Security for Cloud Development

Carlo Mauceli
Chief Technology Officer Microsoft Italia

Microsoft

Security for Cloud Development

- Dimensione del Fenomeno
- Obiettivi degli Attaccanti
- Vulnerability review
- Minori Privilegi Amministrativi
- Regin – Analisi di un Malware
- Come fare per difendersi ?
- Conclusioni

Microsoft

Dimensione Italiana

875M€

Costo annuale per perdite dirette

8,5B€

(0.6% PIL)

danni di immagine e reputazionali, costi di recovery e perdita di business (dati McAfee).

14,1B€

Perdite dovute ad interruzioni operative dei sistemi

Microsoft

Obiettivi degli Attaccanti

Diffusione

Accesso ai sistemi per propagazione massiva (es. botnet e spam)

Furto di dati

Vantaggi politici o economici

Cybercrime

Vantaggio finanziario (es. furto di carte di credito)

Hacktivism

Diffamazione di organizzazioni (defacement, pubblicazione di dati riservati)

Distruzione

Danneggiamento del business (es. cancellazione dei dati)

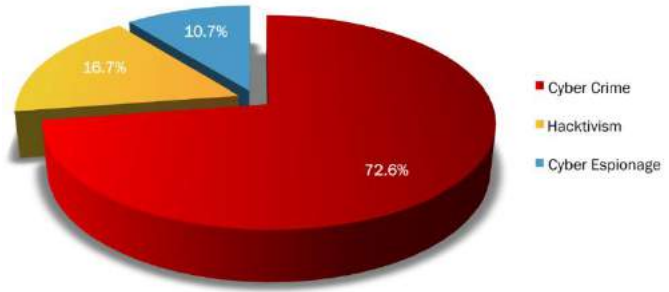
Furto identità

Furto di informazioni personali di clienti, cittadini e di persone in generale

Microsoft

Cybercrime – Le Motivazioni

- Cybercrime (+17% nella prima parte del 2015);
- Hacktivism (-19% nella prima parte del 2015);
- Cyber Espionage (raddoppiato nella prima parte del 2015)



I ricavi dovuti alle attività illecite legate al Cybercrime sono talmente alti che potrebbero ben presto superare quelli relativi al narcotraffico

Microsoft

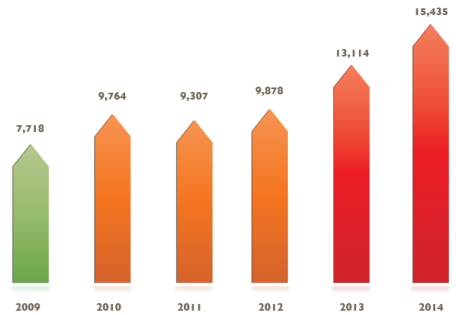
Impatti sul Sistema

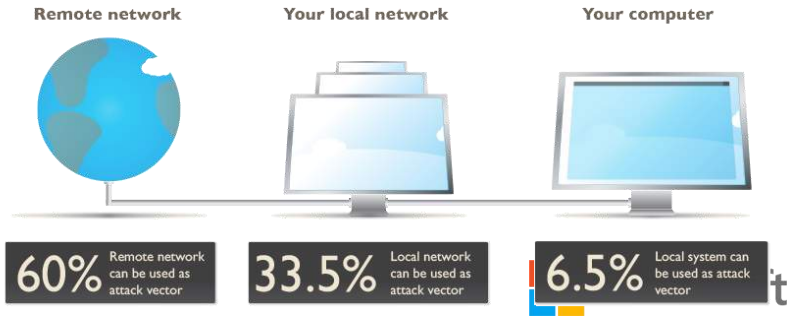
205 giorni in media per identificare una falla di sicurezza

3.5M$ costo medio di una falla di sicurezza

32 giorni per adeguare il sistema

69% delle volte la segnalazione proviene dall'esterno





Fonti: Mandiant M-Trends 2015 Reports – 2013 Ponemon Cost of Data Breach Study - Secunia

Attacchi e Minacce

Social Engineering

23% delle mail phishing viene aperto

11% delle vittime apre l'allegato/link

60% l'attacco ha successo in pochi minuti

Advanced Persistent Threat

Eseguono attacchi avanzati in modo persistente

Una volta all'interno della rete bersaglio tentano la compromissione di sistemi d'interesse

