koliko često, te koliko dugo se zadržava na svakoj. Sakuplja i e-mail adrese (radi spama) ili čak ključeve programskih licenci (u svrhe piratstva). Špijunski kod također može sakupljati imena, brojeve kreditnih kartica, podatke o korisničkim računima te druge osobne podatke. Informacije skupljene špijunskim programima se obično kombiniraju s drugim bazama podataka, te se stvaraju kompletni profili pojedinaca, obitelji, radnih grupa ili čitavih tvrtki. Takvi profili se uglavnom koriste u svrhe direktnog marketinga.

Pored svega, špijunski kod može zagušiti sistemsku memoriju i zauzimati prostor na tvrdom disku, uzrokujući smanjenje performansi. Može zagušiti sustav toliko da računalo postane neupotrebljivo.

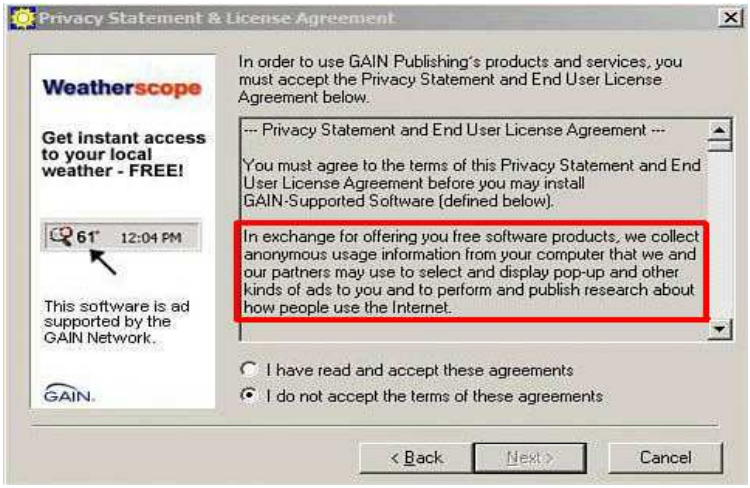
Pomoću maliciozne ActiveX kontrole napadač može postaviti i stražnja vrata (backdoor) u računalo, čime osim dobivanja pristupa informacijama, dobiva i potpunu kontrolu nad inficiranim računalom.

2.1.8. Reklamni kod (adware)

Reklamni kod, odnosno reklamni programi (adware) su najčešće različiti oblici besplatnih (freeware) programa koji od korisnika, u zamjenu za besplatno korištenje, zahtijevaju izvođenje sponzorskih oglasa tijekom rada programa. Iako se pogodba čini korektna, takvi programi obavljaju u pozadini i neke poslove kojih korisnik nije svjestan. Sakupljaju informacije o korisniku, njegovim navikama u surfanju Internetom i korištenju računala. Informacije se skupljaju s ciljem da se na temelju tako formiranog profila korisniku prikazuju upravo one vrste oglasa koje bi ga mogle interesirati.

Korisniku se prikazuju oglasni privremeni (pop-up) prozori prema podacima o njegovim navikama ili čak oglasi vezani za ono što u tom trenutku radi. Mijenjaju se postavke web preglednika, preglednik se preusmjerava na određena web mjesta s ciljem potencijalne prodaje ili slično. Reklamni (adware) programi mogu čak i modificirati određene postavke operacijskog sustava koje se odnose na rad na mreži i znatno narušiti performanse računala.

Problem je taj što je korisnik svjesno instalirao takav program i time pristao na bilo koju radnju koju reklamni kod unutar programa izvodi čitavo vrijeme dok je program instaliran, dakle, ne samo dok je taj program aktivan. Iako neetično, takvo nešto nije i nelegalno jer su obično sve radnje koje program može vršiti navedene u EULA (End User License Agreement) – licenčnom ugovoru koji se prikazuje prilikom instalacije i koje većina korisnika prihvati, a da i ne pročita.



Slika 2.3. - EULA (licenčni ugovor) za program Weatherscope
koji jasno upozorava da će u zamjenu za besplatno korištenje programa
sakupljati informacije o korisniku koji ga instalira

Vrlo je poznat program Kazaa, program za rad s mrežama s ravnopravnim učesnicima (peer-to-peer) koji ima besplatnu inačicu koja sadrži reklamni kod (adware). Kazaa je program kojeg koristi velik broj ljudi, a svoju malicioznu reklamnu (adware) komponentu nimalo ne sakriva – već je jasno navodi prilikom instalacije. Drugi poznati primjeri takvih programa su Weatherscope, Claria (Gator Software), Hotbar, Ezula i drugi.

Po definicijama – bilo kakva aplikacija koja prikazuje transparente i reklame dok je program aktivan naziva se reklamnim kodom (adware).

Bilo kakav program odnosno kod koji šalje podatke nekoj trećoj strani bez znanja korisnika smatra se špijunskim kodom (spyware).

Neki smatraju da je reklamni kod (adware) samo podvrsta špijunskog koda (spyware). Neki poistovjećuju jedno i drugo. Dok drugi izričito razdvajaju ta dva pojma. U osnovi, obje vrste nametnika bez znanja korisnika sakupljaju podatke i šalju ih nekom drugom. Špijunski kod međutim, ima mnogo varijacija od kojih je većina možemo reći veoma podmukla i obavlja velik

broj radnji koji mogu prilično naštetiti žrtvi. Dok je reklamni kod pretežno marketinški usmjeren, manje štetan ali mnogo više iritantan. Ima manje mogućnosti od kojih je glavna zapravo nekontrolirano prikazivanje reklama s osnovnim ciljem prodaje. Očito je da se karakteristike koje imaju špijunski i reklamni programi u nekim elementima preklapaju, što dovodi do zaključka da je nerijetko teško razlučiti što je što.

U svakom slučaju, činjenica je da je velik broj programa koje se smatraju špijunskim kodom, u biti i reklamni kod. To samo dodatno svjedoči o tankoj liniji koja razgraničava jedno od drugog. Lista deset najpoznatijih špijunskih programa iz 2004. godine (tablica 2.1.) jasno prikazuje da su gotovo svi programi s te liste zapravo reklamni.

	NAZIV	PRODAVAČ (distributer)	VRSTA
1.	Gain	www.gainpublishing.com	reklamni kod
2.	Claria (Gator)	www.gainpublishing.com	reklamni kod
3.	Gamespy arcade	www.gamespyarcade.com	reklamni kod skriven unutar igrice
4.	Hotbar	www.hotbar.com	prati aktivnost i navike surfanja
5.	Ezula	www.ezula.com	reklamni kod
6.	BonziBuddy	www.bonzi.com	Prati navike, mijenja početnu stranicu preglednika
7.	Weathercast	www.WhenU.com/products.html	oglasi u vremenskoj prognozi
8.	LinkGrabber 99	www.Netjumper.com	oglasi u pregledniku
9.	TOpicks	www.topicks.com	reklamni kod
10.	Cydoor	www.cydoor.com	reklamni kod

Tablica 2.1 Najpoznatiji špijunski programi 2004. godine

2.1.9. Birači (dialer)

Postoje dvije vrste birača (dialer) – oni dobri i oni loši. Birač (dialer) je u osnovi program instaliran na računalo kao dio operacijskog sustava koji omogućava spajanje na Internet putem analogne modemske veze.

Međutim, sama funkcija takvog programa je i zloupotrijebljena da bi nastalo birač (dialer) koji znači nešto loše – čime je stvorena i ta druga vrsta, ona loša, za koju su čuli gotovo svi korisnici Interneta. Birači uglavnom prekidaju normalnu vezu s pružateljem usluga (ISP – Internet Service Provider) i uspostavljaju skupe međunarodne veze. Uspostavljaju se astronomski skupi pozivi u prekooceanske zemlje i to korištenjem telefonskih centrala u državama koje slabo provode zakone. Isto tako mogu i inicirati preuzimanje komercijalnog sadržaja (download) sa posebnih Web mjesta koji se naplaćuju putem telefonskih računa, po posebnim tarifama. O biračima se često govori putem raznih medija, gdje razne telekomunikacijske tvrtke upozoravaju korisnike na opasnost od visokih telefonskih računa uzrokovanih zloćudnim biračima – računa koji se moraju platiti. Jedna je stvar jasna – birači uzrokuju veliku financijsku štetu.

Računalo može biti zaraženo njima putem ActiveX i JavaScript skripta, pomoću trojanaca ili se mogu skrivati u privitcima spam e-maila. Oni tiho, u pozadini inicijaliziraju modem i ostvaruju pozive dok korisnik ne sumnjajući ništa pregledava Internet, tako da baš i nije moguće primijetiti njihovu aktivnost, prije nego stigne telefonski račun. Da bi birači mogli funkcionirati, modem mora biti spojen na telefonsku liniju, stoga su najveći rizici za korisnike koji koriste klasičnu modemsku vezu (dial-up). Korisnici DSL-a ili širokopojasne veze obično nisu u opasnosti.

2.1.10. Lažno predstavljanje, zavaravanje (spoofing)

U računalnom svijetu zavaravanje, lažno predstavljanje (spoofing) se odnosi na mrežne komunikacije, a znači pretvaranje pojedinca da je netko drugi, falsificiranje identiteta, prikrivanje tragova i sl. Jednostavnije rečeno, podaci se šalju ciljanom računalu na način da se čini kao da stižu od nekog drugog, a ne stvarnog izvora.

Mnoge tehnike lažnog predstavljanje (spoofing) koje postoje, koriste se za ostvarivanje pristupa računalu i pribavljanje informacija, te slanje raznih podataka ili programa ciljanom korisniku. Tako se u svrhe zavaravanja (spoofing) iskorištavaju IP adrese, web adrese i e-mail poruke kao najpoznatije tehnike. Isto tako, nešto rjeđe koriste se i ARP zavaravanje (ARP spoofing), DNS zavaravanje (DNS spoofing) i sl.

IP zavaravanje (IP spoofing) – tehnika zavaravanja korištenjem podataka o adresama unutar paketa koji putuju mrežom. Svaki paket sadrži IP adresu izvorišta i odredišta. Zamjenom ispravne IP adrese izvorišta lažnom, napadač šalje podatke koji naizgled stižu sa legitimne IP adrese, čime je zamaskiran pravi izvor napada.

Tu se zapravo napadač ubacuje u komunikaciju između ciljanog računala i nekog drugog (obično poznatog) korisnika, predstavljajući se kao taj drugi. Da bi takav napad bio uspješno izvršen, napadač prvo mora identificirati mete, onemogućiti onaj sustav kojeg planira „glumiti“ i krivotvoriti njegovu adresu. Zatim je potrebno uspostaviti komunikaciju s ciljanim sustavom, predstavljajući se kao to prethodno onemogućeno računalo. Tu je zapravo sadržana čitava kompleksnost takvog napada jer napadač mora pogoditi ispravni slijedni broj (sequence number) potreban za autentifikaciju i ostvarenje veze.

IP zavaravanje se često koristi za izvršenje DoS napada (denial-of-service) – napada uskraćivanjem usluge.

E-mail zavaravanje (e-mail spoofing) – tehnika krivotvorenja informacija u zaglavlju elektroničke poruke tako da se čini kao da stiže s nekog drugog odredišta, najčešće nekog korisniku poznatog. Protokol koji se koristi za e-mail, SMTP (Simple Mail Transfer Protocol), ne obuhvaća nikakvu autentifikaciju za provjeru izvorišta odnosno pošiljatelja. Zamjenom adrese pošiljatelja, e-mail naizgled stiže od nekog drugog, nekog tko ga nije poslao; i bez implementacije nekih sigurnosnih mjera, gotovo je nemoguće utvrditi pravog pošiljatelja.
Tehniku e-mail zavaravanja najčešće koriste autori virusa. Širenjem virusa putem e-maila uz krivotvorenje adrese pošiljatelja uvelike otežava korisnicima koji prime virus da pronađu izvor. E-mail zavaravanje također koriste i distributeri spam e-maila da bi prikrili svoj identitet. Unutar e-maila se isto tako metode zavaravanja primjenjuju i na poveznice (link) – poveznice koje izgledaju kao legitimne web adrese, zapravo otvaraju sasvim druge stranice. Takve prijevare se obično koriste kao jedna od tehnika neovlaštenog traženja informacija (phishing) koji je objašnjen nešto kasnije.

Web zavaravanje (web spoofing) – tehnika maskiranja web adresa na način da se presreće zahtjev za pregledom nekog web mjesta i zatim se umjesto na traženu web stranicu ili web mjesto korisnika preusmjerava na neku drugu web adresu. Na toj adresi se može nalaziti lažno, nepostojeće web mjesto koje izgleda legitimno ili web mjesto koje „glumi“ neko već postojeće.
Takva lažna web mjesta koja imitiraju neka već poznata, najčešće imaju adrese (URL) vrlo slične onima koje predstavljaju (npr. www.micrsoft.com ili čak www.micr0s0ft.com) pa žrtve misle da su doista pristupaju tim stranicama, jer stranice na koje su preusmjereni doista izgledaju legitimno.

Još jedna opcija je trik koji se počeo koristiti nakon što je na webu omogućeno registriranje imena domena korištenjem drugih skupova znakova (character set) osim latinskog. Na taj način koriste se znakovi koji izgledaju isto ali imaju drugačije značenje, pa su drugačije i kodirani. Na

primjer, slovo y u ćirilici ima drugačije značenje od latiničnog y i koristeći taj podatak netko može registrirati domenu yahoo.com (koristeći ćirilične znakove) bez problema, jer neki web preglednici ne mogu razlučiti (ili prikazati) razliku između te domene i pravog yahoo web mjesta. Pomoću takvih trikova može se vrlo lako lažirati stranica koja osim što izgleda isto, ima i potpuno istu adresu tj. adresa će izgledati isto u adresnoj traci web preglednika.

Web zavaravanje se najčešće koristi za zloupotrebu stranica koje pružaju neke usluge kao npr. Internet kupovina, odnosno stranice koje traže unošenje nekih osobnih podataka, kao brojeve kreditnih kartica ili podatke o korisničkim računima, koje se kradu na taj način.

ARP zavaravanje (ARP spoofing) – (ARP - Address Resolution Protocol) – falsificiranje MAC (Media Access Control) adresa kod Ethernet okvira.

DNS zavaravanje (DNS spoofing) – (DNS – Domain Name Server) – falsificiranje informacija u DNS paketima – preuzimanje uloge, „glumljenje“ legitimnog DNS poslužitelja.

2.1.11. Neovlašteno traženje informacija (phishing i pharming)

Neovlašteno traženje informacija (phishing i pharming) i mnoge druge tehnike varanja korisnika temelje se na socijalnom inženjeringu. Prijevarom, manipulacijom se natjera korisnika da samostalno izvrši neku radnju (instaliranje nekog programa, otkrivanje osobnih podataka i slično). Takva radnja je najčešće njemu samom na štetu, ali je prijevara obično dovoljno dobro izvedena da toga nije svjestan. Barem ne na vrijeme.

Neovlašteno traženje informacija (phishing) uključuje kontaktiranje žrtve putem elektroničke pošte, soba za razgovor (chat rooms) ili usluga trenutnih poruka (instant messaging). Najčešće se šalje neka vrsta obavijesti kako je potrebno unijeti određene osobne podatke sa svrhom potvrde ili ažuriranja korisničkog računa, pozivi na doniranje novca u lažne dobrotvorne svrhe, obavijesti o nekom novčanom dobitku, lažne obavijesti od administratora i slično.

Mnogi korisnici nasjednu na takve prijevare, pogotovo zato što se obično radi o naizgled legitimnim tvrtkama ili uslugama kao što su banke, pružatelji Internet usluga (ISP), tvrtke za Internet trgovinu i slično. Prijevare često uključuju poznata imena kao PayPal, eBay, Best Buy ili poznate banke.

Unutar te obavijesti (najčešće e-maila) nalazi se poveznica (link) na neko web odredište gdje je potrebno unijeti podatke. Klikom na poveznicu, web preglednik otvara stranicu koja izgleda veoma realistično i uvjerljivo. To je tipično neka lažna stranica i nakon unošenja potrebnih podataka, sve te podatke preuzima autor prijevare. Podaci koji se traže su osobni podaci, lozinke, brojevi kreditnih kartica, brojevi bankovnih računa i slično, a cilj je vrlo očit – krađa identiteta i financijska prijevara.

Klikom na takve poveznice, osim krađe osobnih podataka velika je vjerojatnost i da se inicira instalacija i nekakvog malicioznog koda kao špijunskih programa (spyware), crva ili trojanskih konja.

Takva prijevara (phishing) uključuje integraciju više elemenata. Moguće špijunskog koda (spyware) koji sakuplja informacije o korisniku koje se kasnije koriste za slanje prave vrste obavijesti na koju će konkretan korisnik nasjesti. Isto tako, da bi se čitava zamka uspješno izvršila, koriste se tehnike zavaravanja (spoofing) objašnjene u prethodnom poglavlju. Tehnike zavaravanja, lažnog predstavljanja (spoofing) se koriste da bi se lažirale adrese pošiljatelja u e-mailovima koji sadrže varku, za maskiranje poveznica na koje korisnik treba kliknuti, te da bi se lažirala web mjesta na kojima korisnik treba unijeti potrebne podatke.

Činjenica je da poznate tvrtke ili financijske organizacije nikada ne traže od korisnika osobne podatke na takve načine, već obično šalju formalna pisma. Specifično je da su takvi tipovi elektroničkih poruka često puni gramatičkih grešaka i pogrešno napisanih riječi. Često se lažiraju i e-mailovi od Microsofta koji navodno sadrže poveznice na najnovije zakrpe ili se pak te zakrpe navodno nalaze u privitku tog e-maila. Opće je poznato da Microsoft nikada ne prakticira takav pristup, već da je jedini siguran način ručno preuzimanje zakrpa s Microsoftovih stranica ili korištenje usluge automatskog ažuriranja (Automatic Updates). Događa se da se takve poveznice šalju i putem usluga trenutnih poruka (instant messaging) i to na način da se čini kao da pristižu od poznate osobe. Postoje mnogi oblici zavaravanja žrtve od kojih su neki i na prvi pogled vrlo sumnjivi, no ipak dovoljno uvjerljivi naivnom korisniku. Takve vrste prijevara se obično oslanjaju na neznanje i naivnost korisnika koji im zapravo svojevoljno predaju svoje osobne i povjerljive podatke. Osnovna premisa socijalnog inženjeringa na djelu – bilo kakav podatak se može dobiti od nekoga, samo treba pitati na pravi način. Sam izraz „phishing“ je adaptacija engleske riječi „fishing“ – pecanje, a aludira na sam lov i mamac na koji se korisnici trebaju upecati.

Neovlašteno traženje informacija prijevarom (pharming) je također vrsta prijevare s istim ciljem kao i prethodna, no s nešto opskurnijim metodama. Puno je teže takvu prijevaru otkriti čak i stručnjacima, budući da je gotovo nevidljiva. Zastrašujuća je pomisao takve prijevare koja je vrlo suptilna, dakle ne pokušava namamiti korisnika i izmanipulirati ga na neke radnje, a opet, riječ je o ozbiljnom narušavanju sigurnosti.

Izraz „pharming“ je adaptacija engleske riječi „farming“ – uzgoj na farmi. Riječ je o otmici prave adrese i postavljanju imitacije tražene web stranice.

Neovlašteno traženje informacija prijevarom (pharming) se zasniva na tehnikama kompromitiranja DNS (Domain Name Server) poslužitelja, mijenjanjem njihove priručne memorije (cache) na način da pohranjuje krive IP adrese. Tako da korisnik, kada želi posjetiti na primjer, web mjesto svoje banke, biva preusmjeren na krivu (lažnu) stranicu zbog toga što će DNS poslužitelj vratiti krivu IP adresu. Stranica koja će se prikazati će nalikovati na pravu stranicu banke, ali je riječ o imitaciji, lažnoj stranici koja izgleda realno i uvjerljivo, ali kojom upravlja autor prijevare (pharmer). I naravno, nakon unošenja osobnih podataka radi pristupa korisničkom računu, napadač dolazi u posjed povjerljivih osobnih podataka koje dalje iskorištava u svrhe krađe identiteta i financijske prijevare.

Donekle je utješno to što se takva vrsta prijevare događa rjeđe od ostalih (npr. phishing), međutim alarmantno je to što ogroman broj nevinih ljudi biva prevaren i opljačkan iako takvi napadi traju vrlo kratko. Još strašnija je činjenica da tijekom tog procesa web preglednik uredno prikazuje da se nalazi na ispravnom web mjestu iako je ono lažno.

Vrlo je malo toga što pojedinac može poduzeti u obrani od takve prijevare. To je problem kojeg rješavaju pružatelji Internet usluga (ISP) i telekomunikacijske tvrtke i organizacije koje posjeduju DNS opremu na Internetu.

2.1.12. Prijevara (hoax)

„Hoax“ u prijevodu znači prijevara, obmana i to je upravo ono što jest. To je u naravi lažna obavijest koja se širi putem e-maila (spam). Ne sadrži nikakav maliciozan kod i osnovni cilj je prosljeđivanje iste što većem broju korisnika nakon primitka.

Takve prijevare dijele se u dvije osnovne skupine – lažna obavijest o virusima (virus hoax) i lančana pisma.

Lažna obavijest o virusima (virus hoax) je obično e-mail poruka koja sadrži informacije o nekom užasnom virusu (fiktivnom) koji se širi velikom brzinom, inficira ogromne količine

računala i nijedan zaštitni program ga zasad ne može detektirati. To su obavijesti dramatičnih naslova koje većinom sadrže mnoštvo kompliciranih tehničkih izraza (nerijetko izmišljenih) i pozivaju se na poznata imena poput IBM-a, Microsofta ili nekih organizacija koje se bave sigurnošću. Obično unutar iste poruke navode neke prijetnje o posljedicama u slučaju da se ne poduzmu određene mjere. I naravno, svi oni traže od korisnika da proslijedi tu poruku svima iz svog adresara. Iako je riječ o obavijesti o nepostojećem virusu, i takva varka može uzrokovati štetne posljedice. Panika uzrokovana obaviješću motivira korisnike na daljnje prosljeđivanje poruke što uzrokuje preopterećenje e-mail poslužitelja, potrošnju mrežnih resursa, gubitak vremena, troškove uzrokovane smanjenom produktivnošću stručnjaka i administratora koji su zatrpani upitima korisnika, a i sami mogu izgubiti dio vremena na provjeru potencijalne opasnosti.

Isto tako, neke takve prijevare mogu uzrokovati i konkretnu štetu. U obavijesti o novom virusu primatelju se detaljno objašnjava način na koji se može sam riješiti konkretne opasnosti, poduzimanjem neke radnje koja najčešće uključuje brisanje neke datoteke uz detaljne upute kako je pronaći. Korisnici koji nasjednu na takvu zamku mogu ne znajući obrisati neku valjanu sistemsku datoteku što može i ne mora uzrokovati probleme u radu računala.

Primjer je „**Teddy Bear**“ odnosno **JDBGMGR prijevara** koja je prisutna već dosta dugo. Poruka govori o opasnosti od zaraze strašnim Teddy Bear virusom (Teddy Bear – medo, medvjedić). Navodi detaljno kako pronaći konkretnu datoteku te da ju je potrebno ručno izbrisati da bi se riješili virusa. Budući da ta datoteka (jdbgmgr.exe) uistinu postoji na opisanom mjestu i uistinu ima ikonu sa sličicom medvjedića, naivni korisnik je vrlo lako može izbrisati. U ovom slučaju neće nastati neka velika šteta jer je riječ o pomagalu (Java debugger) koji dolazi standardno s operacijskim sustavom i čije brisanje neće omesti rad računala.

Drugu skupinu čine **lančana pisma** (chain letters) ili „pisma sreće“ poznata još od ranije kada su se širila putem pošte, kao prava pisma.

Ta skupina uključuje sve ostale vrste prijevara koje ne sadrže obavijesti o virusima. Tu su molbe za novčanu pomoć za bolesne, obitelji otetih i slično, koje apeliraju na suosjećanje. Prilike za zaradu samo prosljeđivanjem primljene poruke na što više adresa, prijetnje o gubitku novca ili lošoj sreći ako se poruka ne proslijedi. Lažna obećanja o darovima, peticije, obavijesti o terorističkim napadima ili čak obične šale. Nemaju konkretne štetne posljedice i osnovni cilj im je daljnje širenje na što više korisnika. Ipak, njihovo daljnje širenje osim samog gubljenja vremena (i strpljenja), može imati određene štetne posljedice – već navedeno preopterećivanje e-mail poslužitelja do te mjere da ih se čak može privremeno onemogućiti, potrošnja mrežnih resursa i na kraju krajeva – slanje i primanje ogromne količine beskorisnih poruka.

Većina ljudi koja se služi elektroničkom poštom navikla je na primanje spama i ovakvih obavijesti, pa ih je prilično lako otkriti. Dovoljno je promotriti naslov tog nepredviđenog i neželjenog e-maila koji obično dramatično ističe opasnost, nešto važno, nešto besplatno ili neku zaradu, da znamo da je riječ o prijevari i da takve poruke ne treba niti otvarati. Isto tako, većina spam filtara (anti-spam) danas relativno dobro prepoznaje takve poruke i rješava ih se.

2.1.13. Spam

Spam se najčešće kratko definira kao neželjena elektronička pošta koja se masovno šalje velikoj količini korisnika. Nešto nalik na velike količine reklamnih letaka koje vidimo svaki dan utrpane u poštanske sandučiće.

Izraz je usvojen od javnosti na račun jednog Monty Python skeča u kojem se spominje proizvod tvrtke Hormel - začinjena šunka u limenci nazvana SPAM. Iako je to zasmetalo ljudima iz tvrtke Hormel zbog negativne konotacije vezane za njihov mesni proizvod, izraz se jednostavno

zadržao, vjerojatno jer ga je bilo lakše zapamtiti od svih stručnih termina koji su dodjeljivani toj pojavi.

Dakle, riječ je o neželjenim e-mail porukama koje obično sadrže reklame za neke nove i neke sumnjive proizvode, usluge upitne legalnosti, ponude za brzu zaradu, ponude za rad kod kuće i slično. Statistike kažu da je oko 70 – 80% čitave elektroničke pošte koja se razmjenjuje zapravo spam i da jedan od 36 e-mailova sadrži virus ili neku drugu vrstu malicioznog koda.

Spam je više smatran smetnjom nego sigurnosnim problemom. No ipak, iako većinom ne sadrži maliciozan kod, može uzrokovati veću ili manju štetu. Obično veću. Iscrpljuje mrežne i računalne resurse zbog povećanog mrežnog prometa i potrošnje diskovnog prostora e-mail poslužitelja. Tu je očit i problem potencijalnih DoS napada koji osim zauzimanja resursa mogu vrlo lako i potpuno onemogućiti e-mail poslužitelj na neko vrijeme, čak i do nekoliko dana. Smanjuje radnu produktivnost jer je prilična količina vremena potrebna za korisnike elektroničke pošte pregledaju svoje e-mail sandučiće i izbrišu neželjene poruke. Uzrokuje velike troškove tvrtkama koje se pokušavaju boriti s tim problemom, novčana sredstva utrošena na programske alate i ljudske resurse. Pored toga svega, prisutni su i sigurnosni rizici zbog velikog broja malicioznih programa koji se prenose e-mailovima.

Svi korisnici elektroničke pošte su se susreli s problemom spama i već donekle i navikli na sandučiće pretrpane porukama s raznolikim naslovima od pošiljatelja za koje nikad nisu čuli. Međutim, većina neupućenih korisnika se još uvijek pita zbog čega te poruke stižu i kako su ti neznanci došli do njihovih e-mail adresa. Motiv je kao i uvijek naravno novac, i to poprilične svote novca. A do e-mail adresa se dolazi na razne načine. Obično ih sami korisnici učine dostupnima ispunjavanjem Internetskih registracijskih formulara, sudjelovanjem u natjecanjima, Internet anketama, sudjelovanjem u Internet forumima, uslugama za razgovor (chat), obavijesnim skupinama (newsgroup) i slično. Isto tako, nekad je dovoljno i samo odabiranje nekog jednostavnog imena za e-mail adresu.

Ljudi koji šire spam – spameri, koriste se raznim načinima pribavljanja e-mail adresa. Najčešći način je naravno kupovanje. Liste e-mail adresa se kupuju od svakoga tko ih nudi, a cijene variraju od izvora. Ako ih nudi vlasnik nekog web mjesta koji nudi besplatne sadržaje (uz registraciju), novci su sitni. A ako je riječ o nekoj respektabilnoj organizaciji, pogotovo ako se radi o onoj koja se bavi trgovinom, onda se plaća i do nekoliko dolara po svakoj adresi. Najvažnija je valjanost adresa, a respektabilniji izvor na neki način samim imenom garantira valjane adrese, zato je i cijena veća.

Oni koji ne kupuju e-mail adrese na takve načine, koriste se raznim programima za ekstrakciju adresa i sastavljaju vlastite liste. Koriste programe koji izvlače e-mail adrese sa raznih foruma i obavijesnih skupina (newsgroup) - gdje je obično uz poruku ispisana i e-mail adresa autora. Tu su pogotovo interesantne obavijesne skupine (npr. Usenet) i forumi koji se fokusiraju na konkretne teme (kao npr. zdravlje ili rekreaciju) jer sakupljanjem adresa sa takvih mjesta dobivaju gotovu listu potencijalnih kupaca za upravo takve proizvode. Takvi programi se koriste i za ekstrakciju adresa sa raznih osobnih ili poslovnih web stranica (gdje autori obično navedu svoju e-mail adresu), gdje se također mogu koncentrirati na web stranice konkretnog sadržaja.

Isto tako, e-mail adrese se izvlače iz raznoraznih baza podataka, recimo usluga za pronalaženje ljudi (npr. Bigfoot) gdje dobivaju liste adresa koncentrirane na pojedine geografske skupine ili pak ljude s određenim prezimenima.

Nakon što sakupe određenu količinu adresa, počinju slati spam na njih. Koriste se raznim metodama, kao što je otvaranje privremenih korisničkih računa kod raznih pružatelja usluga sa kojih masovno šalju beskorisnu elektroničku poštu i zatim ih zatvaraju prije nego ih netko napadne. Ili, ako im se ne da trošiti vrijeme na konstantno otvaranje i zatvaranje korisničkih računa, koriste se programima za masovno slanje e-mail poruka (mass – mailing), koji se lako

mogu pronaći na Internetu. Na primjer, na web stranicama – Bulk Email Software Superstore (http://www.americaint.com) i Send-Bulk-Email.co.uk (http://www.send-bulk-email.co.uk) može se pronaći mnoštvo takvih programa.

U spam porukama isto tako se često na kraju nalazi poveznica (link) na koju treba kliknuti da bi korisnik navodno bio skinut sa liste za slanje (mailing list). Klikom na takvu poveznicu, u svakom slučaju, spameru ste potvrdili da je poruka primljena i da je vaša e-mail adresa valjana. S tom potvrdom, može vam nastaviti slati spam, ili vašu adresu prodati drugom spamerima. Ili, u najgorem slučaju, klikom se može inicirati preuzimanje ili instalaciju nekog malicioznog programa.

Još jedna bitna stvar koju je potrebno istaknuti je činjenica da većina spam poruka zapravo stiže s računala (većinom privatnih, osobnih računala sa brzom vezom na Internet) koja su zaražena nekom vrstom malicioznog koda. Takav kod „otima“ zaraženo računalo. Napadač dobiva potpunu kontrolu nad inficiranim računalom i koristi ga da bi s njega anonimno slao velike količine spama, a krivnja pada na korisnika koji obično nema pojma o tome. Takvo računalo naziva se zombi.

Upravo se za izvođenje DoS napada spomenutog ranije koristi velika količina računala pretvorena u zombije. Isto tako, zbog velike količine resursa kojim napadač raspolaže, može se izvesti i DDoS napad na npr. neko web sjedište ili pak neki DNS poslužitelj, onemogućivši njegov rad i onemogućivši pristup drugim korisnicima.

Pomoću trojanca koji omogućuje udaljeni pristup (RAT), koji se naziva i bot (skraćeno od robot), može se ostvariti preuzimanje velike količine računala, čime napadač stvara svoju mrežu zombija, koja se naziva i botnet. Takvu mrežu može iskoristiti za recimo neki od navedenih napada, ili pak može prodati drugim napadačima i spamerima za određenu svotu novaca. Za primjer, postojala je jedna takva web stranica – Internet trgovina zombi mrežama koja je nudila 5000 računala za 300 dolara.

Spam je problem na koji treba obratiti posebnu pozornost. To je pojam koji u sebi na neki način objedinjuje skoro pa sve ostale nametnike koji vrebaju Internetom. Od malicioznog koda (virusi, crvi, trojanski konji, špijunski programi...) koji se skrivaju u privitcima, mogu inficirati računalo samim otvaranjem poruke ili se skrivaju iza poveznice (link) unutar poruke koja vješto izmanipulira korisnika da klikne na poveznicu. Zatim prijevara (hoax) koje obično dolaze u obliku e-mail poruke. Pa do neovlaštenog traženja informacija (phishing) i zavaravanja (spoofing) koji su usko vezani sa spamom (zavaravanje poveznicama, web zavaravanje, e-mail zavaravanje...).

Spam integrira sve forme malicioznog koda i socijalnog inženjeringa u jedan sveobuhvatan problem za koji za sada nema kvalitetnog rješenja.

2.1.14. Hakeri (hacker) i krekeri (cracker)

Postoji tri grupe, odnosno vrste ljudi uključene u priču o računalnoj sigurnosti – stručnjaci koji proučavaju to polje i preporučuju preventivne mjere i rješenja; šira javnost koja ustvari osjeća posljedice sigurnosnog sloma i, većinom anonimni, počinitelji raznih napada i nedjela. Ta treća skupina se u svakodnevnom govoru generalizirano proglašava hakerima, iako je to vrlo kontroverzan termin. Javnost ga previše eksploatira, a stručnjaci s oprezom koriste.

Tradicionalno gledano, haker je osoba koja voli istraživati i eksperimentirati sa programskim kodom ili elektroničkim sustavima. Hakeri uživaju u proučavanju i učenju o tome kako funkcioniraju računalni sustavi. Vole otkrivati nove načine i pristupe elektroničkom radu.

U posljednje vrijeme, izraz haker poprima novo značenje, obično s negativnom konotacijom. Izraz je iskrivljivan od medija i javnosti, tumačen i prikazivan na raznolike načine, a danas se

obično odnosi na osobe koje „provaljuju“ u tuđa računala, pogotovo kad je u pitanju neka maliciozna nakana. Striktno gledano, to nije točno. Osoba koja „provaljuje“ u računala je kreker (cracker; crack – razbiti), a ne haker.

U računalnim krugovima, biti prozvan hakerom je nešto pozitivno i znači da je osoba vješta u računalnom programiranju – hakiranje nema veze s malicioznim kodom i nedopuštenim upadima. Današnji haker je uglavnom stručnjak u računalnom i srodnim poljima koji traži načine da iskoristi slabosti ili ranjivosti određene komponente tih polja. Ta komponenta može biti komad sklopovlja (hardware), dio operacijskog sustava ili neka aplikacija.

Hakeri su obično programeri. Kao takvi, posjeduju napredno znanje o operacijskim sustavima i programskim jezicima. To im omogućava da otkrivaju rupe i propuste u sustavima, te uzroke tim propustima.

Nisu svi hakeri stručnjaci, niti su svi zlonamjerni. Mogu biti motivirani čitavim spektrom različitih razloga, od obične znatiželje pa do kriminalnih namjera. U moru različitih asocijacija uz izraz haker, ističe se nekoliko skupina ljudi. Tu imamo programerske genije koji smišljaju inovativne načine kodiranja nekih rješenja. Socijalne aktiviste (koji se nazivaju i haktivisti - hacktivist) koji poduzimaju određene radnje kao oblik protesta na npr. neka politička ili slična pitanja. I naravno, kriminalce koji kradu, kontaminiraju ili uništavaju podatke zbog zarade, dokazivanja moći ili čiste pakosti.

Isto tako, postoji još jedna podjela vezana za motivaciju. Podjela na tri skupine koje se označava po bojama šešira – aluzija na stare vestern filmove u kojima su dobro dečki obično nosili bijele šešire, a loši crne. Pa tako imamo hakere crnih šešira (black-hat hacker) – hakere s malicioznom nakanom da pronađu ili oštete povjerljive i važne podatke. Druga krajnost su hakeri bijelih šešira (white-hat hacker) – legitimni sigurnosni eksperti sa znanjem i iskustvom zlonamjernih hakera ali kojega koriste u svrhe zaštite. Treća skupina su hakeri sivih šešira (grey-hat hacker). Oni, kako se i može iz imena zaključiti, po aktivnostima i motivaciji ne spadaju ni u dobre ni loše, već negdje između. Za njih se smatra da ih više motivira znatiželja, nego maliciozne nakane.

U tome svemu, veoma je bitno istaknuti da hakeri nisu ti koji upadaju u tuđe sustave, „provaljuju“ u računala i preuzimaju kontrolu nad njima. To su aktivnosti jedne druge skupine koja se naziva krekeri (cracker). Krekeri su ljudi koji probijaju ili na neke druge načine narušavaju integritet sustava udaljenih računala s malicioznom nakanom. Nakon što dobiju neovlašten pristup, uništavaju ili kradu vitalne podatke, onemogućuju pristup legitimnim korisnicima ili uzrokuju probleme svojim žrtvama. Obično s ciljem osobne dobiti – slave, zarade ili možda osvete. Ukratko, krekeri obuhvaćaju sve ono negativno što se pridaje hakerima, a to i jesu – hakeri kriminalci (cracker – criminal hacker).

I njih se može podijeliti u dvije osnovne skupine. Tako je tu skupina stručnjaka, vještih krekera koji otkrivaju nove sigurnosne rupe i propuste i često pišu programe koji iskorištavaju te propuste da bi dobili pristup računalima. Na sreću, njih je malo. Drugu skupinu čini zainteresirana mladež koja pronalazi besplatne alate na Internetu i koristi ih za provaljivanje u računala, samo prateći upute; bez nekog znanja o čitavom procesu, već čisto da se mogu pohvaliti (nazivaju se i „script-kiddies“). Ipak, iako ne znaju što konkretno rade, mogu napraviti popriličnu štetu.

Izraz haker je počesto izrabljivan, u romantiziranim prikazima svijeta računala kroz nerealne filmove, u novinskim člancima o milijunskim štetama izazvanim napadima frustriranih čudaka, o upadima u vrhunski zaštićene sustave od strane nadobudnih klinaca i slično. Nije potrebno dodatno isticati kako je to sve stvorilo određenu sliku kod šire javnosti o tome što hakeri jesu i što rade. Slika koja je možda posve netočna ili pak tek malo dalje od istine, ali svakako slika koja se zadržala već duže vrijeme. I obično će tako i ostati još neko vrijeme.

2.2. OPASNOSTI IZNUTRA

Windows operacijske sustave koristi većina ljudi u svijetu. Najviše su korišteni i zato najviše na meti napada. Svaki dan izlaze nova izvješća o novim propustima koji su otkriveni, novim mogućnostima iskorištenja tih propusta i novim napadima. Naravno, izlaze i zakrpe no ponekad se dogodi da su izašle prekasno za neke korisnike, ili jednostavno nisu bile na vrijeme primijenjene.

Zbog svega toga se može postaviti pitanje o kvaliteti i samoj sigurnosti Windows operacijskih sustava. No, da li je toliki broj propusta znak loše kvalitete i manjkavosti operacijskog sustava ili je to samo rezultat činjenice da se najkorišteniji proizvodi najviše proučavaju. Napadač pokušava pronaći način penetriranja u sustave i pisanja malicioznog koda koji se može primijeniti na što veći broj računala. A najbolja garancija za to je ciljanje na one aplikacije i operacijske sustave koji se najviše koriste.

Pored svih virusa, crva i ostalih nametnika koji kruže Internetom, činjenica ostaje da je najveći postotak proboja sigurnosti zapravo uzrokovan problemima iznutra, dakle u operacijskom sustavu i općenitoj zaštiti pojedinog računala.

Mnogi sigurnosni rizici mogu se eliminirati samo redovnim ažuriranjem, primjenom zakrpa i nadogradnji. Ipak, velik broj ljudi to ne radi. Možda zbog nemara ili zbog stava koji mnogi ljudi imaju - da na računalu običnog korisnika i nema nešto vrijedno tolike zaštite. Na računalima postoji mnogo vrijednih informacija kojih ljudi često nisu ni svjesni. Osobni podaci, financijski podaci – sve su to vrijedne informacije koje se mogu unovčiti kao takve ili iskoristiti za krađu identiteta ili financijskih sredstava. Drugi razlog zbog kojeg je bitno zaštititi računalo, je činjenica da zaštitom svog računala, korisnik doprinosi zaštiti drugih. Pored štete koju napadači i maliciozni programi mogu nanijeti računalu i korisniku, isto tako neki mogu „oteti“ računalo i koristiti da za napade na druge.

Nabrajanje svih sigurnosnih propusta i ranjivosti Windows XP operacijskog sustava je sasvim nepotrebno jer je lista preduga i ne govori mnogo o općenitim problemima. Stoga je dovoljno samo generalno spomenuti neke osnovne elemente operacijskog sustava koji su najosjetljiviji na potencijalne napade.

2.2.1. Lozinke

Lozinke su primarna metoda dobivanja pristupa računalu (operacijskom sustavu) ili aplikaciji. Doduše, lozinke isto tako daju lažni osjećaj sigurnosti. Dobra lozinka je jedan od ključnih elemenata sigurnosti, ali često previđen. Razbijanje (cracking) lozinki jedan od najlakših i najčešće korištenih metoda koje napadači koriste da bi zadobili neovlašteni pristup računalu ili mreži.

Lozinke se oslanjaju na tajnost. Nakon što je lozinka kompromitirana, početni vlasnik lozinke više nije jedina osoba koja može dobiti pristup pomoću nje. I tu počinju problemi. Ljudski faktor i tehničke ranjivosti glavni su razlozi zbog kojih su lozinke jedna od najslabijih karika u lancu informacijske sigurnosti. Korisnici odabiru lozinke koje su kratke, jednostavne i predvidljive; ne mijenjaju ih, koriste iste lozinke na više mjesta i zapisuju ih na nesigurnim mjestima. Drugi dio problema uključuju loši mehanizmi za šifriranje, nesigurna pohrana lozinki na računalnim sustavima i aplikacije koje ne skrivaju lozinku na ekranu prilikom upisivanja (prikazuju je dok se upisuje).

Napadači koriste razne metode razbijanja i pribavljanja lozinki. Ciljaju bilo kakve lozinke, no najzanimljivije su im administratorske lozinke pomoću kojih mogu dobiti najviši nivo pristupa i mogu izvršiti gotovo bilo koju radnju na sustavu. Postoje jednostavniji načini, staromodniji, kao i oni napredniji.

