CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Usporedba sigurnosnih rizika poslužitelja Apache i IIS

CCERT-PUBDOC-2008-09-239

+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.

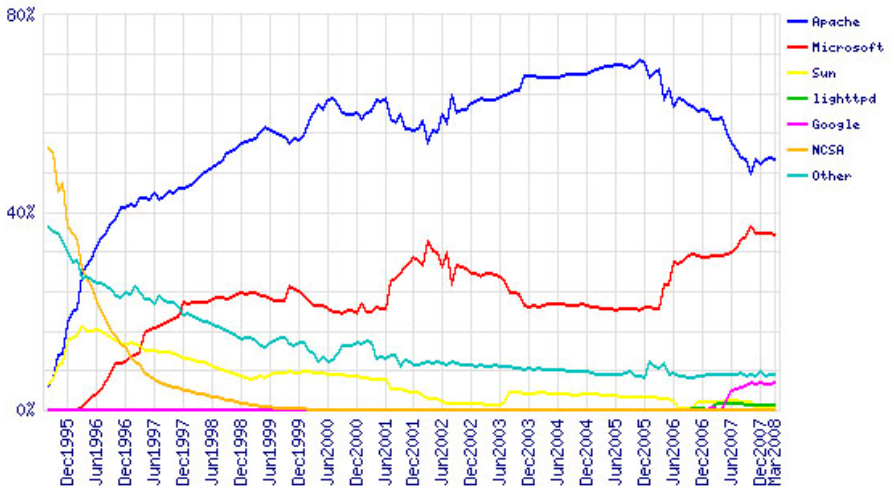
Sadržaj

1. Uvod

Apache i Microsoft Internet Information Server (IIS) su dva danas najzastupljenija web poslužitelja, kojima je funkcija rukovanje web sadržajem. Može se reći da web poslužitelj prima zahtjeve korisnika (od njegovog web klijenta) te na temelju tog zahtjeva i prethodno definiranih pravila oblikuje web stranicu koju dostavlja korisniku (njegovom web pregledniku). Istraživanje provedeno u veljači 2008. godine otkriva da na Internetu postoji oko 160 milijuna web stranica. Usprkos tome što je Microsoft glavni proizvođač programskih rješenja na mnogim poljima, kada su u pitanju web poslužitelji, Apache je uspio napraviti kvalitetan besplatan web poslužitelj koji svojim tehničkim mogućnostima ne zaostaje za IIS-om pa je čest izbor administratora. U prilog toj tvrdnji stoji i činjena da više od polovice Internetskih stranica opslužuje neka od inačica Apache web poslužitelja..

Prema istraživanju kompanije Netcraft, na Internetu je u veljači 2008. godine postojalo 158,209.426 web stranica, što je povećanje od 2,6 milijuna u odnosu na siječanj. Od toga, njih 50,93% koristi Apache poslužitelj, dok 36,20% koristi IIS (slika 1). Dakle, oko 87% svih web stranica poslužuje jedan od ova dva poslužitelja.

Ovi podaci nameću logično pitanje svim administratorima: koji poslužitelj izabrati? Jedna od važnijih stvari prilikom odabira svakako bi trebala biti i razina sigurnosti koju pojedini poslužitelj pruža. Ovaj dokument objašnjava sigurnosne aspekte pojedinog poslužitelja, daje usporedba sigurnosnih rizika ova dva poslužitelja te osnovne savjete kako povećati sigurnost, bilo da se radi o IIS-u ili Apache web poslužitelju.



Slika 1. Zastupljenost web poslužitelja u svijetu (izvor: Netcraft)

2. Povijesni razvoj

2.1. Razvoj Microsoft IIS poslužitelja

Prvi Microsoftov web poslužitelj napravljen je još davne 1995g. kao znanstveni projekt za European Microsoft Windows NT Academic Centre (EMWAC) i bio je distribuiran kao besplatan paket. Kako se EMWAC nije mogao zadovoljavajuće nositi s velikom količinom prometa prema *microsoft.com* web stranici, Microsoft je morao sam razviti vlastiti web poslužitelj – IIS za svoj tadašnji operativni sustav Windows NT 3.51. 1996.g. izlazi Windows NT 4.0 sa novim IIS 2.0, a 1997. izlazi „Service pack 3" zakrpa s podrškom za IIS 3.0. Ova inačica web poslužitelja je po prvi puta imala ugrađenu podršku i za obradu dinamičkih stranica - *Active Server Pages* (ASP). 1998. izlazi IIS inačice 4.0, također kao nadogradnja za Windows NT 4.0 operacijski sustav i donosi unaprijeđeni ASP (inačicu 2.0). U istoj verziji izbačena je podrška za *Gopher* protokol , koja se mogla preuzeti kao zasebni modul. Godine 2000. Microsoft objavljuje operacijski sustav „Windows 2000" s integriranim IIS 5.0 web poslužiteljem, koji sada u sebi ima popriličan niz novih tehnoloških mogućnosti (podrška za ASPI i CGI, modul za obradu XML sadržaja i dr), ali i prvi put značajnija poboljšanja na razini sigurnosti. Jedna od značajnijih novina u inačici 5.0, koju koriste i kasnije inačice IIS-a, jest podrška za nekoliko autentifikacijskih mehanizama:

- *Basic access authentication*
- *Digest access authentication*
- *Integrated Windows Authentication*
- *NET Passport Authentication*

2003. godine na tržištu se pojavljuje operacijski sustav „Windows Server 2003" s podrškom za novu inačicu IIS poslužitelja (6.0), a 2008. godine i „Windows Server 2008/Vista" s IIS 7.0 web poslužiteljem. Najnovija inačica IIS-a (7.0) ističe se po jednoj novoj karakteristici, a to je modularna arhitektura. Za razliku od monolitnog servera koji pogoni sve servise, IIS 7.0 koristi tzv. *core web server engine*. To znači da se moduli za različite funkcije mogu jednostavno dodati po potrebi, a to je velika prednost u očuvanju resursa, ali i sa stajališta sigurnosti jer se koriste samo oni moduli (funkcije) koje su stvarno potrebne. IIS 7.0 inicijalno dolazi s većinom modula koji su korisniku potrebni, a postoji i mogućnost preuzimanja dodatnih modula s javnih Microsoftovih poslužitelja. Moduli koji dolaze u „osnovnoj" instalaciji, a vezani su na sigurnost su:

1. ***HTTP Modules*** – osnovni modul za rukovanje HTTP (eng. Hyper Text Transmission Protocol) paketima
2. ***Security Modules*** –skupina modula koja implementira sigurnosne elemente web poslužitelja. Sadrži module za:
   - autorizaciju korisnika, kao npr: *AnonymousAuthModule*, *BasicAuthModule*, *WindowsAuthModule*),
   - module za rukovanje certifkatima: *CertificateMappingAuthenticationModule*, *DigestAuthModule*, i
   - module za upravljan vezom: *UrlAuthorizationModule* i *RequestFilteringModule*
3. ***Content Modules*** – skupina modula za oblikovanje sadržaja
4. ***Compression Modules*** – moduli za komprimiranje i optimizaciju web sadržaja
5. ***Caching Modules*** – moduli koji se koriste za optimizaciju dohvaćanja sadržaja prema trenutnim zahtjevima klijenata
6. ***Logging and Diagnostics Modules*** – služe za bilježenje aktivnosti web poslužitelja, akcija udaljenih klijenata (prijava, zahtjeva za stranicama, pokušajima autorizacije) te dijagnosticiranju nepravilnosti u radu poslužitelja. U ovu skupinu modula pripadaju:
   - *CustomLoggingModule,*
   - *FailedRequestsTracingModule,*

- *HttpLoggingModule,*
- *RequestMonitorModule i*
- *TracingModule*

Iako se na prvi pogled čini znatno složenija, ova „nova" arhitektura zasnovana na modulima se pokazala kao pozitivan pomak u izradi web poslužitelja. Razlog tome, sa stajališta sigurnosti, je prvenstveno u tome da je lakše definirati, oblikovati i ispitivati manje cjeline (u ovom slučaju module) te poslije te iste povezivati u cjelinu umjesto da se oblikuje jedan „veliki" sustav sa svim uključenim funkcionalnostima.

