Evoluzione della Strategia di Sicurezza

Carlo Mauceli – CTO Microsoft Italia

@carlo_mauceli

Carlo.mauceli@microsoft.com

Agenda

- Cybercrime - Dimensione
- Mitigazione del Rischio
- Catena di Attacco Tipica
- Mitigazioni Critiche
- Prevenzione
- Nuova Direttiva Europea

C’è bisogno di cultura

11 gennaio 2017

L’HUFFINGTON POST

IN COLLABORAZIONE CON IL Gruppo Espresso

Grazie a due fratelli massoni forse questo Paese è entrato nel secolo della guerra digitale.

Eyepyramid, il malware che ha infettato ad opera dei due fratelli Occhionero 18 mila profili web di personaggi sensibili del nostro paese, ci ha trascinato, a nostra insaputa, sulla prima linea del conflitto moderno che sta divampando nel mondo: il controllo delle memorie.

Mentre assistevamo, fra lo scettico e il divertito, alle cronache delle incursioni di hacker nelle elezioni presidenziali americani, riuscendo, nella nostra ignoranza, a fare anche gli spiritosi su come i pifferi di montagna americani venivano suonati dagli intraprendenti ragazzotti russi e cinesi, le mail delle nostre massime autorità erano vetrine di giocattoli per bambini.

Il tema che ora è all'ordine del giorno riguarda proprio la sovranità concreta di uno Stato.

Il punto è che il nostro è uno stato digitalmente in outsourcing, che si appoggia a saperi e competenze estranee e straniere. Gran parte delle memorie Cloud della P.A.è fornito da Amazon. Così ad esempio per la Rai dove la totalità dei suoi algoritmi editoriali sono d'importazione. O per il sistema bancario che si affida completamente a soggetti esterni.

Il punto è : chi sono i reali titolari e amministratori dei dati di questi soggetti, i committenti o gli esecutori dell'appalto? Più concretamente per spiare le amministrazioni pubbliche dello stato italiano non basta contendere i dati ad Amazon o a Google?

Ma non è solo l'apparato statale ad essere vulnerabile e indifeso. Penso ad esempio all'intera infrastruttura della comunicazione italiana, giornali e TV. Chi ne controlla realmente il funzionamento? Pochi fornitori che assicurano le intelligenze e i server attorno a cui si ristrutturano queste imprese editoriali. E il sistema economico, con artigiani e piccole e medie imprese che si affidano a piattaforme estere per gestire i propri market place? E il sistema della formazione che ha affidato a Microsoft l'alfabetizzazione digitale nelle scuole dell'obbligo.

Dimensione del Cybercrime

Social Enginering

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)

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)

Evoluzione degli Attacchi

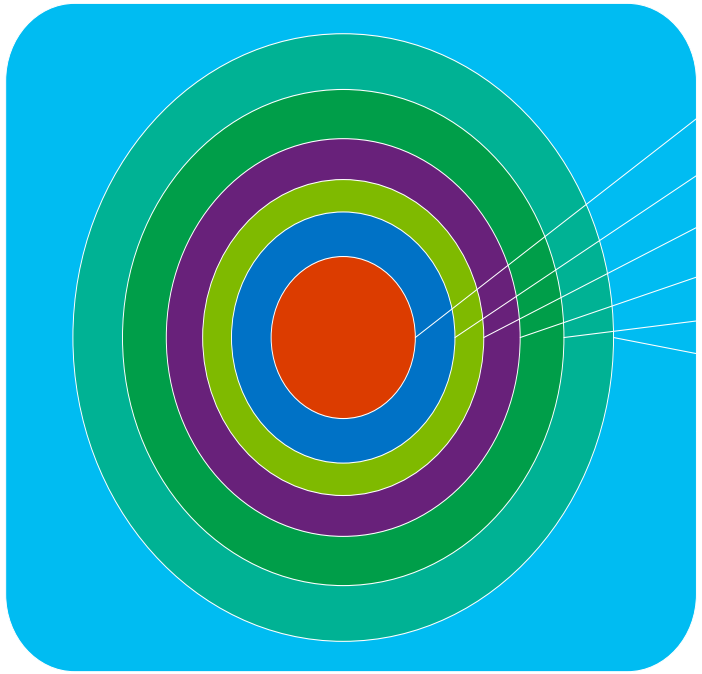
- Si stima che ogni giorno vengono scoperti più di 300.000 varianti di MALWARE (MALicious softWARE)
- Sfortunatamente molte Aziende usano un metodo antiquato di rilevazione delle "infezioni da malware"
- Ciò in quanto, la maggior parte dei computer sono configurati usando la filosofia "*trust everything that runs*": quindi consentono la 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 ☹

