

# Računalna sigurnost na Internetu i lokalnim mrežama III



Verzija 1.0  
Dinko Korunić, 2006.

# Računalna sigurnost na Internetu i lokalnim mrežama III



Verzija 1.0  
Dinko Korunić, 2006.

# O predavaču

- višegodišnji vanjski suradnik časopisa Mrež@, kolumna "Digitalna radionica - Linux"
- 11+ godina iskustva u Unix/Linux i hibridnim Windows višekorisničkim mrežama: dizajnu, postavljanju, održavanju, sigurnosti
- vanjski suradnik SRCE-a i CARNet-a: forenzike provaljenih sustava, predavač, podrška sistem-inženjerima, itd.
- sigurnosni ekspert pri InfoMAR d.o.o.

# Tijekom prezentacije

- **ako što nije jasno - pitajte i tražite objašnjenje!**
- **ako što nije točno - ispravite!**
- **diskusija je poželjna i produktivna - očekuje se vaša suradnja!**
- **podijelimo** zajedno vlastita iskustva i mišljenja - predavanje nije statični, fiksni materijal

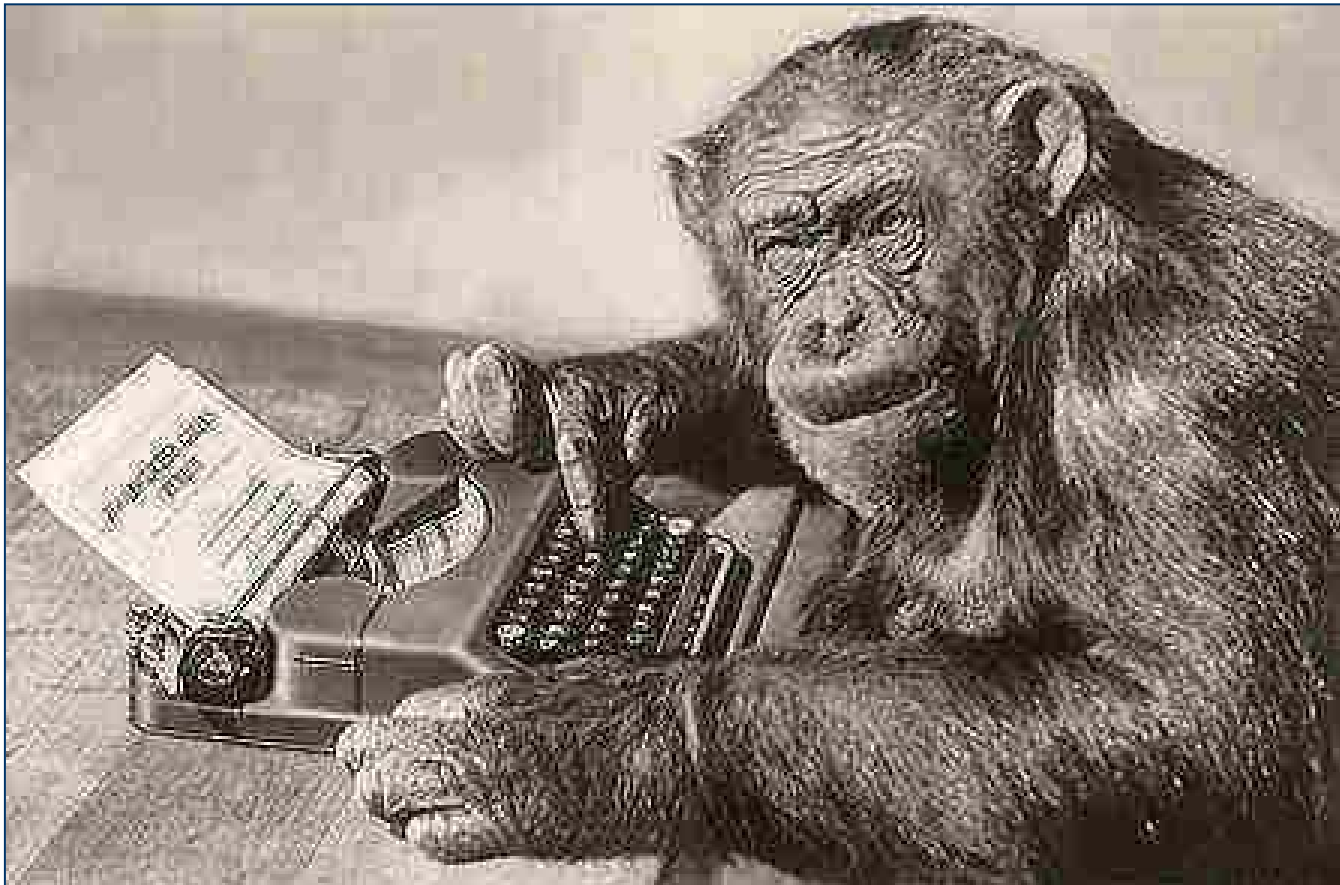
# Sadržaj

- Uvod
- PCI DSS
- Internet danas
- Top 20 problema
- Sigurnost iznutra
- Lozinke
- Skype
- Mobilni uređaji
- Virusi
- Spyware
- Spam
- HIPS
- 19 smrtonosnih grešaka
- Web application firewall
- Reverzni posrednik
- Zapisnici
- Zaključak
- Diskusija

# Sigurnosni ekspert na djelu



# Programer Web aplikacija na djelu



# Mi smo sigurni. Sigurno. Vjerujte.

- CardSystems Solutions, Tucson, Arizona
- kartično procesiranje za MasterCard, Visa, AmericanExpress, Discover
- 22 svibnja 2005 - više od 40 milijuna kreditnih kartica (i **identiteta!**) ukradeno
- podaci:
  - spremljeni **lokalno** unatoč MasterCard preporukama
  - **nekriptirane** datoteke izvan LAN-a na **nezakrpanom** poslužitelju (**poznata** rupa)

# Mi smo sigurni. Sigurno. Vjerujte.

- **uzrok:**
  - manjak **sigurnosnih** provjera
  - nepridravanje **pravila**
- **rezultat:**
  - milijunski **gubici**
  - **nepovjerenje** i gubitak klijenata
  - **tužba**
  - raspad kompanije (ubrzo kupljeni...)

# Sigurnost? Može i još lošije.

- Guidance Software
- proizvod EnCase: FBI, U.S. Secret Service, FBI, New York Police, itd.
- samoprozvani vodeći stručnjaci
- 07 prosinca 2005 - otkrili krađu kreditnih kartice... **14 dana nakon** incidenta!
