



IBM ISS Security Services and Solutions

Fabio Panada
Solution Architect Leader
IBM Internet Security Systems

IBM Internet Security Systems

- Internet Security Systems (ISS) was acquired by IBM October 2006
(founded 1994)
 - World leader in security **intelligence**, **preemptive** security and managed protection services
 - Over 14,000 customers worldwide
- ISS is a key element of our Dynamic Infrastructure stack
- ISS complements Server security goals to “keep the bad guys out” and “let the good guys in”
 - Virtualize securely
 - Achieve and maintain compliance
 - Reduce security cost



Il Report X-Force Trend & Risk

La missione di X-Force®,
il gruppo di ricerca e sviluppo di
IBM Internet Security Systems™ è :

- Ricercare e valutare nuove minacce e protezioni
- Sviluppare tecnologie di assessment e contromisure
- Sviluppare nuove tecnologie per le sfide di domani
- Educare i media e le comunità di utenti



- Ecco i numeri...
- **9.1B** pagine Web & immagini Web analizzate dal 1999
 - 150 milioni nuove aggiunte al mese
- **150M** tentativi di intrusione monitorati giornalmente da IBM ISS Managed Security Services
- **40M** attacchi spam & phishing
- **40K** vulnerabilità documentate
- Milioni di esempi unici di malware
- Gestione di più di **4B** di eventi di sicurezza al giorno per cliente

Principali Trend del 2008

- Le 7,406 nuove vulnerabilità rappresentano il 19% di tutte le vulnerabilità raccolte dalla creazione del database X-Force che risale a più di dieci anni fa.
- La severità è aumentata, con vulnerabilità di severità alta e critica fino al 15.3% e di severità media fino al 67.5 %.
- Una presenza Web sicura sta diventando il tallone d'Achille della sicurezza IT
- Si stanno verificando attacchi massivi agli endpoint non solo attraverso le vulnerabilità dei browser, ma anche tramite documenti e video pericolosi (es. Adobe PDF)
- I principali "Exploit" tipicamente portano all'installazione di Trojans destinati al furto di informazioni, la principale categoria di malware
- La chiusura del sito McColo ha rappresentato l'evento più importante dell'anno in termini di impatto sullo spam

Siti Web – Vulnerabilità delle applicazioni Web

- Vulnerabilità delle applicazioni Web
- Rappresenta la principale categoria di vulnerabilità scoperte (55% nel 2008)
 - Il 74% delle vulnerabilità di applicazioni Web scoperte nel 2008 non dispone di una patch

