How Assess, Evaluate, Optimize a .COM Security Infrastructure

Giuseppe RUSSO
Security Consultant
giurus@Sun.COM

Agenda

- Scenario di riferimento
- Le infrastrutture .COM
- Le minacce all'infrastruttura .COM
- I requisiti di sicurezza del .COM
- Valutazione del livello di sicurezza
  - Valutazione perimetrale
  - Valutazione server
  - Valutazione networking
- Ottimizzazione del sottosistema di sicurezza

Cos'è una .Com?

- La trasformazione del modello di business mediante tecnologia web
- Una nuova segmentazione del mercato:
  - Supply Chain Management
  - Portals
  - Service Providers
  - Customer Relationship Management
  - E−Business

La Prospettiva Dot.Com

The dot.com is about service delivery

Any Service

Any Time

Anywhere

Any Device

MASSIVE scale

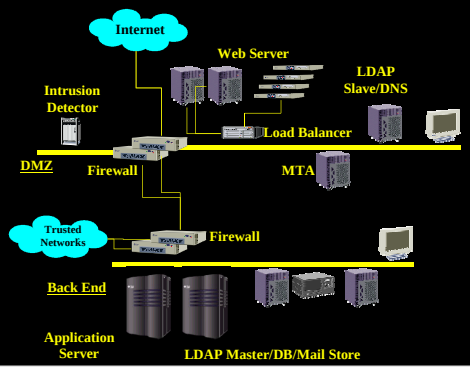
Trust

The Vision: *Service – Driven Network*

Costruire una Architettura Dot−Com

- Non esiste una sola soluzione
- L'architecture non è statica, ma piuttosto dinamica e iterativa
- Una architettura deve coesistere con infrastrutture e sistemi pre−eseistenti

Architettura .COM di riferimento



Sun: The .COM leader

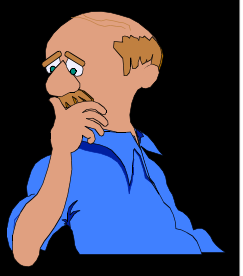
- 80% di applicazioni Internet girano su piattaforma Sun Microsystems
- 75% dei server ISP−based sono su Sun
- 5 dei top 20 ISP's and 80% dell' Internet backbone traffic gira su Sun
- I primi 5 e−Commerce SW vendor con il 73% di market share vendono 80−90% dei loro prodotti su macchine Sun
- Più di 400 leader ISV's sviluppa e rilascia su Sun
- 35% di tutti i servizi Internet sono su macchine Sun

Desideri di business

- Trarre profitto dalle nuove tecnologie e dalla connettività globale
- Rendere disponibili le proprie informazioni e risorse
- Erogare servizi a cui possono accedere tutti
- Accumulare Ricchezza

Le preoccupazioni associate

- La connettività mi espone ad accessi indesiderati...
- Come posso essere certo di erogare servizi a chi ne ha diritto?
- Come coopero nello sviluppo del business con partner che sono anche competitor?



La dicotomia della Rete

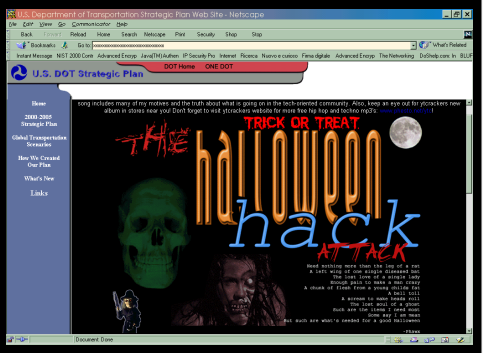
"Any company that is not currently making the transformation to an e−business model will find it extremely difficult, if not impossible, to compete in the global market of the 21st century."