- nisu javili direktno/hitno vlasnicima, već su slali obavijest **običnom postom**

# Sigurnost? Može i još lošije.

- baze nisu bile **enkriptirane**
- čuvali **CVV** brojeve unatoč Visa/MasterCard standardima
- **nepridržavanje** - \$500000 po prekršaju
- i opet ukradeni **identiteti** (adresa, telefon, ime i prezime, CVV, vrijeme isteka kartice)
- navodno: nisu znali da su podaci **spremljeni** negdje na **duže** vrijeme!

# Sigurnost? Može i još lošije.

- *Regular mail was the **quickest way** to contact customers, according to Colbert. "We **don't have e-mail addresses** for everybody, and we found that their **physical addresses are more permanent** than their e-mail addresses," he said.*  
CNET News.com

# Što napraviti?

- *"Protecting customer data is much **less expensive** than dealing with a security **breach** in which records are **exposed** and potentially **misused**."*  
Gartner, Inc.

# Što napraviti?

- **enkripcija** podataka, gdje god bili: baze, datotečni sustavi, operacijski sustav, itd.
- minimalna intruzivnost, maksimalna granularnost u **odvajanju privilegija**
- enterprise **key management**, Crypto API, **enkripcija** sa kraja na kraj
- **zaštita aplikacija: politika i procedure** u razvoju i testiranju "sigurnih" aplikacija i dodatnih aplikacija za **zaštitu** od napada

# Što napraviti?

- upravljanje **enkripcijom** i ključevima
  - enterprise key management, Crypto API
- **redundancija, raznolikost** rješenja, nema **SPOF**, **minimalne** privilegije...
- kvalitetan IT sustav:
  - niz **aktivnih barijera** koje upravljaju **različitim sigurnosnim aspektima**
  - nužno **dobro skaliranje** i moguće **proširivanje**

# Što napraviti?

- **sigurnosna politika...**
- **kvalitetan IT sustav:**
  - kriptografska identifikacija **otporna** na napade,
  - autentikacija, autorizacija, centralna administracija korisnika, delegacija kontrole, upravljanje sjednicama, nema SPOF, minimalne privilegije, povjerljivost podataka, integritet podataka, nemogućnost odricanja, nemogućnost lažnog predstavljanja, trenutno suspendiranje/brisanje dozvola

