CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Usporedba "sandbox" programskih alata

CCERT-PUBDOC-2009-03-259

+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

Korisnici računala često nisu svjesni opasnosti koje im prijete pri pregledavanju Interneta i pokretanju datoteka iz nepoznatih izvora, stoga je vrlo važno naći primjeren način zaštite osobnih informacija, podataka i datoteka. Osim zaštite računala antivirusnim programima, vatrozidima i anti-spam alatima, korisniku su na raspolaganju još neka rješenja koja se pokazuju korisna u specifičnim situacijama.

Jedno od takvih rješenja su „sandbox" alati, koji korisniku pružaju zaštitu od pokretanja neželjenih programa ili programskog koda koji nije ispitan (istraživačke svrhe ili pri izradi novih programa). Sandbox-om se strogo nadgledaju i ograničavaju resursi na računalu, poput prostora na tvrdom disku namijenjenom za privremenu pohranu podataka (*eng. scratch space*) i/ili prostora u memoriji, za pokretanje programa ili kodova koji su potekli iz nepoznatih izvora. Određenom procesu su dodijeljeni ograničeni resursi i pravila kojima se određuju njegove mogućnosti djelovanja na računalu. Sandbox odvaja korisničke zahtjeve i procese od jezgre operacijskog sustava.

U ovom dokumentu će biti objašnjen princip rada „sandbox" alata, njihove primjene, te specifični primjeri nekoliko proizvođača.

2. Opis „sandbox“ mehanizma

Sandbox je virtualno okruženje koje služi kako bi se operacijski sustav i podatke na računalu zaštitilo od zlonamjernih programa, slučajnih izmjena postavki operacijskog sustava ili namjernog nanošenja štete samom operacijskom sustavu.

Sandbox alat može biti vrlo korisno i učinkovito sredstvo zaštite korisnika od zloćudnih programa, koji pregledavanjem zlonamjernih web adresa i korištenjem prijenosnih medija mogu dospjeti na računalo. Sandbox onemogućuje pokretanje i rad neželjenih programa tako da ograničava raspoložive računalne resurse (npr. prostor na tvrdom disku, prostor u memoriji, itd.). Sandbox alatima moguće je još zabraniti ili ograničiti:

- mrežni pristup (za slučaj udaljenih ili lokalnih napada),
- mogućnost pregledavanja podataka i datoteka na poslužitelju ili drugom računalu i
- učitavanje podataka sa vanjskih prijenosnih medija.

Pomoću sandbox alata određuje se razina pristupa nekog programa na računalu. U tom smislu, sandbox alat dodjeljuje programu ili operacijskom sustavu virtualni prostor i onemogućuje njegovo djelovanje unutar operacijskog sustava (fizičkog) računala. Programu nije dopušteno pisati, mijenjati ili čitati datoteke operacijskog sustava.

Kako bi se lakše razjasnio pojam sandbox mehanizma, u nastavku će biti navedeno nekoliko primjera koji se nalaze u svakodnevnoj uporabi (i vrlo su raširena na računalima korisnika):

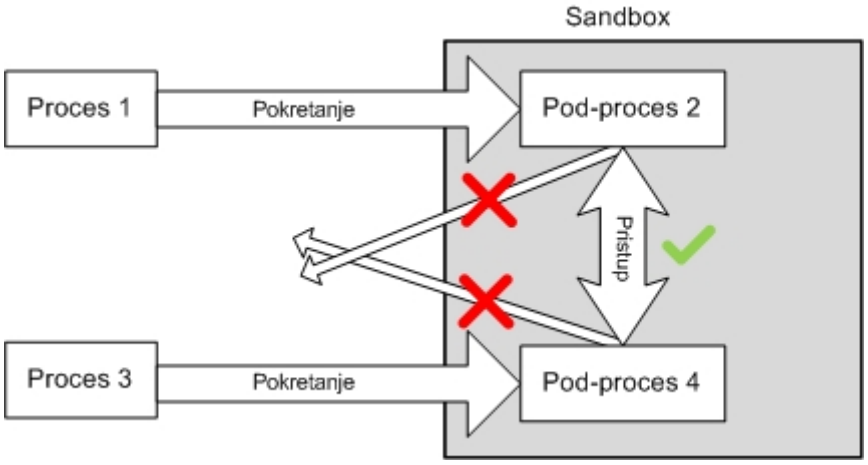
- ***Applet* programi** su nezavisni programi koji se izvršavaju u virtualnim računalima i/ili programima prevoditeljima koji su ujedno i sandbox alati. *Applet* programi su vrlo česti dodaci za web preglednike. Ti programi koriste sandbox mehanizam kako bi na siguran način pokrenuli programske kodove koji se nalaze na web stranicama koje korisnik posjećuje. Tri najčešće korištena applet programa s kojima je većina korisnika upoznata su: Adobe Flash, Java applet te Microsoft Silverlight.
- **Zatvor** (*eng. jail*) je niz ograničenja koja programima postavlja jezgra operacijskog sustava (*eng. kernel*). Ovaj primjer sandbox mehanizma se najčešće koristi kod poslužitelja. Jezgra operacijskog sustava dozvoljava pokretanje više, međusobno izoliranih procesa, umjesto samo jednog. Svakom procesu su nametnuta ograničenja, tako da ne može komunicirati sa drugim procesima. Ako kod jednog procesa pođe nešto po krivu, taj proces ne može uzrokovati neispravno djelovanje drugih procesa. Na jednom se poslužitelju nalazi veći broj međusobno izoliranih web domena, pri čemu su svakoj postavljena određena ograničenja (prostor na tvrdom disku, razina pristupa, itd.).
- **Pokretanje određeno pravilima** (*eng. Rule-based Execution*) daje korisniku potpuni nadzor nad pokrenutim procesima. Ograničenja je moguće postaviti procesima koji se sami umnožavaju u sustavu, onima kojima je dozvoljeno ubacivati programski kod u druge programe te u procese koji imaju pristup Internetu. Ovim je mehanizmom moguće upravljati i razinom ovlasti pisanja ili čitanja određenih podataka na sustavu. Korištenjem ovog mehanizma korisnik smanjuje opasnost od „zaraze“ računala virusima i trojanskim konjima.
- **Virtualna računala** (*eng. Virtual Machine*) su potpuno funkcionalna računala na kojima se operacijski sustav može pokretati putem alata za virtualizaciju. U tom slučaju, virtualnom operacijskom sustavu su nametnuta ograničenja pri korištenju resursa računala, te ih može koristiti jedino posredno putem alata za virtualizaciju. Primjer takvog alata je VMware Workstation.
- **Sandbox mehanizam na stvarnim računalima** je najčešće korišten u tvrtkama koje se bave računalnom sigurnošću. Istraživači koriste sandbox alate kako bi analizirali ponašanje zlonamjernih programa. Stvarajući okruženje koje oponaša računala na koja je usmjeren napad, istraživači mogu saznati na koji način zlonamjerni programi ugrožavaju računala korisnika.
- **Sustavi mogućnosti** (*eng. capability systems*) su sandbox mehanizmi s vrlo jasnim i definiranim pravilima. Svakom programu na računalu se dodjeljuje određena oznaka na temelju koje operacijski sustav razlučuje kojim resursima program ima pristup. Ovakvi mehanizmi su najčešće ugrađeni u jezgru operacijskog sustava.