Sfruttano tecnologie del bersaglio (VPN) e strumenti di amministrazione di sistema e persistono anche per anni

Attacchi Zero-day

Vulnerabilità non note ai produttori

Esiste un mercato di compravendita

Interazione minima con la vittima sia nel caso di client (accesso a pagina web) che server (richiesta verso servizi web)

Malware

Programmi creati con lo scopo di eseguire determinati attacchi e sistemi specifici, spesso fatti ad-hoc

Possono distruggere dati, rubare informazioni, compromettere il business della vittima (xes. Stunex per il protocollo SCADA delle centrali nucleari)

Possono essere adattati e scaricare altri malware

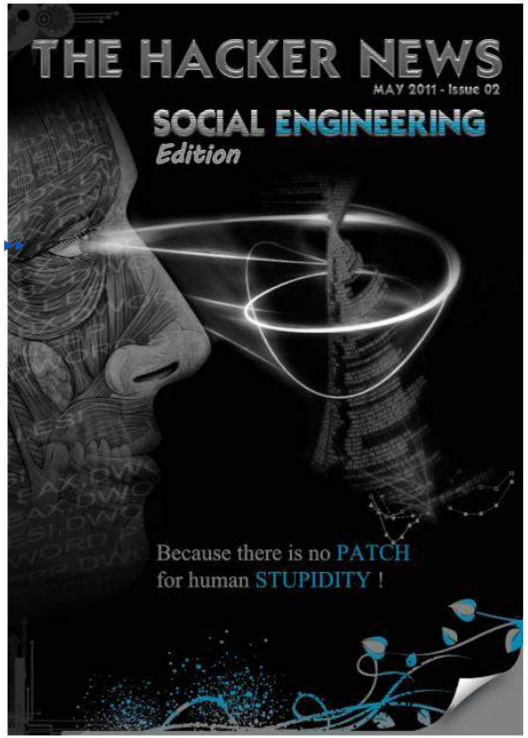
Sintesi del Problema – Semplice no ?

- Una efficace strategia di protezione e mitigazione dei rischi inizia dalla Formazione

- Oggi più che mai gli utenti (e purtroppo anche molti amministratori di rete) rappresentano l'anello debole della sicurezza all'interno di una organizzazione

Microsoft

Sintesi del Problema – Semplice no ?



"People are used to having a technology solution, [but] social engineering bypasses all technologies, including firewalls. Technology is critical, but we have to look at people and processes. Social engineering is a form of hacking that uses influence tactics."

Kevin Mitnick

Microsoft

Partner led today and tomorrow

- Si stima che ogni giorno vengono scoperti più di 300.000 varianti di MALWARE (Malicious Software)
- Sfortunatamente molte Aziende usano un metodo antiquato di rilevazione delle "infezioni da malware"
- Ciò in quanto, la maggior parte dei computer sono configurati usando la filosofia "*trust everything that runs*": quindi consentono l'esecuzione di un processo ancora prima che il sistema di monitoraggio (solitamente basato sull'analisi della presunta firma/impronta del malware) rilevi l'evento come una forma di attacco
- Quindi, solo dopo l'entrata in azione del malware, il "sistema antimalware" tenta di ripulire il computer ed assicurare che l'infezione non si ripeta ☹

Microsoft

Lavorare con Privilegi Minimi

Vulnerabilità che possono essere mitigate rimuovendo i diritti amministrativi

92%	96%	100%	91%
delle vulnerabilità segnalate come Critiche da Microsoft	delle vulnerabilità Critiche di Windows	di tutte le vulnerabilità di Internet Explorer	delle vulnerabilità di Office

"Symantec's senior vice president for information security estimates antivirus now catches just 45% of cyberattacks."

