CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Filtriranje web sadržaja

CCERT-PUBDOC-2009-01-252

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Internet je globalna mreža koja se koristi u privatne, poslovne, obrazovne, znanstvene, informativne i razne druge svrhe. Dostupna je svima i svako računalo s pristupom Internetu sudjeluje u njezinom oblikovanju i stvaranju prometu kroz nju. Posljedično, Internet karakterizira vrlo brzi rast koji potpuno onemogućuje praćenje prometa u mreži. Istovremeno putem Interneta razmjenjuju se povjerljivi podaci, vrše se novčane transakcije i druge osjetljive radnje.

Otklanjanje opasnosti i praćenje prometa na Internetu nemoguće je radi njegove veličine, dostupnosti i brzine rasta. Zato je sigurnost podataka i korisnika na Internetu potrebno je osigurati prepoznavanjem opasnosti i njihovim izbjegavanjem. Upravo je prepoznavanje potencijalno opasnih podataka zadatak filtriranja web sadržaja.

Radi se zapravo o postupku ocjenjivanja web sadržaja kao prihvatljivog ili neprihvatljivog prema određenom kriteriju. Neprihvatljiv sadržaj potom se odbacuje, a prihvatljiv se propušta do krajnjeg korisnika. Sam pojam donosi dosta kontroverzi jer provjera informacija jest pozitivan pojam (kada se primjerice radi o ponašanju djece), ali i negativan jer može značiti cenzuru i oduzimanje sloboda.

2. Opasnosti na Internetu

Internetom kola gomila podataka. Neki od njih su korisni, neki beskorisni, a neki mogu biti štetni. Pornografske stranice štetan su sadržaj za dijete koje na njih naiđe, dok nisu štetan sadržaj za punoljetnog korisnika koji ih sam traži. Programi čija je svrha narušiti učinkovitost rada računala štetni su za bilo kojeg korisnika. Isto vrijedi i za programe pomoću kojih napadač nastoji doći do povjerljivih i osjetljivih podataka. Također, raznorazne stranice i pokušaji prijevare putem poruka elektroničke pošte mogu biti štetni za naivnog korisnika koji na njih nasjedne, dok za upućenog korisnika predstavljaju samo gubitak vremena i beskorisne podatke.

Vješti hakeri koji dobro poznaju mehanizme komunikacije i razmjene podataka na Internetu mogu načiniti štetu, a da korisnik toga nije niti svjestan. Ponekad je za zlouporabu dovoljno navesti korisnika da klikne na naizgled bezazlenu poveznicu (eng. hyperlink) koja ga zapravo preusmjerava na neku neželjenu stranicu, ili koristi ranjivosti njegovog web preglednika kako bi pristupila osjetljivim podacima. Iz ovih razloga važno je poduzeti mjere zaštite vlastitih interesa i sigurnosti na Internetu, a prvi korak pritom je upoznavanje s opasnostima koje ondje vrebaju.

2.1. Štetni programi

Svi štetni programi obuhvaćeni su zajedničkim nazivom „malware“, uključuju programske viruse i crve. Oni se često šire putem poruka elektroničke pošte. Najčešće spominjana vrsta štetnih programa su virusi, no osim njih postoje i:

- crvi (eng. worms),
- tzv. „trojanci“ (eng. trojan horses) te
- programi koji napadaju privatnost (eng. spyware) ili bez dopuštenja korisnika preuzimaju reklame (eng. adware)

Za sve vrste štetnih programa karakteristično je da se preuzimaju i pokreću bez korisnikovog pristanka. U slijedećim odlomcima biti će objašnjena njihova osnovna svojstva i načini korištenja.

2.1.1. Virusi

Riječ je o programskom odsječku koji se nalazi u nekom izvršnom programu, a čije je osnovno obilježje mogućnost prepisivanja vlastitog koda u drugi izvršni program. Nužno je pritom da korisnik program domaćin smatra pouzdanim. Na Windows operacijskim sustavima izvršni programi su datoteke s nastavkom „.exe“, a na Linux sustavima datoteke s „execute“ obilježjem (koje je moguće postaviti „chmod“ naredbom). Pokretanjem tog programa pokreće se i virus. On zatim može prepisati svoj kod u neku drugu izvršnu datoteku i na taj način se replicirati.

Virusi se prenose prijenosom njihovog domaćina - inficiranog izvršnog programa. Prijenos se može odvijati putem memorijskih uređaja kao što su CD i USB, ili putem mreže. Budući da se podaci koji kolaju Internetom puno teže prate, to je najbolji i najčešći način širenja virusa. Načini na koje virusi mogu naštetiti računalu su nekontrolirano prepisivanje memorije, čime se onemogućuje rad drugih programa, brisanje podatka, oštećivanje drugih datoteka itd.

2.1.2. Crvi

Crvi su također programi koji se mogu prepisivati, no ne moraju imati program domaćin. Prenose se mrežom, a u pravilu ne nanose štetu računalima kroz koja prolaze, već opterećuju i otežavaju mrežni promet.

2.1.3. Trojanci

Osnovno obilježje ove vrste štetnih programa sadržano je u njihovom nazivu „Trojanski konj". Riječ je o programu koji se predstavlja kao koristan, no nakon što se pokrene umjesto navodne korisne funkcije pokreće se programski kod čiji je cilj naštetiti računalu i učiniti ga osjetljivim na druge napade koje potom napadač može izvesti.

2.1.4. Spyware

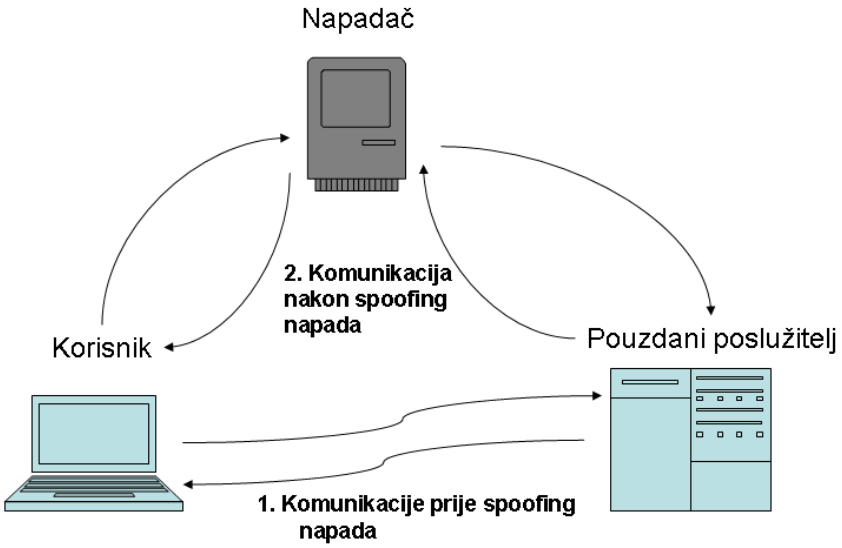
Riječ je o programima koji, kad se nađu i pokrenu na ranjivom računalu, prate korisničke aktivnosti, npr. korisničke unose podataka, aktivnosti na webu i slično. Osim toga, šira skupina štetnih programa uključuje i mogućnost preusmjeravanja korisnika na proizvoljne web stranice, preuzimanje oglasa (eng. adware) pa čak i mijenjanje mrežnih postavki računala, otežavanje mrežnog pristupa itd.

2.2. Krađa identiteta

Ova vrsta zlonamjernog ponašanja na Internetu podrazumijeva neovlašteno otkrivanje osobnih podataka korisnika koji se zatim koriste kako bi se lažnim predstavljanjem ostvario neovlašten pristup, novčana zarada i sl. Neki načini krađe osjetljivih podataka navedeni su još u prošlom poglavlju o štetnim programima. Ovdje se govori o zlouporabama Interneta i naivnosti korisnika čiji je glavni i jedini cilj ova vrsta prijevare.

2.2.1. Spoofing

Spoofing je pojam koji opisuje napad na povjerljivu komunikaciju između dva čvora (računala) u računalnoj mreži. Ostvaruje se tako da se napadač lažno predstavi kao povjerljivi čvor i tako dođe do povjerljivih podataka. Jedna vrsta spoofing napada je „Man-in-the-Middle" napad u kojem napadač uspostavi vezu s oba čvora lažno se predstavljajući te prati i prosljeđuje njihovu komunikaciju. Pritom on doznaje sve informacije koje se razmjenjuju. Posebna vrsta spoofing napada, čija su meta web stranice, naziva se „phishing". Budući da je za Internet karakterističan phishing napad i njegovi korisnici su često meta upravo ovog oblika napada, on se obrađuje u zasebnom (slijedećem) odlomku.