2.2. Apache kroz povijest

Prvu verziju Apache web poslužitelja izradio je Rober McCool 1995 godine., kada je nakon odlaska iz NCSA (1994.) zajedno s nekoliko istomišljenika (Apache grupe) osmislio i izradio Apache HTTP poslužitelj. Prva javno dostupna inačica - 0.6.2, zasnovana je bila na NCSA httpd 1.3 poslužitelju. Apache je bio prva jača alternativa tadašnjem programskom rješenju: „Netscape Communications Corporation web server". U početku, Apache je bio veliki hit zbog svoje jednostavnosti, efikasnosti i naravno cijene (besplatan, otvorenog koda), što dokazuje činjenica da je do sredine 1996. bio najpopularniji web/ poslužitelj. Popularnost 1.3.x inačice Apache web poslužitelja vidljiva je i danas kada veliki broj administratora kojima nisu neophodne novine „modernih" web poslužitelja radije biraju posljednju 1.3.x inačicu Apache-a nego neki noviji poslužitelj. Razlog tome, uz niske zahtjeve za resursima, je svakako sigurnost, koja je kroz brojne iteracije ispravaka i optimiziranja dovedena na vrlo visoku razinu. Dakle, proizvođač (Apache razvojni tim) novu inačicu objavljuje samo u svrhu uklanjanja sigurnosnih propusta, što je sve rjeđe i rjeđe.

2002. izlazi verzija Apachea 2.0, koja donosi brojne novine, uz činjenicu da je gotovo sav programski kôd ponovno napisan (neki izvori tvrde da je čak 90% kôda izmijenjeno). Od glavnih novina mogu se izdvojiti:

- *Threading* – Apache sad može raditi i na računalima s više procesora i/ili jezgri raspoređujući zadatke na raspoložive resurse. novina za sada je dostupna samo za Linux/Unix okruženja, dok se za Windows inačice to tek očekuje.
- *New Apache API* – mnogi problemi s modulima za prioritete i poretke obavljanja procesa, koje su bile problem u inačicama 1.3, su uklonjeni. Rezultat toga je povećanje efikasnosti i fleksibilnosti poslužitelja
- *IPv6 Support* – ugrađena podrška za novi Internet protokol – inačicu IPv6
- *Better support for non-Unix platforms* – dizajneri i programeri nove inačice Apache web poslužitelja posebnu pažnju posvetili su i Windows okruženju tako da se sada puno bolje koriste naredbe operacijskog sustava (npr. API funkcije) i raspoloživi resursi (pravo na procesor, memorija)
- Simplified configuration – mnoge zbunjujuće naredbe za podešavanje su pojednostavljene

Po pitanju sigurnosni, stručnjaci koji razvijaju Apache, svakom novom inačicom donose neke novitete kako bi unaprijedili sustav zaštite bez narušavanja performansi ili mogućnosti poslužitelja. Tako je u posljednjoj inačici (2.2), objavljenoj u prosincu 2005. godine, uvedeno:

- *Smart Filtering* – sustav za obradu upita, koji sada uzima više parametara u obzir prilikom donošenja odluke o daljnjim akcijama (zahtjev korisnika, varijable okoline, prethodni upiti i sl.)
- *Proxying* – promjene u načinu korištenja resursa prilikom rada kao proxy poslužitelj
- *Caching* – poboljšanja u balansiranju opterećenja pojedinog servisa
- *Authn/Authz* – preraspodjela funkcija među modulima *mod_auth_basic*, *mod_auth_db* i *mod_authn_file* te dodavanje novog modula za rad s simboličkim vezama - *mod_authn_alias*

Trenutna inačica – 2.2.9 ne donosi bitna tehnička poboljšanja u odnosu na inačicu 2.2.0, ali zato donosi niz ispravaka uočenih problema, pa se svakako preporuča njeno korištenje.

3. Tehničke karakteristike

3.1. Okruženje za izvršavanje

Uspoređujući IIS i Apache web poslužitelje može se reći da rade na vrlo različiti način, tako da se može reći da svaki ima svojih prednosti i mana, tj. razloga da ga se odabrati, ili ne. IIS je prvenstveno dizajniran, i dostupan je jedino u inačici, za MS Windows okruženja. S verzijom IIS 6.0 jedina platforma koja je podržana je Windows Server 2003 (2k3). Iako je to ograničenje platforme IIS-u veliki hendikep, istodobno omogućava i brojne prednosti u vidu bolje kooperacije s operativnim sustavom, lakšu administraciju i kontrolu kroz niz standardnih alata samog Windows operacijskog sustava.

U IIS 6.0, kooperacija operativnog sustava i samog web poslužitelja jača je nego ikada prije. Za razliku od prethodnih inačica, komponenta zadužena za primanje zahtjeva od klijenata i ona za obradu pristiglih zahtjeva, sada su dvije razdvojene komponente.

Modul jezgre zadužen za primanje zahtjeva - *Kernel mod* (Http.sys), osluškuje i prihvaća zahtjeve klijenata, postavljajući zahtjeve u jedan ili više redova čekanja. IIS potom obrađuje zahtjeve iz redova po principu FIFS (eng. First In First Served) koristeći barem jedan „radni" proces (proces koji obrađuje pojedini zahtjev) da kontrolira izvršenja pojedinačnih zahtjeva i aplikacija. Na primjer ako poslužitelj dobije pet zahtjeva za nekom web stranicom i ima na raspolaganju 2 procesora, *Kernel mod* je taj koji će prva dva zahtjeva proslijediti procesoru na obadu, a preostale staviti u red čekanja. Kada se neki zahtjev obradi, *Kernel mod* modul će iz reda čekanja aktivirati slijedeći zadatak i predati ga na obradu. Ako se pojavi novi zahtjev, isti će biti postavljen na kraj reda čekanja. *Kernel mod* završava svoj posao kada više ne postoji niti jedan zahtjev koji čeka na obradu.

Ovaj razdvojeni proces omogućuje zahtjevima da budu prihvaćeni i u slučajevima kada procesi za obradu zahtjeva nisu aktivni i također omogućuje finiju kontrolu radnih procesa koji upravljaju zahtjevima. Na taj način administrator (ili poslužitelj automatski) mogu ponovno iskoristiti zahtjeve u slučaju aplikacijskih grešaka za koje bi prethodno bilo potrebno gašenje i ponovno pokretanje IIS servisa ili, u iznimnim slučajevima, ponovno pokretanje cijelog servera.

Glavni potez za Apache 2.0 je bilo ponovno pisanje dijelova koda iz prethodnih verzija. Među brojnim promjenama, poslužitelj je sada dostupan izravno na različitim platformama, uključujući (Windows, Linux/Unix). Redizajn poslužitelja omogućio je optimizaciju korištenja posebnosti pojedinog operacijskog sustava, a sve u svrhu boljeg iskorištavanja raspoloživih resursa.

Središnji dio sustava je *Apache Portable Runtime* (APR), koji omogućuje Apache jezgri da radi više - manje na svakom sustavu koji ima prevoditelj programskog jezika C. Skupina multiprocesnih modula (MPMs) pruža potporu za stvarno prihvaćanje i obradu pojedinog zahtjeva. Pod Unix-zasnovanim operacijskim sustavima, to može biti tradicionalni model zasnovan na procesima i podprocesima (eng. forked model) ili novi model koji koristi dretve za paralelnu obradu (eng. threaded model). Na operacijskom sustavu „Windows" se također koristi model temeljen na dretvama, koji je u nekim značajkama sličan modelu kojeg koriste radni procesi IIS-a. Tablični prikaz tih značajki vidljiv je u tablici 1.