# PCI DSS

- odgovor na **uočene** sigurnosne probleme
- **CISP** 2001, inkorporiran 2004. u PCI DSS
- siječanj 2005: Payment Card Industry Data Security Standard
- **ukratko:**
  - izgraditi i održavati **sigurnu mrežu**
  - **čuvati podatke** (samo neke!) o kartičnim korisnicima u **tranzitu** i onim koji **miruju**
  - održavati program **upravljanja ranjivostima**

# PCI DSS

- implementirati **snažne mjere kontrole** pristupa te **provjeravati ih redovito**
- redovito **nadzirati** mrežu i sve sustave
- imati definiranu informatičku **sigurnosnu politiku**
- imati audit **zapisnike** svih navedenih aktivnosti
- 7 rujan 2006 - PCI Data Security Standard v1.1
- sigurnosni pregled - **trenutak** u vremenu
- održavanje sigurnosti - **24/7/365**

# Internet danas

- AvantGarde test 2005
- Windows: SBS 2003, XP SP1, XP SP1 + ZoneAlarm, XP SP2
- Mac OS X 10.3.5 i Linspire Linux
- dva tjedna na otvorenoj mreži na Internetu
- dva tjedna - ustanovljeno **305955** napada
- Windows XP SP1 provaljen unutar prve **4 minute**

# Internet danas

- neprovaljeni:
  - Linux, OS X, XP SP2 i XP SP1 + ZA
  - svaki individualno primili unutar 0.50% od ukupnih 306 tisuća napada
- BBC Jacques Erasmus:
  - Windows XP: bez XP vatrozida, bez antivirusa
  - **8 sekundi** do inficiranja Sasserom
  - **3 crva u 25 minuta**
  - potpuno zaraženo računalo, širi viruse, itd.
  - teško/nemoguće raditi - 100% CPU

# SANS 20 - Windows sustavi

- **Windows servisi:**
  - MSDTC, COM+ Service, Print Spooler Service, Plug and Play Service, Server Message Block Service, Exchange SMTP Service, Message Queuing Service, License Logging Service, WINS Service, NNTP Service, NetDDE Service, Task Scheduler
- **Web preglednici:**
  - Internet Explorer i Mozilla Firefox ranjivosti
- **Office i Outlook Express**

# SANS 20 - Windows sustavi

- **biblioteke** (udaljeno izvršavanje koda):
  - Windows Graphics Rendering Engine, Microsoft DirectShow, Microsoft Color Management Module, HTML Help, Web View, Windows Shell, Windows Hyperlink Object Library, PNG Image Processing, Cursor and Icon Processing, Windows Compressed Folder, JPEG Processing
- **tipične** konfiguracije:
  - slabe lozinke na računalima ili dijeljenom sadržaju, standardne/pogodive lozinke...

# SANS 20 - mrežni uređaji

- **Cisco IOS:**
  - DoS: BGP Processing, SNMP Processing, OSPF Processing
  - izvršavanje koda: IPv6 Processing, Firewall Authentication Proxy
- **Cisco non-IOS:**
  - izvršavanje koda: CallManager, Collaboration Server
  - hardkodiran u/p: Wireless LAN Solution Engine
  - hardkodiran SNMP community: IP/VC

# SANS 20 - mrežni uređaji

- Cisco ostalo:
  - PROTOS IPSec Test Suite
- ostalo:
  - JunOS - niz rupa
  - CheckPoint VPN-1/FireWall-1 - također
  - Symantec Firewall/VPN Appliance i Symantec Gateway Security

# SANS 20 - softver

- ranjivi **backup** softver:
  - Symantec Veritas NetBackup/Backup Exec
  - Symantec Veritas Storage Exec
  - Computer Associates BrightStor ARCserve
  - EMC Legato Networker
  - Sun StorEdge Enterprise Backup Software (Solstice Backup Software)
  - Arkeia Network Backup Software
  - BakBone Netvault Backup Software

# SANS 20 - softver

- ranjivi **AV** softver:
  - Symantec, F-secure, Trend Micro, McAfee, Computer Associates, ClamAV, Sophos
- **PHP** ranjivosti:
  - prosječno 50% Web poslužitelja koristi PHP
  - ranjiv interpreter, uključivanje udaljenih datoteka, udaljeno izvršavanje koda, umetanje SQL naredbi, XML-RPC ranjivosti i sl.
- **baze** podataka:
  - stotine za Oracle, 6 kritičnijih za MySQL