The Wall Street Journal, May 4, 2014

Microsoft

Mappa Attacco - Difesa

PROBLEMI

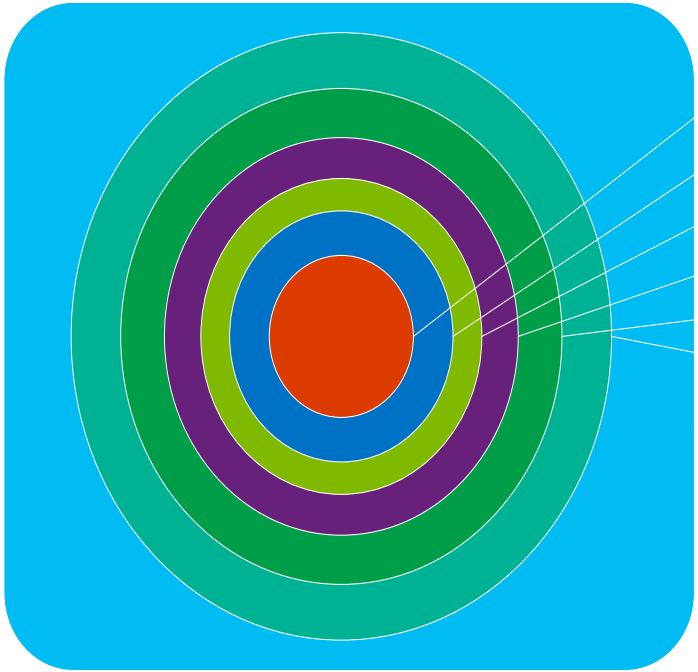
- Impersonificazione dell'utente
- Fuga di informazioni
- Intercettazione dei dati in transito
- Alterazione dei dati in transito
- Diffusione di malware
- Compromissione del dispositivo

CONTROMISURE

- Attivazione di funzionalità di blocco
- Disattivazione delle funzioni disattivate
- Securizzazione delle app
- Installazione di programmi anti-malware
- Aggiornamento costante dei dispositivi

Microsoft

Come fare per difendersi ?



Data
Application
Host
Internal Network
Perimeter
Physical
Policies
Procedures
Awareness

Misure a livello Client

- Lavorare con privilegi minimi
- Utilizzare le Universal Apps
- Mantenere i sistemi aggiornati
- Utilizzare un Antivirus
- Utilizzare EMET
- Aggiornare a Windows 10
- Aggiornare l'HW

Misure a livello infrastrutturale

- Controllare oggetti AD scaduti
- Controllare oggetti AD inutilizzati
- Controllare membri Domain Admins
- Controllare membri Enterprise Admins
- Impostare password complesse
- Impostare durata minima password
- Impostare il blocco account
- Controllare i permessi su share
- Verificare funzionalità backup e restore

https://channel9.msdn.com/Blogs/MVA-Active-Directory-e-oggetti-scaduti

Microsoft Security Platform

Data

1110
1110 1110
1010 1010
1010 1010 1010

Cloud & Datacenter

Applications
(Office 365, SaaS)

Endpoints (Windows 10, Devices)

Device Guard, Credentials Guard,
Windows Hello, Windows Defender,
Windows Advanced Threat Detection

