Sicurezza nelle grandi organizzazioni

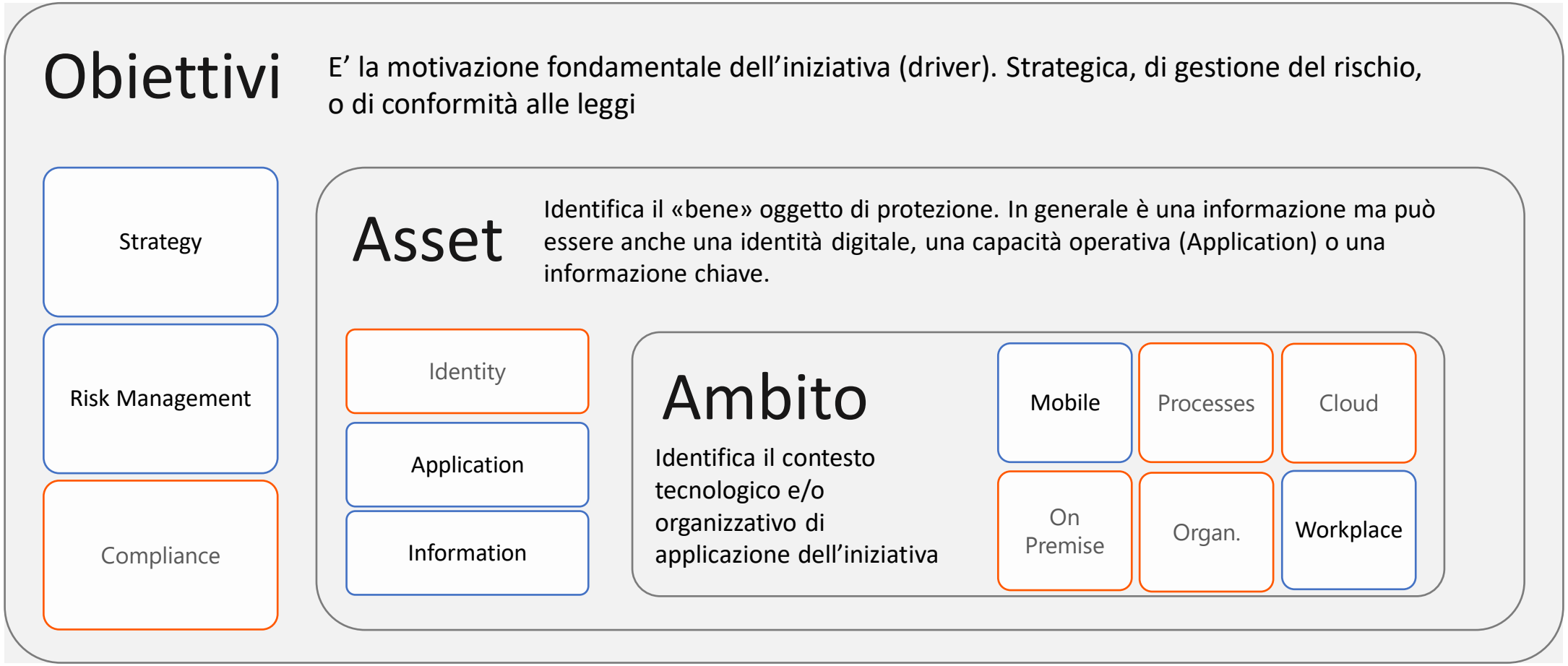
Fabio Vernacotola, Luigi Dragone

16/12/2021

Sezione 1

Progetti di sicurezza, perché…

Iniziative di sicurezza delle informazioni



Obiettivi strategici

- Direttamente correlati al core business dell'organizzazione
- Forniscono all'organizzazione un vantaggio competitivo

Esempi:

- Fornitore di servizi che offre servizi «sicuri» ai propri utenti (Marketing)
- Organizzazione che certifica ISO27001 i propri processi produttivi per poter accedere a gare pubbliche

Risk Management

…evitare gli incidenti ovvero l'impatto economico relativo alla perdita di:

- Riservatezza;
- Integrità
- Disponibilità

Panasonic

Press Release

Panasonic Corporation
http://www.panasonic.com/global

November 26, 2021

Notice of Unauthorized Access to File Server

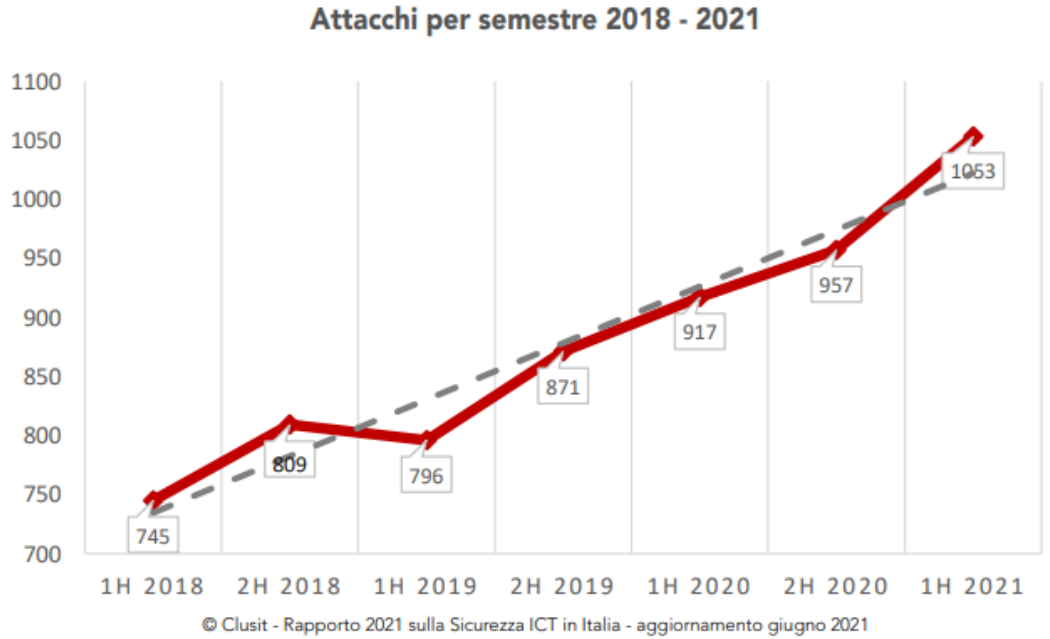
Osaka, Japan - Panasonic Corporation has confirmed that its network was illegally accessed by a third party on November 11, 2021. As the result of an internal investigation, it was determined that some data on a file server had been accessed during the intrusion.

After detecting the unauthorized access, the company immediately reported the incident to the relevant authorities and implemented security countermeasures, including steps to prevent external access to the network.

In addition to conducting its own investigation, Panasonic is currently working with a specialist third-party organization to investigate the leak and determine if the breach involved customers' personal information and/or sensitive information related to social infrastructure.

Panasonic would like to express its sincerest apologies for any concern or inconvenience resulting from this incident.