# SANS 20 - softver

- **DNS:**

- ozbiljne opasnosti za poslužitelje i klijente: trovanje spremnika, preuzimanje sjednica, MitM redirekcija, itd.
- Symantec Gateway Security, Symantec Enterprise Firewall, Symantec VelociRaptor
- DNSmasq DNS Server
- Windows NT/2000 DNS serveri (isporučena konfiguracija)
- Windows DNS forwarder prema ranjivom BIND ili Windows DNS poslužitelju

# SANS 20 - softver

- **multimedijalni** programi:
  - Windows: Windows Media Player, RealPlayer, Apple Quicktime, Winamp, iTunes
  - Mac OS: RealPlayer, Quicktime, iTunes
  - Linux/Unix: RealPlayer, Helix Player
- **razne ostale** ranjivosti:
  - Computer Associates License Manager, Novell eDirectory iMonitor and ZENWorks, Sun Java, HP Radia Management Software, Snort, RSA SecurID Web Agent, itd.

# Sigurnost kompanije - iznutra

- većina sigurnosnih problema - krađa **iznutra**
- PricewaterhouseCoopers 2005 survey "The Global State of Information Security"
  - **33%** informatičkih napada od **internih** zaposlenika - dakle iznutra
  - **28%** inf. napada od **otpuštenih** zaposlenika i partnera
  - **>50%** napada uzrokovano **neovlaštenom** upotrebom privilegija od strane **lokalnih** zaposlenika

# Strogo kontrolirani vlakovi

- sigurnost **iznutra**, pa tek onda **izvana**
- većina najviše proširenih i najozloglašnijih spywarea proširena kroz Internet "**sharing**" mehanizme (IM, IRC, P2P), lokalne diskove, razne kolekcije
- spyware
  - pokazatelj **korisničkog** ponašanja, a ne **greške** u sustavu zaštite
  - spyware se bitno rjeđe dešava kroz systemske nepatchirane rupe

# Strogo kontrolirani vlakovi

- filtriranje na graničnim točkama (vatrozid, usmjernik) nije dovoljno:
  - potencijalno **osjetljivi** podaci dolaze i odlaze sa individualnih računala (IM, VoIP, P2P, VPN)
  - **potpuna** kontrola izrazito **teška**, ako ne i nemoguća
- potrebno je riješiti problem direktno sa korisnikom:
  - sigurnosna **politika**, **edukacija** - a tek onda tehničke **restrikcije**

# Strogo kontrolirani vlakovi

- standardno - desktop lockdown:
  - **GPO** (Group Policy Objects) ili neko treće rješenje - zabrana instaliranja, **bijele** i **crne** liste
  - nije dovoljno! aplikacije je moguće pokretati, instalirati, izvršavati čak i **bez dozvola** (secdrv.sys)
- korisnici često instaliraju spyware jer misle da je **nešto drugo**:
  - P2P, IM, IRC, smileyji, desktop teme, screensaver, problem e-mail forwarduša...

# Strogo kontrolirani vlakovi

- P2P:
  - ranjivosti u samim **aplikacijama** (klijent ili poslužitelj)
  - virusi/crvi/trojanci/itd. se **šire** kroz same dijeljene direktorije i datoteke
  - visoke šanse **infekcije** i **preuzimanja** kontrole
  - **dijeljeni direktoriji** uglavnom nemaju zaštite
  - podložnost **tužbi** (kršenje zakona...)
  - **opterećenje** mrežnim prometom, konekcijama, saturacija usmjerivača/vatrozida

# Strogo kontrolirani vlakovi

- IM:
  - ranjivosti u samim **aplikacijama**, npr. AIM i MSN
  - mogućnost **prijenosa** datoteka - mnogo IM crva u optičaju koristi rečene slabosti
  - moguće **curenje** informacija
  - crvi i roboti koriste IRC za **sinkronizaciju** i komunikaciju s napadačem
  - moguć VoIP ili posredovano prenošenje tuđih poruka - neopravdana **potrošnja** ukupne propusnosti

# Strogo kontrolirani vlakovi

- ostali problemi:
  - **VPN** i **anonimizirajući** softver: Hamachi, Tor, Privoxy, Vidalia
  - **bežične** mreže - standardno se koristi slaba enkripcija ili se uopće ne enkriptira; prevelik doseg pristupnih uređaja; neispravno konfigurirani klijentski uređaji
  - odsutnost **802.1x** autorizacije u mreži, **MAC** pristupnih listi
  - nužan **inventar** uređaja, računala, softvera...