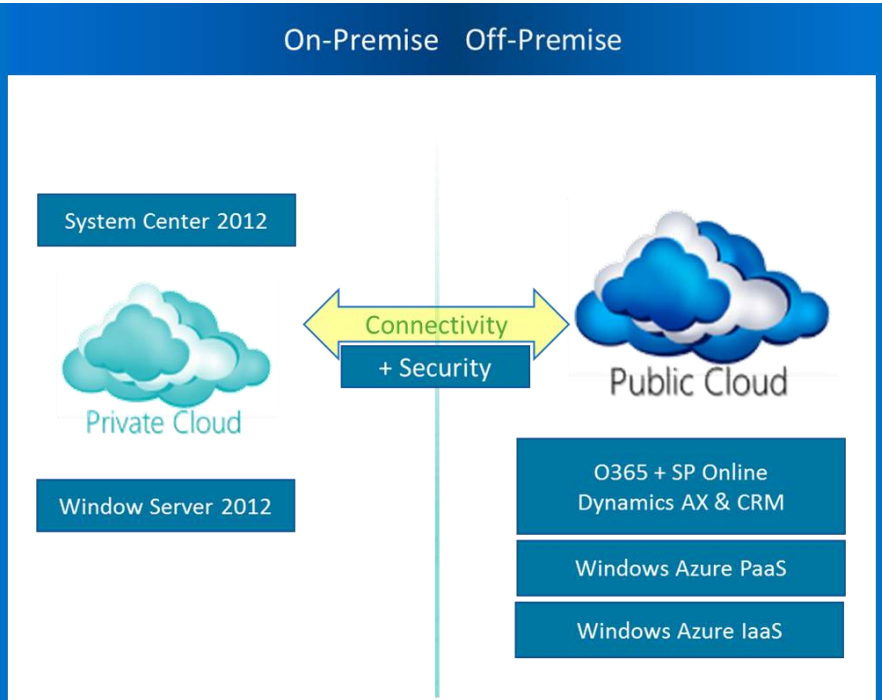
Identity

Il Cloud aiuta a mitigare il rischio

Cloud

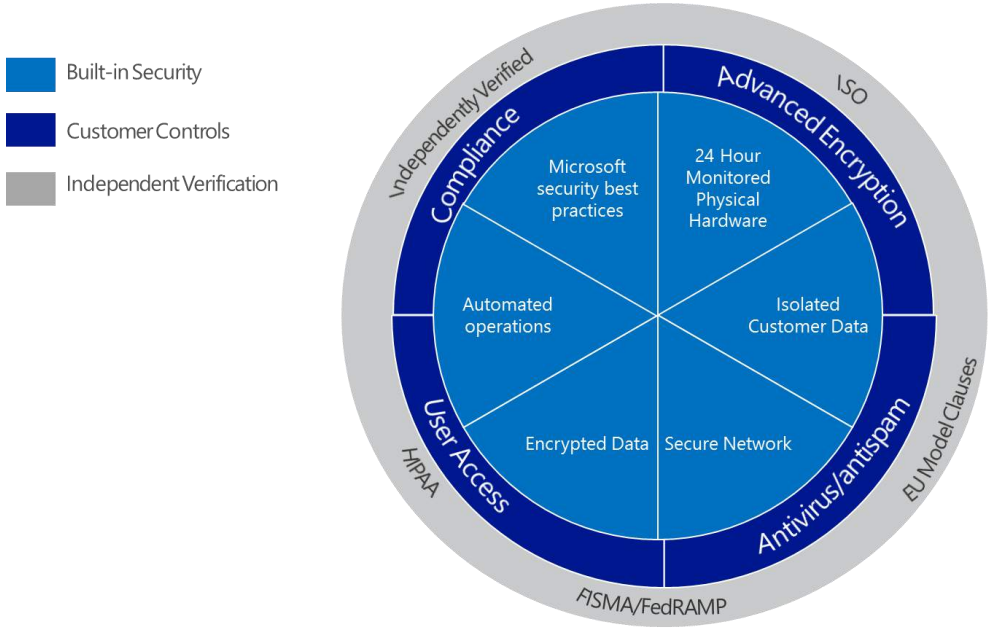
Più dell'**80%** di **nuove apps** sono state distribuite o installate in cloud dal **2012**

70% delle organizzazioni Stanno analizzando o utilizzando le **soluzioni di cloud computing**