Slika 1. „Man in the Middle" spoffing

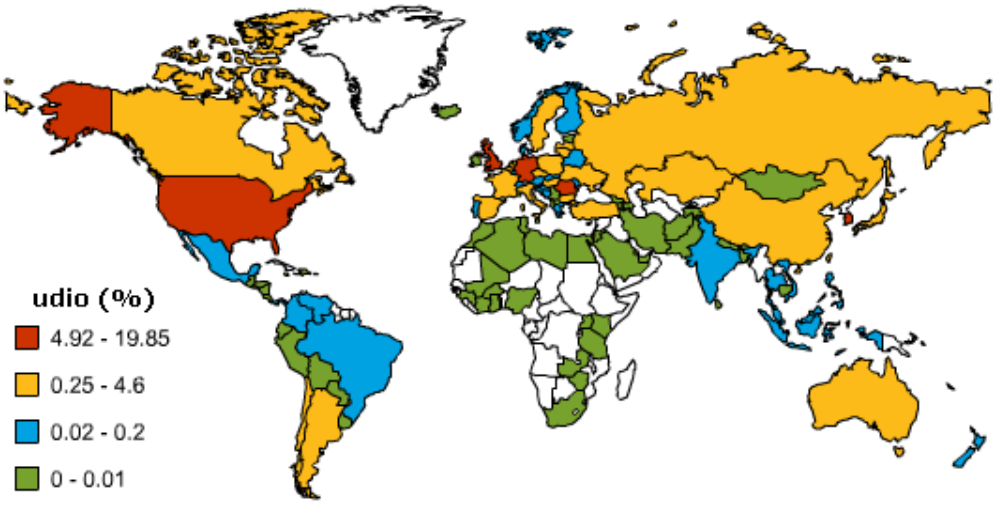
2.2.2. Phishing

Cilj phishing napada je izvući osjetljive korisničke podatke kao što su korisnička imena, lozinke, brojevi kreditnih kartica, PIN brojevi i sl. To se postiže spoofing napadom na web stranice. Napadač oblikuje web stranicu tako da ona jako nalikuje na pravu web stranicu. Najčešće se radi o popularnim društvenim web stranicama kao što su Facebook i Youtube ili web stranicama organizacija preko kojih se izvode novčane transakcije, npr. PayPal. Korisnika se zatim navodi na posjetu ovakve lažno oblikovane stranice. To se pokušava učiniti na različite načine, najčešće putem poruka elektroničke pošte ili IM (eng. Instant Messaging), tzv. „chat" poruka, tako da se:

- umetne poveznica na lažno web odredište,
- predstavi kao administrator i traži obnova korisničkog računa, potvrda lozinke,
- nude neke povlastice ukoliko se uplate novci na lažni račun ili
- pozivaju na sigurnost i traže pritom otkrivanje lozinke samo ovom „pouzdanom" izvoru.

Dio phishing poruka može se prepoznati po tome što je pisan neodređeno. Nigdje nije očito da je poruka namijenjena upravo primatelju koji ju je dobio. Poruke su pisane nestručno i navode neuvjerljiva obećanja. Zahtijevaju se osobni podaci i hitan odgovor. Ipak, napadači su do danas napredovali i velik broj pokušaja phishing napada teško je prepoznati čak i informiranijim korisnicima.

Jedan od načina izbjegavanja ove vrste napada je ignoriranje poveznica danih u poruci. Umjesto toga preporučljivo je utipkati poznatu adresu navedene web stranice u preglednik i/ili provjeriti istinitosti zahtjeva preko te stranice. Korisno je i imati na umu kako ozbiljne organizacije ne kontaktiraju korisnike na ovakve nesigurne i nepouzdane načine.



Slika 2. Udio phishing napada u svijetu u 2008. godini

Izvor: Threat Resource Center

2.2.3. Pharming

Pharming je napad sličan phisingu po tome što mu je cilj preusmjeriti korisnike na zlonamjerno oblikovane web stranice. Opasniji je od phishinga jer se izvodi suptilnije i ne zahtjeva naivne korisničke akcije poput otvaranja web poveznica u sumnjivim porukama elektroničke pošte. Naime, pharming ne podmeće lažne poveznice već napada DNS poslužitelje koji prevode imena poslužitelja u IP adrese, korisnici ih navode u URL zahtjevu. Uspješnim napadom na DNS poslužitelj, napadač stječe mogućnost upravljanja podacima na njemu te pogrešnog prevođenja imena poslužitelja u IP adrese napadačkih stranica. To znači da korisnik može utipkati pouzdanu URL adresu u svoj preglednik i svejedno završiti na nepouzdanoj stranici koja onda može pokušati

instalirati štetne programe na korisničko računalo, navesti korisnika na otkrivanje podataka i druge oblike zlouporabe.

2.3. Neželjene poruke i stranice

Štetni sadržaji mogu biti i sadržani na nekoj web stranici ili u porukama elektroničke pošte u obliku teksta i slika. Tu se radi o reklamama (sumnjivih) proizvoda, lažnim ponudama, web stranicama neprikladnim za određenu društvenu skupinu, ilegalnim web stranicama i sl. Samo postojanje legalnih, nepoželjnih stranica nije toliko problem koliko činjenica da su njihovi vlasnici spremni na raznorazne zlouporabe kako bi naveli korisnike na njihovu posjetu. Između ostalog neki od načina podmetanja takvih stranica i oglasa su navedeni i kao adware ili URL spoofing. Neželjeni web sadržaj ovdje se dijeli na „obični spam", tzv. „scam" poruke i nepoželjne web stranice.

2.3.1. Obični spam

Primjere običnog spama gotovo svaki korisnik Interneta može pronaći u svom spam sandučiću elektroničke pošte, a ponekad i u ulaznoj pošti (ukoliko se poruka automatski ne prepozna kao spam). Riječ je najčešće o reklamama navodno sjajnih i efikasnih proizvoda ili jeftinih izuzetno kvalitetnih imitacija skupih proizvoda. Osim toga sadrže i senzacionalističke napise koji pozivaju korisnika da klikne na poveznicu. Ona naravno vodi na nepoželjnu web stranicu. Obični spam štetan je utoliko što zatrpava korisnikov sandučić elektroničke pošte, troši korisnikovo vrijeme i mrežne resurse. Osim običnog spama u takvim porukama mogu doći i razni oblici prijevara uključujući već opisani phishing.

2.3.2. Scaming

Scam poruke su poruke kojima je cilj novčano oštetiti korisnika. Napadači pritom koriste različite izlike kako bi naivnog korisnika naveli da uplati novce na njihov račun. Bliske su phishingu no ne moraju oponašati stvarnog korisnika. Postoji nekoliko učestalih oblika scam poruka:

1) Lotto scam – poruke u kojima se korisnika obavještava o velikom dobitku na međunarodnoj lutriji na kojoj je izvučena korisnikova adresa elektroničke pošte kao dobitna. Također se traže i njegovi osobni podaci kako bi se mogao provjeriti njegov identitet i isplatiti nagrada. Ovakve poruke baš nikada nisu istinite jer ne postoje međunarodne Internetske lutrije na temelju adresa elektroničke pošte, niti je moguće osvojiti nagradu ukoliko nije uplaćen listić.
2) Nigerian scam – poruke koje najčešće dolaze navodno iz afričkih ili država Bliskog Istoka od osobe koja uz pomoć primatelja poruke može ostvariti veliki novčani dobitak. Ukoliko pristane pomoći, korisniku se obećava određeni primamljivi postotak.

Jedan cilj ovakvih prijevara jest otkrivanje osobnih podataka korisnika. Ti se podaci zatim mogu preprodavati drugim zlonamjernim korisnicima Interneta. Osim toga, na ovaj način nastoji se nelegalno steći novčana dobit. To se postiže obećanjima velikih svota novca naivnom korisniku, pod uvjetom da on uplati relativno mali iznos na prevarantov račun.. Prevaranti su izuzetno uporni i nametljivi, ali kada korisnik uplati novce, najčešće prekidaju komunikaciju. Niti obećane, niti dane novce korisnik nikada neće vidjeti. Osim ova dva oblika scam poruka, prevaranti se mogu javiti i s raznim drugim pričama, a svima je zajedničko to da se u konačnici traže novci pod vrlo neformalnim i sumnjivim uvjetima te bez ikakve garancije.

2.3.3. Neželjene web stranice

Posebna kategorija neželjenih web sadržaja su web stranice. Na Internetu danas postoji preko 100 milijuna web stranica. To znači da sadrži i ogroman broj beskorisnih i štetnih web stranica. Štetnim web stranicama smatraju one koje:

1) sadrže pornografske sadržaje,
2) promoviraju pedofiliju,
3) promoviraju nezdrava ponašanja (anoreksija, bulimija, suicid),
4) sadrže hazardne igre (virtualni kasino) ili

5) potiču mržnju spram pojedinih društvenih skupina, rasa i/ili nacija.

Neke web stranice nepoželjne su zato što su ilegalne, a druge su nepoželjne za određene dobne skupine (npr. stranice s pornografskim sadržajem). Osim toga, nepoželjnost može biti uvjetovana i kontekstom. U firmi pristup raznoraznim zabavnim stranicama umanjuje produktivnost, dok kod kuće nema razloga zašto bi se takav pristup uskratio korisniku.

Web stranice kao štetni web sadržaji donose i određene kontroverze. Štetni programi i prijevare neupitno su nepoželjni sadržaji u svakoj situaciji i tu nema prostora za zlouporabe. S druge strane, web stranice se mogu proglasiti štetnima s ciljem cenzure, uskraćivanja prava na javni govor i slično. Zbog toga filtriranje web stranica osim problema vezanih uz efikasnost uključuje i pitanje društvene ispravnosti, tj. opravdanosti takvog postupka.

2.3.4. Oprezno korisničko ponašanje

Sigurnosti komunikacije u računalnoj mreži prvenstveno doprinosi njezino sigurno oblikovanje, a zatim programski alati koji će pružati različite razine sigurnosti čvorovima (računalima) u mreži, ovisno o njihovim zahtjevima. Primjerice, baza podataka neke banke zahtjeva jaču zaštitu od poslužitelja nekog javnog portala.

Iako sigurnosne aplikacije poput antivirusnih programa otklanjaju neke opasnosti koje su korisniku nevidljive, sigurnosti na Internetu uvelike može doprinijeti i korisničko ponašanje. Poželjno je educirati se o opasnostima i osnovama komunikacijskih protokola Interneta, na računalu uvijek imati uključen vatrozid, antivirusne i druge zaštitne alate. Ne preporuča se preuzimati datoteke sa sumnjivih stranica, pogotovo izvršne datoteke, niti otvarati poveznice u sumnjivim porukama.

Dio prevarantskih stranica može se prepoznati po domenama. Naime, imena poslužitelja i računala oblikuju se prema domenama kojima pripadaju. Najviše domene su državne, npr. hr, uk, i generičke, npr. com, net. Niže domene često su vezane uz organizaciju kojoj računala pripadaju, npr. Microsoft. Za određeno računalo ime se oblikuje na slijedeći način:

računalo.poddomena.domena, npr. www.carnet.hr.