# Čemer sistemskih lozinki

- Cyber-Ark 2006 Enterprise Privileged Password Survey
- tipični IT enterprise:
  - **13%** **router** admin lozinki se ne mijenja
  - **21%** **lokalnih** admin lozinki na **radnim** stanicama se ne mijenja
  - **13%** **serverskih** admin lozinki se ne mijenja
  - **42%** lozinki za **softver/aplikacije** se ne mijenja!
- koristite li **generatore kvalitetnih** lozinki?

# Skype - zlo zatvorenog koda

- VoIP - izrazito popularan, "besplatan"
- Skype - mješavina IM i VoIP rješenja
- defacto **nametnuti** standard
- radi routing **tuđih** poruka (**supernode**)
- **enkripcija** poruka, **closed** source, nat/firewall **traversal**
  - skriva se, prolazi vatrozide
  - teška **kontrola sadržaja**
  - većina vatrozida **neuspješna** u filtriranju

# Skype - zlo zatvorenog koda

- problemi:
  - prijenos **neprovjerenih** datoteka (malware)
  - curenje potencijalno **osjetljivih** informacija
  - u prošlosti bilo **sigurnosnih** problema (npr. prijenos proizvoljnih datoteka sa napadnutog računala)
  - jedini proizvod takvog tipa - pogodna **meta**
  - **pad** produktivnosti
- rješenje?
  - politika i **BlueCoat ProxySG**

# Mobilni uređaji - podaci na dlanu

- pitanje je **čijem** dlanu?
  - manjak **vatrozida**, slabo korištenje **antivirusnog** softvera, manjak snažne **enkripcije**, niz problema oko **wireless** supplicanta
- istraživanja 2005te:
  - **22%** vlasnika PDA uređaja izgubilo svoje uređaje
  - **81%** tih uređaja: **bez** PIN-a i **ikakve zaštite** (enkripcija)
  - **37%** tih uređaja sa **osjetljivim informacijama** (bankovni podaci, računi, lozinke, itd.)

# Mobilni uređaji - podaci na dlanu

- Windows Mobile problemi
  - **skrivene** aplikacije - nevidljive za običnog korisnika (usporedi TaskManager, msconfig, regedit, masa besplatnih programa)
  - masa **loše napisanih** programa koje osjetljive lozinke spremaju u **registry** bez enkripcije ili sa vlastitim (lošim) metodama **enkripcije**
  - supplicant/Windows Mobile greške: **cleartext** WEP lozinke u registryju
  - **ActiveSync sigurnosni** problemi (password box na PC-ju)

# Mobilni uređaji - podaci na dlanu

- standardno upaljeni **BT** i **IR**...
- standardno upaljeni **TCP** i **UDP servisi** viška
- treba koristiti Win Crypto API
- kod drugih proizvođača također nije sjajna situacija:
  - Symbian, XDA, itd.
- dolazi era **mobilnih virusa**:
  - Skullz, Phage, Liberty, Vapor, Cabir, Mosquito...
- stapanje **PDA** i **mobitela**... i kamere

# Digitalni virusi - evolucija vrsta

- CSI/FBI Computer Crime survey 2004:
  - **99%** kompanija koristi AV
  - **78%** napadnute virusima, crvima i trojancima!
- PricewaterhouseCoopers 2005 survey:
  - za UK Department of Trade and Industry
  - **100%** velikih kompanija **koristi** AV
  - **76%** koristi **antispyware** rješenja
  - **43%** ih je bilo zaraženo **malwareom** kroz 2005tu godinu

# Digitalni virusi - evolucija vrsta

- klasifikacija:
  - boot sektor, e-mail, logička bomba, makro, XSS virus, trojanski konj, crv
- način replikacije:
  - nerezidentni, rezidentni, ugnježdajući
- izbjegavanje detekcije:
  - izbjegavanje mogućih mamaca, nevidljivi (stealth), samomodifikacije (jednostavne, enkripcija, polimorfizam, metamorfizam)

# Digitalni virusi - evolucija vrsta

- "novi" problemi: BMP exploit/virus, Java virusi, itd.
- preko **100 tisuća** poznatih inačica
- krajem 2005: cca **117% godišnjeg** rasta
- širenje **P2P** i **piratski** sadržaj - pogoduje širenju virusa
- izrazito brza evolucija, brojne inačice na temelju osnovnog virusa...