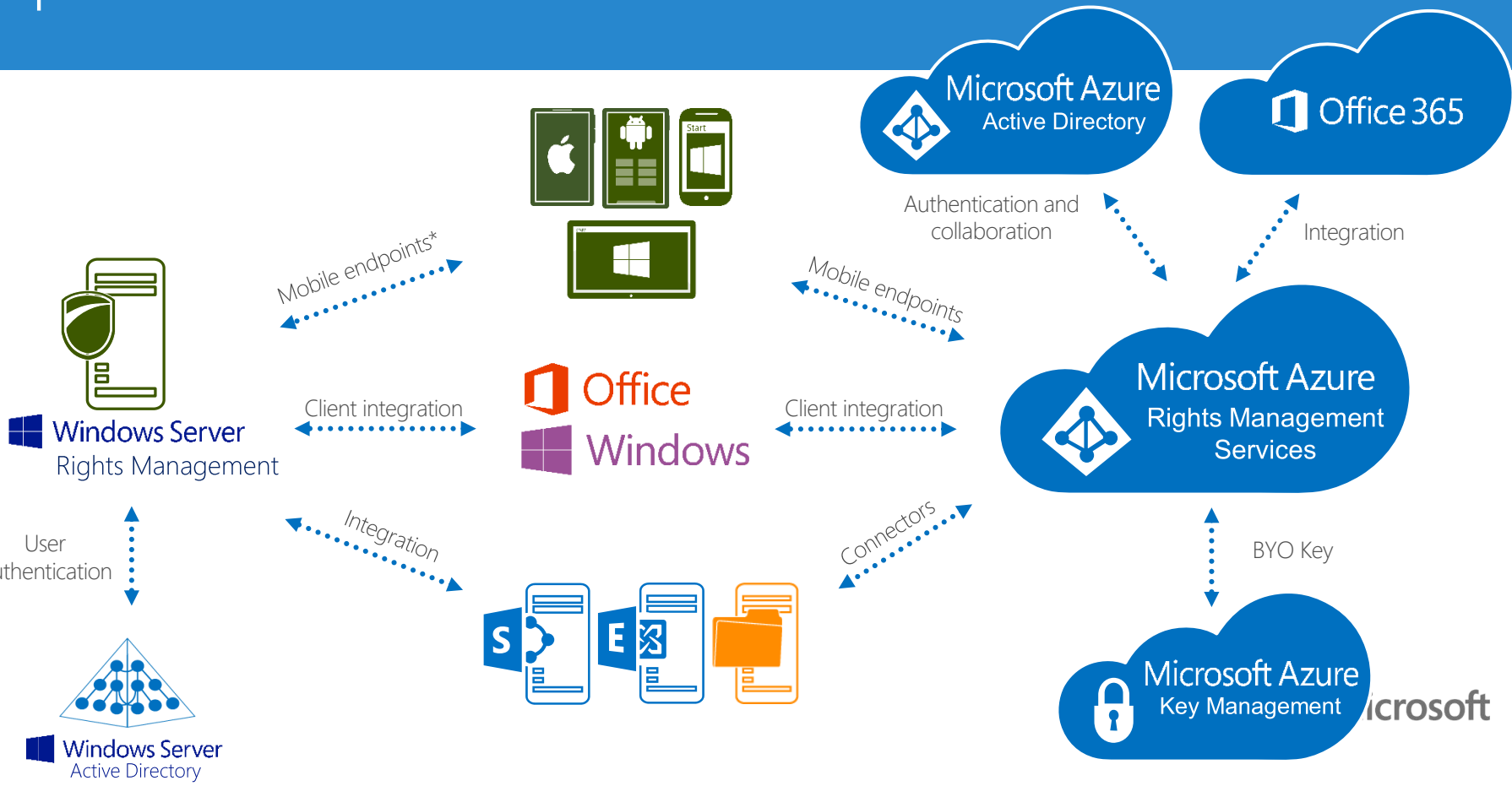
- Progettato da zero per la sicurezza; lo sviluppo di Azure aderisce al modello Microsoft SDL.
- Aderisce a una serie rigorosa di controlli di sicurezza che regolano supporto e operation.
- Sviluppa una combinazione di fattori preventive, reattivi e di difesa.
- Controlli di accesso stretti sui dati sensibili, tra cui l'autenticazione a due fattori per eseguire operazioni sensibili.
- Controlli che migliorano la rilevazione di attività dannose in modo indipendente.
- Livelli molteplici di monitoraggio, logging, e reporting.
- Servizio di incident response 24x7 che mitiga il rischio di attacchi e le attività malevolre

Online Services Security



Microsoft

Ipotesi di scenario architetturale in Cloud



Conclusioni

- La superficie di attacco complessivamente esposta dalla nostra civiltà digitale cresce più velocemente della nostra capacità di proteggerlo.
- I difensori, non riescono ad essere abbastanza efficaci: a fronte di crescenti investimenti in sicurezza informatica, (+8% nel 2014) il numero e la gravità degli attacchi continuano ad aumentare, in un contesto nel quale, peraltro, si stima che 2/3 degli incidenti non vengano nemmeno rilevati dalle vittime.
- Ci si troverà in un mondo completamente integrato in cui la sicurezza informatica potrà dipendere dal contesto specifico. Questo comporta la nascita di un nuovo approccio alla gestione della sicurezza, non più basato sulla compliance ma da un'attenta analisi dei rischi che consente di applicare misure di sicurezza ad hoc.

Microsoft

Siti di Riferimento

	Sito	Url
No Profit	The Open Source Vulnerability Database (OSVDB)	http://osvdb.org
	Common Vulnerabilities and Exposures (CVE)	https://cve.mitre.org
	CVE Details	http://www.cvedetails.com
	Security Focus Vulnerabilities	http://www.securityfocus.com
Gov	US Department of Homeland Security	http://www.dhs.gov
	US Computer Emergency Readiness Team	https://www.us-cert.gov
Profit	Microsoft Security Research and Defense Blog	http://blogs.technet.com/b/srd
	System Administration, Networking, and Security Institute	https://www.sans.org
	Secunia Advisories	http://secunia.com