LEZIONE 2: HYPERVISOR E ARCHITETTURE DI VIRTUALIZZAZIONE

- In questa lezione analizziamo in profondità il ruolo dell'Hypervisor.
- Capiremo cosa significa Type 1 (Bare Metal) e Type 2 (Hosted).
- Studieremo l'impatto di queste scelte sulla sicurezza informatica.

COS'È UN HYPERVISOR

- Un Hypervisor è un software che consente di creare e gestire macchine virtuali (Virtual Machine – VM).
- Si occupa di distribuire le risorse fisiche come CPU (Central Processing Unit), RAM (Random Access Memory) e disco.
- È il cuore dell'infrastruttura virtualizzata.

PERCHÉ È NECESSARIO

- Senza hypervisor ogni server fisico potrebbe eseguire un solo sistema operativo.
- L'hypervisor permette l'esecuzione simultanea di più sistemi operativi isolati.
- Questo migliora l'utilizzo delle risorse hardware.

CONCETTO DI ASTRAZIONE HARDWARE

- Astrazione significa separare il software dall'hardware reale.
- Il sistema operativo Guest non comunica direttamente con la CPU fisica.
- L'hypervisor intercetta e gestisce le richieste hardware.

HYPERVISOR TYPE 1 – BARE METAL

- Bare Metal significa 'su metallo nudo', cioè direttamente sull'hardware.
- Non esiste un sistema operativo host intermedio.
- Offre migliori performance e minore superficie di attacco.

ESEMPI DI HYPERVISOR TYPE 1

- VMware ESXi: soluzione enterprise diffusa nei data center.
- Microsoft Hyper-V Server: integrato nell'ecosistema Windows Server.
- Proxmox VE (Virtual Environment): soluzione open source.

HYPERVISOR TYPE 2 – HOSTED

- Viene installato sopra un sistema operativo esistente (Host OS).
- È ideale per ambienti di test, laboratorio e sviluppo.
- La sicurezza dipende anche dalla sicurezza del sistema host.

ESEMPI DI HYPERVISOR TYPE 2

- Oracle VirtualBox: molto usato in ambito didattico.
- VMware Workstation: diffuso in ambito professionale.
- Parallels Desktop: utilizzato su macOS.

ARCHITETTURA TYPE 1

- Struttura: Hardware → Hypervisor → VM.
- Il minor numero di livelli riduce la complessità.
- È la soluzione tipica dei data center professionali.

ARCHITETTURA TYPE 2

- Struttura: Hardware → Host OS → Hypervisor → VM.
- Se il sistema host viene compromesso, tutte le VM sono a rischio.
- È meno indicato per ambienti mission-critical.

VIRTUALIZZAZIONE DELLA CPU

- La CPU (Central Processing Unit) esegue le istruzioni dei programmi.
- Le tecnologie Intel VT-x e AMD-V permettono virtualizzazione assistita.
- Riduce l'overhead software migliorando le performance.

GESTIONE ISTRUZIONI PRIVILEGIATE

- Alcune istruzioni sono riservate al livello kernel (Ring 0).
- L'hypervisor intercetta queste istruzioni prima che raggiungano l'hardware.
- Questo garantisce controllo e isolamento.

I 4 ANELLI STANDARD (ARCHITETTURA X86)

- **Ring 0 (Kernel Mode):** È il cuore del sistema. Qui risiede il **Kernel**. Ha accesso illimitato a ogni istruzione della CPU e a tutta la memoria fisica. Un errore qui causa il famigerato "Schermo Blu" (BSOD).
- **Ring 1 e Ring 2 (Raramente usati):** In origine erano pensati per i **driver dei dispositivi** e i servizi di sistema meno critici. Oggi quasi tutti i sistemi operativi (Windows, Linux, macOS) saltano questi livelli per semplicità e portabilità, eseguendo i driver direttamente in Ring 0.
- **Ring 3 (User Mode):** È dove girano le tue **applicazioni** (browser, Word, giochi). Il codice è isolato: non può accedere direttamente all'hardware o alla memoria di altri programmi. Se un'app in Ring 3 crasha, il resto del sistema rimane stabile.

RING 0 – KERNEL MODE

- **Massima Autorità (Kernel Mode):** È il cuore del sistema operativo. Mentre le applicazioni normali (browser, giochi, editor di testo) girano nel "Ring 3" (User Mode) e devono chiedere il permesso al sistema operativo per accedere a risorse, il codice nel Ring 0 è il sistema operativo stesso, quindi non ha restrizioni.
- **Interazione Diretta con l'Hardware:** I componenti che girano nel Ring 0 includono il kernel del sistema operativo e i driver di dispositivo. Possono interagire direttamente con processori, RAM, dischi rigidi e periferiche.
- **Sicurezza e Stabilità:** Proprio perché ha privilegi assoluti, un errore nel codice in esecuzione a livello Ring 0 non causa semplicemente la chiusura di un programma, ma spesso porta al "crash" dell'intero sistema, noto come schermata blu (BSOD) su Windows o kernel panic su Linux/macOS.
- **Contesto di Sicurezza:** Il Ring 0 è fondamentale per la sicurezza: se un malware o un rootkit riesce a infiltrarsi in questo livello (kernel-level), diventa invisibile e incontrollabile per i normali antivirus, che operano al Ring 3.

VIRTUALIZZAZIONE DELLA MEMORIA

- La RAM (Random Access Memory) viene suddivisa tra le VM.
- L'hypervisor crea una mappatura tra memoria virtuale e fisica.
- Le Extended Page Tables (EPT) migliorano l'efficienza.