# Digitalni virusi - evolucija vrsta

- načini pretraživanja:
  - **uzorci**: najjednostavniji, najjeftiniji i najslabijeg uspjeha na novim tipovima virusa
  - **heuristika**: **statička** heuristika ograničenog uspjeha, **dinamička** heuristika relativno komplicirana
  - **bihevioralna analiza**: potencijalno vrlo korisna, nužna interakcija sa korisnikom; analiza sekvenci ponašanja

# Digitalni virusi - evolucija vrsta

- proaktivne (heuristika i bihevioralna analiza) metode:
  - **nemoćne** pred sasvim **novim** virusima koji koriste alternativne pristupe problemu
  - znanja proaktivnih metoda su bazirana **isključivo** na **postojećim** virusima
  - u prosjeku detektiraju **manje** od **70%** ItW (In the Wild) virusa, sto ostavlja npr. **2700** nedetektiranih virusa na **9000** ItW virusa
  - najviše vidljivo na 1-2 mjeseca nenadograđivanim AV-ovima (**manjak novih** potpisa/uzoraka)

# Digitalni virusi - evolucija vrsta

- antivirusne nadogradnje **nisu** samo za **uzorke** već i za **bihevioralnu** analizu
- mnogo (**previše**) **heuristike** - mnogo krivo detektiranih (**false positives**) rezultata
- bitno i **vrijeme odgovora** na nove viruse:
  - najbrži Kaspersky (0-2 sata), najsporiji Symantec i e-Trust (10 i više sati)
  - prema [av-comparatives.org](http://av-comparatives.org), [virus.gr](http://virus.gr) i [av-test.org](http://av-test.org) su "najbolji": Nod32, BitDefender, Kaspersky

# Digitalni virusi - evolucija vrsta

- Kaspersky Lab:
  - 2004 godine zabilježeno 422 malwarea za Linux
  - 2005. godine zabilježeno 863 malwarea za Linux
- budućnost
  - **virusi** za PPC-ove i ostale **mobilne** uređaje (Symbian60, Windows Mobile, itd)
  - **Skype** virusi, **WLAN** virusi...

# Spyware - krađa podataka

- kroz 2005. godinu prema dvije Forrester-ove analize (početak i sredina 2005) sa 4. došao na **2. mjesto** kritičnosti
- povećanje od **50%** u Q4 2005
- prvo mjesto: virusi i crvi
- rezultat spywarea:
  - gubitak **performansi** računala, **padovi**, IP problemi, **curenje** privatnih informacija, vrijeme za **popravak**, smanjena **produktivnost**, itd.

# Spyware - krađa podataka

- Gartner: prosječna cijena popravka 1 spyware inficiranog **PC-a** cca **\$375**
- cca **3 tjedna** incidenta na **1000** računala
- godišnji gubici u IT sa 2000 računala:
  - IP gubici: \$20000
  - curenje privatnosti: \$5000
  - gubitak produktivnosti: \$28080
  - cijena IT vremena za popravak: \$117000
  - ukupno **\$170080 godišnje!**

# Spyware - krađa podataka

- 2003: **2%** helpdesk poziva vezanih uz spyware
- 2006: **40%!**
- PricewaterhouseCoopers 1999:
  - velike organizacije u prosjeku gube **2.45** puta povjerljive informacije **godišnje**, a cijena svakog incidenta je **\$500000**
- unutar Fortune 1000:
  - (1000 najbogatijih/najbolje stojećih US kompanija)
  - 1999. cijena curenja bila **\$45 bilijuna**

# Spam - svako jutro pisamce

- prosječan rast od **16% mjesečno**
- organizacija od 100 zaposlenih od kojih svaki dobije 10 spamova dnevno košta dodatnih **\$1300** godišnje
- jednostavnija i jeftinija klijentska rješenja:
- **centralna rješenja** - efikasnija, moćnija, daleko veća cijena, lakše/brže postavljanje
- tehnike: statika, dinamika; crne liste, bijele liste, sive liste; statistika, uzorci...

# HIPS - mnogo malih jedinica

- danas - integriraju se sa **AV** ili **PF**
- prve verzije: **pitaju korisnika** za svako spajanje na Internet i sl.
- **crne** liste, **bijele** liste (liste **uzoraka/potpisa**)
- detekcija **anomalija/biheviioralna** analiza
- **virtualizacija, sandboxing**
- **kernel** dodaci (PaX i sl), NX bit
- od čega štite? virusi, trojanci, crvi, malware...