Rapporto Clusit 2021



World Economic Forum

Risk management

- Rischio = Frequenza di un incidente * impatto del singolo incidente

L'obiettivo dell'organizzazione è quello di:

  - limitare l'impatto;
  - limitare la frequenza;

I rischi di sicurezza possono raggiungere valori economici molto significativi. Secondo l'ultimo data breach report del Ponemon Institute, il costo medio di un data breach nel 2021 è stato di 4,24 milioni di dollari.

* fonte Ponemon Institute 2021

Esempio: infezione ransomware su un server

- Impatto per:
  - Costo per indisponibilità delle applicazioni che utilizzano il server;
  - Costo di ripristino;
  - Costo di inoperatività del personale;

Mitigazione dell’impatto:

- ridondanza dei server;
- immagini virtuali ripristinabili in minor tempo possibile;

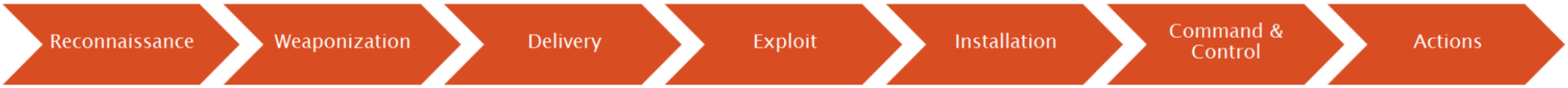
Esempio: infezione ransomware su un server

Ridurre la frequenza

Implementare contromisure come:

- Istruire i dipendenti (Security awareness);
- Limitare l'esecuzione di programmi sui server;
- Limitare l'uso di utenze privilegiate;

- In generale interrompere la *kill chain* tipica degli attacchi ransom



Compliance – Conformità alla norme

E’ un obbiettivo dettato da obblighi di legge:

- Es. Conformità al Regolamento Europeo per la protezione dei dati personali 679/2016 (GDPR)
- Misure minime di sicurezza ICT per le pubblica amministrazioni emanate dall’AgID
- Direttiva NIS

O da accordi/contratti di servizio:

- PCI DSS (Payment Card Industry Data Security Standard)

Sezione 2

Approccio Framework Based per la gestione del sistema di sicurezza aziendale

Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Secondo la ISO27000:

Un SGSI consiste nelle policy, procedure, linee guida e risorse ed attvità associate gestate collettivamente dall'organizzazione allo scopo di porteggere gli asset informativi.

Un SGSI è un approccio sistematico per stabilire, realizzare, condurre, monitorare, rivedere, mantenere e migliorare la sicurezza delle informazioni aziendali al fine di supportare gli obiettivi di business.

Framework di riferimento

- Insieme di «controlli», variamente organizzati, che definiscono cosa una organizzazione deve fare per poter gestire la propria sicurezza informatica.
- I framework rappresentano la formalizzazione di una «best practice» ma possono essere anche di derivazione normativa.
- I framework:
  - consentono una valutazione del proprio livello di sicurezza;
  - semplificano le attività di conduzione del proprio Sistema di Gestione della Sicurezza delle Informazioni;
  - forniscono una base per le attività di audit interno.

ISO/IEC 27001

Dominio

Obiettivo di controllo

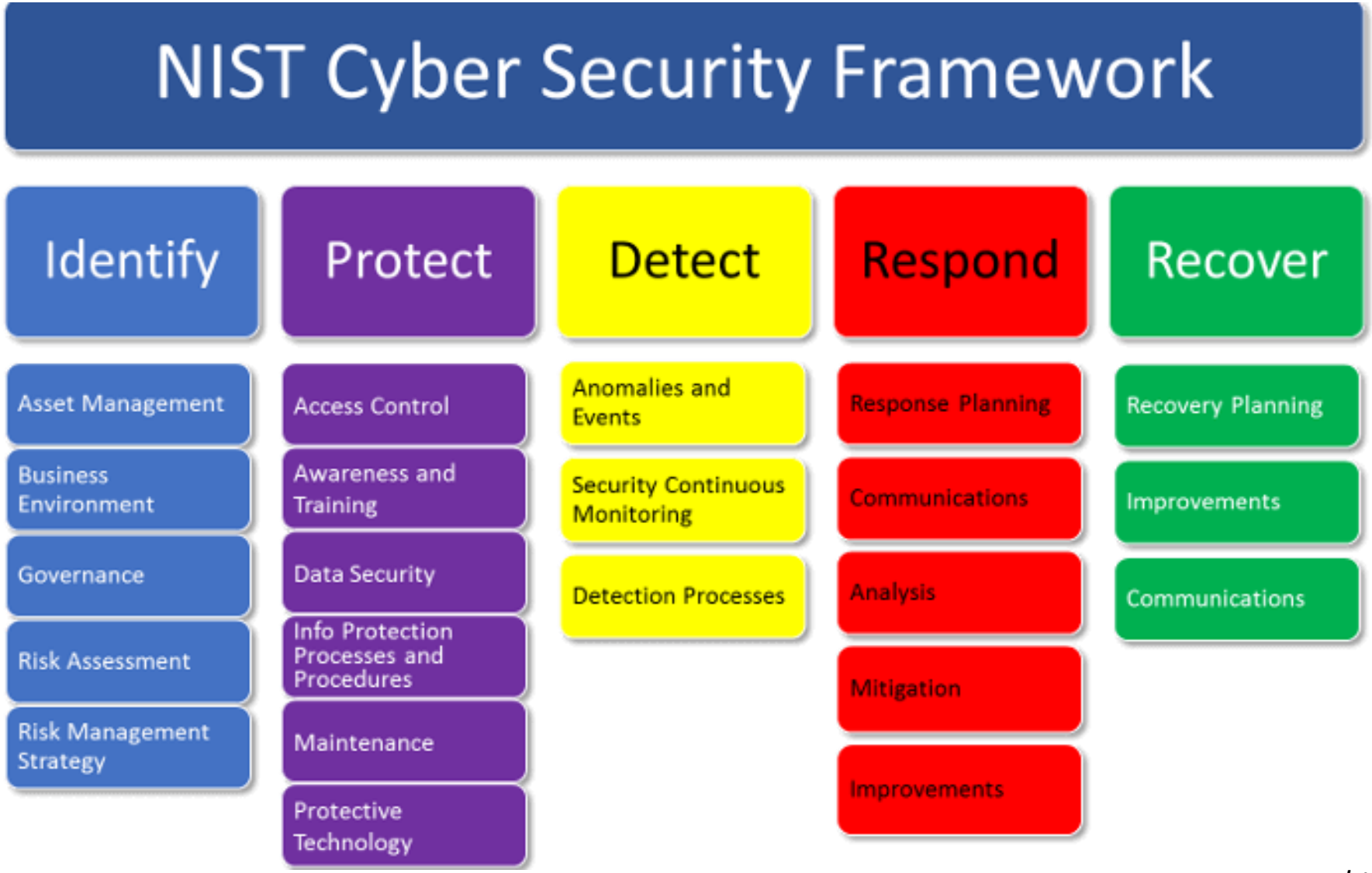
Controlli

A.5 Politiche per la sicurezza delle informazioni		
A.5.1 Indirizzi della direzione per la sicurezza delle informazioni		
Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.		
A.5.1.1	Politiche per la sicurezza delle informazioni	*Controllo* Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	*Controllo* Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