Napadač može dobiti lozinku tako da jednostavno korisnika upita da mu je da (socijalni inženjering) predstavljajući se kao administrator ili neka stručna osoba, s nekim uvjerljivim razlogom. Isto tako, lozinke se mogu doznati „gledanjem preko ramena“ – promatranjem dok korisnik upisuje lozinku. Takve metode se često koriste i u svakodnevnom životu npr. u trgovini dok kupac upisuje PIN za autorizaciju kupnje preko kartice. Isto tako, neki napadači pokušavaju pogoditi lozinke na osnovu podataka koje znaju o žrtvi jer ljudi često kao lozinku koriste ime ljubimca, člana obitelji ili slično.

U naprednije uglavnom se svrstavaju automatizirane tehnike, korištenjem raznih alata i pomagala. Koriste se raznorazni programi za razbijanje lozinki (password-cracking software) kao: LC4, NetBIOS Auditing Tool, John The Ripper, Crack, Pandora, NTFSDOS Professional i sl. Temelje se uglavnom na dva principa otkrivanja lozinki:

- Rječnički napadi (Dictionary attack) kojima se pomoću posebnih alata velikom brzinom isprobavaju sve riječi iz baze lozinki, ne bi li pogodili pravu. Te baze su obično tekstualne datoteke s abecednim popisom tisuća riječi i izraza
- Napadi grubom silom (Brute force attack) – koji mogu pogoditi bilo koju lozinku, uz dovoljno vremena. Takvi napadi se zapravo temelje na isprobavanju svih mogućih kombinacija slova, brojeva i specijalnih znakova dok se ne pronađe prava. Neki alati za takav napad omogućuju i određivanje nekih kriterija, kao određeni znakovi ili duljina lozinke. Lako je zaključiti da takvi napadi mogu trajati dosta dugo, ovisno o kompleksnosti lozinke i brzini računala na kojem se izvršavaju ti alati.

2.2.2. Korisnički računi

Korisnički računi (User Account) su primarno sredstvo kontroliranja pristupa podacima i resursima računala. Upravo zbog toga napadači dobro poznaju osnovne postavke operacijskog sustava po pitanju korisničkih računa.

Korisnički račun koji ima potpuni pristup računalu je administratorski račun. Prilikom instalacije Windows XP operacijskog sustava obvezno je stvoriti najmanje jedan korisnički račun (a može najviše pet) i svi računi stvoreni u tom trenutku automatski su pridruženi administratorskoj grupi i nemaju postavljenu lozinku. U slučaju da korisnik ostavi takve postavke, vrata su širom otvorena za se napadače. Isto tako, veći broj korisničkih računa znači veći sigurnosni rizik. Ako je i postavljena lozinka, napadači znaju da je sve što trebaju da bi dobili pristup računalu valjano korisničko ime i pridružena lozinku administratorskog računa. Da bi odredili koji je korisnički račun na računalu administratorski, napadači koriste razne metode. No, početnici se uglavnom drže uobičajenih navika korisnika pa traže imena poput Administrator, Admin, Home, Obitelj ili ime i varijacije imena korisnika. U svakom slučaju, administratorski račun omogućuje potpuni pristup, sve privilegije koje korisnik može imati i stoga je najveći sigurnosni rizik i potrebno je poduzeti sve moguće mjere zaštite da bi se što više otežalo potencijalnim uljezima.

Postoji još jedan standardni korisnički račun koji predstavlja laku metu napadačima, a to je gost (Guest) korisnički račun. Iako pruža ograničen pristup i privilegije, ipak ima dovoljno funkcionalnosti koje se mogu iskoristiti za upad u sustav.

2.2.3. Datotečni sustav

Prilikom formatiranja tvrdog diska, može se odabrati FAT32 ili NTFS datotečni sustav (File system). Oba imaju svoje prednosti i nedostatke, ali sa sigurnosne perspektive, NTFS nudi više. FAT32 ne omogućuje nikakvu sigurnost mapa i datoteka, što ostavlja sustav otvorenim za napade. NTFS zato omogućuje osiguravanje datoteka na individualnoj razini i ograničavanje pristupa datotekama. NTFS isto tako omogućuje korištenje EFS sustava šifriranja (Encrypting

File System) za dodatnu sigurnost podataka. Kod dijeljenja datoteka, FAT32 ne omogućuje sigurnost na nivou datoteke. I na kraju, NTFS ima potporu za veće datoteke i particije i pruža bolju kompresiju i manje fragmentacije datoteka od FAT32.

2.2.4. Čuvar zaslona

Čuvar zaslona je u početku bio mjera zaštite ekrana monitora. Kod starijih monitora, kad bi neka slika stala predugo, urezala bi se u fosforni sloj i trag bi ostao trajno. Danas je tehnologija izrade monitora toliko napredovala da više nije potreban čuvar zaslona kao zaštita monitora. No, bez obzira na to, čuvari zaslona se često koriste. Danas zapravo pružaju vid zaštite sigurnosti jer se može postaviti lozinka koju je potrebno unijeti svaki put kad se čuvar zaslona aktivira.

Međutim, unatoč očitoj koristi, postoji i ranjivost koja može omogućiti priliku za napad, kod čuvara zaslona koji se uključuje nakon što je ulazni ekran (login screen) prikazan na ekranu više od 10 minuta. Taj čuvar zaslona, odnosno datoteka SCRNSAVE.EXE može biti zamijenjena malicioznim kodom, malom izvršnom datotekom koja napadaču može omogućiti da promijeni korisnikovu lozinku i dobije pristup računalu.

2.2.5. Automatsko pokretanje (AutoRun i AutoPlay)

Jedan od načina napada na računalo može biti korištenjem opcije automatskog pokretanja izmjenjivih medija, kao CD, USB memorijski uređaj ili drugi prijenosni mediji. Napadač ili maliciozni program može inficirati autorun.inf datoteku na mediju ili umetnuti maliciozni korisnički sadržaj (payload) koji će se izvršiti pomoću opcije automatskog pokretanja, na bilo kojem računalu.

2.2.6. Dijeljenje resursa (File and printer sharing i Simple file sharing)

Dijeljenje datoteka i mapa (File and printer sharing) je usluga koja omogućava računalu da dijeli svoje datoteke i pisač s računalima na mreži. Ako računalo nije spojeno na mrežu, ostavljanje te usluge uključenom zapravo nema nikakve koristi, a može predstavljati još jedan sigurnosni rizik.

Sva računala koja nisu dio neke domene, koriste model mrežnog pristupa nazvan **jednostavno zajedničko korištenje datoteka** (Simple File Sharing). To je još jedna od opcija koje su stvorene da bi što više olakšale stvari korisniku, no isto tako je mnogo manje konfigurabilna i pruža niži nivo sigurnosti od klasičnog dijeljenja datoteka i mapa.

2.2.7. Udaljeni pristup (Remote Desktop i Remote Assistance)

Windows XP (Professional) operacijski sustav ima mogućnost koja se naziva **udaljena radna površina** (Remote Desktop) pomoću koje korisnik može pristupiti svom računalu s udaljene lokacije i imati potpuni pristup sustavu. Ta opcija može biti korisna, no opasnost je vrlo očita. Ako napadač otkrije potrebne podatke o korisničkom računu, može dobiti potpuni pristup svim privatnim podacima, kao da sjedi za računalom. Sigurnosni rizik je evidentan i velik. Nije potrebno vršiti napad na računalo, postavljati stražnja vrata (backdoor) i druge maliciozne programe kojima će u konačnici dobiti pristup računalu, već je dovoljno da na pravi način iskoristi već gotovu uslugu operacijskog sustava koja omogućuje upravo to.

Bitno je napomenuti i uslugu koja se naziva **daljinska podrška** (Remote Assistance), koja u analogiji s prethodnom nosi jednak sigurnosni rizik. To je usluga koja omogućuje korisniku da pozove prijatelja, člana obitelji ili neku drugu osobu da se poveže s računalom putem Interneta da bi otklonila neku grešku ili riješila neki problem. U svakom slučaju, bilo kakav oblik pružanja

daljinskog pristupa računalu otvara mogućnost da računalu pristupe i neki neželjeni gosti i to samo pribavljanjem podataka o korisničkom računu.

2.2.8. Usluge Windows operacijskog sustava (Windows services)

Usluga Windows operacijskog sustava (service) program je koji se izvršava u pozadini. Ti programi uglavnom omogućuju neke funkcionalnosti operacijskog sustava ili procesiraju akcije i zahtjeve drugih programa. Mnoge od tih usluga su nepotrebne ili se rijetko koriste. Generalno gledano, svaka usluga koja nije nužna, koja se ne koristi, zapravo predstavlja priliku napadaču da iskoristi ranjivost u nekoj od njih da dobije pristup računalu. Pored toga, kod nekih su usluga dosada i otkrivene ranjivosti koje su se iskorištavale za napade, a izdane su zakrpe za njih.

2.2.9. Skrivene ekstenzije

Kod Windows XP operacijskih sustava automatski (default) je uključena opcija skrivanja poznatih ekstenzija ili proširenja datoteka. Mnogi napadači koriste taj podatak na način da skrivaju viruse unutar datoteka s dvostrukim ekstenzijama (npr. datoteka.txt.vbs). Budući da u tom slučaju korisnik može vidjeti samo prvu ekstenziju, često pretpostavi da je datoteka sigurna i otvori je, što pokrene virus. Iako je tu zapravo očito da će ekstenzija (prva) biti vidljiva samo ako neka datoteka ima više ekstenzija, dok kod svih ostalih datoteka nikakva ekstenzija nije vidljiva, korisnici ipak nasjednu na takav tip prijevare.

Nadalje, pored skrivanja uobičajenih ekstenzija, postoje još neke datoteke čije ekstenzije operacijski sustav također skriva. To su posebne ekstenzije tipa .pif, .shs, .lnk i druge. Takve ekstenzije se ne mogu otkriti na jednostavan način već je potrebno editiranje registara. Tu činjenicu napadači također koriste pa se takve datoteke isto vrlo često koriste za širenje virusa i drugih vrsta malicioznog koda.

2.2.10. Datoteka sa stranicom memorije (Pagefile)

Također poznata i kao virtualna memorija, ta datoteka je digitalno skladište koje pruža dodatni prostor za pohranu. Ponekad se u toj memoriji mogu naći lozinke, korisnička imena i drugi osjetljivi podaci i tu se mogu zadržati i duže vrijeme. To je naravno sigurnosni rizik jer napadač nakon što uđe u sustav može pristupiti toj datoteci i domoći se tih privatnih podataka.

2.2.11. Ispis memorije (Dump File)

Kad nastane problem koji uzrokuje pad sustava ili aplikacije, Windows XP obično šalje podatke o grešci u „skladište“ koje se naziva ispis memorije (Dump File). Te informacije mogu biti korisne u otkrivanju i otklanjanju smetnji, ali su i problematične jer se tu također pohranjuju i privatne informacije kao lozinke za aplikacije i slično. To se može prikazati kao rudnik za napadače i uljeze s Interneta.

2.2.12. VBScript

Visual Basic skripte su tekstualne datoteke s ekstenzijom .vbs koje sadrže programski kod. Kriminalci vrlo često skrivaju viruse i druge oblike malicioznog koda unutar Visual Basic skripta i pridružuju ih e-mail porukama. Nakon otvaranja privitka e-mail poruke, VBScript kod se pokreće i maliciozni kod inficira računalo.

2.2.13. Aplikacije koje se instaliraju na računalo

Postoje mnogi programi koje dolaze s Windows XP operacijskim sustavom čije su ranjivosti već opće poznate. To su uglavnom programi vezani za Internet usluge. Budući da se o njima detaljno govori u kasnijim poglavljima, zasad je dovoljno samo nabrojati neke od njih, kao primjer. Najpoznatiji su Internet Explorer, Outlook Express, Windows Messenger, IIS (Internet Information Services).

U kasnijim poglavljima se ponovno spominju ove ranjivosti (kao i neke druge), dodatne informacije o njima, te načini eliminiranja sigurnosnih rizika koje nose.

3. ZAŠTITA RAČUNALA

3.1. WEB PREGLEDNICI I SURFANJE INTERNETOM

3.1.1. Sigurno surfanje

U samim počecima, prije World Wide Weba, korisnici su mogli pristupiti Internetu putem komandno-linijskog sučelja. Takav pristup zahtijevao je ponešto znanja i većini običnih ljudi bio je zastrašujući, te je i sam broj korisnika Interneta bio malen.

Web preglednici su promijenili stvar pretvarajući Internet u nešto jednostavno i zanimljivo – svaka osoba je samo klikom miša mogla jednostavno „putovati“ tim novim svijetom. Gotovo preko noći milijuni ljudi postali su svakodnevni korisnici Interneta.

Web preglednik je alat, program pomoću kojeg se obavljaju sve radnje vezane za pretraživanje i pregledavanje Interneta, odnosno World Wide Weba. S obzirom na to, potrebno je obratiti dodatnu pozornost na sve sigurnosne aspekte web preglednika – sve elemente koji se zloupotrebljavaju te time postaju ranjivosti, te isto tako sve mogućnosti koje pridonose sigurnijem surfanju.

3.1.2. Jezici korišteni na web stranicama

Kao temeljni jezik WWW-a, HTML i s njim povezani skriptni jezici su naširoko izrabljivani. Iako čisti HTML virusi nisu pretjerano opasni, postoji mnogo načina na koje se HTML može zloupotrijebiti za manipulaciju računalnim resursima.

HTML (Hypertext Markup Language) je osnovni jezik za kreiranje web stranica. To je opisni jezik kojim se definiraju razni atributi kao font, veličina teksta, boje, slike i sl. Međutim, HTML je statičan. Da bi se omogućilo prilagođavanje sadržaja i interaktivnost, mnoga web mjesta koriste dodatne elemente, kao što su skriptni jezici, ActiveX kontrole i Java apleti. Ti mini programi omogućuju da web stranica komunicira s bazama podataka da bi pružila dodatne funkcionalnosti. No, ako web stranica može izvršiti neki program na računalu da bi prilagodila sadržaj korisniku i učinila ga dinamičnim i aktivnim, isto tako može pokrenuti i neki mini program koji može instalirati neki maliciozni kod na računalu.

Skriptni jezici kao JavaScript i VBScript su najveća prijetnja svakom računalu sa web preglednikom. No, ako ih se isključi, web nerijetko jednostavno ne funkcionira.

JavaScript, osim što može manipulirati prozorom preglednika, može pristupiti lokalnom datotečnom sustavu, modificirati registre, pokretati druge programe i kreirati nove datoteke i procese.

JScript je Microsoftov funkcionalni ekvivalent JavaScriptu.

VBScript (Visual Basic Scripting Edition) je Microsoftov skriptni jezik s korijenima u Visual Basic programskom jeziku. Podržan je samo od strane Microsoftovih preglednika. Ističe se po činjenici da je korišten u najvećem broju malicioznih web objekata.

Java apleti i ActiveX kontrole su također veliki sigurnosni rizici.

Java aplet (Java applet) programi koriste poseban podskup Java programskog jezika prilagođen da se izvršava unutar kompatibilnih web preglednika. Mogu unijeti mnogo interaktivnosti u web stranicu – multimedijalne efekte, animacije, glazbu, interaktivne igre, mogu reagirati na pomake miša i koriste se za kreiranje sofisticiranih web formi.

Sigurnosni rizik predstavlja činjenica da sa Java apleti automatski učitavaju i izvršavaju bez korisnikova eksplicitnog dopuštenja. Aplet se izvršava automatski čim se otvori web stranica na

kojoj se nalazi, nerijetko korisnik nije toga ni svjestan. S obzirom na to, logičan je strah jer jedan maliciozan Java aplet može načiniti veliku štetu, gotovo neprimjetno. Upravo zato je velik trud uložen na stvaranje izvrsnog i kompleksnog sigurnosnog modela za Javu (Java sandbox). No, sama kompleksnost garantira neke propuste. Sigurnost je narušena više puta i čak apleti koji ne narušavaju nijedno pravilo mogu izvršiti DoS napade. Šteta koju maliciozni apleti mogu načiniti varira od dosađivanja korisniku, DoS napada, ograničenog upada u sustav pa do kompletnog kompromitiranja sustava. Sreća je da su najgori oblici napada vrlo rijetki i većinu propusta prvi pronađu stručnjaci i profesionalci, te na vrijeme izdaju zakrpe.

ActiveX je grupa Microsoft programskih alata koji omogućuju da Windows programi rade preko mreža.

ActiveX kontrola je izvršni program koji se može automatski prenijeti preko Interneta i obično se izvršava unutar preglednika. Kontrole mogu biti pisane u velikom broju programskih jezika i mogu se ponovo koristiti unutar kontrola pisanih drugim programskim jezikom, dok Java apleti mogu biti pisani samo Java programskim jezikom. No, ActiveX kontrole se mogu izvršavati samo na sustavima koje koriste Win32 API čime su ograničene u odnosu na portabilnost Jave. A i vezane su za Internet Explorer (ili dodatke za ActiveX potporu za druge preglednike). Ali, ActiveX kontrole su puno moćnije od Java apleta. Mogu manipulirati diskovnim sustavima, uspostavljati veze s računalima i mrežama, prenositi datoteke i još mnogo toga, a sve te radnje su nevidljive korisniku. Mogu raditi bilo što, zapravo. Bilo kakva aktivnost virusa, crva i trojanaca može biti ostvarena pomoću ActiveX kontrola. Sigurnosni model je, u usporedbi sa Javinim modelom vrlo loš. Čitava sigurnost temelji se na digitalnim potpisima i rasuđivanju korisnika. Sve ovisi o tome da li korisnik ili njegov preglednik određeni kod prihvati kao pouzdan ili ne.

Dakle, ActiveX kontrole su mnogo moćnije, destruktivnije i nesigurnije od Java apleta, te stoga i mnogo veći sigurnosni rizik.

3.1.3. Kolačići (cookie)

U osnovi, kolačić (cookie) je obična tekstualna datoteka kakve koriste web poslužitelji da bi pohranili informacije o korisniku i njegovim aktivnostima na nekom web mjestu. Poslužitelj zatim koristi te podatke u raznolike svrhe.

Primarna namjena je prilagođavanje sadržaja korisniku i memoriranje nekih postavki koje je korisnik ranije odabrao. Također se koriste na web mjestima gdje korisnici otvaraju korisničke račune, da bi se olakšalo pristup korisničkim računima (login) i autentifikacija korisnika. Osnovna ideja je olakšavanje i unaprjeđivanje iskustva web surfanja.

Pored samo pohranjivanja nekih osobnih podataka o korisniku, kolačići omogućuju web mjestima da prate i navike korisnika. Koliko često pojedini korisnici posjećuju web mjesto, koliko dugo se zadrže ili koje vrste web mjesta posjećuju, što najviše gledaju, kakve ih stvari najviše zanimaju i sl. Te podatke koriste pri dizajniranju web mjesta koja najbolje odgovaraju potrebama posjetitelja i u prilagođavanju postojećih. Mogu koristiti i za skupljanje informacija koje se koriste za ciljano oglašavanje – reklame koje bi mogle zanimati pojedinog korisnika ili praćenje koji su oglasi pojedinom korisniku već prikazani.

Informacije koje se prikupljaju pomoću kolačića često se unose u razne baze podataka, pomoću kojih se stvaraju profili pojedinaca i njihovih navika surfanja. Namjera možda i jest na mjestu, ali je prilično upitno narušavanje privatnosti koje je tu vrlo očito.

Jedan primjer uporabe kolačića bi bio npr. web mjesto za Internet kupovinu - Amazon.com. Pomoću kolačića pohranjuju podatke o proizvodima koje pojedini korisnik pregledava i u skladu s tim korisniku se nude drugi proizvodi koji bi ga mogli zanimati.

Kolačić može biti trajan (persistent) ili valjan samo za vrijeme tekuće aktivnosti preglednika (session cookies). Kolačići prve strane (first – party cookie) stvaraju web mjesta koja korisnik trenutno posjećuje. Kolačići treće strane (third – party cookie) stvaraju druga web mjesta, ne ona koja trenutno posjećujemo. Tu su obično u pitanju neke oglašivačke organizacije koje imaju reklame postavljene na nekim web mjestima i postavljaju kolačiće preko tih web mjesta. Takvi kolačići su obično oni koji skupljaju podatke o navikama korisnika i prilično su invazivni, veća su prijetnja za privatnost.

Kolačić inače pohranjuje samo malu količinu podataka, obično manje od 1 KB, na lokalni tvrdi disk. Prvi podatak je obično neki identifikacijski broj, zatim naziv kolačića, putanja ili naziv domene za koju vrijedi, datum isteka valjanosti i da li kolačić zahtijeva sigurnu vezu. Kolačić ne može sadržavati maliciozan kod. Ne može pristupiti tvrdom disku ili nekom drugom dijelu računala niti narušiti sigurnost. Kolačić u osnovi ne predstavlja neki veliki sigurnosni rizik nijednom računalu, osim narušavanja privatnosti.

No ipak, postojali su primjeri zlouporabe kolačića. Poznata američka banka *Bank One Online* koristila je kolačiće za pohranu korisnikova broja kartice i PIN-a. Informacije u kolačiću se prilikom uporabe šifrirane šalju web mjestu banke. Problem je što su na računalu korisnika podaci pohranjeni kao običan tekst, a s obzirom na preko šesto tisuća klijenata, mnogi od tih kolačića su pohranjeni na nezaštićenim računalima.

Drugi primjer zlouporabe je otimanje kolačića (cookie hijacking). U pravilu kolačiću se može pristupiti samo od strane domena od kojih su stvoreni. Nekoliko je slučajeva poznato u kojima su web mjesta mogla pristupiti svim kolačićima na računalu. Dovoljno je bilo znati naziv kolačića i dodati tri točkice nazivu domene u zahtjevu, koje bi zbunile preglednik. Npr. http://www.primjer.com.../getcookie.cgi

Ako bi podacima u kolačićima mogla pristupiti neka zlonamjerna osoba mogla bi ih iskoristiti za imitiranje korisnika. Stvoriti kopiju, imitaciju originalnog kolačića i pristupiti nekom web mjestu predstavljajući se kao netko drugi. Opasnost je najočitija kod kolačića koji omogućuju automatski pristup korisničkom računu. Ako dođe do otimanja kolačića, napadač može bez problema pristupiti korisničkom računu samo posjetom konkretnog web mjesta.

Postojao je propust u IIS-u (Internet Information Services) koji je omogućavao otimanje kolačića, čak i kod sigurnih SSL sjednica. Microsoft je objavio zakrpe kako bi minimizirao štetu.

Većina preglednika danas omogućava potpuno ili djelomično blokiranje kolačića. Ipak, potpuno blokiranje kolačića će onemogućiti normalno surfanje jer neka web mjesta jednostavno neće raditi bez njih, ali određena razina konfigurabilnosti ipak postoji.

Ovisno o tome koji se preglednik koristi, određene mogućnosti manipuliranja kolačićima su dostupne. Od blokiranja svih kolačića, blokiranja samo kolačića treće strane (third – party) pa do blokiranja ili prihvaćanja kolačića samo pojedinih web mjesta. Isto tako može biti dostupna i opcija pri kojoj korisnik osobno odobrava svaki pojedini kolačić. Iako je takvo nešto iznimno naporno, odličan je uvid u to koliko zapravo kolačića biva postavljano na računalo, a da korisnik toga nije ni svjestan.

Pored opcija koje nam nude preglednici, postoje i razni alati koji služe za rad s kolačićima treće strane. Takvi alati, kao npr. Cookie Pal, Cookie Crusher ili MagicCookie Monster nude mnogo više fleksibilnosti i mogućnosti manipuliranja kolačićima. Od jednostavnog definiranja web mjesta kojima se dozvoljava postavljanje kolačića, do mogućnosti čitanja i brisanja kolačića na računalu. Isto tako se mogu prihvaćati ili blokirati pojedini kolačići, za vrijeme samog surfanja. Mnogi vatrozidi i programi za detekciju špijunskog koda (anti-spyware) nude mogućnost selektivnog blokiranja kolačića kao i brisanje već postavljenih.

3.1.4. Kupovina putem Interneta: SSL i certifikati

Kupovina putem Interneta je vrlo sklizak teren. Pored svih prednosti koje pruža razgledanje i kupnja iz udobnosti vlastitog doma, takav pristup krije mnoge rizike. Mnogi su rizici, a i mnoge metode barem pokušaja zaštite takvih oblika transakcija.

Kod kupnje u običnoj trgovini, situacija je relativno jednostavna. Očito je da osoba tad posluje s upravo onom trgovinom u kojoj se nalazi. A kod kupnje kreditnom karticom, trgovac obično zatraži neki oblik isprave kako bi potvrdio da je kupac ona osoba za koju se izdaje. I sve je više manje jasno.

Kod kupovine putem Internet korisnik ne može biti siguran da je web mjesto na kojem se nalazi uistinu pravo web mjesto tvrtke s kojom želi poslovati. Budući da danas svatko može zakupiti domenu i postaviti web mjesto, a i zato što napadači ponekad mogu presresti ili preusmjeriti pokušaj povezivanja s nekim web mjestom, mora postojati neki način dokazivanja da je web mjesto legitimno. To se obično radi korištenjem digitalnih certifikata izdanih od neke pouzdane treće strane. Kad osoba želi pribaviti digitalni certifikat od tvrtki kao VeriSign ili Thawte, certifikat se ne izdaje dok osoba ne pruži valjan dokaz svog identiteta.

Takve tvrtke ipak temelje svoje poslovanje na respektabilnosti svoje „riječi“, odnosno certifikata koji izdaju, te stoga nepobitno moraju potvrditi identitet osobe koja ga traži. Korisnik može biti sumnjičav da li je neko web mjesto legitimno, ali prihvaća „riječ“ tih trećih stranki kad prihvati certifikat.

Glavni web preglednici danas imaju mogućnost korištenja SSL-a (Secure Socket Layer). SSL je protokol koji pruža način dokazivanja autentičnosti web poslužitelja, te šifrira podatke koji se prenose između preglednika i poslužitelja i pored toga provjerava promet da bi osigurao da podaci nisu modificirani na neki način.

SSL u kombinaciji sa HTTPS-om (Secure Hypertext Transfer Protocol*)* pruža najpopularniji oblik šifriranja veze, sjednice (session). HTTPS obično radi preko TCP/IP priključne točke 443, za razliku od uobičajenog HTTP protokola koji radi preko priključne točke 80. URL (Uniform Resource Locator) nekog HTTPS web mjesta obično započinje s https:// umjesto http://. SSL koristi digitalne certifikate za autentikaciju i šifriranje jedne ili obje strane sigurne veze.

Prilikom posjete sigurnom web mjestu, HTTPS zatraži certifikat. Poslužitelj tad predoči certifikat, a preglednik ga procjenjuje. Ako web poslužitelj ima valjan digitalni certifikat, web preglednik će automatski uspostaviti vezu pomoću SSL-a. Ako je veza osigurana SSL-om, unutar prozora preglednika se obično negdje nalazi sličica zaključanog lokota (gdje, ovisi o pregledniku koji se koristi).

Ako poslužitelj nema digitalni certifikat, web preglednik će uspostaviti običnu vezu, vezu koja nije sigurna. No, ako web preglednik ima certifikat koji je istekao ili nije valjan; ako je certifikat izdan od izvora koji nije u pregledniku definiran kao pouzdan ili ako certifikat nije vezan na isti poslužitelj s kojim je preglednik u tom trenutku spojen, obično se prikaže neka vrsta obavijesti ili upozorenja i korisnik treba sam izabrati da li će prihvatiti taj certifikat ili ne. U takvim slučajevima uputno je dobro razmisliti o tome da li je tvrtka koja je vlasnik web mjesta respektabilna i da li je to uistinu ispravan poslužitelj, a ne podvala odnosno maliciozna kopija. Certifikat ne bi trebalo prihvatiti ako korisnik nije potpuno siguran u valjanost certifikata i legitimnost web mjesta.

SSL je odobren kao standard za preglednike od strane organizacije W3C (World Wide Web Consortium) i koristi ga većina komercijalnih web mjesta. Može se koristiti za osiguravanje bilo kojeg TCP/IP protokola, ali obično se koristi za šifriranje HTTP prometa. Postoje različite verzije SSL-a uključujući SSL 2.0 i SSL 3.0. Microsoft je kreirao sigurni protokol nazvan PCT 1.0 (Private Communications Technology) da bi pružio bolju sigurnost od SSL 2.0. No, nije

korišten ni približno koliko SSL. TLS (Transport Layer Security) je još jedan sigurni protokol, po nekima nazvan SSL 3.1 i može biti postavljen kao metoda zaštite, po izboru. Većina preglednika podržava SSL i ako je odabir više sigurnosnih protokola dozvoljen, dobro ih je sve uključiti i koristiti s odgovarajućim web mjestima.

SSL protokol koristi kombinaciju asimetrične kriptografije ili kriptografije javnog ključa (public key cryptography), jednosmjernog raspršivanja (hashing) i simetrične kriptografije da bi omogućio sigurnu komunikaciju uključenih strana. Komponente tog procesa koje uključuju tehnike raspršivanja (hash) i javne – privatne ključeve koriste se za autentifikaciju poslužitelja i stvaranje i šifriranje ključa koji se koristi za ostatak komunikacije. Nakon što su ti koraci završeni, sam prijenos podataka šifrira se simetrično jer je simetrično šifriranje dosta brže od asimetričnog. Svaka veza odnosno sjednica (session) koristi novi ključ, a sam ključ se šifrira asimetrično, da bi se sigurno dostavio drugoj strani.

Kriptografija javnog ključa (public key cryptography) koristi dva povezana ključa za sigurnu komunikaciju. Kod takvog oblika šifriranja, izvorišna strana generira dva ključa – privatni i javni. Samo izvorišna strana poznaje i drži glavni, privatni ključ. Svi ostali sudionici mogu imati javni ključ. Samo korisnik (korisnici) s privatnim ključem mogu kreirati šifriranu poruku, koja se može dešifrirati samo odgovarajućim javnim ključem. Iako je javni ključ upravo to – javan, budući da je poruku mogla šifrirati samo ona strana koja ima privatni ključ, to je garancija da je poruka stigla od očekivane strane. Javnim ključem se može šifrirati poruka koju zatim može dešifrirati samo strana koja posjeduje pravi privatni ključ. Službeni naziv takvog tipa kriptografije je asimetrična kriptografija.

Simetrična kriptografija je jednostavnija i brža. Koristi samo jedan ključ kojim se poruke i šifriraju i dešifriraju. Problem takvog pristupa je da čitava sigurnost leži u tajnosti tog jednog ključa. Prva opasnost leži u samoj distribuciji ključa. Strana koja generira ključ treba taj ključ na neki način sigurno dostaviti drugoj strani. Nakon razmjene ključa, njegova tajnost treba biti osigurana tijekom čitave komunikacije, da bi podaci koji se razmjenjuju ostali tajni.

Zbog svega navedenog, obično se koristi kombinacija ta dva pristupa. Sama komunikacija se radi brzine odvija pomoću simetričnog šifriranja, a asimetrično se koristi za sigurnu razmjenu ključa. Nakon toga, sva sigurnost je usmjerena na očuvanje tajnosti simetričnog ključa.

No, potreban je oprez čak i kod naizgled sigurnih SSL veza, upravo zato što se SSL oslanja na ključeve. Šifriranje podataka koji putuju od poslužitelja do preglednika, kao što je već rečeno, obavlja se pomoću privatnog ključa (ključa simetrične kriptografije). Mnogi web poslužitelji pohranjuju svoje privatne ključeve na području kojem mogu pristupiti i napadači. Ako napadač pribavi privatne ključeve poslužitelja, može stvoriti kopiju web mjesta (spoofing), a korisnik ne bi mogao uočiti razliku jer se digitalni certifikat podudara. Napadač bi u tom slučaju mogao i dešifrirati sve podatke koji se izmjenjuju u toj vezi.

Još je jednu mogućnost potrebno razmotriti. Mogućnost da neko maliciozno web mjesto također može imati valjan certifikat od pouzdane treće strane. Web preglednik tada uspostavlja SSL vezu i zaključani lokot je prikazan, no to zapravo samo govori da je uspostavljena sigurna SSL veza s tim poslužiteljem i da su podaci koji se razmjenjuju šifrirani. To, na kraju krajeva zapravo ništa ne govori o tome da li je poslužitelj s kojim komuniciramo siguran, pa je ipak potrebno imati dozu opreza i biti siguran da li se zna s kim se zapravo uspostavlja veza.

3.1.5. Financijske transakcije

U današnjim vremenima, osim kupovine preko Interneta, većina financijskih transakcija može se obaviti uz samo nekoliko klikova mišem. Uvid u bankovne račune moguć je u bilo koje doba dana. Prebacivanje sredstava s jednog računa na drugi; kupovanje i prodavanje dionica. Investicijske organizacije posluju preko Interneta. Plaćanje računa je moguće čak i ako tvrtka s

kojom se posluje nije dostupna preko Interneta – mnoge banke danas omogućuju da se računi drugim tvrtkama plaćaju direktno s web mjesta banke.

Sve te usluge pružaju veliki komfor. Pored toga naravno skrivaju i mnoge opasnosti, rizike koje obično uključuju velike financijske gubitke. Riječ je o novcu, o financijskim i osobnim podacima. Svaki oblik narušavanja sigurnosti može rezultirati velikom štetom. Potrebna je velika količina opreza i određene mjere predostrožnosti da bi se što više smanjila mogućnost katastrofe.

Mjere i rizici su gotovo isti kao i kod Internet kupovine. Korisnik mora biti siguran da je web mjesto koje posjećuje valjano i sigurno. Trebalo bi imati valjan digitalni certifikat izdan od pouzdane organizacije. Također treba obratiti pozornost na sličicu zaključanog lokota koji indicira sigurnu komunikaciju prije bilo kakve transakcije. SSL veza i digitalni certifikati su način na koji se može znati da je komunikacija sigurna i da osoba razmjenjuje podatke s pravim poslužiteljem. Većina takvih web mjesta koriste kombinaciju korisničkog imena i lozinke za autentifikaciju korisnika. Korisničko ime i lozinka su načini dokazivanja da osoba koja pristupa korisničkom računu uistinu ima pravo pristupa. Zato je važno odabrati dobru, snažnu lozinku i čuvati korisničko ime na sigurnom. Isto tako najbolje bi bilo koristiti različita korisnička imena i lozinke za svaki račun da bi u slučaju kompromitiranja informacija s jednog web mjesta, ostali računi ostali zaštićeni.

Još jedan ozbiljan problem kad je riječ o financijskim web mjestima je i dramatičan porast neovlaštenog traženja informacija (phishing). Kao što je ranije spomenuto, vrlo je važno imati na umu činjenicu da nijedna iole respektabilna tvrtka ne bi tražila korisničko ime, lozinku, broj kartice ili bilo koji drugi povjerljivi podatak putem e-maila. Isto tako, nikada se ne bi trebalo kliknuti na poveznicu (link) unutar elektroničke poruke da bi se posjetilo neko financijsko web mjesto.

3.1.6. Filtriranje sadržaja (content filtering)

World Wide Web je vrijedan izvor sadržaja koji mogu biti korisni, obrazovni, zabavni i sl. Sadrži i mnogo web stranica upitnog sadržaja. Pornografske stranice, stranice koje nameću nasilje ili mržnju u nekom obliku i zlonamjerne stranice koje pokušavaju inficirati računalo virusom ili kompromitirati sigurnost instalacijom trojanskog konja ili neke druge vrste malicioznog koda.

Posjećivanjem samo poznatih i etabliranih web mjesta može se biti relativno siguran da se neće naletjeti na neki sumnjivi ili maliciozni sadržaj. Ali već kod korištenja tražilica kao što su Google ili Yahoo nema garancije da će rezultati neke pretrage biti samo „dobre“ stranice. Za djecu postoji mnogo veći rizik da slučajno nalete na neki od tih „loših“ stranica. Za web mjesta koja djeca posjećuju, kao stranice s igricama ili glazbom veće su mogućnosti da mogu odvesti korisnika do nekog štetnog sadržaja.

Poglavito kad su djeca u pitanju, a i u drugim situacijama, postoje sredstva pomoću kojih se mogu blokirati takva web mjesta na način da ih preglednik uopće neće prikazati. Dostupan je čitav niz aplikacija koje filtriraju web sadržaj prije nego se prikaže u prozoru preglednika.

Osim samog filtriranja sadržaja nude i razne druge opcije „roditeljske kontrole“ kao nadzor aktivnosti, vremensko ograničavanje, ograničavanje obavijesnih skupina (newsgroup) i razgovora (chat), filtriranje elektroničke pošte i slično.

Najpoznatiji takvi alati su NetNanny, CyberSitter, CyberPatrol i slični. Pored komercijalnih, postoje i besplatni kao K9, Naomi, We-blocker i sl.

Filtriranje sadržaja uglavnom funkcionira na dva načina. Neki alati održavaju bazu podataka web mjesta za koje je poznato da ulaze u jednu od kategorija koje bi bilo dobro blokirati. Oni zatim

blokiraju pristup bilo kojem web mjestu koje se nalazi u bazi podataka – ovisno o načinu na koji je filtar sadržaja konfiguriran.

Druga metoda je procjena sadržaja u realnom vremenu i potraga za ključnim riječima i frazama ili nekim drugim elementima koji naznačuju nepodoban sadržaj.

Neki proizvodi koriste i kombinaciju tih dviju metoda.

3.1.7. Savjetnici (Site Advisor)

Kao dodatak sigurnosti pri surfanju, postoji alat koji, kao što mu samo ime kaže – savjetuje. Site Advisor (SA) je program koji pomaže korisniku procijeniti sigurnost nekog web mjesta prije nego mu pristupi. Razvio ga je istraživački tim sveučilišta MIT, a nedavno ga je kupila tvrtka McAfee Inc.

Site Advisor je kompatibilan s Internet Explorer i Mozilla Firefox web preglednicima. Radi na način da npr. prilikom neke Google pretrage pokraj svakog rezultata pretrage prikazuje malu ikonicu i prelaskom miša preko ikonice prikaže se preporuka za konkretno web mjesto. Za rangiranje koristi se princip boja gdje crvena označuje ozbiljne probleme i preporuku da se izbjegava konkretno web mjesto; žuta znači da se preporučuje oprez, da možda postoji opasnost, a zelena označava da je web mjesto dokazano sigurno.

Može se preuzeti s web stranice http://www.siteadvisor.com/download/ie2.html.

SA nudi samo preporuku za konačnu odluku, no korisnik je taj koji odlučuje da li će preporuku slijediti ili ne, tako da nema ograničenja. Isto tako, web mjesto Site Advisora nudi opciju Internetske provjere pojedinog web mjesta, dakle bez potrebe za instalacijom samog programa. Unošenjem potrebnih podataka o domeni na predviđeno mjesto (dostupno na svakoj stranici tog web mjesta), prikazuju se informacije o pojedinom web mjestu.

Postoje i drugi sustavi za procjenu sigurnosti web mjesta. Većina ih je usmjerena na određene vrste zaštite ili određene vrste web mjesta. Na primjer, sustav za procjenu sigurnosti koji pruža SafeSurf uglavnom je usmjeren na sigurnost djece i procjenu web mjesta prema tome koliko su sigurni za djecu. Tvrtka buySAFE nudi alat Shopping Advisor, dodatak za web preglednike koji prikazuje procjenu sigurnosti za web mjesta koja nude usluge prodaje putem Interneta (e-commerce).

3.1.8. Privatnost i anonimnost na Internetu

Prilikom surfanja webom, svaki korisnik neprimjetno ostavlja digitalni trag, a informacije cure na sve strane. Osobne informacije ne mogu se sakriti. Napravljen je kompromis u kojem su privatnost i anonimnost zamijenjene za sigurnost i komfor. Bez obzira na to, nekim ljudima je njihova privatnost veoma bitna. Na kraju krajeva, svaki bi korisnik trebao imati pravo sam izabrati kojim organizacijama i pojedincima želi dati vlastite podatke na raspolaganje.

Nažalost, to je danas rijetko slučaj. Osim što gotovo svatko može saznati ponešto o drugome bez velikog truda, te se informacije često i zloupotrebljavaju. Web mjesta sakupljaju podatke o korisnicima na razne načine. Osnovna sredstva kojim se koriste su generalne informacije koje dobiju od preglednika, podaci koje korisnici unose u forme, tehnike praćenja i kolačići (cookie).

Web preglednici šalju određenu količinu predefiniranih informacija web poslužiteljima prilikom pristupanja nekom web mjestu. Tip preglednika, verziju, operacijski sustav koji se koristi, IP adresu, ISP, pohranjene kolačiće i slično.Web mjesta često traže od korisnika da unese neke osobne informacije u HTML forme. Bilo koja informacija unesena i predana web mjestu može biti pohranjena, korištena i prodana, stoga je potrebno biti oprezan.

Novi trend u prikupljanju informacija o korisnicima uključuje kod unutar web stranice koji, dok je aktivan u memoriji, može pratiti tijek surfanja korisnika. Pravila World Wide Weba dopuštaju web mjestima da doznaju odakle su korisnici došli (kojim putem) do tog web mjesta (referring site) i isto tako koje su mjesto sljedeće posjetili. Ta druga mogućnost je ona koja nosi veću opasnost od iskorištavanja. Također se često koriste i već spomenuti kolačići.

Informacije prikupljene na bilo koji od tih načina mogu biti pohranjene u baze podataka, korištene interno ili čak prodane nekim trećim kompanijama. Čak i podaci kao osobne informacije ili broj kreditne kartice unesen u web formu može biti legalno prodan bilo kakvoj kompaniji, čak i pornografskim web mjestima ili spamerima. Pored toga, ponekad je dovoljno da napadač dozna IP adresu korisnika i koji tip preglednika koristi, da to iskoristi za napad. Isto tako, bilo kakve informacije koje su kopirane i ostale pohranjene u međuspremniku (Clipboard) mogu vrlo lako biti dostupne napadačima.

Dakle, samim bezopasnim surfanjem, bez ikakvih drugih radnji, otkrivamo dovoljno informacija o sebi koje mogu biti iskorištene na razne načine. Stoga je potrebno biti veoma oprezan i sačuvati sve što se sačuvati da.

Postoje razne mjere opreza kojih se korisnici mogu pridržavati da bi se zaštitili, pored već spominjanih kao što su sigurne lozinke i dobro čuvana korisnička imena, SSL i slično.