S tim da poddomena može biti složena od niza viših i nižih poddomena. Prevođenje ovakvih imena (eng. Fully Qualified Domain Name, FQDN) u IP adrese obavlja se pomoću hijerarhijski organiziranog sustava DNS poslužitelja.

Uzmimo za primjer podstranicu tvrtke Microsoft čija je adresa *office.microsoft.com*. Prevarant može svoju stranicu nazvati *microsoft.office.sn.com* i podmetnuti je naivnom korisniku. Na prvi pogled doista se čini da se radi o Microsoftovoj stranici, no poznavanje načina na koji se dodjeljuju imena web odredištima otkriva da je riječ o *sn* poddomeni koja u ovom slučaju nema veze sa tvrtkom Microsoft, a *microsoft.office* je proizvoljan naziv nekog odredišta u toj domeni. Slično vrijedi i za adrese elektroničke pošte.

Navodne ozbiljne ponude poslane sa gmail, yahoo i drugih svima dostupnih adresa elektroničke pošte najčešće su lažne. Osim toga spam poruke u pravilu se šalju sa nesuvislih besmislenih adresa. Primjeri nepoželjnih adresa su *tequila_ik@hotmail.com* ili *l_jcharlette_xi@wmle.com*. Preporuča se i ignoriranje raznoraznih sumnjivih ponuda lake zarade novca, navodnih dobitka na lotu, bilo u porukama, bilo u tzv. „pop-up“ aplikacijama. Osobit oprez preporuča se kod ostavljanja svoje adrese elektroničke pošte i osobnih podatka na Internetu što nikako nije poželjno činiti na nepouzdanim stranicama.

3. Web filtriranje

Web filtriranje je automatsko prepoznavanje poželjnih ili nepoželjnih vrsta web sadržaja. Osim prepoznavanja uključuje i odbacivanje nepoželjnog, a propuštanje poželjnog sadržaja do krajnjeg korisnika. Metode web filtriranje različite su za različite oblike štetnog sadržaja, no općenito se mogu podijeliti prema smještaju filtra u mreži:

1) Web filtar se nalazi kao program na računalu koje štiti.
2) Web filtar se nalazi na posrednom (eng. proxy) računalu te može štiti više računala u mreži. Ovaj način zaštite nudi se i kao Internetska usluga na koju se moguće pretplatiti.

Web filtri u obliku programa instaliranih na računalu štite samo računalo domaćina. Sav promet dolazi do računala te se na njemu filtrira. Problem kod ovakvog pristupa je opterećenje procesorskog vremena i memorije korisničkog računala, u svrhu filtriranja sadržaja. Web filtar koji se nalazi na posrednom računalu štiti cijelu mrežu računala koja preko njega pristupaju Internetu. Sav se promet filtrira na ulazu u zaštićenu mrežu čime se povećava brzinu komunikacije i rasterećuju računala u njoj.

Osim toga filtri se mogu podijeliti prema načinu primjene:

1) Programski alat (eng. software) – češće se koristi za pojedina računala i u pravilu sporije obavlja filtriranje.
2) Fizički uređaj (eng. hardware) – češće se koristi za zaštitu računalne mreže i učinkovitiji je u radu jer je sklopovski i programski prilagođen obavljanju funkcije filtriranja.

Osim ove dvije podjele metode web filtriranja mogu biti:

1) Statične – pretražuju se baze poznatih štetnih web sadržaja.
2) Dinamičke – ocjena štetnosti donosi se analizom podataka. Najčešće se zasnivaju na algoritmima umjetne inteligencije i strojnog učenja.

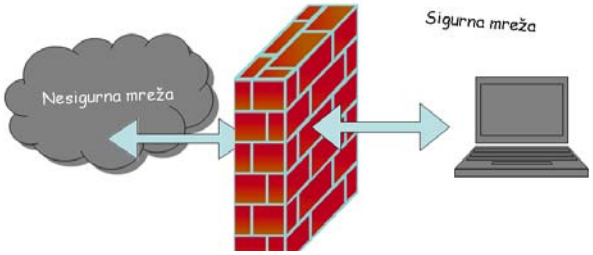
Metode koje se zasnivaju na statičkom pristupu točnije su u prepoznavanju štetnih sadržaja jer se oslanjaju na baze već provjerenih podataka. Ipak, budući da se štetni sadržaji stvaraju puno većom brzinom nego što se baze mogu ažurirati, ovaj pristup ne omogućuje prepoznavanje novijih i prethodno neoznačenih opasnosti. Dinamičke metode analiziraju svaki novi sadržaj što ih čini sporijima, ali omogućuje prepoznavanje novih, neoznačenih, a štetnih podataka. Problem kod dinamičkih metoda je taj što one nisu sasvim točne i često puta mogu pogrešno ocijeniti sadržaj štetnim ili sigurnim. Budući da obje metode imaju svoje prednosti i nedostatke, današnji filtri ih u pravilu koriste kombinirano. U ovom poglavlju opisuju se pobliže metode filtriranja različitih vrsta štetnog web sadržaja.

3.1. Vatrozid

Vatrozid je osnova zaštite računala, odnosno računalne mreže. Radi se o uređaju ili programu instaliranom na računalo koji predstavlja poveznicu između sigurne i nesigurne mreže. Sigurna mreža može predstavljati više računala ili samo jedno računalo.

Vatrozid radi na mrežnom sloju, tj. provjerava IP pakete provjerom IP adrese i priključnice (eng. port) preko koje komunicira određena usluga). Odluka o prihvaćanju ili odbacivanju IP paketa donosi se na temelju kriterija postavljenih od strane korisnika ili administratora mreže. Ukoliko neka vrsta prometa nije posebno odobrena, vatrozid ju ocjenjuje nepoželjnom te se paketi odbacuju. Osim odobravanja i odbacivanja paketa vatrozid i bilježi sumnjive događaje te šalje upozorenja o pokušajima narušavanja sigurnosti.

Načini rada vatrozida dijele se na statički i dinamički, a osnovna razlika je ta što se kod statičkog načina rada pregledava samo pojedini paket, dok se u dinamičkom načinu rada paketi vodi računa o uspostavljenim vezama te se paketi provjeravaju u okviru veze kojoj pripadaju čime se omogućuje bolja provjera.



Slika 3. Vatrozid u računalnoj mreži

Vatrozid dakle provjerava samo dolaze li podaci iz dopuštene mreže. Danas vatrozidi sve češće omogućuju i praćenje odlaznog prometa prema sličnim pravilima tretiranja kao i za dolazni promet. Vatrozid je moguće zaobići ukoliko napadač lažira IP adresu te se predstavi kao prihvatljiv izvor. Ukoliko ova vrsta napada uspije, vatrozid nije u mogućnosti prepoznati štetan programski kod, spam, scam poruke ili nepoželjan sadržaj jer on nije oblikovan tako da provjerava podatke koji se prenose IP paketom. On provjerava samo pošiljatelja i priključnicu te ocjenjuje njegovu pouzdanost. Provjeru sadržaja moguće je uključiti dodatnim specijaliziranim filtrima kao što su antivirusni alati, spam i phishing filtri te alati za filtriranje web sadržaja..

3.2. Antivirusni alati

Antivirusni alati su programi koji analiziraju datoteke s izvršnim programskim kodom, a cilj im je otkriti zlonamjerni kod. U početku su antivirusni alati bili specijalizirani isključivo za prepoznavanje virusa, dok danas mogu prepoznati i druge vrste štetnih programa. Također, antivirusni alati nude mogućnost otklanjanja zlonamjernog programskog koda no vrlo često to nisu u mogućnosti u potpunosti napraviti. Zato postoji posebna kategorija antivirusnih alata koji su specijalizirani za otklanjanje pojedinih vrsta virusa.

Datoteke se u pravilu pregledavaju prilikom stvaranja, otvaranja, slanja ili primanja, a dobra sigurnosna politika podrazumijeva i periodičnu provjeru svih datoteka u sustavu (npr. jednom tjedno). Antivirusni alati ne mogu prepoznati izvor virusa i opasna web odredišta, oni jedino raspoznaju prisutnost zlonamjernog koda u datoteci na svom računalu.

Postoji više metoda analize sumnjivog programskog koda, a antivirusni alati u pravilu kombiniraju njihovo korištenje kako bi postigli najvišu učinkovitost. Metode i osobitosti antivirusnih programa opisane su u sljedećim odlomcima.

3.2.1. Prepoznavanje poznatih virusa

Metode koje se zasnivaju na pretraživanju baza poznatih virusa – ova metoda pretražuje sumnjivi kod i uspoređuje ga s kodom u bazi poznatih virusa. Ukoliko se pronađe sličnost, kod se proglašava virusnim, a inficirana datoteka se izolira ili pokušava popraviti. Ovaj način provjere koristan je jer se najveći broj napada na sustave izvodi zapravo poznatim virusima. Ipak ne pruža zaštitu od novih virusa ili naprednijih oblika zlonamjernog programskog koda koji se može kriptirati ili mijenjati kako bi postao neprepoznatljiv antivirusnom programu koji se zasniva samo na ovoj metodi.

Druga metoda koja se zasniva na sličnim principima je metoda prepoznavanja sigurnog koda. Ona odobrava pokretanje samo programskog koda koji je prethodno označen kao siguran. Iako ovakav pristup jest teoretski najsigurniji, teško ga je provoditi zbog velike količine aplikacije koje danas postoje na operacijskim sustavima.

3.2.2. Prepoznavanje sumnjivog ponašanja

Ova vrsta pristupa analizi programskog koda zasniva se na prepoznavanju naredbi koje su označene kao potencijalno opasne. Takvo označavanje naredbi zasniva se na heuristici, odnosno traženju dovoljno dobrog rješenja koje ne mora davati dobar rezultat u svim slučajevima. Primjer potencijalno opasne naredbe je prepisivanje drugog izvršnog koda. Program koji sadrži ovakvu

naredbu može, ali i ne mora biti virus. Također, alat se može zasnivati na virtualizaciji okoline u kojoj se program pokreće te procjeni štete koja potom nastaje.