Značajke	IIS	Apache
Independent Request Handler	Da	Da (djelomično)
Multiple Process Request Handlers	Da	Da
Thread Support	Da	Da (ovisno o OS-u)

Tablica 1. Mogućnosti web poslužitelja za obradu razdvojenih procesa

3.2. Dinamičke komponente

Primarno dinamično okružje za razvoj dinamičkih komponenti je Active Server Pages (ASP). Ovo je općenito naziv za rješenje koje omogućuje da se programski kod ugradi u HTML stranice. Te *ASP stranice* poslužitelj raščlanjuje prije nego se pošalju klijentu kao HTML. ASP sustav omogućava programerima da rade u velikom broju različitih programskih jezika, uključujući i Visual Basic, VBScript, JavaScript, Java i C / C++, uz ostale „open source" alternative, kao što su Perl i Python. Osim toga, IIS i dalje nudi podršku tradicionalnim CGI metodama kao i, uz vlastite načine filtriranja, sustava izvršavanja u obliku ISAPI filtara.

Apache je dizajniran za rad sa širokim rasponom jezika, bilo putem CGI modula ili pomoću dinamičkih modula koji izravno povezuju prevoditelj (eng. language interpreter) u Apache okružje. Ovo značajno ubrzava izvršenje dinamičkih komponenata za jezike kao što su PHP, Perl ili Python.

Oba sustava podržavaju Java Server Pages (JSP) model pa je moguće seliti JSP aplikacije između dvije platforme sa samo nekoliko (manjih) izmjena. Ostali jezici se također, s više ili manje „dodatnog posla", mogu preoblikovati za rad alternativnim poslužiteljem (npr. ASP stranice za IIS u PHP stranice za Apache). Čak se i sama ASP tehnologija može primijeniti na Unix/Linux sustavima kroz komponentu *„ChilliSoft ASP"*, ili Apache module: *ASP* i *modmono*.

Jedan element koji trenutno ne može biti emuliran pod Unix/Linux okruženjima je *Microsoft.NET environment IIS*. Ovaj paket koristi IIS na poslužitelju „Windows Server 2003" kao element integracije web poslužitelja s *.NET Frameworkom,* razvojnim okruženjem za samostalne aplikacije. Pregled dostupnih komponenti za izradu dinamičkog sadržaja dan je u tablici 2.

Značajke	IIS	Apache
ASP	Da	Da, s Chilisoft, Apache:ASP ili modmono
CGI	Da	Da
Perl	Da	Da
Python	Da	Da
PHP	Da	Da
JSP	Da	Da
.NET Integrated	Da	Ne

Tablica 2. Popis podržanih dinamičkih komponenti

3.3. Sigurnosni elementi poslužitelja

Jedan od najvažnijih elemenata web poslužitelja, jest svakako i način zaštite, kako podataka na samom poslužitelju, tako i informacija koje se razmjenjuju između klijenta i poslužitelja. IIS iskorištava pogodnosti koje proizlaze iz bliske integracije s operativnim sustavom na način da isti korisnik i/ili grupa zadužena za konfiguraciju samog web poslužitelja je istovremeno i legitimni korisnik/grupa operacijskog sustava koji ima potrebne ovlasti (definirane kao i za bilo kojeg drugog lokalnog korisnika na poslužitelju). To također smanjuje dodatnu administraciju na samo jedan sustav i omogućuje administratoru da automatski dozvoli ulaz korisnicima putem intraneta, uz pretpostavku da su već dokazali autentičnost unutar Windows okruženja.

Zato jer se isti sustav koristi kroz cijeli OS, to se može također iskoristiti i za definiranje prava pristupa različitim komponentama datotečnog sustava na računalu (ili domeni) na kojem se IIS poslužitelj i nalazi. Na primjer, kada se korisnik prijavi na nekoj web lokaciji, njegova sposobnost da ulazi u direktorije unutar te lokacije je definirana samo jednim skupom (eng. set) korisničke i grupne strukture.

S druge strane, sigurnost i administracija Apache poslužitelja nije toliko dobro integrirana s korištenim operacijskim sustavom. Iako postoje moduli i slični dodaci koji podržavaju niz različitih autorizacijskih izvora, uključujući i Microsoftov Active Directory, Unix *passwd* datoteke ili LDAP poslužitelj, nedostaje jednostavnost i transparentnost u podešavanju i administriranju takvih sustava. Zbog toga je Apache web poslužitelj relativno izoliran od sustava na kojem se nalazi. Primjer ove izoliranosti može se vidjeti u slučaju kada se podesi sustav autorizacije na temelju *passwd* datoteke operacijskog sustava Linux/Unix. Uspješnom autorizacijom sa svojim korisničkim računom klijent dobiva prava pristupa, ali za daljnje rukovanje podacima ima prava koja su dodijeljena poslužitelju (a ne njemu).

U pogledu sigurnih transakcija, oba sustava (Apache 2.2 i IIS6) imaju podršku za SSL enkripcijskom tehnologijom i mogu se koristiti s IPSec implementacijom te IPv6 protokolom. Usporedni pregled autentifikacijskih metoda prikazan je u slijedećoj tablici:

Značajke	IIS	Apache
Secure Login	Da	Da
SSL	Da	Da
Basic Authentication	Da	Da
Digest Authentication	Da	Da
LDAP Authentication	Da	Da
Active Directory Authentication	Da	Da, samo s modulima drugih proizvođača
Passport Authentication	Da	Ne

Tablica 3. Popis sigurnosnih tehnika za autentifikaciju

3.4. Performanse

Procjena performansi je uvijek teška, jer ma koliko su sustavi međusobno slični , samo minimalna promjena u njihovoj konfiguraciji može imati dramatični učinak na rezultate mjerenja performansi. Moguće je odabrati pobjednika na temelju „čiste" instalacije oba sustava na istom sklopovlju, ali to onda nije stvarni prikaz pravih performansi sustava na tom području. Naime, i Apache i IIS sustav, mogu se konfigurirati da budu vrlo efikasni ili nedovoljno efikasni i time iskriviti rezultate usporedbe.

Umjesto toga, bolje je pogledati mogućnosti svakog sustava. IIS ima brojne značajke osmišljene za poboljšanje performansi. Model izvršavanja koji se temelji na korištenju radnih proces ima bolje performanse na višeprocesorskim strojevima, kao i ASP i ISAPI ekstenzije koje omogućuju aplikacijama da se izvršavaju izravno iz procesa koji rukuje zahtjevima. Upravljački program modula jezgre (Http.sys) IIS poslužitelja sposoban je posluživati stranice izravno iz priručne memorije (eng. cache) ili vanjske memorije za statičke i dinamičke komponente, eliminirajući potrebu za slanjem zahtjeva radnim procesima. IIS automatski sprema stranice generirane iz dinamičkih elemenata kako bi ubrzao odziv.

Apache ima slične pogodnosti. Većinu informacija moguće je spremiti u pričuvnu memoriju, a alatima kao mod_php, mod_perl omogućiti izvršenje dinamičkih i predefiniranih (eng. template) stranica gotovo jednako brzo kao i statičnih stranica. Kao što to rade ASP i ISAPI filtri pod IIS-om, tako ovi moduli učinkovito stavljaju prevoditelj izravno u Apache-ovo okruženje, isključujući potrebu za izvođenje vanjske aplikacije, čime se uvelike poboljšavaju ukupne performanse sustava.

Tablica 4 donosi usporedni prikaz funkcionalnosti za poboljšavanje performansi IIS i Apache web poslužitelja.

Značajke	IIS	Apache
In-Memory Cache	Da	Da
On Disk Cache	Da	Da, s mod_file_cache dodatkom
Built-In Execution support	Da, s odgovarajućim ISAPI filterom	Da, s odgovarajućim modulima
Cached Execution support	Da, s ASP/ASP.NET podrškom	Da, s mod_perl dodatkom i dr.