Na svakom web mjestu koje traži registraciju ili unos osobnih podataka, dobro je potražiti tekst o politici privatnosti (privacy policy). Ako je tekst lako pronaći i razumjeti, velika je vjerojatnost da je vjerodostojan. Poveznica na politiku privatnosti trebala bi biti lako uočljiva i vidljiva već na početnoj stranici. Tekst bi jasno trebao govoriti točno kakve informacije se prikupljaju, za što će biti korištene i da li će biti dijeljene s bilo kim drugim. Također bi trebala postojati opcija da korisnik može ograničiti dijeljenje ili prodaju informacija ako želi.
Ako web mjesto nema politiku privatnosti ili ju je teško pronaći i razumjeti, to web mjesto bi trebalo smatrati sumnjivim.

Web mjesta koja traže osobne podatke također bi trebala imati i pečat privatnosti (privacy seal). To je jedan novitet koji bi trebao dodatno omogućiti korisniku povjerenje u to da je web mjesto legitimno i može mu se vjerovati. Pečat bi trebao biti potvrda da se web mjesto pridržava objavljene politike privatnosti. Također osigurava i mehanizam za obradu pritužbi potrošača koji smatraju da je njihova privatnost narušena. Dvije organizacije koje izdaju takve pečate su TRUSTe i BBB Online. Te organizacije provjeravaju web mjesta i kontroliraju njihovu primjenu politike privatnosti, te rješavaju sporove.

Slika 3.1. - Pečati privatnosti organizacija BBB OnLine i TRUSTe

Postoji još načina na koji korisnici mogu zaštiti svoji privatnost. Neki od njih su npr. korištenje usluga za anonimno surfanje ili anonimnih poslužitelja opunomoćenika (proxy server), ili korištenje tzv. posrednika. Usluge za anonimno surfanje (anonymizer) rade na način da potpuno prikrivaju korisnikov identitet i to na način da blokiraju pristup korisnikovom računalu, pa web mjesta ne mogu postaviti kolačiće (cookie), detektirati tip preglednika ili identificirati IP adresu. To su korisni alati za zaštitu identiteta, ali usluga ide u oba smjera pa tako mogu štititi i identitet kriminalaca.

Druga vrsta alata za zaštitu privatnosti su posrednici (intermediary odnosno infomediary). Oni „pregovaraju“ u ime korisnika ili potrošača o količini osobnih podataka koji će biti dostupni bilo kojem web mjestu.

Korištenje anonimnih poslužitelja opunomoćenika (proxy) štiti privatnost korisnika skrivajući sve osobne i ostale podatke od web mjesta. Anonimni poslužitelj opunomoćenik stoji između korisnika i web mjesta koja posjećuje. Umjesto pristupanja web mjestu direktno, preglednik komunicira s poslužiteljem opunomoćenikom (proxy) i govori mu koje web mjesto korisnik želi posjetiti. Na taj način web mjesto „vidi“ taj poslužitelj, a ne korisnikovo računalo. Ne može vidjeti kolačić, saznati IP adresu korisnika, vidjeti listu posjećenih stranica, pregledati međuspremnik i sl. Ne može „ispitati“ korisnikov sustav jer zapravo korisnikovo računalo nikad nije u direktnom kontaktu s web mjestom. Surfanje je doista anonimno, bez tragova.

Trenutno najpoznatije tvrtke koje nude usluge anonimnog surfanja su IDZap.com (http://www.idzap.com) i Anonymizer.com (http://www.anonymizer.com). Obje nude dvije razine usluge – besplatni, osnovni nivo i premium pretplatu. Osnovna ograničenja besplatne usluge su te da nema potpore za HTTPS, dakle nema sigurnih veza, samo obični HTTP; te činjenica da iako web mjesta ne mogu saznati identitet korisnika, njegov ISP (pružatelj Internet usluga) ili čak, ako osoba koristi tvrtkin poslužitelj opunomoćenik (proxy) i administrator može pratiti sve stranice koje su posjećene.

Korištenjem premium usluge i sigurnost i anonimnost je potpuna, nitko ne može vidjeti što korisnik radi jer je i sama veza korisnika sa anonimnim poslužiteljem sigurna, pomoću SSL-a. Dakle, komunikacija korisnika sa poslužiteljem je sigurna i šifrirana, a isto tako i tražene stranice koje poslužitelj dostavlja korisnikovom pregledniku putuju od poslužitelja opunomoćenika u šifriranom obliku.

Još jedan primjer je i Freedom WebSecure (http://www.zeroknowledge.com), program jedne kanadske tvrtke (Zero-Knowledge Systems) koji radi na sličan način, ali koristi jače šifriranje. Korisnik se povezuje na njihov poslužitelj, koji zatim preusmjerava korisnika na željeno web mjesto. No, za razliku od prethodnih, ova usluga zapravo korisniku pruža neki pseudonim (alias), odnosno drugi identitet, te korisnik zapravo kruži Internetom pod nekim drugim imenom. Zapravo, omogućava korisniku da specificira do pet pseudonima i profila. Ali, ako web mjesto i pokuša ući u trag korisniku, trag će dovesti samo do Zero-Knowledge Systems poslužitelja.

I razni drugi anonimni poslužitelji opunomoćenici dostupni su na Internetu. Postoji i mnoštvo besplatnih, no problem kod mnogih je što su često nedostupni (offline) ili su vrlo spori. Za pronalazak najboljeg, najjednostavnije je posjetiti web mjesto http://www.atomintersoft.com/products/alive-proxy/proxy-list na kojem je dostupna lista anonimnih poslužitelja opunomoćenika s dodatnim informacijama o svakom, uključujući prosječno vrijeme odziva, aktivno vrijeme rada (uptime) i vrijeme kad je poslužitelj zadnji put provjeravan. Nakon odabira poslužitelja s najvećim postotkom aktivnog vremena, potrebno je njegovu IP adresu i priključnu točku koji koristi unijeti u postavke web preglednika i konfigurirati sve potrebno, da bi anonimno surfanje bilo moguće.

Još jedna mogućnost je korištenje aplikacije koja sama automatski konfigurira preglednik da koristi poslužitelj opunomoćenik, i sama pronalazi najbrži. Na primjer, program GhostSurf (http://www.tenebril.com/products/ghostsurf) koristi višestruke anonimne poslužitelje opunomoćenike i uvijek traži najbržeg. Inače je komercijalan alat, ali se može preuzeti besplatno na probno razdoblje od 15 dana (trial).

Kao primjer jedne posredničke usluge (infomediary) mogu se navesti mogućnosti koje nudi Lumeria. To je usluga koji se temelji na ideji da, ako su osobne informacije tako vrijedne kompanijama, trebali bi biti spremni platiti za njih. Korisnik može stupiti u kontakt s Lumeriom i predati osobni profil (http://www.superprofile.com), uključujući osobne interese. Oglašivači

šalju reklame i oglase Lumerii. Ako je korisnik zainteresiran za npr. kozmetiku, Lumeria prosljeđuje korisniku oglase vezane za to područje. Na taj način korisnik ostaje anoniman, nepoznat oglašivačima, a oglašivači ipak dobiju što su tražili. Osim što sam kontrolira tko dobiva te osobne podatke, teoretski može usput nešto i zaraditi.

3.1.9. Web preglednici

Web preglednik je aplikacija koja traži, postavlja zahtjev (request) za web stranicama i informacijama od HTTP poslužitelja i zatim interpretira i prikazuje rezultate. Podaci koje poslužitelj vraća sadrže kodove za prikaz (opisnike, tagove), slike, grafike, skriptni kod, audio datoteke i sve ostale podržane oblike web sadržaja.

Preglednik radi na način da traži podatke od web poslužitelja, a komunikacija je obično inicirana korisnikovim upisivanjem web adrese (URL – Uniform Resource Locator) u adresnu traku. Uspostavlja se TCP/IP veza, obično preko priključne točke 80 koja je inače dodijeljena HTTP protokolu. Web poslužitelj prihvaća vezu. Klijentov preglednik šalje GET zahtjev, koji indicira poslužitelju da pošalje podatke. Odgovor uključuje niz ASCII znakova, koji slijede pravila HTML formatiranja. Nakon što je odgovor poslan, poslužitelj prekida vezu. Svaki naknadni zahtjev za dodatnim informacijama smatra se neovisnim od ostalih.

Danas najpoznatiji i najviše korišteni web preglednici su Internet Explorer, Mozilla Firefox i Opera.

Svaki preglednik sadrži mogućnosti konfiguriranja postavki rada, prikaza i sigurnosti. Opcije za konfiguriranje sigurnosti, kao i svega ostalog, razlikuju se kod svih preglednika, kao i kod različitih verzija pojedinog preglednika. Nove verzije preglednika izlaze često, a obično uključuju ojačanje sigurnosti, brže surfanje i lakšu uporabu.

Web preglednik je zapravo prevodioc (interpreter). Svaki pojedini preglednik barata primljenim podacima na način na koji je programiran. Činjenica je da nijedna dva preglednika neće neku web stranicu prikazati na identičan način.

Međutim, činjenica je da većina korisnika ne poznaje definicije i stručnu terminologiju, niti se zamara time. Najveći postotak ljudi svakodnevno koristi Internet, ali ih ne zanima što je to sve zapravo, niti način na koji to sve funkcionira. Neki čak nisu ni čuli za pojam preglednika, iako svakodnevno koriste programe poput Internet Explorera ili Mozilla Firefoxa. Ipak, za većinu korisnika web preglednik je jednostavno „program za surfanje“, ili kako mu samo ime kaže, pregledavanje weba, odnosno web stranica.

No, web preglednik ne služi samo za pregledavanje web stranica; koristi se i za pokretanje ugrađenih aplikacija, provjeru e-maila, pregledavanje obavijesnih skupina (newsgroup), preuzimanje sadržaja, gledanje videa, slušanje glazbe i mnoge druge radnje. Zapravo, web preglednici postaju sve sofisticiraniji alati, koji služe za mnogo više osim prikazivanja HTML koda.

Više mogućnosti nosi sa sobom i više problema. Preglednici su postali najveći rizik za sigurnost i privatnost na Internetu. Pored već spomenutih informacija koje svako web mjesto može izvući iz web preglednika korisnika koji mu pristupa, koje i same po sebi mogu uzrokovati dovoljno štete, još je mnogo drugih podataka koje odaju tragove o aktivnostima svakog korisnika.

Sve što se radi i vidi putem web preglednika je ostaje negdje pohranjeno, i na kraju i praćeno i pregledavano. Preglednik bilježi podatke o svakoj posjećenoj web stranici, svakoj slici, videu, glazbenim datotekama i ostalom sadržaju koji korisnik pregleda, podatke o korisničkim imenima i lozinkama, preuzetim datotekama i unesenim pojmovima za pretragu. Sve te informacije su zabilježene i spremljene, osim ako korisnik ne konfigurira preglednik na način da te podatke odbacuje.

Određena količina informacija ostaje pohranjena u već dosta spominjanim kolačićima (cookie). Potrebno je konfigurirati način na koji preglednik postupa s kolačićima tako da dopušta samo one najnužnije, kako bi se što više smanjili rizici koje nose.

Web preglednici čuvaju zapis o svakom posjećenom web mjestu. Popis posjećenih web mjesta čuva se u datoteci history (povijest, prošlost). U bilo kojem trenutku se u pregledniku može vidjeti popis svih prethodno posjećenih web mjesta u određenom periodu, ovisno o postavkama preglednika. To može biti korisno u mnogim situacijama, ali isto tako, bilježenje svih aktivnosti otvara mogućnost napadačima da dobiju uvid u korisnikove aktivnosti i možda čak i neke povjerljive informacije o korisničkim računima. Potrebno je optimalno odrediti period čuvanja zapisa i redovno brisati zapise o povijesti.

Također se čuva povijest otipkanih adresa, pretraživanih pojmova, posjećenih poveznica i prijenosa datoteka. Pohranjivanje otipkanih adresa i pojmova pretraga također se koristi za automatsko popunjavanje prilikom upisivanja. Iako korisna, takva opcija također može na neki način ugrožavati sigurnost i privatnost korisnika.

Većina modernih preglednika koriste lokalnu pričuvnu memoriju (cache) za poboljšanje performansi. Sve stranice i njihove komponente (slike, multimedijalni sadržaji i sl.) privremeno su pohranjeni na tvrdom disku. U slučaju da određena stranica ponovno zatreba, sadržaj se vrlo brzo učita iz memorije, bez potrebe za ponovnim preuzimanjem s poslužitelja.

Preglednici omogućavaju samo određenu razinu manipuliranja postavkama pričuvne memorije. Moguće je odrediti količinu memorije koja će biti odvojena za pohranu web sadržaja i postavke osvježavanja pohranjenih podataka, te mogućnost brisanja čitavog sadržaja pričuvne memorije.

Zabrinutost izaziva i mogućnost malicioznog koda da pristupi sadržaju spremljenom u pričuvnoj memoriji i zloupotrijebi nađene podatke. Dobri preglednici ulažu veliki trud u prevenciji manipulacije pričuvnom memorijom. Ugrađene sigurnosne mjere pokušavaju spriječiti mogućnost pogađanja ili otkrivanja lokacije tih privremenih datoteka. Sposobnost programa, odnosno koda da otkrije ili pogodi lokaciju pohranjenog sadržaja može u potpunosti kompromitirati neko računalo.

Mnogi preglednici u pričuvnu memoriju pohranjuju čak i lozinke. Pri svakom unošenju korisničkog imena i lozinke, preglednik nudi opciju pohranjivanja tih podataka, nakon čega ih može automatski sam unijeti pri svakom posjetu tog web mjesta. Ta opcija služi kao olakšavanje, ali značajno narušava sigurnost preglednika. Svaka osoba s pristupom računalu i pregledniku može iskoristiti te podatke za pristup zaštićenim web mjestima. Jedina mogućnost koju preglednici nude vezana za pohranu tih podataka je uključivanje ili isključivanje te opcije.

3.1.10. Internet Explorer

Kao program koji je uključen u instalaciju svakog Windows operacijskog sustava, Internet Explorer je najpopularniji web preglednik u upotrebi. No, kao najšire korišten preglednik, također je postao i glavna meta napadačima. Unatoč popularnosti, često je kritiziran u proteklim godinama zbog brojnih propusta koji su otkriveni. Microsoft je uvijek brz u izdavanju zakrpa za sve otkrivene mane, ali se Internet Explorer i dalje spominje kao loš, nesiguran preglednik sa mnoštvom propusta i sigurnosnih rizika. Nameće se logično pitanje – da li to mišljenje proizlazi iz stvarne manjkavosti tog preglednika ili pak iz mogućnosti da upravo zato što je najšire korišten, najviše se i proučava i analizira? Realna je mogućnost da Internet Explorer nije toliko lošiji, već da ostali preglednici nisu toliko korišteni, pa svi njihovi propusti nisu zapravo još otkriveni. Bez obzira na to, ostaje činjenica da su sigurnosni propusti Internet Explorera vrlo često eksploatirani, iskorišteni za razne napade, te je stoga svakako nesigurniji od ostalih.

Najveći sigurnosni rizik predstavlja podrška za sve glavne skriptne jezike, interaktivne komponente kao što su AciveX kontrole i vlastiti JVM (Java Virtual Machine). Sve te naizgled korisne mogućnosti često su postajale oružje za zlonamjerne napadače koji ciljaju na Windows sustave.

Pored toga, nije posve korisnički nastrojen. Prilično je neorganiziran i opcije za podešavanje rada, čišćenje i održavanje preglednika raširene su na mnogo različitih mjesta..

U prilog Internet Exploreru ide činjenica da je to iznimno konfigurabilan preglednik koji nudi mnoštvo korisnih i efektivnih sigurnosnih opcija i komponenata. Promišljenim konfiguriranjem ponuđenih postavki može se poprilično podignuti nivo sigurnosti preglednika i već u startu eliminirati mnoge rizike i mogućnosti napada. Na kraju krajeva, pored svih svojih prednosti i nedostataka, Internet Explorer je dobar preglednik s kojim su se svi susreli i na koji su se navikli; i koji sa svakim novim izdanjem postaje sve bolji i nudi sve više mogućnosti.

Internet Explorer 6 izašao je 2001. godine. Verzija koja je bila uključena u Windows XP operacijski sustav i dugo bila aktualna. Verzija 7 koja je uključena kao dio Windows Vista operacijskog sustava, izdana je 2005. godine, ne samo kao odgovor na Firefox i ostalu konkurenciju, već kao logičan slijed s obzirom na sigurnosna pitanja. Korisnici Windows XP operacijskog sustava došli su do sedme verzije najvjerojatnije putem Windows ažuriranja (Windows Update). Krajem 2008. godine očekuje se i Internet Explorer 8. Trenutno je dostupna Beta 1 verzija, a uskoro se očekuje i Beta 2.

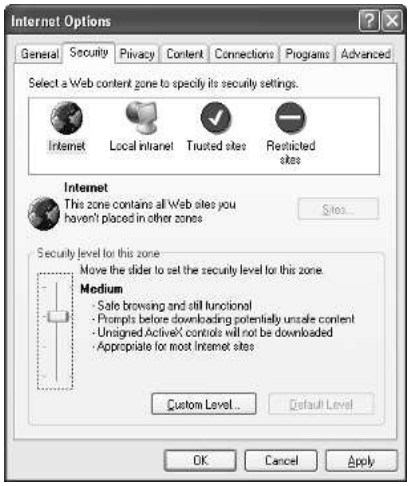
Internet Explorer 6

Internet Explorer 6 kompleksniji je i nudi više mogućnosti od prethodnih verzija.. U verziji 6 ponuđen je niz novih i korisnih funkcionalnosti. Iznimna konfigurabilnosti i niz sigurnosnih opcija ostavljaju dovoljno prostora da ga se učini mnogo sigurnijim nego što se to ljudima čini.

Postavke vezane za sigurnost, kao i samu Internet vezu, i ostalo, dostupne su unutar dijaloškog okvira Internet opcije (Internet Options) do kojega se može doći na više načina. Na primjer, pomoću izbornika Alati (Tools) u prozoru preglednika, preko Upravljačke ploče (Control panel) ili desnim klikom i odabirom opcije Svojstva (Properties) na ikonu Internet Explorera na radnoj površini, u traci za brzo pokretanje (Quick Launch) ili u izborniku Start.

Sigurnost

Jedna od najmoćnijih sigurnosnih opcija Internet Explorera je mogućnost kategoriziranja web mjesta u zone, prema sadržaju (Web content zone) i konfiguriranja različitih sigurnosnih pravila za svaku zonu i time i za sva web mjesta smještena unutar te zone. To zapravo pruža mogućnost da web mjesta s visokim potencijalnim faktorom rizika smjestimo u zonu sa najrestriktivnijim postavkama, a web mjesta koja se smatraju sigurna u zone s malo blažim, slobodnijim postavkama. Sigurnosne zone i postavke vezane za njih vidljive su na kartici Sigurnost (Security), u dijaloškom okviru za Internet postavke.



Slika 3.2. - Kartica Sigurnost (Security) unutar dijaloškog okvira Internet Opcije (Internet Options)

Određene su četiri sigurnosne zone: Internet, Lokalni intranet, pouzdana web mjesta i ograničena, nepouzdana web mjesta.

Postoje četiri pretpostavljena sigurnosna nivoa koja se mogu odabrati za svaku zonu: visoki, srednji, srednji do niski i niski.

Visoki nivo (High) je najsigurniji način korištenja Interneta, ali s ograničenom funkcionalnošću. Sve manje sigurne opcije su onemogućene. Sav ActiveX sadržaj je onemogućen, kao i preuzimanje sadržaja (download). I dodatno, postoji niz ograničenja vezanih za pristup podacima i zahtjeve za podacima.

Srednji nivo (Medium) omogućava sigurnost, a i funkcionalnost i u većini slučajeva postavke tog nivoa su najbolje za korištenje. Srednji nivo ne dopušta preuzimanje nepotpisanih ActiveX kontrola i prikazuje se obavijest prije preuzimanja potencijalno nesigurnog sadržaja.

Srednji do niski nivo (Medium – low) dopušta izvršavanje većine sadržaja bez obavijesti, no i ipak ne dopušta nepotpisane ActiveX kontrole. Te postavke su sigurne za intranet korisnike.

Niski nivo (Low) uključuje tek osnovna upozorenja i poneke zaštitne mjere. Sav aktivan sadržaj može se izvršavati. Takve postavke ne preporuča se koristiti osim ako nije riječ o web mjestu kojem korisnik potpuno vjeruje.

Učinkovito korištenje sigurnosnih zona zahtijeva informiranost o svim opasnostima koje postoje i razumijevanje svih različitih sigurnosnih postavki koje mogu biti primijenjene na svaku zonu, te ponešto razboritosti u određivanju koje web mjesto smjestiti u koju zonu.

Internet zona je zona koja se odnosi na sva web mjesta koja nisu izričito dodijeljena nekoj drugoj zoni. To zapravo znači da sva web mjesta pripadaju Internet zoni, ukoliko nisu drugačije konfigurirana. Sigurnosni nivo koji je standardno pridružen toj zoni je srednji (Medium). Taj predodređeni nivo općenito se smatra optimalnim za Internet zonu.

Lokalna intranet zona (Local Intranet) je posebna zona korištena za označavanje svih web mjesta koja pripadaju privatnoj mreži. Na primjer, ako na računalu unutar kućne mreže radi neki web poslužitelj, smatra se dijelom intranet zone. Sigurnosni nivo koji je standardno pridružen toj zoni je srednji do niski (Medium - low). Međutim, Microsoft sada preporučuje postavljanje sigurnosnog nivoa na srednji (Medium), kao i kod Internet zone.

Klikom na polje Mjesta (Sites) unutar intranet zone otvara se dijaloški okvir u kojem su dostupne još tri dodatne opcije koje određuju koja web mjesta će biti uključena u intranet zonu. Moguće je odabrati uključivanje:

- svih lokalnih web mjesta koja nisu dodana nekoj drugoj zoni

- svih web mjesta koja su postavljena da zaobilaze poslužitelj opunomoćenik (proxy)
- sva web mjesta referencirana UNC putanjama ili dostupna preko Mojih mrežnih mjesta (My network places)

Internet Explorer sve URL-ove koji ne sadržavaju točke, kao npr. http://localhost, smatra lokalnim web mjestima.

Prema standardnim postavkama, sve tri opcije su uključene i obično ih je preporučljivo ostaviti uključenima. U tom dijaloškom okviru također je moguće kliknuti na polje Dodatno (Advanced) i urediti listu web mjesta koja su uključena u intranet zonu. U slučaju da se neko lokalno web mjesto ne smatra dovoljno pouzdanim za konkretne sigurnosne postavke, najbolje ih je eksplicitno dodijeliti nekoj drugoj zoni.

Zona pouzdanih web mjesta (Trusted sites) je lista web mjesta i domena koja su eksplicitno smatrana pouzdanima, koja se ručno konfigurira. Na tu listu se mogu dodati npr. web mjesta banke, pružatelja e-mail usluga i druga pouzdana web mjesta koja korisnik često posjećuje. Standardni sigurnosni nivo je niski (Low). Kad je neko web mjesto dodano zoni pouzdanih web mjesta, postavke niskog sigurnosnog nivoa dozvoljavale su slobodnu uporabu tih web mjesta bez sigurnosnih ograničenja. Ipak, u posljednje vrijeme Microsoft je počeo preporučivati da bi čak i za zonu pouzdanih web mjesta trebalo koristiti srednji nivo sigurnosti.

Zona ograničenih web mjesta (Restricted sites) je lista web mjesta i domena koja korisnik smatra nepovjerljivima, nepouzdanima, koja se ručno konfigurira. Sve manje sigurne opcije surfanja su onemogućene prilikom posjeta web mjestu koje se nalazi na toj listi. Standardni pridruženi sigurnosni nivo je visoki (High).

U slučaju da ponuđene zone ne zadovoljavaju potrebe nekog korisnika, uz nešto manipulacije registrima moguće je čak i kreirati novu, korisničku prilagođenu zonu.

Za dodavanje web mjesta u svim zonama osim Internet zone (i spomenute intranet zone kod koje je potreban jedan korak više), potrebno je odabrati opciju Mjesta (Sites), unijeti URL i kliknuti na Dodaj (Add).

Brisanje je jednako jednostavno. Potrebno je samo odabrati URL iz liste i kliknuti na Ukloni (Remove).

Prilikom dodavanja web mjesta zonama, potrebno je imati na umu neke činjenice. Standardno je pretpostavljen HTTP protokol, pa je npr. unošenje www.microsoft.com ekvivalentno unosu http://www.microsoft.com. Bez obzira na opciju zahtjeva verificiranja za HTTPS koja je ponuđena u istom dijaloškom okviru (koja je standardno uključena), moguće je kombinirati zaštićena i nezaštićena web mjesta unutar svake zone. Potrebno je samo isključiti tu opciju prilikom unošenja web mjesta koje ne koristi HTTPS protokol. Unošenje potpune putanje za neku web stranicu koja je dio web mjesta zapravo dodaje čitavo pripadajuće web mjesto u konkretnu zonu. Za premještanje web mjesta iz jedne zone u drugu potrebno ga je prvo izbrisati iz zone u kojoj se trenutno nalazi jer Internet Explorer ne dozvoljava duplicirane unose.

Nadalje, dodavanje web mjesta na listu ograničenih radi se na jednak način kao i dodavanje ostalim zonama; no čitav proces pojedinačnog dodavanja svakog web mjesta koje se može smatrati opasnim može biti prilično iscrpljujuće. U tom slučaju može se iskoristiti neki od pomagala, alata napravljenih baš za tu svrhu. Jedan takav alat je IE-SPYAD2, koji dodaje opsežnu listu web mjesta i naziva domena povezanih s Internet oglašivačima i programerima malicioznog koda u Internet Explorerovu zonu ograničenih web mjesta. Alat je besplatan i redovno ažuriran. Može se preuzeti na http://netfiles.uiuc.edu/ehowes/www/resource.htm

Iako su standardne postavke pridružene svakom sigurnosnom nivou obično zadovoljavajuće za većinu korisnika, svaki korisnik može ručno promijeniti postavke svake zone i prilagoditi ih

prema vlastitim željama. Klikom na polje Prilagođeni nivo (Custom level) otvara se dijaloški okvir sa sigurnosnim postavkama (Security Settings). Svaka opcija nudi tri parametra za podešavanje: omogući (Enable), onemogući (Disable) i pitaj (Prompt).

Dostupne su postavke vezane za ActiveX kontrole, preuzimanje (download) sadržaja, Java postavke, postavke koje se odnose na skripte, autentifikacijske postavke te ostale, dodatne postavke. Većina postavki je već sama po sebi razumljiva i možda i optimalna, no neke je ipak korisno izmijeniti i dodatno ojačati sigurnost.

Internet Explorer 6 pruža niz postavki kojima se može ograničiti i kontrolirati kolačiće (cookie). Prethodne verzije Internet Explorera nudile su samo mogućnost blokiranja svih kolačića ili upit za odobravanje svakog pojedinog. Vrlo je očito koliko su obje opcije nepraktične. Internet Explorer 6 podržava standard nazvan P3P (Platform for Privacy Preference) koji omogućava Internet Exploreru da pregleda kolačiće, utvrdi kako će biti upotrijebljeni i zatim odluči što s njima. Ta mogućnost nije savršena i standard se još razvija, ali je veliki korak naprijed u ojačanju privatnosti na Internetu.

Privatnost

Postavke vezane za privatnost i postupanje s kolačićima dostupne su unutar kartice Privatnost (Privacy).

Šest mogućnosti baratanja kolačićima uključuju blokiranje ili dopuštanje svih kolačića, te četiri dodatna nivoa privatnosti.

Visoki nivo ne dopušta stvaranje kolačića koji uključuju osobne podatke, bez eksplicitne suglasnosti. Web mjesta koja nemaju definiranu kompaktnu izjavu o privatnosti ne mogu postavljati kolačiće. (Compact Privacy statement – tekst koji navodi točno kako će kolačići biti korišteni, te njihovo vrijeme trajanja).

Srednji do visoki nivo blokira kolačiće treće strane s web mjesta koja nemaju kompaktnu izjavu o privatnosti. Blokiraju se i kolačići treće strane koji koriste osobne informacije bez eksplicitne suglasnosti, kao i kolačići prve strane (first-party) koji koriste osobne informacije bez implicitne suglasnosti korisnika.

Srednji nivo odobrava kolačiće prve strane koji koriste osobne informacije bez implicitne suglasnosti, ali takvi kolačići bivaju izbrisani prilikom zatvaranja Internet Explorera. Blokirani su kolačići treće strane kao i kod prethodnog nivoa. Srednji nivo je nivo koji je standardno postavljen.

Niski nivo prihvaća sve kolačiće prve strane. Kolačići treće strane s web mjesta bez kompaktne izjave o privatnosti su blokirani, dok su kolačići treće strane koji koriste osobne informacije bez implicitne suglasnosti dopušteni, ali bivaju izbrisani prilikom izlaska iz Internet Explorera.

Opcija Uvezi (Import) omogućava uvoženje politike privatnosti s nekog drugog računala.

Opcija Dodatno (Advanced) omogućuje napredne opcije za određivanje kako će se postupati s kolačićima unutar Internet zone. Napredne postavke nadjačavaju automatsko baratanje kolačićima. U slučaju da ponuđene automatske postavke nisu zadovoljavajuće, moguće ih je nadjačati ovim postavkama. No, budući da se njima određuje baratanje svim kolačićima prve i treće strane, bez obzira na njihove kompaktne izjave o privatnosti i podatke koje koriste, možda to i nije najbolja ideja. Postavke su uniformne, ili dozvoljavaju ili blokiraju sve. Dozvoljavanje svih zapravo znači da i nema neke zaštite; blokiranje svih onemogućuje pristup web mjestima koji zahtijevaju rad s kolačićima; dok opcija upita za svaki pojedini kolačić većinom ispadne vrlo zamorna i nepraktična.

Pored šest ponuđenih razina postavki vezanih za privatnost moguće je i nadjačati odabrani nivo te odrediti specifičan način postupanja s kolačićima za pojedina web mjesta.

Kao opcija koja pruža najviši nivo zaštite, možda je najbolje odabrati visoki nivo privatnosti, te dodati popis pojedinih web mjesta za koja kolačići uvijek dopušteni.

Pored kartice Privatnost (Privacy) još su neke opcije dostupne za rad s kolačićima. Moguće je isto tako i otvoriti i pregledati informacije zapisane u bilo kojem od kolačića koje je Internet Explorer pohranio. Uvid u njih moguć je na kartici Općenito (General). Opcija Privremene Internet datoteke (Temporary Internet Files) odnosi se na sve podatke koje Internet Explorer pohranjuje prilikom surfanja, uključujući datoteke history, pričuvnu memoriju, kolačiće i sl.

Klikom na polje Postavke (Settings) otvara se dijaloški okvir s postavkama vezanim za privremene Internet datoteke Klikom na opciju Vidi datoteke (View files) otvara se mapa koja sadržava sve privremene kolačiće, kao i spremljene stranice i grafičke elemente. Kolačiće je jednostavno naći u toj mapi, samo treba potražiti tekstualne datoteke čiji nazivi počinju sa „Cookie“. Informacije koje sadržavaju moguće je vrlo jednostavno vidjeti, otvaranjem u npr. Bloku za pisanje (Notepad).

Tim putem moguće je vidjeti samo privremene, dok su trajni kolačići vezani za korisnički profil pohranjeni na drugom mjestu, unutar C:\Document and settings*Korisnik* (ime korisničkog računa, Username).

Unutar dijaloškog okvira Postavke (Settings) nalaze se i druge postavke vezane za privremene Internet datoteke. Tu je i lokacija na računalu gdje se te datoteke pohranjuju, koju je moguće izmijeniti, te količina prostora na tvrdom disku koja je rezervirana za te privremene datoteke.

Količina prostora koji se odvaja za te svrhe može se izmijeniti, smanjiti da bi se oslobodio diskovni prostor. Činjenica je da previše privremenih Internet datoteka i kolačića može usporiti surfanje. Stoga je dobro i redovno čistiti odnosno brisati te privremene datoteke u određenom razdoblju, da bi se poboljšale performanse, a i sam sigurnosni rizik koji nose takve pohranjene datoteke. Na kartici Općenito, pod Privremene Internet datoteke dostupna je opcija Obriši (Delete) koja omogućuje brisanje svih privremenih Internet datoteka.

Sadržaj

Kartica Sadržaj (Content) nudi postavke vezane uz web sadržaj, kao što i sam naziv kaže.

Kao što je već poznato, pored korisnog, na webu se može naići i na mnoštvo nepoželjnog sadržaja. Od web stranica koje uključuju neumjesno i neprikladno jezično izražavanje i nasilan sadržaj, do onih koje šire mržnju ili sadrže eksplicitnu pornografiju; čak i osnovna pretraga može odvesti do stranica koje većina ljudi smatra neprikladnima.

Za rješavanje tog problema Internet Explorer nudi funkciju koja se naziva Savjetovanje o sadržaju (Content Advisor). Pomoću te opcije moguće je kontrolirati vrste sadržaja i web mjesta kojima je moguće pristupiti. Kad je savjetnik o sadržaju uključen, ako korisnik pokuša pristupiti web stranici sa sadržajem koji je zabranjen prema postavkama, Internet Explorer neće prikazati takvu stranicu već će prikazati poruku s upozorenjem. Prilikom prvog uključivanja te opcije moguće je odrediti posebnu nadzornu lozinku, kojom se zaštićuju sve postavke.

Moguće je odrediti nivoe blokiranja, odnosno dopuštanja sadržaja za sva web mjesta prema kategorijama: jezik, golotinja, seks i nasilje. Isto tako, moguće je nadjačati te postavke za pojedina web mjesta, pa za neka odrediti da se uvijek dopuštaju ili uvijek blokiraju.

Za kontroliranje pristupa potencijalno uvredljivim ili nepoćudnim web mjestima, opcija savjetovanja o sadržaju oslanja se na rangiranje, ocjenjivanje sadržaja (content rating).

Internet Explorer standardno koristi ugrađene odrednice preuzete od organizacije za ocjenjivanje Internet sadržaja, ICRA (Internet Content Rating Association); iako se mogu instalirati i drugi sustavi za ocjenjivanje sadržaja.

Web mjesta mogu navesti ocjenu sadržaja tako da Internet Explorer zna da li da dopusti ili blokira neko web mjesto. Ako web mjesto želi ocjenu sadržaja, administrator ispunjava formular na web mjestu ICRA organizacije, koja zatim procjenjuje administratorove odgovore i pruža neku recimo etiketu (label), oznaku koju administrator uključuje u web mjesto. Kad netko želi pristupiti web mjestu pomoću Internet Explorera, čita se ta oznaka o ocjeni i poduzima odgovarajuća radnja, ovisno o postavkama. Postavkama je moguće odrediti i da Internet Explorer blokira, odnosno ne prikazuje ni web mjesta koja nemaju ocjenu sadržaja (isključenjem opcije Korisnici mogu vidjeti web mjesta koja nemaju ocjenu sadržaja (Users Can See Sites That Have No Rating) u kartici Općenito, u postavkama savjetnika o sadržaju (Content Advisor)).

ICRA je neovisna organizacija i ne cenzurira, pa čitava procjena zapravo ovisi u potpunosti o odgovorima koje administrator ponudi na pitanja. Ustvari, ocjena sadržaja ovisi o poštenju i iskrenosti administratora. Ipak, većina web mjesta koja žele ocjenu sadržaja, to rade u najboljoj namjeri, radi privatnosti i zaštite djece.

Sama činjenica da sve ovisi o riječima onoga koji zapravo vodi konkretno web mjesto jasno govori da takav mehanizam nije idealan. Kao dodatna zaštita, može se koristiti i neki od mnoštva dostupnih neovisnih alata za procjenu sadržaja i savjetovanje, te filtriranje sadržaja, koji su obrađeni ranije u ovom poglavlju. Razlika je što se takvi alati ne oslanjaju na ocjene web mjesta od strane njih samih, već imaju vlastite mehanizme procjenjivanja.

Unutar kartice Sadržaj, nalazi se još jedna funkcionalnost na koji bi trebalo obratiti pozornost. Opcija automatskog popunjavanja (AutoComplete) omogućuje da Internet Explorer pamti sve ono što je upisano, kao URL-ove, pojmove pretraga, podatke upisivane u forme, obrasce na web stranicama. Kada korisnik krene ponovno unijeti te podatke, Internet Explorer ih pokuša sam dovršiti. Ako je ponuđeni završetak točan, nije potrebno podatak unijeti to kraja, već samo pritisnuti tipku Enter. Neki ljudi smatraju tu mogućnost veoma korisnom, dok je drugima naporna. Ipak, u svakom slučaju ta opcija je sigurnosni rizik, jer se svi ti podaci koji se koriste za automatsko popunjavanje pohranjuju u memoriju računala. Najveći rizik predstavlja mogućnost pamćenja lozinki i korisničkih imena. Iako korisno i olakšava proces pristupa korisničkim računima, ostaje činjenica da su sve te lozinke onda pohranjene u memoriji i bilo koji napadač može lako doći do njih i iskoristiti ih. Zbog toga je najbolje isključiti sve ponuđene opcije automatskog popunjavanja, te obrisati one podatke koji su već pohranjeni.

Napredne opcije

Kartica Dodatno (Advanced) nudi niz dodatnih postavki vezanih za različite kategorije: Dostupnost (Accessibility), Pregledavanje (Browsing), HTTP, Multimedija, Ispisivanje (Printing), Traženje (Searching) i Sigurnost (Security). Standardne postavke su obično dobre, no ipak, dobro je proučiti ponuđene opcije i odabrati one koje najbolje odgovaraju osobnim potrebama. Moguće je i dodatno ojačati sigurnost, npr. uključivanjem opcije za automatsko brisanje privremenih Internet datoteka prilikom zatvaranja Internet Explorera.

Čitava sigurnost Internet Explorera dodatno je ojačana izdavanjem i instalacijom uslužnog paketa 2 (Service Pack 2). Dodan je niz novih sigurnosnih mogućnosti da bi se pojačala otpornost na maliciozne prijetnje i omogućila veća kontrola nad pokušajima preuzimanja elemenata kao što su recimo ActiveX kontrole. Većina poboljšanja zapravo je interna i odnosi se na samu arhitekturu preglednika, ali dodane su i tri nove opcije koje su vidljive korisnicima i dostupne za konfiguriranje. To je mogućnost Internet Explorera da radi s dodacima (Add-on), nova integrirana funkcija blokiranja privremenih (pop-up) prozora i informativna traka koja prikazuje obavijesti kada neko web mjesto pokuša preuzeti datoteku, prikazati privremeni prozor ili instalirati ActiveX kontrolu na korisnikovo računalo.

Internet Explorer 7

Sedma verzija najkorištenijeg preglednika donijela je mnoga sigurnosna poboljšanja kao i modernizirano korisničko sučelje. Sučelje uključuje korištenje kartica ili jahača (tab) čime postaje usporedivo s onim kod Firefox i Opera preglednika. Neki elementi prozora premješteni su da bi bili vidljiviji, upravo radi kartica; kao i druge nove osobine. Internet Explorer 7 je vrlo intuitivan preglednik koji je po svojim sposobnostima i sigurnosti u rangu s ostalim uobičajenim alternativama.

Microsoft je implementirao nove ili dopunjene sigurnosne opcije da bi osigurano sigurnije surfanje i lakše održavanje sigurnosti, kao npr.:

- ActiveX kontrole, bolna točka Internet Explorera, standardno su onemogućene. Poboljšanje opcije manipuliranja dodacima (Add-on Manager) omogućuje punu kontrolu nad dodacima i opciju brisanja neželjenih AcitveX kontrola.
- Osim toga, čitava lista dostupnih opcija za prilagođavanje sigurnosnih zona, sigurnosnih nivoa, naprednih postavki i ostalog, proširena je da bi se poboljšala sigurnost i konfigurabilnost
- Novi filtar (phishing filter) aktivno skenira i pazi na potencijalno neovlašteno traženje informacija i lažna web mjesta. Filtar pruža zaštitu od neovlaštenog traženja informacija (phishing), Internetskih prijevara i web zavaravanja (spoofing) i blokira web mjesta ako je potrebno. Filtar je opcijski, ali nema razloga da ga se ne koristi. Iznova se ažurira nekoliko puta u satu. Poboljšana sigurnosna statusna traka (Security Status Bar) mijenja boju da bi privukla pažnju. Obavijesti filtra i lokot koji označava sigurnu vezu sada su smješteni pored adresne trake, da bi bili vidljiviji
- Način postupanja s URL-ovima je također redizajniran da bi se smanjila mogućnost zlonamjernog iskorištavanja. Ako neko pouzdano ili „ne-zabranjeno“ web mjesto pokuša preuzeti i izvršiti skriptu s nekog zabranjenog web mjesta, skriptu neće biti moguće izvršiti
- Prikazat će se obavijest u slučaju da neko web mjesto pokuša nezaštićeno prenijeti lozinku
- Internet Explorer nudi zaštićeni način rada (Protected Mode) koji omogućuje surfanje s onemogućenim svim dodacima (ActiveX, dodaci (plug-in), BHO i sl.)

To su samo neke nove mogućnosti koje podižu IE na nivo usporediv s ostalim popularnim preglednicima. Prelazak s verzije 6 na verziju 7 je svakako preporučljiv, čak i ako Internet Explorer nije glavni preglednik koji se koristi. Ipak, sam prelazak na bolju verziju ne garantira savršenu sigurnost. Još uvijek su potrebne optimalne postavke, svi potrebni zaštitni programi (redovno ažurirani) i maksimalna količina opreza pri surfanju. Kao i praćenje svih obavijesti, novih otkrivenih propusta i ažurna primjena svih izdanih zakrpa i nadogradnji.

3.1.11. Alternativni preglednici weba

Bez obzira na sve kritike upućene na račun Internet Explorera, ostaje činjenica da je kao najviše korišten, najviše na meti napadača. To je razlog zbog kojeg mnogi korisnici odabiru opciju alternativnog web preglednika. Ono što se zaboravlja je da bilo koji drugi preglednik, ako postane korišten od većine, automatski postaje glavna meta napada. Dobro je uzeti u obzir neku od alternativa. Iako je za pristup nekim web stranicama potrebno koristiti Internet Explorer (npr. Windows update), sa stajališta zaštite dobro je koristiti neki drugi preglednik za sve ostalo.

Određeni osjećaj sigurnosti ipak proizlazi iz znanja da ste ipak malo manje na meti. Svi preglednici koji se danas bore za dio tržišta, učili su iz grešaka prethodnih verzija Internet

Explorera i pronašli drugačije načine rješavanja najvećih rizika, te ih to čini donekle sigurnijima. Danas je sve to postala velika borba za prevlast u kojoj su konkurenti relativno izjednačeni po opcijama i sigurnosti, te su one stvari koje boljeg čine boljim u nekom trenutku zapravo tek nijanse. Ipak, ta kompetitivnost ih tjera da sve više rade na poboljšanjima, na sigurnosti i jednostavnosti uporabe što je vrlo dobro za svakog korisnika.