Mehanizam	Upotreba	Zaštita
Applet programi	Pokretanje programskih kodova sa web stranica	Zaštita od zlonamjernih programskih kodova koji se nalaze na web stranicama.
Zatvor	Odvajanje više web domena na istom poslužitelju	Zaštita od širenja neispravnog djelovanja jednog procesa na druge procese.
Pokretanje određeno pravilima	Ograničavanje mogućnosti programa na računalu	Sprječavanje djelovanja i „zaraze“ zlonamjernim programima.
Virtualna računala	Virtualno pokretanje i/ili ispitivanje programa i operacijskih sustava	Zaštita od nepoželjnog djelovanja ispitivanih alata na operacijski sustav računala.
Sandbox na stvarnim računalima	Analiza ponašanja programa	Zaštita od „zaraze“ zlonamjernim programima i mijenjanja postavki na računalu.
Sustavi mogućnosti	Određivanje razine ovlasti nekog programa	Zaštita od nedozvoljenog pokretanja programa nepoznatih autora.

Tablica 1. Mehanizmi rada sandbox alata

Način rada sandbox mehanizma je također jednostavno objasniti na slijedeći način:

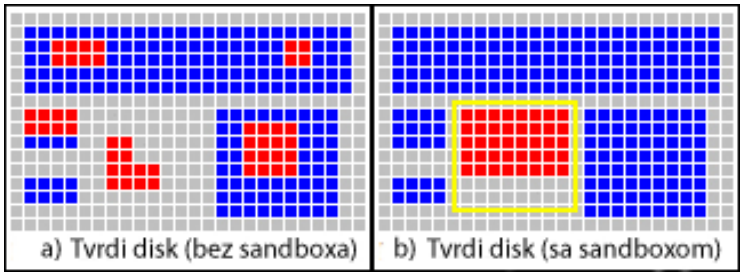
- Ako „proces 1“ pokrene „pod-proces 2“ unutar sandboxa, ovlasti „pod-procesa 2“ će biti ograničene na podskup ovlasti „procesa 1“.
- „Proces 1“ je pokrenut na stvarnom računalu, pa će stoga imati i pristup svim procesima na računalu. Međutim, „pod-proces 2“ će imati pristup samo onim procesima koji su pokrenuti u istom sandboxu, što znači da su im nametnuta ista ograničenja i nemaju utjecaja na operacijski sustav. Tako neće moći prouzročiti štetu na stvarnim procesima računala.
- Izuzevši bilo kakve propuste unutar sandbox alata koji bi se mogli iskoristiti kako bi se nanijela šteta računalu, opseg potencijalne štete koju bi „pod-proces 2“ mogao prouzročiti svodi se na razinu pojedinog sandbox-a.



Slika 1. Prikaz principa rada sandbox mehanizma

Dakle, čak i u slučaju da korisnik preuzme s Interneta zlonamjerni program (virus, crv, trojanski konj, keylogger, itd), ta datoteka će biti ograničena unutar sandbox-a i neće imati nikakav utjecaj na operacijski sustav korisnika niti njegove datoteke.

Bez uporabe sandbox alata podaci koje korisnik preuzima sa Interneta ili bilo kojih drugih medija, izravno se zapisuju na tvrdi disk i većinom imaju pristup gotovo svim procesima ili datotekama. Zapisivanje podataka na tvrdi disk prikazano je Slikom 2.



Slika 2. Zapisivanje podataka na tvrdi disk
(a) bez sandbox mehanizma i (b) korištenjem sandbox mehanizma
Izvor: Sandboxie

Siva boja označava prazan prostor na tvrdom disku, plava označava programske datoteke i datoteke operacijskog sustava, a crvena novi, potencijalno opasni sadržaj. Vidljivo je da pri zapisivanju podataka kod tvrdog diska bez sandboxa ne postoji nikakvo ograničenje gdje se podaci smiju zapisivati, tj. datoteke zapisane na tvrdom disku mogu komunicirati sa datotekama operacijskog sustava.

Suprotno tome, kao što je prikazano na Slici 2., kod zapisivanja na tvrdi disk sa sandbox alatom, vidljivo je da se unutar sandbox-a (žuti okvir) novi sadržaj zapisuje zadanim redoslijedom i potpuno je izoliran od programskih datoteka i datoteka operacijskog sustava (to je zadaća sandbox alata). Novi sadržaj je, kao što je ranije rečeno, ograničen na djelovanje unutar sandboxa i nije mu omogućeno komuniciranje sa datotekama u sustavu. Za zaštitu je ključno upravo razdvajanje datoteka u sandboxu (virtualno) i datoteka na računalu (operacijski sustav, programske datoteke, podaci).

3. Primjena „sandbox" alata

Zbog dostupnosti Interneta na gotovo svim lokacijama, poput javnih pristupnih točaka (*eng. public access point*), edukacijskih ustanova, Hot-Spot točaka i tvrtki, te učestalog korištenja prijenosnih medija, potrebno je ugraditi neku vrstu zaštite kako bi se korisnike, podatke i datoteke na računalima zaštitilo od neželjenih pristupa i izmjena.

Sandbox alati se primjenjuju i kod istraživanja sigurnosti te ispitivanja novih programa kako ne bi došlo do neželjenih aktivnosti na računalima.

3.1. Javne pristupne točke

Mjesta poput javnih pristupnih točaka su okruženja za zajedničko korištenje računala. Poslovni se model uspješne javne pristupne točke zasniva na usluzi kvalitetnog i pouzdanog pristupa Internetu, pritom smanjujući dodatne troškove nabavke novih računala i održavanja postojećih.

Javne pristupne točke mogu biti poprilično grubo okruženje za računala zbog velikog broja korisnika koji koriste ponuđene usluge. Teško je pouzdati se u činjenicu da će se svi anonimni korisnici odnositi prema računalu s pažnjom „dobrog gospodara". Većina javnih pristupnih točaka korisnicima ne postavlja nikakva ograničenja, što se može pokazati kobnim za ispravan rad računala. U takvim slučajevima vrlo su česta pojava virusi, crvi i drugi zlonamjerni programi koji mogu naštetiti svakom budućem korisniku. U ovakvoj situaciji povećavaju se troškovi održavanja postojećih računala.