A.13 Sicurezza delle comunicazioni		
A.13.1 Gestione della sicurezza della rete		
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.		
A.13.1.1	Controlli di rete	*Controllo* Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	*Controllo* I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione nelle reti	*Controllo* Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

NIST Cyber Security Framework

National Institute of Standards and Technology

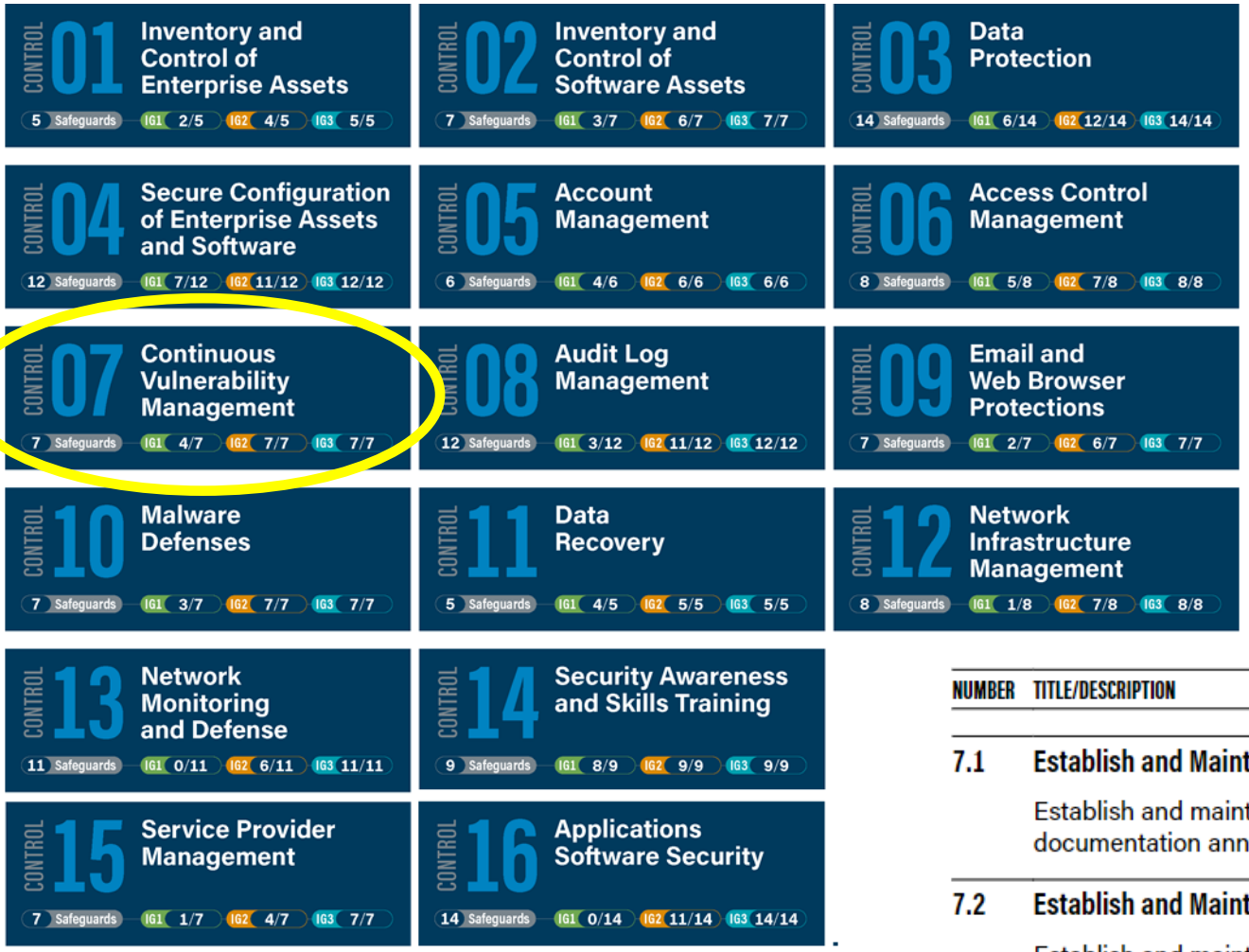


The **National Institute of Standards and Technology** is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness.

https://www.nist.gov/cyberframework

CIS Security Controls

Il Center for Internet Security è un'organizzazione non profit, fondata nell'ottobre 2000. La sua missione è "identificare, sviluppare, convalidare, promuovere e sostenere le migliori pratiche di difesa informatica e costruire e guidare le comunità per creare un ambiente di fiducia in cyberspazio"



NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
7.1	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
7.2	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●

Sezione 3

Cloud Computing

Cos’è il Cloud Computing?

Col il termine Cloud Computing si denota in genere un modello di elaborazione basato su risorse di calcolo, archiviazione e reti disponibile tramite Internet:

- Si tratta essenzialmente di approccio al Computing come Utility (a.e., energia elettrica, telefonia)
- Basato su piattaforme composte da componenti hardware e software integrate tramite reti di trasmissione
- Si appoggia (sovente) sulla rete Internet per fornire i servizi ai clienti / utenti
- Fa ampio uso di tecnologie di virtualizzazione per ottimizzare l’uso delle risorse

Una piattaforma cloud nasconde all’utente la complessità e i dettagli dell’infrastruttura sottostante, offrendo in genere agli utenti un semplice interfaccia grafica oppure un’interfaccia di programmazione (API o web service), abilitando approcci di tipo software-defined

Queste piattaforme, inoltre, possono fornire servizi a richiesta (on-demand), sempre disponibili e accessibili da qualsiasi ambiente

I servizi sono, in genere, elastici e tariffati a consumo (pay-per-use) in base alle richieste:

- Le piattaforme cloud garantiscono elevati livelli di scalabilità

I servizi cloud sono differenziati in base al mercato cui sono offerti come:

- Utenti finali / consumatori / cittadini
- Imprese
- Governi e istituzioni

Caratteristiche del Cloud Computing

Attributi caratterizzanti:

- Accesso tramite rete
- Multi-tenancy e risorse condivise
- Elasticità
- Pay-per-use e servizi a consumo
- Self-provisioning delle risorse
- Risorse disponibili a richiesta (on-demand)

Attributi comuni:

- Elevata scalabilità
- Omogeneità
- Virtualizzazione
- Resilienza
- Distribuzione Geografica
- Service-oriented
- Sicurezza evoluta

Il Cloud Computing vs gli approcci convenzionali

Conventional Computing:

- Eterogeneità
- Fornitura manuale delle risorse
- Hardware dedicato
- Capacità fissa
- Pay per capacity
- OPEX & CAPEX
- Gestito da amministratori di sistema e di rete

Cloud Computing:

- Uniformità
- Fornitura automatizzata (self-provisioning)
- Hardware condiviso
- Capacità elastica
- Pay per use
- OPEX
- Gestuito tramite API / Software Defined (SDDC / SDN)

Modalità di deploy di servizi di Cloud Computing

Cloud Pubblico – servizi cloud forniti da un soggetto terzo (CSP), le risorse possono essere condivise tra più clienti

Cloud Privato – servizi cloud implementati nell'infrastruttura di una singola organizzazione

