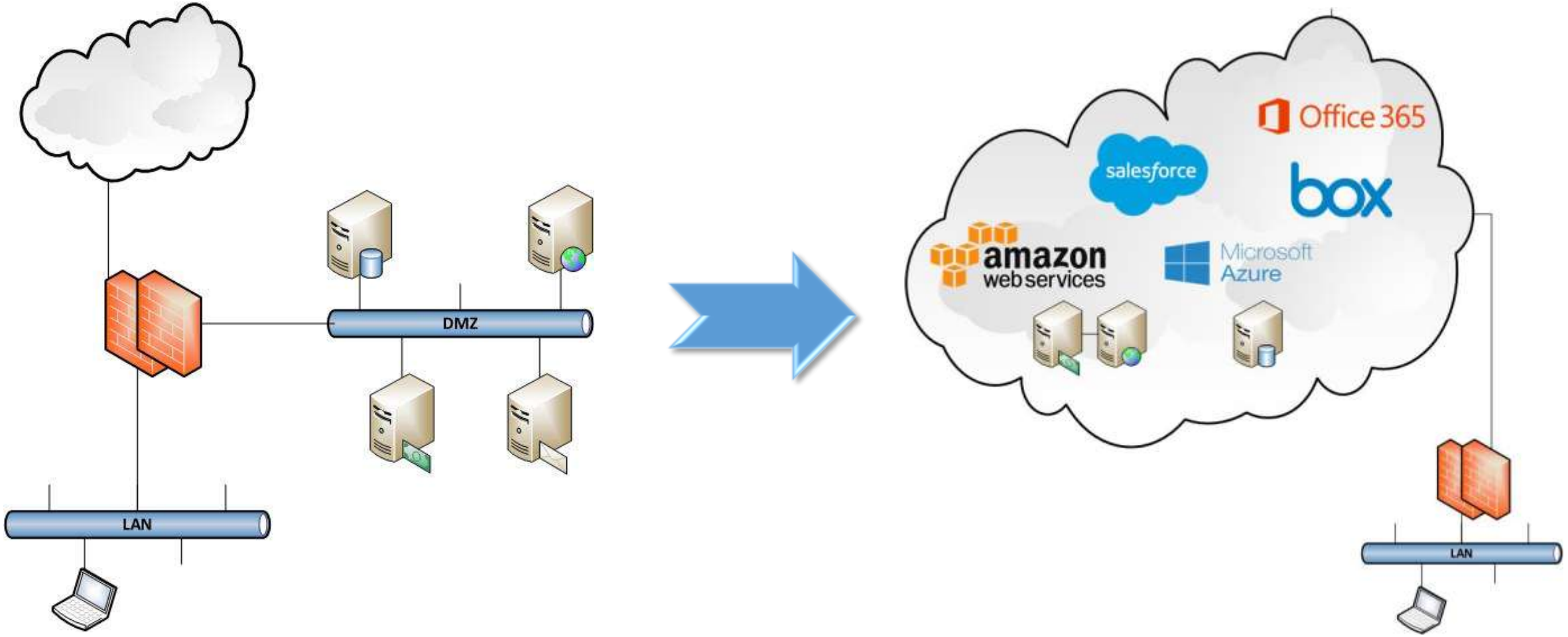
Dalla protezione del perimetro
Alla protezione del Cloud

Marco Coppolino – CIO
Gianluigi Crippa – Strategic Business Development

Chi Siamo

- Società di **CON**sulenza **SYS**temistica che dalla metà degli anni 90 si occupa di Application Delivery e Sicurezza, cioè del raggiungimento di quel punto di equilibrio tra la disponibilità del dato e la sua protezione.
- In una visione Cliente Centrica abbiamo evidenziato quattro valori fondamentali, quali: **persone**, **innovazione**, **professionalità** e **fiducia**.

Dal Perimetro al Cloud



Tre modalità di utilizzo cloud

- **IaaS – Infrastructure as a Service**: intera struttura a disposizione dell'utente (es. Amazon Web Services, MS Azure)
- **PaaS – Platform as a Service**: istanza di sistema operativo a disposizione dell'utente (es. MS Dynamics)
- **SaaS – Software as a Service**: utilizzo del solo software applicativo, nessuna interazione con il sistema operativo e la struttura (es. MS Office365, SalesForce)

Indubbi vantaggi…

- Risparmio su manutenzione hardware (servers, condizionamento, spazio datacenter,…).
- Risparmio su manutenzione software (patch S.O., patch applicativo, configurazione e ottimizzazione,…)
- Disponibilità risorse pressoché illimitata.
- Accesso da qualsiasi punto.

…Indubbi problemi di sicurezza

- Accesso da qualsiasi punto.
- Password non sicure.
- Locazione fisica dei dati.
- Nessun controllo di attivazione dei software da parte del reparto IT (Shadow IT).
- Nessun controllo sulle operazioni svolte all'interno delle applicazioni.