Korištenjem sandbox alata javne pristupne točke štite svoje vlasništvo (računala), ali ujedno i korisnike od gubitka podataka. Sandbox alat onemogućuje korisnicima da rade neovlaštene promjene na računalu, instaliraju svoje programe ili brišu sistemske datoteke. Kod javnih pristupnih točaka najčešće se koriste mehanizmi pokretanja određenog pravilima, sandboxa na stvarnim računalima i sustavi mogućnosti.

3.2. Edukacijske ustanove

U edukacijskim ustanovama računala su nastavna pomagala. Vrlo je važno da računala rade ispravno kako se vrijeme ne bi trošilo na popravak i osposobljavanje računala već na učenje novih sadržaja. U učionicama može postojati manji broj računala na kojima se veći broj učenika izmjenjuje. Računala bi uvijek trebala biti podešena na način na koji će nabolje služiti svim korisnicima.

Najveći problem predstavlja nedolično ponašanje krajnjih korisnika,koji često pokušavaju:

- fizički oštetiti računala,
- instalirati ilegalne programe,
- mijenjati korisničke zaporke i zaporke administratora,
- učitavati zabranjene datoteke,
- mijenjati sistemske postavke i
- brisati datoteke.

Još jedan sličan primjer su knjižnice, u kojima korisnici koriste računala kako bi pronašli informacije na Internetu, tj. računala koriste u istraživačke svrhe. Kako se računala ne bi morala često popravljati, što također ide na štetu korisnicima, ugrađeni su sandbox alati koji ograničavaju i štite korisnike i računala od neželjenih akcija i njihovih utjecaja na podatke. U edukacijskim ustanovama se u primjeni mogu naći mehanizmi sandboxa na stvarnim računalima i pokretanja određenog pravilima.

3.3. Ispitivanje i razvoj programa

Sandbox alati se pokazuju vrlo korisnim i proizvođačima programskih paketa jer omogućuju sigurno ispitivanje proizvoda prije objave. Kada se neki program ispituje unutar sandbox sustava, moguće je bez ikakvih rizika po ostala računala lokalne mreže saznati da li postoje propusti u programu i koje su njegove osjetljive točke.

Pomoću sandbox alata može se otkriti da li u programu postoji određeni propust kojeg napadači mogu iskoristiti kako bi ugrozili korisnike. Određeni zlonamjerni programi su napravljeni kako bi pronašli i iskoristili specifični sigurnosni propust u operacijskom sustavu ili programima. Ako postoji neki zlonamjerni program kojim je moguće iskoristiti propuste u programu, proizvođači programa ga mogu

izolirati pomoću nekog sandbox alata i tako riješiti pronađeni propust. Najčešće se primjenjuju mehanizmi virtualnih računala i sandboxa na stvarnim računalima.

3.4. Analiza zlonamjernih programa

Proizvođači sigurnosnih alata svakodnevno koriste sandbox alate koji im omogućuju da izoliraju zlonamjerne programe kako bi zaštitili korisnike. Sandbox alat omogućuje korisniku da pokreće programe unutar virtualnog ispitnog „laboratorija" bez ikakvih posljedica i utjecaja na operacijski sustav i datoteke koje se nalaze na stvarnom fizičkom računalu. Upravo radi ovoga, sandbox alati se ubrajaju i u alate za otkrivanje i suzbijanje zlonamjernih programa.

Kao što je ranije objašnjeno, sandbox alat će npr. dopustiti virusu da izvršava svoj kod unutar zaštićenog virtualnog okruženja, ali neće dozvoliti njegovo djelovanje izvan zaštićenog dijela (kojeg štiti sandbox alat). Proizvođači sigurnosnih alata potom prate što zlonamjerni program radi i kako djeluje. Pri analizi zlonamjernih programa najučinkovitiji mehanizam zaštite je sandbox na stvarnom računalu.

3.5. Sigurnost

Uz konvencionalne načine zaštite (antivirusni programi, vatrozidi, anti-spam alati, itd.) vrlo se često koriste i sandbox alati koji sprječavaju nedozvoljenu instalaciju programa s Interneta. Korisnicima se često događa da zajedno s programom koji preuzimaju s Interneta preuzmu i neki drugi program koji se neovlašteno instalira i sadrži neku štetnu funkcionalnost (šalje udaljenom napadaču podatke o računalu, skuplja informacije o računalima lokalne mreže itd.). Ovakvih je programa na Internetu sve više i potrebno je obratiti pažnju i preuzimati datoteke jedino sa službenih stranica proizvođača. Ukoliko se korisniku svejedno dogodi slučaj da preuzme „dodatak" sa željenim programom, korištenjem sandbox alata neće biti ugrožen jer će program biti pohranjen i pokrenut u sandboxu. Sandbox će potom onemogućiti djelovanje zlonamjernog programa, tj. neće mu dopustiti djelovanje na datoteke programa izvan sandboxa i operacijskog sustava.

Također, sandbox alati se koriste za zaštitu od phishinga, tj. krađe informacija (korisnička imena, zaporke, povjerljivi podaci). Vrlo često, računalo korisnika biva zaraženo nekim oblikom zlonamjernog programa koji pohranjuje podatke koje korisnik zapisuje na računalu. Jedan od takvih programa je keylogger – alat koji prati i zapisuje sve što je korisnik napisao na tipkovnici te kasnije to šalje napadaču. Ukoliko korisnik ne primjeni zaštitu, neće biti svjestan da je njegovo računalo zaraženo. Sustavi mogućnosti i pokretanje određeno pravilima korisniku mogu pružiti primjerenu zaštitu (jer zlonamjernom programu neće dopustiti slanje podataka).

Kako bi se povećala sigurnost računala koriste se gotovo svi mehanizmi zaštite navedeni u poglavlju 2.

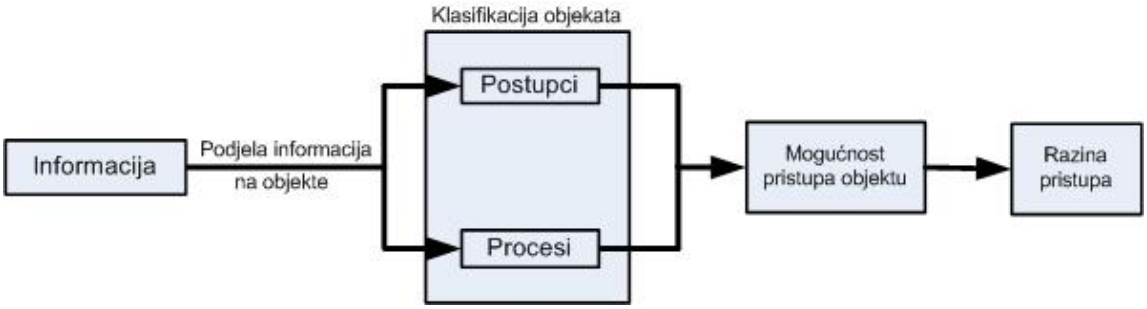
4. Primjeri sandbox alata kroz povijest

Sandbox alati su već duže vrijeme prisutni kao način zaštite. Ovi alati su u samim začecima zaokupili pažnju istraživača, pa se kao rezultat pokazala intenzivna uporaba ove vrste zaštite od zlonamjernih programa. Butler Lampson je u svojem dokumentu „Zaštita" 1971. godine opisao apstraktan model sandbox alata naglašavajući svojstva nekoliko postojećih mehanizama koji su služili za zaštitu i nadzor razine pristupa. Većinu ovih mehanizama smatra se pretečama današnjih sandbox alata. U nastavku će biti navedeno nekoliko sandbox alata koji su se pojavljivali kroz povijest.