Cloud Ibrido – Combinazione di cloud pubblico e privato

Cloud di Comunità – servizi cloud implementati in un'infrastruttura di diverse organizzazioni con obiettivi condivisi

Modelli di servizio

Software-as-a-Service (SaaS)

- Consente agli utenti di utilizzare un'applicazione ospitata nell'infrastruttura del fornitore
- Le applicazioni sono accessibili mediante diversi dispositivi (a.e., web, mobile, ecc.)
- L'utente/consumatore non ha nessun controllo o visibilità dell'infrastruttura tecnologica sottostante e può accedere solo alle funzioni applicative espressamente autorizzate
- Esempi: MS Office 365, Google Apps, Salesforce,

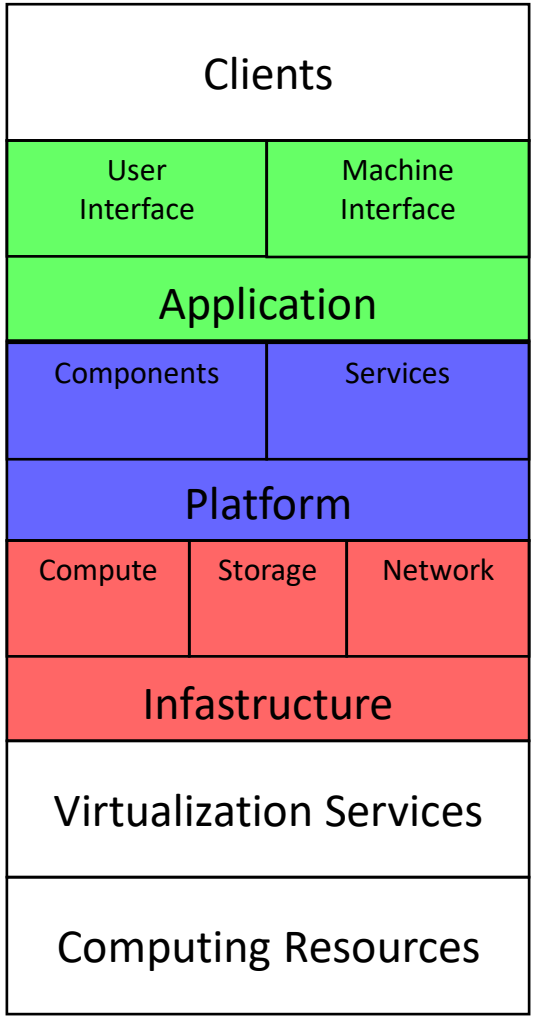
Platform-as-a-Service (PaaS)

- Consente ai clienti di installare ed utilizzare nell'infrastruttura del fornitore delle applicazioni acquistate o sviluppate dal cliente, compatibilmente con le caratteristiche di tale infrastruttura (a.e., linguaggi di programmazione, tool)
- Il cliente non ha nessun controllo o visibilità dell'infrastruttura tecnologica sottostante
- Il cliente ha il controllo delle applicazioni che rilascia e può gestirne la configurazione
- Esempi: MS Azure App Service, Google App Engine, RedHat OpenShift

Infrastructure-as-a-Service (IaaS)

- Consente al cliente di eseguire il provisioning di risorse di calcolo, archiviazione, rete e servizi correlati (a.e., controllo accessi, monitoraggio)
- Il cliente può configurare ambienti di elaborazione in cui installare applicazioni di qualsiasi tipo
- Il cliente non ha il controllo o visibilità dell'infrastruttura sottostante, ma ha il controllo dei sistemi operativi delle macchine virtuali e dei servizi di rete virtualizzati
- Esempi: MS Azure VM, AWS EC2, OpenStack

Stack tecnologico

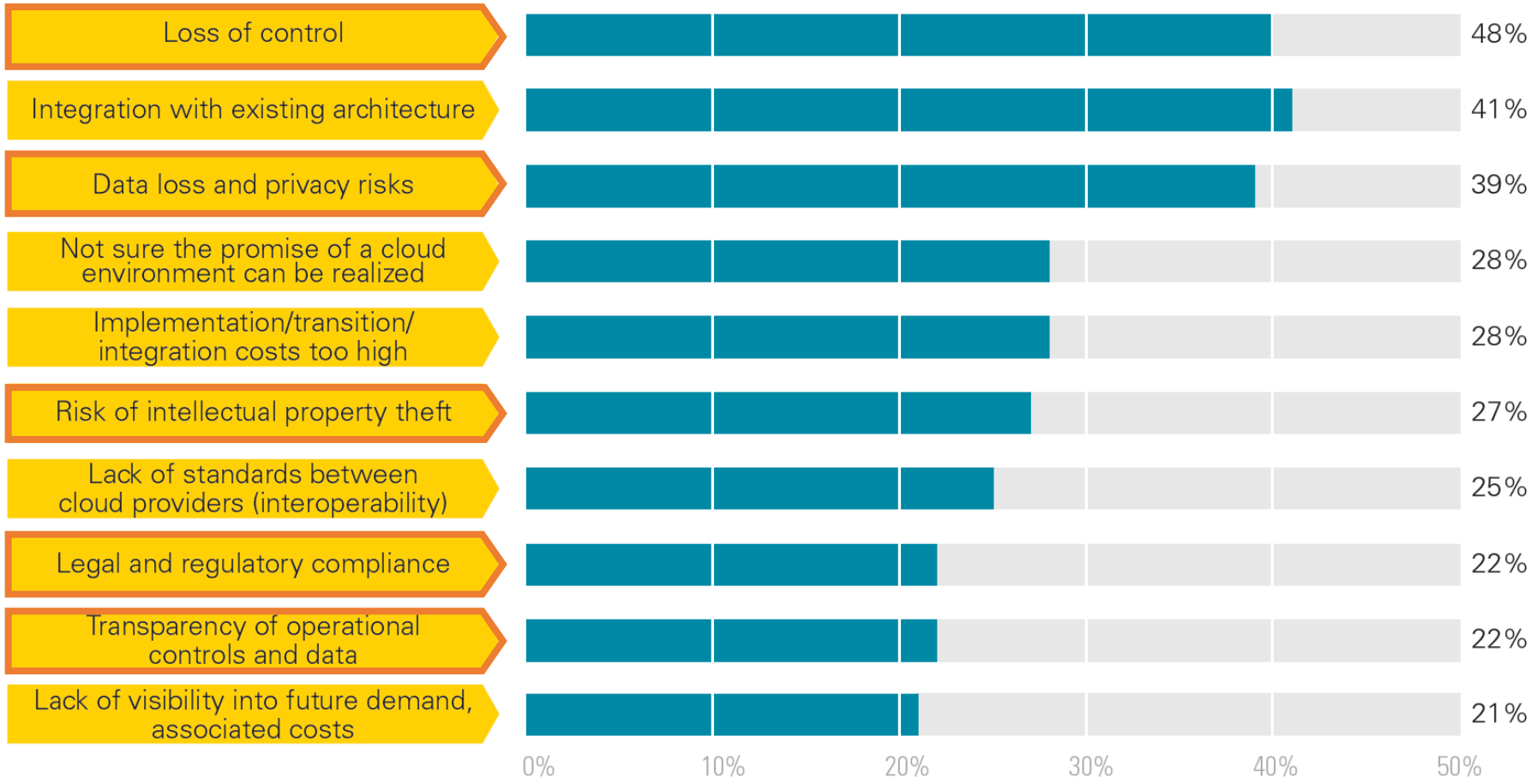


Sezione 4

Cloud Security

Principali criticità dei servizi Cloud nella percezione dei clienti

Nonostante l'indubbio successo del Cloud Computing molti dei principali punti di criticità sono associati ad aspetti di sicurezza e compliance