Sintesi del Problema

- 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

Mitigazioned el Rischio Lavorare con Privilegi Minimi



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

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

Mitigazioned el Rischio Lavorare con Privilegi Minimi

Vulnerabilità che possono essere mitigate rimuovendo i diritti amministrativi

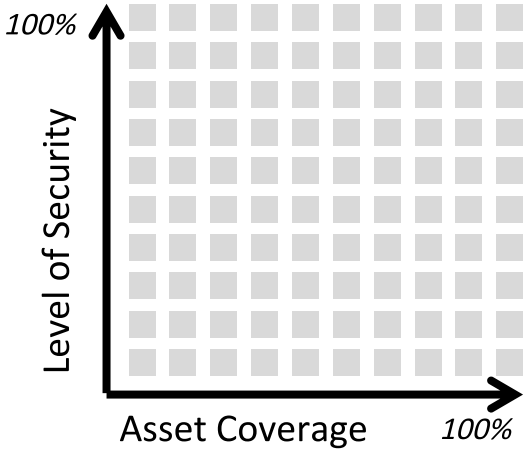
92% delle vulnerabilità segnalate come Critiche da Microsoft	**96%** delle vulnerabilità Critiche di Windows	**100%** di tutte le vulnerabilità di Internet Explorer	**91%** delle vulnerabilità di Office

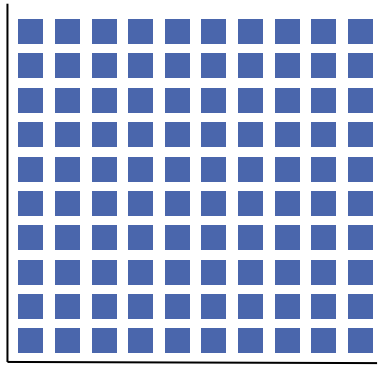
"Symantec's senior vice president for information security estimates antivirus now catches just 45% of cyberattacks."

The Wall Street Journal, May 4, 2014

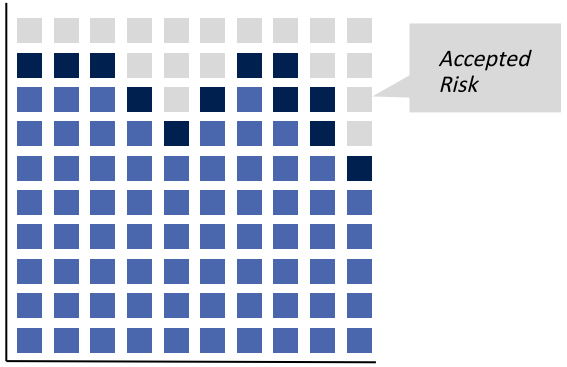
Mitigazioned el Rischio Il Problema

- Problematica complessiva
- Risorse limitate
- Alte aspettative

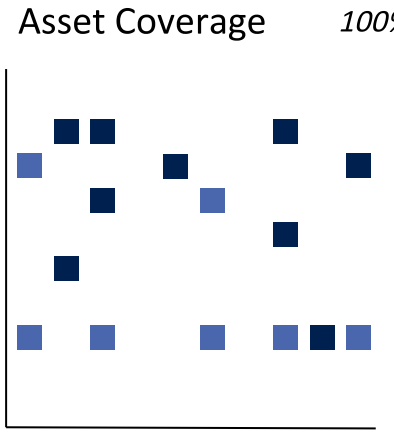




Idealmente …
(quale standard di sicurezza ?

