

LEZIONE I: INTRODUZIONE ALLA VIRTUALIZZAZIONE

- Virtualization: tecnica che permette di eseguire più sistemi operativi su un unico hardware fisico
- Cybersecurity: protezione di sistemi, reti e dati da accessi non autorizzati
- Obiettivo: comprendere il ruolo della virtualizzazione nella sicurezza moderna

OBIETTIVI DELLA LEZIONE

- Comprendere il concetto di Virtual Machine (VM = macchina virtuale simulata via software)
- Capire il ruolo dell'Hypervisor (software che gestisce le VM)
- Preparare l'ambiente di laboratorio per attività pratiche

EVOLUZIONE DEI SISTEMI IT

- Bare Metal: server fisico dedicato ad un solo sistema operativo
- Problema: risorse CPU (Central Processing Unit) e RAM (Random Access Memory) sottoutilizzate
- Necessità di consolidamento infrastrutturale

PROBLEMI INFRASTRUTTURA FISICA

- Bassa scalabilità
- Backup complessi
- Ripristino lento
- Test difficili
 - Test di sistemi operativi
 - Test di reti virtuali
 - Test di ripristino (molto importanti)

CONSOLIDAMENTO

- Il consolidamento non significa solo "avere meno macchine", ma agire in modo olistico sull'infrastruttura:
- **Virtualizzazione dei Server:** È il pilastro principale. Permette di far girare più sistemi operativi e applicazioni su un singolo server fisico, riducendo drasticamente il numero di macchine fisiche.
- **Consolidamento dello Storage:** Centralizzare i dati in soluzioni di storage condiviso (SAN o NAS) invece di utilizzare dischi locali sparsi su numerosi server.
- **Consolidamento dei Data Center:** Ridurre il numero di sale server o data center fisici per ottimizzare costi di raffreddamento, alimentazione e gestione.
- **Razionalizzazione delle Applicazioni:** Eliminare applicazioni duplicate o obsolete.



PERCHÉ SI CONSOLIDA

- **Riduzione dei costi (TCO - Total Cost of Ownership):** Minori costi per hardware, licenze software, energia elettrica e manutenzione.
- **Maggiore efficienza:** Aumenta il tasso di utilizzo delle risorse (server non più quasi inattivi).
- **Gestione semplificata:** Meno macchine fisiche significano meno amministrazione, patch e monitoraggio.
- **Maggiore sicurezza e affidabilità:** La centralizzazione facilita il backup, il disaster recovery e l'applicazione di policy di sicurezza.
- **Spazio ridotto:** Meno server fisici richiedono meno spazio fisico nel data center.

TIPI DI CONSOLIDAMENTO

- **Geografico:** Raccogliere in un unico sito fisico macchine dislocate in diverse sedi.
- **Logico/Virtuale:** Utilizzare tecnologie di virtualizzazione (come VMware, Hyper-V, KVM) per unificare i carichi di lavoro.



NASCITA VIRTUALIZZAZIONE

- Server consolidation: più server logici su uno fisico
- Isolamento: ogni VM indipendente dalle altre
- OPEX (Operational Expenditure) ridotti: minori costi operativi

ISOLAMENTO

- In ambito informatico e sistemistico, l'**isolamento** si riferisce all'insieme di tecniche, logiche o fisiche, atte a separare componenti di un sistema IT — come processi, applicazioni, macchine virtuali, reti o database — al fine di impedirne l'interazione diretta, la condivisione di risorse non autorizzata o la propagazione di minacce.
- È un pilastro fondamentale della sicurezza informatica (Cybersecurity) e della stabilità dei sistemi (System Administration), utilizzato per compartimentare infrastrutture e dati.

ISOLAMENTO A LIVELLO DI PROCESSO E SISTEMA OPERATIVO

- **Process Isolation:** Meccanismo del sistema operativo che assicura che ogni processo in esecuzione sia indipendente. Un processo non può accedere alla memoria o alle risorse di un altro, a meno che non sia esplicitamente consentito.
- **Sandboxing:** Tecnica che esegue programmi o codice in un ambiente ristretto (una "sabbiera") per isolarli dal sistema operativo ospite, proteggendo quest'ultimo da malware o comportamenti anomali.
- **Containerizzazione (es. Docker):** Separa le applicazioni a livello di utente, consentendo loro di girare in ambienti isolati pur condividendo lo stesso kernel del sistema operativo.



ISOLAMENTO DI VIRTUALIZZAZIONE E HARDWARE

- **Virtual Machines (VM):** Utilizzo di hypervisor per separare completamente i sistemi operativi, garantendo che una VM non acceda alle risorse fisiche (CPU, RAM, disco) di un'altra.
- **Isolamento Fisico:** Metodo estremo che separa fisicamente i computer e le reti da internet o da altre reti non attendibili per proteggere dati critici.

