HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost Windows Vista operacijskog sustava

CCERT-PUBDOC-2007-03-187

CARNet CERT u suradnji s LS&S

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

Rezultat toga rada ovaj je 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

Nakon gotovo pet godina od izdavanja Windows XP sustava, Microsoft je izdao novi operacijski sustav naziva Windows Vista. Ovo je izdanje najprije objavljeno pod nazivom „Longhorn“ 22. srpnja 2005. godine, nadogradnja sustava završena je 8. studenog 2006. godine, a konačna distribucija započela je 30. siječnja 2007. s nazivom „Vista“.

Windows Vista je grafički orijentiran operacijski sustav za korištenje na osobnim računalima, uključujući kućne i poslovne radne površine, prijenosna računala i medijske centre. Prema tvrdnji Microsofta, Windows Vista sadrži stotine novih obilježja u odnosu na prijašnja izdanja sustava. U značajnije novitete se uključuju novo grafičko sučelje i vizualni stil Windows Aero. Također, poboljšane su mogućnosti pretraživanja, uvedeni su novi alati za stvaranje multimedijskih sadržaja, a sasvim je redizajnirano umrežavanje, audio podsustavi te moduli za podršku pisača i zaslona.

Ukoliko se uzmu u obzir prethodna izdanja operacijskih sustava Microsofta, Vista je najsigurnija izgrađena verzija Windows sustava do sada. Broj potencijalnih vrsta napada koji se mogu izvesti na Vista sustavima je smanjen u odnosu na broj koji je bio vezan uz starije inačice sustava. Ovakve sigurnosne značajke trebale bi rezultirati poboljšanjem u obrani od nekoliko rasprostranjenih zlonamjernih aplikacija koje ciljaju na ranjivosti jezgri operacijskih sustava.

U nastavku dokumenta opisane su novosti u odnosu na starije Windows sustave te su dani opisi svih novih elemenata sustava koji utječu na sigurnost operacijskog sustava. U drugom dijelu dan je pregled Internet Explorer preglednika, sedme inačice, koji je integriran u sami operacijski sustav radi pružanja sigurnosti na višoj razini.

2. Sigurnost Windows Vista operacijskog sustava

Windows Vista sadrži poboljšanja koja će napadačima otežati napad na računala na kojima je instaliran taj sustav. Windows XP sustavi s prvim paketom sigurnosnih zakrpa SP1 (*Service Pack* 1), izgrađeni su tako da daju relativno dobru zaštitu od napada. Drugim sigurnosnim paketom SP2 je poboljšan vatrozid za zaštitu od zlonamjernih korisnika i od programa koji bi bez znanja korisnika pokušavali pristupiti Internetu s računala ili računalu s Interneta. Iako je ovo bio napredak u sigurnosti, još uvijek se radilo o jednostavnom rješenju u usporedbi s ponudama sličnih aplikacija na tržištu. To je razlog zašto se pojavila potreba za nadogradnjom i ovog segmenta operacijskog sustava. Vista ima napredniji vatrozid u odnosu na navedene. Internet Explorer inačice 7 posjeduje *anti phishing* filtar, ali isto tako usporava kretanje željenim stranicama što umanjuje ugodnost korištenja. Novi mehanizam zaštite temeljen na korisničkim računima, implementiran je sa ciljem zaštite korisnika od vlastitih pogrešaka – onemogućavanja instalacije zlonamjernih aplikacija. To se prvenstveno odnosi na one slučajeve kada korisnici nemaju dovoljno znanja o radu na računalu. Unatoč tome i činjenici da sustav za svaku takvu akciju traži potvrdu, odabirom omogućavanja nastavka rada može se učiniti sve što se želi, bez obzira na moguće posljedice. Dakle, za potpunu sigurnost i korisnik mora biti dovoljno osviješten i educiran. Iako postoje poneki propusti, sa stajališta sigurnosti operacijski sustav Windows Vista bolji je izbor u odnosu na Windows XP sustave.

Jezgra sustava je temeljna komponenta svakog operacijskog sustava na kojoj je izgrađena i sigurnost cijelog sustava. Kako drugi programi ovise o njoj, greška u njezinom radu može prouzročiti nefunkcionalnost aplikacija ili funkcioniranje na neželjen način. U novijim izdanjima operacijskog sustava, koncept jezgre sustava i sigurnost postaju glavne značajke tehnološkog napretka. Ispravnom implementacijom jezgre smanjuje se mogućnost provale ili od strane napadača ili od strane nepoželjnih programa koji mogu skriti svoju prisutnost na sustavu. Iz ovog razloga Microsoft je investirao u poboljšanje sigurnosti i pouzdanosti jezgre Windows Vista operacijskog sustava. Upotrijebljene su neke nove tehnologije za umanjenje spomenutog problema. Upravljački programi su redizajnirani te zahtijevaju ispravne digitalne potpise proizvođača. Iz jezgre je odvojena skupina programskih funkcija koja nema izravnu vezu sa zadaćama operacijskog sustava. PatchGuard tehnologija štiti ključne dijelove operacijskog sustava od izmjena jezgre ili programskih dodataka u njoj. Važno je za napomenuti da samo 64-bitna inačica Windows Vista sustava podržava ovu tehnologiju, a proizvođači programske podrške koja zadire u takve funkcije, primjerice antivirusnih aplikacija, najavljuju potencijalne probleme svojih aplikacija u radu na tim inačicama sustava.