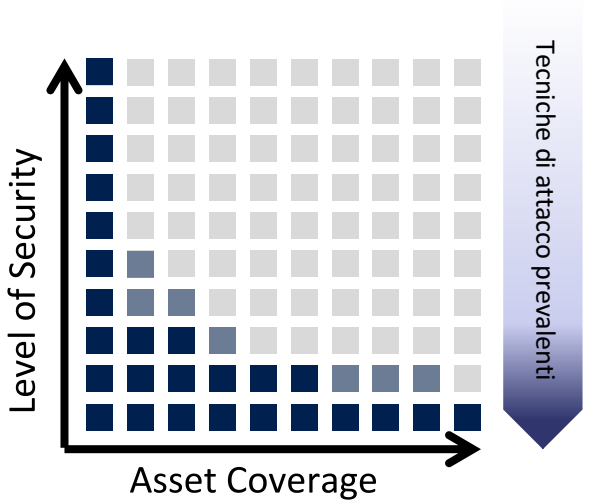


Che tipo di rischio assumere ?



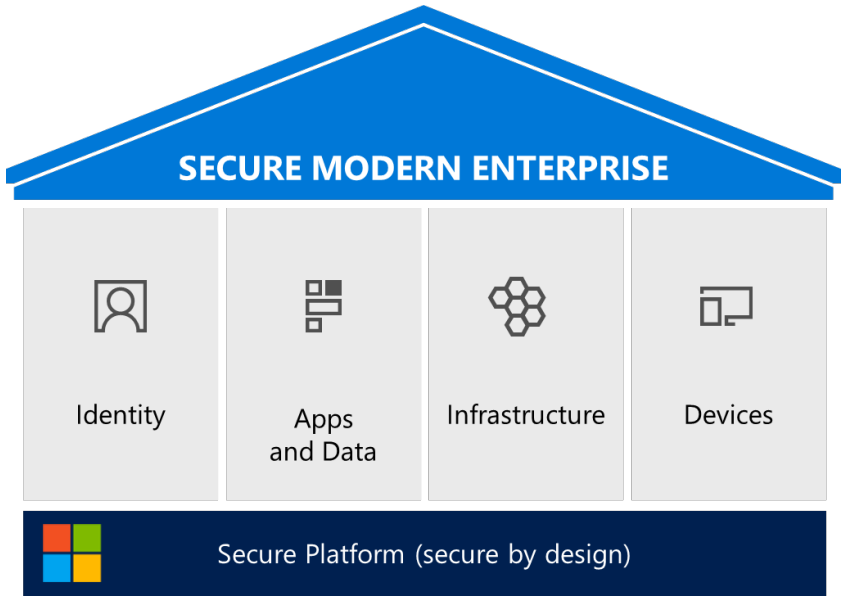
Attuale livello di difesa

Mitigazioned el Rischio Il Problema



1. Riservare investimenti più profondi
2. Prioritizzare le tecniche di difesa in modalità proattiva
3. Fare efficienza (tecnologia/processi/re-use, ecc.)

Mitigazioned el Rischio Definire un approccio moderno



Identità
Considerare l'identity come il perimetro di sicurezza primario e proteggere i sistemi di identità con attenzione particolare sulle credenziali di accesso degli account amministrativi

Apps & Data
Allineare investimenti in security e priorità di business includendo applicazioni, dati e sistemim di comunicazione