4.1. Hydra

Hydra je nastala 1975. godine i radila je na principu sustava mogućnosti (*eng. capability-based system*). Svakom programu na računalu su dodijeljene oznake na temelju kojih operacijski sustav razlučuje kojim resursima program ima pristup. Zaštitna jezgra je omogućavala mehanizmima da primjenjuju pravila u korisničkim programima koji komuniciraju s jezgrom sustava. Kako bi zaštitilo računalo Hydra je primijenila pravila:

- Podjele informacija na zasebne objekte.
- Klasifikacije objekata prema namjeni. Neke vrste objekata (poput postupaka i procesa) su unaprijed ugrađeni u Hydru, ali također postoje i mehanizmi za stvaranje novih objekata.
- Korištenja mogućnosti kako bi se odredilo da li je moguć pristup objektu.
- Određivanje razine pristupa.
- Stvaranje modula koji se nazivaju podsustavi. U podsustavima se zapisuje zastupljenost i ugrađivanje svih radnji za svaku vrstu objekta. Korisnik je mogao pristupiti objektima koristeći ispravne poveznice.



Slika 3. Prikaz rada programa Hydra

Hydra se pokazala važnom zbog slijedećih karakteristika:

- zaštita,
- „sandboxing",
- sigurnost,
- virtualizacija i
- kvaliteta usluge.

Zaštitom je ograničeno koji se programi mogu pokrenuti, dok „sandboxing" ima namjenu razdvajanja procesa operacijskog sustava i procesa koje je korisnik pokrenuo. Što se tiče sigurnosti, Hydra je onemogućavala bilo kakvu aktivnost procesa za koje nisu postojala pravila. Virtualizacija je omogućila korisniku da bez posljedica uočljivih u radu operacijskog sustava koristi proizvoljne programe. Korisnici su bili uvjereni u kvalitetu usluge Hydre, jer je tada bila jedno od najučinkovitijih sredstava zaštite ove vrste.

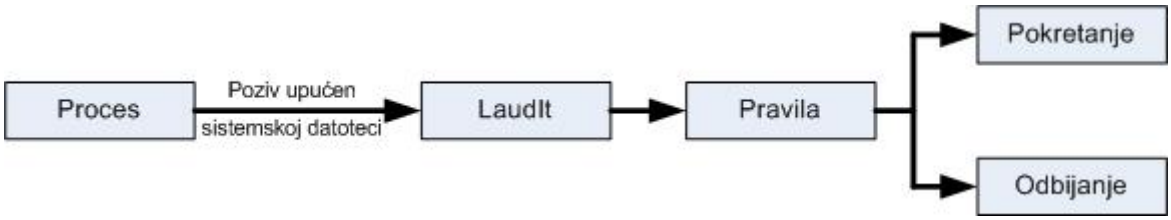
4.2. TRON

TRON je modul koji je ugrađen kao dio jezgre operacijskog sustava „Ultrix" (operacijski sustav temeljen na „Unix"-u). Temeljio se na principu nadziranja razine pristupa. Koristeći TRON, korisnik je mogao odrediti ovlasti nekog procesa u pristupanju sistemskim datotekama (zasebne datoteke, popisi datoteka i njihov smještaj). TRON je također omogućavao zaštićena područja - okruženja s ograničenim pristupom i posebno određenim pravilima koja su označavala razinu pristupa.

Pravilima je određeno da li će neki proces imati dozvolu pisati, čitati, pokretati, brisati i mijenjati sistemske datoteke.

4.3. LaudIt

LaudIt je prvi puta ugrađen u Linux jezgru 1977. godine i bio je jedan od prvih mehanizama za presretanje poziva sistemskim datotekama. LaudIt je također bio i prvi mehanizam te vrste koji je bilo moguće prilagoditi i programirati. Napravljen je kao modul koji je bilo moguće učitavati u jezgru operacijskog sustava. Radio je tako da je dinamički pratio pozive sistemskim datotekama i nudio korisniku različite razine zaštite.



Slika 4. Prikaz rada mehanizma LaudIt

Korisničko sučelje i sučelje za programiranje (*eng. Application Programming Interface*) su omogućili korisniku da odabere razinu zaštite. Ukoliko bi neki proces dobio poziv za pokretanje, LaudIt bi prvo provjerio u pravilima da li je određeno da se taj proces smije ili ne smije pokrenuti i na temelju tih pravila pokrenuo ili odbio pokrenuti željeni proces.

5. Usporedba popularnih programskih alata danas

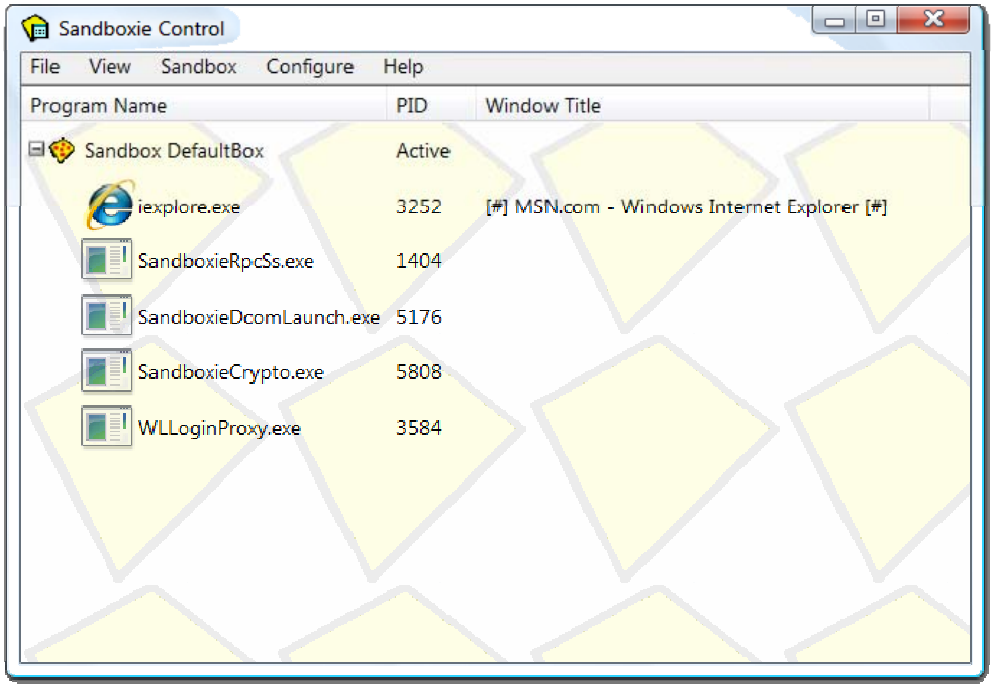
Niti jedan programski alat nije univerzalan, jer različiti korisnici imaju različite zahtjeve. Vrsta potrebne zaštite je drugačija kod svakog korisnika. Kako bi korisnici dobili što bolji uvid u prednosti i mane, te samu sigurnost i zaštitu koju današnji sandbox alati pružaju, u nastavku će biti navedeni najpopularniji primjeri.