Hurwitz Group

"I just wanted to prove how insecure these sites are"

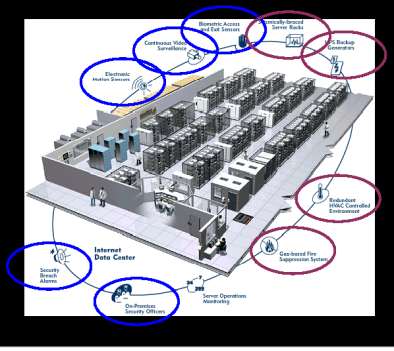
Suspected Malicious Hacker

Uno dei casi reali



Dipartimento dei trasporti degli Stati Uniti

Le Server Farm Internet



Chi attacca le Server Farm?

- Alcuni statistiche FBI hanno portato ai seguenti risultati:
  - Attacchi esterni da gruppi di hacker, cracker
    - 30 %
  - Attacchi interni da dipendenti
    - 70 %
- le minacce maggiori arrivano dagli utenti abilitati

The dark side of the Net

- Threat Space
- Hackers
- Crackers
- Worm/Virus
- Denial of Service
- Ecc...

Strumenti utilizzati

- In passato (*metá anni '80*)
  - i Tools piú comuni erano compilatori C, debugger simbolici, codice sorgente UNIX ed operazioni manuali.
- Oggi
  - Tool moderni che eplorarano automaticamente vulnerabilitá dei sistemi e delle reti
  - i piú comuni: SATAN, Crack, mappers, ecc...
  - distribuzione delle informazioni via internet

Attacchi Storici

- The Cuckoo's Egg (86−87)
  - spionaggio, dalla Germania EST ai danni dei Lawrence Livermore National Laboratories (CA)
- Internet Worm (88)
  - inizia come un gioco, esplora fault nei comandi *sendmail* e *finger*, riesce ad infettare macchine giá ripulite, coinvolge circa 6000 macchine in Internet, produce *denial of service* massivi

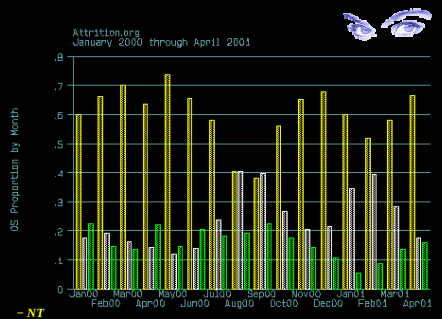
I nuovi attacchi

- Buffer Overflow
- Weak Passwords and Packet Sniffing
- Email Vulnerabilities
- IP Spoofing and Connection Hijacking
- File Sharing

I nuovi attacchi (cont.)

- RPC Services
- X Windows Servers
- Dos & DDos
- DNS
- Viruses and Trojan Horses
- Mobile Code

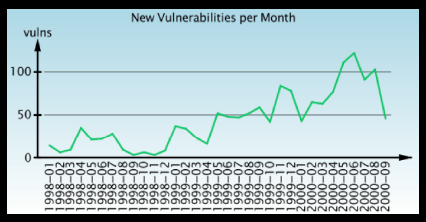
I numeri delle violazioni...



– NT
– Linux
– Altri

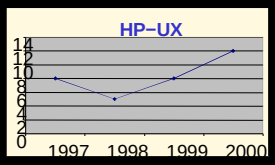
Fonte: Attrition.org

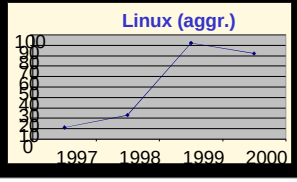
Nuove vulnerabilità al mese



Fonte: Bugtraq

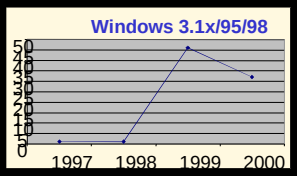
Vulnerabilità di OS per anno

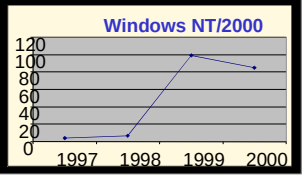




Fonte: Bugtraq

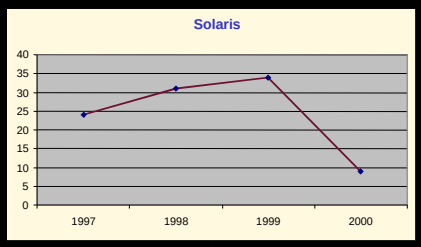
Vulnerabilità di OS per anno (cont.)