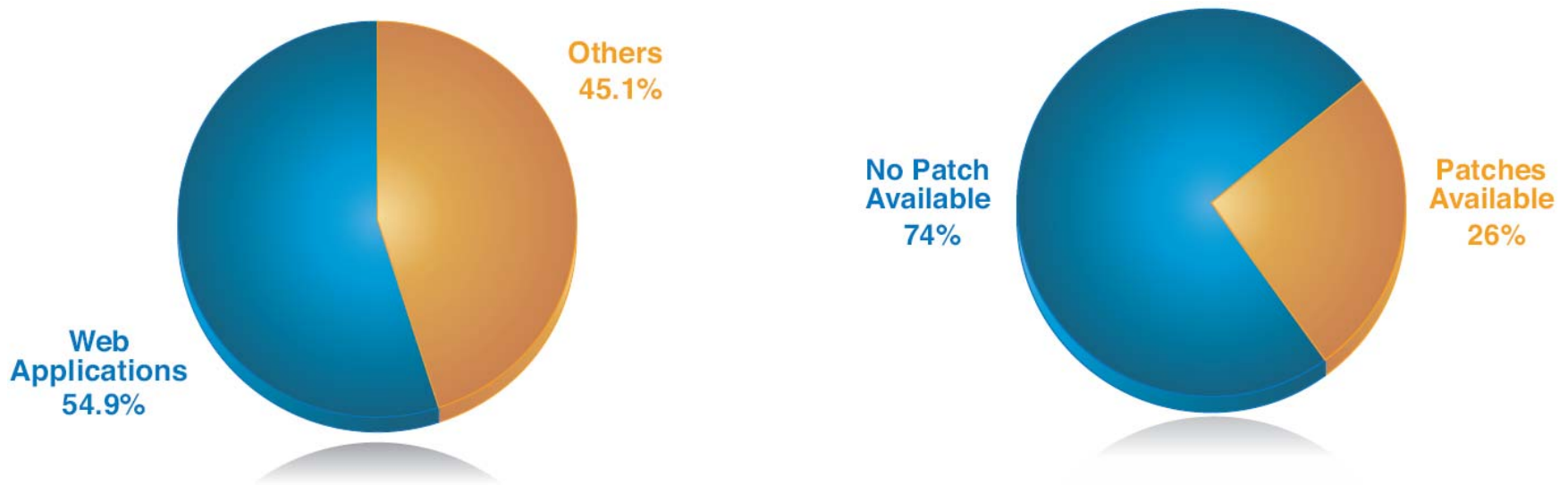


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

I sistemi operativi più vulnerabili

- I 10 sistemi operativi più vulnerabili rappresentano il 75% di tutte le vulnerabilità di sistema operativo scoperte nel 2008
- Molti sistemi operativi sono rimasti nella top five degli ultimi 3 anni:
 - Apple Mac OS X
 - Apple Mac OS X Server
 - Linux Kernel
 - Microsoft Windows XP (with one exception in 2007)

Operating System	Percentage
Apple Mac OS X Server	14.3%
Apple Mac OS X	14.3%
Linux Kernel	10.9%
Sun Solaris	7.3%
Microsoft Windows XP	5.5%
Microsoft Windows 2003 Server	5.2%
Microsoft Windows Vista	5.1%
Microsoft Windows 2000	4.8%
Microsoft Windows 2008	4.1%
IBM AIX	3.7%
Others	24.9%

Table 7: Operating Systems with the Most Vulnerability Disclosures, 2008

Aspetti economici degli Exploit

- Il settore della Sicurezza deve imparare ad includere le motivazioni criminali nelle procedure di risposta per la sicurezza
- Gli aspetti economici (costi e benefici) giocano un ruolo importante nella probabilità di sfruttamento degli exploit
- Le vulnerabilità critiche possono non essere così critiche come sembrano
- Il costo della monetizzazione e dello sfruttamento dell'exploit deve essere pesato con l'opportunità

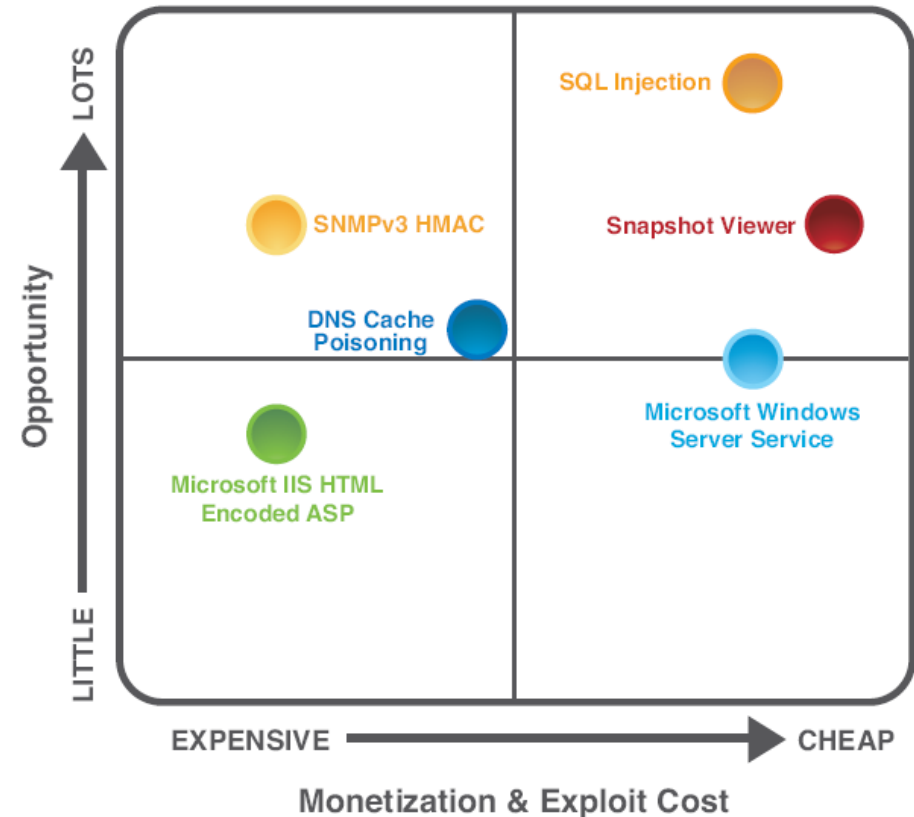


Figure 7: Exploitability Probability Quadrant

Esempi quotidiani di Server breach.