Tablica 4. Popis značajki za poboljšavanje izvođenja dinamičkih stranica

3.5. Administracija

Ova dva sustava razlikuju se radikalno kada je u pitanju administriranje. Osnovni način administriranja Apache poslužitelja je kroz jednostavnu tekstualnu konfiguracijsku datoteku. Također, razvijen je veliki broj alata koji kroz grafičko sučelje omogućavaju promjene konfiguracijskih parametara poslužitelja. Ovaj način podešavanja poslužitelja koristit će manje iskusni administratori, dok će administratori s dobrim poznavanjem poslužitelja (ili Linux/Unix okruženja) preferirati izravnu izmjenu konfiguracijske datoteke – *http.conf*. Ovdje je važno napomenuti da je moguće naići na inačicu Apache poslužitelja čija je središnja konfiguracijska datoteka *apache.conf*, te sve češće da, uz tu osnovnu datoteku, sustav koristi još nekolicinu konfiguracijskih datoteka za definiranje pojedinih cjelina (popisane su u osnovnoj konfiguracijskoj datoteci). Početnicima se može preporučiti alat *Apache Management Console*, jednostavan i intuitivan besplatni alat za konfiguraciju Apache-a. Nakon bilo koje promjene (izravno u konfiguracijskoj datoteci ili putem sučelja) potrebno je ponovno pokrenuti poslužitelj.

IIS s druge strane nudi niz različitih sučelja za izmjenu konfiguracije sustava. Iako je temeljni oblik prvenstveno pohranjen u XML datoteci, IIS sustav omogućuje administratoru promjenu konfiguracije i dok sustav radi. Za daljinsku podršku (eng. remote support,) Windows Server 2003 također uključuje telnet poslužitelj, koji sadrži modul *XML Metabase*, pomoću kojeg je omogućeno korištenje različitih alata iz komandne linije za daljinsko administriranje poslužitelja. Pri tome treba pripaziti, jer se telnet protokolom poruke razmjenjuju u nekriptiranom obliku pa ako postoji mogućnost presretanja paketa napadač može doći do osjetljivih informacija o sustavu, ili čak i modificirati podatke koji se razmjenjuju.

Različita uređivačka sučelja uključuju GUI sučelja putem *Microsoft Management Console*, administracija sustava bazirana na web aplikacijama, skup alata iz komandne linije za dodavanje, ažuriranje, i konfiguriranje različitih komponenti. Administratori mogu uređivati i samu XML datoteku na „živo“ (dok sustav radi), a spremljene promjene automatski se reflektiraju u IIS sustavu bez potrebe za ponovnim pokretanjem poslužitelja. XML format olakšava izvoz i uvoz konfiguracijskih informacija između poslužitelja za dijeljenje konfiguracijskih detalja.

Značajke	IIS	Apache
Text File Configuration	Da, kroz XML metabase	Da
Command Line Management	Da	Djelomično
Remote CLI	Da	Da
Web-Based Management	Da	Da
GUI-Based Management	Da	Da, rješenja „trećih“ strana

Tablica 5. Načini pristupa podešavanja web poslužitelja

3.6. Pouzdanost poslužitelja

IIS 6.0 nudi opširnu administraciju i kontrolu sustava nad radnim procesima koji kontroliraju najviše zahtjeva. Da bi se pouzdanost dodatno poboljšala, IIS također može kategorizirati aplikacije, dajući im vlastite dijelove memorije i prostor za izvršavanje ili koristiti prostor koji se dijeli s ostalim aplikacijama. To znači da kada neka aplikacija uzrokuje problem, ona nestaje unutar radnog procesa i ne utječe na bilo koju drugu aplikaciju. Dakle, prekida se samo aplikacija koja se ne može nastaviti izvršavati, dok sve ostale aplikacije i sami IIS poslužitelj rade neometano.

Apache automatski obrađuje mnogo procesa, ali memorijska i aplikacijska izolacija je još uvijek jedan problem koji nije učinkovito riješen ili pokriven. Apache izbjegava neke od problema tako da automatski ponovno koristi komponente, s tim da jezgra sustava i dalje ostaje u funkciji čak i u slučaju ozbiljnog kvara na jednoj od komponenti. Međutim, unatoč promjenama u kôdu Apache poslužitelja zamijećen je nemali broj slučajeva u kojima je jedino rješenje ponovno pokretanja Apache poslužitelja.

Jedan primjer je konfiguracija samog Apache sustava. Za web lokaciju koja radi na IIS baziranom poslužitelju, većina ažuriranja i poboljšanja neće imati nikakvog učinka na pristup korisnika, jer promjene u konfiguraciji su izvršene dok je sustav bio aktivan. Za Apache je međutim potrebno ponovno pokretanje sustava (eng. restart) da bi promijene imale učinka.

Značajke	IIS	Apache
Process/Thread Management	Da	Da
Isolated Applications	Da	Djelomično
Live Configuration Editing	Da	Ne

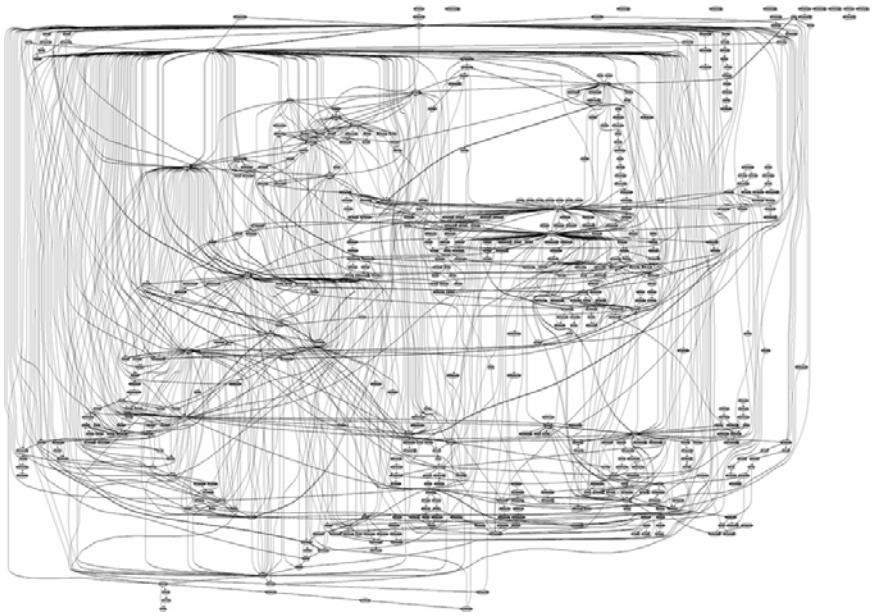
Tablica 6. Pouzdanost u radu i aktivacija izmjena unutar sustava

4. Utjecaj operacijskog sustava na sigurnost

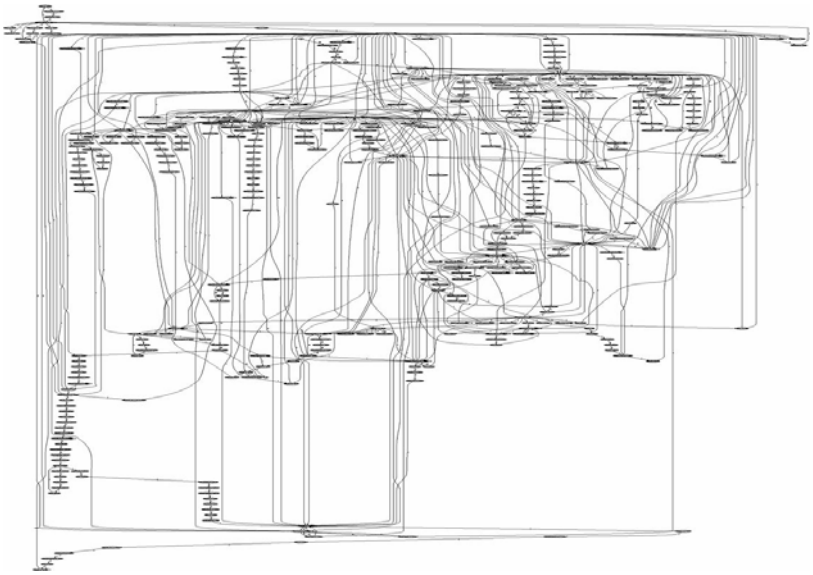
Kako su web poslužitelji u većini slučajeva javno izloženi na Internetu, njihova sigurnost je vrlo bitna za sigurnost cjelokupnog računalnog sustava. Tim Google-ovih stručnjaka zaduženih za sigurnost je krajem 2007. godine radio veliko ispitivanje stanja sigurnosti web poslužitelja diljem svijeta. Ovo ispitivanje uključivalo je više od 80 milijuna domena iz gotovo svih zemalja svijeta, a rezultati su pokazali da je više od 70.000 domena bilo zaraženo nekom vrstom malicioznog programa. Posebno je iznenadila činjenica da su u nekim državama uglavnom pronađene ranjive inačice Apache web poslužitelja, a u drugim prevladavale ranjive inačice IIS-a. Primjera radi, u Njemačkoj su skoro svi maliciozni programi bili prisutni na Apache poslužiteljima, u SAD-u 75% ranjivih poslužitelja koriste Apache, dok je recimo u Južnoj Koreji 75% ranjivih web poslužitelja neka od inačica IIS-a. Potpuna suprotnost Njemačke je Kina, gdje su gotovo svi uočeni propusti pronađeni na web stranicama koje poslužuje IIS. Kada se pogleda globalna statistika, može se zaključiti da su Apache i IIS podjednako (ne)sigurni web poslužitelji.