Fonte: Bugtraq

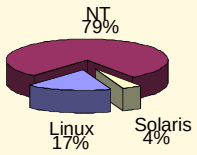
Vulnerabilità di OS per anno (cont.)



Fonte: Bugtraq

Situazione in Italia

Sistemi operativi violati dal 98 ad oggi

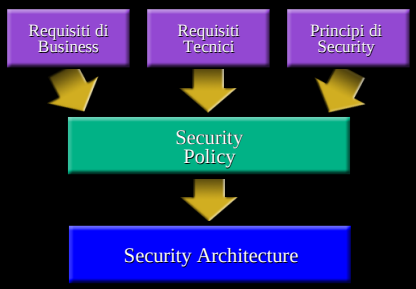


Fonte: Attrition

Come evitare tutto questo?

- Un approccio corretto ed una metodologia di Sicurezza consolidata
- Utilizzo di tecnologia up−to−date
- Un team di lavoro competente
- Un Progetto di Sicurezza globale

SecurityFramework



Sicurezza: i requisiti fondamentali

I requisiti fondamentali

- **Identificazione**
- **Autenticazione**
- **Autorizzazione**
- **Integrità**
- **Riservatezza**
- **Non ripudio**

i requisiti fondamentali (cont.)

Identificazione

la richiesta di indentità di un utente

- **possesso di una username, di un elemento di identificazione (card, certificato, smart card)**
- **necessità di un repository unico per tutti gli utenti, affidabile, sicuro, scalabile**
- **directory server X.500 con accesso via LDAP**
- **utilizzo in un infrastruttura a chiave pubblica**
- **elemento centrale delle applicazioni I*net**

i−Planet Directory Server
i−Planet Certificate Management Server

i requisiti fondamentali (cont.)

Autenticazione

la dimostrazione dell'indentità di un utente

- **possesso di una password, un pin, una passphrase**
- **Simple Password, Challenge / Response**
- **Token card, Smart card, Java Card**
- **Sistemi biometrici**

Solaris Pluggable Authentication Module (PAM), Kerberos, JAAS, Java Card

i requisiti fondamentali (cont.)

Autorizzazione

l'abilitazione dell'utente ad eseguire le operazioni per le quali è stato identificato ed autenticato, in un determinato istante

- **controllo accessi a livello di sistemi e reti**
  - **network perimetral defense (firewall)**
- **controllo accessi a livello applicativo**
  - **proxy**

SunScreen SecureNet, i−Planet Portal Server, i−Planet Proxy Server, Java Security model

i requisiti fondamentali (cont.)

Riservatezza

l'abilitazione dell'utente ad eseguire in forma riservata le operazione ritenute sensibili

- **Crittografia dei dati**
- **tunneling end to end, end to node**
- **virtual private network**
- **IPSec, SKIP, IKE**

SunScreen SecureNet, SKIP
Solaris 8 (IPSec con IKE, SKIP)
Sun Crypto Accellerator I

i requisiti fondamentali (cont.)

Integrità

la certezza che un dato non venga alterato durante la trasmissione o nella sua memorizzazione

- **algoritmi di hashing : md5, sha−1**
- **verifica dell'integrità dei codici eseguibili**

Sun Solaris fingerprint database, Solaris C2, Solaris ITSEC E3/F−C2, Trusted Solaris, Bruce Project

i requisiti fondamentali (cont.)