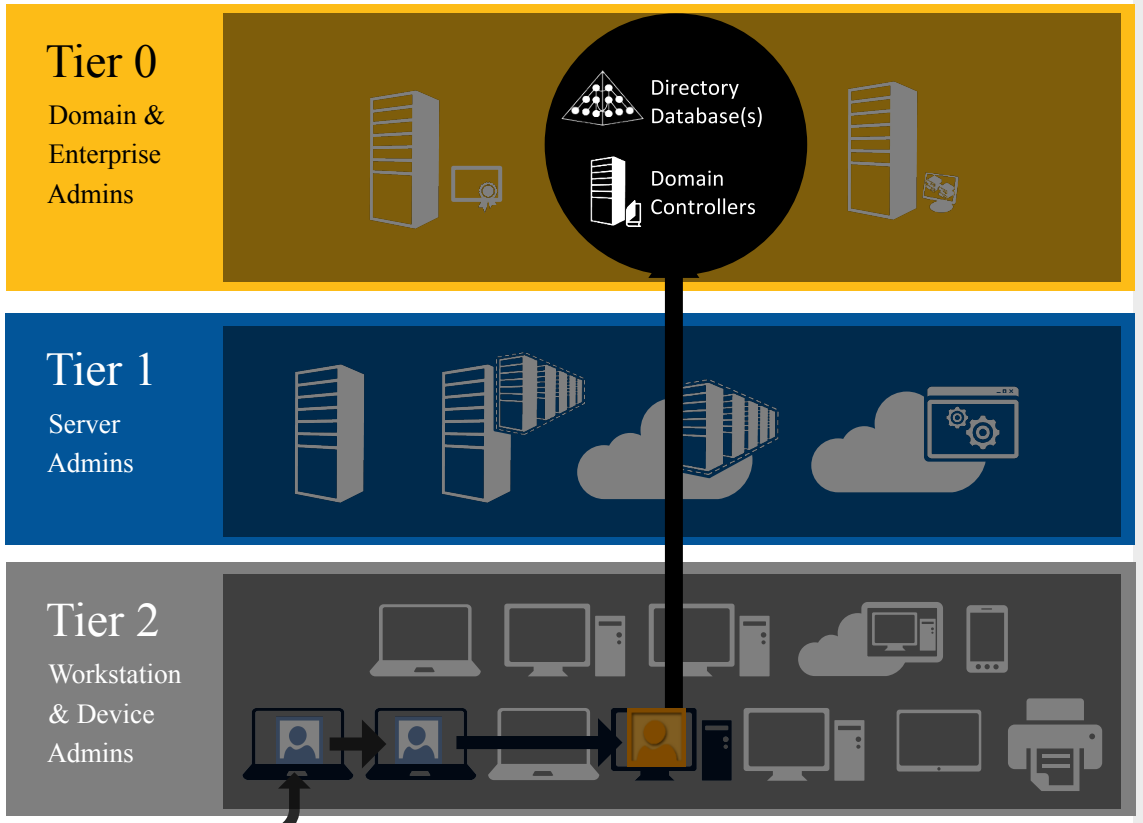
Infrastructura
Operare su piattaforme moderne e utilizzare l'intelligenza del cloud per identificare sia gli attacchi che le vulnerabilità

Devices
Accedere agli asset da "trusted devices" con hardware sicuro, user experience e sistemi di threat detection