Danas su pored Internet Explorera najpoznatiji preglednici za Windows sustave Mozilla Firefox i Opera.

Mozilla Firefox

Najpopularnija alternativa Internet Exploreru, koju odabire sve veći broj korisnika. Preglednik koji je prvi put izašao 1995. godine vrlo je brzo stekao popularnost. Napravljen je upravo kako bi izravno konkurirao Internet Exploreru, pokušaj da se u maloj instalacijskoj datoteci ponudi brz preglednik koji neće biti osjetljiv na tipične ranjivosti svog konkurenta. Od samog početka to je besplatan program (open–source) s mogućnošću značajnog proširenja funkcionalnosti instalacijom mnoštva besplatnih ekstenzija.

Korištenje kartica (tab), pamćenje lozinki, vrlo brzo prikazivanje web stranica, zumiranje sadržaja, provjera pravopisa, integrirane tražilice, elegantna integracija sa programima za detekciju virusa, zaštita od neovlaštenog traženja informacija (phishing), blokiranje privremenih (pop-up) prozora, dostupnost na preko 40 svjetskih jezika, korisnička potpora, jednostavno održavanje i iznimna konfigurabilnost samo su neke od karakteristika koje čine Firefox odličnim programom i preglednikom koji odabire veliki postotak korisnika.

Smatra se vrlo sigurnim preglednikom, sa zajednicom stručnjaka koji stalno rade na poboljšanju, ispravljanju svih otkrivenih problema i redovnom izdavanju nadopuna i novih verzija preglednika. Dodatna prednost u tom pogledu je otvorenost koda koja omogućuje svima da doprinesu unaprjeđenju sigurnosti.

Trenutna verzija Mozilla Firefox preglednika je verzija 3 (odnosno 3.1.0.2.). Može se preuzeti na http://www.mozilla.com/en-US/firefox/

Opera

Vrlo „malen“, kompaktan preglednik kojeg je razvila jedna norveška kompanija. Iznimno hvaljen i visoko ocjenjivan preglednik nudi dobru alternativu Internet Exploreru. Moćan, ugodna izgleda, i iznimne lakoće uporabe, Opera je preglednik malo pomalo osvaja tržište.

Do verzije 8, to je bio komercijalni proizvod koji je trebalo platiti. U ponudi je bila i besplatna verzija koja je sadržavala reklame i oglase. Plaćena verzija nije sadržavala oglase, nudila je potporu za elektroničku poštu i 6 mjeseci besplatne usluge Opera Web Mail.

Od verzije 8 nadalje, Opera je besplatan preglednik. Koristi kartice (tab), iznimno brzo prikazuje web stranice, ima ugrađeno blokiranje privremenih prozora, integriran e-mail klijent, besplatnu e-mail uslugu, integrirane tražilice, pamćenje podataka o korisničkim računima (Wand), mogućnost mijenjanja izgleda (skin) i tema, zumiranje sadržaja, geste miša i potporu za glasovne naredbe. Konfiguriranje i održavanje je relativno jednostavno, jer su sve glavne postavke smještene na jednom mjestu, unutar izbornika alati (Tools). Čitav preglednik je dobro organiziran i intuitivan.

Po pitanju sigurnosti, smatra se iznimno sigurnim preglednikom. Nove verzije često izlaze, a svaki otkriveni propust ažurno je adresiran i ispravljen u najbržem roku, bez obzira na težinu. Svaki sigurnosni propust eliminiran je izdavanjem nove verzije. Zbog toga je jako bitno, kao i kod bilo kojeg drugog preglednika ili programa koji utječe na sigurnost, uvijek imati instaliranu najnoviju verziju. Trenutno aktualna verzija Opera web preglednika je 9.52. Može se preuzeti na http://www.opera.com/products/desktop/

3.2. ELEKTRONIČKA POŠTA

Slanje i primanje elektroničke pošte jedna je od najčešćih radnji koje se izvode na računalu. Zbog mogućnosti dostavljanja poruka gotovo odmah, bilo gdje na svijetu, elektronička pošta pruža brzinu i učinkovitost s kojom se klasična poštanska usluga ne može niti mjeriti. No, jednako učinkovito kako dostavlja legitimne poruke, toliko je efikasna i u distribuiranju malicioznih programa i neželjenih spam poruka.

Koncept elektroničke pošte ima korijene još u ARPANET-u, u ranim sedamdesetim godinama prošlog stoljeća. Od svojih početaka kao komandno-linijski program koji je koristila nekolicina ljudi, za razmjenu šačice informacija, ideja e-maila je polagano evoluirala u ono što danas koristimo.

Danas je e-mail primarno sredstvo poslovne i privatne komunikacije za milijune ljudi. Milijarde poruka dnevno šalju se naprijed i natrag preko Interneta. Nažalost, prema statistikama oko 70-80 % od čitave elektroničke pošte koja se razmjenjuje su neželjene komercijalne poruke, odnosno spam, a jedan od 36 e-mailova sadrži neki oblik malicioznog koda.

Po pitanju neželjene pošte to možda i nije toliko različito od standardnog poštanskog sandučića. Većina klasične pošte koju danas primamo sastoji se od kataloga, oglasa i reklama. No opet, sadržaj elektroničke pošte može biti mnogo štetniji za nas od reklamnih kataloga koji zatrpavaju naše sandučiće.

Sposobnost komunikacije s bilo kim na svijetu gotovo trenutno čini e-mail savršenim za mnoge oblike komunikacije. Međutim, upravo zbog brzine i raširenosti uporabe, e-mail je jedna od najčešćih metoda širenja raznoraznih vrsta malicioznih programa. Zbog toga je ključno držati se osnovnih pravila i poduzeti potrebne mjere predostrožnosti kako bi e-mail komunikacija bila i učinkovita i sigurna.

Privitci e-mail poruka su mnogim korisnicima velika prednosti, vrlo korisna mogućnost brze i jednostavne razmjene raznih privatnih i poslovnih informacija, slika, programa i drugih datoteka. Ali isto tako, kod većine malicioznih e-mailova, onaj maliciozni dio nalazi se unutar privitka. Raznim tehnikama socijalnog inženjeringa korisnika se tekstom u tijelu e-mail poruke pokušava nagovoriti, uvjeriti da otvori privitak i pokrene datoteku, te time inficira računalo.

Pored samo uvjerljivog nagovora, uskoro su uslijedile i druge tehnike zavaravanja, pa se elektroničke poruke maskiraju na način da korisnik misli da stižu od njemu poznate osobe. Veća je vjerojatnost da će korisnik otvoriti poruku od nekog rođaka ili radnog kolege pa počinje stvaranje virusa i malicioznih programa koji sami sebe šalju na sve adrese iz adresara e-mail klijenta na zaraženom računalu. Stoga je potrebno imati na umu da bi čak i e-mail sa poznate adrese mogao biti sumnjiv, te da opreza nikad dosta. Pogotovo s obzirom na činjenicu da je u nekim situacijama čak dovoljno i samo otvoriti e-mail poruku da bi se računalo inficiralo, dakle, opasnosti se ne kriju samo u privitcima.

Budući da je danas većina korisnika svjesna da je velika vjerojatnost da se u privitku koji sadrži neku izvršnu datoteku skriva neki maliciozni program, usvojili su naviku ne otvarati takve privitke, osim ako točno znaju o čemu je riječ ili očekuju primitak takve datoteke. No, kao dodatna metoda zavaravanja, često se maliciozni programi maskiraju na način da im se maskira ekstenzija, odnosno stavlja se dvostruka ekstenzija. A budući da je na većini računala običnih korisnika uključeno skrivanje ekstenzija, ona koja naznačava potencijalnu opasnost ostaje skrivena. Ali, iako bi većina pametnih korisnika trebala shvatiti da, ako je uključeno skrivanje ekstenzija, nikakva ekstenzija ne bi trebala biti vidljiva, ipak nasjednu na takve varke te i otvaraju takve datoteke.

Većina e-mail klijenata danas nudi mogućnost filtriranja e-mail poruka po raznim pravilima, što je vrlo korisno. No, kako liste blokiranih vrsta datoteka rastu, pisci malicioznih programa pronalaze nove vrste izvršnih datoteka i nove načine skrivanja.

U svakom slučaju, privitke bi trebalo otvarati samo ako korisnik potpuno vjeruje pošiljatelju i upoznat je s onim što se nalazi u privitku, te ako je potpuno siguran da konkretni e-mail stiže upravo s adrese s koje piše da stiže. U protivnom, privitke e-mailova s nepoznatih adresa ili privitke sumnjivim e-mailovima nipošto ne bi trebalo otvarati.

Što se tiče spama, na nikakve spam e-mail poruke ne bi trebalo odgovarati, te ih zapravo ne bi trebalo niti otvarati. Takve poruke obično imaju naslove koji odmah u startu naznačuju da je riječ o spamu, te bi ih trebalo odmah izbrisati jer nikad ne možemo znati da li se u njima nalaze samo iritantne reklame ili neke prijevare i maliciozni programi. Te, isto tako, vlastitu e-mail adresu nikad ne bi trebalo javno objavljivati na web stranicama ili ih unositi u razne web formulare. Za takve slučajeve, osim izbjegavanja takvih situacija uopće, dobro je koristiti i dodatni e-mail račun, e-mail adresu odvojenu za upravo takve svrhe.

Dostupni izbori što se tiče usluge elektroničke pošte su korištenje e-mail klijenta, na računalu, koji preuzima i pregledava e-mail poruke sa POP3 računa (Post Office Protocol), ili pregledavati e-mail na web stranicama, odnosno koristiti e-mail sandučiće na webu (web based e-mail). Oba pristupa imaju svoje prednosti i nedostatke.

Korištenje e-mail klijenta, koji zapravo služi kao posrednik između e-mail poslužitelja i korisnika omogućuje razne pogodnosti i sigurnosne mjere koje takvi programi pružaju. Najpoznatiji e-mail klijent je Outlook Express, koji dolazi s Windows operacijskim sustavima i većina korisnika se služi njime upravo zato jer je besplatan i već dostupan samo instalacijom Windows operacijskog sustava. No, korištenje e-mail klijenta zahtijeva rad s elektroničkom poštom s tog jednog računala na kojem je instaliran e-mail klijent i konfiguriran e-mail račun.

Web e-mail sustavi kao što je Hotmail, Yahoo! mail i slični pružaju pogodnost pristupanja e-mail sandučićima i slanje i primanje elektroničke pošte na bilo kojem računalu koje je povezano s Internetom.

U slučaju odabira web e-mail usluge, najbolje je odabrati one pružatelje usluga koji nude i razne sigurnosne opcije, kao što je skeniranje privitaka programima za detekciju virusa, spam filtriranja, mogućnost šifriranja e-mail poruka i pristup e-mail računu preko sigurne veze (SSL).

Isto tako, prilikom pristupanja web e-mail sandučiću s nekog javnog računala također treba paziti da se privatni podaci ne spremaju na računalu (u priručnoj memoriji, cache), te se uvijek odjaviti s računa nakon završetka rada.

3.2.1. Outlook Express

Outlook Express je dizajniran za rad u paru s Internet Explorerom. Pruža većinu funkcionalnosti i mogućnosti za upravljanje elektroničkom poštom koju napredniji korisnici trebaju i zahtijevaju. U prošlosti je to bio jednostavan e-mail klijent koji je pružao mogućnost spajanja na POP (Post Office Protocol) ili IMAP (Internet Message Access Protocol) e-mail poslužitelje i preuzimanja ili slanja e-mail poruka. Danas nudi mnoge napredne opcije i ima mnogo više toga za ponuditi, pogotovo za jedan besplatan e-mail klijent.

Međutim, kao besplatan e-mail klijent koji dolazi sa Windows operacijskim sustavom, koristi ga velika većina korisnika. Situacija je slična kao i kod Internet Explorera. Kao najkorišteniji, najviše je na meti napadača. Često mu se prigovara mnoštvo propusta i općenita nesigurnost. Mnogi su maliciozni programi pisani s izravnom namjerom da iskorištavaju neke poznate propuste tog e-mail klijenta. Činjenica jest da su propusti Outlook Expressa jasno naglašavani i često iskorištavani. No, opet se povlači isto pitanje, da li je to zato što je Outlook Express uistinu

loš e-mail klijent, ili je to zato što je jednostavno najviše na meti? Kako god bilo, sa svakom novom verzijom Outlook Express sve više napreduje. Radi se na sigurnosti i nudi se sve više mogućnosti. Trenutno aktualna verzija je Outlook Express 6.

Outlook Express je dosta fleksibilan i konfigurabilan, te je korištenjem svih mogućnosti koje nudi i ispravnim konfiguriranjem moguće poprilično podignuti nivo sigurnosti koji pruža.

Da bismo Outlook Express konfigurirali na najviši nivo sigurnosti i tako ga maksimalno zaštitili, potrebno je odabrati najstrože postavke. To međutim može oduzeti neke funkcionalnosti, no to je opet pitanje izbora između udobnosti ili sigurnosti.

One najvažnije sigurnosne postavke Outlook Expressa nalaze se u dijaloškom okviru Opcije (Options), kartica Sigurnost (Security). Dijaloški okvir je dostupan unutar izbornika Alati (Tools).

Unutar stavke „Zaštita od virusa“ (Virus Protection) ponuđeno je nekoliko opcija koje omogućuju pojačanje sigurnosti. Prva ponuđena opcija odnosi se na sigurnosne zone Internet Explorera. Potrebno je odabrati da li će Outlook Express koristiti Internet zonu ili zonu ograničenih web mjesta. Odabrana zona primjenjuje iste postavke konfigurirane za tu zonu unutar dijaloškog okvira za postavke Interneta. Odabir Internet zone znači manju sigurnost, ali više funkcionalnosti, dok korištenje zone ograničenih web mjesta pruža veću sigurnost jer blokira svu elektroničnu poštu koja je povezana s web mjestima koja se nalaze na listi ograničenih. Preporuka je, naravno, odabrati onu sigurniju opciju.

Slika 3.3 - Kartica Sigurnost (Security) unutar dijaloškog okvira za postavke Outlook Express e-mail klijenta

Opcija koja bi svakako trebala biti uključena je „Upozori me kada druge aplikacije pokušaju poslati poruke u moje ime“ (Warn me when other applications try to send mail as me). Samo ime dovoljno govori, te je u svakom slučaju dobro uključiti tu opciju koja štiti korisnika od onih vrsta malicioznih programa koji koriste adresar da bi slali kopije samog sebe slanjem lažnih e-mail poruka u ime korisnika koji o tome ništa ne zna.

Sljedeća dostupna opcija je potpuna zabrana spremanja ili otvaranja privitaka koji bi mogli sadržavati viruse (Do not allow attachments to be saved or opened that could potentially be a virus). Mehanizam blokiranja privitaka uveden je tek sa šestom verzijom tog e-mail klijenta. Iako pruža izvrsnu zaštitu od virusa i drugog malicioznog koda, postavka je zapravo vrlo

restriktivna i zabranjuje čitanje ili spremanje svih privitaka koje Outlook Express smatra opasnima. U odlučivanju što je zapravo opasno, Outlook Express koristi istu listu koju koristi i Internet Explorer kada provjerava datoteke koje korisnik preuzima (download). Lista se sastoji od dva dijela. Prvi dio čini predefinirana lista ekstenzija koje se uvijek smatraju opasnima, a to su obično izvršne datoteke (.exe, .bat, .bas, .cmd, .com i sl.). Kad je uključeno blokiranje privitaka, takve vrste datoteka su uvijek blokirane. Drugi dio čini lista tipova datoteka za koje je uključena opcija Potvrdi otvaranje nakon preuzimanja (Confirm Open After Download). Prema standardnim postavkama u tu listu su uključene datoteke koje se generalno smatraju sumnjivima kao Jscript/JavaScript datoteke (ekstenzija .js), Windows Installer paketi (ekstenzija .msi) i sl. Međutim, također su blokirani i Internet prečaci (.url), komprimirane datoteke (.zip), Office dokumenti (.doc, .xls i sl.). Zapravo, samo obične tekstualne datoteke (.txt) i slikovne datoteke (.gif) mogu proći kroz filtar privitaka.

Tu je opciju preporučljivo koristiti, ali pritom i prilagoditi restriktivna pravila. Listu zabranjenih vrsta datoteka je moguće donekle modificirati, barem onaj drugi dio liste, dakle one koje nisu predefinirane kao opasne. Moguće je recimo definirati vrste datoteka koje smatramo sigurnima i koje bi uvijek trebalo dozvoliti. Modificiranje liste moguće je izvršiti korištenjem dijaloškog okvira Odrednice mape (Folder Options) dostupnog unutar Upravljačke ploče ili u izborniku Alati (Tools) unutar svakog prozora mape. Unutar dijaloškog okvira potrebno je odabrati karticu Vrste datoteka (File Types), te unutar liste Registrirane vrste datoteka (Registered file types) pronaći ekstenziju za vrstu datoteke za koju želimo izmijeniti postavke. Nakon odabira željenog unosa, klikom na Dodatno (Advanced) otvara se novi dijaloški okvir u kojem je potrebno samo isključiti opciju Potvrdi otvaranje nakon preuzimanja (Confirm Open After Download) i potvrditi izmjene klikom na Uredu. Postupak je potrebno ponoviti za sve vrste datoteka koje želimo definirati kao sigurne. No, isto tako treba biti svjestan činjenice da bi mijenjanje tih postavki moglo utjecati i način na koji će s njima postupati Internet Explorer.

U slučaju da korisnik primi e-mail poruku sa privitkom koji Outlook Express blokira, pored prethodno objašnjene metode (koja, kao što je već rečeno nije moguća za većinu izvršnih datoteka) druga mogućnost je i privremeno isključiti blokiranje privitaka, te nakon spremanja ili otvaranja privitka ponovno uključiti tu opciju.

Još jedna ponuđena sigurnosna opcija je blokiranje slika i ostalog vanjskog sadržaja unutar HTML e-maila. E-mail poruke u HTML formatu omogućuju obogaćivanje teksta slikama i drugim elementima. Problem s takvim porukama je da se maliciozni kod može skrivati unutar HTML koda i aktivirati se nakon otvaranja e-mail poruka. Stoga je osim blokiranja slika i ostalog vanjskog sadržaja dostupna i opcija prikazivanja svih e-mail poruka kao čisti tekst (plain text). Da bi se ta mogućnost koristila, dovoljno je na kartici Čitanje (Read) uključiti opciju Čitaj sve poruke kao čisti tekst (Read all messages in plain text). Nadalje, pored te opcije, unutar kartice Slanje (Send) pod Format slanja pošte (Mail sending format) dostupna je opcija Čisti tekst (Plain text). Odabirom te opcije sve poruke se pišu i šalju kao čisti tekst čime smo osigurali sigurnost e-mail poruka koje šaljemo našim prijateljima, obitelji i poznanicima.

Nadalje, na kartici Sigurnost, unutar stavke Sigurni e-mail (Secure e-mail) nalaze se postavke vezane za digitalne certifikate. Da bi koristili sigurni e-mail potrebno je pribaviti digitalni certifikat od tvrtki kao što je VeriSign ili Thawte. Uključenjem opcije Digitalno potpiši sve odlazne poruke (Digitally Sign All Outgoing Messages), zajedno s porukom šalje se i certifikat kao dokaz da poruka stiže od upravo tog korisnika, te da nije modificirana u prijenosu. Moguće je i odabrati opciju šifriranja sadržaja i privitaka za sve odlazne poruke (Encrypt Contents And Attachments For All Outgoing Messages) što zapravo osigurava da nitko drugi osim primatelja kojem je namijenjena, neće moći pročitati poslanu poruku. Iako te sigurnosne opcije zapravo pružaju dobru zaštitu, primatelj poruke mora moći pročitati potpis i dešifrirati poruku da bi cijela stvar funkcionirala, što zahtjeva određenu proceduru konfiguriranja usluge da bi se mogla koristiti.

Budući da nije vjerojatno da će obični korisnik imati potrebu digitalno potpisati i šifrirati svaku poruku, umjesto uključivanja tih opcija (koje se zatim primjenjuju na sve odlazne poruke) moguće je digitalno potpisati i/ili šifrirati pojedinačne poruke odabirom odgovarajuće opcije prilikom sastavljanja pojedine poruke.

Pored postavki dostupnih unutar dijaloškog okvira Opcije (Options), postoje i neke druge postavke na koje je potrebno obratiti pozornost.

Outlook Express ima funkciju, opciju koja se naziva Okvir za pretpregled (Preview pane) koji omogućava upravo to, pretpregled poruke samo odabirom, bez potrebe za otvaranjem poruke dvostrukim klikom. Unatoč pogodnosti, korištenje okvira za pretpregled je zapravo jednako kao i otvaranje poruke – neprikladne slike se mogu prikazati, poruke mogu biti dekodirane, opasne skripte se mogu izvršavati, virusi se mogu pokrenuti i sl. Stoga, za zaštitu privatnosti, potrebno je onemogućiti, isključiti okvir pretpregleda.

Potrebno je kliknuti na mapu dolazne pošte (Inbox), zatim u izborniku Prikaz (View) odabrati Izgled (Layout) te isključiti opciju Prikaži okvir za pretpregled (Show Preview pane) i potvrditi izmjene klikom na Primjeni (Apply). Postupak je potrebno ponoviti i za sve ostale mape u kojima se pregledavaju ili pohranjuju poruke. Nakon toga potvrditi sve klikom na Uredu.

Outlook Expres nudi i još neke korisne opcije.

Moguće je vidjeti detalje e-mail poruke bez samog otvaranja poruke. Korištenje pasivnog preglednika (passive viewer) pomaže na siguran način utvrditi da li je neki e-mail siguran i da li ga otvoriti ili ne. Unutar mape dolazne pošte (Inbox) ili neke druge mape u kojoj se pohranjuju, desnim klikom na e-mail koji je u pitanju i odabirom Svojstva (Properties) otvara se dijaloški okvir. Odabirom kartice Detalji (Details) i opcije Izvorni kod poruke (Message source) otvara se novi prozor. U tom prozoru prikazuje se zapravo sami kod poruke, te je podebljanim slovima prikazan naslov ili zaglavlje poruke. A normalnim slovima je prikazan glavni tekst odnosno tijelo e-mail poruke. Ako ono što je prikazano dovoljno svjedoči da je e-mail poruka sigurna, onda se može normalno otvoriti; a ako nije, treba je izbrisati.

Još jedna veoma korisna mogućnost koji nudi Outlook Express je filtriranje e-mail poruke. Moguće je samostalno definirati neka pravila po kojima će poruke biti filtrirane, te odgovarajuće radnje za razne situacije.

Filtriranje je moguće po pošiljatelju, po predmetu (naslovu), po specifičnim riječima bilo gdje u poruci i još mnoge druge mogućnosti. Moguće je recimo filtrirati sve poruke na način da one koje sadrže određenu riječ, recimo bomba ili Viagra ili slično, automatsku budu premještene u mapu Izbrisani predmeti. Mogućnosti je mnogo i svakako bi ih bilo dobro iskoristiti. Postavljanje pravila moguće je unutar dijaloškog okvira koji je dostupan odabirom izbornika Alati (Tools) i opcije Pravila poruka -> Pošta (Message Rules -> Mail).

To je jedna korisna metoda borbe protiv spama. Međutim, s obzirom na sve veću pošast neželjenih i napornih e-mail poruka, možda bi bilo najbolje bitku protiv njih voditi korištenjem nekih od specijaliziranih programa za detekciju spama (anti-spam). Tu su npr. Norton AntiSpam ili McAfee SpamKiller ili recimo Cloudmark Desktop koji je zapravo dodatak (plug-in) za Outlook Express. Takvi alati filtriraju e-mail poruke korištenjem raznih tehnika za otkrivanje svega što bi moglo biti spam i uvelike smanjuju broj tih neželjenih poruka.

Dakle, s pravim postavkama veliki se napredak može napraviti. Isto tako, potrebno je redovno ažurirati Outlook Express, instalirati nadopune koje se izdaju, te nove verzije kako dolaze.

Pored svih postavki koje su dostupne, najvažniji element u radu s elektroničkom poštom je i dalje oprez. Veliki dio problema se može potpuno izbjeći samo pridržavanjem osnovnih pravila na koja nas upozoravaju na svakom koraku i korištenjem zdravog razuma.

Ipak, s obzirom na sve optužbe upućene na račun sigurnosnih propusta Outlook Expressa, mnogi ljudi odluče početi koristiti nešto drugo. Neki alternativni e-mail klijent. Dakle, moguće je potpuno ukloniti Outlook Express (Dodaj ili ukloni Windows komponente) ili samo odrediti neki drugi e-mail klijent kao zadani, kao glavni (Set program access and defaults)

Popularna alternativa je Outlook, nešto kao unaprijeđeni, obogaćeni Outlook Express koji dolazi kao dio Microsoft Office paketa. Za Outlook se također često kaže da ima i on popriličan broj svojih mana, a mnogi ga izbjegavaju i zbog same činjenice da je to sličan proizvod od iste tvrtke, a za ovog čak treba i platiti. Iz tih ili mnogih drugih razlika odabiru neke druge, ne-Microsoft alternative. Među njima je vjerojatno najpopularniji Thunderbird, e-mail klijent tvrtke Mozilla, čiji je proizvod i nadaleko poznati web preglednik Firefox. Pored Mozilla Thunderbirda, tu su i Eudora, Pegasus Mail, Netscape Mail i ostali, te npr. za korisnike Opera preglednika, e-mail klijent koji je integriran u preglednik.

3.3. ZAŠTITNI PROGRAMI

Najbolji način zaštite računala od napadača i malicioznog koda je korištenje aplikacija napravljenih upravo za te svrhe. Vatrozid je nužna zaštita računala jer predstavlja prvu crtu obrane od malicioznih aplikacija i pokušaja provaljivanja. Računalo ima 65536 priključnih točaka pomoću kojih je moguće uspostaviti kontakt. Da bi ih se zaštitilo, potrebno je imati dobar vatrozid koji je redovno održavan i ažuriran kad je potrebno. Nekad je bilo dovoljno samo imati instaliran vatrozid kako bi korisnik bio zaštićen na Internetu, no danas se ta vremena čine prilično dalekima. Svakodnevno nastaju nove vrste i oblici malicioznog aplikacija, pa je potrebno sve više vrsta zaštitnih programa da bi se postigla zadovoljavajuća sigurnost.

Postoji mnoštvo zaštitnih alata (anti-malware), skenera koji su razvijeni da štite računalo od pojedinih tipova malicioznih aplikacija. Većina tih alata usmjerena je na specifičnu vrstu prijetnje. Na primjer, program za detekciju virusa (anti-virus) služi za zaštitu od virusa, programi za detekciju špijunskog koda (anti-spyware) programi štite od špijunskog (spyware) i reklamnog (adware) koda, programi za detekciju trojanaca (anti-Trojan) štite od trojanskih konja itd.

Nakon otkrivanja nametnika na računalu, odgovarajući zaštitni program premješta zaraženu datoteku u karantenu – područje za dezinfekciju i uklanjanje, čime se sprečava da maliciozni kod uspostavi kontakt s drugim programima ili inficira druge datoteke.

Nijedan zaštitni program nije uvijek sto posto učinkovit. Moguće je da nekad neće moći detektirati ili otkloniti neki specifični maliciozni program i potrebno se poslužiti drugim sredstvima. No ipak, zaštita je pouzdana dok su god zaštitni programi ažurirani najnovijim definicijama. Sve nadopune i zakrpe treba primijeniti čim su izdane. Većina takvih programa može obavljati ažuriranje automatski ili je moguće postaviti raspored, vrijeme ažuriranja.

Mnogi zaštitni programi imaju sposobnost otkrivanja i otklanjanja i drugih vrsta nametnika osim onih za koje su direktno namijenjeni. Tako na primjer, programi za detekciju virusa detektiraju viruse, ali i crve i mnoge trojanske konje. Razlog tome je činjenica da se granice između klasifikacije malicioznih aplikacija sve više smanjuju, te postoji sve više miješanih prijetnji – malicioznih programa s višestrukim komponentama koje se mogu svrstati u više kategorija. No, ipak je najbolje koristiti više različitih vrsta zaštitnih programa za postizanje maksimalne zaštite. Individualni zaštitni programi uvijek su najbolji u onome što im samo ime implicira odnosno kategorija zaštitnih programa u koju spadaju.

Dva su glavna elementa zaštite koju takvi programi pružaju. Stalni nadzor, zaštita u realnom vremenu (real-time monitoring, real-time protection) je komponenta koja konstantno skenira, u realnom vremenu, što zapravo omogućava prevenciju, otkrivanje prijetnji prije instalacije malicioznih aplikacija ili inficiranja računala. Pored zaštite u realnom vremenu koju je potrebno stalno držati uključenom; mogućnost skeniranja čitavog sustava također je iznimno važna funkcija. Najbolje je jednom tjedno ili čak i češće pokrenuti skeniranje čitavog računala, sa svim zaštitnim programima po redu, i to kada računalo nije spojeno na Internet (offline). Iako bi taj postupak mogao dosta trajati, ovisno o veličini tvrdog diska i količini podataka na njemu, to je vrlo važan korak u održavanju zaštite računala.

3.3.1. Programi za detekciju virusa (anti – virus)

Program za detekciju virusa (anti-virus) je apsolutno nužno imati, za sve aktivnosti, bilo na Internetu ili ne. Takvi programi su dizajnirani da otkrivaju i uklanjaju viruse, pružajući i aktivnu zaštitu i skeniranje na zahtjev. Moguće je skenirati pojedine datoteke, mape, dijelove računala ili čitavo računalo. Aktivna zaštita trebala bi biti dostupna i uključena stalno, bez obzira da li je računalo priključeno na Internet ili ne, u slučaju da korisnik pokuša na primjer otvoriti neku zapakiranu datoteku koja sadrži maliciozni kod ili slično.

Postoje dvije vrste tehnika detektiranja virusa. Prva tehnika, koju koristi većina programa za detekciju virusa je tehnika „traženja“ poznatih virusa. Pretražuju se datoteke u potrazi za potpisom poznatih, već otkrivenih virusa, prema podacima iz definicija koje se preuzimaju ažuriranjem. Druga tehnika, koja se naziva i heuristika, ne temelji se na traženju poznatih virusa, već se pregledava računao u potrazi za anomalijama. Traži se bilo što sumnjivo, bilo kakva aktivnost koja bi mogla biti maliciozna (u ovom slučaju virusna), kao npr. pokušaji modificiranja veličine neke izvršne datoteke i sl. Takve tehnike ne mogu detektirati prisutnost virusa, ali mogu upozoriti korisnika da se nešto sumnjivo događa u sustavu.

Nakon instalacije programa za detekciju virusa potrebno ga je održavati ažuriranim. Redovno svakodnevno preuzimanje novih definicija neophodno je za održavanje snažne protuvirusne zaštite. Isto tako, pored najnovijih definicija, uvijek je dobro imati i posljednju verziju programa. Svaki takav alat sa svakom novom verzijom dobiva neka poboljšanja ili nove funkcionalnosti.

Važno je također uvijek imati uključen samo jedan program za detekciju virusa s aktivnom zaštitom, jer inače problemi mogu nastati zbog konflikta koji se stvara između više aktivnih programa za detekciju virusa. Ukoliko se planira koristiti program za rad s ravnopravnim korisnicima (P2P program), alat za trenutne poruke ili e-mail klijent, takve je programe potrebno instalirati neposredno prije programa za detekciju virusa.

Koji je program za detekciju virusa najbolji, na to je pitanje teško odgovoriti. Programi kao što je NOD32, Kaspersky Antivirus, BitDefender, Norton Antivirus i sl. su među najboljima na većini top lista i među njima se uvijek vodi borba za prvo mjesto. Razlike su tek u nijansama, pa je tako jedne godine jedan na prvom mjestu, druge drugi, a isto tako rezultati se mogu razlikovati i ovisno o tome tko provodi istraživanje i testiranje. No, pri procjeni koliko je „dobar“ neki takav program ne ocjenjuje se samo uspješnost u detektiranju malicioznih aplikacija, nego i drugi faktori, kao što je brzina skeniranja, lakoća uporabe, zauzimanje računalnih resursa i sl. Neki takvi programi smatraju se izvrsnima u detektiranju nametnika, ali im se prigovara to što skeniranje traje duže nego kod ostalih, ili to što zauzimaju veliku količinu resursa (memorije, procesorskog vremena i sl.). Stoga je prilikom izbora dobro i te faktore uzeti u obzir. NOD32 npr. je veoma cijenjen zato što ima visok postotak detekcije, koristi heurističke tehnike i iznimno je lagan kad su u pitanju sistemski resursi. Ta posljednja karakteristika je možda i presudna kod korisnika koji imaju nešto slabija računala. Kaspersky je cijenjen i hvaljen po iznimnoj sposobnosti detektiranja virusa i inficiranih datoteka, ali mu neki zamjeraju što je vrlo zahtjevan po pitanju sistemskih resursa te što samo skeniranje traje dosta dugo u odnosu na neke druge takve alate.

U svakom slučaju, oni „najbolji“ programi za detekciju virusa su komercijalni alati, dakle treba ih platiti. Doduše, svaki od njih se može besplatno preuzeti i koristiti kroz određeni probni period. Postoji i mnoštvo besplatnih alata, a mnoge tvrtke koje proizvode komercijalne takve programe nude i besplatne inačice svojih proizvoda, s nekim ograničenjima. Mnogi od tih besplatnih su također vrlo cijenjeni i hvaljeni programi. Postavlja se pitanje da li je potrebno platiti da bismo imali dobru zaštitu? Mišljenje mnogih je da su i oni besplatni u većini situacija sasvim dovoljni, te da svaki program za detekciju virusa obavlja svoju funkciju, pod uvjetom da je redovno ažuriran i održavan.

Najpoznatiji komercijalni alati su:

Eset NOD32	http://www.eset.com/products/nod32.php
Kaspersky Anti-virus	http://www.kaspersky.com/kaspersky_anti-virus
Norton Antivirus	http://www.symantec.com/norton/antivirus
BitDefender Antivirus	http://www.bitdefender.com/
McAfee Anti-virus i VirusScan	http://www.mcafee.com

Najpoznatiji besplatni su:

Avast! Antivirus Home Edition http://www.avast.com/eng/avast_4_home.html
AntiVir Personal Edition Classic http://www.free-av.com/
AVG Free Anti-virus http://free.avg.com/ww.download-avg-anti-virus-free-edition

3.3.2. Programi za detekciju špijunskog koda (anti – spyware)

Programi za detekciju špijunskog koda (anti-spyware) su još jedan oblik zaštite koji sve više postaju nužnost, a ne samo dodatak. Takvi programi obično detektiraju špijunski (spyware) i reklamni (adware) kod, te možda i neke druge oblike malicioznih aplikacija. Sve više ljudi postaje svjesno činjenice da obje vrste nametnika mogu nanijeti veliku štetu; narušiti našu privatnost i krasti naše povjerljive informacije što može rezultirati raznim problemima, od krađe identiteta, do financijske štete. Zbog toga je vrlo važno imati i koristiti program za detekciju špijunskog koda .

Potreban je najmanje jedan program koji pronalazi i uklanja špijunski kod; koji bi trebao uključivati i komponentu aktivne zaštite, zaštite u realnom vremenu, kako bi komplementirao aktivnu zaštitu koju pruža program za detekciju virusa.

Mnogi besplatni programi za detekciju špijunskog koda su zapravo izvrsni u skeniranju na zahtjev, ali ne uključuju zaštitu u realnom vremenu. Isto tako, kod besplatnih obično nije dostupna opcija automatskog ažuriranja. No ipak, to nisu razlozi da ih se izbjegava. Korištenje više od jednog takvog alata koji samo skenira na zahtjev omogućit će bolju zaštitu, pokrivanje više prijetnji. Dakle, za postizanje što bolje zaštite od tih tipova računalnih nametnika dobro bi bilo odabrati jedan program za detekciju špijunskog koda koji pruža stalni nadzor u realnom vremenu, te možda i još par njih koji samo skeniraju na zahtjev. Ne možemo nikad biti sigurni da samo zato što neki program za detekciju špijunskog koda nije detektirao špijunski kod, da ga na računalu nema. Realna je mogućnost da će jedan program za detekciju špijunskog koda otkriti nametnike koje drugi neće, stoga nije naodmet imati i potporu.

Aplikacije za otkrivanje špijunskog koda skeniraju računalo u potrazi za špijunskim kodom, malicioznim reklamnim kodom i otimačima (hijacker – otimač, maliciozna aplikacija koja „otima“ web preglednik na način da prikazuje neke druge web stranice, a ne one tražene).

Nadzor u realnom vremenu skenira aktivne datoteke na računalu, tražeći inficirane.

Pravilo je isto kao i za sve zaštitne programe, da bi program za detekciju špijunskog koda (anti-spyware) bio efektivan, potrebno ga je redovno ažurirati! I naravno, redovno provoditi skeniranje. Neki imaju mogućnost automatskog skeniranja prema postavljenom rasporedu. Ako odabrani alat nema tu mogućnost, skeniranje je potrebno pokretati ručno.

Najpoznatiji besplatni programi za detekciju špijunskog koda su Ad-aware Free i Spybot Search & Destroy. Oba su hvaljeni i slove kao programi koji odlično obavljaju svoj posao. Dok je Ad-aware Free zapravo besplatna inačica Ad-aware Pro programa kod koje je samo isključena aktivna zaštita (Ad-watch) i automatsko ažuriranje; Spybot S&D je sam po sebi besplatan i nudi i aktivnu zaštitu (iako je ona standardno isključena); te isto tako, nudi i opciju imunizacije koja nudi preventivnu zaštitu od poznatih prijetnji.

Još jedan poznati besplatni takav zaštitni program je i Spyware Blaster. Taj program zapravo ima drugačiji, striktno preventivni pristup zaštiti, s fokusom na glavnu ulaznu točku – web preglednik. Nakon instalacije detektira web preglednik/e (ima podršku za Internet Explorer i Mozilla Firefox) i štiti ih od preuzimanja i instaliranja špijunskog koda. Program je besplatan, samo je za opciju automatskog ažuriranja potrebno platiti godišnju naknadu, dok je ručno ažuriranje i dalje besplatno.

Ad-aware Free	http://lavasoft.com/products/ad_aware_free.php
Spybot Search & Destroy	http://www.safer-networking.org/hr/spybotsd/index.html
Spyware Blaster	http://www.javacoolsoftware.com/spywareblaster.html

Od komercijalnih takvih alata, najpoznatiji su:

CounterSpy	http://www.sunbeltsoftware.com/Home-Home-Office/Anti-Spyware/
Spyware Doctor	http://www.pctools.com/spyware-doctor/
Ad-aware Pro	http://lavasoft.com/products/ad_aware_pro.php
SpySweeper	http://www.webroot.com/En_US

Isto tako, prilikom kupnje komercijalnih programa za detekciju špijunskog koda a potrebno je biti dosta oprezan. Veliki broj lažnih takvih programa (koji ili ne rade ili su ustvari špijunski kod) postoji na Internetu, sa svrhom prijevare i zarade na naivnim ljudima. Potrebno je paziti i dobro se informirati. Postoji dosta web mjesta na kojim se mogu naći informacije i popisi poznatijih lažnih programa za detekciju špijunskog koda a koji kruže Internetom. Jedna takva lista može se pronaći na web mjestu: www.spywarewarrior.com/rogue_anti-spyware.htm

3.3.3. Programi za detekciju trojanaca (anti – Trojan)

To su programi koji traže konkretno – trojanske konje. Trojanski konji nisu virusi, detektiranje trojanaca zahtijeva drugačije parametre. Isto tako, programi za detekciju trojanskih konja detektiraju i stražnja vrata (backdoor) i programe koji bilježe udarce tipki (key logger).

Neki proizvođači programa za detekciju virusa pružaju i alate za eliminiranje pojedinih trojanskih konja. No, iako većina programa za detekciju virusa uspješno rješava i dosta trojanaca, dostupni programi za detekciju trojanskih konja su vrlo efektivni i čine odličan dodatak zaštiti računala. Korištenjem i programa za detekciju virusa i programa za detekciju trojanaca pokriva se veći dio prijetnji i uvelike povećava otpornost sustava na maliciozni kod.

Kao i kod većine ostalih zaštitnih programa, komercijalni programi za detekciju trojanaca uključuju i nadzor u realnom vremenu, dok besplatne verzije nisu.

I za njih vrijede pravila kao i za sve ostale – redovno ažuriranje, redovna nadogradnja i redovno skeniranje računala.

Komercijalni takvi alati su npr.

Anti-Trojan Shield	http://www.atshield.com/
Trojan Hunter	http://www.misec.net/
The Cleaner	http://www.moosoft.com/TheCleaner/TheCleaner
Trojan Remover	http://www.simplysup.com/tremover/download.html
a-squared Anti-Malware	http://www.emsisoft.com/en/
Tauscan	www.agnitum.com/products/tauscan

Besplatni su npr.:

a-squared Free	http://www.emsisoft.com/en/software/free/
The Cleaner freeware	http://www.moosoft.com/cleaner5/cleaner5free.exe
Swat It	http://www.lockdowncorp.com/bots/downloadswatit.html

3.3.4. Programi za detekciju alata za dobivanje administratorskih ovlasti na sustavu (anti – rootkit)

Zbog prirode skrivanja od operacijskog sustava i ostalih programa, otkrivanje alata za dobivanje administratorskih ovlasti na sustavu (rootkit) nije jednostavan zadatak i većina standardnih zaštitnih programa ih ne može uočiti niti ukloniti.

Na tržištu postoji dosta programa za detekciju tih vrsta malicioznog koda (anti-rootkit program) koji se mogu grupirati u kategorije prema metodologiji koju koriste za detekciju. Neki na primjer, koriste detekciju potpisa. Drugi se oslanjaju na usporedbi rezultata skeniranja računala na više nivoa. Postoji mnogo tehnika, no većina ih se oslanja na heuristički pristup, traže anomalije u sustavu i bihevioralne karakteristike takvih alata.

Neki takvi zaštitni programi su vrlo obuhvatni i mogu detektirati skrivene procese, datoteke, priključne točke, pogonske programe i registarske unose raznih vrsta alata za dobivanje administratorskih ovlasti (rootkit). Drugi se koncentriraju samo na njihovu direktnu detekciju. Mnogi takvi zaštitni programi otkrivaju alate za dobivanje administratorskih ovlasti i ispisuju sve promjene koje učine na sustavu, ali ne pružaju nikakvu mogućnost njihovog uklanjanja. No, nekolicina ih ima i mogućnost otkrivanja i otklanjanja.