Očita je prednost ovakvih metoda to što pruža mogućnost prepoznavanja novih virusa. Nedostatak je taj što u pravilu stvara značajan broj lažnih upozorenja. Ukoliko od korisnika traži akciju prilikom svakog upozorenja s vremenom postoji vjerojatnost da će korisnik automatski zanemarivati upozorenja bez obraćanja pažnje na sadržaj.

3.2.3. Svojstva antivirusnih alata

Kod instaliranja i korištenja antivirusnih alata potrebno je imati na umu nekoliko specifičnosti:

- Imaju visoka prava pristupa datotekama kako bi mogli pronaći viruse – uspješan napad na antivirusnu aplikaciju omogućuje stjecanje punog administratorskog pristupa računalu.
- Usporavaju rad sustava – što u situacijama niskog rizika od virusa može biti neopravdan vremenski trošak.
- Na jednom operacijskom sustavu nije uputno istovremeno pokretati više od jednog antivirusnog alata jer mogu dovesti do konflikta, zauzimanja resursa te lažnih dojava virusa.
- Razni besplatni neprovjereni antivirusni alati koji se nude na Internetu mogu biti zapravo zlonamjerno oblikovani programi koji narušavaju sigurnost sustava pa se stoga savjetuje korištenje poznatih antivirusnih rješenja.

3.3. Filtri nepoželjne pošte

Filtri nepoželjne elektroničke pošte već su integrirani u veliki broj Internetskih servisa za elektroničku poštu kao što su Gmail, Yahoo, Hotmail i drugih. Oni analiziraju dolaznu poštu te ukoliko se ona prepozna kao nepoželjna, sprema se u zasebni pretinac koji korisnik može pregledati ukoliko ga zanima, no nema izravan neizbježan kontakt s takvom poštom. Osim filtara koji otklanjaju takvu poštu u sandučiću, na izloženost ovoj vrsti nepoželjnog web sadržaja uvelike utječe sam korisnik svojim ponašanjem. U idućim odlomcima objašnjene su neke metode automatskog filtriranje nepoželjne pošte. Osim toga opisuje se i poželjno korisničko ponašanje.

3.3.1. Označavanje spam poruka

Filtri često koriste tehnike prepoznavanja nepoželjnih poruka prema listama zlonamjernih IP adresa s kojih te poruke dolaze, adresama poznatih pošiljatelja tzv. „spam“ poruka. To su tzv. crne liste (eng. Blacklist). Druga, oštrija politika provjere poruka, zasniva se na tzv. bijelim listama (eng. Whitelist) koje sadrže dopuštene domene s kojih pošta smije pristizati, dok se sve ostale domene smatraju nepoželjnima. Distribuirane tehnike označavanja spam poruka zasnivaju se na činjenici da se nepoželjne poruke u pravilu šalju velikom broju korisnika. Ukoliko jedan korisnik poruku označi kao nepoželjnu, ta se informacija prosljeđuje i svim drugim primateljima. Osim ovih metoda, postoji i tehnika koja privremeno odbacuje poruke (eng. Greylisting). Ona se zasniva na pretpostavci da će legitimni MTA (eng. Mail Transfer Agent) programi pokušati poruku poslati ponovno nakon određenog vremenskog perioda. Budući da napadači uglavnom koriste nekvalitetno oblikovane programe, koji ne podržavaju tu mogućnost, na ovaj način otklanja se dio neželjenih poruka.

3.3.2. Provjere RFC standarda

Osim što zlonamjerni korisnici rabe loše oblikovane programe, često i koriste druga računala kako bi lažirali domene. Riječ je o računalima kojima je prethodnim napadom stečen neovlašten pristup te se lažno prikazuju kao izvor zlonamjernih poruka. Legitimni korisnici takvih zlouporaba nisu svjesni pa se takva računala nazivaju i zombi računala. Budući da napadači zombi računalima nemaju puni pristup, ne mogu ih koristiti za oblikovanje poruka već samo za lažiranje adrese. Nepoželjne poruke zato uglavnom ne zadovoljavaju sve zahtjeve internetskih protokola i nemaju ispravno oblikovana zaglavlja. Uključivanje provjera prema SMTP protokolu i drugim standardima Internetske komunikacije u značajnoj mjeri doprinosi otklanjanju nepoželjnih poruka.

3.3.3. Statističko filtriranje

Ova vrsta filtriranja zasniva se na algoritmima umjetne inteligencije koji na temelju poznatih uzoraka nepoželjnih poruka uče prepoznavati nove, dotad neviđene, poruke. Najčešći takav algoritam jest Bayesov klasifikator. On na temelju statističkih analiza sadržaja nepoželjnih poruka i onih koje to nisu, oblikuje pravila koja se zatim primjenjuju na sve nepoznate ulazne poruke. Ova metoda omogućuje prepoznavanje neželjene pošte koji dolazi u naizgled legitimnim porukama. Pošiljatelji takvih poruka nastoje ga zaobići izmjenjivanjem riječi toliko da zavaraju filtar, a ostanu razumljive primatelju pošte, npr. riječ „viagra" filtru predstavlja kritičnu riječ koja upućuje na to da je vrlo vjerojatno riječ o spam poruci. Maskiranjem te riječi u „v1@gr@", moguće je zaobići filtar, a da pritom smisao poruke ostane jasan korisniku. Provjerom sandučića, u koji se odlažu poruke obilježene kao nepoželjne, lako je uočiti kako ovakvi filtri mogu biti poticajni za kreativnost napadača koji će smisliti raznorazne izraze i načine da dođu do krajnjeg korisnika. Primjerice tekst će sakriti u sliku, reklamu zamaskirati pričicom, iznaći nove načine da opišu riječi i izraze koji se smatraju vrlo vjerojatno nepoželjnima, poput viagra, erectile disfunction, rolex i sl.

3.3.4. Korisničko ponašanje

Budući da svaka tehnika automatskog prepoznavanja neželjenih poruka ima svoje prednosti i nedostatke, filtri se oblikuju tako da njihovim kombiniranim korištenjem dosegnu najvišu učinkovitost. Ipak, vrlo veliku ulogu u zaštiti od takvih poruka ima i korisničko ponašanje. Informiranje o značajkama tzv. „spam" poruka olakšava se prepoznavanje istih. Tako na primjer spam poruke se uglavnom šalju velikom broju korisnika istovremeno, adrese s kojih dolaze čudno su i nesuvislo oblikovane, sadrže poveznice, imaju karakteristične reklamne sadržaje ili sumnjive ponude. Prijave takvih poruka doprinose prepoznavanju neželjene pošte. Zaštita od neželjenih poruka u prvom redu podrazumijeva držanje adrese elektroničke pošte tajnom. Odavanje svoje adrese na različitim nepouzdanim web stranicama čini ju dostupnom pošiljateljima neželjene pošte koji njima međusobno i trguju. Nije loša praksa imati neku adresu koja se koristi samo za situacije u kojima se traži odavanje adrese nepouzdanom izvoru s kojim korisnik nema namjere kasnije komunicirati (npr. kod registracija na neke javne forume).

Također, odgovaranje na spam poruke ne preporuča se jer se na taj način izvoru neželjenih poruka otkriva da je adresa aktivna čime se on potiče na daljnju zloupotrebu. Otvaranje web poveznica u porukama također se ne preporuča jer se isto tako odaje aktivnost adrese elektroničke pošte, a može se raditi i o pokušaju phishinga ili drugih napada na web preglednik. Budući da mnogi napadi koriste ranjivosti HTML preglednika, a neželjene informacije sadržane su u HTML-u ili slikama, poželjno je onemogućiti automatsko prikazivanje HTML sadržaja, URL-ova i slika u porukama. Korisnik ih može ručno omogućiti nakon što utvrdi da nije riječ o neželjenoj poruci.

3.4. Filtriranje web stranica

Fitriranje web stranice posebna je kategorija web filtriranja jer se sadržaji koje filtrira ne mogu uvijek proglasiti apsolutno štetnima. Osim toga filtriranje web stranica veže se uz cenzuru na Internetu. Zato ovaj oblik web filtriranja nije u potpunosti prihvaćen u svijetu te postoje brojne grupe koje se bore za njegovo potpuno uklanjanje.

Kod nas je CARNet početkom 2007. godine započeo s primjenom sustava za filtriranje nepoćudnih sadržaja na školskim računalima. Budući da se škole preko CARNeta spajaju na Internet i djeca postaju izložena svim sadržajima na njemu. Ovakva inicijativa ima za cilj zaštitu djece filtriranjem web sadržaja koji bi im mogli naštetiti[13].

3.4.1. Liste prihvatljivih i neprihvatljivih web stranica

Liste slične ovima već su spomenute u okviru filtriranja spam poruka i virusa. Riječ je o listama koje sadrže (ne)prihvatljive web stranice. Korisnicima je pritom dozvoljen pristup svim stranicama koje nisu označene kao nepoželjne.

Već spomenuta inačica lista poznatih stranica su i bijele liste kojima je pristup dozvoljen, dok se sve druge smatraju nepoželjnima. Ovakve liste pogodne su u situacijama kada je prihvatljiv pristup malom broju stranica koje se smatraju korisnima, primjerice u poslovnim, obrazovnim okruženjima

ili na računalu kojem bez nadzora pristupa dijete. Liste prihvatljivih web stranica nepogodne su kad je u pitanju širok pristup Internetu jer je nepraktično i nemoguće održavati i provjeravati tako veliki broj stranica.

Općenito, nedostaci ove metode leže u tome što ne postoji mogućnosti prepoznavanja štetnosti web stranice ukoliko ona nije već jednom prepoznata kao nepoželjna. S druge strane, najveća prednost ove metode jest brzina filtriranja jer je potrebno (samo) provjeriti je li domena web stranice označena kao nepoželjna (nema potrebe za učitavanjem svake stranice). Crne i bijele liste mogu se koristiti i za ograničenja koja nameće sam korisnik.