Mitigazioned el Rischio Definire un approccio moderno

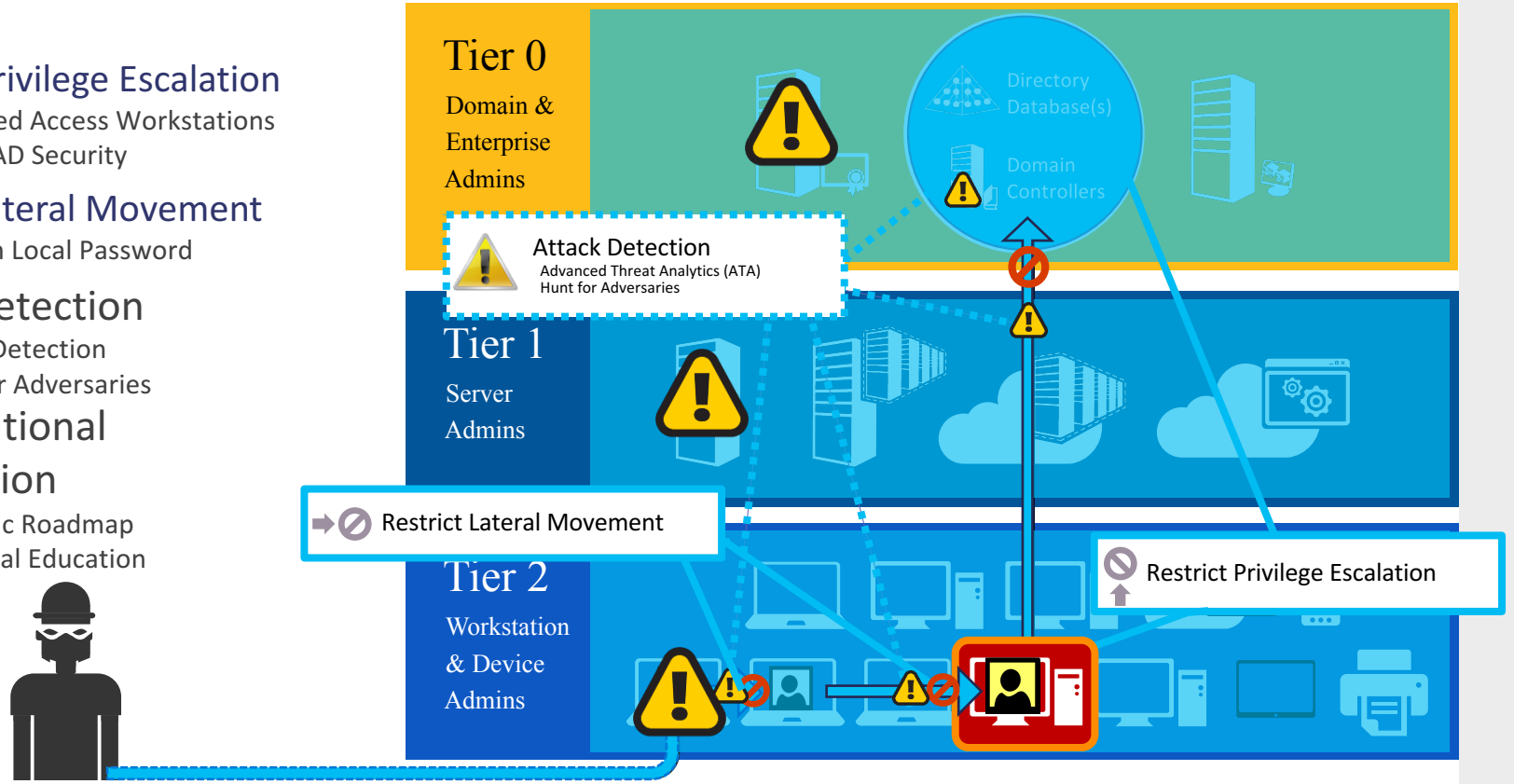
24-48 Hours

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Furto di credenziali
   b. Compromissioni di host e credenziali
3. Aumento dei Privilegi
   a. Ottenere credenziali di Domain Admin
4. Eseguire la missione di attacco
   a. Furto di dati, distruzione dei sistemi, ecc.
   b. Presenza persistente