Programi za detekciju alata za dobivanje administratorskih ovlasti se razlikuju prema jednostavnosti uporabe. Variraju od vrlo jednostavnih programa namijenjenih početnicima, do onih koji generiraju izvješće o skeniranju koje i najiskusniji korisnici teško mogu protumačiti.

Jedan od najopsežnijih programa za detekciju i uklanjanje takvih malicioznih alata je IceSword. To je zapravo komplet pomagala za analizu sustava i detekciju i otklanjanje alata za dobivanje administratorskih ovlasti, u jednom paketu. Može detektirati većinu poznatih takvih nametnika, ali potrebno je znati interpretirati rezultate koje prikaže nakon skeniranja i znati kako efektivno „razoružati“ zloćudne alate.

GMER, također ima multifunkcionalni pristup, a u nekim slučajevima i nadilazi sposobnost detekcije koju ima IceSword, ciljajući na najsofisticiranije tehnike kakve koriste najopasniji alati za dobivanje administratorskih ovlasti.

BlackLight i UnHackMe su najjednostavniji alati za detekciju alata za dobivanje administratorskih ovlasti. BlackLight odlično otkriva skrivene procese tih alata, te datoteke i mape. No, ne može detektirati one koji koriste naprednije tehnike. Isto tako, nema mogućnost uklanjanja. Ako postoje skrivene datoteke, moguće ih je preimenovati da bi se spriječilo njihovo učitavanje prilikom podizanja sustava; čime takav zloćudni alat postaje neaktivan i nakon toga je moguće ukloniti preimenovane datoteke. Prilikom uklanjanja datoteka, potreban je oprez.

UnHackMe je definitivno najlakši i najpogodniji za početnike. Vrlo jednostavne za uporabu, te pruža i mogućnost uklanjanja alata za dobivanje administratorskih ovlasti. Moguće je odabrati opciju automatskog uklanjanja ili odabrati radnje koje će se izvršiti nad unosima pronađenim skeniranjem

Rootkit Revealer je izvrstan alat za detekciju tih nametnika koji pronalazi sve sumnjive datoteke skrivene od operacijskog sustava i ostalih programa. Analizira registre i sistemske API pozive, te upozorava na svaku pronađenu nepravilnost. Međutim, ne pruža mogućnost uklanjanja.

BlackLight i UnHackMe su komercijalni alati, dok su ostali navedeni besplatni.

IceSword	http://www.antirootkit.com/software/IceSword.htm
GMER	http://www.gmer.net/files.php
BlackLight	http://www.f-secure.com/blacklight/
UnHackMe	http://greatis.com/unhackme/buy.htm
Rootkit Revealer	http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx

Još jedan alat koji je korisno spomenuti, a može se svrstati u ovu kategoriju je Microsoftov Malicious Software Removal Tool. Taj program automatski i neprimjetno u pozadini skenira računalo u potrazi za nizom prijetnji, uključujući crve, trojance koji postavljaju stražnja vrata (backdoor Trojan) i uobičajene alate za dobivanje administratorskih ovlasti (rootkit) nakon preuzimanja novih Microsoft Windows nadopuna. Omogućuje i otkrivanje i uklanjanje svih pronađenih prijetnji, a većina korisnika nije ni svjesna tog procesa. Nova verzija programa je izdana svaki mjesec zajedno s Windows nadopunama (Windows Update).

Moguće je izvršiti i MSRT skeniranje na Internetu u bilo kojem trenutku, posjetom skenera na adresi: www.microsoft.com/security/malwareremove/default.mspx#run

Prilikom pokretanja intenzivnog skeniranja čitavog sustava programima za detekciju alata za dobivanje administratorskih ovlasti, potrebno je što više smanjiti broj lažno pozitivnih rezultata isključivanjem svih aktivnih komponenti sustava. Potrebno je zaustaviti sve aktivnosti, zatvoriti sve otvorene prozore i programe, isključiti računalo s Interneta, onemogućiti svu aktivnu zaštitu i bilo kakvo programirano skeniranje. Zapravo, trebalo bi se suzdržati od uopće korištenja računala, uključujući dodirivanje tipkovnice ili miša. Moguće je da bilo kakva aktivnost zapravo uzrokuje lažno pozitivni nalaz takvih programa. Isto tako, s obzirom na vrlo čestu pojavu lažno pozitivnih rezultata, potrebno je detaljno analizirati sve nalaze prije poduzimanja bilo kakve radnje.

Trenutno dostupni takvi zaštitni programi većinom mogu detektirati sve poznate alate za dobivanje administratorskih ovlasti. No, budući da su različiti programi usmjereni na različite tehnike, važno je kombinirati takve programe radi bolje učinkovitosti. Recimo, korištenje kombinacije Rootkit Revealer i BlackLight omogućuje da se njihove karakteristike nadopunjuju, te pruže bolju zaštitu; a usporedba njihovih rezultata skeniranja može biti od pomoći u razlučivanju stvarnih nametnika od lažno pozitivnih nalaza.

Nakon korištenja programa za uklanjanje alata za dobivanje administratorskih ovlasti preporučljivo je skeniranje računala sa ažuriranim programima za detekciju virusa (anti-virus) i špijunskog koda (anti-spyware).

3.3.5. Vatrozid

Vatrozid (firewall) je apsolutno nužna zaštita. Bez njega je računalni sustav širom otvoren većini trojanskih konja i jednostavnih hakerskih pokušaja. Hakeri redovito koriste programe za pretraživanje koje koriste za ispitivanje i traženje otvorenih priključnih točaka i aplikacijskih ranjivosti.

Nezaštićen sustav je vrlo lako kompromitirati, nakon čega se može koristiti kao sredstvo za napad na neke veće ciljeve, onemogućujući da se pravom napadaču uđe u trag. Vlasnici tih računala mogu biti držani zakonski odgovornima za zločine za koje nisu u znali da njihova kompromitirana računalna oprema izvršava. Isto tako, ti kompromitirani sustavi postaju opasnost za sve ostale korisnike.

Vatrozid je ili sklop ili aplikacija koja okružuje računalni sustav svojevrsnim štitom, ograničavajući pristup potencijalno opasnoj, neželjenoj ili skrivenoj komunikaciji računala s Internetom.

Na računalu postoji 65536 priključnih točaka (od 0 do 65535), ali samo manji broj ih je aktivno korišten čitavo vrijeme. IANA (Internet Assigned Numbers Authority) je organizacija zadužena za dodjeljivanje priključnih točaka za specifičnu uporabu. Većina kućnih korisnika koristi vrlo mali broj dodijeljenih priključnih točaka. Dvije priključne točke određene su za slanje (priključna točka 25) i primanje (priključna točka 110) elektroničke pošte i koristi ih većina korisnika, te priključna točka 80 koji se koristi za traženje i primanje web stranica.

Kućni korisnici standardno koriste manje od 25 priključnih točaka za svakodnevnu komunikaciju na Internetu. Ostale, nekorištene priključne točke su generalno nepotrebne pa je poželjno i sigurno blokirati ih, onemogućiti im komunikaciju s Internetom. Zapravo, ako te priključne točke nisu blokirane, mogu ih iskoristiti maliciozni programi, potpuno neprimjetno. Blokiranje nekorištenih priključnih točaka je jedna od najvažnijih funkcija vatrozida. Dobro je i ograničiti koje aplikacije mogu koristiti potrebne priključne točke. Blokiranje ili dopuštanje aplikacijama korištenje potrebnih priključnih točaka ili pristup Internetu u potpunosti je još jedna važna funkcija koju imaju vatrozidi.

Dvije osnovne vrste vatrozida koje postoje su sklopovski i aplikacijski vatrozidi. Aplikacijski vatrozidi se instaliraju kao bilo koji drugi program na računalu. Sklopovski vatrozidi ugrađeni su u sklopovlje.

Sklopovski vatrozid je maleno nisko-naponsko računalo u zasebnoj kutiji koje je smješteno između širokopojasnog modema i korisnikovog računala ili računala spojenih u lokalnu mrežu (LAN). Ispravno ime za takav uređaj je sklopovski usmjernik (hardware router)

Sklopovski vatrozid je izvrsna zaštita protiv upada u sustav. Ako se napadač uspije probiti, sve što će naći je prazan prostor. Sklopovlje nema nikakvih programa koji mogu biti iskorišteni za pristup aplikacijama na računalu. No, iako mogu spriječiti ili omesti pokušaj napada i probijanja u sustav, sklopovski vatrozidi ne pružaju nikakvu zaštitu od malicioznih programa koji inficiraju računalo putem malicioznih web mjesta ili instalacijom neke aplikacije. Isto tako, ne mogu zaštiti od malicioznih aplikacija koje se potajno same pokreće unutar legitimnih sistemskih procesa.

Dostupni su usmjernici koji uključuju sklopovski vatrozid, kao i samostalni sklopovski vatrozidi. Moguće ih je kupiti po razumnim cijenama, dok su oni najpoznatiji i navodno najkvalitetniji iznimno skupi.. Proizvođači najpoznatijih sklopovskih vatrozida su tvrtke kao što je CISCO ili D-link. Uobičajene cijene takvih uređaja su za obične korisnike ipak prevelike, ili jednostavno neželjeni trošak.

Sklopovski vatrozidi su preporučena zaštita za mreže, bežične mreže, a za širokopojasni Internetu mogu služiti kao dodatna zaštita korisnicima koji to žele. Međutim, običnim korisnicima takva dodatna zaštita nije potrebna, dobar aplikacijski vatrozid je sasvim dovoljan. Zapravo, u svakom slučaju, aplikacijski vatrozid je nužan, bez obzira da li se koristi sklopovski vatrozid ili ne.

Osnovna razlika između sklopovskih i aplikacijskih vatrozida je u tome što aplikacijski vatrozidi mogu kontrolirati i izlazni i ulazni pristup, ovisno o tome koja aplikacija prima ili šalje pakete.

Aplikacijski vatrozidi rade koristeći nekoliko komponenti ugrađenih duboko u jezgru operacijskog sustava. Te komponente presreću ulazne i izlazne pakete prije nego su procesirani i prije nego im je dopušten pristup višim nivoima sustava. Budući da su ugrađeni tako duboko u operativnom sustavu mogu nadgledati svaki paket i vidjeti koje aplikacije pokušavaju poslati pakete ili osluškuju pristigle; tako da mogu blokirati pakete u slučaju da šalje ili prima nepoznat program ili program kojemu je to zabranjeno. Taj proces se može generalno nazvati aplikacijska kontrola paketa na temelju pravila (software rule-based packet control). Vatrozidi koriste postavke, pravila (firewall rules) da bi znali što blokirati, a što ne.

Pravila se mogu kreirati ručno ili usput, postavljanjem vatrozida u stanje „učenja“. Korištenjem učenja za postavljanje pravila, vatrozid će upozoravati na radnje ili aplikacije u hodu, kako se događaju. Kad prikaže upozorenje, korisnik može odobriti radnju ili je zabraniti jednokratno, a može i odrediti da se odabir zapamti i usvoji kao pravilo. U tom slučaju više se neće ponavljati to isto upozorenje za tu istu radnju, već će se primijeniti pravilo. Taj postupak može se činiti kao vrlo zamoran, ali obično i nije toliko. Naravno, potrebno je određeno razdoblje „treniranja“ vatrozida, ali ne oduzima toliko vremena. Većina boljih aplikacijskih vatrozida već ima postavljena pravila za najpoznatije web preglednike i e-mail klijente i za većinu komponenti koje koristi operativni sustav, a koje zahtijevaju mogućnost pristupa Internetu.

Vatrozidi pohranjuju zapise o svim blokiranim pokušajima pristupa. Možda bi bilo korisno povremeno pregledati te zapise, jer mogu otkriti neke korisne informacije. Možemo utvrditi koji su procesi pokušali uspostaviti udaljenu vezu i slati pakete podataka. To nam može uvelike pomoći u otkrivanju potencijalnih malicioznih aplikacija na računalu, možda neka stražnja vrata (backdoor) koja pokušavaju uspostaviti vezu s napadačem i sl.

Aplikacijski vatrozidi također trebaju biti redovno ažurirani, kao i ostali zaštitni programi. Razlozi tomu su mnogi, uključujući ispravljene greške, dodatne sigurnosne komponente ili funkcionalnosti, konflikti s drugim aplikacijama i sl. Većina trenutno dostupnih vatrozida pruža mogućnost automatskog ažuriranja.

Većina aplikacijskih vatrozida također omogućuje skrivanje priključnih točaka (port stealthing), što je uvijek bolje od blokiranja priključnih točaka.

Postoje web mjesta na kojima je moguće izvršiti provjeru vatrozida i utvrditi da li su priključne točke dobro zaštićene. Primjer takvog web mjesta je Steve Gibsonov www.grc.com, koji nudi mnoštvo korisnih informacija vezanih za sigurnost i nekoliko dostupnih testova. Na web stranici ShieldsUP! do koje vodi poveznica s naslovne stranice moguće je odabrati između nekoliko testova, od kojih je za testiranje zaštite priključnih točaka potrebno odabrati „All Service Ports test“. Odabirom te opcije provest će se testiranje zaštite svih priključnih točaka od 0 do 1055, unutar kojih su sve priključne točke koje će gotovo svaki uobičajeni korisnik ikad trebati. Nakon testiranja prikazuju se rezultati za sve priključne točke. Zelena boja označava skrivene priključne točke (stealth), plava boja označava priključne točke koje nisu skrivene, ali su blokirane, dok crvena boja označava prisutnost otvorenih i nezaštićenih priključnih točaka, a to je jasna ranjivost koju treba eliminirati što prije. Naravno, najbolji rezultat bi bio prikaz svih priključnih točaka u zelenoj boji, što znači da su skriveni, odnosno zaštićeni na najbolji način.

Za efektivnu sigurnost treba koristi samo jedan aplikacijski vatrozid. Istovremeno korištenje dva vatrozida može rezultirati njihovom kolizijom i rezultati mogu biti nepredvidivi. To je također bitno zbog činjenice da kod Windows XP SP2 operativnih sustava standardno uključen ugrađeni Windows vatrozid.

Windows vatrozid ili ICF (Internet Connection Firewall) je uredu za neke minimalne sigurnosne zahtjeve, ali za efektivnu zaštitu potrebno je koristiti neki drugi vatrozid. Osnovni razlog zbog kojeg je ugrađeni Windows vatrozid neadekvatan je činjenica da je jednosmjeran, nema mogućnost blokiranja odnosno nadzora izlaznog prometa. Neke vrste virusa i trojanskih konja ga mogu čak i onemogućiti, potpuno isključiti. Prednost Windows vatrozida je da pruža osnovnu zaštitu onih neopreznih korisnika koji inače ne bi obratili pozornost na potrebu dobre zaštite i ne bi uopće instalirali vatrozid. Novi Windows vatrozid, automatsko ažuriranje i Sigurnosni centar su poboljšanja uvedena sa SP2, koji ciljaju najviše na upravo takve korisnike i njihovu zaštitu. Svi ostali savjesni korisnici trebali bi isključiti taj zadani vatrozid unutar Sigurnosnog centra (u upravljačkoj ploči) i instalirati neki drugi vatrozid.

Dostupan je velik broj kvalitetnih vatrozida na tržištu, a mnogi vrlo efektivni i hvaljeni aplikacijski vatrozidi su i besplatni za kućnu uporabu. Postoje oni koji su sami po sebi besplatni, a dostupne su i besplatne verzije poznatih komercijalnih vatrozida. Oni komercijalni obično nude besplatnu upotrebu kroz određeni probni period (trial)

Najpoznatiji komercijalni aplikacijski vatrozidi su:

Zone Alarm Pro	www.zonealarm.com
Agnitum Outpost Firewall	http://www.agnitum.com/products/outpost/index.php
CA Personal Firewall	http://shop.ca.com/firewall/personal_firewall.aspx
Sunbelt Personal Firewall	http://www.sunbeltsoftware.com/Home-Home-Office/
Online Armor Personal Firewall v2	http://www.tallemu.com/

Najpoznatiji besplatni vatrozidi su:

Comodo Firewall Pro	http://www.personalfirewall.comodo.com/
Zone Alarm Free	http://www.zonealarm.com/
Online Armor Free	http://www.tallemu.com/

3.3.6. Sigurnosni paketi

Pored svih pojedinih zaštitnih alata, još jedan oblik zaštite dostupan je korisnicima, a to su sigurnosni paketi. Kompleti alata koji obično ujedinjuju vatrozid, alat za detekciju virusa, alat za detekciju špijunskog koda, filtriranje sadržaja, zaštitu od neovlaštenog traženja informacija (phishing) i razne druge komponente u jedan paket. Iako su to poprilično veliki proizvodi, cilj je da budu sva potrebna zaštita na računalu. Prednosti takvih sigurnosnih paketa su komotnost koju pruža konfiguriranje i upravljanje samo jednim proizvodom, te uska integracija svih sigurnosnih komponenti koja omogućuje veću učinkovitost.

Kvaliteta takvih paketa procjenjuje se prema kvaliteti svih komponenti, konfigurabilnosti, lakoći uporabe, zahtjevu za sistemskim resursima i naravno učinkovitosti. Svi takvi sigurnosni paketi su komercijalni proizvodi.

Najpoznatiji su:

Kaspersky Internet Security	http://www.kaspersky.com/kis_latest_versions
ESET Smart Security	http://www.eset.com/smartsecurity/
Panda Platinum Internet Security	http://www.pandasecurity.com/
Norton Internet Security	http://www.symantec.com/norton
Trend Micro Internet Security	http://us.trendmicro.com/
McAfee Internet Security Suite	http://us.mcafee.com/root/Package.asp?pkgid=273

3.3.7. Alati za analizu sigurnosti sustava

Pored svih zaštitnih programa, korisno bi bilo instalirati i upoznati se s programima za analizu sigurnosti sustava. Takvi alati omogućuju istraživanje dijelova sustava na koje maliciozni programi često utječu. Sistematsko nadgledanje sustava pomoću tih alata omogućuje uočavanje anomalija prije nego se pretvore u veći problem.

Kao primjer, tvrtka Sysinternals (tvrtka koju je kupio Microsoft) pruža besplatno preuzimanje nekih od najboljih alata za analizu Windows sustava.

Neki od mnoštva ponuđenih alata pružaju mnogo bolje zamjene za alate koji su ugrađeni u Windows XP operacijski sustav, kao što su Windows Task Manager (Process Explorer), TCPView (NetStat), Autoruns (MSConfig) i sl.

Čitav popis tih besplatnih alata, opisi i preuzimanje moguće je putem web stranice
http://technet.microsoft.com/en-us/sysinternals/bb545027.aspx

3.4. AŽURIRANJE OPERACIJSKOG SUSTAVA I APLIKACIJA

Kad je riječ o održavanju računala sigurnim, najvažnija stvar koja se može napraviti je redovno preuzimanje i instaliranje najnovijih nadogradnji, dopuna i zakrpa. Zaštitni programi svakako pridonose sigurnosti sustava, ali napadi i maliciozni programi obično iskorištavaju poznate propuste i ranjivosti. Ako je računalo zaštićeno svim dopunama i zakrpama, te ranjivosti više ne postoje, pa napadi i maliciozan kod obično neće funkcionirati. Potrebno je biti dobro informiran o najnovijim otkrivenim propustima i ranjivostima, te redovno instalirati zakrpe i dopune koje će te ranjivosti eliminirati.

3.4.1. Ažuriranje Windows operacijskog sustava (Windows Update)

Windows XP je izniman operacijski sustav. Sastavljen je od milijuna linija programskog koda (otprilike četrdesetak). Unutar tog mnoštva linija koda provukla se nesumnjivo i prilična količina grešaka (bug). To je razumljivo i ne može se izbjeći.

No ipak, Microsoft se trudi držati stvari pod kontrolom izdavanjem zakrpa da bi učinio svakog korisnika i njegov operacijski sustav sigurnijim. Tu u priču ulazi ažuriranje Windows operacijskog sustava (Windows Update). Kako greške bivaju otkrivene i identificirane, ispravljaju se, a one ozbiljnije eliminiraju pomoću dopuna i zakrpa (update, patch, hotfix). Kako se dopune akumuliraju, sakupljaju se i izdaju kao komplet, u obliku uslužnih paketa (service pack).

Da bi korisnik bolje razumio rizik koji nosi pojedina otkrivena ranjivost ili greška, svakoj sigurnosnoj prijetnji dodijeljena je tzv. ocjena težine (severity rating). Kao generalno pravilo sve dopune označene kao kritične (Critical) ili važne (Important) trebale bi biti instalirane čim prije. One s ocjenom umjerene (Moderate) ili niske (Low) težine ne predstavljaju ozbiljan rizik, ali ipak mogu na neki način utjecati na operacijski sustav.

Ažuriranje sustava može se obaviti ručno ili automatski.

Ručno ažuriranje obavlja se posjećivanjem Microsoftovog web mjesta (http://windowsupdate.microsoft.com/) na kojem se mogu naći sve potrebne zakrpe, dopune ili nadogradnje. Moguće je samostalno pregledati sve dostupne i odabrati željene zakrpe i dopune, a moguće je i odabrati opciju da se skenira računalo te prikažu sve zakrpe i dopune koje je potrebno primijeniti na konkretno računalo. Isto tako, moguće je odabrati automatsku instalaciju svih predloženih datoteka, ili odabrati one koje želimo preuzeti.

Potrebno je imati na umu podatak da se mjestu za Windows ažuriranje može pristupiti samo preko Internet Explorera. Pristup tom web mjestu pomoću drugih preglednika nije dopušteno.

Osim ručnog ažuriranja, postupak je moguće konfigurirati da se odvija automatski, pomoću ugrađene funkcije automatskog ažuriranja (Automatic Updates). Kao što samo ime kaže, taj usluga automatski provjerava i traži nove zakrpe i dopune koje utječu na sigurnost sustava. Funkciju automatskog ažuriranja moguće je konfigurirati pomoću predviđenog dijaloškog okvira do kojeg je moguće doći desnim klikom na Moje računalo (My Computer) i odabirom Svojstva (Properties), te zatim kartice Automatsko ažuriranje (Automatic Updates).

Moguće je odabrati između nekoliko postavki koje određuju kako će funkcionirati automatsko ažuriranje. Ako je automatsko ažuriranje uključeno, moguće je odrediti da se sve predložene datoteke za ažuriranje automatski preuzimaju i instaliraju u neko određeno vrijeme. Moguće je i odabrati postavku da se sve datoteke preuzimaju, ali ne instaliraju samostalno ili da se korisnika samo obavijesti o novim dopunama i zakrpama, a da on sam odluči što i kako želi preuzeti. Dostupna je i opcija potpunog isključivanja te usluge.

Usluga automatskog ažuriranja je vrlo korisna, a za neke korisnike i idealna ako ne žele da se gnjave ili da ih sustav gnjavi, već da sve sam obavi. Međutim, neke je dodatne faktore također

potrebno uzeti u obzir. Prvo, usluga automatskog ažuriranja samo instalira dopune visokog prioriteta koje direktno utječu na sigurnost računala. Zbog toga je isto tako potrebno redovno posjećivati web mjesto za ažuriranje Windows operacijskog sustava i pregledati ostale ponuđene dopune i nadogradnje.

Drugo, iako postavljanje svakodnevnog automatskog ažuriranja u određeno vrijeme može uštedjeti dosta vremena i gnjavaže, jer se sve odvija neprimjetno u pozadini, potrebno je imati na umu i to da neke zakrpe mogu izazvati i razne probleme. Možda je najbolje pričekati neki period, možda tjedan ili dva, u slučaju da se ispostavi da je neka zakrpa problematična.

Automatsko ažuriranje definitivno treba biti uključeno, ali je s obzirom na spomenuto, možda najbolje odabrati opciju samo obavještavanja o novim dopunama i zakrpama, te pričekati i dobro ih provjeriti prije preuzimanja i instaliranja.

Microsoft redovno objavljuje kratak pregled (www.microsoft.com/technet /security/current.asp) (Security Bulletin) svih sigurnosnih zakrpa kao i članke vezane za njih, u bazi znanja (Knowledge Base). Microsoft također izdaje i sigurnosne savjete (Security Advisory) (www.microsoft.com/technet/security/advisory/default.mspx). Moguće je i pretplatiti se na redovno primanje obavijesti putem elektroničkih biltena (Newsletter) (www.microsoft.com/technet/security/bulletin /notify.asp).

Svi ti resursi mogu se pokazati korisnim izvorom informacija. No opet, to su informacije koje izdaje sam Microsoft. Stoga je možda ipak bolje potražiti i malo dalje. Postoje razna web mjesta na kojima je moguće vidjeti da li, i kakve probleme izaziva neka zakrpa. Razne revizije, izvješća ljudi koji su imali problema s nekim zakrpama, članci i sl. Primjer takvog web mjesta je recimo AskWoody.com na kojem se redovno održava stranica s procjenom pouzdanosti Microsoftovih zakrpa (Microsoft Patch Reliability Ratings). „Windows secrets“ (Windows tajne), web mjesto i brošura Briana Livingstona također redovno sadrži revizije zakrpa i njihovih nuspojava.

Još jedna dobra ideja je izvršiti Google pretragu neke zakrpe prije instaliranja.

Daleko najdetaljnije informacije mogu se naći u obavijesnim skupinama (newsgroup), forumima i sličnim mjestima, iako podaci pronađeni na takvim mjestima mogu biti subjektivni, pa im nije dobro potpuno vjerovati. No, u svakom slučaju, svaki podatak o mogućim problemima koje izaziva neka zakrpa je uvijek dragocjen. Bolje je biti siguran, jer nekad problemi koji nastaju mogu biti veliki.

3.4.2. Uslužni paketi (Service Pack)

Sigurnosna nadopuna je zakrpa koja rješava samo jedan, pojedini sigurnosni problem, dok je uslužni paket (Service Pack) opsežna kolekcija nadopuna koje su grupirane kao jedan veliki paket. Kao generalno pravilo, uslužni paket uključuje sve sigurnosne nadopune koje su mu prethodile, kao i neke manje ispravke i poboljšanja koja nisu vezana za sigurnost. Na taj način, instalacijom uslužnog paketa unaprjeđuje se čitav operacijski sustav, ne samo sigurnosni aspekti. Isto tako, uslužni paketi su kumulativni, zbirni – dovoljno je instalirati samo posljednji uslužni paket, nije potrebno instalirati i one ranije izdane. Prilikom instalacije novog uslužni paketa, nije potrebno ukloniti one starije, ako su ranije instalirani.

Sa sigurnosnog stajališta, preporučljivo je imati instaliran posljednji uslužni paket. U slučaju da se to ne učini, moguće je da će nedostajati neke vrlo važne sigurnosne nadopune i sustav će biti izložen riziku.

Uslužni paket 1

Uslužni paket 1 (Service Pack 1 - SP1) izdan je 9. rujna 2002. godine. Sadrži razne sigurnosne i operativne ispravke i nadopune, poboljšanje pouzdanosti sustava, Microsoft .NET Framework,

ugrađenu potporu za korištenje novih uređaja kao npr. Tablet PC i novu verziju Windows Messengera, verziju 4.7. Najuočljivije nove mogućnosti su potpora za USB 2.0, te novo pomagalo u upravljačkoj ploči, unutar opcije Dodaj ili ukloni programe (Add or remove programs) – opcija Postavi pristup programu i zadane vrijednosti (Set Program Access and Defaults). To novo pomagalo omogućuje određivanje zadanih programa za pojedine aktivnosti kao pregledavanje weba ili slanje e-pošte, kao i skrivanje pristupa nekim ugrađenim programima (Internet Explorer, Outlook Express, Windows Messenger, Java Virtual Machine i Windows Media Player). Dakle, omogućuje se korištenje npr. nekog drugog web preglednika ili e-mail klijenta osim ugrađenih, kao glavne, zadane. To je pomagalo prvi put uvedeno kod Windows 2000 operacijskog sustava, sa uslužnim paketom 3. U Uslužni paket 1 dodan je i Microsoftov JVM (Java Virtual Machine), kao i potpora za IPv6 (IP - Internet protokol verzije 6)

U veljači 2003. godine (3. veljače) Microsoft je izdao i Uslužni paket 1a (SP1a). Jedina razlika između stare i te nove verzije uslužnog paketa je što je kod verzije 1a samo izbačen Java Virtual Machine (zbog tužbe tvrtke Sun Microsystems)

Uslužni paket 2

Uslužni paket 2 (Service Pack 2 - SP2), kodnog imena „Springboard“ izdan je 6. kolovoza 2004. godine, nakon nekoliko odgoda. Nakon konačnog izdavanja, uslužni paket 2 učinio je Windows XP mnogo sigurnijim i pouzdanijim i vrlo brzo postao gotovo sastavni dio svake nove instalacije Windows XP operacijskog sustava.

Unesene su mnoge izmjene i dopune operacijskog sustava i pojedinih njegovih elemenata, kao i ugrađenih aplikacija. Dodane su i neke nove funkcionalnosti uključujući poboljšanu Wi-Fi potporu i čarobnjaka za jednostavno postavljanje bežične mreže i potporu za Bluetooth.

Uslužni paket 2 unosi nova sigurnosna unaprjeđenja, uključujući veliku reviziju ugrađenog vatrozida koji je preimenovan u Windows vatrozid (Windows firewall) i standardno uključen. Donosi i značajnu novinu, Windows sigurnosni centar (Windows Security Center) unutar upravljačke ploče koji omogućuje pregled i konfiguriranje općenite sigurnosti sustava, na jednoj lokaciji, uključujući status ugrađenog vatrozida, Windows ažuriranje (Windows Update - status i postavke automatskog ažuriranja), te status aplikacije za detekciju virusa (redovno se provjerava da li je instalirana i ažurirana). Ako je ugrađeni vatrozid isključen, sigurnosni centar redovno provjerava da li se koristi neki drugi vatrozid. U slučaju da vatrozid ili program za detekciju virusa ne postoji, isključen je ili nije ažuriran, sigurnosni centar upozorava korisnika na to. Ustvari, ako nastane bilo kakav problem s vatrozidom, programom za detekciju virusa ili automatskim ažuriranjem, pojavljuje se ikona koja označava problem i prikazuje odgovarajuća poruka.

Nadalje, neka sigurnosna unaprjeđenja unesena su u pregledavanje weba i rad s elektroničkom poštom. Pored općenitog unaprjeđenja sigurnosti i stabilnosti, dodane su i neke nove mogućnosti. U Internet Explorer dodana je funkcija blokiranja privremenih (pop-up) prozora (koja je standardno uključena), te sprečavanje preuzimanja i izvršavanja potencijalno štetnog sadržaja bez znanja korisnika.

Kod Outlook Expressa blokirano je prikazivanje slika unutar e-mail poruka s ciljem reduciranja spama. Isto tako, spriječeno je otvaranje potencijalno štetnog sadržaja u privitcima e-mail i trenutnih poruka (instant messaging).

Izmjene kod Internet Explorera i Outlook Expressa mogu zapravo stvoriti probleme nekim korisnicima zbog onemogućavanja nekih funkcija, zbog čega može doći do teškoća s pregledavanjem nekih web stranica ili primanjem elektroničke pošte. Instalacijom uslužnog paketa 2 sve postavke Internet Explorera i Outlook Expressa vraćaju se na standardne, zadane vrijednosti. Za postizanje (ili vraćanje) željene funkcionalnosti možda je potrebno dodatno konfiguriranje postavki web preglednika i e-mail klijenta i izmjene postavljenih vrijednosti.

Uslužni paket 3

Nakon nekoliko testnih verzija (Release Candidate), konačna verzija uslužnog paketa 3 izdana je 6. svibnja 2008. godine. Nakon objave vrlo brzo je uključena u automatske nadopune. Ukupno 1174 stavke uključene su u treći uslužni paket.

U SP3 sadržane su sve prethodno izdane sigurnosne i operativne zakrpe i nadopune; kao i ranije objavljene nadogradnje, uključujući nadogradnju MMC-a (Microsoft Management Console) na verziju 3, WPA (WiFi Protected Access) na verziju 2, Windows Installer 3.1 verzija 2, MSXML 6, RDP 6 (Remote Desktop Protocol) i ostalo.

Od novih mogućnosti i funkcija koje su uključene u treći uslužni paket, najznačajnije su:

- potpora za NAP (Network Access Protection) kojom je mrežnim administratorima omogućeno postavljanje pravila, politike sistemske konfiguracije i zdravlja koje je potrebno zadovoljiti da bi se omogućila komunikacija. Ta funkcionalnost omogućava interakciju s NAT funkcijom ugrađenom u Windows Vista i Windows Server 2008.
- detekciju „crne rupe“ kod usmjernika („Black hole“ router detection) – dodavanjem te funkcionalnosti, koja je standardno uključena, sustav može detektirati usmjernike koji neispravno odbacuju pakete (odbacuju ih bez dojave). To je također funkcionalnost preuzeta iz Windows Vista operacijskog sustava
- kriptografski modul (Kernel Mode Cryptographic Module) – novi jezgreni modul koji sadrži implementaciju i potporu za nekoliko različitih kriptografskih algoritama – SHA2 algoritmi raspršivanja (SHA256, SHA384 i SHA512)
- kao i kod Windows Vista i Windows Server 2003 SP2 operacijskih sustava, moguće je izvršiti kompletnu instalaciju operacijskog sustava (Windows XP SP3) bez upisivanja ključa. Operacijski sustav traži od korisnika unošenje ključa kasnije, kao dio „Genuine Advantage“ funkcije.

SP3 vrijedi samo za 32-bitne verzije operacijskog sustava. Moguće ga je instalirati na sustave koji koriste Internet Explorer verzije 6 i 7 i Windows Media Player verzije 9 i više. Unatoč ranijim pretpostavkama, u SP3 nije uključen Internet Explorer 7.

Iako je u pravilu svaki uslužni paket integracija prethodnih paketa i ostalih nadopuna, sada se navodi da je potrebno instalirati barem SP1, a preporučuje se (iako nije potrebno) instalirati SP2, prije instaliranja SP3.

Prije instalacije SP3 potrebno je obratiti pozornost na neke uvjete koji trebaju biti ispunjeni. Pored logične činjenice da mora biti dovoljno slobodnog prostora na tvrdom disku (minimalno 1500 MB), možda je potrebno i privremeno isključiti program za detekciju virusa (ovisno o tome da li dopušta izmjenu sistemskih datoteka). Isto tako, SP3 nije moguće instalirati ako su na računalu već instalirane nadopune:

- Microsoft Shared Computer Toolkit
- Remote Desktop Connection (RDP) 6.0 MUI pack (Update 925877 for Windows XP).

Ako su instalirane, potrebno ih je ukloniti prije instalacije SP3.

Iako se uvijek preporučuje imati instaliran najnoviji uslužni paket, potrebno je istaknuti i to da je već objavljen popis (release notes) nekoliko problema koji mogu nastati instalacijom SP3. Problemi koji mogu nastati su:

- Internet Explorer: U slučaju da je na računalu prije instalacije SP3 instaliran Internet Explorer 7 ili beta verzija Internet Explorera 8, nakon instalacije uslužnog paketa više nije moguće ukloniti Internet Explorer. Da bi se izbjegao taj problem, potrebno je paziti da te verzije preglednika nisu instalirane prije SP3. U slučaju da je problem već nastao,

potrebno je deinstalirati SP3, zatim deinstalirati Internet Explorer i nakon toga reinstalirati SP3.

- Microsoft Dynamics Retail Management System: u slučaju korištenja Microsoft Dynamics RMS-a (Store Operations ili Headquarters) prije instalacije SP3, potrebno je instalirati nadopune vezane za Microsoft Dynamic RMS; u protivnom bi moglo doći do gubitka podataka, funkcionalnosti ili rušenja aplikacija. Za ispravak problema potrebno je potražiti da li je dostupna odgovarajuća zakrpa.
- Multilingual User Interface (MUI) Pack – kod instalacije SP3 na računalo sa SP2 i višejezičnim korisničkim sučeljem i nakon odabira drugog jezika neki elementi ostat će na engleskom jeziku. Za ispravak tog problema potrebno je preuzeti Multilingual User Interface Pack nadopunu za Windows XP SP3
- Remote Desktop Connection: ako je na ranije računalu instalirana predverzija Remote Desktop Client 6.1 (KB 937468), nakon instalacije SP3 na zaslonu će se neprestano ispisivati poruka – samo za svrhe testiranja („For testing purposes only. Build 2600.xp_sp2_gdr...“) i neće biti moguće deinstalirati KB 937468 korištenjem opcije Dodaj ili Ukloni programe. Da bi se izbjegao taj problem potrebno je ukloniti KB 937468 prije instalacije SP3. Za ispravak tog problema, ako je već nastao, potrebno je ukloniti testni certifikat koji je odgovoran za prikaz te poruke.
- Skripte: U slučaju da se promjene regionalne i jezične postavke na neke različite od onih koje su bile korištene kad je uslužni paket instaliran, određeni aspekti VBScripta (kao DateValue () funkcija) i Jscripta (kao toLocaleString metoda) neće funkcionirati ispravno. Na primjer, takve skripte će prikazivati datum, vrijeme brojeve ili valute u netočnom formatu. Za ispravak problema potrebno je potražiti odgovarajuću zakrpu.

Ti otkriveni problemi sa SP3 su dodatna potpora tvrdnji da je najbolje pričekati određeno vrijeme prije instaliranja najnovijih nadopuna.

3.4.3. Ažuriranje instaliranih aplikacija

Ažuriranje operacijskog sustava najnovijim nadopunama i uslužnim paketima je naravno veoma važno, ali isto tako potrebno je obratiti pozornost na ostale instalirane aplikacije. Nije toliko uobičajeno da su individualni programi podložni istim vrstama sigurnosnih prijetnji kao operacijski sustav, ali se ipak događa. Kod bilo kojih programa, kao što su vatrozidi ili odabrani web preglednik, moguće je da trenutno instalirana verzija nekog programa zapravo predstavlja sigurnosni rizik. Zato je potrebno paziti na status i ostalih programa i redovno primjenjivati posljednje zakrpe i nadopune i za njih. Najbolji način na koji se može biti informiran o najnovijim dostupnim nadopunama je provjeravanje na web mjestu proizvođača pojedinog programa. Većina tih web mjesta uključuje i odjeljak posvećen potpori, preko kojeg je moguće preuzimati nadopune kako se izdaju. Za uvid u točnu verziju nekog programa koja je instalirana na računalu, dovoljno je kliknuti Pomoć -> O programu (Help -> About Program) unutar prozora programa.

Postoji i mnoštvo web mjesta koja nude sigurnosne preporuke i otkrivene ranjivosti vezane za pojedine programe, kao i najnovije otkrivene prijetnje, kao na primjer virusi i sl. Primjeri takvih web mjesta su:

CERT Coordination Center — www.cert.org
Bugtraq — www.securityfocus.com/archive/1
Secunia — www.secunia.com
CIAC — www.ciac.org

3.5. POSTAVKE OPERACIJSKOG SUSTAVA

3.5.1. Korisnički računi i grupe

Korisnički računi (user accounts) služe za kontroliranje pristupa podacima i resursima računala. Na najnižem nivou, korisnički račun nije ništa više od objekta na Windows XP sustavu koji predstavlja pojedinog korisnika, objekta definiranog korisničkim imenom i eventualno (bilo bi dobro) lozinkom.

Korisnički računi predstavljaju osnovu na koju se svi ostali sigurnosni koncepti i mehanizmi oslanjaju. Zapravo, korisnik može instalirati bilo kakav zaštitni program, od vatrozida do anti – programa, a sav trud je uzalud ako se korisnički računi ispravno ne implementiraju i propisno ne zaštite. Pravilnim konfiguriranjem korisničkih računa i postavki vezanih za njih, te njihovim pravilnim korištenjem moguće je uvelike ojačati sigurnost sustava.

Pristup i postavke za sve one korisničke račune kojima je moguće lokalno pristupiti moguć je odabirom Upravljačka ploča -> Korisnički računi (Control Panel -> User Accounts)

Postoji više vrsta korisničkih računa koji pružaju različite količine prava i privilegija na sustavu. Windows XP uključuje pet različitih tipova korisničkih računa: administratorski račun (Computer Administrator account), ograničeni račun (Limited account), standardni račun (Standard account), gost korisnički račun (Guest account) i specijalni korisnički račun (Special user account).

Administratorski korisnički račun ima najvišu razinu privilegija, potpunu kontrolu nad sustavom i pravo izvršavanja bilo kakve radnje na računalu. Jedino ograničenje je da administrator ne može obrisati svoj račun ili promijeniti vrstu u ograničeni ako je to jedini, dakle, na računalu mora postojati barem jedan administratorski račun.

Ograničeni korisnički račun je osmišljen za svakodnevnu uporabu. Ograničenja se sastoje u tome da nema privilegija instalirati sklopovski uređaj, ni aplikaciju i ne može mijenjati sistemsku konfiguraciju ili brisati važne datoteke. Cilj je da se spriječi korisnike da učine neke potencijalno štetne ili opasne izmjene na sustavu.

Standardni korisnički račun uključuje se kada Windows XP (Professional) sustav postane dijelom mrežne domene. Sličan je ograničenom računu, samo što ima mogućnost instaliranja sklopovlja i aplikacija dok god radnja ne utječe na ostale korisnike.

Gost račun služi uglavnom za korisnike koji nemaju svoj korisnički račun. Vrlo je ograničen, standardno isključen i nema postavljenu lozinku (i ona se ne može postaviti klasičnim pristupom lokalnim korisničkim računima). Zbog svojih postavki predstavlja sigurnosni rizik i najbolje ga je ostaviti isključenim i ne koristiti.

Iako specijalni korisnički račun tehnički gledano ne postoji, ponekad se može naići na dodatne korisničke račune osim ovih postavljenih. U nekim situacijama, neki programi zahtijevaju stvaranje korisničkog računa, da bi ispravno radili. Takvi korisnički računi su obično skriveni od korisnika, iako su ponekad i vidljivi. Takvi (vidljivi) računi, kao što je npr. ASP.NET račun (kojeg u određenoj situaciji kreira .NET framework) ne predstavljaju sigurnosni rizik i moguće ih je ukloniti. Postoje i drugi skriveni korisnički računi koje, osim pojedinih aplikacija kreira i operacijski sustav. Sve korisničke račune, uključujući one skrivene moguće je vidjeti odabirom:

Upravljačka ploča -> Administrativni alati -> Upravljanje računalom -> Lokalni korisnici i grupe -> Korisnici (Control Panel -> Administrative tools -> Computer Management -> Local Users and Groups -> Users). Unutar tog dijaloškog okvira moguće je mijenjati sve postavke vezane za sve korisničke račune (mijenjanje vrste korisničkog računa, preimenovanje, dodavanje, mijenjanje i resetiranje lozinki, isključivanje i brisanje korisničkih računa), kao i dodavati nove.