KPMG International's Global Cloud Provider Survey

Implicazioni del Cloud per la Sicurezza

L’innovazione apportata dal Cloud Computing, sia dal punto di vista tecnologico che di processo nell’offerta di servizi IT evoluti ha diverse implicazioni in termini di sicurezza, sia positive che negative

Contro	Pro
• Rischi derivanti dalla condivisione delle infrastrutture IT • Rischi derivanti dalla perdita di controllo e visibilità sui propri dati	• Nuove opportunità per l’implementazione dei controlli di sicurezza • Nuovi controlli di sicurezza basati sulle piattaforme Cloud (Security-as-a-Service)

Esempi di rischi legati alla condivisione delle infrastrutture IT

Contro

- Rischi derivanti dalla condivisione delle infrastrutture IT
- Rischi derivanti dalla perdita di controllo e visibilità sui propri dati

Condivisione della «cattiva reputazione»

- Indirizzi IP condivisi inseriti in black-list
  - Servizi anti-spam che hanno bloccato gli archi di indirizzamento IP del Cloud Service Provider (CSP) bloccando l'accesso in modo indiscriminato (a.e., Spamhouse con AWS)
- Data-center sequestrato o bloccato

Attacchi cross-tenant / cross-VM

- La compromissione, tramite una VM, dell'hypervisor mette a rischio le altre VM ospitate sullo stesso server fisico, anche se di altri clienti
- La compromissione di un servizio condiviso rende potenzialmente accessibili i dati di diversi clienti
- Un dispositivo di storage riassegnato tra due clienti e non correttamente sanificato può rendere accessibili i dati del vecchio utente al nuovo

Criticità nell'adozione del cloud circa la sicurezza dei dati

Contro
• Rischi derivanti dalla condivisione delle infrastrutture IT
• Rischi derivanti dalla perdita di controllo e visibilità sui propri dati

Limitazione d’uso	Data la facilità con cui in ambienti cloud si possono combinare dati da più fonti, come si può garantire che le informazioni sono utilizzate solo per gli scopi autorizzati / leciti?
Retention	Le informazioni vengono archiviate per un tempo compatibile con le esigenze di protezione? Sono disponibili meccanismi di protezione e backup? Le informazioni vengono conservate anche dopo l’uso consentito?
Cancellazione	Le informazioni sono cancellate in modo sicuro?
Protezione	Quali meccanismi di protezione della sicurezza delle informazioni sono disponibili (a.e., cifratura, controllo accesso, integrità)?
Accountability	Come è possibile identificare eventuali incidenti di sicurezza o furti di informazioni (data breach)?
Accesso	Com’è possibile controllare gli accessi alle informazioni archiviate in cloud? Quali meccanismi di autenticazione, autorizzazione e audit sono disponibili?

Normative circa la protezione dei dati

Contro

- Rischi derivanti dalla condivisione delle infrastrutture IT
- Rischi derivanti dalla perdita di controllo e visibilità sui propri dati

Le criticità legate alla tutela dei dati possono dipendere da requisiti interni all'organizzazione, come da vincoli normativi (a.e., tutela privacy, protezione infrastrutture critiche) o derivanti da standard di settore (a.e., dati finanziari, sanitari)

Le normative di tutela della privacy sono molto eterogenee tra diversi Paesi:

- Le direttive Europee (a.e., EU GPDR) sono molto più stringenti delle normative degli USA (che possono variare da stato a stato)
- La normativa della Cina vieta l'esportazione dei dati sui propri cittadini
- Negli USA, i dati archiviati in cloud pubblico sono meno tutelati di quelli ospitati in server privati, perché possono essere sequestrati senza preavviso

Per ovviare a questi problemi i Cloud Service Provider possono offrire:

- Siti collocati nei diversi Paesi dove installare i propri workload in modo da garantire che le informazioni siano archiviate e gestite in modo compatibile con la normativa locale
- Ambienti differenziati con specifiche certificazioni di conformità (a.e., PCI-DSS per dati sulle carte di pagamento, HIPAA/HITECH per i dati sanitari)

I benefici per la sicurezza delle informazioni

Pro
• Nuove opportunità per l'implementazione dei controlli di sicurezza
• Nuovi controlli di sicurezza basati sulle piattaforme Cloud (Security-as-a-Service)

- Uniformità e semplicità di gestione con meccanismi software-defined, come API, template di configurazione o strumenti automazione
- Distribuzione geografica delle applicazioni e delle informazioni (a.e., off-site storage)
- Disponibilità del dato e dei servizi
- Protezione delle risorse fisiche
- Facilità di ripristino / recovery (a.e. dopo incidente)
- Strumenti di monitoraggio evoluti

Security-as-a-Service

Pro
• Nuove opportunità per l'implementazione dei controlli di sicurezza
• Nuovi controlli di sicurezza basati sulle piattaforme Cloud (Security-as-a-Service)

- E-mail filtering / protection
- Web content filtering
- Vulnerability management
- Identity management
- Security monitoring
- Backup
- Business continuity / Disaster recovery
- Cifratura e gestione delle chiavi

Il modello commerciale del Cloud Computing rende accessibili anche ad organizzazioni medio-piccole controlli di sicurezza evoluti altrimenti appannaggio solo delle grandi organizzazioni o enti governativi

Technology - Azure Security Services

Protect Azure and your entire multi-cloud environment with built-in security, powered by AI.

Access control
Identity and Access Management

Azure Active Directory

Your universal platform to manage and secure identities.

Security Governance
Security Posture Management

Azure Security Center

Security posture management for your hybrid cloud workloads.

Access Control and Asset Protection
Cloud Access Security

Microsoft Cloud App Security

Multifunction visibility, control over data travel, and sophisticated analytics.

Security Operations (SecOps/SOC)
Threat Protection

Azure Sentinel

Intelligent security analytics for your entire enterprise.

Azure Defender

Built-in threat protection for your hybrid cloud workloads.

Azure Defender for IoT

Agentless asset discovery, vulnerability management, and threat detection for IoT/OT devices.

Asset Protection and Innovation Security
Apps and Data Security

Azure Confidential Computing

Protect your data and code while in use in the cloud.

Azure Key Vault

Safeguard cryptographic keys and other secrets.

Azure Attestation

Store and process confidential data with confidence.

Azure Dedicated HSM

Your hardware security module (HSM) in the cloud.

Asset Protection and Innovation Security
Network Security

Azure Firewall

Cloud-native firewall to protect Azure virtual networks.

Azure Firewall Manager

Central network security policy management.

Azure Web Application Firewall

Protect web/mobile apps and APIs from common web vulnerabilities.

Azure Front Door

Fast, reliable and secure cloud CDN with threat protection.