3.4.2. Kategorizacija stranica

Ideja na kojoj se zasniva ova metoda je stvaranje baze URL adresa koje su kategorizirane prema svom sadržaju. Takva baza omogućila bi alatima za filtriranje da na temelju samog zahtjeva (dakle nema potrebe za dohvaćanjem stranice) smjeste stranicu u određenu kategoriju. Zatim na temelju ograničenja koja vrijede za trenutnog korisnika odrede je li pristup toj stranici dozvoljen ili nije. Primjeri takvih kategorija mogu biti: obrazovanje, pornografija, nasilje i sl.

Problem kod ove metode je nemogućnost kategorizacije svih stranica koje postoje na Internetu, odnosno nemogućnost praćenja rasta Interneta. Budući da je trenutno nemoguće stvoriti bazu koja bi se redovito ažurirala i sadržavala sve stranice koje postoje na Internetu, ostaje pitanje stranica koje nisu u bazi. Njih se mora ili tretirati kao dopuštene, zabranjene, ili se za svaku pojedinu stranicu mora postaviti upit administratoru mreže što nije najučinkovitiji način. Osim toga, budući da se klasifikacija stranica mora obavljati automatski jer je to vremenski jedini prihvatljivi način, javlja se i problem pogrešne klasifikacije.

3.4.3. Analiza sadržaja

Budući da same liste nisu dovoljne za raspoznavanje poželjnih i nepoželjnih web stranica, razvijaju se i metode analize sadržaja. One uključuju:

- analizu ključnih riječi u korisničkim zahtjevima ili pojmovima koje pretražuju,
- jednostavnu analizu poželjnih i nepoželjnih riječi na stranici - ovakve metode oslanjaju se na prepoznavanje kritičnih riječi koje upućuju na nepoželjnost web stranice. Primjer nepoželjne riječi u programima koji provjeravaju pristup djece internetu može biti riječ „seks“. Ukoliko se zabrani svaka stranica koja u sebi sadrži riječ seks, jasno je da će nepoželjnima biti proglašeni i medicinski ili biološke sadržaji.
- složeni algoritmi – oni uzimaju u obzir pojedine riječi, ali i kontekst u kojem se te riječi nalaze. Time se smanjuje mogućnost pogrešnog prepoznavanja stranice, no ne otklanja se potpuno. U pravilu ovdje se radi o statističkim ili heurističkim algoritmima.

Nedostatak ovakvih metoda, osim neučinkovitosti u analizi samog konteksta, može biti i lako skrivanje nepoželjnih sadržaja u druge (dozvoljene) sadržaje, filtru nerazumljive formate kao što su slikovni. Osim toga ukoliko algoritmi ne mogu analizirati različite jezike, lako ih je zaobići jednostavnim prevođenjem teksta. Još jedan nedostatak ove metode je činjenica da se svaka stranice mora učitati i analizirati što predstavlja određen vremenski i procesorski trošak. Taj se trošak značajno povećava ukoliko se provode složeniji algoritmi za analizu sadržaja.

Dodatno u analizu sadržaja može ući i analiza slika. Ova metoda osobito je korisna kod otkrivanja pornografskih stranica. Problem pak leži u složenosti i cijeni tehnologija za analizu slikovnih datoteka.

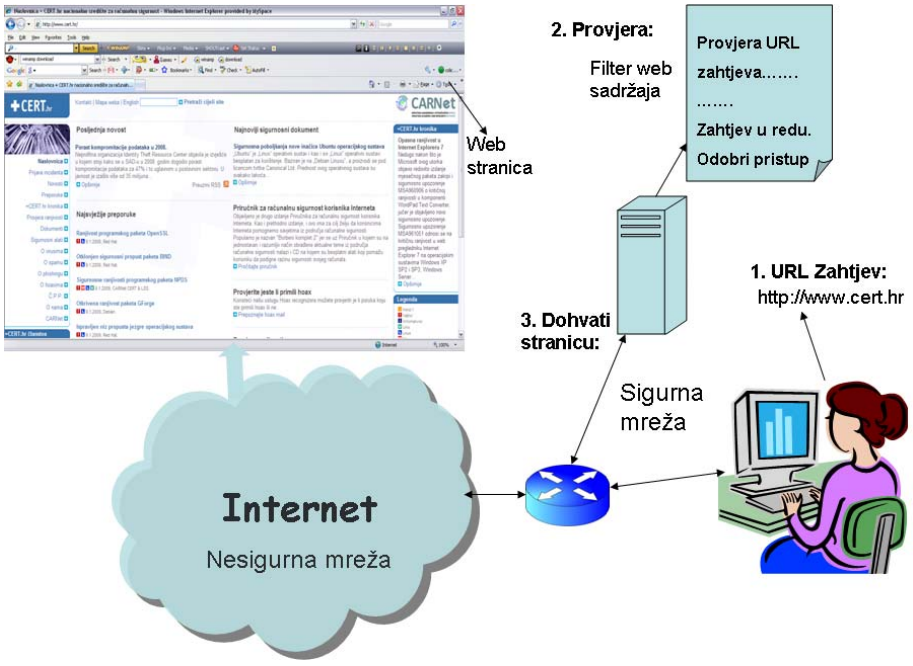
3.4.4. Mješovite metode

Budući da niti jedna metoda sama po sebi ne nudi odgovarajuću zaštitu, programi za filtriranje web sadržaja danas koriste više metoda istovremeno. Profinjenija rješenja uključuju i analizu konteksta stranice, a uzimaju u obzir i jezik stranice. Također, na temelju svake nove stranice ažuriraju se baze, ali i preoblikuju alati za dinamičku analizu, tj. novi uzorci se koriste za dodatno poboljšanje kriterija klasifikacije. Čak i sa svim naprednim mogućnostima, danas ne postoji alat koji bi zadovoljavao visoke zahtjeve točnosti kategorizacije stranica. Zato se oni općenito u Internetu ne koriste. Ipak, za privatne potrebe napredniji alati koji koriste više metoda klasifikacije mogu biti dovoljno dobro rješenje.

3.4.5. Nepoželjne web stranice

Potreba za filtriranjem web sadržaja javlja se iz više razloga:

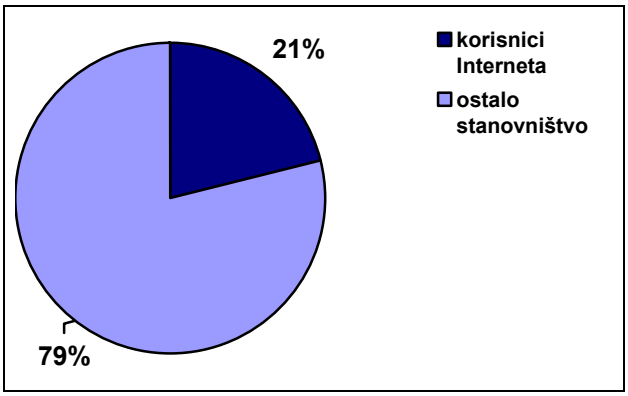
- Zaštita od ilegalnih sadržaja na Internetu kao što su pedofilske stranice, sadržaji koji šire mržnju, potiču na sukobe između različitih društvenih ili nacionalnih skupina, nude štetne informacije poput načina na koje je moguće proizvesti eksplozivne naprave, potiču na samoubojstvo, anoreksiju i sl.
- Zaštita djece koja Internet danas koriste kao i odrasli i imaju pristupe informacijama koje ne razumiju niti mogu procijeniti njihove opasnosti. Zaštita djece uključuje zaštitu od svih sadržaja koji su ilegalni te od nekih koji nisu ilegalni, ali su neprimjereni za dječji uzrast, poput pornografije. Osim toga djeca imaju pristup raznim društvenim mrežama i aplikacijama za razmjenu poruka u realnom vremenu (eng. chat). Preko njih mogu stupiti u kontakte sa raznim vrstama zlonamjernih ljudi i kriminalaca.
- Zaštita korporativnih interesa. Ova vrsta filtriranja odnosi se na tvrtke čiji zaposlenici imaju pristup internetu. U interesu tvrtke je da oni imaju pristup bitnim i korisnim podacima te da mogu komunicirati međusobno. No na slobodnom Internetu je jednako lagano doći do korisnih, ali i do drugih sadržaja. Mogućnost zaposlenika da pristupaju Internetu smanjuje produktivnost, ponekad stvara i neugodnu atmosferu na poslu, ukoliko netko naočigled svih pristupa posebno neprihvatljivim stranicama. Prema nekim statistikama 44% zaposlenika gleda neprimjerene video sadržaje tijekom radnog vremena.



Slika 4. Uloga web filtra u računalnoj mreži

3.4.6. Statistike

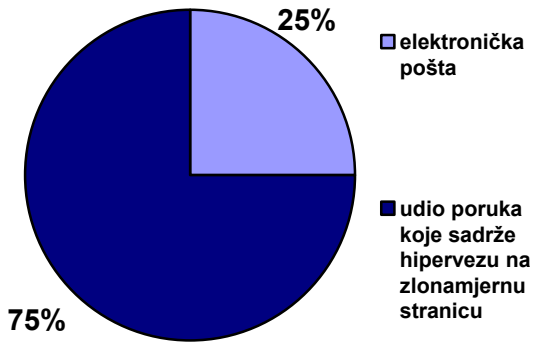
Statistike o rastu Interneta pokazuju da je broj korisnika od 2000. godine do danas porastao za 305% [10], tako da danas Internet broji nešto manje od milijardu i pol korisnika i oko 35 milijuna web odredišta. To je ogroman broj korisnika među kojima su i kriminalci i djeca.