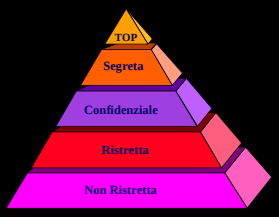
Non ripudio

l'impossibilità per un utente di negare la sua partecipazione ad una transazione

- **supporto nella definizione dell'infrastruttura a chiave pubblica**
- **disegno di architetture di sicurezza a più livelli**

JCE Java Cryptographic Estension

i requisiti fondamentali (cont.)



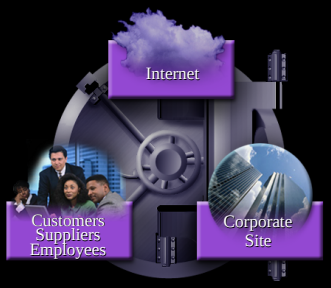
Esigenza di classificare le informazioni = **Trusted Solaris**

Riassumendo.....

- l'*autenticazione* degli utenti
- l'*integrità* delle risorse
- la *confidenzialitá* delle informazioni trattate
- la *privacy* degli individui coinvolti
- la massimizzazione della *Trustworthiness*
- la *classificazione* delle informazioni

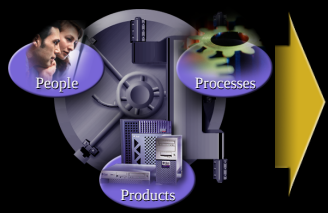
Consentono di realizzare un ambiente .COM di cui ci si puó fidare

Security Architecture Components



- Access Control
- Identification
- Authentication
- Authorization
- Privacy
- Integrity
- Non−Repudiation
- Certificates

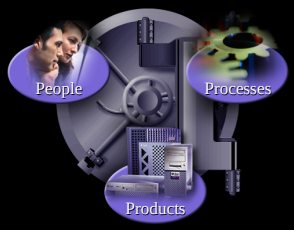
Security Solutions



- Single Sign−On
- Host Security
- Perimeter Defense
- Compartments
- Remote Access
- Electronic Commerce
- Public Key Infrastructure

Il Successo di una soluzione di Security

Sun Security Services



- Affiancamento nella definizione della Politica di Sicurezza
- Enterprise Security Assessment
- Disegno ed Implementazione di architetture di Firewalling, VPN, PKI
- Hardning dei sistemi
- Predisposizione sistemi operativi classificati ITSEC
- Integrazione di servizi di sicurezza

Enterprise Security Assessment

- Il servizio di ESA fornisce un assessment di:
  - Politiche di sicurezza in vigore
  - standard e linee guida nel Data−Center
  - Analisi dei server che erogano servizio
  - probing di tutti i servizi IP che possono essere esplorati da Internet e da un host presente sulla rete (aka Penetration Test)
  - Produce una fotografia del livello di sicurezza del Data−Center

Aree di indagine

- Il framework delle indagini si articola nei seguenti punti:
  - *Access & route control*
  - *Firewalling & Network isolation*
  - *Encryption*
  - *Authentication*
  - *Authorizzation*
  - *Standardizzation*

La metodologia ESA

- Kick off meeting
- Acquisizioni informazioni
- Analisi dei server che erogano i servizi
- Penetration Test
- Analisi dei dati
- Elaborazione punteggi e presentazione al management

La metodologia di ESA − *fase 1*

Kick off meeting

- Evidenzia le aspettative del cliente
- Definisce lo staff utente che seguirà il lavoro di assessment

La metodologia di ESA − *fase 2*

Interviste a personaggi chiave

- E' il primo meccanismo per collezionare i dati
- Consente di evidenziare la tipologia della rete, i sistemi critici, il livello attuale di sicurezza
- Il successo di questa fase è proporzionale alla collaborazione degli utenti coinvolti

I personaggi Chiave

- il Responsabile della Sicurezza
- il Network Manager
- l'Amministratore della Sicurezza
- il responsabile dell'amministrazione dei sistemi
- il responsabile dello Sviluppo Applicativo
- il responsabile del Supporto Tecnico
- gli amministratori di Firewall, Extranet e di eventuali apparati Modem
- un Utente Finale