5.1. Sandboxie

Sandboxie je komercijalan sandbox program za 32-bitne Windows operacijske sustave. U trenutku pisanja dokumenta posljednja inačica programa bila je 3.34. Koristi se za sandbox zaštitu:

- datoteka,
- tvrdih i drugih diskova,
- datoteka za registraciju (*eng. registry keys*),
- procesa,
- poveznica,
- komponenata pokretačkih programa (*eng. driver objects*),
- e-pošte i
- mnogih drugih datoteka.

Posjeduje veliki broj konfiguracijskih postavki i kvalitetno grafičko sučelje koji su orijentirani prema naprednijim korisnicima. Program je svrstan u kategoriju tzv. *shareware* programa, tj. besplatan je za korištenje prvih 30 dana, a po isteku tog vremenskog perioda, pri pokretanju programa korisniku se javlja upozorenje da registrira (kupi) proizvod. U besplatnoj inačici su također onemogućene neke funkcije što će pojedinim korisnicima vjerojatno zasmetati. Program je moguće preuzeti sa ovlaštenih web stranica, a registracijski kod je moguće kupiti putem Internet trgovine koja je navedena na ovlaštenoj stranici proizvoda. Cijena navedena na web stranici odnosi se na osobnu upotrebu, i nema vremenski rok trajanja što ovaj proizvod čini vrlo traženim.



Slika 5. Prikaz izgleda korisničkog sučelja Sandboxie programa

Izvor: Sandboxie

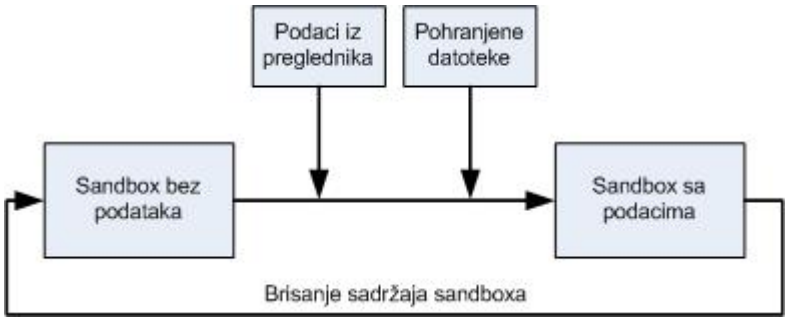
Sandboxie nudi veliki broj konfiguracijskih postavki kroz dva glavna pogleda:

1. Programi (*eng. Programs*)
2. Datoteke i mape (*eng. Files and Folders*)

Sandboxie uspješno zaustavlja crve, trojanske konje, rootkitove, mijenjanje sistemskih datoteka i zlonamjerne programe koji na neki način žele naštetiti računalu i korisniku jer programima unutar sandboxa nije dopuštena izravna komunikacija sa operacijskim sustavom.

Princip rada Sandboxie alata je najjednostavnije opisati na slijedeći način:

1. na tvrdi disk se zapisuju podaci, slično kao i na listu papira
2. svaki program koji korisnik pokreće „zapisuje nešto na list papira“
3. kada korisnik pregledava Internet, njegov preglednik zapisuje podatke o posjećenim stranicama na „list papira“
4. Sandboxie alat se može zamisliti kao „omot“ koji se stavi preko lista papira
5. programi umjesto na „list papira“ zapisuju podatke na „omot“ kojim je prekriven „list papira“
6. kada korisnik izbriše aktivni (npr. odjavi se sa računala) sandbox, briše „omot“ na kojem su podaci, a „list papira“ ostaje potpuno čist



Slika 6. Prikaz rada programa Sandboxie

Sandboxie omogućuje pokretanje gotovo svih programa u sandboxu, ali kao preporuka koje bi programe trebalo pokretati u sandboxu navedeni su:

- web preglednici,
- programi za čitanje e-pošte i vijesti,
- programi za komunikaciju (pismenu ili glasovnu),
- programi za povezivanje ravnopravnih računala (*eng. peer-to-peer*) i
- računalne igre (naročito igre koje se igraju putem Interneta).

Ukoliko korisnik koristi Sandboxie kao zaštitu od zlonamjernih programa, mogućnosti zaraze su vrlo malene (ali ne i u potpunosti uklonjene). Taj slučaj vezan je uz propuste u samom programu. No, program se vrlo često nadograđuje, tako da su mogućnosti zaraze svedene na minimum. Kako bi korisnik bio siguran, preporuča se korištenje antivirusnog programa u kombinaciji sa Sandboxie alatom. Ako se koristi kombinacija antivirusnog programa i Sandboxie programa, potrebno je prvo postaviti antivirusni programa, a potom Sandboxie. Na ovaj će način antivirusni program štititi datoteke izvan sandboxa i služiti kao druga linija obrane od zlonamjernih programa.

Jedan od nedostataka Sandboxie alata jest da istovremeno s jednim virtualnim sandboxom može štititi samo jedan program ili proces. Korisnik je u mogućnosti pokrenuti više virtualnih sandboxa, ali u tom slučaju može doći do osjetnog pada performansi krajnjih korisničkih programa.

Nedostatak Sandboxie alata je također što neki legalni i zlonamjerni programi ipak imaju utjecaja na rad računala. Sandboxie uspijeva spriječiti njihovo zlonamjerno djelovanje, ali ne i potpuno ih ukloniti sa sustava. Posljedice mogu biti ispisivanje greški, usporavanje ili potpuno blokiranje rada računala. Ovaj nedostatak uzrokovan je činjenicom da Sandboxie ne može imitirati pokretačke programe operacijskog

sustava (pokretački programi grafičke kartice, matične ploče, tvrdog diska, itd.). Međutim, ovaj nedostatak niti u kojem slučaju neće ugroziti stvarne korisničke podatke na računalu.