Heartland Struggles to Measure Extent of Massive Security Breach

Data breach could be industry's biggest ever, experts say

Jan 21, 2009 | 05:08 PM

Hannaford, Security Industry Hunt for Cause of Massive Breach

Speculation runs rampant a grocery retailer attempts to find out how 4.2 million credit card records were stolen

Mar 18, 2008 | 10:07 AM

IT Worker Indicted for Setting Malware Bomb at Fannie Mae

IT contractor deployed highly malicious script before his administrative rights were terminated

Jan 29, 2009 | 05:42 PM

IBM solutions focus on critical customer needs

IBM ISS brings services together with IBM and partner technology to reduce the cost and complexity of managing risk in an organization.

ISS Security Focus Areas

Security Governance	Threat Mitigation	Data Security	Identity and Access Management
<ul style="list-style-type: none"> ▪ Security Risk Management ▪ Security Program Design and Management ▪ Regulatory and Standards Compliance ▪ Privacy ▪ Security Education and Training 	<ul style="list-style-type: none"> ▪ Network Protection ▪ Endpoint System Protection ▪ Application Security ▪ Security Enablement and Vulnerability Management 	<ul style="list-style-type: none"> ▪ Enterprise Content Protection ▪ Endpoint Data Protection ▪ Activity Compliance Monitoring and Reporting ▪ Messaging Security 	<ul style="list-style-type: none"> ▪ Identity Assessment and Strategy ▪ Identity Lifecycle Management ▪ Access Management ▪ Strong Authentication Solutions

IBM Internet Security Systems Product Offerings

proventia[®]management
SiteProtector™



Vulnerability Scanning Appliance

- Vulnerability Discovery
- Remediation Recommendation, prioritization and assignment
- Tracking to resolution
- Compliance Reporting

proventia[®]network
Enterprise Scanner

NEW Data Security Services and Data Loss Prevention (DLP)

Data Leakage – A holistic approach to ensure that data does not find its way outside of controlled environments

proventia[®]network

Protection Appliances

Proventia Network IPS – GX Models

- Preemptive Security for Networks
- Identifies & analyzes >140 protocols
- Bi-directional deep packet decode using Protocol Analysis Module
- Sized by segments and network throughput to protect (10Mb to 5 Gb in line)
- Virtual Patch Technology – ahead of the threat – protection against zero day attacks with X-Press Updates

proventia[®]network

Protection Appliance

Multifunction Appliance – MX UTM
“All-in-One” Protection Appliance

- IDS/IPS
- FW / VPN
- AntiVirus (signature & behavioral)
- AntiSpam
- Web Filter
- Spyware

proventia[®]server

Real Secure Server Sensor

Real Secure Server Sensor

- Solaris, AIX, HP-UX & Windows
- Firewall
- Intrusion Protection
- Protects SSL applications

proventia[®]server

Protection Agent

“Multi-layered” Protection

- Windows & Linux
- Firewall
- Intrusion Protection
- Provides monitoring of Windows Registry, users, files and directory

Proventia
endpoint secure control

Desktop Protection Agent

System / Data Protection & System Management Agent

- Firewall
- Intrusion Protection
- Antivirus (signature & behavioral)
- Device control
- DLP
- NAC
- Whole disk encryption
- Patch management
- Power management
- Compliance/SCAP/FDCC
- Software deployment/removal

Our security-rich software agents are designed to help support most operating systems against multiple types of server attacks.

IBM Internet Security Systems™ – server protection is comprised of two products:



IBM Proventia® Server Intrusion Prevention System (IPS) provides server protection for:

Microsoft® Windows®

Linux®

VMware Guest Operating System (OS)

IBM RealSecure® Server Sensor provides server protection for:

Microsoft® Windows®

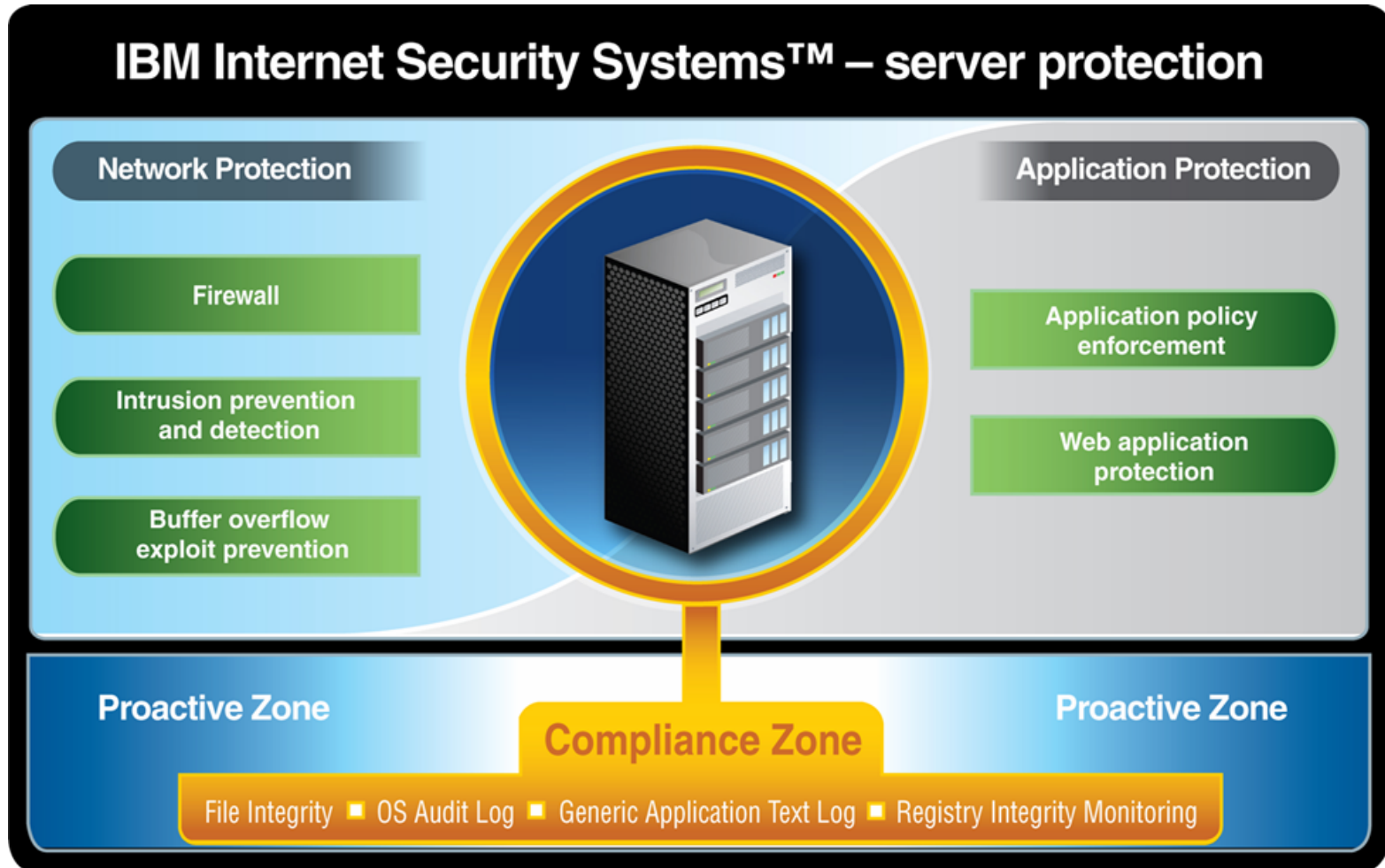
AIX™

Solaris

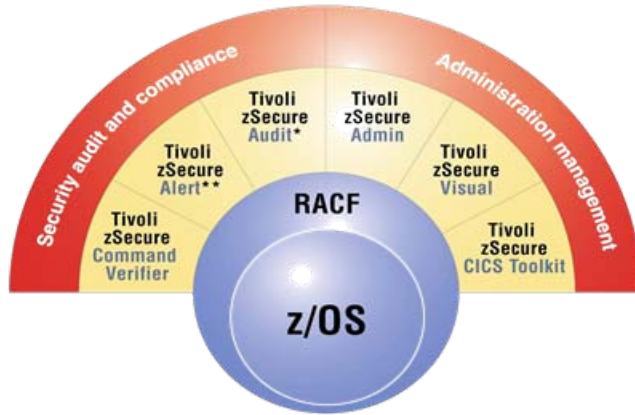
HP-UX



IBM ISS server protection provides multilayered prevention technologies to help you prevent server intrusion.