OVERCOMMIT DELLA MEMORIA

- È possibile assegnare più RAM virtuale rispetto alla RAM fisica.
- Funziona perché non tutte le VM usano tutta la memoria simultaneamente.
- Un eccesso può causare degrado prestazionale.

VIRTUALIZZAZIONE DELLO STORAGE

- I dischi virtuali sono file (VDI, VMDK).
- Thin Provisioning alloca spazio solo quando necessario.
- Thick Provisioning riserva tutto lo spazio immediatamente.

VIRTUALIZZAZIONE DELLA RETE

- Ogni VM possiede una vNIC (Virtual Network Interface Card).
- Il traffico passa attraverso un vSwitch (Virtual Switch).
- Permette segmentazione e isolamento del traffico.

MODALITÀ BRIDGE (PONTE)

- . **Funzionamento:** La VM o il dispositivo si connette direttamente alla rete fisica tramite l'hardware host, comportandosi come se fosse un dispositivo fisico separato collegato allo stesso switch o router.
- **Indirizzo IP:** Riceve un indirizzo IP **nella stessa sottorete** dell'host (es. se l'host è 192.168.1.5, la VM potrebbe essere 192.168.1.10).
- **Visibilità:** È visibile e accessibile da altri dispositivi nella LAN fisica e viceversa.
- **Ideale per:** Servizi di rete, server web/FTP, VoIP, o quando la macchina virtuale deve essere trattata come una macchina fisica reale nella rete.

MODALITÀ NAT (NETWORK ADDRESS TRANSLATION)

- **Funzionamento:** La VM crea una rete virtuale interna privata. Il sistema host agisce da router, traducendo gli indirizzi tra la rete interna e la rete esterna.
- **Indirizzo IP:** Riceve un indirizzo IP privato (es. 10.0.2.x), diverso da quello dell'host.
- **Visibilità:** È isolata dalla rete locale fisica. Altri computer in rete non possono vedere la VM, ma la VM può accedere a Internet tramite l'host.
- **Ideale per:** Navigazione Internet, test in ambiente isolato, sicurezza (la VM è protetta dal firewall dell'host), notebook in viaggio su reti pubbliche.

FULL VIRTUALIZATION

- Simula completamente l'hardware fisico.
- Il sistema operativo guest non necessita modifiche.
- Massima compatibilità con sistemi legacy.

PARAVIRTUALIZATION

- Il sistema operativo guest è modificato per collaborare con l'hypervisor.
- Utilizza driver ottimizzati.
- Migliora le prestazioni rispetto all'emulazione completa.

CONTAINER VS VM

- I container virtualizzano il sistema operativo, non l'hardware.
- Le VM virtualizzano l'hardware completo.
- Le VM offrono maggiore isolamento di sicurezza.

VM ESCAPE

- VM Escape è un attacco che permette di uscire dalla macchina virtuale.
- L'attaccante tenta di raggiungere l'hypervisor.
- È un rischio grave in ambienti cloud multi-tenant.

SURFACE OF ATTACK

- La superficie di attacco comprende tutti i punti vulnerabili.
- Un hypervisor deve essere minimale e aggiornato.
- La gestione patch è fondamentale.

ISOLATION

- L'isolamento impedisce che una VM compromessa attacchi le altre.
- È un principio chiave nella cybersecurity.
- Richiede corretta configurazione di rete e permessi.

MULTI-TENANT

- Multi-tenant significa più clienti sulla stessa infrastruttura.
- È tipico dei servizi IaaS (Infrastructure as a Service).
- Richiede forte separazione logica tra ambienti.

PRIVILEGE LEVELS

- Ring 0: livello kernel con privilegi massimi.
- Ring 3: livello utente con privilegi limitati.
- L'hypervisor opera con privilegi elevati per controllare le VM.

HARDWARE ASSISTED VIRTUALIZATION

- Le CPU moderne includono estensioni dedicate.
- Riduce il lavoro software dell'hypervisor.
- Migliora sicurezza e performance.

HIGH AVAILABILITY (HA)

- HA significa High Availability, alta disponibilità.
- Permette continuità del servizio in caso di guasto hardware.
- Le VM possono riavviarsi su un altro host.

LIVE MIGRATION

- Consente di spostare una VM attiva su un altro server.
- La memoria viene trasferita in tempo reale.
- Nessuna interruzione percepibile dall'utente.

LOGGING E MONITORING

- Il logging registra eventi e accessi.
- Il monitoring controlla CPU, RAM e traffico.
- Fondamentale per incident response.

HARDENING DELL'HYPERVISOR

- Hardening significa rafforzamento della sicurezza.
- Disabilitare servizi non necessari.
- Limitare accesso amministrativo e usare autenticazione forte.

BEST PRACTICE DI SICUREZZA

- Principio del minimo privilegio.
- Segmentazione della rete di management.
- Backup della configurazione dell'hypervisor.

SCENARIO REALE AZIENDALE

- Cluster di hypervisor in data center.
- VM dedicate a Web Server, Database e Firewall.
- Monitoraggio centralizzato tramite console di gestione.

ERRORE TIPICO STUDENTE

- Non abilitare VT-x o AMD-V nel BIOS.
- Allocare troppe risorse alla VM.
- Confondere modalità NAT e Bridged.

LABORATORIO PREVISTO

- Installazione di un hypervisor Type 2.
- Creazione di una VM Linux.
- Analisi consumo CPU e RAM.

OBIETTIVI PRATICI DELLA LEZIONE

- Comprendere architettura hypervisor.
- Valutare impatti sicurezza.
- Prepararsi alla segmentazione di rete della prossima lezione.

RIEPILOGO FINALE

- L'hypervisor è il cuore dell'infrastruttura virtualizzata.
- Type 1 per ambienti enterprise.
- La sicurezza dipende dalla configurazione corretta.