# 19 smrtonosnih grešaka u sigurnosti aplikacija

- **preljevi** spremnika
- problemi oko nizova za **formatiranje** ispisa
- **umetanje SQL** naredbi
- **umetanje općih** naredbi
- kriva/neispravna/nedostatna **obrada grešaka**
- **XSS** - skriptiranje sa poslužitelja na poslužitelj
- nedovoljno **zaštićen mrežni promet**

# 19 smrtonosnih grešaka u sigurnosti aplikacija

- korištenje **magičnih URL-ova** i **skrivenih formi**
- neispravno **korištenje SSL-a**
- korištenje slabih/nedostatnih **sustava** za **lozinke** ili samih lozinki
- neuspješno **spremanje** i **zaštita** podataka
- **curenje** informacija
- neispravan **pristup datotekama**
- greška u **rasponu cjelobrojnih** varijabli

# 19 smrtonosnih grešaka u sigurnosti aplikacija

- **slijepo vjerovanje** mrežnim podacima (izvorište, odredište...)
- neispravno/nedostatno **baratanje signalima** (race conditions)
- izmjena **ključeva** bez **autentifikacije**
- izostanak korištenja **kriptografski snažnih slučajnih brojeva**
- nedostatna **iskoristivost**...

# Web application firewall

- vršite li **službenu** provjeru web aplikacija?
- funkcije:
  - **audit** (IDS: promet, sadržaj, pojedine transakcije, tokovi)
  - **kontrola** pristupa (IPS - vatrozid, prevencija), arhitekturni zahvat (distribucija, virtualizacija, preusmjeravanje, itd.)
  - **jačanje** sigurnosti (filtriranje nekog sadržaja, specifičnih grešaka i sl.)
  - IDS i IPS: mrežni L3/L4 nivo analize, općenita detekcija napada/malwarea/... i akcije

# Web application firewall

- HIDS: uglavnom se ne analizira mrežni promet, već **ponašanje** individualnih aplikacija/računala/logovi/datoteke/...
- NIDS **nije** dovoljan!
  - L7 analiza vrlo **složena**
  - HTTP donosi vrlo **kompleksan** set problema
  - primjeri: XMLRPC, SOAP, HTTPS, itd.
  - nužan **specijaliziran** i **optimiziran** L7 uređaj
- upiti se **preusmjeruju** (posreduju) kroz WAF, analiziraju i propuštaju/odbacuju/filtriraju

# Web application firewall

- nije uvijek moguće riješiti problem u samoj aplikaciji
  - tuđe **komponente**, **zatvoreni** kod
  - uvijek postoje **greške** - rijedak je softver 100% korektan
  - svjež **ranjivosti** u tuđim dijelovima - npr. frameworku, interpreteru, poslužitelju itd.
- sustav je uvijek **provaljiv** - bitno je smanjiti i **ograničiti** potencijalnu štetu odgovarajućim **zahvatima**

# WAF - reverzni posrednik

- za **poznate** probleme:
  - filtriranje po **statičkim** pravilima
  - **negativni** pristup - crne liste: sto je opasno - allow all, deny some
- za **nepoznate** probleme:
  - detekcija **anomalija** u protokolu: provjera standarda, konteksta, itd.
  - provjera **podataka** u **unosu**: tipovi, sadržaj, lokacija, itd. provjera u browseru nije dovoljna!

# WAF - reverzni posrednik

- **pozitivni** pristup - bijele liste: što je dozvoljeno - allow some, deny all; dobro za stabilne Web aplikacije
- **trenutno rješavanje** sigurnosnih problema - ne treba čekati proizvođača aplikacije
- upravljanje **stanjima**:
  - forsiranje **definirane** početne stranice/stanja
  - promatranje pojedinog **korisnika/sjednice individualno**

# WAF - reverzni posrednik

- detekcija/reakcija **brute-force** napada
- upravljanje **vremenom trajanja** sjednice
- prevencija **preuzimanja** sjednice
- praćenje povijesti sjednice - samo linkovi iz prethodnog upita su dozvoljeni
- sprečavanje curenja (osjetljivih) informacija

# Sistemski zapisnici

- **automatizirani** pregled logova
- **koncentracija i agregacija** 100% svih postojećih zapisnika
- minimalno dostupni **3 mjeseca online, 1 godinu** spremljeni
- **izvori - sve!**
  - **mrežne** komponente: vatrozidi, preklopnici, usmjernici, IDS-ovi i detekcija, posrednici, sadržajni filteri, bežične pristupne točke, itd.