Veliki utjecaj na sigurnost pojedinog programskog rješenja, a samim time i web poslužitelja, značajno ovisi o složenosti kako pojedinih dijelova samog programa tako i o složenosti sistemskih poziva koje koristi proučavani program. Usporedbe radi, u jednom ZDNet-ovom članku objavljena su dva dijagrama Sana Security-a (Slika 2.). Pravilnija struktura procesa u Linux okruženju nije slučajna već je to rezultat višegodišnjeg razmišljanja, oblikovanja, optimiziranja i prilagođavanja jezgre operacijskog sustava koja seže od prvih inačica operacijskih sustava Unix do danas. Dobar dizajn operacijskog sustava osigurava jasnu podjelu jezgre i aplikacijskog sloja, čime je upravljanje kompleksnim sustavima pojednostavljeno. Kod jednostavnijih i preglednih veza između jezgre i aplikacijskog sloja moguće je uočiti i ukloniti zavisnosti među procesima čime se znatno podiže sigurnost cijelog sustava.

Upravo zbog te složene strukture sistemskih poziva, Microsoftovi stručnjaci su prisiljeni raditi zakrpe na način da ugrađuju iznimke koje „premošćuju“ problem umjesto da mijenjaju dio programskog koda u kojem je propust izvorno uočen. Rezultat toga je stalno povećanje izvornog programskog koda, a to je uvijek potencijalna opasnost za nove propuste.



Slika 2. Dijagram razvoja procesa na windows platformi



Slika 2. Dijagram razvoja procesa na linux platformi

5. Savjeti za administratore

Kao i kod svih drugih programskih rješenja, pravilno podešavanje web poslužitelja, nadgledanje rada sustava, redovito osvježavanje zakrpama i pravilno postavljanje ovlasti pristupa (korisnicima dati samo nužne ovlasti koje su im potrebne da odrade svoj posao) neophodni su elementi za siguran i zaštićen web poslužitelj. U nastavku poglavlja slijede osnovni savjeti administratorima web poslužitelja, neovisno radi li se o IIS ili Apache programskom rješenju.

5.1. Primjena sigurnosnih zakrpi

Zlonamjerni korisnici najčešće iskorištavaju otkrivene, opisane i dokumentirane sigurnosne propuste u pojedinom web poslužitelju. Kako i Microsoft i Apache redovito objavljuju sigurnosne zakrpe kojima se uklanjaju uočeni propusti, svim administratorima savjetuje se da zakrpu primijene na poslužitelj kojeg administriraju u što kraćem vremenu od njenog izdavanja . Također, potrebno je pratiti i web portale koji javljaju uočene propuste i u slučajevima kada zakrpe ne postoje (CERT, SANS i sl.). Ukoliko se uoče propusti visokog rizika (otkrivanje osjetljivih informacija, pokretanje programskog koda, preuzimanje ovlasti drugih korisnika) za koje trenutno ne postoje zakrpe, administratori bi trebali razmotriti mogućnost da „žrtvuju“ dio funkcionalnosti kako bi dodatno zaštitili ranjivi poslužitelj. Primjer toga može biti da se pristup web poslužitelju ograniči samo na računala u lokalnoj mreži.

5.2. Ovlasti nad datotečnim sustavom

Kako se web poslužitelji najčešće pokreću s povećanim ovlastima, od iznimne je važnosti pravilno podesiti sustav tako da se dohvaćanje i pohranjivanje podataka na poslužitelj obavlja sa smanjenim ovlastima nego što ima sam poslužitelj (tj. korisnik koji ga je pokrenuo). Pri tome je poželjno definirati samo jednu lokaciju na poslužitelju gdje se ti podaci mogu nalaziti, a web poslužitelju eksplicitno zabraniti pristup ostalim dijelovima sustava. Uz čitanje i pisanje, posebnu pažnju potrebno je posvetiti i definiranju ovlasti s kojima se pokreću izvršne datoteke na poslužitelju.

5.3. CGI skripte

Prvo i osnovno pravilo prilikom korištenja CGI skripti je povjerenje u autora koji piše te skripte. Bilo da su namjere programera zle, ili nije niti svjestan problema koje njegovi programi rade, uključivanje loše oblikovanih skripti narušava sigurnost cijelog sustava. Naime, kako se te skripte pokreću izravno na operacijskom sustavu s ovlastima korisnika koji je pokrenuo ranjivi poslužitelj, njihovim iskorištavanjem napadač može zaobići sva ostala ograničenja postavljena na razini web poslužitelja. Ukoliko je moguće, savjetuje se izbjegavati korištenje CGI skripti, a ako to nije moguće onda treba detaljno ispitati skripte prije njihove primjene u sustavu. Povećavanje sigurnosti u korištenju CGI skripti u određenoj mjeri moguće je napraviti tako da se skripte smiju pokrenuti samo u određenim direktorijima računala.

5.4. Zaštita postavki poslužitelja

Postavke poslužitelja, jednom kada ih administrator postavi i isproba, u principu, ne bi trebalo mijenjati. Zbog toga, a u svrhu zaštite, preporuča se ukidanje prava izmjene konfiguracijskih datoteka svim korisnicima. Dodatno se savjetuje izračunavanje *hash* vrijednosti svih konfiguracijskih datoteka nakon što se podešavanje završi, te kasnije redovito kontroliranje da se originalna i nova *hash* vrijednost ne razlikuju. U slučaju da se pojavi razlika, administrator treba posumnjati na ilegalne izmjene postavki poslužitelja te shodno tome i reagirati.

5.5. Praćenje dnevnika (log datoteka)

Posljednja, ali ne i manje bitna aktivnost, u očuvanju sigurnosti web poslužitelja jest redovito praćenje dnevnika (log datoteka) koje sustav prijavljuje (oba poslužitelja su oblikovana tako da svaki zahtjev, akciju i pogrešku bilježe u posebne – log datoteke). Iz informacija zapisanih u log datotekama iskusni administrator može vidjeti pokušaje napada na sigurnost, njihovu učestalost pa čak i tko je napad pokušao izvesti (tj. IP adresu s koje je napad izvršen). Log datoteke treba pratiti dnevno te pri uočavanju bilo kakve nepravilnosti odmah reagirati.