Još jedan nedostatak jest da Sandboxie sve odluke prepušta korisniku, tj. nema ugrađen sustav razlučivanja sigurnih i nesigurnih procesa i programa. Ovaj nedostatak zna vrlo često završiti loše po korisnika koji nema dovoljno znanja o zlonamjernim programima koji se nalaze na Internetu. Takvim korisnicima se savjetuje korištenje drugih alata za zaštitu (antivirusni programi, vatrozidi, anti-spam programi, itd.)

Sandboxie je moguće pokrenuti na Microsoft Windows 2000, XP, Vista te Microsoft Windows Server 2003 operacijskim sustavima. Na službenim stranicama je objavljeno da su ovo jedini operacijski sustavi koji će zasad biti podržani.

5.2. Faronics Deep Freeze

Deep Freeze je program namijenjen za više operacijskih sustava (Linux, Mac OS X i Microsoft Windows). Program nije besplatan, ali je svakako preporučljiv za korištenje u ustanovama u kojima veliki broj korisnika ima pristup računalima. Deep Freeze daje administratorima računala mogućnost da zaštite datoteke operacijskog sustava i postavke bez da korisnicima onemoguće normalan i učinkovit rad.

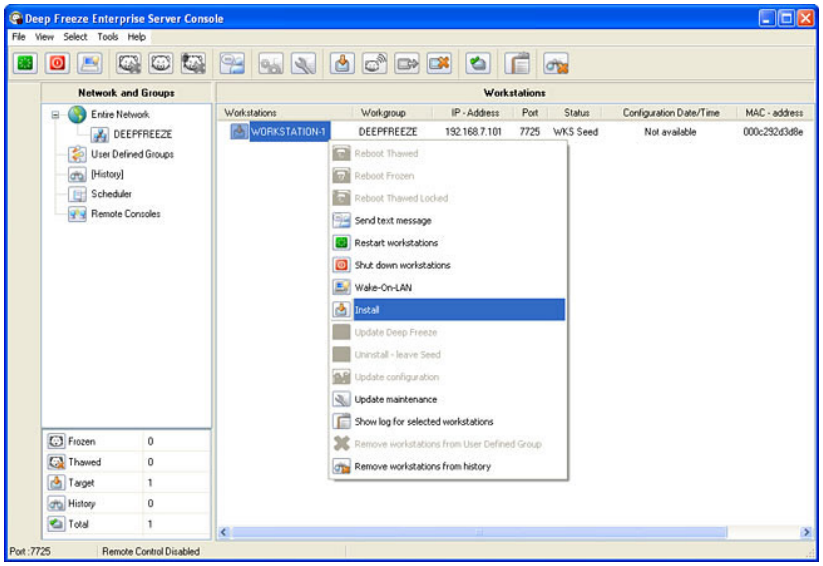
Kada se Deep Freeze postavi na računalo, napravljena šteta, bilo da je posljedica namjerne ili nenamjerne radnje, nije trajna jer se svakim ponovnim pokretanjem računala brišu izmjene i vraća se početno snimljeno stanje.

Ovaj program može zaštititi operacijske sustave brisanjem izmjena i vraćanjem početnog stanja od slijedećih problema:

- mijenjanja i gubitka postavki,
- lošeg odabira postavki,
- zlonamjernih programa i
- provala u sustav i pada sustava.

Program dolazi u nekoliko inačica koje su razvrstane prema mjestu uporabe:

- Faronics Deep Freeze Standard Edition - namijenjen za kućnu uporabu, jedna licenca
- Faronics Deep Freeze Enterprise Edition - namijenjen za poslovna okruženja, više licenci
- Faronics Deep Freeze Server Edition - namijenjen za upotrebu na poslužiteljima



Slika 7. Prikaz izgleda korisničkog sučelja programa Deep Freeze

Izvor: Faronics

Odmah nakon instalacije, Deep Freeze pohranjuje zatečeno stanje računala i obilježava ga kao normalno. Nakon što je Deep Freeze zabilježio stanje računala, korisnik može dodavati nove programe, mijenjati postavke, izrađivati nove datoteke i pohranjivati ih na računalu, pregledavati web stranice, itd. Međutim, nakon ponovnog pokretanja računala, Deep Freeze će vratiti računalo na stanje koje je zabilježio i tako izbrisati sve u međuvremenu nastale promjene. Ukoliko korisnik želi u postojeće stanje dodati neke nove programe ili postavke, morati će privremeno onesposobiti Deep Freeze i ponovno snimiti stanje koje će program vraćati nakon ponovnog pokretanja računala.

Deep Freeze je najveću primjenu pronašao u edukacijskim ustanovama zbog ograničenja koja je moguće postaviti korisnicima. Također, koristi se i u tvrtkama, političkim organizacijama, javnim pristupnim točkama i knjižnicama jer omogućuje da, usprkos velikom broju korisnika, računala ispravno funkcioniraju.

U programu Deep Freeze, inačicama 5.2 i 5.3, pronađen je sigurnosni propust kojim je lokalnim napadač mogao zaobići zaštitu programa zaporkom i na taj način onesposobiti djelovanje programa Deep Freeze. Prijavljeno je da je propust riješen u Deep Freeze inačici 5.5.

Faronics Deep Freeze koristiti se na operacijskim sustavima:

- Microsoft Windows 95,98, ME, 2000, XP, Vista, 2003 Server Edition,
- Novell SLED Linux i
- Mac OS X od inačice 10.3, pa nadalje.

5.2.1. Prednosti i nedostaci

Jedna od prednosti ovog programa je svakako što korisnici mogu raditi promjene na sustavu (isprobavati nove programe, mijenjati postavke, itd.), bez opasnosti da te promjene ostanu trajno zapisane. Nakon ponovnog pokretanja računala sve promjene jednostavno nestaju. Korisnici zapravo mogu napraviti samo „virtualne“ promjene na sustavu. Ukoliko se želi snimiti neko novo stanje sustava, korisnik mora izvršiti promjene koje želi i potom snimiti trenutačno stanje, te ga označiti kao novo početno stanje.

Jedan od nedostataka je što Deep Freeze ne nadzire postavljanje određenih programa na računalo. Na primjer, ukoliko je korisnički račun označen kao „ograničen“ (*eng. limited*), bez obzira na to da li je tom računu dozvoljeno ili ne postavljati nove programe, neke će instalacijske datoteke pretpostaviti da korisnik nema ovlasti da bi instalirao željeni program i prikazati poruku da mora biti administrator sustava da bi izveo željenu radnju.