Evolution of Security: Adding a Security Layer to the Platforms



Tivoli zSecure adds:

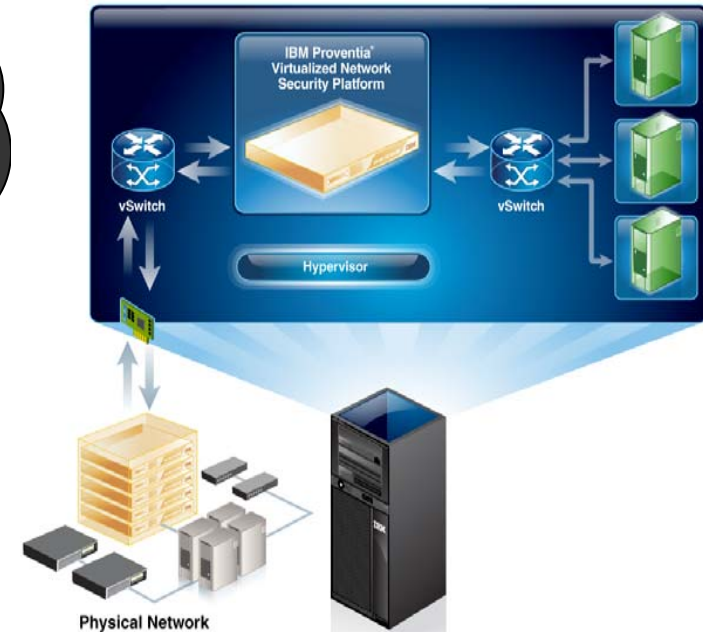
•End to end mainframe security:

- Access control and provisioning
- Monitoring and compliance remediation



Proventia Server Security adds:

- Multi-layered security
- File Integrity Monitoring
- Application control
- Compliance



Proventia Virtualized Security Platform adds:

- Protection for traffic between virtual network segments
- Enables security to be delivered in the cloud

Bsafe: La gestione della sicurezza dei dati su System i

Bsafe / iSeries

Bsafe/Enterprise Security For IBM System i.

Bsafe/Enterprise Security

E' una soluzione di sicurezza globale per i sistemi System i per prevenire l'uso improprio del sistema. È una combinazione di strumenti di controllo degli accessi al Server System i per exit-point, monitoraggio, auditing, reporting, allarme IDS e gestione della sicurezza normalizzati in un unico prodotto. Le sue funzioni di controllo ed analisi sono gestite attraverso un'interfaccia GUI di facile utilizzo.

Bsafe/Enterprise Security

Utilizza un'architettura di tipo client/server. Il software principale di protezione e reporting risiede internamente sul Server System i fornendo una protezione nativa, mentre le definizioni ed il controllo sono gestite per mezzo di una interfaccia GUI semplice ed intuitiva installabile su uno o più computer della rete Aziendale.

Bsafe/Enterprise Security

Fornisce la risposta univoca ai problemi chiave affrontati dai dirigenti aziendali e dal personale addetto alla sicurezza dei Server's System i in questa odierna epoca della conformità e controllo delle informazioni Aziendali.

Progetto di Implementazione Bsafe.

Settore: Credito al Consumo.

Le principali applicazioni del cliente, specializzate per la gestione di finanziamenti e credito al consumo risiedono su una partizione dedicata di un Server System i. Nel tempo parte di queste applicazioni 5250 sono state riviste o ridisegnate adottando una architettura SOA. Il server System i e la sua partizione di produzione sono diventati DataBase server di applicazioni che possiedono e pubblicano servizi web.

Business challenge:

A seguito della crescita del volume di affari, del turn over in azienda del personale di Front Office, dell'utilizzo di applicazioni web è stato richiesto al reparto IT dell'azienda di normalizzare le procedure e gli strumenti utili a garantire adeguata sicurezza nell'accesso ai dati sul server System i così come ad aumentare l'efficienza delle misure di controllo in atto.

Solution:

Attraverso l'adozione del prodotto Bsafe sono state gestite e risolte le richieste fatte al reparto IT dell'azienda. E' stata inizialmente data priorità in materia di sicurezza al controllo, tramite exit program, degli accessi al server System i tramite il protocollo TCP/IP (FTP), successivamente alle richieste DataBase (ODBC) ed in fine alla gestione/storicizzazioni/reportistica delle modifiche di sistema registrate sul System Audit del server System i.

Benefits:

- Bsafe si è rivelato per il cliente uno strumento versatile ed efficiente, ha permesso di rispondere alle richieste della direzione che chiedeva maggior controllo degli accessi, garantendo una facile interpretazione delle informazioni tracciate, rivelandosi uno strumento altrettanto utile per la generazione della reportistica.
- Adottando il prodotto Bsafe il cliente ha avuto la possibilità di conoscere quello che è successo, quando e chi l'ha fatto e, naturalmente, la possibilità di monitorare (e stop, se necessario), ODBC e le attività FTP.
- La creazione in azienda con risorse interne di uno strumento simile, avrebbe richiesto in progettazione, sviluppo e test un numero di ore uomo superiori al costo dell'investimento effettuato con l'acquisto del prodotto.



Grazie.

Fabio Panada
fabio.panada@it.ibm.com

IBM Internet Security Systems