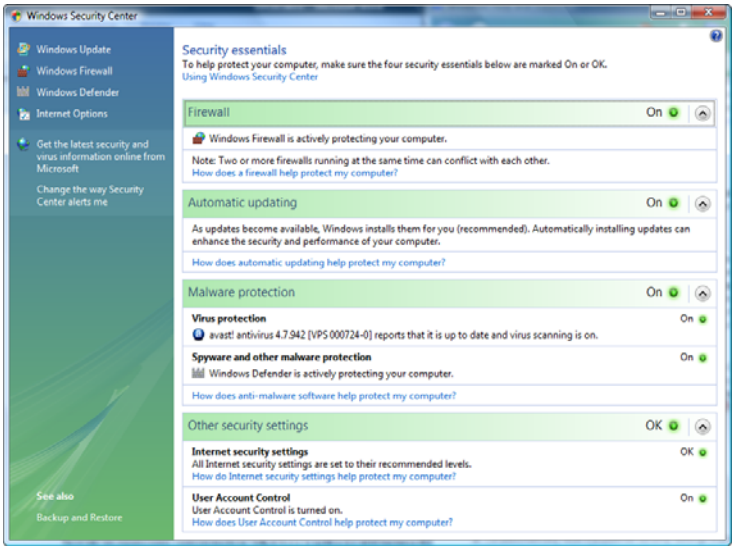
Zakrpa jezgre (eng. *kernel patch*) je mehanizam koji omogućuje modificiranje ili zamjenu dijelova jezgre operacijskog sustava, a može se iskoristiti u legitimne, ali i nelegitimne svrhe. U drugom slučaju mogu se pojaviti problemi u tri različita segmenta: pouzdanosti, performansama i sigurnosti operacijskog sustava. Drugim riječima, neovlaštena izmjena jezgre može rezultirati nepoželjnim ponašanjem operacijskog sustava, nestabilnošću sustava i pojavom problema nepravilnog funkcioniranja poput pojavljivanja plavog ekrana nastalog usred pojave pogreške u radu operacijskog sustava (eng. *Blue Screen of Death - BSoD*). To može rezultirati gubitkom podataka ili sličnim problemima. Spomenuti sigurnosni mehanizam uočava aktiviranje neželjene akcije, te operacijskom sustavu nalaže gašenje računala. Iako mehanizam ne pruža apsolutnu zaštitu, on ipak štiti sustav od manipuliranja važnim programskim funkcijama. Ukoliko se sve uzme u obzir, opisana tehnologija jedna je od najvažnijih zaštita od neželjenih akcija koje mogu uzrokovati ozbiljne probleme u radu operacijskog sustava. Novi mehanizam je i slučajno određivanje adresnog prostora (eng. *Address Space Layout Randomization – ASLR*). Njime se onemogućuje iskorištavanje mehanizama umetanja programskog koda na proizvoljne memorijske lokacije odnosno manipuliranje adresama.

3. Sigurnosni elementi Windows Vista operacijskog sustava

Vista operacijski sustav dolazi s nekoliko različitih aplikacija namijenjenih održavanju sigurnosti sustava. U nastavku su navedene značajnije od njih i dani su kratki opisi njihovog rada.

3.1. Windows Security Center

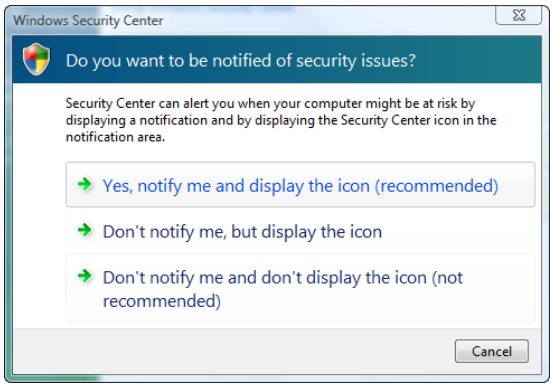
Windows Security Center je aplikacija uključena u Microsoft Windows XP i Vista operacijske sustave. Ona omogućava korisnicima pregled i mijenjanje postavki računalne sigurnosti. Sustav omogućuje nadzor nekoliko sigurnosnih modula uključujući postavke vatrozida, automatsku instalaciju sigurnosnih zakrpi, postavke vezane uz sigurnosne proizvode poput antivirusa, postavke Internet sigurnosti te sigurnosne postavke korisničkog računa.



Slika 1: Windows Security Center

S ovakvim sigurnosnim centrom može se vidjeti koja je aplikacija aktivna na računalu, npr. koji vatrozid ili koji antivirusni program korisnik ima na sustavu. Također se može provjeriti status vatrozida, instalirati zakrpe i postaviti korisničke račune. Windows Security Centar provjerava sljedeće elemente:

- **vatrozid** – da li je instaliran i uključen;
- **antivirusni program** – da li je instaliran, ima li najsvježije definicije virusa te da li je omogućen sigurnosni pregled odnosno ispravno funkcioniranje aplikacije;
- **anti-spyware program** – da li je instaliran, ima li najnovije definicije *spyware* programa te da li je omogućen rad te aplikacije.



Slika 2: Windows Security Center - definiranje pojave upozorenja

Ukoliko Windows sustav detektira problem sigurnosne prirode, Security Centar prikazuje upozorenje u obliku *oblačića* (eng. *baloon*). Dvostrukim klikom na oblačić otvara se Security Centar i dobiva se informacija s objašnjenjem kako ispraviti nastali problem.
Windows Vista Security također promatra status postavki korisničkog računa (eng. *User Account Control*) i Internet sigurnosti. Ako je korisnik prijavljen na sustav kao standardan korisnik na računalu koje nije dio domene i programska podrška treba izvesti neku akciju koja obuhvaća promjene na razini

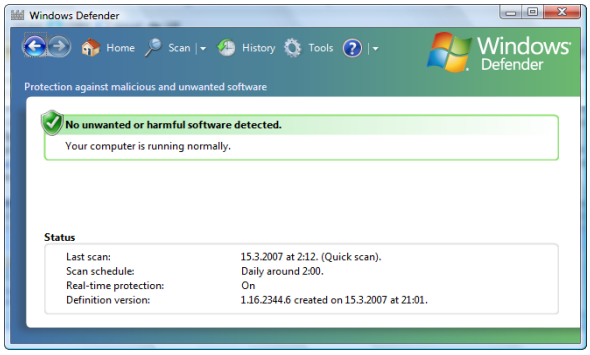
konzistentnosti sustava, operacijski sustav traži zaporku administratora. Ukoliko korisnik radi s administratorskim ovlastima, Windows Vista postavlja upit za provedbu aktivnosti tako da bi korisnik bio svjestan akcije koja će biti izvedena.