COS'È LA VIRTUALIZZAZIONE

- Astrazione hardware: il software non vede direttamente la CPU reale
- Guest OS: sistema operativo installato nella VM
- Host OS: sistema operativo fisico sottostante

COMPONENTI PRINCIPALI

- Host: macchina fisica reale
- Hypervisor: software di gestione virtualizzazione
- VM: ambiente isolato con hardware simulato
- Virtual Disk: file che rappresenta un disco fisico

TIPI DI VIRTUALIZZAZIONE

- Server Virtualization: server logici
- Desktop Virtualization (VDI = Virtual Desktop Infrastructure)
- Network Virtualization: reti simulate
- Storage Virtualization: dischi logici aggregati

VIRTUALIZZAZIONE E SICUREZZA

- Sandbox: ambiente isolato per analisi malware
- Malware Analysis: studio comportamento software malevolo
- Forensics: analisi post-incidente

SOC E VIRTUALIZZAZIONE

- SOC (Security Operations Center): centro monitoraggio sicurezza
- Replica ambienti compromessi
- Test attacchi senza rischi reali

SOC

- struttura centralizzata — composta da persone, processi e tecnologie — dedicata al monitoraggio, alla rilevazione, all'analisi e alla risposta proattiva contro le minacce informatiche.

FUNZIONI PRINCIPALI DEL SOC

- **Monitoraggio h24 (24/7):** Sorveglianza costante di reti e dispositivi per individuare anomalie in tempo reale.
- **Rilevazione delle minacce (Detection):** Utilizzo di strumenti come SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response) e SOAR (Security Orchestration, Automation and Response) per identificare potenziali violazioni.
- **Analisi e Investigation:** Gli analisti SOC (analisti di sicurezza) esaminano gli avvisi generati per distinguere i falsi positivi dalle minacce reali.
- **Incident Response (Risposta agli incidenti):** Azioni immediate per contenere, eradicare e mitigare gli effetti di un attacco, come l'isolamento di un dispositivo infetto.
- **Threat Intelligence:** Raccolta di informazioni sulle nuove minacce e vulnerabilità per adeguare le difese prima che vengano sfruttate.

VM VS FISICO

- Provisioning: creazione rapida sistemi
- Rollback: ritorno stato precedente
- Portabilità: VM copiabile come file

PROVISIONING

- processo di creazione, configurazione e messa a disposizione di risorse IT (hardware, software, reti, macchine virtuali, account utente) affinché siano pronte all'uso

TIPI DI PROVISIONING:

- **Server Provisioning**: Configurazione di server fisici o virtuali con il sistema operativo, software e risorse di rete necessari.
- **User Provisioning (Utenti)**: Creazione, gestione e rimozione di account utente e privilegi di accesso (es. Active Directory, app SaaS).
- **Network Provisioning**: Configurazione delle risorse di rete (switch, router, firewall) per garantire connettività.
- **Service Provisioning**: Attivazione di servizi specifici, spesso in contesti cloud o telecomunicazioni.

- **Provisioning vs Configurazione:** Il provisioning mette a disposizione la risorsa (es. crea la VM), mentre la configurazione imposta i dettagli specifici (es. installa le applicazioni).
- **Automazione:** Negli ambienti moderni, il provisioning manuale è sostituito dall'automazione (IaC) per ridurre errori, migliorare la coerenza tra ambienti (sviluppo, test, produzione) e accelerare i tempi.
- **Vantaggi:** Maggiore efficienza, riduzione degli errori manuali, sicurezza migliorata (gestione corretta dei diritti di accesso) e rapidità nel rilascio di nuovi servizi.
- **Deprovisioning:** È il processo inverso, ovvero la rimozione o il recupero di risorse e accessi non più necessari.



SNAPSHOT

- Snapshot: fotografia dello stato sistema
- Utile nei penetration test
- Riduce downtime (tempo inattività)

SNAPSHOT

- copia virtuale, immediata e in sola lettura dello stato di un sistema (macchina virtuale, disco o volume) in un preciso momento
- **Funzionamento:** Quando viene creato uno snapshot, il sistema "congela" il disco originale e crea un file differenziale (delta file) dove vengono salvate tutte le nuove modifiche. Lo snapshot originale rimane immutato.
- **Differenza col Backup:** A differenza di un backup tradizionale (copia completa e indipendente), lo snapshot è un'istantanea "point-in-time" strettamente dipendente dal disco originale e risiede solitamente sullo stesso storage.
- **Utilizzi comuni:** Sono fondamentali prima di aggiornamenti di sistema, installazioni di patch, o per test, consentendo di annullare rapidamente le modifiche se qualcosa va storto.

CLOUD COMPUTING

- IaaS (Infrastructure as a Service): server virtuali nel cloud
- Elasticity: risorse dinamiche
- Multi-tenant: più clienti stesso hardware

RISCHI SICUREZZA

- **VM Escape:** attacco che esce dalla macchina virtuale e prende possesso dell'hypervisor
- **Lateral Movement:** movimento laterale nella rete: tattica utilizzata dagli attaccanti per spostarsi attraverso una rete compromessa, muovendosi da un endpoint iniziale a sistemi, server e dati sempre più critici.
- **Misconfiguration:** configurazione errata

PREPARAZIONE LABORATORIO

- Abilitare Intel VT-x / AMD-V (estensioni CPU virtualizzazione)
- Installare hypervisor hosted
- Configurare NFS su NAS

CREAZIONE VM

- Allocare RAM e CPU virtuali
- Creare Virtual Disk Image (VDI)
- Montare file ISO (immagine disco installazione OS)

TEST VM

- Ping: verifica rete
- Resource monitoring: controllo risorse
- Boot test: verifica avvio corretto

BUONE PRATICHE

- Naming convention: nomi standard VM
- Backup immagini
- Documentazione configurazioni

RIEPILOGO

- Virtualizzazione base della sicurezza moderna
- Permette simulazioni e test controllati

PROSSIMA LEZIONE

- Hypervisor Type 1 vs Type 2
- Architetture e sicurezza