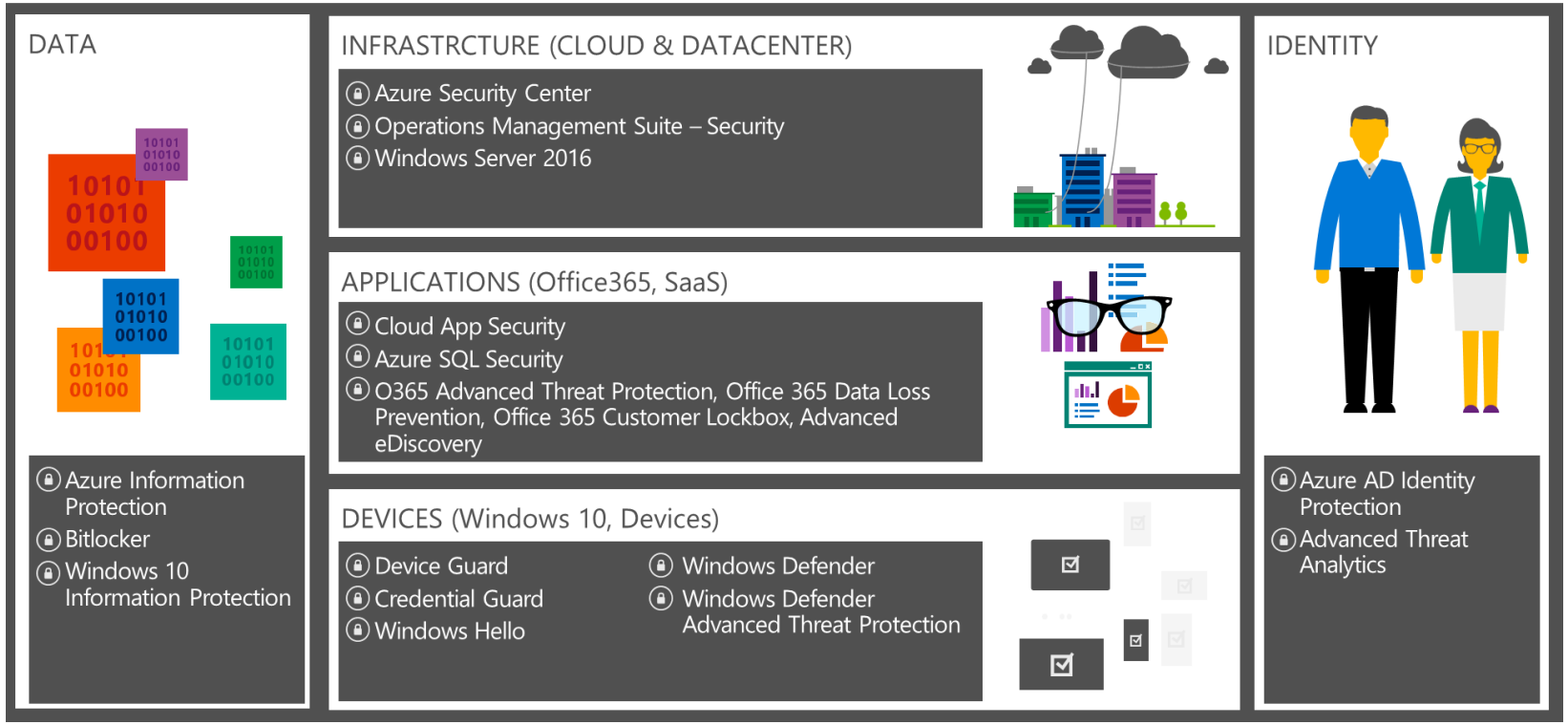


Mitigazioni Critiche

1. Restrict Privilege Escalation
   a. Privileged Access Workstations
   b. Assess AD Security
2. Restrict Lateral Movement
   a. Random Local Password
3. Attack Detection
   a. Attack Detection
   b. Hunt for Adversaries
4. Organizational Preparation
   a. Strategic Roadmap
   b. Technical Education