3.2. Windows Defender

Windows Defender alat poznat je pod nazivom Microsoft AntiSpyware. Radi se o programskoj podršci, proizvodu samog Microsofta. Razvijen je s namjerom sprečavanja i izolacije programa koji skupljaju osobne podatke korisnika bez njihovog znanja (eng. *spyware*). Windows Defender je dio Windows Vista sustava, a besplatan je za preuzimanje i za sve prethodne inačice. Nakon instalacije Vista sustava korisnici ne moraju neposredno mijenjati niti jednu od njegovih postavki. S Windows Defender paketom, korisnici se mogu koncentrirati na korištenje vlastitih računala umjesto na brigu o njhovoj sigurnosti. Ova programska podrška osigurava sljedeće elemente.

- **Sigurnosnu zaštitu u realnom vremenu** (eng. *real-time protection*) - automatski obavlja nadogradnju i provjeru neposredno prije i tijekom izvođenja programa.
- **SpyNet zajednicu** - Microsoftova SpyNet zajednica pomaže korisnicima da vide kako ostali korisnici opisuju aplikacije koje još nisu klasificirane. Pristup takvim podacima pomaže korisnicima da se lakše odluče hoće li ili neće koristiti pojedine programe na vlastitom računalu.
- **Pregledavanje** - korisnici mogu koristiti Windows Defender za sigurnosni pregled tzv. *spyware* aplikacija i ostalih neželjenih programa, za određivanje pregleda u zadano vrijeme i za automatsko uklanjanje svakog uočenog zlonamjernog programa.

Za ispravno korištenje Windows Defender alata potrebno je imati najsvježije definicije zlonamjernih programa. Windows Defender upotrebljava definicije kako bi odredio je li pregledavani program tzv. *spyware* ili neki drugi potencijalni neželjeni program. Tijekom svog rada upozorava korisnike o mogućem riziku njihovog korištenja. Windows Defender surađuje s Windows Update mehanizmom radi automatske nadogradnje novih definicija odmah nakon njihova objavljivanja. Nakon sigurnosnog pregleda, u ovisnosti o potencijalnoj opasnosti zlonamjernih programa, Windows Defender opisuje probleme s najvećim, visokim, srednjim i niskim riziom, te rizikom koji do trenutka provjere nije klasificiran. Na taj način omogućava korisniku da odluči hoće li nastaviti s korištenjem problematičnog programa ili neće. Ukoliko pretraženo računalo nema problematičnih programa, Windows Defender će prijaviti poruku koja je prikazana na sljedećoj slici.



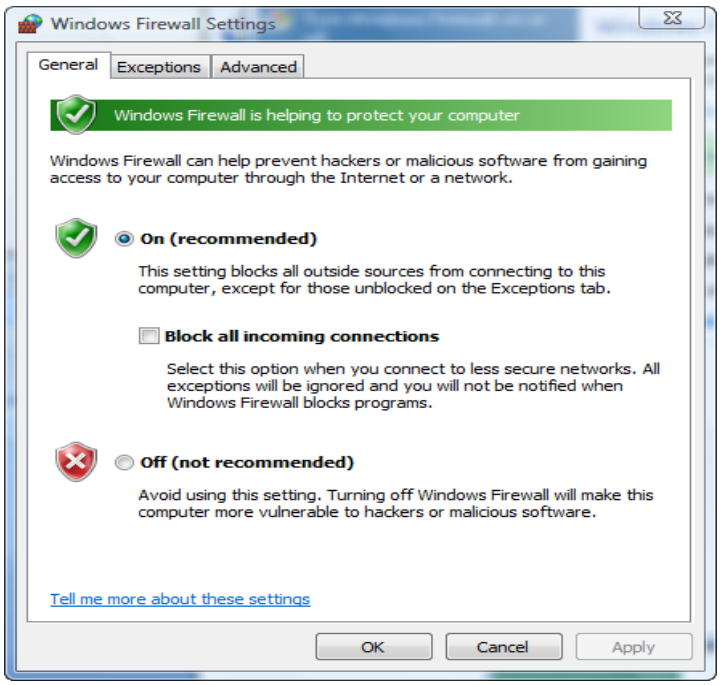
Slika 3: Windows Defender

3.3. Windows Firewall

Vatrozid je programska ili sklopovska podrška koja provjerava informacije koje dolaze s Interneta ili neke druge mreže, te ih zaustavlja ili im dopušta prolaz do operacijskog sustava korisnika. To ovisi o sigurnosnim pravilima vatrozida. Osim što može pomoći u obrani od napadača ili nepoželjnih programa vatrozid također može zaustavljati pakete koji se šalju s korisnikovog računala ostalim računalima na istoj mreži ili na Internetu.

Postoje tri mogućnosti među temeljnim postavkama aplikikacije Windows Firewall:

- **On (recommended)** - kada je Windows Firewall uključen svi pokušaji ostvarivanja komunikacije na potencijalno opasnim priključcima (eng. *port*) su onemogućeni. Ukoliko korisnik želi omogućiti ostvarivanje veze na nekom zabranjenom priključku, može ga dodati u listu iznimki (eng. *exceptions list*).
- **Block all incoming connections** - blokira sve dolazne inicijative za uspostavljanjem veze s korisnikovim računalom. Ova se postavka primjenjuje kada je potrebna maksimalna zaštita, npr. kada je poznato da neki od virusa ili crva kola Internetom. Način funkcioniranja je takav da korisnik nije upoznat sa svim pokušajima pristupa računalu, a pri tome se ignorira popis iznimki. Iako ovakav način funkcioniranja osigurava računalo na viskoj razini sigurnosti, još uvijek je omogućeno čitanje većine web stranica, slanje i primanje elektroničke pošte, te slanje i primanje trenutnih poruka (eng. *instant messages*).
- **Off (not recommended)** - korisnicima se preporuča da izbjegavaju ovu postavku ukoliko nemaju neki drugi vatrozid koji je pokrenut na njihovom računalu. Isključivanje Windows Firewalla može učiniti računalo nezaštićenim od napadača i zlonamjernih aplikacija.