Il ciclo delle interviste – *fase 2a*

- Le interviste coprono i seguenti temi:
  - Politica di Sicurezza in uso
  - Controllo degli accessi: *Sicurezza Fisica*
  - Controllo degli accessi: *Sicurezza dei Dati*
  - Backup dei Dati
  - Privacy e Riservatezza
  - Autorizzazione/Autenticazione
  - Integrità delle informazioni
  - Management

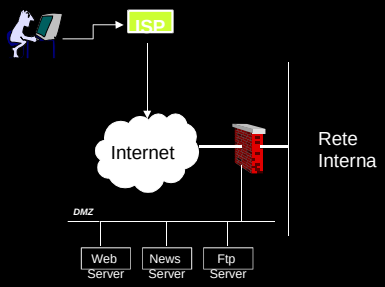
Analisi dei server

- raccolta dello stato delle patches tramite Patchdiag
- accolta dati delle misconfigurazione dei files di ogni singolo sistema tramite Titan *http://www.fish.com/titan*
- raccolta di ulteriori dati ad hoc

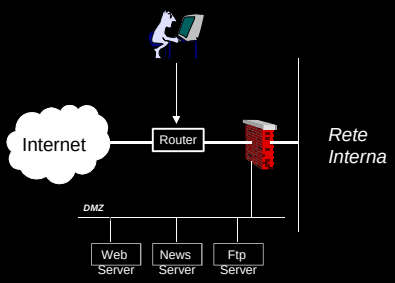
Altre infos....

- .....sui pakages installati
- .....sui logging
- .....sulla configurazione della rete
- .....sui processi in esecuzione
- .....sul NTP
- .....sulla configurazione del Kernel
- .... altre informazioni

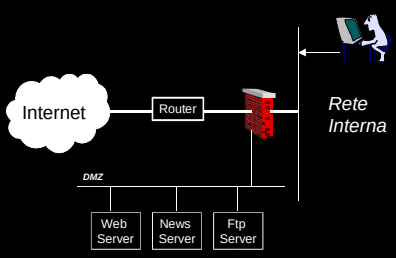
Probing da Internet



All'ingresso del firewall



Dalla rete Interna



Network Probing …. *cont*

- Gli strumenti per il probe fanno uso di agent intelligenti
- Il probe tiene conto delle diverse piattaforme nella rete Unix, NT, ecc.
- Strumenti utilizzati: Titan, Autohack, Satan, ISS, Crack, Probe tools, Nmap, Nessus, ecc.

Conosci il tuo nemico

Hacker mentality & underground life

Hacker strategy

- Vulnerability Oriented

  si lascia guidare dalle vulnerabilità note e fa intenso uso di script già disponibili

- Target Oriented

  è interessato ai server che erogano servizi e non conosce le vulnerabilità a priori

Vulnerabilty oriented

- Non ricerca informazioni specifiche
- Cerca di ottenere i privilegi di root nel modo più semplice possibile
- Si concentra su un numero limitato di vulnerabilità
- Presto o tardi trova un sistema con le vulnerabilità che si aspetta
- Non ha scrupoli a fare danni che spesso sono involontari

Script Kiddies

Target oriented

- Spesso è alla ricerca di informazioni riservate
- Ottiene i privilegi di root con metodi non noti
- E' molto cauto e tratta il sistema come se fosse il suo
- Vive in simbiosi con il sysadm dei quali ne studia il comportamento

Approcci Intrusivi

- Selezione del target, background info
  - Whois, nslookup
- Probing preliminare
  - Nmap, Pop probe, Smtp probe, DNS
- Ricerca di backdoors
- Technical attack o social engineering
  - Overflow, DoS etc.