Microsoft Security Assets

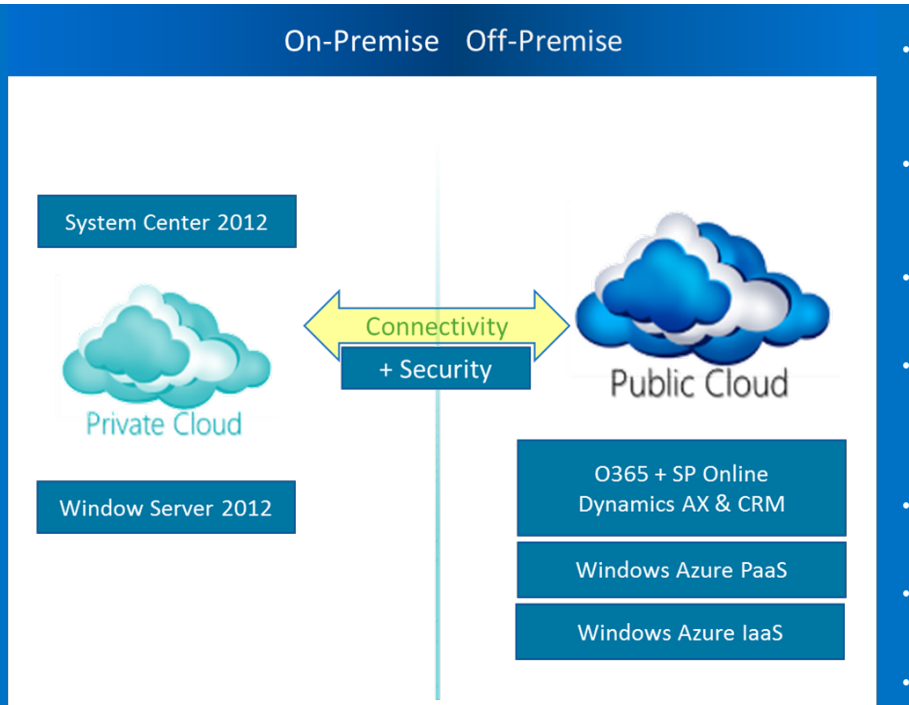


Il Cloud come fattore mitigante

Cloud

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

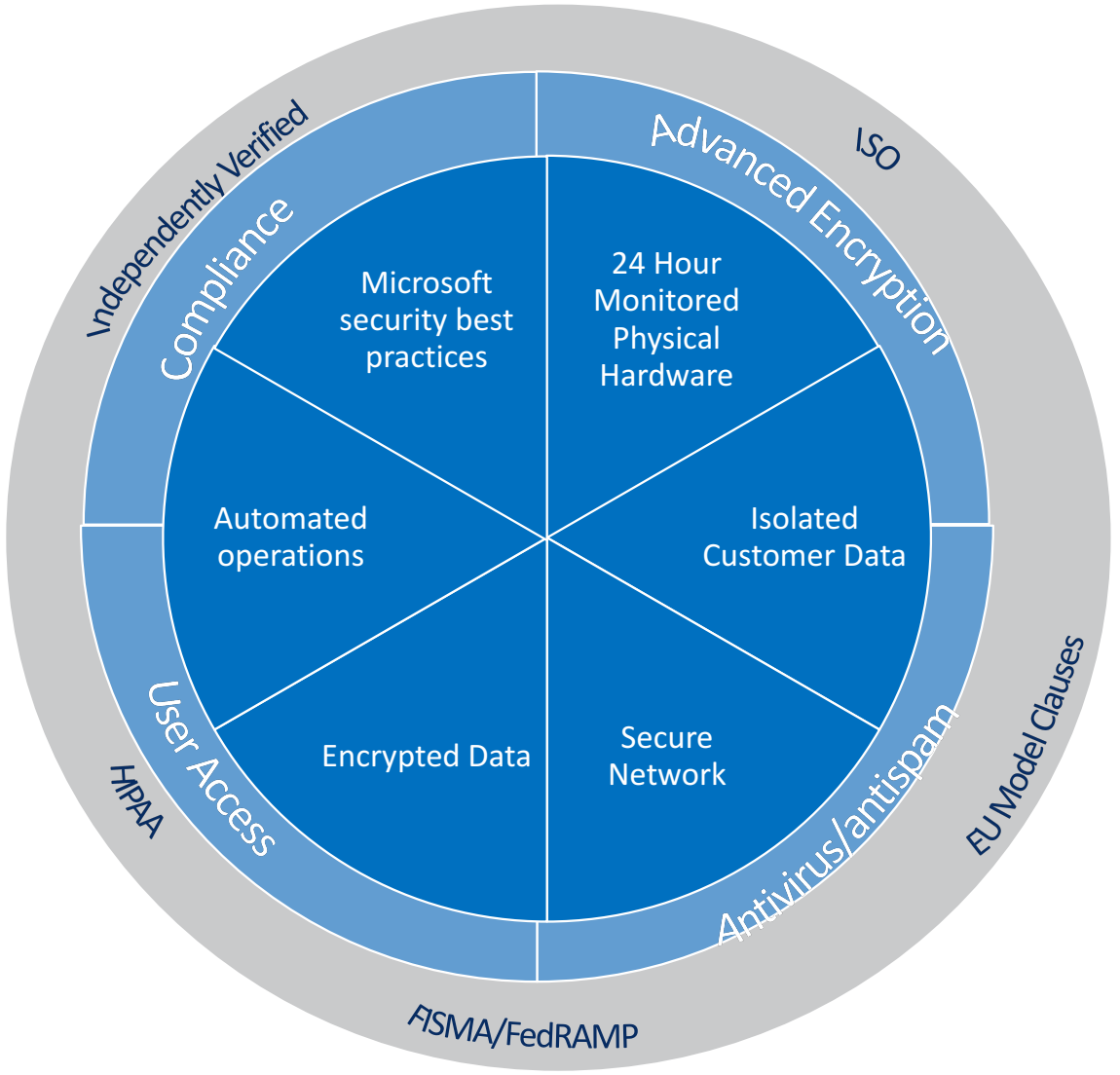
70% delle organizzazioni Stanno analizzando o utilizzando le **soluzioni di cloud computing**