Slika 4: Postavljanje Windows Firewall aplikacije

3.4. Users Account Control

U prijašnjim izdanjima Windows sustava većina korisničkih računa je imala ovlasti lokalnog administratora. Takvim postavkama korisnici su imali ovlasti i mogućnosti potrebne za instaliranje i podešavanje aplikacija, pokretanje pozadinskih aplikacija i pomoćnih upravljačkih programa (eng. *device driver*) te za instaliranje servisa. Iako je ovaj pristup bio pogodan za korisnike, učinio je računala i mreže ranjivijima na zlonamjerne programe koji imaju mogućnost uništavanja podataka, izmjene postavki poput onesposobljavanja vatrozida i kompromitiranja potencijalno osjetljivih podataka. Iako je Windows korisničke račune bilo moguće postaviti u način rada s ograničenim mogućnostima, to je u isto vrijeme ograničavalo i produktivnost pojedinog korisnika. Takav princip onemogućava jednostavne i relativno bezopasne aktivnosti poput postavljanja sata, spajanja na bežičnu mrežu ili instaliranja pisača.

Kako bi se poboljšala sigurnost te izbjegli navedeni problemi, Windows Vista uključuje mehanizam kontroliranja korisničkih računa (eng. *Users Account Control - UAC*). UAC je novi pristup koji odvaja standardne korisničke mogućnosti i aktivnosti od onih za koje je potrebna administratorska razina pristupa. Iako su smanjene mogućnosti za korisnika bez administratorskih ovlasti, ovaj pristup još uvijek omogućuje neograničen svakodnevni rad. Implementacija UAC mehanizma ima dvije prednosti.

Prva je jednostavna mogućnost povećavanja ovlasti standardnog korisnika, a to uključuje mnoge potencijalno opasne sigurnosne aktivnosti za koje je potrebno imati administratorske ovlasti. Za omogućavanje potpunog rada na ograničenom skupu administratorskih poslova bez prekidanja, standardni korisnički računi imaju dodatne mogućnosti koje omogućavaju obavljanje aktivnosti poput izmjene vremenske zone ili sličnih postavki sustava, instaliranje novih fontova ili dodavanje pisača. Ukoliko standardni korisnik pokušava obaviti posao koji zahtjeva administratorski pristup, poput instaliranja nove aplikacije ili modificiranja određenih sistemskih postavki, traži se zaporka administratora. Ovaj pristup pomaže u smanjenju rizika za svakog korisnika. Druga prednost UAC mehanizma čini korisnike s administratorskim ovlastima sigurnijima u radu jer im ograničava pristup potencijalno opasnim sustavskim funkcijama. Za administratore koji moraju svakodnevno izvoditi uobičajene poslove poput provjeravanja elektroničke pošte ili korištenja web preglednika, dodatne kontrole su potrebne kako bi osigurale da se administratorske ovlasti koriste kada su one uistinu potrebne. S prvobitnim postavkama administratorski račun će se odvijati u tzv. *Administrator Approval Mode* načinu rada. Korisničko sučelje Windows Vista sustava uključuje brojna poboljšanja što korisnicima olakšava uočavanje aktivnosti koje zahtijevaju administratorske povlastice. To uključuje i opis tražene akcije i označavanje administratorske aktivnosti odgovarajućom ikonom. Budući da je velik broj starijih aplikacija napisan pod pretpostavkom da će korisnici imati administratorske ovlasti prilikom instalacije, a nerijetko i korištenja, Microsoft omogućava da se te aplikacije pokreću i korištenjem standardnih korisničkih računa. UAC dijaloški okviri (eng. *dialog boxes*) su također redizajnirani kako bi se jasnije uočio naziv programa koji zahtjeva ovlasti administratora u svrhu lakše identifikacije potencijalno opasne aplikacije.

Slika 5: User Accounts

Ukoliko je potrebno dopuštenje ili lozinka za potpuno obavljanje željene aktivnosti, UAC će se obratiti korisniku s jednom od sljedećih poruka:

- **Sustavu je potrebno dopuštenje korisnika za nastavak** (eng. *Windows needs your permission to continue*) – svaka potencijalno opasna aktivnost je detektirana i od korisnika se zahtijeva odluka o daljnjem nastavku rada. Korisnik treba provjeriti ime sporne aplikacije i na temelju toga odlučiti radi li se o legitimnoj aplikaciji kojoj može dozvoliti nastavak rada ili o nekoj neželjenoj kojoj može zabraniti nastavak izvođenja.
- **Programu je potrebno dopuštenje za nastavak** (eng. *A program needs your permission to continue*) - program za koji je potrebno ovo dopuštenje nije sastavni dio Windows sustava. Također, ima nevaljani digitalni potpis koji označava njegovo ime i objavljivača. Ova poruka korisniku obznanjuje da se određeni program želi pokrenuti.
- **Neidentificirani program želi pristupiti Vašem računalu** (eng. *An unidentified program wants access to your computer*) – nepoznati program je onaj program koji nema valjane digitalne potpise proizvođača. Ovakav program ne označava nužno opasnost, to može na primjer biti neki od starijih, legitimnih programa koji ne sadržavaju potpise. Međutim, potrebno je povećati oprez te omogućiti pokretanje programa samo ukoliko je njegova ispravnost nedvojbena.

- **Program je blokiran** (eng. *This program has been blocked*) - ovakva poruka označava program koji je administrator sustava eksplicitno blokirao te mu onemogućio izvođenje. Da bi se pokrenuo ovakav program, potrebno je obratiti se administratoru računalnog sustava.

Zapisi registra sustava i datoteka imaju različite pristupne razine; nove datoteke i novi ključevi registra mogu biti upisani samo ako proces ima dovoljnu razinu ovlasti.
Slijedeća tablica prikazuje razine pristupa i odgovarajuće ovlasti.