Una strategia di attacco

- Non INTRUSIVA
- Indaga sulle Misconfigurazioni
- Non provoca Denial of Services (DoS)
- può sfruttare account esistenti

- Obbiettivi:
  - *Gain Root privileges*
  - *Ricavare informazioni di rilievo*

Una strategia di attacco (cont.)

- Individuare il Target:
  http://www.my−target.com
- Individuare hops
- Trovare i sistemi e reti connessi al target
- Rilevare i Servizi da essi erogati
- Utilizzare macchine Ponte
- Individuare e sfruttare accounts privilegiati

La metodologia di ESA − *fase 4*

Analisi dei dati

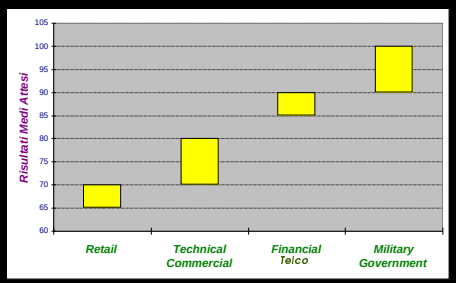
- I dati raccolti durante la fase delle interviste sono analizzati confrontandoli con le politiche di sicurezza aziendali
- I dati collezionati durante il *penetration test* sono analizzati per evidenziare discrepanze dalla politica ed eventuali *bug* di sicurezza

La metodologia di ESA − *fase 5*

Redazione del Report e Presentazione

- I dati raccolti nelle interviste e nel probe sono elaborati e redatti in un documento finale
- Il documento contiene la *fotografia* della rete dal punto di vista della *Sicurezza*.
- Il core del documento è una valutazione numerica del livello raggiunto, confrontato con i punteggi *best practice.*
- Sono evidenziati i problemi più importanti riscontrati e le relative raccomandazioni
- Il documento è presentato ufficialmente

Valutazione numerica



Hardening dei sistemi

- L'hardening di un sistema e' funzione del livello di servizio che quella stazione deve erogare.
- Serve ad ottenere un adeguato livello di rafforzamento delle autodifese dei sistemi operativi
- Bisogna predisporre un progetto ad Hoc.

First Point

- Installare tutte le patches raccomandate e quelle inerenti la sicurezza
- Disattivare, e possibilmente rimuovere, tutti i servizi TCP/IP non necessari. In particolare considerare servizi quali: *inbound mail, telnet, FTP, echo, discard, daytime, chargen, time, DNS, rsh, rexec, rlogin, uucp, NFS...*

Second Point

- Applicare il ragionamento precedente anche ad eventuali software applicativi che utilizzano sevizi di rete
- Installare dei Wrapper TCP su tutti i servizi restanti. L'utilizzo di strumenti wrapper consente di permettere/negare l'utilizzo dei servizi configurati direttamente sulla stazioni

Third Point

- Valutare la possibilità di installare dei meccanismi di IP Filtering direttamente sulla stazione associandoli ai servizi attivi sulla macchina
- Installare meccanismi di accesso remoto che utilizzino strong authentication e cifratura della connessione. Tipicamente si usano per sostituire comandi quali *rlogin, rsh*, ecc.

Fourth Point

- Installare il software applicativo. Se esso utilizza risorse di rete confinarlo in un ambiente chroot
- Analizzare i permessi del file system allo scopo di identificare eventuali incongruenze per la sicurezza.

Controlli Successivi

- Alla ripartenza del sistema occorre predisporre:
  - ✗ una probing analisys del sistema mediante portscanner, allo scopo di identificare quali sono i servizi ancora attivi sulla stazione. Verificare che essi siano coerenti con la politica di sicurezza adottata.
  - ✗ Effettuare il test dell'applicazione. Se essa utilizza servizi di rete accertarsi che questi siano coerenti con la politica di sicurezza.

I punti salienti dell'hardening

- Ottimizzazione dell'Auditing
- Boot Files
- Network Services
- Access Control
- Time Synchronization


Giuseppe Russo
giurus@sun.com
We're the
dot in .com™
Sun
microsystems