- 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

Il Cloud come fattore mitigante

- Built-in Security
- Customer Controls
- Independent Verification



Microsoft Security Platform

Identity

Protect against identity compromise:

Detect and respond to identity-based threats:

Azure Active Directory Identity Protection

Advanced Threat Analytics

Protect against password attacks:

Windows Hello

Microsoft Passport

Credential Guard

Apps & Data

Boost productivity with cloud access while keeping information protected:

Manage cloud application usage:

Microsoft Cloud App Security

Protect against data leakage:

Azure Information Protection

Office 365 Data Loss Prevention

Windows Information Protection

SQL Server Advanced Threat Protection

Protect against malware and phishing attacks:

Office 365 Advanced Threat Protection

Respond to security incidents:

Office 365 Customer Lockbox, Advanced eDiscovery

Devices

Ensure device security while enabling mobile work and BYOD:

Protect against malware attacks:

Windows Defender

Device Guard

UEFI Secure Boot

Trusted Boot

Manage mobile devices and applications:

Windows Intune

Respond to malware attacks and APTs:

Windows Defender Advanced Threat Protection

Infrastructure

Hybrid environments demand a new approach to infrastructure security:

Gain visibility into your security health:

Azure Security Center

Operations Management Suite Security

Protect against threats:

Microsoft Azure, Windows Server, SQL Server

Detect and respond to threats:

Microsoft Azure Security Center

Microsoft "OMS Security"

INTELLIGENT SECURITY GRAPH

Industry Partners

Antivirus Network

CERTs

...

Cyber Defense Operations Center

Malware Protection Center

Cyber Hunting Teams

Security Response Center

Digital Crimes Unit

...

Conditional Access

Cloud App Security

Event Management

Rights Management

Key Vault

Security Center

...

Active Protection Service

Windows Update

Office 365 Advanced Threat Protection

SmartScreen

Advanced Threat Analytics

Azure Active Directory

Active Directory

Identity

Office 365

PaaS

IaaS

SaaS

Apps and Data

Infrastructure

Device

Global Data Protection Regulation

The new EU GDPR

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws.

You have to comply with GDPR by May 2018.

Here's what it means for your business:

Tough penalties: fines of up to:

4% of annual global revenue or **€20 million** whichever is greater

The **definition of personal data** is now broader and includes identifiers such as:

genetic & biomedical | ip & devices | online | location | cultural & social | economic | mental | pseudonymised

Obtaining consent for processing personal data must be clear, and must seek an affirmative response. YES

Data subjects have the **right to be forgotten** and erased from the records.

Controllers must have a **legal basis** for processing and collecting personal data.

Users may request a copy of personal data in a **portable format**.

The appointment of a **data protection officer** (DPO) will be mandatory for companies processing high volumes of personal data.

Controllers must report a **data breach** no later than **72 hours** after becoming aware of the breach.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Data Processors can be held **directly liable** for the security of personal data.

Data controllers must ensure adequate contracts are in place to **govern Data Processors:** the entire contract chain must comply with the GDPR.

Global Data Protection Regulation Obblighi

Fa obbligo a tutti gli Stati Membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;

Istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di Informazioni tra gli Stati Membri;

Crea una rete di gruppi di intervento per la rete informatica in caso di incidente (rete CSIRT);

Stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;

Global Data Protection Regulation Obiettivi

La direttiva ha l'obiettivo di promuovere la cultura del risk management e incoraggiare lo scambio di Informazioni tra il pubblico e il privato con una strategia preventiva.

- Sicurezza dei sistemi e delle infrastrutture;
- Gestione degli incidenti;
- Gestione della continuità operativa;
- Monitoraggio, audit, testing;
- Conformità a standard internazionali.

Conclusioni

- La superficie di attacco complessivamente esposta dalla nostra civiltà digitale cresce più velocemente della nostra capacità di proteggerla.
- 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.


Grazie

Domande e Risposte

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