Ako se više korisnika služi jednim računalom, obično svaki koristi svoj korisnički račun, kako bi mogao imati vlastitu mapu Moji dokumenti, te personalizirati sustav, prilagoditi postavke vlastitim željama i ukusu. Međutim, veći broj korisničkih računa znači i veći broj meta potencijalnom napadaču. Stoga je važno ograničiti broj korisničkih računa. U nekom obiteljskom kućnom okruženju na primjer, koristiti odvojene korisničke račune za odrasle, a imati jedan zajednički za djecu. U svakom slučaju, potrebno je ukloniti sve dupliciranе ili nekorištene korisničke račune.

Budući da najvišu razinu privilegija ima administratorski račun, to je korisnički račun na koji napadači najčešće ciljaju, i naravno onaj kojega treba najviše zaštititi. Većina ljudi zna da Windows XP operacijski sustav postavlja korisnički račun nazvan Administrator, te da je prilikom instalacije postavljen bez lozinke. Samo te informacije su dovoljne napadačima da provale u veliki broj računala.

Iako postoji dovoljan broj načina na koji napadač može znati koji je korisnički račun uistinu administratorski račun, preporučljivo je preimenovati taj račun da bi ga bilo malo teže pronaći. Na taj način moguće je efektivno zaštiti računalo od hakera početnika. Najbolje je odabrati ime koje nešto znači korisniku, ali koje ne odaje očito da je riječ o administratorskom računu. Nazvati ga varijacijom osobnog imena, Admin, LocalAdmin ili nešto slično još uvijek navodi na to da je riječ o administratorskom računu i neće zavarati napadača zadugo. Promjenu imena ugrađenog administratorskog računa moguće je izvršiti pomoću dijaloškog okvira Upravljanje računalom, unutar upravljačke ploče (odabirom Lokalni korisnici i grupe -> Korisnici, te desnim klikom na administratorski račun i odabirom opcije Preimenuj; odnosno Local Users and groups -> Users ... Rename). Pored promjene imena, potrebno je postaviti i kompleksniju lozinku na taj korisnički račun.

Još jedan način promjene imena administratorskog, a i gost korisničkog računa je unutar lokalnih sigurnosnih postavki, odabirom Upravljačka ploča -> Administrativni alati -> Lokalna pravila sigurnosti -> Lokalne politike -> Sigurnosne opcije (Control Panel -> Administrative tools -> Local security Policy -> Local Policies -> Security Options)

Unutar tog dijaloškog okvira, u dijelu koji se odnosi na korisničke račune (Accounts) moguć je pregled i izmjena statusa administratorskog i gost računa (uključen/isključen), kao i izmjena imena oba računa. Unutar opcije izmjene imena, u opisu postavke jasno se savjetuje preimenovanje oba računa, upravo u sigurnosne svrhe, da bi zavarali napadača.

Kao dodatak prethodnom savjetu, pored promjene imena pravog administratorskog računa dobro bi bilo također stvoriti i lažni administratorski račun.

Svaki napadač koji uspije dobiti pristup sustavu i vidi da ne postoji administratorski račun, shvatiti će da je jedan od ostalih postojećih sigurno zapravo administratorski. Stoga bi, nakon preimenovanja pravog administratorskog računa trebalo stvoriti novi korisnički račun, s ograničenim pravima (Ograničeni korisnički račun) i nazvati ga Administrator. Naravno, iako postoje sofisticirani načini utvrđivanja koji je korisnički račun administratorski, to će ipak dodatno otežati početnicima.

Još jedna bitna stvar vezana za administratorski korisnički račun je i ta da Windows XP operacijski sustav prilikom instalacije kreira i još jedan skriveni administratorski račun, bez lozinke, koji nije vidljiv nikome. No, bilo koja osoba koja zna da postoji, može ga iskoristiti za pristup sustavu, stoga je i taj račun potrebno osigurati. Taj korisnički račun postoji za slučaj neke krajnje nužde i nije ga preporučljivo brisati, stoga mu je najbolje dodijeliti snažnu lozinku. Skrivenom administratorskom računu moguće je pristupiti samo u sigurnom načinu rada (Safe Mode). Prilikom podizanja sustava, pritiskanjem tipke F8 prikazuje se izbornik koji nudi nekoliko opcija. Odabirom opcije „Safe Mode“ sustav se pokreće u sigurnom načinu rada. Već na ulaznom ekranu dobrodošlice (Welcome screen) vidljiv je i taj korisnički račun. Lozinku mu je moguće jednostavno dodijeliti odabirom Upravljačka ploča -> Korisnički računi.

Nadalje, po pitanju sigurnosti, najbolje bi bilo što je više aktivnosti moguće obavljati pomoću ograničenog korisničkog računa, te administratorski koristiti samo kada je to apsolutno nužno. To može u neki situacijama izazvati frustracije zbog ograničenja, ali sigurnosti radi, za svakodnevnu uporabu – ograničeni korisnički računi. Svakodnevno korištenje korisničkih računa s ograničenim pravima može uvelike smanjiti potencijalni rizik.

Instaliranje programa pri tome je ograničeno, a neki programi odbijaju uopće i raditi ako je korisnik prijavljen na ograničeni korisnički račun. Na raznim web mjestima, kao i na Microsoftovim stranicama može se pronaći popis takvih programa. Način da se takvim problemima doskoči i izbjegne stalno odjavljivanje i prijavljivanje, je mogućnost pokretanja programa (ili instalacije programa) unutar jednog korisničkog računa, kao neki drugi korisnik (i s njegovim privilegijama). To je moguće odabirom opcije Pokreni kao (Run As) dostupne desnim klikom na ikonu željenog programa. Dakle, moguće je i s ograničenim korisničkim računom pokrenuti neki program kao administrator, sve što je potrebno je upisati lozinku dodijeljenu tom računu.

Nadalje, još jedna mogućnost koja bi mogla proći u nekim situacijama je postaviti program da se pokreće u načinu kompatibilnosti (compatibility mode) s nekom starijom verzijom Windows operacijskog sustava. Ta postavka je dostupna na kartici Kompatibilnost, unutar svojstava (desni klik na ikonu programa, zatim Svojstva).

Ako to ne prođe, onda ostaje opcija Pokreni kao. Moguće je čak i konfigurirati određene postavke da nije potrebno odabirati desni klik, pa Pokreni kao, već da klikom na prečac programa (to vrijedi samo za prečace do programa) automatski traži unošenje lozinke za korisnički račun (desni klik na prečac -> Svojstva -> kartica Prečac -> Dodatno -> Pokreći s različitim vjerodajnicama; odnosno desni klik, Properties -> Shortcut tab -> Advanced -> Run with different credentials).

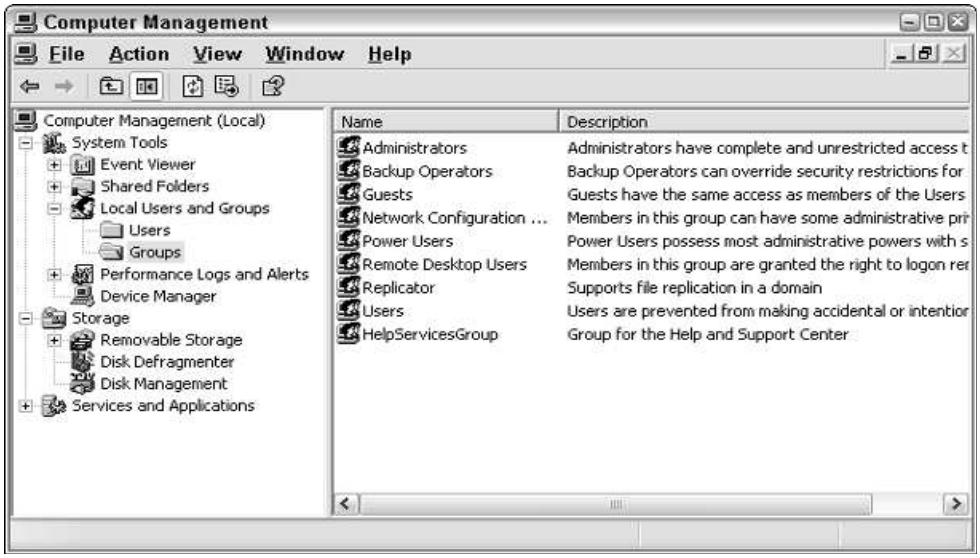
Nije potrebno dodatno naglašavati važnost dodjeljivanja lozinki svim korisničkim računima. Čak i ako samo jedna osoba koristi računalo, svaki nezaštićeni korisnički račun predstavlja sigurnosni rizik. No, u pravilu ne bi trebalo dodavati, mijenjati ili resetirati lozinke za druge korisničke račune osim tijekom procesa stvaranja. Ako se vrše izmjene na lozinkama drugih korisničkih računa doći će do gubitka pristupa šifriranim datotekama, pohranjenim Internet certifikatima i pohranjenim lozinkama za web mjesta. Umjesto toga, bilo kakva izmjena nad lozinkom nekog korisničkog računa treba se vršiti kad je taj korisnički račun aktivan, dakle, treba se odjaviti sa sustava i pristupiti tom konkretnom korisničkom računu.

Korisničke grupe

Korisničke grupe su zbirke, grupe korisnika, odnosno korisničkih računa. Na Windows XP sustavu, grupe se koriste za dodjeljivanje (odnosno zabranu) prava izvođenja radnji ili pristupa mapama i datotekama, skupinama korisnika. Windows XP sadrži nekoliko ugrađenih korisničkih grupa, ali administrator može također stvarati i nove, prilagođene grupe, za zadovoljavanje različitih potreba.

Korisnici sa sličnim potrebama mogu biti pridruženi istoj grupi, a zatim se čitavoj grupi kolektivno dodjeljuju prava i dozvole. Kad je korisnik pridružen nekoj grupi, automatski nasljeđuje sva prava dodijeljena toj grupi. Iako inicijalno traži više posla, takav pristup je generalno mnogo lakši za upravljanje i mnogo bolji.

Windows XP Professional operacijski sustav uključuje devet različitih ugrađenih korisničkih grupa, kao što je prikazano na slici 3.4. Svaka od ugrađenih korisničkih grupa ima posebna prava i privilegije. Na primjer, članovi grupe Super-korisnika (Power user) mogu kreirati korisničke račune, lokalne grupe, dodavati ili uklanjati korisnike iz grupa. Članovi Gost (Guest) grupe ne mogu raditi ništa od toga. Tu su također ugrađene grupe za administratore, općenite korisnike i ostale.



Slika 3.4. - Dijaloški okvir Upravljanje računalom (Computer Management)

Za upravljanje korisničkim grupama koristi se dijaloški okvir Upravljanje računalom (unutar Upravljačka ploča -> Administrativni alati) kao i za korisničke račune. Odabirom opcije Lokalni korisnici i grupe -> Grupe (Computer Management -> Local users and groups -> Groups) moguće je vidjeti popis svih korisničkih grupa, dodavati im korisnike i uklanjati ih (pomoću svojstava svake grupe).

Sa sigurnosnog aspekta, najbolje bi bilo prijaviti se u sustav kao administrator te sve ostale korisničke račune pridružene administratorskoj grupi, prebaciti u grupu Super-korisnik.

Za stvaranje nove grupe dovoljno je na tom istom mjestu odabrati desni klik -> Nova grupa (New Group), dodijeliti joj ime i opis, te dodati članove. Sve izmjene postanu aktivne sljedeći put kad se korisnik prijavi u sustav. Sve korisnički stvorene grupe mogu se jednostavno i brisati.

Prilikom kreiranja nove grupe, automatski joj se dodjeljuju prava generičke grupe općenitih korisnika (User). No, ta prava, kao i zadana prava svih ostalih grupa mogu se modificirati prema vlastitim željama i potrebama. Iako takvo nešto nije baš preporučljivo, jer može zakomplicirati otkrivanje smetnji (troubleshooting) kad stvari pođu krivo, to se svakako može uraditi. Postavke vezane za prava korisničkih grupa nalaze se unutar dijaloškog okvira lokalnih sigurnosnih postavki (Upravljačka ploča -> Administrativni alati -> Lokalna pravila sigurnosti -> Lokalne politike -> Dodjela korisničkih prava odnosno, Control Panel -> Administrative tools -> Local Security Policy -> Local Policies -> User Rights Assignment).

Isto tako, moguće je pojedinim korisničkim grupama, korisničkim računima ili čak pojedinim korisnicima iz neke grupe omogućiti različita prava pristupa nad pojedinim mapama, datotekama ili čak čitavim particijama.

3.5.2. Lozinke

Lozinke su doista jedna od, ako ne i najslabija karika u sigurnosti bilo kojeg sustava. Mišljenje mnogih je da je svaki sustav onoliko siguran koliko su i lozinke kojima se štiti. Iako su korisnički računi osnova sigurnosti Windows XP sustava, moglo bi se reći i to da implementacija korisničkih računa i grupa u kombinaciji sa slabim lozinkama zapravo i nema neki koristan efekt. Jedan dio problema je činjenica da korisnici često odabiru kratke, jednostavne i lako pamtljive lozinke, te pored toga koriste te iste slabe lozinke za više različitih korisničkih računa. Tu je još i problematika sigurnosti samog pohranjivanja lozinki unutar operacijskog sustava; te činjenica da je, pored današnjih sve bržih računala i sve naprednijih gotovih alata, razbijanje lozinki postalo relativno jednostavan zadatak. Zbog toga je veoma važno koristiti što bolje lozinke koje će biti

malo teže pogoditi, te iskoristiti sve mogućnosti koje nudi Windows XP operacijski sustav sa svojim sigurnosnim politikama.

Glavna stvar je da za sve korisničke račune odabiremo lozinke koje su kompleksne i time omogućuju viši nivo zaštite. Međutim, jednako je važno odabrati lozinke koje možemo zapamtiti. Odabiranje i korištenje dobrih lozinki uključuje tri glavna koraka: odabiranje dobrih i snažnih lozinki, izbjegavanje osnovnih grešaka i redovno mijenjanje lozinki.

Pitanje koje je oduvijek aktualno je što zapravo lozinku čini dobrom i snažnom. Točan i konkretan odgovor zapravo se ne može sa sigurnošću ponuditi, ali određenih pravila bi se uvijek trebalo držati prilikom odabira. Lozinka bi se trebala sastojati od najmanje osam znakova. Što je dulja lozinka, to bolje. Windows XP operacijski sustav ima potporu za lozinke duljine do 127 znakova. Dobra lozinka bi trebala uključivati i velika i mala slova, te brojeve. Isto tako, trebala bi sadržavati najmanje jedan (preporučljivo i više) od posebnih znakova, kao što su: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? . /, ako su takvi znakovi dozvoljeni.

To su naravno neki minimumi kojih bi se trebalo držati. Duga lozinka, recimo petnaestak ili više znakova, s dosta specijalnih znakova, brojeva i velikih i malih slova sigurno pruža dobru zaštitu od napadača koji koriste i najnaprednije alate za probijanje lozinki. Međutim, idealne kompleksne lozinke nisu od velike koristi ako ih korisnik ne može zapamtiti.

Postoji dosta trikova za stvaranje snažnih lozinki koje je relativno lako zapamtiti. Recimo, korištenje prvih slova iz neke rečenice ili pjesmice; ili zamjena nekih riječi ili slova nekim specijalnim znakovima. Na primjer, lozinka „JsAK.I23g!". Takva jedna lozinka možda na prvi pogled izgleda kao slučajan niz znakova koji je teško zapamtiti, ali je zapravo samo kombinacija prvih slova svih riječi, te brojeva i znakova iz dviju jednostavnih rečenica: „Ja sam Andrea Kozina. Imam 23 godine!"

Drugi primjer uključuje zamjenu slova brojevima i specijalnim znakovima koji im nalikuju. Izraz „sigurna lozinka" može se lako pretvoriti u: „$1gurn@_L0Z1NK@", čime zapravo na jednostavan i zanimljiv način dobivamo upravo to – sigurnu lozinku. I to lozinku od čak 15 znakova koju je lako zapamtiti.

Pored tih osnovnih pravila koja su dobra podloga za stvaranje snažnih lozinki, postoji i nekoliko grešaka koje ljudi često rade, a koje je potrebno izbjegavati.

Za dobre lozinke nikad ne bi trebalo koristiti bilo koji dio korisničkog imena ili čak punog imena, kao ni imena prijatelja, članova obitelji, mjesta, ljubimaca. Hakeri vrlo dobro znaju da većina ljudi koristi slabe lozinke temeljene na osobnim podacima. Daleko prevelik broj ljudi se oslanja na detalje koje je lako otkriti, kao imena djece ili ljubimaca, omiljenu sportsku momčad i slično, da bi zaštitili i one najvažnije i najpovjerljivije korisničke račune. Također nikad ne bi trebalo koristiti podatke kao što je datum rođenja, broj telefona, adresu ili druge osjetljive informacije, bilo osobne, obiteljske ili poslovne. Za lozinke se ne bi trebale koristiti nikakve riječi, izrazi ili akronimi koji se mogu pronaći u rječnicima.

Nijedna lozinka se ne bi trebala koristiti za više različitih računa, odnosno lozinka ne bi smjela biti jednaka ili nalikovati niti jednoj drugoj lozinki koja se koristi. Niti jednu lozinku ne bi trebalo držati u uporabi kroz duži period.

I pored toga valja napomenuti da lozinke nikad ne bi trebalo odavati nikome, govoriti ih nikome, uključujući obitelj i prijatelje, niti lozinke zapisivati na mjestima koja su dostupna drugima.

Zadnji korak je redovno mijenjanje lozinki. Kao jedna od najčešćih greški, kao što je već navedeno, je korištenje istih lozinki kroz dugi period vremena ili čak stalno. Kao generalno pravilo, lozinke za sve važnije korisničke račune trebalo bi redovno mijenjati, recimo svako 30 do 90 dana. Češće mijenjanje lozinki pomaže poboljšanju cjelokupne sigurnosti jer korištenje istih kroz duži period povećava izloženost riziku.

Osnovni tipovi lozinki s kojima treba raditi jedan korisnik Windows XP operacijskog sustava i korisnik Internet usluga su: lozinke za korisničke račune, lozinke za web mjesta i elektroničku poštu, lozinke za Internet usluge, te lozinke za zaštitu mapa i datoteka. U nekim slučajevima korisnik sam odabire lozinku, dok im je u drugim slučajevima lozinka dodijeljena od treće strane. Bez obzira na način na koji su pribavljene, te činjenicu da su neki korisnički računi važniji od drugih, sve lozinke su važne i treba ih tako i tretirati; zapamtiti ih i propisno osigurati.

Po pitanju lozinki vezanih za operacijski sustav, točnije Windows XP, postoje neke mogućnosti kojima se mogu uvesti pravila i uvjeti vezani za određivanje i održavanje lozinki. Administrator računala može implementirati određenu politiku (password policy), pravila koja će uvjetovati stvaranje sigurnih lozinki i njihovu izmjenu kroz određeni period, kao i neke druge postavke. U slučaju da vlasnik, odnosno administrator nije jedina osoba koja koristi konkretno računalo, kreiranje takve politike je dobar način osiguravanja da i ostali korisnici slijede pravila i koriste dobre lozinke. No, ako i nema drugih korisnika, to je opet dobar način da osoba sama sebe prisili da se pridržava politike i bez obzira na situaciju, ne zanemari pravila.

Postavke politike lozinki dostupne su unutar dijaloškog okvira lokalnih sigurnosnih postavki (Local security settings) do kojih je moguće doći pomoću upravljačke ploče (Upravljačka ploča -> Administrativni alati -> Lokalna pravila sigurnosti; odnosno Control panel -> Administrative tools -> Local Security Policy).

Politika vezana za lozinke, grupirana unutar politike korisničkih računa (account policies) omogućava administratoru da stvori pravila koja se odnose na duljinu i rok trajanja lozinke, njenu kompleksnost, te da li korisnici mogu ponovo koristiti ranije korištene lozinke. Također je moguće odrediti što činiti ako i kad korisnik unese određeni broj pogrešnih lozinki, uključujući to da li će korisniku u tom slučaju biti zabranjen pristup korisničkom računu i na koliko dugo.

Unutar grupe „Politika lozinki“ (Password Policy) dostupno je šest postavki:

- Omogućavanje pamćenja lozinke (Enforce Password History) – uključenjem te opcije moguće je odrediti broj jedinstvenih lozinki koje moraju biti korištene prije nego se neka stara može ponovo upotrijebiti. Može se odabrati broj između 0 i 24, dok je standardna postavljena vrijednost 0. Možda bi bilo dobro uključiti tu opciju i odabrati neki razuman broj lozinki, recimo pet.
- Maksimalno trajanje lozinke (Maximum Password Age) – uključenjem te opcije moguće je odrediti maksimalni broj dana koji se neka lozinka može koristiti, nakon čega sustav traži da se promijeni. Tu opciju je preporučljivo uključiti i odrediti neki razumni vremenski interval, recimo 90 dana. Ako je taj interval predug, napadač ima veće šanse doći do lozinke, a ako je prekratak, to je za korisnika prevelik posao i veća je mogućnost da će se zapisivati i pohranjivati na nesigurnim mjestima jer nije lako zapamtiti lozinke koje se često mijenjaju.
- Minimalno trajanje lozinke (Minimum Password Age) – uključenjem te opcije moguće je odrediti minimalan broj dana koji korisnik mora koristiti neku lozinku. Ta se opcija koristi da bi upotpunila pamćenje lozinki, jer prisiljava korisnike da koriste neku sigurnu lozinku određeni period, da ne mogu vratiti lozinku na neku njima dražu vrijednost, koja možda i nije sigurna. Dobro je minimalno trajanje lozinke postaviti na barem jedan dan.
- Minimalna duljina lozinke (Minimum Password Length) – uključenjem te opcije moguće je odrediti minimalnu duljinu (broj znakova) koju lozinka mora imati. Kao što je već navedeno, preporuka je da minimalna duljina bude osam znakova.
- Lozinka mora zadovoljiti uvjete kompleksnosti (Password Must Meet Complexity Requirements) – uključenjem te opcije korisnicima se uvjetuje da lozinka mora imati najmanje šest znakova, mora sadržavati barem tri od navedene četiri vrste znakova

(velika i mala slova, brojevi i specijalni znakovi (!, & i slični)), te da ne smije sadržavati dio ili cijelo korisničko ime ili puno ime. Tu opciju je najbolje uključiti kako bi korisnik bio prisiljen kreirati sigurne lozinke

- Pohrana lozinke korištenjem reverzibilnog šifriranja (Store passwords using reversible encryption) – tu opciju je najbolje ostaviti isključenom, te je uključivati samo u slučaju da je takvo nešto potrebno. Takav način pohrane lozinki je zapravo kao da se pohranjuju u tekstualnom obliku, onako kako jesu.

Unutar grupe „Politika zabrane pristupa računu“ (Account Lockout Policy), odabirom opcije – Granica zabrane pristupa, moguće je odrediti broj dozvoljenih pogrešnih pokušaja prije blokiranja. Odabirom broja pokušaja (možda uobičajena tri ili pet pokušaja) koji je različit od nule, postaje dostupna opcija Trajanje zabrane pristupa, kojom je moguće odrediti koliko će dugo korisnički račun biti blokiran (u minutama), nakon prekoračenja broja pogrešnih unosa. Dobro je odrediti neko vrijeme, možda 15 minuta. Treća postavka odnosi se na resetiranje brojača pogrešnih pokušaja i potrebno ga je postaviti na vrijednost koja je jednaka ili manja od trajanja zabrane pristupa, pa recimo onda na 10 minuta. Postavke vezane za zabranu pristupa dobro je koristiti jer pomaže u obrani od potencijalnih napada grubom silom (brute-force attack). Budući da se redom pokušavaju razne lozinke, ovako će se takav napad zaustaviti nakon nekog broja pokušaja i na dovoljno vrijeme da napadač odustane od napada.

Nakon primjene svih pravila i kreiranja vlastite sigurne lozinke moguće je provjeriti koliko je ta lozinka zapravo sigurna. Postoji mnoštvo programa za testiranje sigurnosti lozinki, no jednostavniji način je provjera na nekom od web mjesta koji to omogućuje, kao npr. SecurityStat.com (www.securitystats.com/tools/password.php). Alat nakon unosa testira lozinku te je zatim ocjenjuje i prikazuje rezultate i eventualno neke savjete. Preporučljivo je ipak za testiranje ne unijeti baš onu stvorenu lozinku, već neku koja je slična.

Postoje i razni programi koji služe za sigurnu pohranu lozinki. Program kao npr. Any Password (www.anypassword.com/index.html) koji je besplatan, omogućuje pohranu svih lozinki, korisničkih imena i ostalih vezanih informacija unutar stablaste baze podataka kao šifrirane, lozinkom zaštićene datoteke. Sve što je potrebno pamtiti je glavna lozinka programa (Master password). Za razliku od nekih drugih, omogućuje i kopiranje lozinki i lijepljenje na potrebno mjesto, nakon čega automatski čisti međuspremnik (Clipboard).

U slučaju nedostatka kreativnosti u smišljanju lozinki, moguće je poslužiti se nekim od dostupnih web mjesta koja nude generatore slučajnih lozinki (kao www.randpass.com) ili neki od dostupnih programa za generiranje lozinki, kao na primjer program Advanced Password Generator (www.segobit.com/apg.htm). To možda i nije loša opcija za generiranje sigurnih lozinki, ali takvu lozinku najvjerojatnije nije lako zapamtiti jer je ipak samo niz slučajnih znakova.

3.5.3. Polazni programi i procesi

Prilikom podizanja sustava, nakon prijavljivanja na sustav započinje inicijalizacija svih programa i procesa koji se nalaze na polaznim (startup) listama operacijskog sustava. Pored inicijalizacije raznih pomagala i aplikacija potrebnih za ugodan rad računala, obično se automatski pokreće i niz programa i procesa koji su ustvari nepotrebni. Većina takvih programa prilikom instalacije sama sebe postavlja na polazne liste. Pored svih tih korisnih i nepotrebnih programa i mnoštvo malicioznih programa se nakon inficiranja računala postavlja na liste za automatsko pokretanje kako bi osigurali da se pokrenu čim se računalo pokrene.

Zaustavljanje automatskog pokretanja programa je nešto teži zadatak zbog činjenice da ne postoji jedna jedinstvena lokacija na kojoj se svi nalaze i na kojoj ih je moguće isključiti. Upravo

taj podatak maliciozni programi često koriste pa se skrivaju na razna mjesta kako bi ih što teže bilo otkriti i onemogućiti.

Potrebno je revidirati sve liste automatskog pokretanja, te isključiti sve nepotrebne i sumnjive stavke, kako zbog ubrzavanja procesa podizanja i ubrzavanja samog rada računala, tako i zbog sigurnosnih razloga.

Naravno, sve programe koji su potrebni treba ostaviti. Među takvim programima nalaze se i svi zaštitni programi poput vatrozida ili programa za detekciju virusa za koje je važno da se pokrenu za vrijeme podizanja sustava kako bi zaštita bila što učinkovitija.

Postoji nekoliko lokacija vezanih za automatsko pokretanja. Neki programi se pokreću automatski prilikom podizanja sustava zato što se nalaze unutar mape Polazni programi (Startup), drugi zbog postavki unutar registra itd. Zbog toga je, za efektivno isključivanje potrebno kombinirati nekoliko tehnika.

Mapa Polazni programi sadrži prečice od kojih svaka pokreće program svaki put kada se računalo uključi ili ponovo pokrene. Jedan dio programa koji se automatski pokreće moguće je eliminirati jednostavnim brisanjem prečica unutar mape.

Mapu Polazni programi moguće je vidjeti već u startnom izborniku (Start -> Svi programi -> Polazni programi; odnosno Start -> All Programs -> Startup). Inače je smještena unutar C:\Documents and Settings*ime korisničkog računa*\Start Menu\Programs\Startup.

Potrebno je samo unutar te mape obrisati prečice do programa za koje ne želimo da se automatski pokreću. Potrebno je isto napraviti i za C:\Documents and Settings\All Users\Start Menu\Programs\Startup i C:\Documents and Settings\Default User\Start Menu\Programs\ Startup.

Sljedeće, potrebno je očistiti mapu Planirani zadaci (Scheduled Tasks), unutar C:\WINDOWS\ Tasks. Jednostavno se obrišu prečice do programa za koje ne želi da se automatski pokreću prema zadanom rasporedu.

Još jedan način je korištenje pomagala za sistemsku konfiguraciju, MSConfig (Microsoft System Configuration Utility). Pomagalo pokrećemo odabirom Start -> Pokreni (Start -> Run) i upisivanjem msconfig u polje Otvori (Open) prikazanog dijaloškog okvira.

Za zaustavljanje automatskog pokretanja programa, odabire se kartica Startup i ukloni se kvačica pored programa kojeg se želi zaustaviti. Ponekad može biti problematično razlučiti koji su programi zapravo navedeni. Neki su jasno označeni, no većina je predstavljena nekom frazom ili nizom slova, kao npr. ctfmon. U ovom slučaju ctfmons.exe predstavlja program koji aktivira usluge kao što je prepoznavanje govora i rukopisa, za Microsoft Office. U svakom slučaju, ako podaci koji su tu prikazani ne govore dovoljno o čemu se zapravo radi, takve programe ne bi trebalo dirati prije nego se ustanovi točno o čemu je riječ (pretraživanjem na Internetu ili sl.).

Prilikom zaustavljanja programa, najbolje je proces odraditi zaustavljanjem jednog po jednog programa, radije nego grupno. Treba biti siguran da zaustavljanje nekog programa neće uzrokovati neke probleme, stoga je najbolje zaustaviti jedan program i zatim ponovno pokrenuti računalo. Kod korištenja pomagala za sistemsku konfiguraciju u tom procesu, nakon svakog ponovnog pokretanja računala prikazat će se upozorenje o izvršenoj radnji. Za isključivanje prikaza tih upozorenja, dovoljno je isključiti odgovarajuću stavku u dijaloškom okviru. Prije korištenja ove metode, možda bi bilo dobro pokušati potražiti opciju za isključivanje automatskog pokretanja direktno unutar konkretnog programa. Dosta programa nudi tu opciju.

Pomagalom za sistemsku konfiguraciju većinom nije moguće identificirati i onemogućiti baš sve programe koji se automatski pokreću prilikom podizanja računala. Zato je potrebno posegnuti u registre da bismo pronašli preostale. Za pronalazak tih programa potrebno je otvoriti pomagalo za upravljanje registrima (Registry Editor) te odabrati `HKEY_CURRENT_USER\ Software\`

Microsoft\ Windows\ CurrentVersion\ Run. U lijevom okviru prozora nalaze se neki od programa koji se automatski pokreću. U polju Data prikazana je putanja i naziv izvršne datoteke, da bi mogli utvrditi o kojem je programu riječ. Desnim klikom na program i odabirom Delete moguće je ukloniti sve programe koje se automatski pokreću, a vezani su za trenutno aktivni korisnički račun. Za uklanjanje programa za sve korisnike sustava potrebno je odabrati HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run. Te istim postupkom obrisati sve ostale neželjene programe.

Pored svih metoda koje su dostupne u sklopu operacijskog sustava, mnogi ljudi zapravo preporučuju izbjegavanje MSConfig pomagala ili izmjene registara, te umjesto toga korištenje nekog od neovisnih programa napravljenih upravo za te svrhe. Mišljenje mnoštva ljudi je da neki takvi programi zapravo mnogo bolje obavljaju taj zadatak od pomagala ugrađenih u operacijski sustav, te da u mnogim slučajevima, isključivanjem nekog programa pomoću MSConfig pomagala velik broj njih uspije vrlo brzo ponovno dospjeti na listu programa za automatsko pokretanje.

Primjer jednog takvog programa je ranije spomenuti Autoruns, besplatan alat koji može prikazati sadržaje različitih polaznih (autostart) lokacija u sustavu. Dolazi u verziji sa grafičkim korisničkim sučeljem ili u komandno-linijskoj verziji. Proizvod je dostupan na web stranici http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx.

Još jedan primjer je Mike Linova besplatna aplikacija Startup Control Panel, koja pruža mnogo više kontrole nad programima koji se automatski pokreću. Može se preuzeti na web stranici www.mlin.net/StartupCPL.shtml. Postoje dvije verzije, jedna koja se smješta unutar upravljačke ploče operacijskog sustava, dok druga radi kao klasičan program.

Druga vrsta programa koja se može koristiti u kombinaciji s prethodnom su programi koji nadgledaju sustav, točnije registre i upozoravaju korisnika o svakom pokušaju nekog programa da se doda na listu za automatsko pokretanje. Primjer takvog alata je program od istog autora kao i prethodni, naziva Startup Monitor. To je također besplatan program i može se preuzeti na web stranici www.mlin.net/StartupMonitor.shtml

3.5.4. Windows usluge (Windows services)

Svaki Windows XP sustav prilikom podizanja, pored programa automatski pokreće i niz usluga (services) koje omogućuju funkcioniranje različitih elemenata operacijskog sustava. Usluge su programi koji se kontinuirano izvršavaju u pozadini, obrađuju zahtjeve drugih programa ili one s mreže. Usluge se izvršavaju bez direktne interakcije s korisnikom, zapravo korisnik većinom nije ni svjestan njihova izvršavanja. Pored svih Windows usluga i mnogi programi dodaju vlastite usluge kao dio instalacijskog procesa i te su usluge potrebne za ispravno funkcioniranje programa.

Iako je većina usluga potrebna za izvršavanje uobičajenih zadataka, jedan dio njih je obično nepotreban za većinu korisnika, a neke mogu predstavljati i realan sigurnosni rizik, ako su uključene. Isključivanje nepotrebnih usluga i usluga koji predstavljaju potencijalni rizik je uvijek dobra ideja sa sigurnosne perspektive, a korisno je i po pitanju performansi računala. Svaka aktivna usluga na Windows XP sustavu troši resurse računala (npr. memoriju), bez obzira na to da li se koristi ili ne. Isključivanje nepotrebnih usluga može značajno poboljšati performanse i ubrzati rad računala.

Neželjene ili nepotrebne usluge mogu biti zaustavljene, pokrenute, prekinute ili ponovno nastavljene, od strane bio kojeg korisnika s administratorskim pravima.

Konfiguriranje ponašanja usluge obavlja se pomoću dijaloškog okvira Usluge (Services) ili u nekim slučajevima kroz postavke registara.

Dijaloški okvir za upravljanje uslugama dostupan je odabirom Upravljačka ploča -> Administrativni alati -> Usluge (Control Panel -> Administrative tools -> Services) ili direktnim pokretanjem „services.msc“ pomoću Start -> Pokreni (Start -> Run).

Unutar dijaloškog okvira Usluge, sve usluge koje su trenutno aktivne definirane su kao Započeti (Started) unutar polja Status. Sve ostale usluge se ne izvršavaju u tom trenutku. Način podizanja (Startup type) je polje koje definira kada i da li operacijski sustav pokreće uslugu. Ako je to polje definirano kao Automatski (Automatic), to znači da se ta konkretna usluga pokreće automatski prilikom podizanja sustava. Ručno (Manual) znači da se usluga pokreće samo po potrebi, dakle kada neki program to traži. Onemogućeno (Disabled) znači da je ta usluga isključena, onemogućena i neće biti pokrenuta nikada, čak i ako je neki program treba.

Isključivanje usluga koje su ključne za rad sustava može zapravo dovesti do toga da se računalo ne može uopće uključiti, odnosno da se operacijski sustav ne može podignuti. Zaustavljanje nekih usluga može uzrokovati neke probleme kojima je prilično teško ući u trag. U svakom slučaju, prije zaustavljanja neke usluge potrebno je poduzeti sve potrebne korake i dobro se informirati o konkretnoj usluzi prije izmjene načina podizanja.

Prilikom isključivanja usluge za koju se smatra da je sustav ne koristi, siguran prvi korak je zaustavljanje usluge bez mijenjanja načina podizanja. Nakon toga bi bilo pametno koristiti računalo neko vrijeme s tom postavkom da bi se uvjerilo da je ta usluga uistinu nepotrebna. U slučaju bilo kakvog neuobičajenog ponašanja, anomalija u radu računala, treba ponovno pokrenuti uslugu i vidjeti da li to rješava problem. Ako se unutar dijaloškog okvira za upravljanje uslugama zatim naiđe na uslugu koja je aktivna, a prethodno je zaustavljena, jasno je da je neki dio sustava ponovno pokrenuo uslugu jer je bila potrebna. U tom slučaju bi potpuno isključivanje te usluge moglo uzrokovati probleme.

Zaustavljanje, pokretanje, prekidanje i nastavljanje neke usluge može se izvršiti pomoću izbornika dostupnog desnim klikom, dok su sve ostale postavke dostupne unutar dijaloškog okvira Svojstva (Properties). Kartica Ovisnosti (Dependencies) prikazuje dodatne informacije o tome da li je usluga nepotrebna. Prikazuje da li neka druga usluga (i koja) ovisi o toj usluzi i da li ta usluga treba neku drugu za rad. Isto tako treba paziti da li neka funkcija, neka aplikacija operacijskog sustava treba određenu uslugu za rad, te prije isključivanja usluge, isključiti tu funkciju.

Pored osnovnih podataka o svakoj usluzi vidljiv je i opis gotovo svake usluge, međutim ti opisi su rijetko detaljni ili od pomoći. Dodatne informacije je dobro potražiti recimo na Internetu. Pored informacija o uslugama na raznim web mjestima moguće je pronaći i savjete i prijedloge o tome koje usluge bi bilo dobro isključiti. U svakom slučaju, bez obzira na prijedloge treba biti oprezan. Za neke je možda ipak najbolje ne isključivati ih, nego ih postaviti da se pokreću po potrebi, ručno (Manual).

Windows usluge koje mogu direktno utjecati na sigurnost sustava, odnosno predstavljaju potencijalni sigurnosni rizik i koje bi možda bilo dobro isključiti (ili barem postaviti na ručno pokretanje) su:

Internet Information Services – usluga nije standardno instalirana, ali je prisutna ako je instalirana bilo koja komponenta vezana za nju (kao npr. ugrađeni web ili FTP poslužitelj). Ako je taj usluga uključena, a trenutno se ne koriste nikakve IIS usluge, treba je isključiti.

Messenger – usluga (koji nema veze s popularnim MSN Messenger programom) se koristi zajedno s Alerter uslugom za slanje administrativnih obavijesti ili upozorenja. Budući da se te usluge često zloupotrebljavaju i pomoću tih usluga oglašivači otvaraju privremene (pop-up) prozore na radnoj površini, obje bi trebale biti isključene. Nakon SP2, Messenger usluga je standardno isključena.

DCOM Server Process Launcher (DCOM potpora) – DCOM (Distributed Component Object Model) pruža prihvatljivo programsko sučelje za programere koji pišu mrežne aplikacije, ali je povezivan s podosta sigurnosnih problema. Otkriveno je dosta primjera zloupotrebe (exploit), koji omogućuju brzo širenje crva i drugih vrsta malicioznog koda. Budući da vrlo mali broj aplikacija zapravo koristi DCOM i većini korisnika neće trebati, najbolja opcija bilo bi isključivanje ove usluge.

Error reporting service – usluga koja pruža potporu za uslugu izvještavanja o greškama i slanja izvješća Microsoftu. Za zaštitu privatnosti, a i sprečavanje zamornih poruka, prvo je potrebno isključiti funkciju (Upravljačka Ploča -> Sustav -> Napredno -> Izvještavanje o greškama; Control Panel -> System -> Advanced -> Error Reporting)) i nakon toga isključiti tu uslugu.

Netmeeting Remote Desktop Sharing – usluga koja omogućava udaljenim korisnicima povezivanje s radnom površinom i interakciju pomoću Netmeeting programa. Zbog očitog sigurnosnog rizika koji nosi bilo kakvo udaljeno povezivanje, ako se Netmeeting ne koristi, trebalo bi ga isključiti

Remote Desktop Help Session Manager – ključna komponenta Windows XP daljinske podrške (Remote Assistance) omogućuje korisnicima povezivanje s drugim Windows XP sustavima. Daljinska podrška standardno nije omogućena (treba je uključiti unutar upravljačke ploče). Budući da je ta funkcija može predstavljati sigurnosni rizik, ako se daljinska podrška ne koristi usluga bi trebala biti onemogućena, isključena.

Remote Registry – usluga koja omogućuje udaljeno povezivanje i modificiranje registara tog i drugih računala na mreži. Ta mogućnost je ponekad korisna, za udaljeno upravljanje u velikim tvrtkama, no isto tako ima i veliki potencijal za zloupotrebu koju je teško otkriti i tu uslugu bi svakako trebalo isključiti.

Routing and Remote Access – omogućava potporu za dolazne modemske i VPN veze. Ta usluga obično nije potrebna u kućnim okruženjima i trebalo bi je isključiti.

SSDP Discovery Service – usluga koja funkcionira u kombinaciji s Universal Plug and Play uslugom i može predstavljati ozbiljan sigurnosni rizik za računalo. U slučaju da se UPnP usluga isključi, trebalo bi i ovu uslugu isključiti. Ako je ova usluga isključena, usluge udaljene radne površine (Remote Desktop) i daljinske podrške (Remote Assistance) neće raditi.

Telnet – usluga koji omogućava udaljeni pristup i upravljanje putem komandno-linijskog sučelja. Budući da predstavlja sigurnosni rizik, ako se Telnet ne koristi, uslugu bi trebalo isključiti.

Universal Plug and Play device host – usluga koja se odnosi na Universal Plug and Play standard (a ne mogućnost automatske detekcije sklopovskih uređaja), omogućava različitim vrstama mrežnih uređaja međusobno povezivanje i komunikaciju. No, budući da također predstavlja i ozbiljan sigurnosni rizik, ako se ne koristi trebalo bi je isključiti.

3.5.5. Ostale sigurnosne postavke

Pored svih mogućnosti zaštite i poboljšanja sigurnosti dostupnih unutar Windows XP operacijskog sustava i ostalih postavki obrađenih u ovom poglavlju, potrebno je navesti i sve one ostale postavke koje je dobro primijeniti, koje se većinom odnose na ranjivosti obrađene u poglavlju 2.2. (Opasnosti iznutra).

Datotečni sustav

Budući da NTFS datotečni sustav nudi više mogućnosti od FAT32, pogotovo po pitanju sigurnosti, sve particije tvrdog diska bi trebale biti formatirane u NTFS. Prilikom instalacije operacijskog sustava, NTFS je primarna opcija i ona standardno odabrana.

U slučaju da su particije tvrdog diska formatirane FAT32 datotečnim sustavom, postoji mogućnost konverzije postojećih particija u NTFS bez ponovnog formatiranja (koje bi značilo brisanje svih podataka). Pomoću ugrađenog komandno-linijskog pomagala CONVERT.EXE moguće je promijeniti FAT32 particije u NTFS. Takva konverzija je jednosmjeran postupak pa nije moguće iz NTFS napraviti konverziju u FAT32 zbog sigurnosnih razloga, što i nije loše.