Također, nedostatak je što Deep Freeze zapravo štiti korisnika samo nakon ponovnog pokretanja računala. Ukoliko se radi o slučaju da prethodni korisnik nenamjerno pregledavanjem web stranica zarazi računalo zlonamjernim programom i nakon završenog rada samo odjavi svoj račun, slijedeći korisnik će imati problema u radu. Primjerice, ako je računalo zaraženo nekim oblikom zlonamjernog programa koji pamti upisana korisnička imena i zaporke, sigurnost svih korisnika prije ponovnog pokretanja računala biti će ugrožena. Stoga se preporuča prvo ponovno pokrenuti računalo, koristiti antivirusne programe i izbjegavati nepouzdana web odredišta.

Ukoliko se radi o računalu na kojem je postavljeno više operacijskih sustava, postoji opasnost od stvarnog zapisivanja podataka. Ako se drugi operacijski sustav pokrene sa tvrdog diska ili nekog prijenosnog medija, korisnici će imati stvarni pristup podacima i postoji mogućnost da se nanese značajna šteta. Jedini način zaštite od ove situacije jest postavljanje tvrdog diska na kojem je postavljen Deep Freeze kao jedinog s kojeg se može učitavati operacijski sustav.

5.3. Windows SteadyState

Windows SteadyState je alat koji je razvila tvrtka Microsoft. Ovaj alat daje administratorima sustava napredne mogućnosti zaštite računala koje dijeli veći broj korisnika. Zaštita se sastoji od zaštite podataka na tvrdom disku i naprednog rukovođenja korisničkim računima. Koristi se na mjestima poput javnih pristupnih točaka, škola, knjižnica, itd. SteadyState je dostupan svim korisnicima koji koriste legalne verzije 32-bitnih operacijskih sustava Microsoft Windows XP i Vista.

Slika 8. Prikaz izgleda korisničkog sučelja programa Windows SteadyState

Izvor: Microsoft

Instalacijsku datoteku je moguće preuzeti izravno sa službenih stranica potpuno besplatno. Microsoft preporuča korištenje ovog programa na računalima kojima se koristi veći broj korisnika. Također, savjetuje se da SteadyState koriste i korisnici koji imaju samo jedno računalo jer uvijek može doći do nenamjernog nanošenja šteta operacijskom sustavu ili zaraze zlonamjernim programima.

Windows SteadyState administratorima omogućuje napredno rukovođenje korisničkim računima, tj. omogućuje administratorima da odrede koje će ovlasti korisnici imati na računalu. Moguće je postaviti zabrane na mijenjanje, čitanje i pisanje u datoteke, brisanje sistemskih datoteka, instalaciju novih programa, itd. Okruženja u kojima se ovaj program koristi (javne pristupne točke, edukacijske ustanove, itd.) zahtijevaju potpunu slobodu pregledavanja sadržaja, bilo da se radi o Internetu ili podacima na samom računalu. U Windows SteadyState ugrađen je i Windows Disk Protection čije će značajke biti opisane u nastavku.

5.3.1. Windows Disk Protection

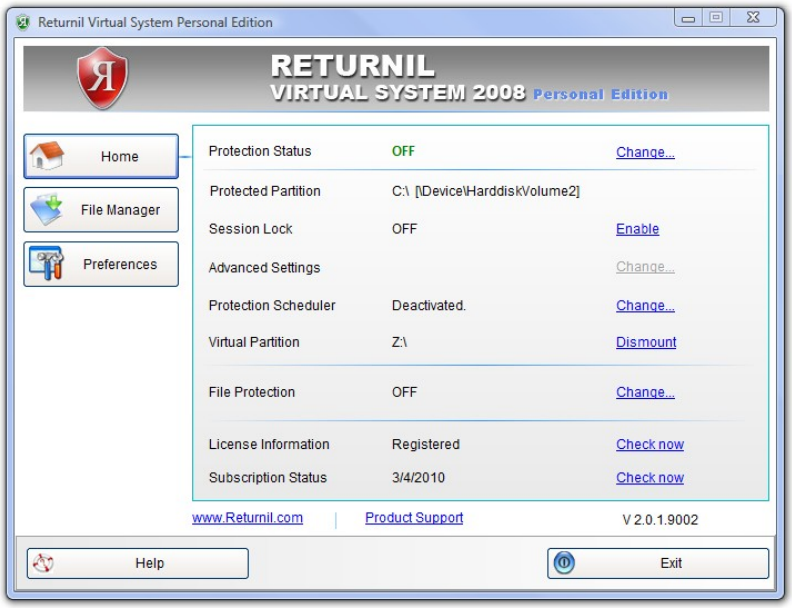
SteadyState posjeduje mogućnost vraćanja računala na neko zadano prethodno stanje, svaki put nakon ponovnog pokretanja ili kada administrator sustava odredi. Kada je Windows Disk Protection uključen, sve napravljene promjene se pohranjuju u priručnu memoriju (*eng. cache*) tvrdog diska. Windows Disk Protection nudi tri načina zaštite.

	Način rada	**Opis**
Uklanjanje svih promjena pri ponovnom pokretanju	Odbacivanje promjena	Kada se operacijski sustav pokrene, sve promjene zapisane u priručnoj memoriji se brišu.
Privremeno zadržavanje promjena	Zadržavanje promjena	Kada se operacijski sustav pokrene, sve promjene zapisane u priručnoj memoriji ostaju. Ovaj se način rada deaktivira nakon nekog vremena i ponovno se prebacuje na odbacivanje promjena.
Trajno zadržavanje svih promjena	Izvršavanje promjena	Kada se operacijski sustav pokrene, sve promjene zapisane u priručnoj memoriji se zapisuju na tvrdi disk. Sve promjene ostaju trajno zapisane.

Tablica 2. Prikaz načina rada Windows Disk Protection

5.4. Returnil Virtual System

Returnil Virtual System je tehnologija virtualizacije koja u potpunosti pohranjuje trenutačno stanje operacijskog sustava ili računala, te stvara virtualni disk na kojem je moguće pohraniti dokumente, datoteke i podatke koristeći *System Protection* alat. Returnil Virtual System radi samo na operacijskim sustavima Microsoft Windows Server 2003, XP i Vista. Za osobnu upotrebu program je moguće besplatno preuzeti i koristiti.



Slika 9. Prikaz izgleda korisničkog sučelja programa Returnil Virtual System

Princip rada programa Returnil Virtual System je vrlo jednostavan. Program korisniku pruža učinkovit i pametan način sprječavanja neželjenih i zlonamjernih promjena na operacijskom sustavu i tvrdom disku. Korisnik sve promjene unosi u virtualnom okruženju, tako da promjene neće biti primijenjene na stvarno računalo. Returnil Virtual System radi, slično Windows SteadyState i Faronics Deep Freeze programima, tako da pohranjuje odabrano stanje računala, te nakon ponovnog pokretanja briše sve promjene i vraća zabilježeno stanje.

Ukoliko korisnik odluči isključiti Virtual Protection, sve promjene napravljene u nastavku će i nakon ponovnog pokretanja biti zapamćene.