Slika 5. Udio korisnika Interneta u svjetskom stanovništvu[10]

Količine podataka koje kolaju Internetom su ogromne, a istraživanja o sigurnosti Interneta [14] pokazuju slijedeće:

- 75% opasnih web stranica legitimne su stranice koje su kompromitirane hakerskim napadom
- Preko polovice najpopularnijih web stranica bile su mete uspješnih zlouporaba
- Gotovo 90% poruka elektroničke pošte su neželjene poruke, a svaka dvjestota sadrži u sebi virus.
- Oko 3 četvrtine poruka elektroničke pošte sadrži poveznice na zlonamjerno oblikovane stranice (Slika 6.)
- Primijećen je pad pornografskih poruka elektroničke pošte te porast phishing napada putem poruka elektroničke pošte
- Oko polovice napada čiji je cilj otkriti osjetljive podatke izvodi se putem Web-a
- Najviše neželjenog sadržaja u porukama elektroničke pošte dolazi kao HTML, slike ili URL poveznice.



Slika 6. Poveznice na zlonamjerne web stranice u porukama elektroničke pošte

Pornografija je najčešći oblik nepoželjnog sadržaja na Internetu, a djeca su najosjetljivija skupina. Istraživanja na ovu temu pokazala su kako:

- Pornografske stranice čine 12% ukupnog broja web odredišta

- Jedna četvrtina svih zahtjeva na internetskim tražilicama otpada na pornografiju
- 100 000 web stranica nudi dječju pornografiju
- 1 od 7 djece navodi se na seksualne radnje, a 90% takvih pokušaja događa se na Internetskim chat-ovima.
- Procjenjuje se da su djeca prvi put izložena pornografiji na Internetu s 11 godina
- 90% susreta s pornografskim sadržajima događa se za vrijeme domaćeg rada na Internetu
- Pornografski sadržaji često se skrivaju iza naizgled bezazlenih i djeci zanimljivih pojmova poput Pokemon, Action Man i sl. [11]

Očito je pornografija jedna od najprisutnijih vrsta sadržaja na Internetu što je izravna posljedica velike korisničke potražnje za njom. Opasnosti koje proizlaze iz ovakvih okolnosti su zlouporaba seksualnosti osjetljivih korisnika kao što su djeca. Internet je pogodno područje za seksualno maltretiranje u obliku neželjenih neprimjerenih poruka, slika, lažnog predstavljanja i pedofilije, a iz navedenih statistika lako je donijeti zaključak o ozbiljnosti ovih prijetnji. I upravo zbog toga javlja se legitimna potreba za ugradnjom različitih filtra web sadržaja kako bi se zaštitili korisnici koji nisu u mogućnosti se samostalno štititi.

3.4.7. Kontroverze

Filtre web stranica osim privatnih i poslovnih korisnika u više navrata pokušale su uvesti ISP (eng. Internet Service Provider) kompanije. Ova vrsta web filtriranja predstavlja poseban problem jer ograničava pristup svim korisnicima Interneta koji su povezani preko te kompanije. Osim toga, otvara se mogućnost zlonamjernog upravljanja web sadržajem i uvođenjem naplata za odobravanje pristupa pojedinim domenama. Time Internet prestaje biti slobodna mreža, a pružatelji pristupa Internetu postaju i njegovi vlasnici. Još jedno loše svjetlo na filtriranje web stranica baca i činjenica da ga koriste zatvorene zemlje poput Kine, Vijetnama i Bjelorusije. One to čine kako bi provjeravale pristup korisnika podacima koji otkrivaju propuste i loše strane vladajućeg režima. Time se zapravo onemogućuje razvoj kritičkih pogleda i svijesti o pravom stanju stvari u državi te se upravlja percepcijom političke stvarnosti stanovništva.

Problem kod web filtriranja nije zapravo samo web filtriranje već mogućnosti zlouporabe koje nudi. Osim toga, danas dostupni alati imaju značajan broj nedostataka i često ne blokiraju sve štetne stranice, ali i pogrešno blokiraju one stranice koje nisu štetne. Neučinkovitost i omogućivanje cenzure glavni su argumenti protivnika ove vrste filtriranja na globalnoj razini.

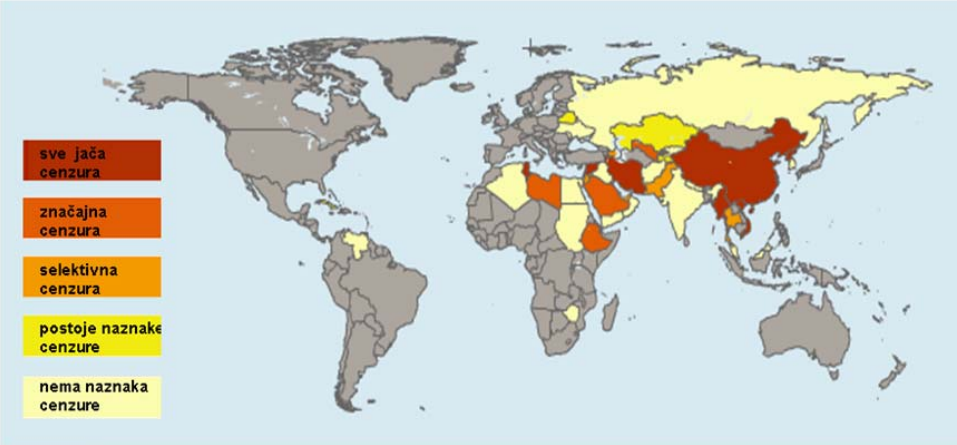
Ipak, web filtriranje na lokalnoj razini čija je svrha zaštita djece ili povećanje radne produktivnosti ne znači negativnu cenzuru, a s kvalitetnim alatom može biti i dovoljno učinkovito. Primjerice, u kompanijama se mogu dopustiti samo korisne stranice, a nove se dodaju ukoliko ih zaposlenici predlože i uprava odobri. Zaposlenici su ograničeni samo na radnome mjestu koje niti nije predviđeno za slobodne aktivnosti na Internetu. Ograničavanje Internetskog prometa u obrazovnim ustanovama također je svrhovito, kao i zaštita računala koje bez nadzora roditelja koristi dijete. U ovim slučajevima web filtriranje nosi puno više prednosti nego mana te ga je korisno uzeti u obzir.

3.4.8. Organizacije za borbu protiv cenzure

Neke od organizacija koje se bore protiv cenzure na Internetu su:

- ACLU (eng. American Civil Liberties Union) – organizacija osnovana u Americi 1920. godine čiji je cilj zaštita građanskih prava, zajamčenih ustavom i zakonom, svim građanima Sjedinjenih Američkih Država. Organizacija danas broji preko pola milijuna članova i simpatizera.
- Reporters Without Borders – novinarsko udruženje osnovano 1985. godine čiji cilj rada je sloboda medija, borba protiv cenzure i zaštita novinara. Riječ je o međunarodnoj organizaciji koja putem ogranka i dopisnika djeluje na svih pet kontinenata.
- Censorware Project i Peacefire.org – projekti kojima je cilj educirati korisnike o manama web filtriranja. Peacefire.org je osnovan 1996. godine s ciljem zastupanja prava maloljetnika na slobodu govora, a danas broji preko 7000 članova. Censorware projekt je započela grupa pravnika, pisaca i aktivista 1997. godine, a cilj joj je razotkrivanje neučinkovitosti alata za web filtriranje i njihovih zlouporaba.

- OpenNet Initiative – grupa preko koje surađuju priznata svjetska sveučilišta (Harvard, Cambridge, Oxford i Toronto), s ciljem istraživanja i informiranja javnosti o načinima na koji pojedine države cenzuriraju informacije dostupne njihovim građanima. Na stranicama ove grupe mogu se pronaći interaktivne mape koje pokazuju prisutnost cenzure Interneta u svijetu (slika)



Slika 7. Prisutnost cenzure u svijetu
Izvor: OpenNet Initiative

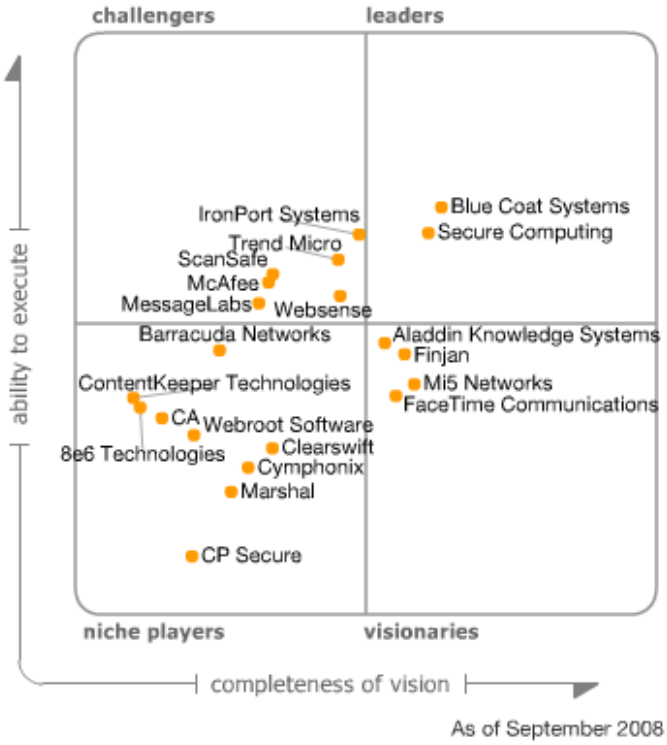
4. Programski alati

Programski alati i uređaji za filtriranje web sadržaja omogućuju automatsku zaštitu pojedinačnih računala ili mreža od štetnih programa, web stranica i drugih nepoželjnih sadržaja. Neki od njih nude integriranu zaštitu od virusa, neželjene pošte, phishinga i nepoželjnih web stranica, dok drugi nude specijalizirane usluge (filtri elektroničke pošte, antivirusni programi). Osim toga neki od njih su komercijalni, dok su drugi besplatni. Neki od komercijalnih programa dostupni su besplatno za privatne korisnike. U nastavku su opisani neki od popularnijih alata.