6. Sigurnosni mehanizmi zaštite

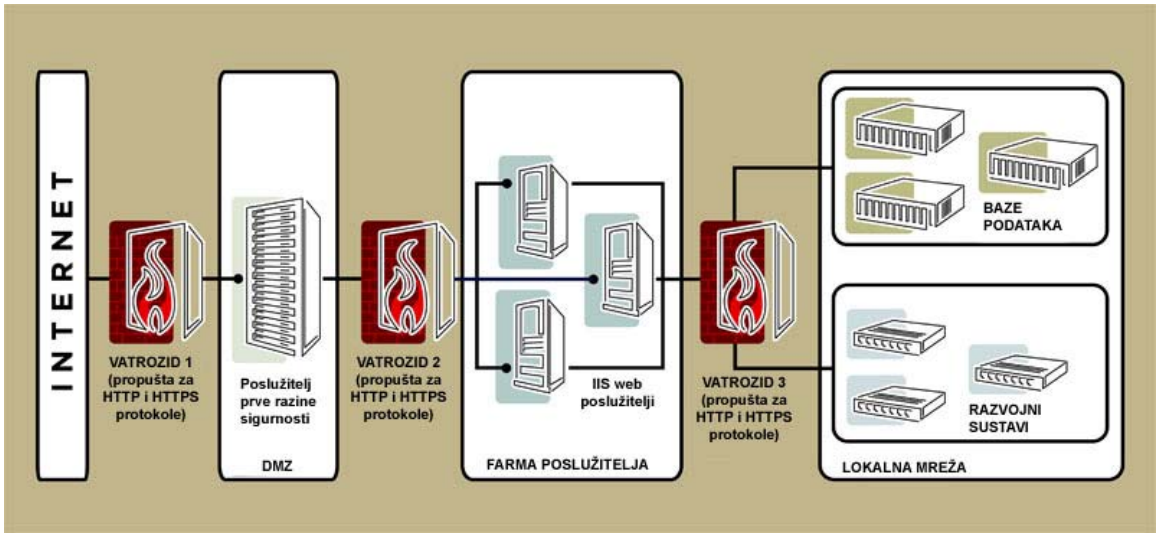
Objavljivanjem dodatka za IIS 6.0 web poslužitelj – *Microsoft IIS Lockdown,* sigurnost Microsoftovog poslužitelja je značajno podignuta. Ovaj alat omogućava gašenje nepotrebnih opcija web poslužitelja smanjujući time broj potencijalnih sigurnosnih prijetnji. U prilog navedenoj tvrdnji ide i istraživanje iz 2005. godine koje je provela tvrtka Secunia, a čiji rezultati pokazuju drastično smanjenje broja sigurnosnih propusta na računalima na kojima se koristi *IIS Lockdown*.

S druge strane, istraživanja koja je iznio SANS institut o najkritičnijim ranjivostima za Windows i Unix/Linux platformu, stavljaju IIS na prvo mjesto po broju ranjivosti u zadnjih par godina. Ove podatke treba uzeti s rezervom, jer je vrlo vjerojatno da je ranjivost pojedinog ispitivanog sustava uvjetovana nepravilnom konfiguracijom i/ili održavanjem, a ne propustima u samom alatu. Najbolji primjer je Windows 2000 Server koji se distribuira s inicijalno instaliranim i pokrenutim IIS poslužiteljem, iako nema potrebe za tim web poslužiteljem. Mnogi administratori su postali svjesni ove činjenice, kao i rizika koju donosi, tek tijekom navale poznatog „Nimda" i „Code Red-a" virusa.

Na starijim sustavima više, od sigurnosti samog web poslužitelja, zabrinjavaju pogrešno oblikovane aplikacije koje koriste i/ili aktiviraju neke IIS servise bez znanja korisnika ili administratora sustava. Tako su, na primjer, mnoge trgovine otkrile da je IIS aktivin tek kad ih je napao Nimda ili Code Red i iskoristio njihov Web poslužitelj.

6.1. Model dvostrukih poslužitelja

Kako je prilično teško zaštiti web poslužitelj od izravnog napada, neki administratori sustava primijenili su metodu „dvostrukih poslužitelja". Naime, radi se o tome da se stavi npr. Apache web poslužitelj ispred farme IIS poslužitelja (slika 3). Ovaj „ulazni" poslužitelj ima implementirani 1. nivo sigurnosne zaštite, a zatim se dodatni elementi postavljaju na pojedini aplikacijski poslužitelj. Ovu ideju osmislio je M. Brewer, CEO u tvrtci Covalent Tehnology. Kao i svaka tehnika zaštite i ova ima svoje prednosti i mane pa postoje i različita stajališta je li bolja ili lošija od tradicionalne metode. U prilog ovakvom načinu zaštite svakako ide postojanje dvije razine zaštite, dok glavni nedostatak predstavlja problem administracije većeg broja, i to različitih, poslužitelja.



Slika 3. Model dvostrukih poslužitelja prema M.Brewer-u

6.2. Vatrozid i proxy poslužitelj

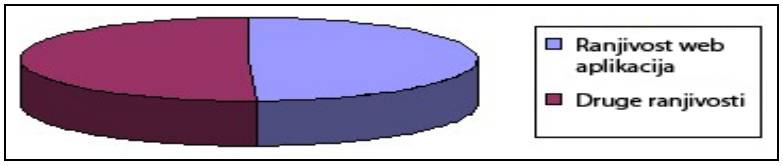
U zaštiti bilo kojeg računalnog resursa s pristupom Internetu, pa tako i web poslužitelju, potrebno je koristiti vatrozide. Vatrozid je uređaj ili programsko rješenje koje se postavlja između Interneta i unutarnje (zaštićene) mreže, a koristi se za filtriranje ulaznog i izlaznog prometa. Kada se govori o vatrozidu za web poslužitelje osnovna podešavanja su:

- Ograničiti dolazni promet samo na priključnice (eng. port) na kojima osluškuje web poslužitelj (tipično 80 i 443)
- Zabraniti izlazni promet na sistemskim priključnicama (priključnice od 0 do 1024)

Slična metoda je korištenje proxy poslužitelja. Ovom metodom od udaljenog korisnika se „skriva" stvarna adresa poslužitelja na način da se sav promet odvija preko nekog trećeg poslužitelja – proxy-a. Na taj način napadaču je onemogućen izravan napad na web poslužitelj, tj. prije nego i započne, napad mora na neke druge načine saznati koje je to računalo na kojem se nalazi web poslužitelj.

6.3. Zaštita web aplikacija

I male i velike organizacije podjednako koriste Web zasnivane aplikacije kao što su „Content Management Systems" (CMS) i Wiki sustavi, razni portali, forumi (phpForum, phpBB) i druge. Veliki broj organizacija također razvija i održava svoje vlastite web aplikacije potrebne za poslovanje. Svaki tjedan se prijavi stotine ranjivosti koje su aktivno iskorištavane i u komercijalnim i web aplikacijama i onima otvorenog koda. Potrebno je imati na umu da su osobno izgrađene web aplikacije također napadnute i izrabljivane, iako se ranjivosti tih programa ne prijavljuje i ne prati u javnim bazama podataka o ranjivosti. Istraživanja su također pokazala da je gotovo polovina ranjivosti web poslužitelja izravna posljedica pogrešno oblikovane web aplikacije. Administratorima se preporuča korištenje dostupnih programa za ispitivanje web aplikacija (npr. Nikto, Hellstorm, Acunetis i sl.) kako bi se na vrijeme uočili, i uklonili propusti.