Razina pristupa	Ovlasti korisnika
Visoka	Administrativne - može se instalirati programe u *Program Files* mapu te se omogućava pisanje u osjetljiva područja registra poput HKEY_LOCAL_MACHINE
Srednja	Korisničke - može se stvarati i podešavati datoteke u korisničkim direktorijima documents te omogućava pisanje u posebna korisnička polja, poput HKEY_CURRENT_USER
Niska	Nepovjerljive - omogućeno je samo pisanje po niže pristupačnim mjestima, poput *Temporary Internet Files\Low* mapi ili HKEY_CURRENT_USER\SOFTWARE\LOWREGISTRY ključu

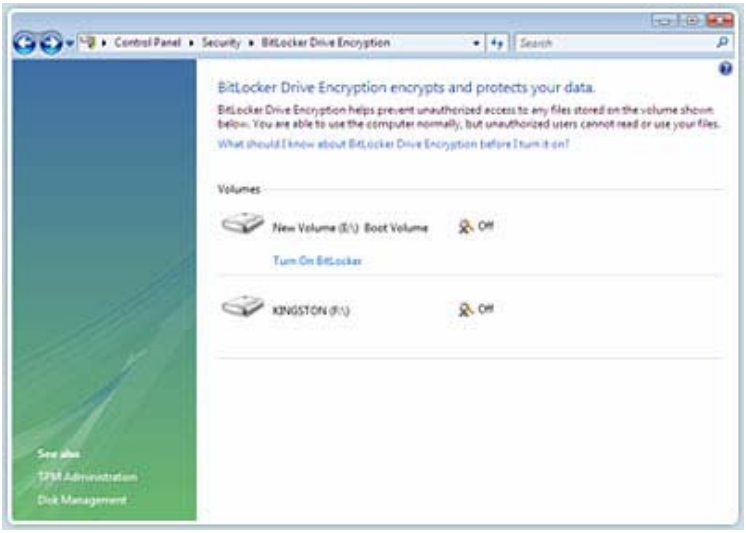
Tablica 1: Razine pristupa i ovlasti korisnika

Microsoftove preporuke su da se korisnici prijavljuju na računala koristeći korisnički račun srednje razine ovlasti. Ovakav pristup omogućuje obavljanje svakodnevnih poslova. Ukoliko korisnici žele upotrebljavati administratorske poslove, poput instaliranja novih programa ili izmjenjivanja postavke koje se tiču i ostalih korisnika, ne mora se obaviti odjava pa ponovno prijava s odgovarajućim korisničkim računom. Vista će tražiti za dopuštenje ili unos administratorske zaporke prije nego izvede zadatak. Ako se u ovakvom načinu rada u sustavu pojave potencijalno opasne aplikacije koje žele izvesti nesigurne operacije na računalu, sustav će to prijaviti korisniku i tražiti daljnje upute za nastavak rada.

3.5. BitLocker Drive Encryption

BitLocker Drive Encryption je potpuno novi sigurnosni element u Windows Vista operacijskom sustavu, a omogućava značajnu zaštitu za operacijski sustav na računalu i pohranjivanje podataka na disku. BitLocker mehanizam obavlja sigurnosno kodiranje (eng. *encryption*) podataka, a oni ostaju nečitljivi i kada sustav nije u pogonu. Time se može zaštititi od tzv. *offline* napada – vrste napada izvedenog onemogućavanjem ili zaobilaskom instaliranog operacijskog sustava koji uključuje i fizičko odstranjivanje tvrdog diska. BitLocker mehanizam je namijenjen korisnicima s iznimno visokim zahtjevima na sigurnost pohranjenih podataka, a isporučuje ga se jedino s Ultimate inačicom sustava. Dizajniran je za sustave koji sadrže tzv. *Trusted Platform Module - TPM* kriptografski mikročip i odgovarajuće inačice BIOS (eng. *Basic Input Output* System) sustava. TPM se u suradnji sa BitLockerom koristi za omogućavanje pristupa zaštićenim podacima. Tri su načina djelovanja ovog mehanizma:

- **Transparentan operacijski način** oslobađa korisnika brige o mehanizmu kodiranja podataka. Ključ koji se upotrebljava za kodiranje diska je zapečaćen TPM čipom i predaje se operacijskom sustavu u ranom stupnju pokretanja samo ukoliko su sve prethodno učitane komponente ispravne u sigurnosnom smislu.
- **Korisnička autentikacija** je način koji zahtjeva od korisnika autorizaciju u trenutku prije početka pokretanja sustava. Podržana su dva načina autentikacije – korištenje tajnog broja (eng. *Personal identification number – PIN*) i korištenje USB uređaja koji sadrži potreban sigurnosni ključ.
- **Isključivo USB autentikacija** je način kod kojeg korisnici moraju u računalo uključiti USB uređaj koji sadrži odgovarajući ključ. Potrebno je primijetiti da ovaj način zahtjeva odgovarajuću podršku BIOS programa.



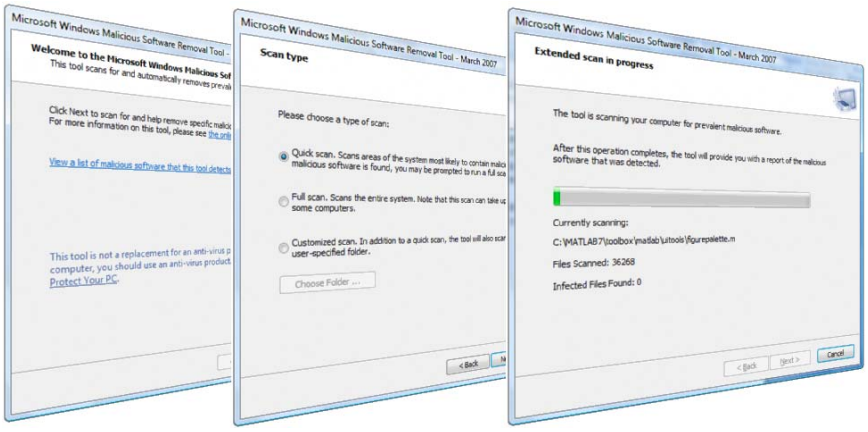
Slika 6: BitLocker Drive Encryption

Prema Microsoftovim podacima, korištenje BitLocker mehanizma može biti opasno ako korisnik izgubi zaporku. Naime, zasada ne postoji način za provedbu rekonstrukcije podataka. Ovo je jedan od mnogih problema koji su uzeti u obzir od pojave ovog mehanizma kao sastavnog dijela Vista operacijskog sustava.