Konverziju je jednostavno izvršiti, otvaranjem naredbenog retka (Start -> Svi programi -> Pomagala -> Naredbeni redak; odnosno Start -> All programs -> Accessories -> Command Prompt) i unosom naredbe kao npr. convert d: /fs:ntfs, gdje **d:** označava da će se konverzija izvršiti za D particiju. Nakon unosa naredbe i pritiska tipke Enter, potrebno je unijeti naziv (label) za tu particiju i time se korisnički postupak završava.

Proces može trajati od nekoliko sekundi do nekoliko minuta, ovisno o veličini particije i broju datoteka koje sadrži. Ponekad je možda potrebno i ponovno pokrenuti Windows XP da bi proces konverzije mogao biti dovršen. Kao mjera opreza, prije bilo kakvog pokušaja konverzije trebalo bi napraviti sigurnosnu kopiju (backup) svih podataka. Ako nešto pođe krivo prilikom konverzije, postoji manja mogućnost gubitka pristupa dijelu podataka ili svim podacima koji su se nalazili na particiji.

Najvažnije mogućnosti koje pruža NTFS datotečni sustav su mogućnost konfiguriranja različitih prava pristupa mapama i datotekama, za različite korisnike; te mogućnost korištenja šifriranja (EFS - Encrypting File System). Moguće je vrlo jednostavno šifrirati datoteke ili čitave mape, te postavljati različita prava pristupa šifriranim datotekama. Postupak je vrlo jednostavan, dovoljno je otvoriti svojstva datoteke ili mape koju se želi šifrirati (desnim klikom), odabrati opciju Dodatno (Advanced), te odabrati opciju šifriranja. Nakon toga je još ponuđen odabir šifriranja samo te datoteke ili i mape unutar koje se nalazi, ako se šifrira datoteku, odnosno odabir šifriranja samo te mape ili svih podmapa i sadržanih datoteka, ako se šifrira mapu. Sve šifrirane datoteke imaju umjesto crnih, zelena slova. Dodavanjem datoteke u neku šifriranu mapu, ta mapa automatski također postaje šifrirana.

Šifriranje je svakako mogućnost koju bi trebalo iskoristiti. Pored šifriranja datoteka koje sadržavaju privatne podatke, moguće je dodatno pojačati zaštitu sustava od napadača šifriranje Temp mape i Izvanmrežnih datoteka. Temp mapa sa nalazi unutar WINDOWS mape (Moje računalo\ Lokalni disk (C:)\WINDOWS\Temp). Izvanmrežne datoteke (Offline files) predstavljaju opciju koja omogućuje spremanje web stranica ili mrežnih mapa na računalo kako bi mogli biti pregledavani i kad računalo nije spojeno na Internet ili na mrežu. Iz sigurnosnih razloga, to bi trebalo izbjegavati, ali ako ih korisnik želi zadržati i koristiti, dobro ih je barem šifrirati. Postavke izvanmrežnih datoteka dostupne su unutar Odrednice mape, kartica Izvanmrežne datoteke (Folder options -> Offline files).

Čuvar zaslona

Da bi se spriječila ranjivost čuvara zaslona, obrađena u poglavlju 2.2. potrebno je napraviti neke izmjene unutar registra. Otvaranje dijaloškog okvira za upravljanje registrima moguće je na više načina, recimo odabirom Start -> Pokreni (Start -> Run) i upisom „regedit“ unutar otvorenog dijaloškog okvira. Nakon toga potrebno je odabrati: HKEY_USERS -> .DEFAULT -> Control Panel -> Desktop i u prozoru s desne strane pronaći stavku SCRNSAVE.EXE. Dvostrukim klikom na tu stavku otvara se dijaloški okvir u kojem je potrebno u polju „Value data“ umjesto vrijednosti „logon.scr“ unijeti „none“. Nakon toga dvostrukim klikom na „ScreenSaveActive“ otvara se dijaloški okvir na kojem je potrebno u polju „Value data“ izbrisati broj 1 i unijeti „No“.

Bilo bi dobro iskoristiti i mogućnost koju nudi čuvar zaslona, pa postaviti da se traži lozinka korisničkog računa svaki put kad se čuvar zaslona aktivira. Budući da bi takvo nešto bilo prilično iritantno prilikom rada, bolje je vrijeme aktiviranja čuvara zaslona postaviti na neku veću vrijednost, recimo 10 minuta. Postavka Kod nastavka zaštiti lozinkom (On resume, password

protect) dostupna je u postavkama čuvara zaslona, unutar svojstava prikaza (Display properties). Dijaloški okvir postavki prikaza dostupan je jednostavno, desnim klikom na radnu površinu i odabirom Svojstva (Properties), odnosno odabirom Start -> Upravljačka ploča -> Prikaz (Start -> Control Panel -> Display).

Automatsko pokretanje (AutoRun i AutoPlay)

Za inficiranje računala može se iskoristiti (a i događalo se) opcija automatskog pokretanja sadržaja s prijenosnih medija. Inficiranjem autorun.inf datoteke koja se automatski učitava prilikom priključenja nekog prijenosnog medija osigurava se inficiranje računala bez potrebe da se uopće otvori ili prikaže sadržaj. Metoda je efektivna, pogotovo s obzirom na činjenicu da tako inficirano računalo obično dalje inficira i sve nove izmjenjive medije koji se priključe na računalo (kao npr. USB prijenosna memorija), na koje je moguće pisati. Dalje ti mediji inficiraju svako novo računalo na koje su priključeni i maliciozni kod se širi velikom brzinom.

Zbog toga bi možda iz sigurnosnih razloga bilo dobro isključiti opciju automatskog pokretanja.

Za isključivanje automatskog pokretanja CD i DVD medija, potrebno je radnju ponoviti za sve CD i DVD pogone na računalu. Desnim klikom na CD/DVD pogon i odabirom Svojstva (Properties) otvara se dijaloški okvir na kojem je potrebno odabrati karticu AutoPlay. Za sve vrste sadržaja pojedinačno potrebno je za Akciju odabrati – Odaberi radnju za izvođenje (Select an action to perform) i zatim – Ne izvršavaj nikakvu radnju (Take no action).

Za isključivanje automatskog pokretanja svih vanjskih izmjenjivih pogona i uređaja, na Windows XP SP2 sustavima dovoljno je samo jednom izmijeniti postavke, unutar Grupne politike (Group Policy). Potrebno je odabrati Start -> Pokreni (Start -> Run), te u otvorenom dijaloškom okviru u polje Otvori (Open) upisati gpedit.msc da bi se otvorio dijaloški okvir za upravljanje Grupnom politikom. Zatim je potrebno odabrati Konfiguracija računala -> Administrativni predlošci -> Sustav (Computer Configuration -> Administrative Templates -> System) i u prozoru s desne strane pronaći opciju Isključi AutoPlay (Turn off AutoPlay). Dvostrukim klikom otvara se dijaloški okvir unutar kojeg je potrebno odabrati Omogući (Enable), te odabrati Svi pogoni (All drives) i zatim OK. Tu je vidljivo i da se na isti način može isključiti AutoPlay i za samo CD pogone. Ako na računalu postoji više korisničkih računa, ta postavka se primjenjuje na sve.

Dijeljenje resursa (File and printer sharing i Simple file sharing)

Ako računalo nije spojeno na neku lokalnu mrežu ili slično, a to obično i jest slučaj u kućnim okruženjima, nema potrebe za dijeljenjem resursa (kao npr. pisača) ili dijeljenjem datoteka. Stoga je iz sigurnosne perspektive najbolje isključiti takve usluge jer, ako se ne koriste, ostaviti ih uključenima može predstavljati sigurnosnu ranjivost.

Za isključivanje dijeljenja datoteka i pisača (File and printer sharing) potrebno je odabrati Upravljačka ploča -> Mrežne veze -> Lokalna veza (dvostruki klik) -> kartica Općenito (Control Panel -> Network connections -> Local Area Connection -> General)

Unutar kartice Općenito (General) potrebno je jednostavno isključiti opciju Dijeljenje datoteka pisača za Microsoft mreže (File and Printer Sharing for Microsoft Networks) i potvrditi izmjene klikom na OK.

Jednostavno zajedničko korištenje datoteka (Simple file sharing) je mogućnost dijeljenja datoteka organizirana na način da što više olakša korisnicima taj postupak. Osim na mreži, često i na računalima koja nisu dio mreže postoji potreba za dijeljenjem datoteka, ako se računalom služi više korisnika sa odvojenim korisničkim računima. Međutim, zbog načina na koji je organizirana, usluga jednostavnog dijeljenja datoteka je za većinu korisnika ograničena, nedovoljno fleksibilna i opet nedovoljno sigurna zaštita privatnih datoteka. Sa svih stanovišta,

kako funkcionalnog tako i sigurnosnog, najbolja opcija je isključivanje jednostavnog dijeljenja datoteka. Isključivanjem te opcije sustav se dodatno zaštićuje od potencijalnih napadača, te postaju dostupne opcije ručnog konfiguriranja, s mnogo više mogućnosti. Ručno konfiguriranje NTFS dopuštenja (permission) omogućuje više nivoa dozvola, te je moguće doslovno specificirati točno koji korisnik (i u kojoj mjeri) može imati pravo pristupa nekoj mapi.

Za isključivanje Jednostavnog zajedničkog korištenja datoteka (Simple file sharing) potrebno je otvoriti dijaloški okvir za odrednice mapa (Folder options), odabrati karticu Prikaz (View) i isključiti opciju Koristi jednostavno zajedničko korištenje datoteka (Use simple file sharing).

Odrednice mapa moguće je pronaći unutar upravljačke ploče ili u izborniku Alati (Tools) unutar svakog prozora mape.

Udaljeni pristup (Remote Desktop i Remote Assistance)

Ako se takve usluge ne koriste i nisu potrebne, bilo kakva mogućnost udaljenog pristupa računalu očit je sigurnosni rizik jer zapravo predstavlja otvorena vrata svim napadačima. Uz prave informacije dovoljno je samo iskoristiti uslugu koja omogućuje upravo to, udaljeni pristup i kontrolu nad računalom. Zbog toga je potrebno isključiti usluge Udaljene radne površine (Remote Desktop) i Daljinske podrške (Remote Assistance), odnosni, ako su isključene, ostaviti ih isključenima. Za isključivanje obje usluge potrebno je otvoriti postavke sustava (desnim klikom na Moje računalo i odabirom Svojstva; ili unutar upravljačke ploče) i odabrati karticu Udaljeno (Remote), te isključiti obje ponuđene opcije, kao što je prikazano na slici 3.5.

Slika 3.5. - Kartica Udaljeno (Remote) za upravljanje opcijama udaljenog pristupa unutar dijaloškog okvira za svojstva sustava (System Properties)

Skrivene ekstenzije

Skrivene ekstenzije ili proširenja mogu skrivati i neke druge stvari, koje mogu biti vrlo štetne. Stoga je najbolje da je sve vidljivo. Za otkrivanje poznatih ekstenzija datoteka potrebno je otvoriti dijaloški okvir za odrednice mapa (Folder options) unutar upravljačke ploče (ili u izborniku Alati, svakog prozora mape), odabrati karticu Prikaz (View) i isključiti opciju Sakrij proširenja za poznate tipove datoteka (Hide extensions for known file types).

Druga skupina datoteka sa skrivenim ekstenzijama su posebne datoteke operacijskog sustava. Za otkrivanje tih ekstenzija potrebno je izmijeniti postavke unutar registara. Budući da taj postupak nije jednostavan kao prethodni, napadači isto tako vrlo često posežu za manipulacijama takvih datoteka, te je upravo zato dobro isključiti skrivanje i tih ekstenzija.

Potrebno je odabrati Start -> Pokreni (Start -> Run) i upisati „regedit“ u polje Otvori (Open) prikazanog dijaloškog okvira. U pomagalu za upravljanje registrima (Windows Registry Editor) zatim odabiremo izbornik Uređivanje -> Pronađi (Edit -> Find). U dijaloškom okviru za pretraživanje potrebno je unijeti izraz „NeverShowExt“ (pri čemu treba paziti da je izraz točno unesen) i pokrenuti pretraživanje. Nakon pronalaska unosa s odgovarajućim imenom, potrebno ga je izbrisati. Odabirom Uređivanje -> Pronađi sljedeći (Edit -> Find Next) ili jednostavno pritiskom na tipku F3 pretraga se nastavlja i traži se sljedeći unos odgovarajućeg imena. Pretragu je potrebno završiti do kraja registra i obrisati svaki pronađeni unos koji odgovara pojmu pretrage.

Slika 3.6. - Dijaloški okvir za pretraživanje registra

Datoteka sa stranicom memorije (Pagefile)

Unutar te datoteke, odnosno virtualne memorije mogu se naći razni osjetljivi podaci i tu se mogu zadržati čak i duže vrijeme. Što duže stoje, predstavljaju veći sigurnosni rizik. Zbog toga je dobro napraviti izmjene unutar registara i uključiti opciju da operacijski sustav očisti datoteku prilikom svakog isključivanja računala.

Unutar pomagala za upravljanje registrima (Start -> Pokreni -> regedit) potrebno je odabrati HKEY_LOCAL_MACHINE -> System -> CurrentControlSet -> Control -> Session Manager -> Memory Management.
U desnom okviru prozora zatim se odabere stavka ClearPageFileAtShutdown. Dvostrukim klikom na taj unos otvara se dijaloški okvir u kojem je u polju „Value Data“ umjesto vrijednosti 0 potrebno upisati 1 i prihvatiti izmjene klikom na OK.

Ispis memorije (Dump File)

Unutar „skladišta“ koje se naziva Ispis memorije (Dump File), pored informacija o greškama i problemima nastalim u radu operacijskog sustava ili aplikacija, mogu se naći i razne osjetljive i privatne informacije. Iako informacije pohranjene u toj datoteci mogu biti korisne prilikom otkrivanja i otklanjanja smetnji (troubleshooting), radi zaštite sigurnosti možda bi bilo dobro onemogućiti stvaranje takvog „odlagališta“. U slučaju da ipak zatreba, dovoljno je obrnuti postupak onemogućavanja i ponovno ga uključiti.

Za isključivanje, potrebno je otvoriti dijaloški okvir s postavkama Sustava (System) i to odabirom Start -> Upravljačka ploča -> Sustav (System) ili jednostavno desnim klikom na ikonu Moje računalo (My computer) i odabirom Svojstava (Properties). U prikazanom dijaloškom okviru zatim odaberemo karticu Dodatno (Advanced) i opciju Postavke (Settings) za Pokretanje i oporavak (Startup and recovery). U novom dijaloškom okviru zatim, unutar opcije Spremanje podataka o ispravljanju grešaka (Write debugging information) u okviru s padajućim popisom odabere se „nema“ (none), i prihvate se izmjene klikom na Uredu.

VBScript

Visual Basic Skripte su tekstualne datoteke s ekstenzijom .vbs koje sadrže programski kod. Kriminalci vrlo često skrivaju viruse i druge oblike malicioznog koda unutar Visual Basic

Skripta i pridružuju ih e-mail porukama. Nakon otvaranja privitka e-mail poruke, VBScript kod se pokreće i maliciozni kod inficira računalo.

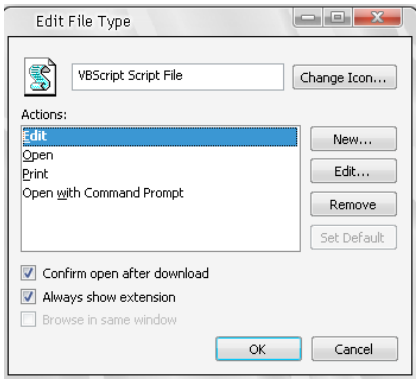
Budući da se VBScript i Jscript skriptni jezici često zloupotrebljavaju za inficiranje računala malicioznim kodom, postoji mogućnost potpunog onemogućavanja VBScript skripta. Za onemogućavanje VBScript skripta potrebno je otvoriti odrednice mapa (Folder options), te u tom dijaloškom okviru odabrati karticu Vrste datoteka (File types). Unutar Registriranih vrsta datoteka (Registered file types) potrebno je pronaći VBS ekstenziju i VBScript skriptnu datoteku (VBScript Script File) i taj unos izbrisati. Postupak je potrebno ponoviti i za sljedeće vrste datoteka:
- JScript Script File (ekstenzija - JS)
- JScript Encoded Script File (ekstenzija - JSE)
- VBScript Encoded Script File (ekstenzija - VBE)
- Windows Script File (ekstenzija - WSF).

Međutim, tim postupkom se potpuno briše čitava ta grupa skriptnih datoteka, te nakon toga više nije moguće raditi s njima. U slučaju da je takav korak previše drastičan, možda je bolje izabrati neko srednje rješenje, da se ipak zaštiti na neki način, ali da se ne izgubi sva funkcionalnost i mogućnost rada s tim skriptnim datotekama.

Drugačijom izmjenom određenih postavki moguće je zadržati mogućnost korištenja VBScript skripta, ali se može spriječiti njihovo automatsko pokretanje.

Na istom mjestu, unutar dijaloškog okvira za odrednice mapa (Folder Options) i kartice Vrste datoteka (File Types), u popisu vrsta datoteka i ekstenzija potrebno je pronaći unos VBScript Script File (ekstenzija VBS) i odabrati taj unos, te zatim kliknuti na opciju Dodatno (Advanced).

Unutar novog dijaloškog okvira koji se zatim otvori (kao što je prikazano na slici 3.7.), u okviru Radnje (Actions) potrebno je odabrati opciju Edit i zatim je postaviti kao zadanu (Set Default). Nakon toga uključiti obje od ponuđenih opcija Potvrdi otvaranje nakon preuzimanja (Confirm open after download) i Uvijek prikaži ekstenziju (Always show extension), te prihvatiti izmjene klikom na Uredu. Radnju je potrebno ponoviti i za sve ostale povezane vrste datoteka kao i kod prethodnog primjera.



Slika 3.7. - Dijaloški okvir za uređivanje postavki vrste datoteke (File Type)

Aplikacije

IIS (Internet Information Services)

Windows XP Professional ima ugrađeni web poslužiteljski program nazvan IIS (Internet Information services) također nazivan i osobni web poslužitelj (Personal web server). IIS nije standardno instaliran.

Dosta mu se prigovaralo zbog mnoštva pronađenih propusta koji su se iskorištavali za razne vrste napada. Microsoftova web platforma je s vremenom dosta opadala ugledom i često se preporučivalo prebacivanje na Apache, popularni UNIX web poslužitelj.

S obzirom na broj pronađenih propusta i količinu izdanih zakrpa za njih, veoma je važno redovno ažuriranje. No i dalje postoji mnoštvo lijenih korisnika ili neznalica koji koriste nesigurne i nezaštićene web poslužitelje.

Ako je na računalu instaliran IIS, a ne koristi se, najjednostavnije ali i najefektivnije rješenje je isključiti ga, onemogućiti. To se jednostavno može postići odabirom Dodaj ili ukloni programe (Add or remove programs) unutar upravljačke ploče, te zatim odabirom Dodaj ili ukloni Windows komponente (Add or remove Windows components) i isključenjem Internet Information Services (IIS). Izmjene potvrđujemo i postupak završavamo klikom na Završi (Finish). Te nakon toga isključiti, onemogućiti sve uključene Windows usluge (Windows services) koje su vezane za IIS.

U slučaju da se ipak koriste takve usluge, potrebno je poduzeti određene korake i držati se nekih pravila kako bi napad na računalo preko IIS-a bio što manja mogućnost.

Potrebno je redovno provjeravati ažurnost IIS računala, pogotovo onih koji su postavljeni na automatsko ažuriranje, kako bi osiguralo da dobivaju sve zakrpe potrebne za održanje sigurnosti. Zakrpe, ispravke i nadopune je potrebno primjenjivati što je prije moguće, čim su izdani i dovoljno testirani.

Web sadržaj bi trebalo osigurati i korištenjem IIS poslužiteljskih dopuštenja (permissions) i NTFS dopuštenja, ne samo jednim od njih.

Potrebno je zatvoriti sve one priključne točke (port) koje nisu apsolutno nužne, odnosno instalirati vatrozid i skriti (stealth) sve priključne točke. Mudro bi bilo i izbrisati sve web stranice i direktorije, pogotovo administrativne instalacijske skripte, koje bi mogle biti upotrijebljene za pribavljanje punog prava pristupa računalu.

ISAPI (Internet Services Application Programming Interface) omogućuje interakciju IIS sa tehnologijama poput ASP-a, .NET-a, i drugih dinamičkih jezika. No, to također predstavlja i sigurnosnu ranjivost. ISAPI filtre bi trebalo koristiti samo ako su potrebni. Sve nekorištene ISAPI filtre bi trebalo izbrisati.

Te, na kraju krajeva, možda bi bilo dobro i razmisliti o alternativama, koristiti Apache za poslužitelje koji su povezani na Internet, a IIS koristiti samo interno.

Windows messenger

Windows messenger je alat za trenutne poruke (instant messaging - IM) koji dolazi s Windows XP operacijskim sustavom. Zaključno sa verzijom 5.1 Microsoft je prestao s razvijem tog alata i usredotočili su se na razvoj Windows Live Messengera (prijašnjeg MSN Messengera). Dodatke za Windows Messenger više nije moguće preuzeti, već se korisnicima preporučuje da preuzmu Windows Live Messenger s Interneta i koriste njega. Dakle, bez potrebe za ikakvom analizom tog alata, dovoljno je s obzirom na taj podatak reći da je najbolji potez ukloniti Windows Messenger, na isti način kao i IIS, unutar upravljačke ploče odabrati Dodaj ili Ukloni programe, zatim Dodaj ili ukloni Windows komponente, te odabrati Windows messenger.

Nakon toga, ako se koristi takav oblik komunikacije, potrebno je razmotriti alternative. Pored one najpoznatije, Windows Live Messengera, koji je i preporučen kao zamjena, tu su još i Yahoo! Messenger, AOL Messenger i slični. Isto tako, moguće je i odlučiti se za aplikaciju koja nije samo IM program. Dobar primjer za to je Trillian, alat za razgovor (chat) koji podržava sve navedene, kao i ICQ i IRC, te pruža i dodatne sigurnosne mogućnosti koje drugi individualni IM

alati ne nude, kao što je šifrirana komunikacija, potpora za poslužitelje opunomoćenike (proxy) i sl. Trillian dolazi u besplatnoj i komercijalnoj Pro verziji.

Pored alata koji se koristi, u općenitoj komunikaciji trenutnim porukama bi se trebalo inače držati nekih pravila. Trenutne poruke su vid komunikacije koji koristi nekoliko stotina milijuna ljudi na svijetu. A s obzirom na sam koncept, postoji mnoštvo ranjivosti koje se iz dana u dan sve više iskorištavaju. Razne vrste malicioznih programa i spama usmjerene su samo na IM programe i komunikaciju trenutnim porukama. Nisu rijetki crvi koji dalje šalju sami sebe svima na listi prijatelja, uz razne neuobičajene tekstove i izjave, princip sličan kao i kod e-mailova, socijalni inženjering i privitci.

S obzirom na činjenicu da većina takve komunikacije putuje Internetom nezaštićena, nešifrirana, potrebno je paziti i nikada ne razmjenjivati privatne ili osjetljive podatke.
Treba biti pažljiv u dijeljenju nadimaka i dodavanju kontakata na listu prijatelja. Oprezno pristupiti dijeljenju datoteka. Uvijek bi trebalo koristiti program za detekciju virusa, održavati ga ažurnim, te njime skenirati sve datoteke koje se preuzimaju putem IM alata, prije njihova otvaranja. Isto tako, treba redovno ažurirati IM alat, redovno instalirati sve sigurnosne zakrpe i koristiti uvijek najnoviju verziju tog programa.

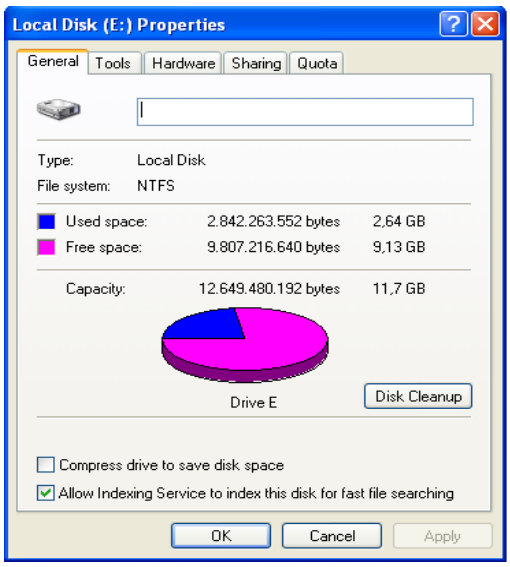
Nikad ne klikati na linkove umetnute u tekst trenutnih poruka, čak i ako dolaze od „poznate“ osobe. Sve poruke od osoba koje nisu na listi prijatelja treba odbiti; a slučaju primanja nekih neuobičajenih ili čudnih tekstova od nekog s liste prijatelja, treba prekinuti sjednicu i kontakt ukloniti s liste.

4. PRAKTIČNI DIO (eksperiment)

4.1. INSTALIRANJE OPERACIJSKOG SUSTAVA

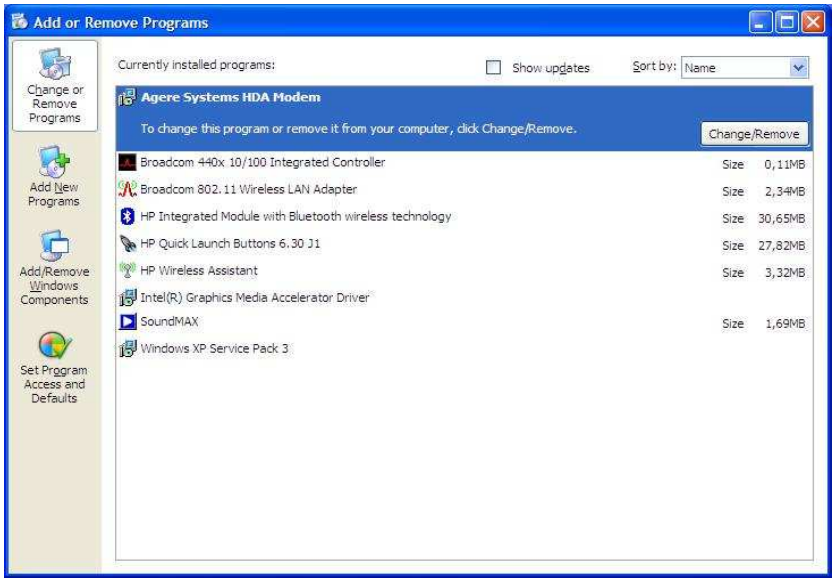
Na prijenosnom računalu s tvrdim diskom kapaciteta 120 GB za izvođenje eksperimenta odvojena je particija kapaciteta 11,7 GB (Local Disk (E:)).

Na odvojenoj particiji instaliran je Windows XP Professional operacijski sustav s integriranim uslužnim paketom 2 (Service Pack 2). Nakon instalacije, zauzeće tvrdog diska iznosi 2,64 GB., kao što je vidljivo na slici 4.1.



Slika 4.1. - Zauzeće tvrdog diska nakon instalacije operacijskog sustava

Nakon instalacije operacijskog sustava, na računalu je instaliran uslužni paket 3 (Service Pack 3). Instalacija Windows XP Professional operacijskog sustava s integriranim uslužnim paketom 2 je odabrana zbog toga što je za instalaciju uslužnog paketa 3 potrebno imati instaliran minimalno uslužni paket 1, a preporučuje se uslužni paket 2. Nakon instaliranja uslužnog paketa 3, na računalo su instalirani svi potrebni pogonski programi (driver) – slika 4.2.



Slika 4.2. Prikaz popisa instaliranih programa nakon instalacije uslužnog paketa 3 i pogonskih programa

Nakon instalacije pogonskih programa obavljeno je ažuriranje operacijskog sustava. Uspostavljena je veza s Internetom i s Windows Update web mjesta preuzete sve preostale važne nadopune i zakrpe koje nisu instalirane uslužnim paketom 3.

4.2. POSTAVKE OPERACIJSKOG SUSTAVA

Prilikom instalacije operacijskog sustava, kao Ime računala (Computer Name) uneseno je – Home, a kao naziv administratorskog korisničkog računa koji se kreira prilikom instalacije (Your Name) uneseno je korisničko ime „Korisnik“ i odabrana lozinka prethodno navedena kao primjer u poglavlju rada koje govori o lozinkama – „$1gurn@_L0Z1NK@“.

Nakon instalacije operacijskog sustava, uslužnog paketa 3 i pogonskih programa, te ažuriranja operacijskog sustava, započeta je primjena svih predloženih izmjena u postavkama operacijskog sustava.

Automatsko ažuriranje

Opcija automatskog ažuriranja (Automatic Updates) postavljena je na način da je odabrana opcija „Obavijesti me, ali nemoj automatski preuzimati ili instalirati nadopune“ (Notify me, but don't automatically download or install them).

Korisnički računi i lozinke

Budući da je osnovnom administratorskom korisničkom računu već dodijeljeno korisničko ime koje ne daje naslutiti da je riječ o administratorskom računu i postavljena sigurna lozinka, kreira se novi korisnički račun s ograničenim pravima (Limited user) kojemu je dodijeljeno korisničko ime „administrator“ i postavljena lozinka „JsAK.I23g!“, koja je također navedena kao primjer sigurne lozinke u poglavlju rada koje govori o lozinkama.

Nakon toga je računalo ponovno pokrenuto u sigurnom načinu rada (Safe Mode) da bi se pristupilo skrivenom administratorskom računu. Tom korisničkom računu je promijenjeno korisničko ime u „Bezimeni“ i dodijeljena lozinka „&eZ1mEN!“.

Prilikom ponovnog pokretanja računala u normalnom načinu rada izmijenjene su postavke politike lozinki (Password policy). Postavka omogućavanja pamćenja lozinki je uključena i odabrana vrijednost od pet jedinstvenih lozinki koje moraju biti korištene prije nego se neka stara može ponovo upotrijebiti. Postavka maksimalnog trajanja lozinke postavljena je na 90 dana, a minimalno trajanje lozinke postavljeno na 1 dan. Uključena je i opcija minimalne duljine lozinke i najmanji broj znakova koji mora sadržavati postavljen na 8. Opcija koja traži da lozinka mora zadovoljavati uvjete kompleksnosti također je uključena, dok je opcija pohrane lozinke korištenjem reverzibilnog šifriranja isključena.

Postavke vezane za politiku zabrane pristupa računu (Account lockout policy) izmijenjene su na način da je opcija Granica zabrane pristupa uključena i broj pokušaja postavljen na 5. Prilikom postavljanja te vrijednosti, za ostale dvije opcije (Trajanje zabrane pristupa i Resetiranje brojača pogrešnih pokušaja) ponuđena je vrijednost od 30 minuta, koja je ostavljena.

Windows usluge

Windows usluge koje su u poglavlju 3.5.4. navedene kao usluge koje direktno utječu na sigurnost isključene su. Na računalu nije instaliran IIS, pa vezane usluge ne postoje. Usluge „Alerter“ i „Messenger“ su instalacijom uslužnog paketa 2 standardno isključene i takvima su ostavljene. Isključene su usluge „DCOM Server Process Launcher” i “Error reporting”. Usluga “Netmeeting Remote Desktop Sharing” također je već isključena pa postavke nisu mijenjane. Usluga „Remote Desktop Help Session Manager” koja je bila postavljena na ručno pokretanje, isključena je. Prije isključivanja te usluge, u postavkama sustava (System), unutar kartice

Udaljeno (Remote) isključena je opcija daljinske podrške (Remote Assistance). „Remote Registry" usluga je isključena, kao i usluge „SSDP Discovery Service" i "Universal Plug and Play device host". Usluge „Routing and Remote Access" i"Telnet" ostavljene su isključenima.

Čuvar zaslona

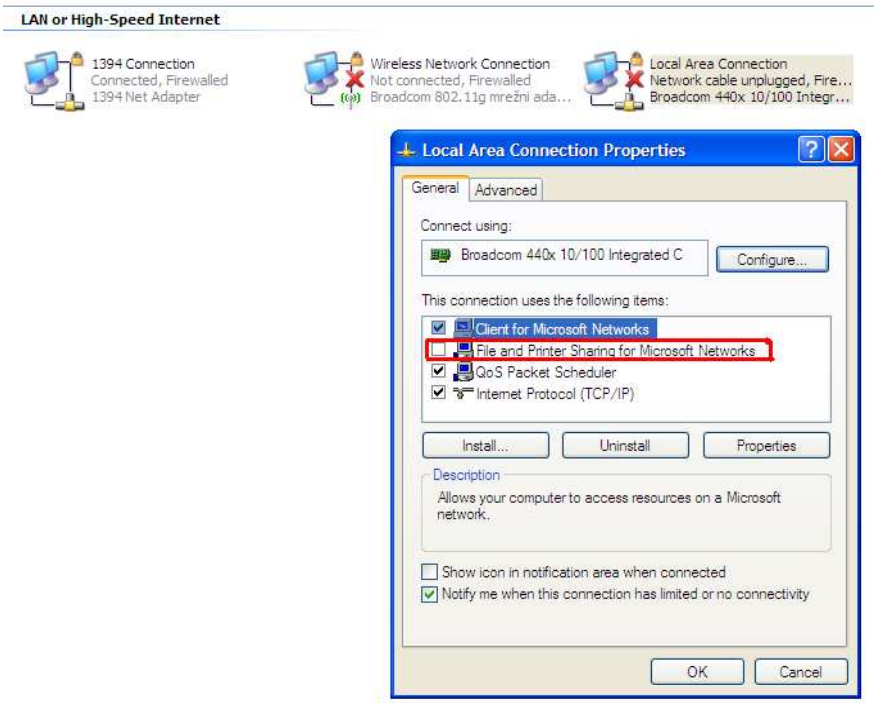
Za čuvar zaslona uključena je opcija zahtjeva za unošenjem lozinke korisničkog računa (On resume, display welcome screen), te unutar pomagala za rad s registrima promijenjene su vrijednosti datoteke SCRNSAVE.EXE i stavke „ScreenSaveActive" da bi se eliminirala spominjana ranjivost.

Automatsko pokretanje (AutoRun i AutoPlay)

Usluga automatskog pokretanja za dostupni DVD pogon, kao i za sve vanjske izmjenjive pogone i uređaje je isključena.

Dijeljenje resursa (File and printer sharing i Simple file sharing)

Dijeljenje datoteka i pisača je isključeno i to za sve dostupne mrežne veze (slika 4.3.)



Slika 4.3. – Isključivanje dijeljenja datoteka i pisača za dostupne mrežne veze

Usluga jednostavnog zajedničkog korištenja datoteka (Simple file sharing) također je isključena.

Postavke za obje vrste ekstenzija, one uobičajene, kao i posebne ekstenzije operacijskog ustava su izmijenjene na način da je uključeno prikazivanje tih ekstenzija.

Za datoteku sa stranicom memorije (Pagefile) izmjenom unutar registara postavljeno je da operacijski sustav očisti datoteku prilikom svakog isključivanja računala.

Ispis memorije (Dump File) je također isključen.

Za postupanje sa skriptnim jezicima Windows operacijskog sustava (VBScript Script File, JScript Script File, JScript Encoded Script File, VBScript Encoded Script File, Windows Script File) postavke su izmijenjene na način da je zadržana mogućnost njihova korištenja, ali je spriječeno njihovo automatsko pokretanje.

Unutar opcija za dodavanje i uklanjanje Windows komponenti, uklonjen je Windows Messenger.

4.3. INSTALIRANJE ZAŠTITNIH PROGRAMA

Instaliran je osnovni komplet besplatnih zaštitnih programa:

Program za zaštitu od virusa – AVG Anti-Virus Free Edition

Programi za zaštitu od špijunskog koda – Spybot Search & Destroy i Spyware Blaster

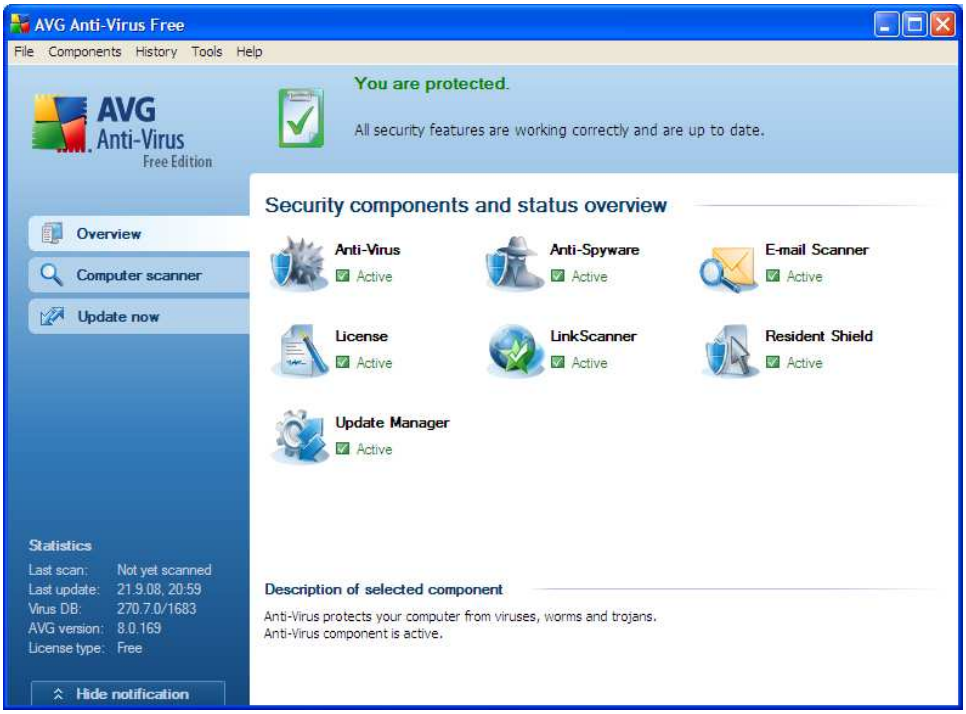
Vatrozid – Comodo Firewall Pro

Program za zaštitu od virusa – AVG Free 8.0

(http://free.avg.com/ww.download-avg-anti-virus-free-edition)

AVG Anti-Virus Free Edition, poznati program koji ima aktivnu zaštitu od virusa i špijunskog koda, mogućnost skeniranja računala, provjeru sigurnosti za rezultate pretraživanja, automatsko ažuriranje i besplatan je za kućnu osobnu uporabu.

Nakon instalacije AVG Free programa (verzije 8.0.169) i njegovog ažuriranja, zaštita od virusa je aktivirana (slika 4.4).



Slika 4.4. – Sučelje AVG Free 8.0 programa

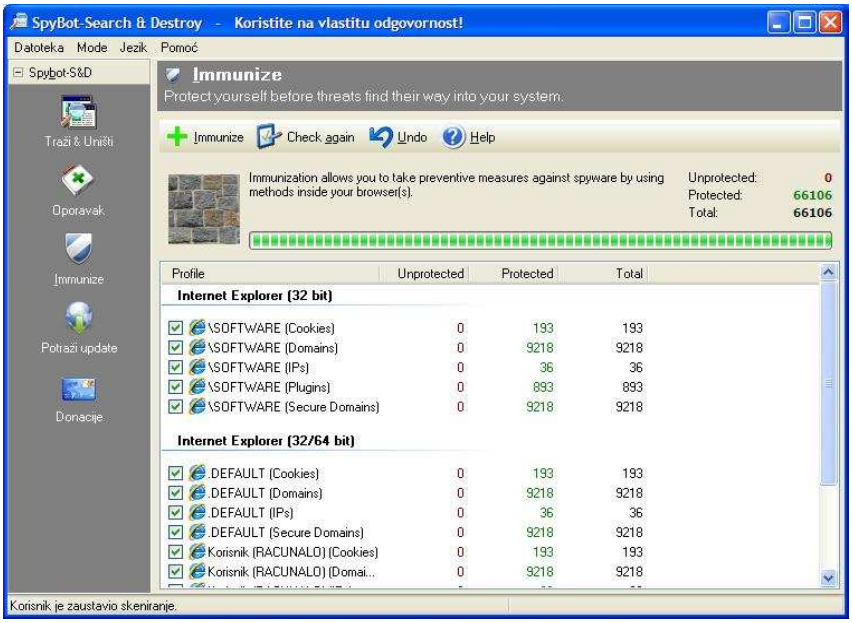
Programi za zaštitu od špijunskog koda

Spybot Search & Destroy

http://www.safer-networking.org/hr/spybotsd/index.html

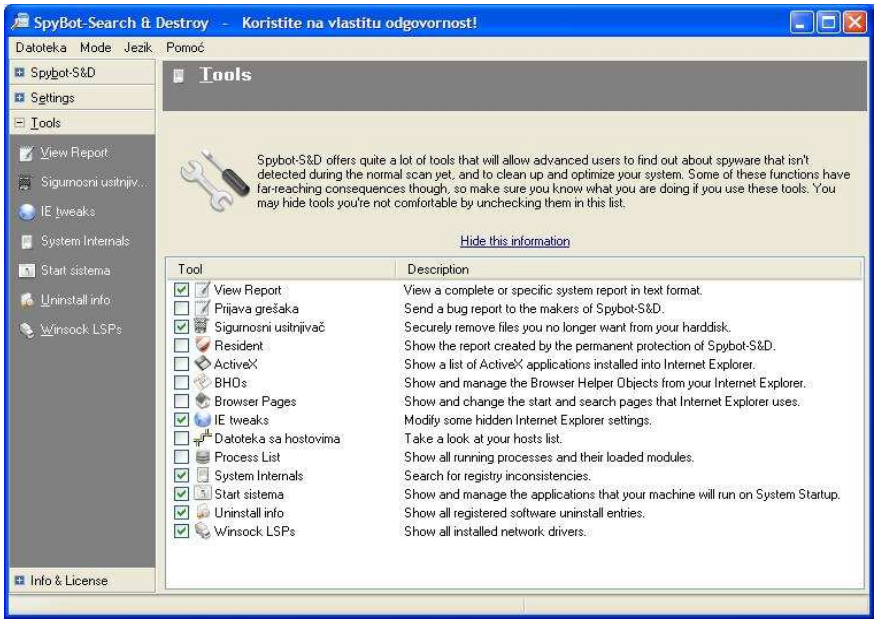
Spybot Search & Destroy, vrlo poznat i cijenjen program za skeniranje špijunskog koda, reklamnog koda, otimača i drugih malicioznih programa, ranije spominjan u poglavlju o zaštitnim programima. Besplatan je, ima podršku za 40 različitih jezika, uključujući i Hrvatski. Ima mogućnost imunizacije (Immunize) koja sprečava postavljanje kolačića koji prate navike i instaliranje nekih poznatih malicioznih programa s tim da mogućnost imunizacije radi sa sva tri najpoznatija web preglednika. Isto tako, nudi i aktivnu zaštitu Internet Explorera (Resident SDHelper) i aktivni nadzor čitavog sustava (Resident TeaTimer) koji obavještava korisnika o aktivnostima procesa i pokušajima izmjena postavki registara i sl.