Slika 4. Zastupljenost ranjivosti aplikacija na web poslužitelju
(od listopada 2006 do studenog 2007)

6.4. Rizici vanjskih sustava

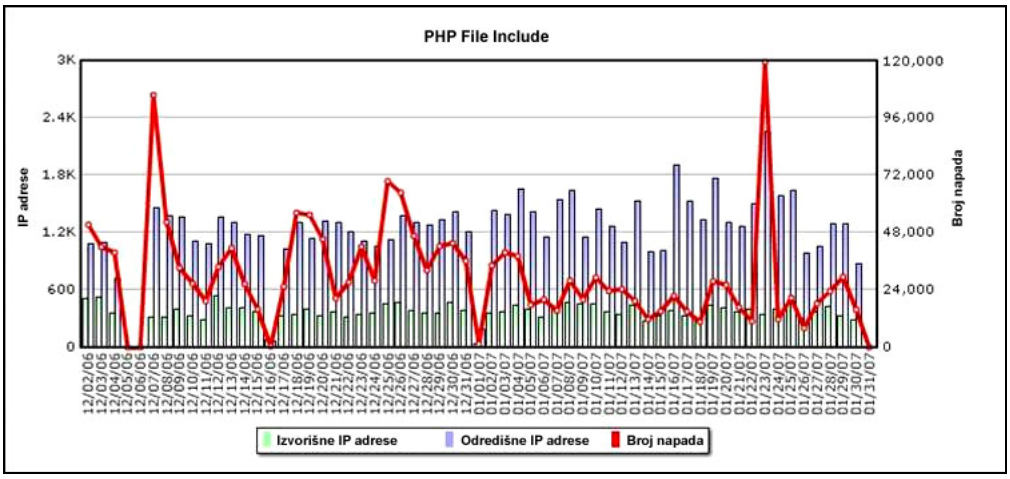
Da bi se zaštitili podaci na nekom poslužitelju nije se dovoljno koncentrirati samo na sigurnost web poslužitelja, već je potrebno provjeriti sigurnost ostalih sustava koje web poslužitelj koristi. Posebnu pažnju treba posvetiti i sistemskim pozivima prema bazama podataka ili PHP prevodiocu te obradi ulaznih nizova koje poslužitelj prima od udaljenog (često i nepoznatog) klijenta. U nastavku će biti prikazani neki od osnovnih tipova napada koji iskorištavaju ovakve ranjivosti.

6.4.1. Uključivanje udaljene PHP datoteke (eng. PHP inclusion)

PHP je najrašireniji skriptni jezik koji se koristi za izgradnju dinamičkih web sadržaja te je stoga česta meta napada. PHP prevodilac za Apache dolazi s tako postavljenim inicijalnim postavkama da omogućava funkcijama za rad s datotečnim sustavom učitavanje konfiguracijskih parametra s bilo koje lokacije na Internetu (opcija: *allow_url_fopen*). Kada PHP skripte, koje su dio neke web stranice, udaljenom korisniku omoguće izmjenu datoteka na operacijskom sustavu, moguć je scenarij uključivanja proizvoljnih malicioznih datoteka s bilo koje lokacije na Internetu. To u konačnici napadaču može omogućiti:

- Izvršavanje proizvoljnog programskog koda
- Uključivanje proizvoljnih PHP skripti u rad ranjivog poslužitelja
- Preuzimanje većih ovlasti na Windows računalima

Koliko je ovaj propust čest može se vidjeti na slijedećem grafikonu:



Slika 5. Broj „PHP File Include“ napada zabilježenih prema testnim poslužiteljima kompanije TippingPoint IPS

6.4.2. Podmetanje SQL nizova

Napad podmetanjem SQL nizova (eng. SQL injection) je sve češći tip napada na web poslužitelje. Radi se o metodi slanja posebno oblikovanog URL niza, koji će zbog pogrešnog načina na koji ga aplikacija obrađuje, omogućiti napadaču uvid i izmjenu podataka u bazi za koje napadač inače nema ovlasti. Važno je naglasiti da je napad izravna posljedica lošeg oblikovanja web aplikacija, a ne nedostataka samih web poslužitelja. Kao zaštitu, korisnicima se preporuča ugradnja podsustava za obradu ulaznih nizova prije korištenja i/ili obrade.

6.4.3. Cross-Site Scripting (XSS)

Još jedan tip napada koji uzima sve više maha je „Cross-Site Scripting". Radi se o tehnici kada se raznim elementima prevare, bilo u obliku malicioznog programa na klijentskom računalu, bilo izmjenom podataka na web poslužitelju, korisnika preusmjerava na maliciozni poslužitelj bez njegovog znanja. Kod ovog tipa napada, jednaku važnost kao i zaštiti poslužitelja potrebno je posvetiti i zaštiti klijentskih računala. Dodatno je potrebno korisnika poučiti kako da provjeri pripada li stranica kojoj pristupa stvarno navedenom vlasniku (URL adresa, certifikati i sl.)

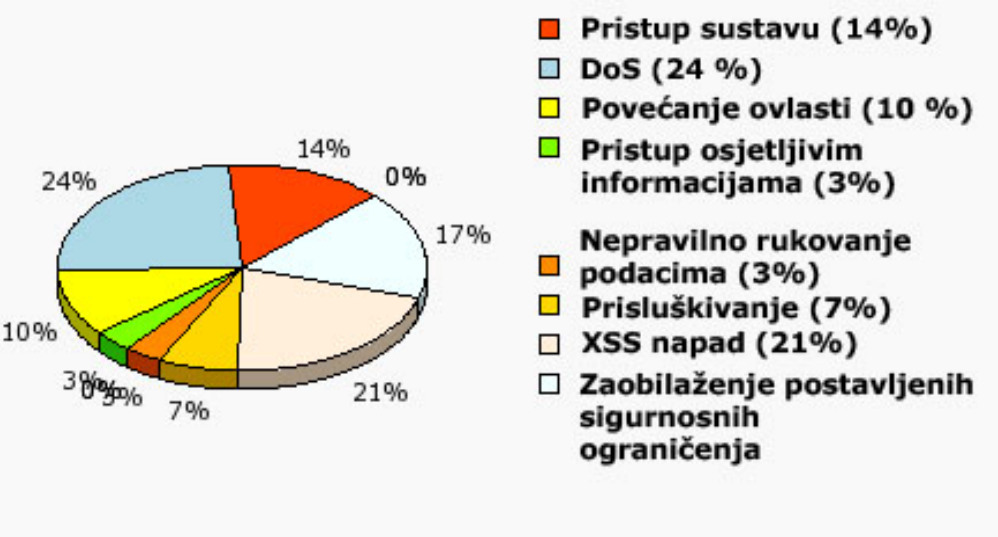
7. Pregled sigurnosnih propusta

Neki od osnovnih parametara za ocjenjivanje sigurnosti pojedinog web poslužitelja svakako su: broj prijavljenih sigurnosnih propusta, dostupnost zakrpa, vrijeme potrebno za objavljivanje zakrpe od trenutka otkrivanja propusta te broj prijavljenih provala u sami sustav. U nastavku je prikazana statistika za pojedini poslužitelj u 2008. godini.

7.1. Sigurnosni propusti Apache web poslužitelja

7.1.1. Apache inačica 1.3.x

U razdoblju od 2003. do 2008. godine za ovu inačicu Apache web poslužitelja uočeno je 18 sigurnosnih propusta. Od svih propusta, samo jedan je visokog stupnja rizika, dok su ostali srednjeg (28%) ili niskog stupnja. Sve propuste visokog i srednjeg stupnja proizvođač je u potpunosti ispravio, dok je samo jedan propust niskog stupnja riješen djelomično. Udjeli pojedinog tipa propusta prikazani su u nastavku:



Slika 6. Podjela propusta Apache 1.3.x poslužitelja prema vrsti napada

Izvor: Secunia Security Team

Važno je napomenuti da tijekom 2008. godine nije zabilježen niti jedan propust u ovoj inačici Apache-a pa on predstavlja idealno rješenje za web stranice gdje je sigurnost iznimno važna (toliko važna da se žrtvuju i neka profinjenija tehnološka rješenja novijih inačica).

7.1.2. Apache 2.0.x

U posljednjih pet godina (razdoblje od 2003. do 2008. godine), koliko Secunia-ini stručnjaci prate otkrivanje propusta, za 2.0.x inačice Apache poslužitelja otkriveno je ukupno 37 sigurnosnih propusta. Od tih 37 propusta samo jedan je visokog stupnja rizika (3%), dok su ostali srednjeg ili nižeg stupnja. Iako za 4 propusta nisu objavljene zakrpe, kako se radi o propustima jako niskog prioriteta (Not Critical), može se reći da je sve potrebne zakrpe proizvođač i izdao. Propusti su uglavnom omogućavali DoS (41%) i XXS (16%) napade te neovlašteni pristup datotekama na poslužitelju (12%). Detaljniju analizu ove inačice Apache-a zainteresirani mogu pronaći na Secunia-inim službenim stranicama:

http://secunia.com/advisories/product/73/?task=statistics

Što se tiče propusta u 2008. godini, za ovu inačicu poslužitelja pronađena su samo dva sigurnosna propusta, i to nižeg stupnja rizika. Jedan propust je proizvođač ispravio, dok su za drugi napravljene djelomične zakrpe (eng. partial fix).