3.6. Malicious Software Removal Tool

Čak i s poduzetim prikladnim sigurnosnim mjerama postoji određeni rizik da će zlonamjerne aplikacije (eng. *malware*) proći provjeru antivirusnog programa ili čak onemogućiti daljnje djelovanje antivirusnog programa. Programska podrška koja odstranjuje zlonamjerne aplikacije (eng. *Malicius Software Removal Tool*) je dizajniran upravo za sprječavanje takvih situacija. Kada je ovakav alat u funkciji on pronalazi i odstranjuje sve zlonamjerne aplikacije koje pronađe na korisnikovom računalu. Iako alat nije potreban ukoliko se konstantno koristi osvježeni antivirusni program, njegovim korištenjem se dobiva dodatna razina zaštite. Distribuira se zajedno s Vista sustavom te se može besplatno dobiti za korištenje s XP operacijskim sustavom.
Kada je alat pokrenut može se odabrati koji tip sigurnosnog pregleda korisnici žele:

- **Brzo** (eng. *Quick*): ukoliko se odabere ovaj način, Malicious Software Removal Tool će pretražiti sva polja na računalu na koje se sumnja da sadrže zlonamjerne aplikacije.
- **Potpuna** (eng. *Full*): s ovim načinom pretrage će cijeli sustav biti provjeren. Korisnici bi trebali koristiti ovakav način pregledavanja u razumnim vremenskim razmacima, iako ovakva pretraga može potrajati i nekoliko sati u ovisnosti o sustavu.
- **Uobičajena** (eng. *Custom*): izborom ovakvog načina pregleda potrebno je i odabrati nad kojim se mapama ili područjima računala želi obaviti sigurnosna provjera.



Slika 7: Sigurnosni pregled računala

4. Sigurnosne tehnologije Internet Explorer 7 web preglednika

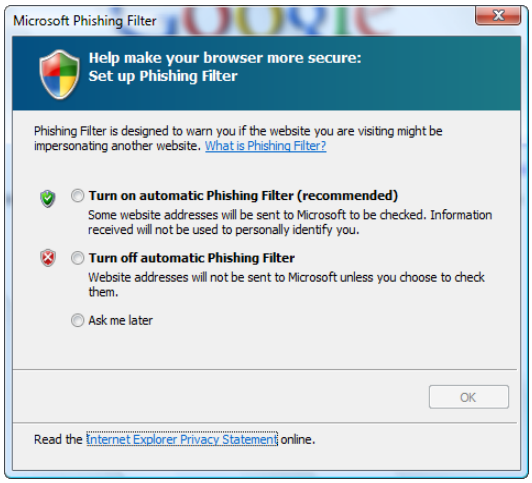
Učestalo korišten web preglednik Internet Explorer doživio je svoju sedmu inačicu (IE7), a isporučuje se kao dio Vista sustava. Važna novost je integriranje kartica za preglednije „surfanje" Internetom te implementacija mnoštva manjih značajki. Iako je IE7 dostupan i za Windows XP operacijske sustave, njegova potpuna funkcionalnost dolazi do izražaja tek na Vista sustavima. Najvažnije je napomenuti njegovu razinu integracije u operacijski sustav, pri čemu se koristi i prethodno opisani UAC mehanizam za umanjivanje sustavskih prava aplikacija pokrenutih iz preglednika. Razlog tome je umanjivanje ovlasti potencijalno opasnih aplikacija koje dolaze s posjećivanih web poslužitelja.

4.1. Internet Explorer 7

Odluka za nadogradnju postojećeg web preglednika se pojavila tijekom ulaska u tržište Mozilla Firefox web preglednika. Prva inačica paketa IE7 objavljena je 27. lipnja 2005. godine, a koristila se isključivo za tehnička testiranja. Prva inačica za javnost postala je dostupna 31. siječnja 2006. Konačna inačica izdana je 18. listopada 2006. godine. Radi se o pregledniku namijenjenom pružanju zaštite od tzv. *phishing*-a te varljivih zlonamjernih aplikacija i sličnih potencijalno opasnih prijetnji. Također, preglednik omogućuje potpunu kontrolu korisnika nad ActiveX kontrolama. U IE7 su ispravljeni neki od važnijih propusta iz prijašnjih inačica, poboljšane su podrške za web standarde. Ima i noviteta poput tzv. *Tab* načina rada, podrške za internacionalne nazive domena (*Internationalized Domain Name support - IDN)* i tzv. *antiphishing* filtra. Nova inačica ima i mehanizam za blokiranje web aplikacija - tzv. *applet*-a poput Flash i Java aplikacija.