Cloud Security - Intelligence

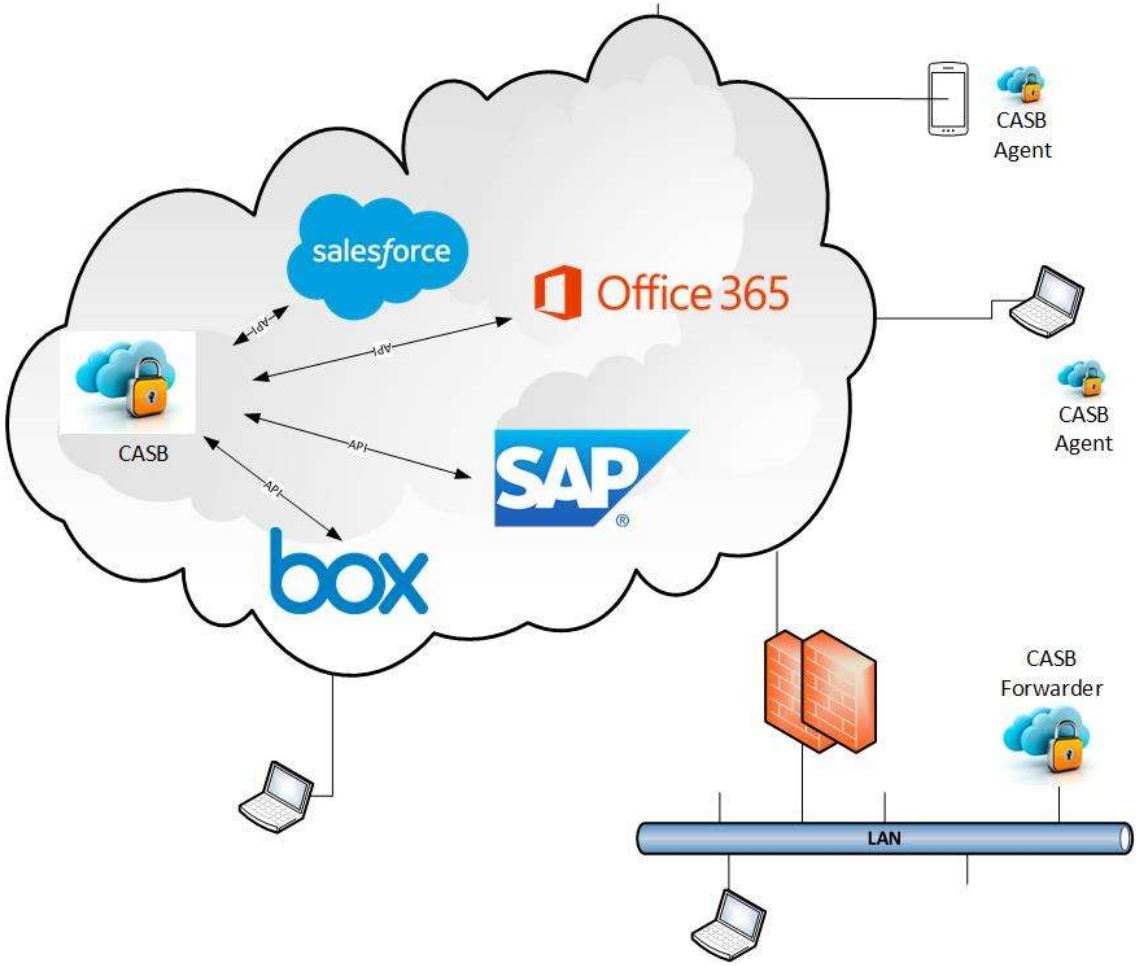
- **Threat Intelligence**
  - Comunità formata da vendors, hackers, utenti, gateways per interscambio informazioni su minacce.
  - Le informazioni collezionate vengono utilizzate dai sistemi anti-malware, IPS, URL Filtering, anti-APT.
  - Esempio: **Check Point ThreatCloud** (https://www.checkpoint.com/products-solutions/threat-intelligence)
- **Sandboxing**
  - Macchine virtuali nelle quali eseguire files sospetti per controllare la presenza di attacchi zero-day.
  - Esempio: **Check Point SandBlast** (https://www.checkpoint.com/products/threat-emulation-sandboxing)

Cloud Security – IaaS/PaaS

Network Security sul Cloud

- L'architettura di un datacenter si sposta da un modello fisico a virtualizzato.
- Le tecnologie di Network Security devono quindi adattarsi ad un concetto di rete virtuale.
- Micro-segmentazione
  - Il firewall si sposta da un modello «North-South» ad un modello «East-West»
  - La protezione viene quindi applicata ad ogni singola Virtual Machine

Cloud Security - SaaS



CASB

- *Cloud Access Security Broker*
- Controlla le operazioni che vengono svolte all'interno di un applicazione SaaS.
- Blocca le eventuali operazioni considerate non sicure (es. pubblicazione documenti confidenziali, sharing non consentiti,…).
- Modalità di controllo:
  - Forwarder on-premise
  - Agent
  - Agentless (Interfacciamento con API dei vendor SaaS)