# Sistemske zapisnice

- **poslužitelji**: Web, podatkovni, AAA, DNS, mail, NTP, imenički, itd.
- **aplikacije**: vlastite, kupljene, Web, Internet, ...
- **nužnost**:
  - centralna **konzola**, centralni **poslužitelj**,  
višestruki **spremnici**, **redundancija**
  - specijalizirani **senzori** nad sektorima, senzori na odgovarajućim opasnim točkama
  - posebno računalo za **nadzor/pregled** - npr. više monitora i pregled uživo

# Sistemske zapisnici

- **kontinuirana analiza** za prijetnjama
- **korelacija** događaja
  - uživo, u stvarnom vremenu
  - ne u stvarnom vremenu - vremenski prozori, itd.
- preduvjeti za uspješnu forenziku/audit/...
- nužno spremanje u **odgovarajućem** obliku:
  - najčešće poseban **binarni** format - problem: nemoguća ručna analiza bez dodatnih alata
  - moguće **rekonstruirati** cijelu sliku događaja po potrebi

# Sistemske zapisnici

- **korisnički** pristup, izvršene **akcije**, neuspjela **logiranja**, upotreba **autentikacijskih** i autorizacijskih mehanizama, **startanje** logova, promjene na **sistemskim** objektima, itd.
- nužno postojanje kopije **sirovih netaknutih** logova - **zakonom** definirano
  - **višestruke** kopije - DA, ali **organizirano** i **nedvosmisleno** (sigurnosna politika...)

# Sistemske zapisnici

- nužan centralizirani **alerting i reporting** za sve uređaje, računala i sustave:
  - **rana upozorenja** na napade, neovlašteno korištenje, zlouporabu
  - lakša **izolacija i rješenje** problema
  - korištenje **mobitnih telefona** ili pagera za dojavu **incidenata**
  - **jasni, nedvosmisleni, kratki, organizirani izvještaji**
  - **redovni izvještaji**, statistika, pregled...

# Korporativna mreža

- centralni L3/L4 **vatrozid** sa osnovnom L7 analizom te IDS i IPS mogućnostima
- centralni **Web** aplikacijski **vatrozid** sa AV mogućnostima
- **usmjernici** sa anti-DoS/DDoS mogućnostima
- **klijentski** AV/anti-spyware/vatrozid/IPS/IDS sa **push** načinom rada i admin **konzolom**
- centralni **log spremnik** i **analizator**

# Korporativna mreža

- centralizirani korporativni **Web** filter:
  - **L7 analiza** sadržaja: eliminacija spyware, malware, virusa, porno i inog neprikladnog sadržaja
  - zaštita **privatnosti**: filtriranje zaglavlja, sadržaja, cookie-ja
  - **bijele** i **crne** liste stranica, DNSBL
  - uklanjanje **reklama**, **phishing** detekcija, kvalitetna **klasifikacija sadržaja** (unaprijed i u stvarnom vremenu)
  - ... u nastavku detaljnije

# Korporativna mreža

- centralizirani **e-mail** filter:
  - blokiranje **nepoželjnih priloga**, virusa, opasnih **ekstenzija** (vbs, scr, pif, exe, com itd.), mobilnog koda, **aktivni HTML**, **phishing** detekcija
  - **crne, bijele i sive** liste: **statički i dinamički**
  - e-mail klasifikacija **sadržaja**: **statički** (fiksna pravila), **dinamički** (statistika: bayesian, sbph)
  - blokiranje spama **iznutra i izvana**: virus + spamming = spam iznutra, dolazak na crne liste itd.

# Korporativna mreža

- centralizirani općeprisutni **vatrozid**:
  - zone **rizika**, **segmenti**, **DMZ** za pojedine servise
  - **blokiranje** IM, P2P, VoIP, pojedinih aplikacija (osnovna L7 analiza)
  - **IPS** i **IDS** funkcije: u stanju prepoznati napad i poduzeti odgovarajuće **akcije**... npr. DNS analiza
- centralizirani **antivirus**:
  - **kontrola**, **push** updates, **reportovi**, **scheduled** skeniranje, **antispyware**, itd.
  - lokalni minijturni **vatrozidi** za svako računalo

# Korporativna mreža

- centralizirani **backup** sustav
  - inkrementalni, puni, diferencijalni
  - dnevni, tjedni, mjesečni, godišnji
- centralizirani **inventarni** sustav
- centralizirani **zapisnički** sustav
- centralizirana **administracija** svih računala
  - Microsoft AD, WSUS, itd.

# Diskusija!