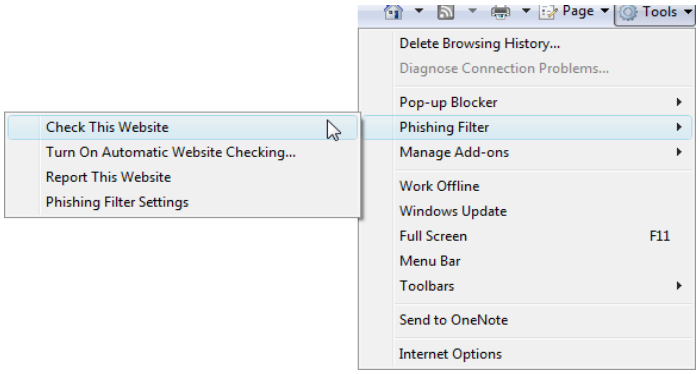
4.2. *Phishing* filtar

Phishing je jedan od oblika prijevare koji podrazumijeva skup aktivnosti kojima neovlašteni korisnici korištenjem lažnih poruka elektroničke pošte i lažnih web stranica, većinom financijskih organizacija, pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka. To su JMBG, korisnička imena i zaporke, PIN brojevi, brojevi kreditnih kartica i sl. Tijekom prethodnih godina *phishing* je postao jedan od velikih problema za korisnike Interneta. Internet Explorer implementira napredan mehanizam za borbu protiv ovakvih prevara uvođenjem Phishing Filter zaštite u svoju sedmu inačicu.
Phishing Filter je novitet u Internet Exploreru koji pomaže u pronalaženju bio kojeg oblika iznude osobnih podataka na web stranicama. Ovaj filtar koristi tri načina zaštite. Prvo uspoređuje adrese sumnjive stranice s adresama web stranica koje se nalaze na Microsoftovom popisu. Taj popis nalazi se na korisnikovom računalu. Nakon toga pomaže u analiziranju stranica koje se posjećuju tako da provjerava sadržaj i njegovu sličnost s karakterističnim sadržajem *phishing* poruka odnosno web stranica. Na kraju, uz dopuštenje korisnika šalje adresu problematične stranice Microsoftu kako bi se provjerilo da li je ona u popisu osvježenih izvještaja *phishing* stranica. Ukoliko se stranica pronađe u bazi, IE7 će prikazati upozoravajuću poruku.



Slika 8: Uključivanje *phishing* filtra

Za ručnu provjeru stranice potrebno je otvoriti Internet Explorer, zatim učitati stranicu koju se želi analizirati, odabrati opciju *Tools* te odabrati *Phishing Filter.* Konačno, potrebno je odabrati *Check This Website* opciju.



Slika 9: Provjera web stranice *Phishing Filter*-om

4.3. *Protected Mode* način rada

Sigurnosni način rada Internet Explorera, tzv. *protected mode*, je svojstvo koje zlonamjernim programima otežava neprimjetno instaliranje na korisnikovo računalo. Sigurnosni način rada omogućuje uobičajeno korištenje web usluga te instaliranje programa bez dovođenja računala u rizik kakvom bi bio podložan tijekom korištenja računa s administratorskim ovlastima. Naime, privilegije programa pokrenutih iz IE7 tijekom ovog načina rada su vrlo male, tolike da onemogućavaju pisanje po disku i utjecanje na druge procese ili njihov prostor u memoriji. Zaštitni način rada je uključen tvornički, a indikator je prikazan u statusnoj liniji.

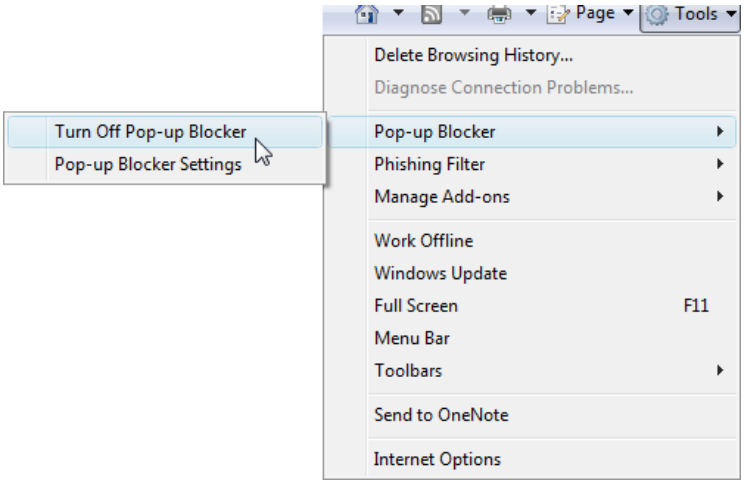
Slika 10: Indikator načina rada

U dodatku koji upozorava da web stranica želi instalirati neželjeni program, Internet Explorer će upozoriti korisnika o tome. Ako se želi isključiti ova mogućnost te dopustiti pokretanje spornog programa na bilo kojoj web stranici, potrebno je odabrati opciju *Always allow websites tu use this program to open web content*.

4.4. *Pop-up Blocker* mehanizam

Riječ je o mehanizmu za onemogućavanje otvaranja prozora koji se otvaraju zajedno s web stranicama kojima korisnik pristupa. Njihova svrha najčešće je prikazivanje reklama. Tzv. *Pop-up Blocker* je modul

Internet Explorer preglednika koji blokira većinu *pop-up* prozora. Korisnici mogu odabrati koju razinu blokiranja žele, od blokiranja pojave svih neželjenih prozora do dopuštanja pojave samo onih prozora koje žele vidjeti. Ovaj mehanizam je tvornički postavljen u aktivno stanje. Ukoliko se blokiranje želi isključiti ili ponovno uključiti potrebno je otvoriti Internet Explorer, odabrati izbornik *Tool*, te odabrati opciju *Pop-up Blocker* kao što je prikazano na sljedećoj slici.

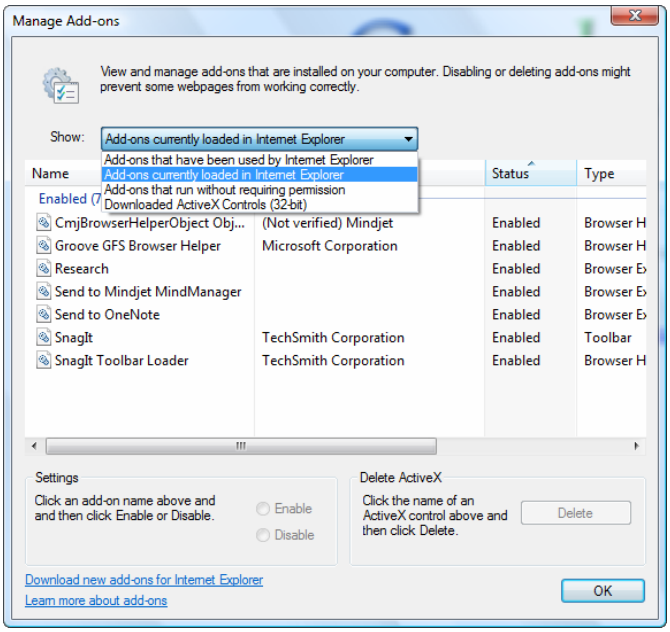


Slika 11: Postavljanje *Pop-up blocker* modula

4.5. *Add - on Manager*

Među web preglednicima trend je implementacija mogućnosti dodavanja programskih priključaka s različitim funkcionalnostima (eng. *add-on*). Riječ je i programskim proširenjima poput dodatnih alatnih traka, animiranja kursora i sl. Priključci se uobičajeno preuzimaju s Interneta te se tijekom njihove instalacije traži dopuštenje korisnika. Međutim, neki od njih se mogu instalirati i bez korisnikova znanja. Ovo se može dogoditi ako se, na primjer, instaliranjem nekog programa instalira i programski priključak. Da bi se provjerilo koji od *add-on* programa su instalirani, potrebno je otvoriti Internet Explorer i odabrati izbornik *Tools*, *Manage Add-on* te na posljetku *Enable or Disable Add-ons*. Nakon navedenih koraka pojavljuje se prozor (prikazan na slijedećoj slici) s izbornikom za pregledavanje koji nudi sljedeće opcije:

- odabirom prve opcije *Add-ons that have been used by Internet Explorer*, prikazati će se popis programskih dodataka koji su instalirani na korisnikovom računalu,
- kako bi se prikazalo one dodatke koji se trenutno koriste potrebno je odabrati *Add-ons currently loaded in Internet Explorer*,
- odabirom *Add-ons that run without requiring permission* prikazuju se dodaci koji su pokrenuti bez korisnikova znanja,
- kako bi se dobio uvid u isntalirane ActiveX kontrole, potrebno je odabrati *Downloaded ActiveX Controls (32-bit)*.



Slika 12: Podešavanje dodataka u IE7

4.6. Digitalni potpisi

Digitalni potpis je elektronska sigurnosna oznaka koja se dodaje u datoteke. Potpis omogućava provjeru izvora datoteka te osigurava autentičnost poruke. Ukoliko datoteka ne sadrži valjani digitalni potpis, ne postoji način na koji se može dokazati da je ona zaista iz izvora kojim se predstavlja. Pored toga, datoteka s neispravnim digitalnim potpisom može sadržavati i zlonamjerne aplikacije. U ovakvom je slučaju sigurnije ne otvarati spornu datoteku. Čak ni za datoteku s valjanim potpisom nije moguće sa sigurnošću reći da je bezazlena, tako da se korisnici moraju osloniti na povjerenje koje imaju prema izvoru digitalnog potpisa odnosno dokumenta.

4.7. Sigurnost web transakcija

IE7 podržava 128-bitni sigurnosni (SSL) priključak za korištenje sigurnih web stranica i prijenos potencijalno osjetljivih informacija. Navedeni alat pomaže pri stvaranju šifrirane poveznice na takve web stranice. Kada se pošalje informacija na spornu stranicu, ona se kriptira na korisnikovom računalu i dekriptira na odredišnom računalu. Kako bi korisnici bili sigurni da koriste sigurnu vezu, Internet Explorer će prikazati zaključanu ikonu u statusnoj liniji (eng. *Security Status bar*). Ova opcija je vrlo korisna ukoliko korisnici zahtijevaju pristup financijskim ili nekim drugim osjetljivim podacima putem Interneta.

5. Zaključak

Nakon niza godina Microsoft je izdao novu inačicu operacijskog sustava koja sadrži brojne izmjene u odnosu na prethodnu inačicu Windows XP. Neka poboljšanja su uočljiva već pri kratkom radu sa sustavom, a tu se mogu nabrojati nadogradnja grafičkog korisničkog sučelja, izmjena funkcionalnosti nekih često korištenih aplikacija poput Windows Explorera i sl.

Velikom broju korisnika svakako su važne i nadogradnje ovog sustava na području lokalne i Internet sigurnosti. Budući da je Internet Explorer jedan od najčešće korištenih web preglednika, Microsoft je doradio i funkcionalnost te aplikacije kao i njenu integraciju u operacijski sustav. To se manifestira i smanjenjem ovlasti koje dobivaju web aplikacije pokrenute iz samog preglednika.

Obzirom da je konačna inačica Windows Vista operacijskih sustava dostupna tek kraće vrijeme, za očekivati je odgovarajuće sigurnosne nadogradnje i ispravke postojećih pogrešaka koje će tek biti uočene masovnim korištenjem sustava. Unatoč tome što se, prema dosad iznesenom, vidi značajan napredak u pogledu sigurnosti, vrijeme i količina uočenih propusta ipak će donijeti konačnu ocjenu novih sigurnosnih elemenata Vista sustava.

6. Reference

[1] Microsoft Corporation, http://www.microsoft.com/windows/products/windowsvista/default.mspx, ožujak 2007.

[2] Microsoft Corporation, http://msdn2.microsoft.com/en-us/windowsvista/default.aspx, ožujak 2007.

[3] Patrick Schmid, Achim Roos, http://www.tomshardware.com/2007/01/29/xp-vs-vista, ožujak 2007.

[4] Microsoft Corporation, http://www.windows-vista-update.com/Windows_Vista_vs_Windows_xp.html, ožujak 2007.

[5] Microsoft Corporation, http://www.microsoft.com/technet/technetmag/issues/2007/02/VistaKernel/, ožujak 2007.

[6] Scott Field, http://blogs.msdn.com/windowsvistasecurity/archive/2006/08/11/695993.aspx, ožujak 2007.

[7] Microsoft Corporation, http://www.microsoft.com/security/default.mspx, ožujak 2007.

[8] Microsoft Corporation, http://www.microsoft.com/technet/technetmag/issues/2006/11/Defender/?topics=/technet/technetmag/issues/2006/11/Defender, ožujak 2007.

[9] Microsoft Corporation, http://www.microsoft.com/technet/windowsvista/security/guide.mspx, ožujak 2007.

[10] Microsoft Corporation, http://technet.microsoft.com/en-us/windowsvista/aa905062.aspx, ožujak 2007.

[11] Symantec Corporation, http://www.symantec.com/avcenter/reference/Windows_Vista_Security_Model_Analysis.pdf ožujak 2007.

[12] Microsoft Corporation, WindowsVistaSecurityWP.doc, lipanj 2006.

[13] Symantec Corporation, http://www.symantec.com/avcenter/reference/Windows_Vista_Kernel_Mode_Security.pdf, ožujak 2007.