La pubblicazione delle applicazioni in cloud

La cosa peggiore che possiamo fare è pubblicare una applicazione senza … sicurezza, possibilità di gestire e garantire l'availabilty, gestione dell'identità di chi accede alla applicazione

- **cosa fare per mettere in sicurezza una applicazione:**
  - protezione DoS/DDoS
  - WAF
  - DNSSEC

Attacchi DoS/DDoS sul cloud

Downtime - Distributed Denial of Service (DDoS)

DDoS è un attacco coordinato che produce un volume di richieste IP (UDP o TCP) molto elevato, verso uno specifico "servizio / ip:porta", al fine di impedire l'accesso al contenuto, al servizio web o ad un servizio IT generico, da parte di utenti reali.

- gli attacchi sono oggi giunti alla terza fase che si avvale del mondo IoT: cosa significa?
- perché proprio dal cloud le difese più efficaci e robuste per proteggerci da attacchi DoS/DDoS?

Attacchi DoS/DDoS: terza fase

- Prima fase
  - sorgente degli attacchi: perlopiù rete di pc
  - 2005/2009: attacchi di poche decine di Mbps (2-30Mbps)
  - pensiamo ad Anonymous
- Seconda fase
  - sorgente degli attacchi: rete di server
  - 2010/2014: attacchi di qualche decine di Mbps (50-100Mbps)
  - gruppi criminali che creano BOTNET
- Terza fase
  - sorgente degli attacchi: dispositivi IoT
  - 2015/2017: **giga attacchi da 300 Gbps / 600 Gbps**
  - gruppo criminali che sviluppano script per gestire dispositivi IoT (MIRAI)

DoS/DDoS – la difesa arriva dal cloud

Scrubbing

"scrubbing": questo termine si riferisce a tecniche per collezzionare, analizzare e filtrare traffico, per rimuovere richieste malevoli, e permettere le richieste legittime

Perché il CLOUD?

- perché gli attacchi arrivano dal cloud
- LARGEST ATTACK: 620Gbps
- AVARAGE ATTACK: 30Gbps
- BANDA dei DC: massimo 4-5Gbps
- COSA CHIEDERE:
  - MITIGATION SLAs: per i diversi tipi di attacco, uno SLA definito
- COSA VALUTARE: la capacità del scrubbing center in Tbps

Attacchi Applicativi e WAF cloud

Data Breach

- Data Breach si verifica quando il contenuto di un sito web, di un servizio IT, è reso accessibile a chi non dovrebbe averne accesso
- Esempi di contenuto "obiettivo" di un data breach sono: dati finanziari, dati di clienti, proprietà intellettuale o in generale informazioni sensibili

Attacchi Applicativi e WAF cloud

Defacement

- Web vandalism. Quando un "attacker" sostituisce il sito web reale, con un loro sito web con contenuto malevolo o offensivo
- Tipicamente ciò avviene quando un "attacker" è in disaccordo con la vittima per motivazioni politiche, per tipologia di cliente, per motivi di partnerships.

WAF – difesa cloud

WAF

Un Web Application Firewall è un dispositivo di protezione che analizza le richieste del livello ISO/OSI applicativo (protocollo HTTP, DNS, etc.) e blocca le richieste che cercano di utilizzare specifiche vulnerabilità applicative.

Gli attacchi applicativi:

- dopo anni vediamo ancora molti attacchi di tipo SQL injection:
  - oggi rappresentano ancora il 52% degli attacchi
- il 68% degli attacchi sono ancora per applicazioni HTTP
  - ci si può proteggere esponendoli in HTTPS

WAF – difesa cloud

Perché WAF CLOUD?

- **un firewall WAF in cloud è facile da installare da mantenere e fornisce una configurazione di regole automatiche, predefinito e consolidate privo di falsi positivi**
  - protezione dagli attacchi web applicativi più comuni
- Cloud offre anche una protezione da "Application Layer DDoS attack", con tecniche di:
  - Rate Controls/Rate Sphaping
  - Network Layer Controls
  - Geo/IP Blocking

Attacchi alle applicazioni e DNSSEC

Analyzing DNSSEC problems for www.consys.it

.	✓ Found 2 DNSKEY records for . ✓ DS=19036/SHA-256 verifies DNSKEY=19036/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
it	✗ No DS records found for it in the . zone ✗ No DNSKEY records found
consys.it	✗ No DS records found for consys.it in the it zone ✗ No DNSKEY records found ✓ www.consys.it A RR has value 79.62.35.196 ✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

…. c'è ancora molta da fare

Maggiori Informazioni

- ci trovi al desk clusit

- marco.coppolino@consys.it - **M: +39 345 5415430**

- gianluigi.crippa@consys.it - **M: +39 348 7015121**

- CONSYS.IT www.consys.it - info@consys.it - **T: 02 93507379**

Grazie.

CONSYS.IT
via Magenta, 77/4 - 20017 Rho (MI)
T +39 02.93507379
M +39 3455415430
info@consys.it
www.consys.it