7.1.3. Apache 2.2.x

Kako Apache 2.2x koristi praktično istu jezgru programa (dodani su samo novi moduli), broj propusta je sličnog karaktera kao i kod 2.0.x inačice. Radi se o 38 propusta u posljednjih pet godina (2003. – 2008. godina), s naglaskom na propuste vezane uz DoS i XSS (oba s udjelom od po 38%), te pristupom osjetljivim informacijama sustava i datotekama na poslužitelju (u oba slučaja radi se o 3 propusta). U 2008. godini su uočena jednaka 2 propusta kao i kod inačica 2.0.x s jednakim rezultatom.

7.2. Sigurnosni propusti IIS web poslužitelja

7.2.1. IIS 5.x

U posljednjih 5 godina za programski paket IIS inačica 5.x detektirano je 12 sigurnosnih propusta, a od njih samo jedan u 2008. godini. Od tih uočenih propusta jedan je iznimno visokog rizika (udaljeni napadač može dobiti administratorske ovlasti), njih četiri je visokog rizika, a ostatak (7 propusta) je niskog ili vrlo niskog rizika. Većina uklonio je proizvođač pojedinog poslužitelja, a važno je napomenuti kako ne postoji niti jedan prijavljeni propust za kojeg ne postoje zakrpe. Bez obzira na ove službene podatke, kako se IIS inačice 5.X više ne razvija, a uskoro se očekuje i prestanak davanja podrške od strane Microsofta, administratorima se savjetuje korištenje novije inačice.

7.2.2. IIS 6

Kod trenutno najraširenije inačice Microsoft IIS web poslužitelja, 6. generacije, od 2003. do danas je primijećeno i službeno objavljeno pet sigurnosnih propusta. Sve propuste je proizvođač ispravio (80%) ili napravio modifikacije u sustavu da se propusti ne mogu iskoristiti (20%). Na slici 7 vidljiv je odnos broja propusta pojedine razine.

Slika 7. Podjela propusta IIS 6 poslužitelja prema razini sigurnosnog rizika

Izvor: Secunia Security Team

Uočeni propusti napadaču su omogućavali:

- Neovlašteni pristup sustavu – 2 slučaja
- DoS napad – 2 slučaja
- Pristup osjetljivim i/ili zaštićeni sistemskim podacima – 1 slučaj

Što se tiče 2008. godine, uočena su „samo“ dva propusta, za koje je Microsoft izdao odgovarajuće zakrpe. U oba slučaja radi se o propustima visoke razine, a napadaču su omogućavale neovlašteni pristup sustavu i neovlašteno dobivanje većih ovlasti te DoS napad.

7.2.3. IIS 7.x

Jedini za sada službeno prijavljeni i opisani propust kod IIS web poslužitelja najnovije inačice datira iz veljače 2008. godine. Radi se o propustu niske razine (CVE-2008-0074) koji lokalnom korisniku omogućava stjecanje povećanih ovlasti na nedozvoljeni način. Microsoft je izdao zakrpu koja ispravlja ovaj uočeni propust.

7.3. Izdavanje zakrpa za uočene propuste

Kao što vidljivo, oba proizvođača su ažurna što se tiče izdavanja zakrpi za uočene propuste (pogotovo onih koji značajnije mogu narušiti sigurnost sustava i podataka). Iskustvo govori da je u objavljivanju zakrpa, ili barem privremenih rješenja, brži Apache. Za njega vrijedi pravilo da se zakrpe izdaju 2 – 3 dana nakon otkrivanje propusta, dok je kod Microsofta moguć slučaj čekanja i do tjedan dana jer je njegova politika da zakrpe za sve svoje proizvode izdaje jednom tjedno.

Što se tiče većeg broja propusta kod Apache-a nego kod IIS-a, to je i za očekivati jer napadači, a i stručnjaci koji rade na razvoju sigurnosti, imaju dostupan izvorni kod Apache web poslužitelja, dok je on u slučaju IISa poslovna tajna. Moglo bi se čak reći i da je Apache „bolje ispitan“ te zbog toga i sigurniji poslužitelj.

8. Zaključak

Bez obzira na niz razlika između ova dva sustava, izbor između njih svodi se uglavnom na potrebe i zahtjeve organizacije, te u manjoj mjeri, osobne potrebe i sklonosti administratora koji ga koristite. Na primjer, mnogi programeri vole raditi u Perlu na Unix zasnovanom Apache okolišu, iako su Perl i Apache dostupni i na Windows platformi, a Perl je i podržan odvojeno pod IIS. Tim korisnicima „prirodnije" je izabrati Apache, a zbog dobrog poznavanja Linux/Unix okruženja, i kod tog odabira neće pogriješiti. Drugi pak korisnici, koji su bolje upoznati s Microsoftovim rješenjima, izabrat će IIS, i opet ispravno postupiti. Njima je prirodnija filozofija administracije Windows sustava, a to je jako bitno u redovitom praćenju i održavanju sustava.

Što se tiče samih uočenih propusta i načinjenih zakrpi, naklonost velikog dijela administratora lagano je na strani Apache-a. Osnovni razlog leži u tome što su u slučaju Apache web poslužitelja svi detalji dostupni (otvorenost koda), dok je u slučaju IISa (kao i ostalih MS proizvoda) sve prekriveno velom tajne. Zna se samo da je propust pronađen, što se može napraviti iskorištavanjem istog, i da je Microsoft objavio zakrpe. Ništa više. I broj dosad ispravljenih propusta u najraširenijim inačicama Apache-a (2.0.x) i IIS-a (6), 37 u odnosu na 6, daje naslutiti da je Apache bolje ispitani poslužitelj po pitanju sigurnosti.

Važno je napomenuti i financijski aspekt, i ne zanemariti troškove implementacije i održavanja komercijalnih poslužitelja. Apache je besplatan i može se instalirati i na operacijski sustav Windows i na besplatne operativne sisteme kao što je Linux. IIS je dostupan samo kao dio operacijskih sustava Windows Server 2003 i 2008 čija cijena nije baš malena.

Bez obzira na prikazane pozitivne i negativne strane pojedinog poslužitelja, najkvalitetnija zaštita za oba sustava svodi se na redovito ažuriranje sustava najnovijim zakrpama, pravilnim podešavanjima sustava te redovitim praćenjem rada sustava (log datoteke, opterećenost resursa i sl.).

9. Reference

[1] IT world, http://www.itworld.com/070907websecurity, travanj 2008.

[2] RedMond Mag, http://redmondmag.com/features/article.asp?EditorialsID=471&a=#findit, svibanj 2008.

[3] ServerWatch, http://www.serverwatch.com/tutorials/article.php/10825_3074841_2, rujan 2008.

[4] SANS,http://www.sans.org/top20/?utm_source=web-sans&utm_medium=text-ad&utm_content=Free_Resources_Homepage_top20_free_rsrcs_homepage&utm_campaign=Top_20&ref=27974#s1, svibanj 2008.

[5] Trial by fire, http://garywiz.typepad.com/trial_by_fire/2006/05/, travanj 2006.

[6] SlideShare, http://www.slideshare.net/george.james/web-servers-architecture-and-security/, rujan 2008.

[7] Secunia, http://secunia.com/advisories/, rujan 2008.

[8] Apache, http://httpd.apache.org/docs/2.2/new_features_2_0.html, rujan 2008.

[9] Wikipedia, http://en.wikipedia.org/wiki/Security_through_obscurity, rujan 2008.

[10] Learn IIS, http://learn.iis.net/page.aspx/121/iis-7-modules-overview/#Reference, svibanj 2008