Naziv alata	Vrsta alata	Dostupnost
SpamAssassin	spam filtar za Linux operacijske sustave	besplatno
SpamAware	spam filtar za Windows Outlook/Outlook Express – koristi SpamAssassin mehanizam	besplatno
AVG	antivirusni program za Windows XP i Windows Vista sustave	besplatno za privatne korisnike
ClamAV	antivirusni alat za Unix/Linux operacijske sustave	besplatno
SafeSqiud	filtriranje web sadržaja preko posrednog poslužitelja	besplatno za mreže do dvadeset računala

Tablica 1. Besplatni alati za filtriranje sadržaja

U ovom poglavlju dani su kratki pregledi četiriju komercijalnih alata koji nude integrirane usluge web filtriranja, a prvenstveno su namijenjeni poslovnim korisnicima. Na slici je dana usporedba komercijalnih alata s obzirom na tehnološki pristup i položaj na tržištu.

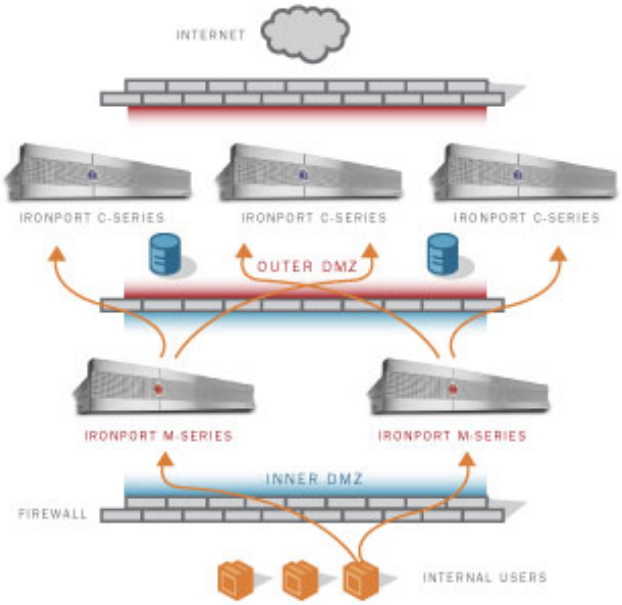


Slika 8. Usporedba različitih tehnologija

Izvor: Magic Quadrant for Secure Web Gateway

4.1. IronPort

IronPort je jedna od vodećih tvrtki u svijetu koje se bave filtriranjem web sadržaja. IronPort uređaji u sebi integriraju zaštitu od nepoželjne pošte, virusa, omogućuju jednostavno upravljanje pravilima i konfiguracijom, preusmjeravanje pošte i brojne napredne mogućnosti. Filtri elektroničke pošte otklanjaju 80% nepoželjnih poruka na razini Internetske veze čime se rasterećuje promet kroz mrežu. Budući da se radi o sklopovskim rješenjima koja su vrlo brza, imaju mogućnosti prihvaćanja velikih broja dolaznih veza (npr. do 10000). Dobitnici su brojnih priznanja i nagrada osobito za filtriranje elektroničke pošte. Riječ je o visoko kvalitetnim što se odražava i na cijeni koje se kreću od 10 000 dolara naviše.

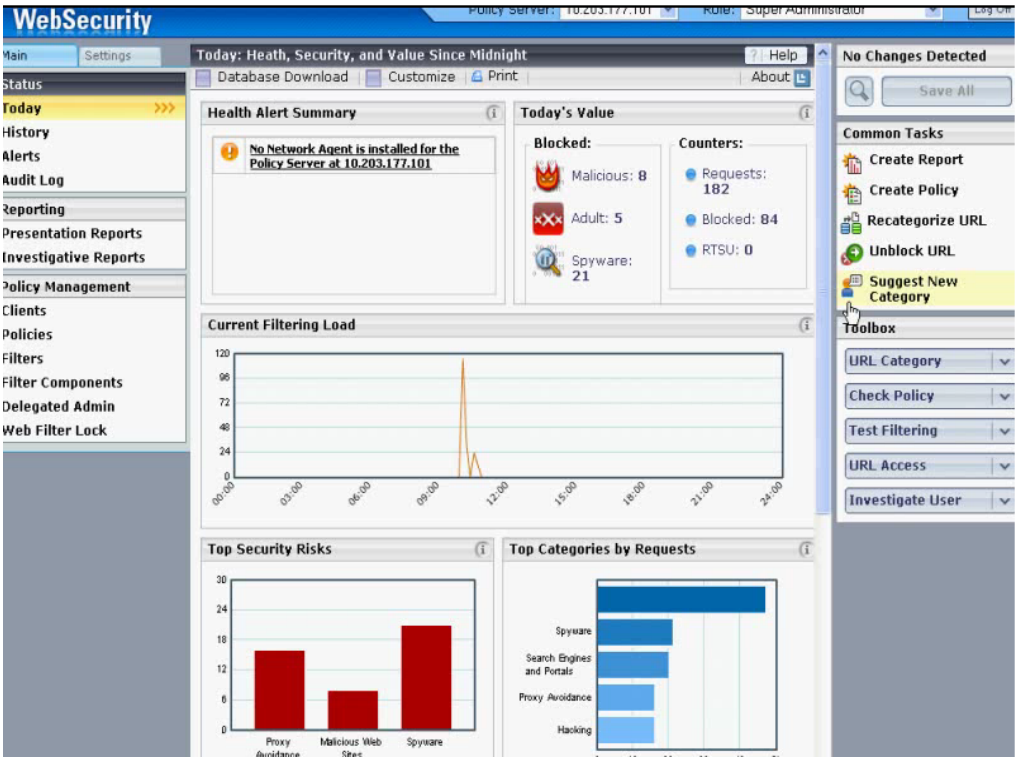


Slika 9. Mrežna mapa IronPort sigurnosnih uređaja

Izvor: Security Management Appliance

4.2. Websense

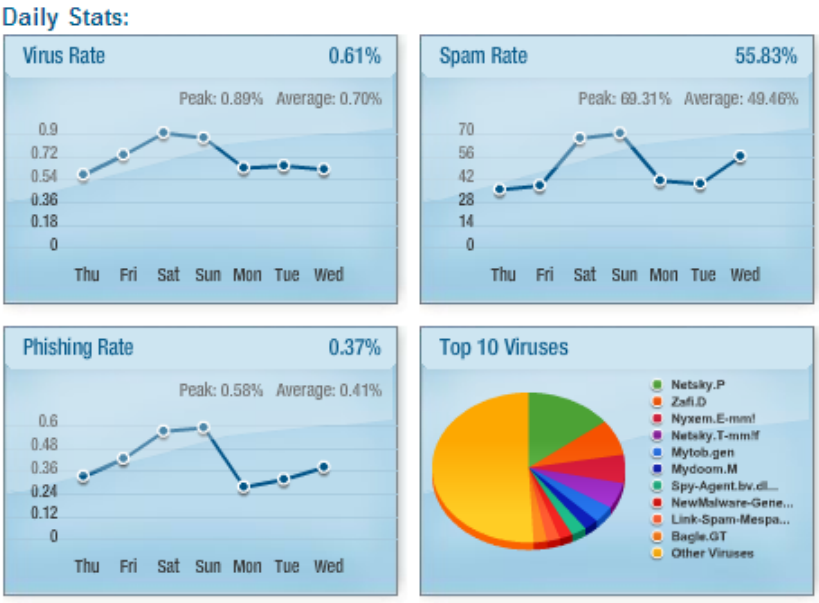
Websense nudi usluge web filtriranja, zaštitu radnih stanica od nepoželjne pošte, virusa i drugih vrsta štetnih programa, administratorima omogućuje nadzor komunikacije porukama i općenito cijelog prometa prema Internetu. Osim toga Websense nudi i usluge filtriranja web stranica, a u svojoj bazi sadrži kategorizaciju preko 9 milijuna web stranica. Treba napomenuti da je bilo optužbi na račun ove tvrtke za neučinkovitost filtra web stranica, no nepotpuna učinkovitost takvih filtra općeniti je problem. Jesu li Websense usluge filtriranja web stranica značajno kvalitetnije od drugih rješenja, teško je reći. Websense rješenja namijenjena su prvenstveno korporativnom tržištu, a budući da su oblikovana kao Internetske usluge na koje se korisnici pretplaćuju cijene su povoljnije i kreću se od oko 1000 dolara godišnje.



Slika 10. Isječak korisničkog sučelja Websense Web Filter alata

4.3. Messagelabs

MessageLabs nudi usluge filtriranja web sadržaja od nepoželjnih poruka, virusa i drugih oblika štetnih sadržaja. Prvi su u svijetu uveli filtriranje virusnih programa kao Internetsku uslugu. Nisu među najkvalitetnijim ponuđačima, no svakako su među cijenom najpristupačnijima. To je dijelom vezano i uz činjenicu da, poput tvrtke Websense, filtriranje nude kao Internetsku uslugu. Dakle, nikakvi uređaji i programski alati nisu potrebni niti osoblje koje bi se brinulo za takve uređaje. Usluge su im pouzdane i uvijek dostupne, a cijene se kreću već od nekoliko stotina dolara.



Slika 11. MessageLabs dnevne statistike

Izvor: MessageLabs Intelligence

4.4. CA eTrust Secure Content Manager

Riječ je o proizvodu koji integrira antivirusnu zaštitu, sigurnost poruka elektroničke pošte i zaštitu od nepoželjne pošte, praćenje odlaznog prometa i zaštitu podataka, filtriranje URL adresa i blokiranje nepoželjnih web stranica. Osim toga, korisniku se omogućuje i oblikovanje pravila prema kojima će se filtrirati elektronička pošta.