Returnil Virtual System korisniku omogućuje:

- uklanjanje posljedice udaljenih napada,
- nestanak virusa, trojanskih konja, crva i spam-a nakon ponovnog pokretanja,
- nametanje postavki i zaštita privatnosti korisnika na Internetu,
- smanjenje istrošenosti tvrdog diska korištenjem memorije,
- smanjenje vremena potrebnog za održavanje,
- smanjenje ili potpuno otklanjanje potrebe za defragmentacijom tvrdog diska,
- otklanjanje posljedica otvaranja e-pošte zaražene zlonamjernim programima,
- uklanjanje tragova na temelju kojih bi se moglo zaključiti što je korisnik radio,
- ubrzavanje pregledavanje Interneta i rad računala te
- jednostavno i lako postavljanje i instalacija.

Prema izvješćima tvrtke Secunia u programu Returnil Virtual System nisu pronađeni sigurnosni propusti.

6. Budućnost „sandbox“ alata

Obzirom na broj i vrste zlonamjernih programa korisnicima se preporuča koristiti neki od sandbox mehanizama. Često se događa da korisnici, zbog nedovoljnog opreza, propusta u programima za zaštitu i/ili pojave novih vrsta zlonamjernih programa ugroze svoje podatke i operacijski sustav. Pojavom novih vrsta zlonamjernih programa korisnici su sve više ugroženi, a teško je reći hoće li konvencionalni načini zaštite poput antivirusnih programa i vatrozida biti dostatno osiguranje i u budućnosti. Sandbox alati se zasnivaju na drugačijem principu zaštite - razdvajanju datoteka operacijskog sustava od datoteka i podataka koji se zapisuju na računalo od strane programa ili korisnika. Kao što je već ranije naglašeno, zbog virtualizacije i odvajanja datoteka operacijskog sustava i rada korisnika, mogućnost da računalo bude zaraženo zlonamjernim programom je svedena na minimum.

Teško je predvidjeti na koji će način sandbox alati napredovati u budućnosti. Postoji mogućnost spajanja sandbox alata i drugih alata za zaštitu u jedan programski paket, što bi svakako pridonijelo povećanju sigurnosti korisnika.

Iako sandbox alati danas nisu u primjeni na svakom računalu, uz činjenicu da je broj sigurnosnih incidenata u stalnom porastu, sve veći broj korisnika će se odlučiti za ovu vrstu zaštite.

Internet je izvor informacija, ali istovremeno i izvor problema. Ustanove koje omogućuju korisnicima da pristupaju podacima putem Interneta morati će primijeniti najmodernije i najkvalitetnije načine zaštite radi obrane od napadača, ali i od korisnika.

Ako razvoj ovih alata bude napredovao kao dosad, velik broj korisnika će se odlučiti na sandbox mehanizam zaštite. Međutim, kako niti jedan element ne pruža potpunu zaštitu, preporuča se koristiti sandbox u kombinaciji sa nekim drugim alatom za zaštitu (antivirusni programi, vatrozidi, anti-spam alati, itd.) kako bi se ukupna razina sigurnosti korisnika povećala. Sandbox može poslužiti kao prva linija zaštite, ali svakako treba imati i implementirano i dodatno osiguranje (antivirus, vatrozid,..) ukoliko se dogodi da neki zlonamjerni program uspije proširiti svoje djelovanje izvan sandboxa.

7. Zaključak

Svaki oblik zaštite podataka i datoteka u računalnom svijetu ima svoje prednosti i nedostatke. Isto vrijedi i za *sandbox* alate. Sandbox alati korisniku pružaju visoku razinu sigurnosti. Čak i ako se dogodi da se zlonamjerni program pojavi unutar sandboxa, ponovnim pokretanjem računala „problem“ nestaje. Iako većina sandbox alata stvara virtualna okruženja u kojima korisnik radi, moguće je trajno pohranjivati podatke i datoteke. Svaki od gore navedenih programa funkcionira drugačije, konačan rezultat uvijek je isti.

Veliki mrežni sustavi, poput onih u tvrtkama (sa mnogo računala i velikim brojem korisnika) napadačima predstavljaju potencijalnu žrtvu. Ukoliko ih se ne zaštiti primjerenom zaštitom, može doći do gubitka vrijednih podataka i otkrivanja povjerljivih informacija. Edukacijske ustanove i ustanove koje pružaju usluge pristupa Internetu svakako trebaju uvrstiti *sandbox* alate među programe koje moraju posjedovati. Velik broj korisnika znači i velik broj grešaka i zaraza (namjernih ili nenamjernih) što znači utrošak velikog broja sati na održavanje postojećih računala.

Još jedna prednost navedenih alata je cijena. Primjerice, kupnjom registracijskog ključa za program Sandboxie korisnik dobiva mogućnost doživotnog korištenja i nadogradnje na novije inačice za jedno plaćanje. Windows SteadyState je program koji je besplatan za preuzimanje i korištenje, jedini uvjet je posjedovanje legalne verzije neke inačice Windows operacijskog sustava. Sigurnost koju korisnik dobiva upotrebom sandbox alata svakako je najveća prednost pred drugim alatima za zaštitu.

8. Reference

[1] Sandbox mehanizam, http://en.wikipedia.org/wiki/Sandbox_(computer_security), veljača 2009.

[2] Upotreba sandbox alata, http://www.kernelthread.com/publications/security/sandboxing.html, lipanj 2004.

[3] Primjena sandbox alata u javnim pristupnim točkama, http://www.microsoft.com/windows/products/winfamily/sharedaccess/seeit/internetcafe.mspx, ožujak 2009.

[4] Primjena sandbox alata u edukacijskim ustanovama, http://www.microsoft.com/windows/products/winfamily/sharedaccess/seeit/classroom.mspx, ožujak 2009.

[5] Sandboxie, http://www.sandboxie.com/, ožujak 2009.

[6] Sandboxie, http://en.wikipedia.org/wiki/Sandboxie, ožujak 2009.

[7] Sandbox zaštita na Internetu, http://pcworld.about.com/od/securit1/Sandbox-Security-Versus-the-Ev.htm, rujan 2008.

[8] Deep Freeze, http://en.wikipedia.org/wiki/Deep_Freeze_(software), ožujak 2009.

[9] Deep Freeze, http://www.faronics.com/html/deepfreeze.asp, ožujak 2009.

[10] Deep Freeze pregled, http://www.macworld.com/article/50113/2006/03/deepfreeze203.html, ožujak 2006.

[11] Windows SteadyState, http://en.wikipedia.org/wiki/Windows_SteadyState, ožujak 2009.

[12] Returnil Virtual System, http://en.wikipedia.org/wiki/Returnil_Virtual_System, ožujak 2009.

[13] Returnil Virtual System, http://www.returnilvirtualsystem.com/rvspersonal.htm, ožujak 2009.