Azure DDoS Protection

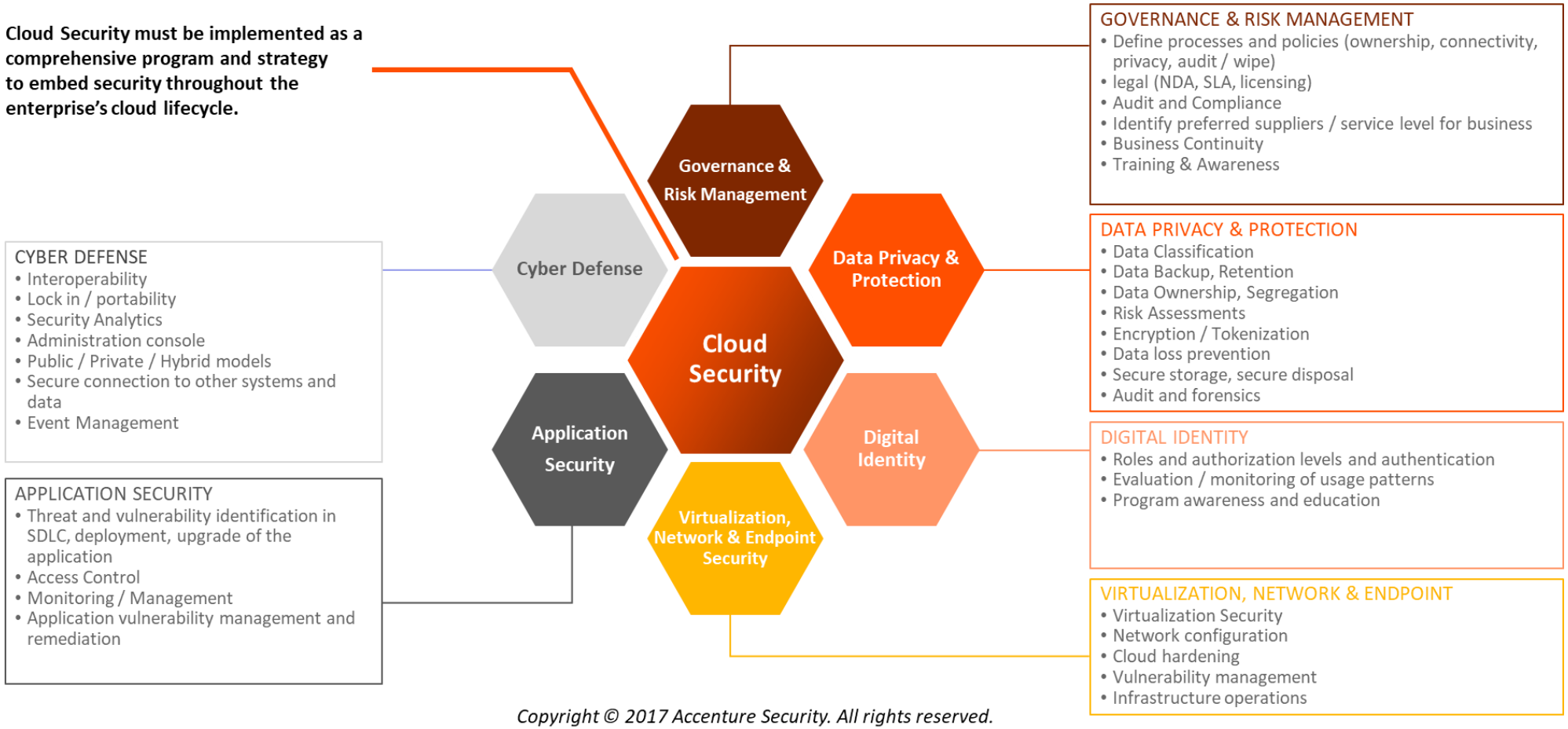
Always-on monitoring to protect against DDoS attacks.

Azure Bastion

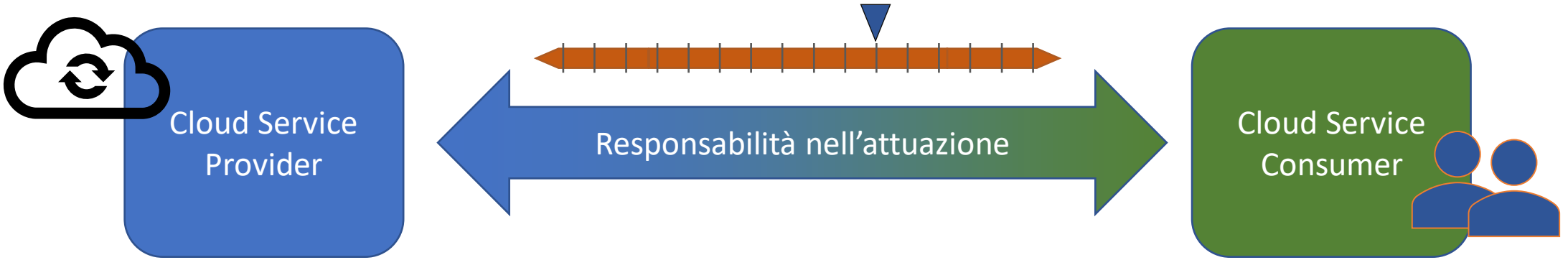
Private and fully managed RDP and SSH access to your VMs.

Componenti di un programma di Cloud Security

Per bilanciare correttamente le esigenze di innovazione e agilità con quelle di protezione e compliance è essenziale che l'adozione delle tecnologie Cloud sia gestito con un programma che tenga in dovuto conto gli aspetti di Information Security



A chi spettano controlli di sicurezza?



Responsabilità del cliente

Gli ambienti Cloud sono condivisi, per cui, il fornitore (Cloud Service Provider – CSP) garantisce la sicurezza dell'ambiente, ma è responsabilità del cliente proteggere le risorse, le applicazioni e i dati che vi colloca

Il CSP può richiedere, ad es., al cliente di:

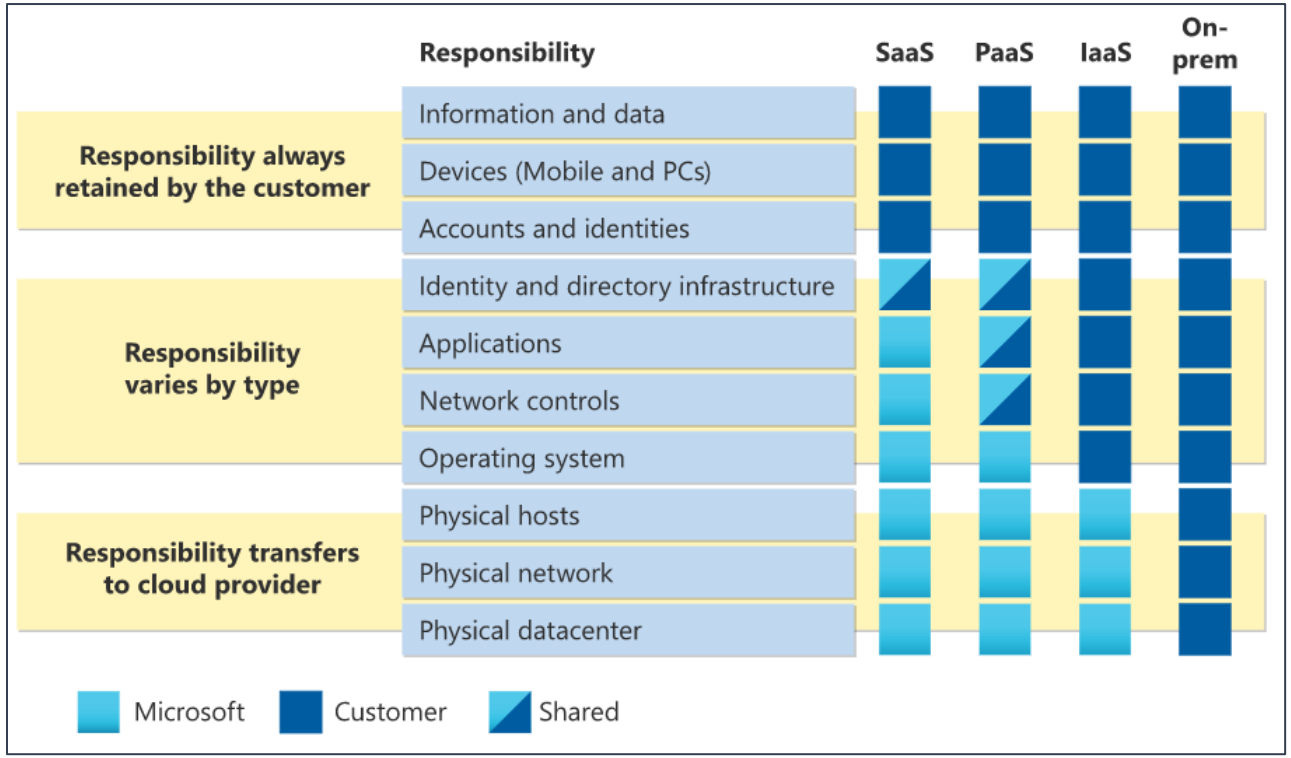
- Aggiornare il sistema operativo delle VM
- Non eseguire port-scan o pen-test
- Ruotare periodicamente password e chiavi
- Eseguire test di vulnerabilità delle applicazioni
- Sanare tempestivamente le vulnerabilità

Sharing the Security Responsibilities

Because you're building systems on top of the AWS cloud infrastructure, the security responsibilities will be shared: AWS manages the underlying infrastructure but you must secure anything you put on the infrastructure. This includes your AWS EC2 instances and anything you install on them, any accounts that access your instances, the security group

Modello di Responsabilità Condivisa

Microsoft Azure Shared Responsibility Model



Cloud Security Frameworks

- **ISO/IEC 27017:2015**:ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: additional implementation guidance for relevant controls specified in ISO/IEC 27002; additional controls with implementation guidance that specifically relate to cloud services. This Recommendation | International Standard **provides controls and implementation guidance for both cloud service providers and cloud service customers**.
- **Cloud Security Alliance Controls Matrix**: is a cybersecurity control framework for cloud computing. It is composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology. It can be used as a tool for the systematic assessment of a cloud implementation, and **provides guidance on which security controls should be implemented by which actor within the cloud supply chain**.

ISO/IEC 27017

Norma elaborata congiuntamente da ISO e IEC, come parte dello standard ISO/IEC 27K, per ridurre i rischi di sicurezza delle informazioni derivanti dall'adozione delle tecnologie del Cloud Computing

Include la definizione di specifici controlli di sicurezza e fornisce le linee guida per l'adozione all'interno di un SGSI

- Ripartizione delle responsabilità tra cloud service provider e cloud consumer
- Restituzione degli «asset» al termine del contratto
- Protezione e separazione degli ambienti virtuali dei clienti
- Configurazione delle risorse virtuali
- Attività amministrative e processi di gestione della piattaforma cloud
- Monitoraggio delle attività dei clienti
- Gestione delle risorse e delle reti virtuali

Cloud Security Alliance (CSA)

- Organizzazione che raggruppa tra i principali fornitori e utenti di soluzioni basate su tecnologie di Cloud Computing espressamente dedicata a favorire lo sviluppo di tecnologie cloud che garantiscano i massimi livelli di protezione delle informazioni
- Si prefigge di:
  - Promuovere un modello condiviso di definizione dei requisiti di sicurezza tra utenti e fornitori di servizi cloud
  - Promuovere lo sviluppo e l'adozione delle buone pratiche di sicurezza
  - Sviluppare e condurre programmi di sensibilizzazione e formazione
  - Sensibilizzare l'opinione pubblica e le istituzioni sull'importanza della protezione delle informazioni in ambiente cloud
- Il programma STAR (Security, Trust, Assurance, and Risk) rappresenta uno dei più importanti standard per la sicurezza degli ambienti cloud
  - Comprende una matrice di controlli di sicurezza specifici per il cloud: Cloud Control Matrix (CCM)
  - Prevede un processo di assessment e certificazione dei fornitori che adottano lo standard con un registro pubblico

Esempio: sicurezza «convenzionale» vs Cloud-based

Network Firewall

Network Firewall

- I network firewall (o firewall) sono tra i principali controlli di sicurezza in ambito rete
- Permettono di implementare policy di controllo del traffico tra reti e host distinti basate su regole formulate considerando i livelli L3-L4 dello stack ISO/OSI