CARNet mreža koristi ovaj sustav za filtriranje web stranica za škole, a filtriranje se obavlja na temelju kategorizacije stranica koju vrši navedeni alat. Osim toga, omogućuje se i ručno zabranjivanje prikazivanja određene stranice. Kategorizacija stranica odvija se neprekidno, a nove inačice baze podataka automatizirano se provjeravaju svakih nekoliko sati. Svaka Internetska stranica se može nalaziti u jednoj ili više kategorija, a kategorije koje CARNet filtrira za škole su:

- Drugs (droge)
- Gambling (kockanje)
- Gambling Related (kockanje)
- Gruesome Content (sablažnjivi, morbidni sadržaji)
- Hate Speech (govori mržnje)
- Hacking (računalni napadi)
- Malicious Sites (zlonamjerno oblikovane stranice)
- Nudity (golotinja)
- Profanity (bogohuljenje)
- Pornography (pornografija)
- School Cheating Information (informacije o varanju u školama)
- Spam
- Tobacco (duhan)
- Violence (nasilje)

5. Zakonske osnove

Prema Ustavu Republike Hrvatske [17] osobne i političke slobode i prava uključuju:

- slobodu mišljenja i izražavanja misli. Sloboda izražavanja misli obuhvaća osobito slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa i slobodno osnivanje svih ustanova javnog priopćavanja. Zabranjuje se cenzura. (čl. 38.)
- Sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva. Samo se zakonom mogu propisati ograničenja nužna za zaštitu sigurnosti države ili provedbu kaznenog postupka.(čl. 36.)
- Zabranjeno je i kažnjivo svako pozivanje ili poticanje na rat ili uporabu nasilja, na nacionalnu, rasnu ili vjersku mržnju ili bilo koji oblik nesnošljivosti. (čl. 39.)

Slobode medija iz Zakona o medijima [20] opisane su u članku 3:

- (2) Sloboda medija obuhvaća osobito: slobodu izražavanja mišljenja, neovisnost medija, slobodu prikupljanja, istraživanja, objavljivanja i raspačavanja informacija u cilju informiranja javnosti; pluralizam i raznovrsnost medija, slobodu protoka informacija i otvorenosti medija za različita mišljenja, uvjerenja i za raznolike sadržaje, dostupnost javnim informacijama, uvažavanje zaštite ljudske osobnosti, privatnosti i dostojanstva, slobodu osnivanja pravnih osoba za obavljanje djelatnosti javnoga informiranja, tiskanja i raspačavanja tiska i drugih medija iz zemlje i inozemstva, proizvodnju i objavljivanje radijskog i televizijskog programa, kao i drugih elektroničkih medija, autonomnost urednika, novinara i ostalih autora programskih sadržaja u skladu s pravilima struke.
- (3) Slobode medija dopušteno je ograničiti samo kada je i koliko je to nužno u demokratskom društvu radi interesa nacionalne sigurnosti, teritorijalne cjelovitosti ili javnoga reda i mira, sprječavanja nereda ili kažnjivih djela, zaštite zdravlja i morala, zaštite ugleda ili prava drugih, sprječavanja odavanja povjerljivih informacija ili radi očuvanja autoriteta i nepristranosti

sudbene vlasti samo na način propisan zakonom.

- (4) Zabranjeno je prenošenjem programskih sadržaja u medijima poticati ili veličati nacionalnu, rasnu, vjersku, spolnu ili drugu neravnopravnost, kao i ideološke i državne tvorevine nastale na takvim osnovama, te izazivati nacionalno, rasno, vjersko, spolno ili drugo neprijateljstvo ili nesnošljivost, poticati nasilje i rat.

Na temelju Ustava i Zakona o medijima zaključuje se o potrebi provjere sadržaja na Internetu, ali i o potrebi da se te provjera provodi vrlo precizno, tako da se ne naruše temeljna prava na slobodu mišljenja i pristupa informacijama. Budući da je trenutno nemoguće takvu provjeru na Internetu provoditi zaista kvalitetno, u Hrvatskoj ne postoje zakonski koji bi dopuštali filtriranje web sadržaja javnim mrežama.

Zakon o telekomunikacijama [19] nalaže javnim operaterima (pravnim osobama koje raspolažu telekomunikacijskom mrežom) sa znatnijom tržišnom snagom pružanje otvorenog pristupa mreži (čl. 52). Pristup se prema članku 58. može ograničiti samo iznimno radi:

- sigurnosti rada telekomunikacijske mreže,
- održavanja cjelovitosti telekomunikacijske mreže,
- sposobnosti međusobnog funkcioniranja telekomunikacijskih usluga ili
- zaštite podataka

Ovaj zakon se ne odnosi na privatne mreže poput poslovnih mreža ili akademskih mreža kao što je CARNet koje omogućuju pristup samo određenoj skupini korisnika. Takva privatna mreža može ograničiti pristup Internetu u skladu s vlastitim i interesima svojih korisnika.

6. Zaključak

Štetni sadržaji na Internetu prisutni su u različitim oblicima, kao programi kojima je cilj narušiti rad računala ili ukrasti podatke, kao zlonamjerno oblikovane web stranice, poruke elektroničke pošte, IM poruke, neprikladni slikovni, video ili tekstualni sadržaji itd. Zaštita računala koje je priključeno na nesigurnu mrežu poput Interneta podrazumijeva nekoliko postupaka. Prvi je uključivanje osnovne zaštite, vatrozida. Drugi korak je korištenje pouzdanih antivirusnih programa. S obzirom na količinu nepoželjnih poruka koja danas stiže na pretince elektroničke pošte, potrebno je koristiti i filtre takvog sadržaja. U određenim uvjetima (škole, tvrtke) koriste se i filtri web stranica kako bi se spriječio pristup neprihvatljivim web stranicama. Takve usluge mogu koristiti i roditelji zabrinuti za sigurnost svoje djece. Sloboda pružatelja usluga pristupa Internetu na uvođenje ograničenja na Internetsku komunikaciju dosta je kontroverzna ideja koja ima brojne protivnike. Problem je što bi se na taj način bitno promijenio smisao Interneta kao slobodne mreže. Osim toga otvorio bi se prostor za zlouporabe i uvođenje cenzure.

Osim automatske zaštite računala, od iznimne je važnosti informirati se o opasnostima i dobrom korisničkom ponašanju na Internetu. Svaki korisnik Interneta treba biti sposoban prepoznati i izbjeći sumnjive sadržaje te znati kako postupiti kada dođe u kontakt s njima. S obzirom na raširenost i ulogu Interneta u svijetu, razumijevanje njegovog funkcioniranja nije više dovoljno ostaviti stručnjacima (informatičarima). Internet ulazi u svijet i svijet postaje Internet, sve važne informacije kolaju Internetom, na njemu se nalaze povjerljivi podaci velike većine stanovništva. Iz tog razloga opasnosti koje ondje vrebaju nisu samo virtualne, već su vrlo stvarne. Razumijevanje Interneta, svijest o postojećim opasnostima, odgovorno ponašanje i korištenje računalne zaštite nužni su kako bi ovu nesigurnu mrežu, svaki korisnik za sebe učinio sigurnim mjestom.

7. Reference

[1] Antivirus software, http://en.wikipedia.org/wiki/Antivirus_software, siječanj 2009.

[2] E-mail filtering, http://en.wikipedia.org/wiki/Spam_filter, siječanj 2009.

[3] Limbo malware CCERT-PUBDOC-2008-11-247, http://www.cert.hr/documents.php?lang=hr, studeni 2008.

[4] About Peacefire.org, http://www.peacefire.org/info/about-peacefire.shtml, siječanj 2009.

[5] OpenNet Initiative, http://opennet.net/about-oni, siječanj 2009.

[6] OpenNet Initiative , GLOBAL INTERNET FILTERING MAP, http://map.opennet.net/filtering-pol.html, siječanj 2009.

[7] James Ashton, £400m web fraud firm MessageLabs plans float, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article4493256.ece, kolovoz, 2008.

[8] Peter Firstbrook, Lawrence Orans Gartner, RAS Core Research Note G00160130, Magic Quadrant for Secure Web Gateway, http://mediaproducts.gartner.com/reprints/securecomputing/160130.html, rujan 2008.

[9] Whitepaper: Understanding Web Filtering Technologies, http://www.bloxx.com/assets/downloads/US/bloxx_whitepaper_webfilter_us.pdf, siječanj 2009.

[10] INTERNET USAGE STATISTICS, http://www.internetworldstats.com/stats.htm, siječanj 2009.

[11] Pornography Statistics, http://www.familysafemedia.com/pornography_statistics.html, siječanj 2009.

[12] Filtriranje sadržaja, http://www.carnet.hr/filtriranje_sadrzaja, siječanj 2009.

[13] EU program SaferInternet, http://public.mzos.hr/Default.aspx?art=8927&sec=3167, siječanj 2009.

[14] Websense Security Labs™, State of Internet Security Q1 – Q2, 2008, http://securitylabs.websense.com/content/Assets/WSL_Report_Web_1h08.pdf, siječanj 2009.

[15] Threat Resource Center, http://securitylabs.websense.com/content/CrimewarePhishing.aspx, siječanj 2009.

[16] David Mertz, Spam filtering techniques, http://www.ibm.com/developerworks/linux/library/l-spamf.html, siječanj 2009.

[17] Ustav Republike Hrvatske, http://narodne-novine.nn.hr/clanci/sluzbeni/232289.html, siječanj 2009.

[18] Zakon o pravu na pristup informacijama, http://narodne-novine.nn.hr/clanci/sluzbeni/307079.html, siječanj 2009.

[19] Zakon o telekomunikacijama, http://narodne-novine.nn.hr/clanci/sluzbeni/306319.html, siječanj 2009.

[20] Zakon o medijima, http://narodne-novine.nn.hr/clanci/sluzbeni/306926.html, siječanj 2009.

[21] IronPort M660 - Security Management Appliance, http://www.ironport.com/products/ironport_m660.html, siječanj 2009.

[22] MessageLabs Intelligence, http://www.messagelabs.com/intelligence.aspx, siječanj 2009.

[23] Jonathan Strickland ,How Internet Censorship Works, http://computer.howstuffworks.com/internet-censorship.htm, sječanj 2009.