Nakon instaliranja Spybot Search & Destroy programa (verzije 1.6.0.30), pokrenuto je ažuriranje i zatim imunizacija sustava od svih novih malicioznih programa obuhvaćenih novim preuzetim definicijama (slika 4.5).



Slika 4.5. – Sučelje Spybot Search & Destroy programa, opcija imunizacije

Nakon obavljenog ažuriranja i imunizacije, pregledane su osnovne postavke i uključena aktivna zaštita. Za podešavanje tih postavki potrebno je prijeći u napredni način rada (Advanced Mode) i odabrati opciju Alati (Tools) – slika 4.6.



Slika 4.6. – Napredni način rada, opcija Alati (Tools) s prikazanim standardnim postavkama

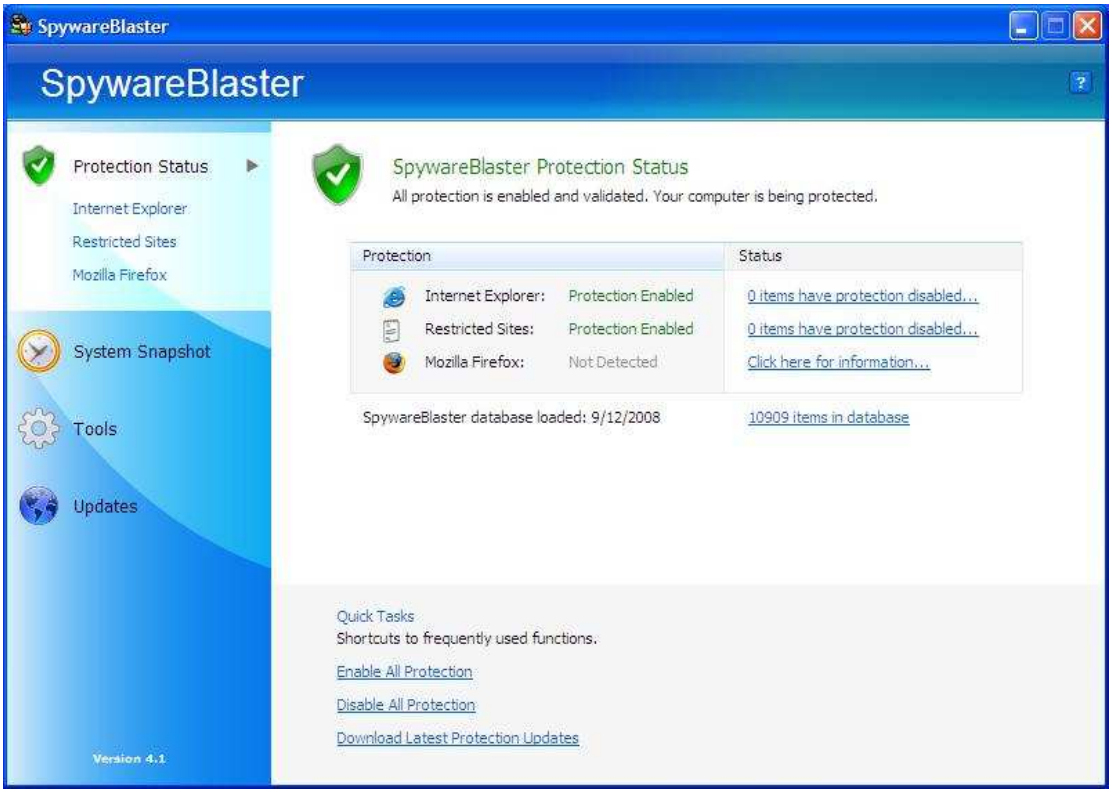
Spyware Blaster

http://www.javacoolsoftware.com/spywareblaster.html

Spyware Blaster je također već spomenut zaštitni program koji ima preventivni pristup zaštiti od malicioznih nametnika. Sprečava instaliranje ActiveX baziranog špijunskog i reklamnog koda, otimača web preglednika (browser hijacker), birača (dialer) i drugih nametnika. Blokira

postavljanje kolačića koji prate navike i instaliranje špijunskog koda za Internet Explorer i Mozilla Firefox preglednike, te ograničava radnje potencijalno malicioznih web mjesta u Internet Exploreru. Za razliku od drugih takvih programa Spyware Blaster ne mora stalno biti aktivan u memoriji da bi zaštita bila na snazi. Besplatan je za osobne i edukativne svrhe. Jedino je za opciju automatskog ažuriranja potrebno platiti godišnju naknadu, dok je ručno ažuriranje i dalje besplatno.

Instaliran je Spyware Blaster program, verzija 4.1, uključena sva zaštita i obavljeno ažuriranje programa. Nakon toga je ponovno uključena sva zaštita uključujući i nove preuzete definicije.



Slika 4.7. – Početni prozor Spyware Blaster programa nakon uključenja čitave zaštita i ažuriranja programa

Comodo Firewall Pro

http://www.personalfirewall.comodo.com/

Comodo vatrozid je dosta poznat i hvaljen besplatni vatrozid. Nudi zaštitu od hakera, špijunskog koda, trojanaca i krađe identiteta.

Defense+, sustav otkrivanja uljeza (Intrusion Prevention System) sprečava instaliranje malicioznih programa. Provjerava integritet svakog programa prije nego dopusti učitavanje u memoriju i upozorava svaki put kad se nepoznata ili nepouzdana aplikacija pokuša pokrenuti ili instalirati. Sprečava nedopušteno modificiranje ključnih datoteka i registarskih vrijednosti operacijskog sustava. Defense+ sustav nudi 5 nivoa zaštite od kojih je najzanimljiviji Clean PC Mode. To je nivo zaštite koji pregleda čitav sustav i registrira sve postojeće programe kao sigurne. Od te točke nadalje, instaliranje je dozvoljeno samo za aplikacije koje se nalaze u Comodo White list Database, bazi podataka s preko milijun pouzdanih, sigurnih programa, te aplikacije za koje korisnik eksplicitno dozvoli instaliranje.

Skrivanje (Stealth Mode) omogućuje potpunu nevidljivost računala hakerima i skeniranju priključnih točaka (port scan).

Ima sučelje koje je dobro organizirano, intuitivno i ugodno za rad, s mnoštvom mogućnosti konfiguriranja i postavljanja pravila. Isto tako, nudi i besplatno ažuriranje.

Na računalu je instaliran vatrozid Comodo Firewall Pro, verzija 3.0.25.378, pri čemu je od ponuđenih 5 nivoa zaštite vatrozida (Firewall Security level) odabran „Training Mode“, odnosno postavljen je u stanje učenja. Korištenjem učenja za postavljanje pravila, vatrozid će upozoravati na radnje ili aplikacije u hodu, kako se događaju. Kad prikaže upozorenje, korisnik može odobriti radnju ili je zabraniti jednokratno, a može i odrediti da se odabir zapamti i usvoji kao pravilo. U tom slučaju više se neće ponavljati to isto upozorenje za tu istu radnju, već će se primijeniti pravilo.

Za Defense+ sustav ostavljen je predloženi, već postavljeni nivo - Clean PC Mode.

Slika 4.8. – Početni prozor Comodo Firewall Pro vatrozida s postavljenim nivoima zaštite

4.4. TESTIRANJE

Nakon instaliranja, ažuriranja i podešavanja operacijskog sustava, te instaliranja potrebnih zaštitnih programa provedeno je testiranje sigurnosti sustava.

Prvi dio testiranja proveden je pomoću programa Nessus.

Nessus je opsežan obuhvatan program za skeniranje sustava u potrazi za potencijalnim ranjivostima. Besplatan je za osobnu uporabu, te uporabu u neprofitne komercijalne svrhe. Može se preuzeti na web mjestu http://www.nessus.org/download/

Skenira u potrazi za ranjivostima koje omogućuju udaljenom napadaču da kontrolira ili pristupi osjetljivim podacima na sustavu. Traži pogrešne konfiguracije postavki (krive postavke, zakrpe koje nedostaju i sl.). Pregledava postavljene lozinke na nekim korisničkim računima sustava. Traži otvorene priključne točke. Ranjivosti za DoS napade TCP/IP stoga (stack), i drugo.

Nessus projekt započet je 1998. godine i trenutno je u trećoj verziji (Nessus 3). Tek s trenutnom verzijom testiranje je omogućeno i za Windows sustave, dok je ranije to bio program namijenjen testiranju sigurnosti UNIX sustava.

Instalacija Nessus Clienta za Windows sustave je spojena s Nessus Windows Server poslužiteljem. Nessus Server se instalira u slučaju korištenja sigurnosnog centra (Nessus Security Center) što je opcija za mrežna okruženja i velike sustave. Za testiranje jednog računala, kao što je slučaj kod ovog eksperimenta, dovoljno je instalirati Nessus Client koji je zapravo optimiziran Nessus 3 skener s grafičkim korisničkim sučeljem. Osnovne funkcionalnosti Nessus Clienta treće verzije su grafičko korisničko sučelje koje prikazuje rezultate skeniranja u realnom vremenu tako da nije potrebno čekati kraj skeniranja za pregled rezultata. Omogućuje kreiranje politika, različitih profila s različitim pravilima skeniranja te spremanje tih politika u .nessus formatu. Sjednica politike, popis ciljeva skeniranja (meta) i rezultati više testova mogu biti spremljeni unutar jedne .nessus datoteke, koja se lako može izvoziti.

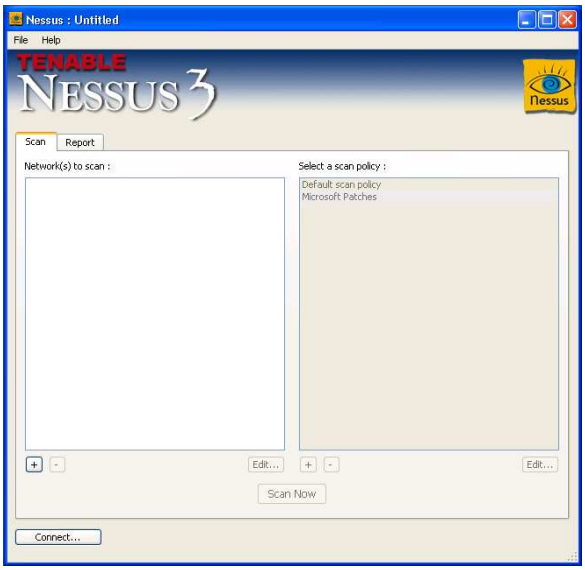
Za preuzimanje programa potrebno je na web mjestu unijeti kontakt podatke. Nessus 3 distribuira se kao izvršna instalacijska datoteka. Instalacija programa izvršava se pomoću instalacijskog čarobnjaka. Instalaciju je potrebno obaviti pomoću korisničkog računa s administratorskim pravima. Prilikom instalacije ponuđena je opcija instaliranja Nessus Servera, Nessus Clienta ili oba.

Nakon odabira instalacije (u ovom slučaju Nessus Clienta) potrebno je unijeti aktivacijski kod koji se dobije putem elektroničke poruke, prilikom registracije na Nessus web mjestu.

Prilikom instalacije Nessus kreira Windows uslugu koja je potrebna za izvođenje skeniranja, te je postavlja na automatsko pokretanje.

Nessus testiranje obavlja korištenjem mnoštva dodataka (plug-in) ili skripta. Novi dodaci se izdaju svaka 24 sata stoga je bitno održavati program ažurnim, da bi skeniranje bilo što je preciznije i točnije moguće.

Na računalu je instaliran Nessus Client, verzija 3.2.1.1 i obavljeno ažuriranje najnovijih dodataka. Nakon instalacije pokrenut je Nessus Client program (slika 4.9)



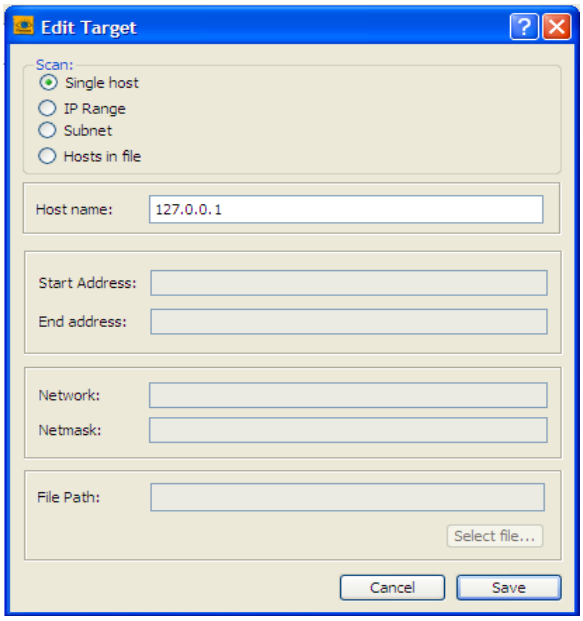
Slika 4.9. – Sučelje Nessus Client programa – početni prozor

Nakon pokretanja potrebno se povezati s Nessus poslužiteljem klikom na Connect i odabirom „localhost”, koji je postavljen kao zadani za Windows sustave.

Nakon povezivanja s poslužiteljem, postavke zadane politike skeniranja moguće je urediti i prilagoditi osobnim potrebama klikom na polje Edit s desne strane prozora. Tada se otvara dijaloški okvir s mnoštvom opcija za uređivanje svih postavki, uključujući postavke mreže, politike skeniranja, odabira svih željenih dodataka (plug-in) koji će se koristiti za skeniranje i

drugo. Za ovaj eksperiment ostavljene su sve zadane postavke, koje su zadovoljavajuće za konkretne potrebe.

Nakon uređivanja postavki potrebno je odabrati cilj testiranja (Network(s) to scan). Klikom na polje s znakom (+) s lijeve strane u početnom prozoru otvara se dijaloški okvir za odabir mete (Edit Target). Kada se testiranje obavlja na samo jednom računalu, odnosno na računalu na kojem je instaliran Nessus, kao što je ovdje slučaj, potrebno je odabrati opciju Single host i u polje Host Name upisati internu IP adresu 127.0.0.1, kao što je prikazano na slici 4.10. i zatim kliknuti na Save.



Slika 4.10. – Dijaloški okvir za odabir mete testiranja

Nakon unosa svih potrebnih podataka, tipka Scan Now postaje dostupna. Testiranje računala jednostavno se započinje klikom na nju. Rezultate skeniranja moguće je vidjeti već prilikom skeniranja, odabirom kartice Report unutar početnog prozora, te klikom na znak +, pokraj IP adrese i odabirom željene stavke. Nakon završetka skeniranja izvješće je moguće izvesti (Export) u obliku .html dokumenta. U slučaju da su postavke politike skeniranja spremljene u .nessus datoteku, rezultate skeniranja moguće je dodati toj datoteci.

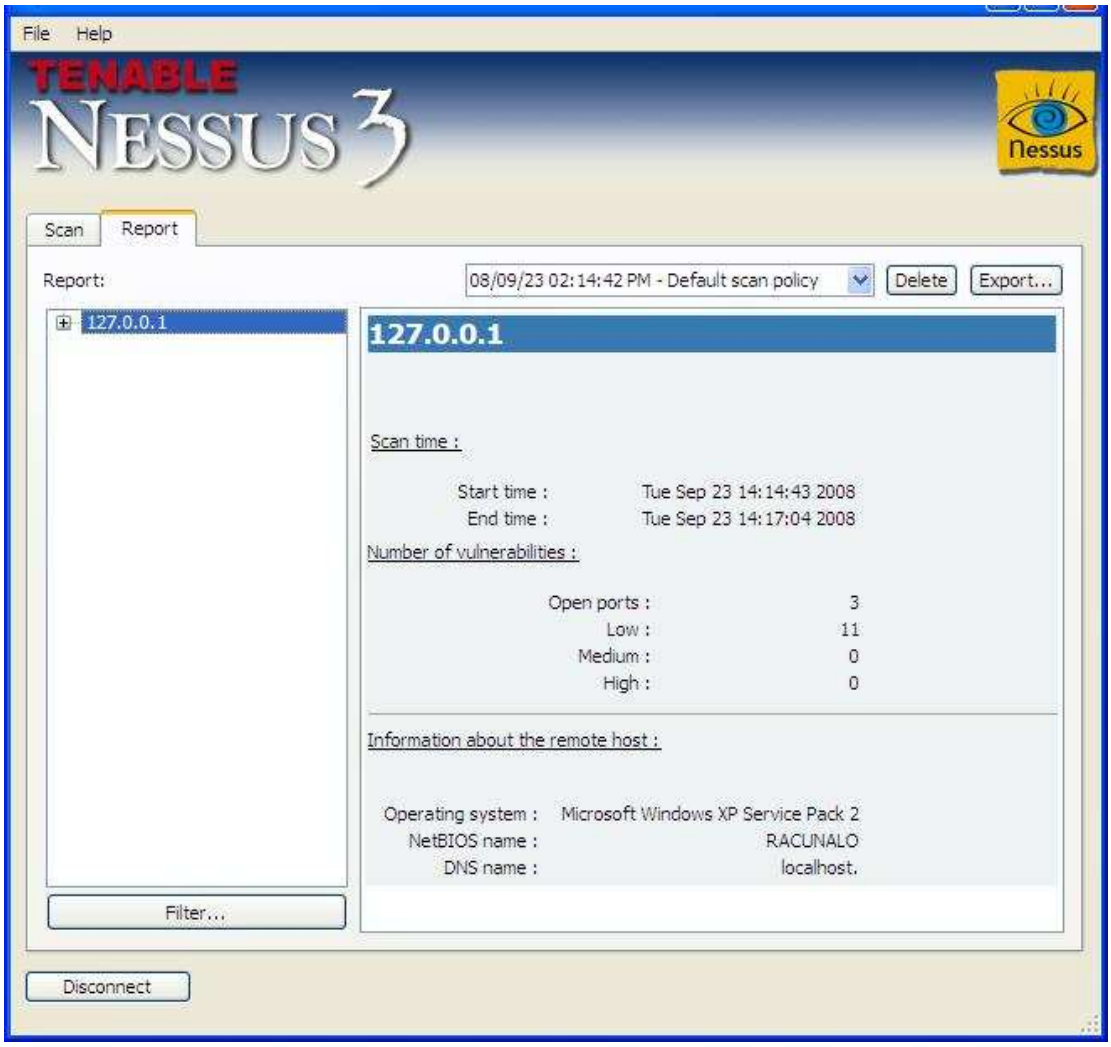
Za pravilne rezultate testiranja, za vrijeme provođenja skeniranja treba imati uspostavljenu vezu s Internetom.

Nakon odabira mete testiranja pokrenuto je testiranje računala korištenog za ovaj eksperiment. Testiranje je započeto 23.09.2008 u 14:14:43 sata, a dovršeno u 14:17:04 sati, dakle testiranje je ukupno trajalo 2 minute i 21 sekundu.

Testiranjem je otkriveno 11 ranjivosti niske težine i 3 otvorene priključne točke. Čitavo izvješće nalazi se u Prilogu, na kraju rada.

Ranjivosti su vezane za poslužitelje koji slušaju na otvorenim priključnim točkama (TCP priključna točka 135 – DCE/RPC poslužitelj i UDP priključna točka 123 – NTP poslužitelj), te više problema vezanih za TCP priključnu točku 445 (ranjivosti koje omogućuju pribavljanje nekih podataka o računalu i mogućnost povezivanja s računalom pomoću „NULL session“ sjednica.

Za sve prijavljene ranjivosti Nessus navodi da je faktor rizika jednak nuli.



Slika 4.11. – Rezultati testiranja unutar prozora Nessusa

Drugi dio testiranja proveden je pomoću jednostavnog besplatnog programa naziva **PC Security Test**, koji se može preuzeti na http://www.pc-st.com/us/download.htm

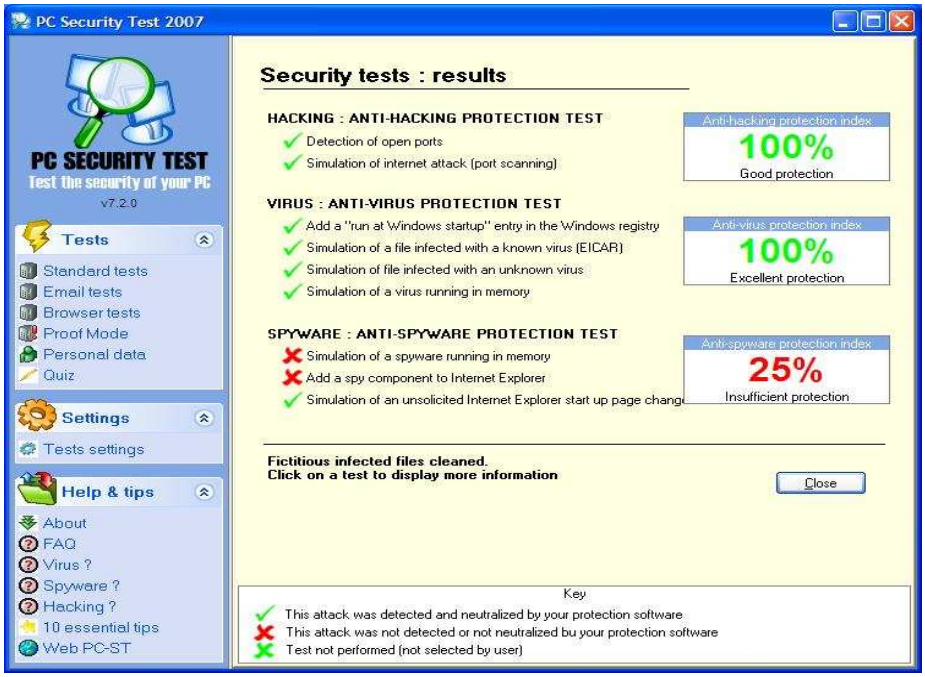
To je program za Windows sustave koji provjerava zaštitu računala od virusa, špijunskog koda i napada. Zapravo provjerava učinkovitost zaštitnih programa.

Testiranje se odvija na način da program simulira viruse, špijunske programe i hakerske napade, te unutar 3 minute čeka i nadgleda reakcije zaštitnih programa. Nakon što test završi, program prikazuje izvješće o testiranim elementima i rezultatima. Pored tog standardnog testa, nudi i nekoliko manjih testova za provjeru sigurnosti web preglednika, e-mail klijenta i slično, te nudi neke kvizove, savjete i dodatne izvore informacija.

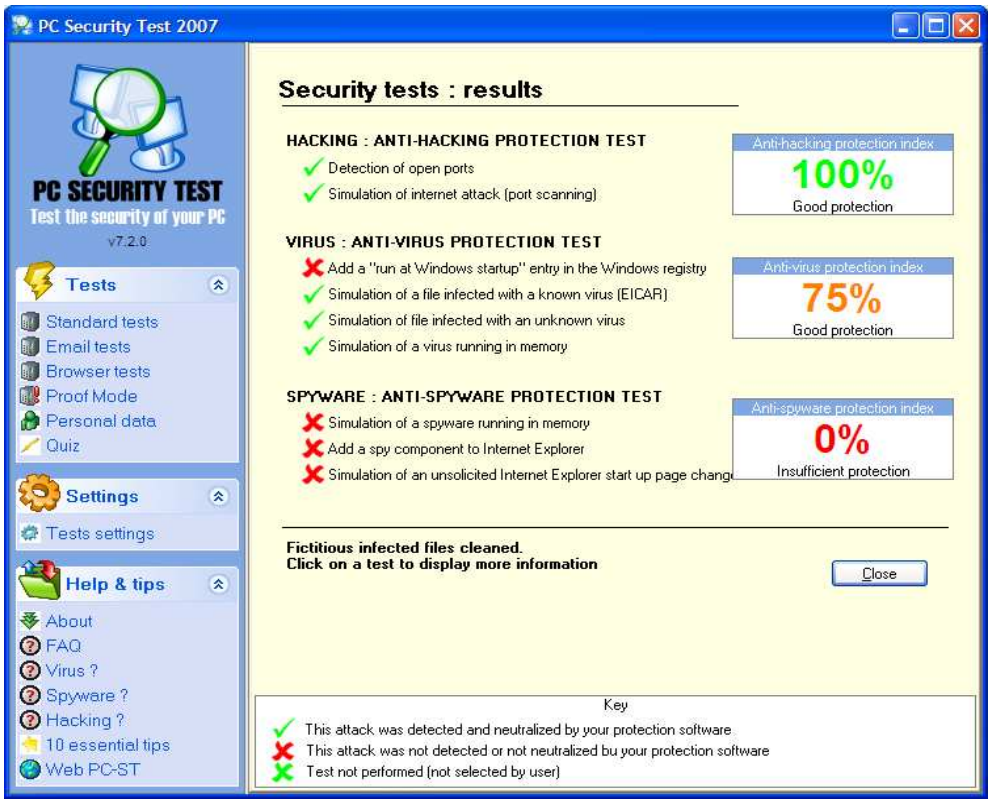
Slika 4.12. – Početni prozor PC Security Test programa

Pokrenut je Standardni test, s instaliranim prethodno navedenim besplatnim zaštitnim programima. Tijekom testiranja AVG Free program je prijavio nekoliko pronalazaka inficiranih datoteka i jedan potencijalno neželjeni program (potentially unwanted program), dok je Spybot S&D aktivna zaštita (TeaTimer) prijavila pokušaj izmjene odnosno dodavanja unosa na listu polaznih programa (Startup) i pokušaj izmjene početne stranice web preglednika. Rezultati testiranja prikazani su na slici 4.13.

Nakon prvog testiranja, napravljeno je još jedno testiranje, ovaj put s isključenom rezidentnom zaštitom Spybot S&D programa, odnosno s isključenim i Resident SDHelper i Resident TeaTimer funkcijama.Rezultati drugog testiranja prikazani su na slici 4.14.



Slika 4.13. - Rezultati testiranja PC Security Test programom



Slika 4.14. – Rezultati testiranja PC Security Test programom, nakon isključenja aktivne zaštite Spybot S&D programa

Jasno je vidljivo da kod isključene komponente aktivne zaštite Spybot S&D programa računalo nema apsolutno nikakve zaštite od špijunskog koda; dok je zaštita tek na 25 % kad je aktivna komponenta uključena. Međutim, kad je aktivna zaštita Spybot S&D programa isključena i rezultati AVG Free programa za zaštitu od virusa su na samo 75 %, a to je zapravo realno stanje koje govori da ni virusna zaštita nije posve učinkovita. Spybot S&D kao prvenstveno zaštita od špijunskog i reklamnog koda zapravo nadopunjuje zaštitu od virusa, tj. nadoknađuje nedostatak AVG Free programa. Vidljivo je da ovakva, besplatna zaštita očito odlično funkcionira po pitanju vatrozida, kod zaštite od virusa situacija je nešto lošija, ali recimo zadovoljavajući, dok je zaštita od špijunskog koda jako loša.

Nakon obavljenog instaliranja operacijskog sustava, njegova ažuriranja i izmjene postavki, zatim instaliranja svih zaštitnih programa i njihova ažuriranja, te instaliranja ažuriranja programa za testiranje sigurnosti i obavljanja svih sigurnosnih testova, zauzeće diskovnog prostora iznosi 6,02 GB.

5. ZAKLJUČAK

Tema ovog rada je postavljanje sigurnog kućnog računala. Da bi se računalo moglo kvalitetno zaštititi, potrebno je analizirati prijetnje koje dolaze s mreže, bilo lokalne bilo cijelog Interneta.

U drugom poglavlju ovog rada obrađene su sve sigurnosne prijetnje, rizike i ranjivosti s kojima se susreću korisnici, u vidu raznih zloćudnih programa, prijevara i zamki, te sigurnosnih propusta i slabosti samog Windows XP operacijskog sustava.

U trećem poglavlju promatrani su i analizirani svi načini zaštite od prijetnji spomenutih u drugom poglavlju, u područjima surfanja webom i korištenja elektroničke pošte, elementima operacijskog sustava, te zaštitnim programima.

Četvrto poglavlje sadržava eksperiment u kojem su na instalaciji Windows XP operacijskog sustava primijenjene sve postavke, izmjene i preporuke navedene u trećem poglavlju. Prema rezultatima eksperimenta da se zaključiti nekoliko stvari.

Testiranje Nessusom pokazuje nekoliko ranjivosti unatoč svim poduzetim mjerama predostrožnosti i izmjenama operacijskog sustava. Sve te mjere doista ojačavaju sigurnost, samo prema Nessusu, ranjivosti još ima. Sama brojka od jedanaest ranjivosti može zvučati alarmantno, no ipak, to su ranjivosti male težine, te je za svaku od njih unutar izvješća navedeno da je faktor rizika – ništa, odnosno da te ranjivosti zapravo ne predstavljaju neki sigurnosni rizik. Iako bi bilo dobro eliminirati i te ranjivosti, to nije nešto oko čega se treba pretjerano zabrinjavati. Stoga, po pitanju sigurnosti operacijskog sustava – ranjivostima i propustima u konfiguraciji operacijskog sustava, može se reći da je sustav siguran.

Po pitanju zaštitnih programa, testiranje je pokazalo da je zaštita odabranim besplatnim vatrozidom dobra, da obavlja svoju funkciju baš kako treba.Dakle, kod odabira vatrozida za kućno računalo nema nekih ograničenja – i besplatna zaštita može biti dobra.

Po pitanju programa za zaštitu od virusa, učinkovitost od 75% nije dovoljna. To je još i samo jedan test, s jednom skupinom virusa, a s obzirom da postoje milijuni različitih vrsta virusa i da nove vrste nastaju svakodnevno – zaštita od 75% je potpuno neadekvatna. Istina je da je odabrani program za zaštitu od virusa zakazao u sprečavanju malicioznog programa da postavi unos na listu polaznih programa, a i da je program za zaštitu od špijunskog koda tu nadoknadio nedostatak, ali valja imati na umu da je tu ipak riječ o četiri elementa koji se provjeravaju tim testom i da samo to nije ni približno dovoljno za neke vjerodostojne rezultate. Daje samo mali uvid u situaciju, a s obzirom da odabrani program nije ispunio uvjete ni na tom malom testu, može se generalno zaključiti da ne pruža dovoljnu zaštitu. Možda je situacija ponešto drugačija kod drugih besplatnih programa za zaštitu od virusa, iako to nije vrlo vjerojatno. Razlike među trima najpoznatijim programima za zaštitu od virusa su obično tek u nijansama. S obzirom na sve te podatke, te činjenicu da je zaštita od virusa danas neophodna, možda je bolje rješenje odlučiti se za neki komercijalni proizvod.

Zaštita od špijunskog koda je u ovom slučaju, može se reći – nikakva. Učinkovitost od 25 %, odnosno samo jedan zadovoljen od tri testa, i to sprečavanje izmjene početne stranice Internet Explorera, dok je kod testova sa špijunskim kodom i dodavanjem špijunske komponente u Internet Explorer zaštita potpuno zakazala. Dakle, s obzirom na zaštitu koju pružaju odabrani programi, potrebno je pronaći neko drugo rješenje, neki komercijalni program s kvalitetnom komponentom aktivne zaštite. Dok su ovi drugi, besplatni programi korisni, ali ne kao primarna metoda zaštite, već kao dodatak, nadopuna nekom drugom programu.

Dakle, može se donijeti generalan zaključak da besplatna zaštita ipak nije dovoljna. Vjerojatnost postoji da bi se pravom kombinacijom nekoliko zaštitnih programa i mogla ostvariti dobra

zaštita, ali to je opet previše mukotrpan posao potrage, kombiniranja, instaliranja i održavanja da bi se posezalo za takvim rješenjima kad već postoje odlični programi koji se mogu kupiti za prihvatljive novce. Danas ionako ljudi sve kupuju, zašto ne i ono što je potrebno za sigurnost svojih računala i podatka.

Opasnosti vrebaju sa svih strana i nezaštićeno računalo na Internetu može opstati tek nekoliko minuta a da ne postane inficirano nekom vrstom nametnika, od kojih bi neki mogao izazvati i velike probleme, bilo računalne, osobne, financijske ili sl. Stav većine ljudi, da na njihovim računalima nema nešto toliko važno da bi bila potrebna tolika zaštita je pogrešan. Pored same važnosti zaštite vlastitih podataka, zaštitom svog računala svaki korisnik štiti i druge. Propisna zaštita računala zahtijeva i vremena i truda, kao i sistemskih resursa jer svi ti programi zauzimaju diskovni prostor i svi njihovi aktivni procesi zauzimaju popriličnu količinu radne memorije, ali to su sve popratne „nuspojave“ koje je potrebno prihvatiti kao takve. Sigurnost računala je stalan proces, a ne proizvod i uspostavljanje i održavanje sigurnosti osobnog računala je odgovornost svakog korisnika.

POPIS LITERATURE

1. Allen, R., Gralla, P.: „Windows XP Cookbook“, O'Reilly Media, Inc., Sebastopol, 2005.
2. Anonymous: „Maximum Security, Fourth Edition“, Que Publishing, SAD, 2002.
3. Aycock, J.: „Computer viruses and Malware“, Springer Science + Business Media, New York, SAD, 2006.
4. Ballew, J.: „Hardcore Windows XP“, Osborne/McGraw-Hill, SAD, 2005.
5. Beaver, K.: „Hacking for Dummies“, Wiley Publishing, Inc., Indianapolis, SAD, 2004.
6. Bott, E., Seichert, C.: „Microsoft Windows Security Inside Out for Windows XP and Windows 2000“, Microsoft Press, Redmond, SAD, 2003.
7. Bradley, T.: „Essential Computer Security“, Syngress Publishing, Inc., Rockland, SAD, 2006.
8. DiNicolo, D.: „PC Magazine Windows XP Security Solutions“, Wiley Publishing, Inc., Indianapolis, SAD, 2006.
9. Erbschloe, M.: „Trojans, Worms and Spyware“, Elsevier Inc., Burlington, SAD, 2005.
10. Gregory, P., Simon, M.A.: „Blocking Spam and Spyware for Dummies“, Wiley Publishing, Inc., Indianapolis, SAD, 2005.
11. Grimes, R. A.,: „Malicious Mobile Code: Virus Protection for Windows“, O'Reilly & Associates, Inc, Sebastopol, SAD, 2001.
12. Harley, D., Slade, R., Gattiker, U.: „Viruses Revealed“, Osborne/McGraw-Hill, SAD, 2001.
13. Hassell, J.: „Hardening Windows, Second Edition“, Apress, Berkeley, SAD, 2006.
14. Jurman, D.: „Sigurnost računalnih sustava“, PC CHIP broj 136, rujan 2006. (str. 68 -111)
15. King, J. R.,: „Geeks On Call Security and Privacy: 5-Minute Fixes“, Wiley Publishing, Inc., Indianapolis, SAD, 2006.
16. Leonhard, W.: „Windows XP Hacks and Mods for Dummies“, Wiley Publishing, Inc., Indianapolis, SAD, 2005.
17. Maran, R., Johnson, K.: „Maran Illustrated Microsoft Windows XP 101 Hot Tips“, maranGraphics Inc. & The Thomson Course Technology PTR, SAD, 2005.
18. Nazario, J.: „Defense and Detection Strategies against Internet Worms“, Artech House, Boston, SAD, 2004.
19. Salomon, D.: „Foundations of Computer Security“, Springer Science+Business Media, SAD, 2006.
20. Simmons, C., Causey, J.: „Microsoft Windows XP Networking Inside Out“, Microsoft Press, Redmond, SAD, 2003.
21. Sinchak, S.: „Hacking Windows XP“, Wiley Publishing, Inc., Indianapolis, SAD, 2004.
22. Skoudis, E., Zeltser, L.: „Malware: Fighting Malicious Code“,, Prentice Hall PTR, New Jersey, SAD, 2003.
23. Stevenson, L., Altholz, N.: „Rootkits for Dummies“, Wiley Publishing, Inc., Indianapolis, SAD, 2007.

24. Tulloch, M.: „Microsoft Encyclopedia of Security“, Microsoft Press, Redmond, SAD, 2003.
25. Walker, A.: „Absolute Beginner's Guide To: Security, Spam, Spyware & Viruses“, Que Publishing, SAD, 2006.
26. Wang, W.: „Steal This Computer Book 3: What They Won't Tell You About The Internet“, No Starch Press, San Francisco, SAD, 2003.
27. Wyatt, A.: „Cleaning Windows XP for Dummies“, Wiley Publishing, Inc., Indianapolis, SAD, 2004.
28. Paladin, D.: „Spyware“, s Interneta http://www.borea.hr/upload/files_tbl_korisni/Spyware.pdf
29. „Računalni virusi“, s Interneta http://www.phy.hr/~dandroic/nastava/rm/racunalni_virusi.pdf
30. CARNet CERT: „Priručnik za računalnu sigurnost korisnika Interneta“, s Interneta http://www.carnet.hr
31. „O phishingu – Savjeti za zaštitu od phishinga“, +CERT.hr nacionalno središte za računalnu sigurnost, s Interneta http://www.cert.hr/plainhtmlpage.php?id=701&lang=hr
32. „Windows XP Security Checklist from LabMice.net“, s Interneta http://labmice.techtarget.com/windowsxp/security/default.htm
33. Corbin, K.: „New Tool Provides Security Ratings for E-Biz Search Results“, s Interneta http://www.ecommerce-guide.com/solutions/secure_pay/article.php/3764161
34. „Mozilla Firefox - Features“, s Interneta http://www.mozilla.com/en-US/firefox/features/
35. „Cool Opera Features“, s Interneta http://www.opera.com/support/tutorials/opera/using/coolfeatures/
36. „Security and Privacy in Opera“, s Interneta http://www.opera.com/security/
37. „Windows XP“, Wikipedia, the free encyclopedia, s Interneta http://en.wikipedia.org/wiki/Windows_XP
38. „Overview of Windows XP Service Pack 3“, s Interneta http://www.microsoft.com/downloads/details.aspx?FamilyID=68C48DAD-BC34-40BE-8D85-6BB4F56F5110&displaylang=en
39. „Steps to take before you install Windows XP Service Pack 3“, s Interneta http://support.microsoft.com/kb/950717
40. „Release Notes for Windows XP Service Pack 3“, s Interneta http://download.microsoft.com/download/c/d/8/cd8cc719-7d5a-40d3-a802-e4057aa8c631/relnotes.htm
41. „Safeguard Instant Messaging“, s Interneta http://www.symantec.com/en/uk/security_response/safeguardim.jsp
42. „Windows Messenger“, Wikipedia, the free encyclopedia,s Interneta http://en.wikipedia.org/wiki/Windows_Messenger
43. „Nessus 3.0 Client Guide“, s Interneta http://nessus.org/documentation/nesus_3.0_client_guide.pdf

PRILOG 1. IZVJEŠĆE NESSUS PROGRAMA

List of hosts

127.0.0.1	Low Severity problem(s) found

[^] Back

127.0.0.1

Scan time :

Start time :	Tue Sep 23 14:14:43 2008
End time :	Tue Sep 23 14:17:04 2008

Number of vulnerabilities :

Open ports :	3
Low :	11
Medium :	0
High :	0

Information about the remote host :

Operating system :	Microsoft Windows XP Service Pack 2
NetBIOS name :	RACUNALO
DNS name :	localhost.

[^] Back to 127.0.0.1

Port general/tcp

Host FQDN

127.0.0.1 resolves as localhost.

Nessus ID : 12053

OS Identification

Remote operating system : Microsoft Windows XP Service Pack 2
Confidence Level : 99
Method : MSRPC

The remote host is running Microsoft Windows XP Service Pack 2

Nessus ID : 11936

Information about the scan

Information about this scan :

Nessus version : 3.2.1.1
Plugin feed version : $Date: 2005/11/08 13:18:41 $
Type of plugin feed : CVS
Scanner IP : 127.0.0.1
Port scanner(s) : synscan
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Max hosts : 20
Max checks : 5
Recv timeout : 5
Scan Start Date : 2008/9/23 14:14
Scan duration : 133 sec

Nessus ID : 19506

[^] Back to 127.0.0.1

Port microsoft-ds (445/tcp)

SMB Detection

A CIFS server is running on this port

Nessus ID : 11011

Using NetBIOS to retrieve information from a Windows host

Synopsis:

It is possible to obtain the network name of the remote host.

Description:

The remote host listens on tcp port 445 and replies to SMB requests.
By sending an NTLMSSP authentication request it is possible to obtain
the name of the remote system and the name of its domain.

Risk factor :

None

Plugin output :

The following 2 NetBIOS names have been gathered :

RACUNALO = Computer name
RACUNALO = Workgroup / Domain name

CVE : CVE-1999-0621
Other references : OSVDB:13577

Nessus ID : 10150

SMB NativeLanMan

Synopsis:

It is possible to obtain information about the remote operating system.

Description:

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Risk factor :

None

Plugin output :

The remote Operating System is : Windows 5.1
The remote native lan manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : RACUNALO

Nessus ID : 10785

SMB log in

Synopsis:

It is possible to log into the remote host.

Description:

The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it using one of the following account :

- NULL session
- Guest account
- Given Credentials

See also :

http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Risk factor :

none

Plugin output :

- NULL sessions are enabled on the remote host

CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595
BID : 494, 990, 11199

Nessus ID : 10394

SMB registry can not be accessed by the scanner

Synopsis:

Nessus is not able to access the remote Windows Registry.

Description:

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Risk factor :

None

Nessus ID : 26917

SMB NULL session

Synopsis:

It is possible to log into the remote host.

Description:

The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it using a NULL session.

A NULL session (no login/password) allows to get information about the remote host.

See also :

http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Risk factor :

None
CVE : CVE-2002-1117
BID : 494

Nessus ID : 26920

[^] Back to 127.0.0.1

Port epmap (135/tcp)

MSRPC Service Detection

Synopsis:

A DCE/RPC server is listening on the remote host.

Description:

The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.

However it is not possible to determine the uuid of this service.

Risk factor :

None

Nessus ID : 22319

[^] Back to 127.0.0.1

Port ntp (123/udp)

NTP read variables

Synopsis:

An NTP server is listening on the remote host.

Description:

An NTP (Network Time Protocol) server is listening on this port.

It provides information about the current date and time of the remote system and may provide system information.

Risk factor :

None

Nessus ID : 10884