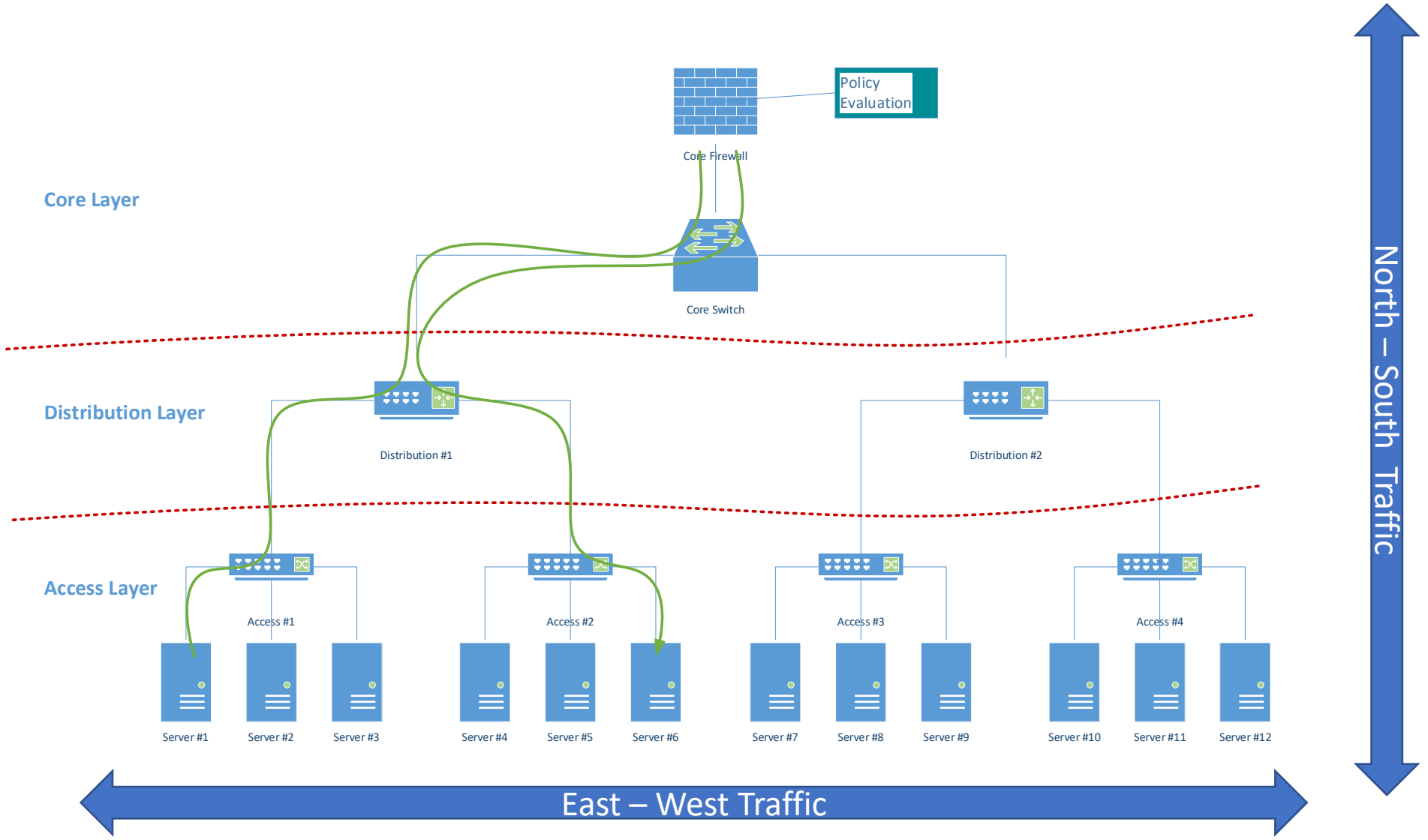
  `Src IP, Src Port, Trg IP, Trg Port ➔ Allow / Deny`
- In generale si parla di Firewall SPI (Stateful Packet Inspection) perché il FW mantiene dinamicamente traccia dello stato della connessione bidirezionale (socket)
- I controlli implementati dai network firewall consentono di:
  - Limitare la superfice di attacco su reti a basso trust (a.e., un server web accessibile su Internet deve accessibile solo sulla porta 443 e protocollo HTTPS)
  - Compartimentare le singole sotto-reti, suddividendole tra ambienti e applicazioni distinte, abilitando il solo traffico lecito / autorizzato
  - Limitare l'impatto di un incidente (a.e., da un sistema compromesso si limita la possibilità di raggiungerne altri tramite il c.d. lateral movement)
  - Monitorare eventuali situazioni anomale (a.e., tentativi di connessione vietati e bloccati potrebbero derivare da un'attività di ricognizione che precede l'attacco effettivo)

Firewall «convenzionali»

- I firewall sono generalmente implementati come appliance di rete con un sistema operativo dedicato e HW specializzato per poter analizzare i pacchetti in transito e valutare se, applicando le regole delle policy (c.d., communication matrix), sono ammessi oppure no e, di conseguenza, inoltrarli al next-hop oppure scartarli (drop)
- Per poter analizzare il traffico di rete, quindi, questi apparati devono essere collocati in maniera tale da poter intercettare tutte le possibili connessioni
- Questo comporta che generalmente si tratta di sistemi collocati a centro-stella (c.d., hub) e la rete deve essere progettata in maniera tale che tutto il traffico sia analizzabile dall'infrastruttura di FW
- Questo approccio ha diverse contro-indicazioni:
  - Per poter analizzare tutto il traffico, potenzialmente lecito, i FW devono essere opportunamente dimensionati
  - La necessità di ispezionare anche le connessioni interne (c.d., traffico East-West) richiede di inoltrare all'hub anche il traffico locale dall'access layer (c.d., firewall pinning): il FW è il default gateway di tutte le subnet
  - L'hub rappresenta un single-point-of-failure (SPOF) per l'intera rete (bisogna prevedere ridondanza HW)
- In genere si tratta di una delle tecnologie di sicurezza più costose da implementare e da gestire
- Le tecnologie più recenti (c.d., NGFW) consentono di creare e gestire architetture più complesse con diversi apparati collocati in punti strategici della rete

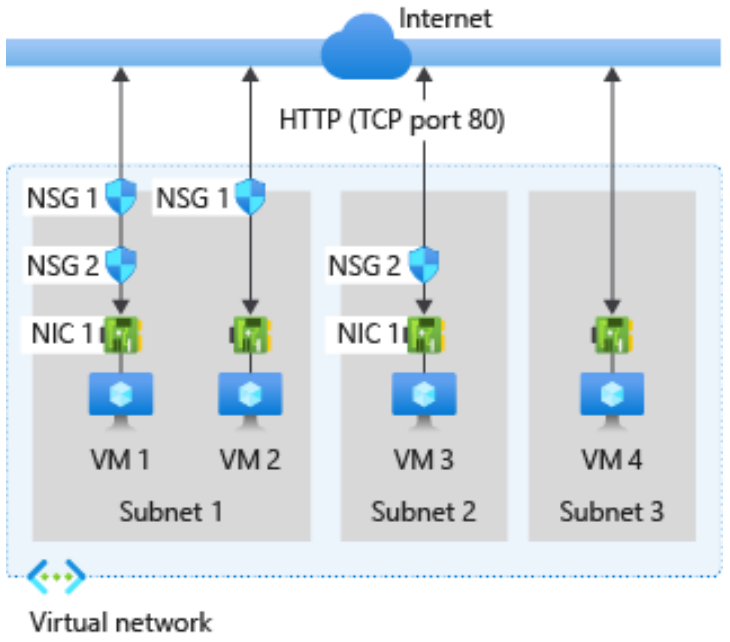
Firewall Pinning

In un’architettura di rete gerarchica (il riferimento per i data-center), il FW è collocato nel core layer, quindi il traffico di rete per poter essere analizzato deve attraversare tutti i layer anche se avviene tra nodi tra cui esiste un percorso più breve



Virtual Firewall (VF)

- Negli ambienti cloud, al contrario, i controlli del traffico di rete mediante filtro su base host e protocollo è implementato da servizi inclusi nel layer di virtualizzazione della rete (c.d., virtual network)
- Le policy di controllo possono essere definite in modo centralizzato e applicate alle varie subnet, host o service end-point (nel caso di risorse PaaS) in modo esplicito oppure sulla base del tagging
- La valutazione delle regole è implementata a livello SW, ma avviene in prossimità delle risorse da proteggere (località), quindi, pur senza apparati HW specializzati, risulta più efficiente perché implementato a livello kernel dall'hypervisor che ospita la VM (c.d., hypervisor-mode VF)
- E' possibile implementare policy di micro-segmentazione (ovvero definendo ambiti di rete in modo estremamente granulare) senza ricorrere a servizi o tecnologie esterne
- Questo tipo di funzionalità viene denotato come Security Group / Network Security Group / Application Security Group



Grazie

- Luigi.Dragone@Avanade.com
- Fabio.Vernacotola@Avanade.com