White paper tecnico: **2023**

Gestione delle principali preoccupazioni in tema di sicurezza quando si modernizza l'infrastruttura del data center

vmware®

Sommario

Gestione delle principali preoccupazioni in tema di sicurezza quando si modernizza l'infrastruttura del data center

Le aziende moderne devono assolutamente difendersi dalla crescita esponenziale delle minacce alla sicurezza informatica. Qualsiasi organizzazione che modernizzi l'infrastruttura cloud vede in tale iniziativa un'opportunità per rivedere le strategie di sicurezza e apportare modifiche per assicurare l'allineamento agli obblighi di sicurezza aziendali.

Gli attacchi informatici minacciano i data center compromettendo le informazioni sensibili archiviate sui server e interrompendo le operation aziendali cruciali. Le aziende spesso archiviano grandi quantità di dati finanziari, personali e aziendali riservati a cui potrebbero accedere persone non autorizzate, le quali potrebbero sfruttarli per un guadagno finanziario o per recare danno all'organizzazione. Esistono decine di categorie di attacchi, dalle violazioni di dati al furto di proprietà intellettuale, fino all'estorsione e al ransomware. Il ransomware è di gran lunga quella più conosciuta. Quando un hacker impedisce di accedere, ad esempio, a carburante, cibo e servizi sanitari a livello nazionale, attira l'attenzione dei governi, dei clienti e degli azionisti.

Inoltre, i data center spesso fungono da hub per l'infrastruttura IT di un'organizzazione e un attacco che va a buon fine in un data center può causare un'interruzione diffusa delle operation. Questo può determinare una perdita di produttività e di entrate,nonché un danno alla reputazione dell'organizzazione.

Figura 1. La protezione dei carichi di lavoro implica un processo, degli strumenti e una strategia.

Gli attacchi informatici non sono una minaccia solo per l'infrastruttura di un'azienda, ma anche per la gestione del suo flusso di cassa. L'impatto sulla spesa di capitale (CapEx) e sulla spesa operativa (OpEx) può essere notevole quando si cerca di mitigare le potenziali minacce, soprattutto quando questi sforzi non rientrano in una strategia di sicurezza globale.

Dal lato CapEx, un'organizzazione potrebbe avere la necessità di investire in nuove tecnologie per la sicurezza o apparecchiature per mitigare il rischio di attacchi futuri e per rispettare i requisiti di compliance normativa. Ciò può includere firewall, sistemi di rilevamento/prevenzione delle intrusioni, crittografia e altri strumenti di sicurezza. Queste direttive possono comportare ulteriori spese non previste se non vengono eseguite nell'ambito di un esercizio di bilancio e di un continuo approccio proattivo.

Dal lato OpEx, potrebbe essere necessario aumentare il personale IT e di sicurezza per garantire la gestione e la manutenzione delle nuove tecnologie di sicurezza, oltre che per formare altri dipendenti sul rilevamento delle violazioni e sulla risposta alle stesse. L'organizzazione potrebbe inoltre avere la necessità di deviare fondi verso la risposta agli incidenti e le indagini forensi in caso di attacco, il che aumenterebbe la spesa operativa complessiva.

La consapevolezza delle minacce informatiche è essenziale per un'efficace strategia di sicurezza

Non tutti gli attacchi informatici sono creati allo stesso modo o hanno lo stesso scopo. I leader IT e gli architetti della sicurezza devono essere consapevoli della gamma di attacchi, modus operandi e fattori di rischio quando progettano una strategia di sicurezza efficace. È importante notare che questo non è un elenco esaustivo di tutti i tipi di attacchi alla sicurezza informatica; nuovi tipi di attacchi vengono sviluppati continuamente. Pertanto, è importante che le organizzazioni abbiano una strategia di sicurezza completa in atto per individuare gli incidenti di sicurezza e rispondere in modo tempestivo.

I più comuni tipi di attacchi informatici nel panorama di oggi

Distributed Denial of Service (DDoS)
Questi attacchi inondano la rete di un data center con una grande quantità di traffico, sovraccaricandola e rendendola non disponibile per gli utenti legittimi.

Phishing
Sono attacchi che utilizzano l'e-mail o altre forme di comunicazione per indurre gli utenti a fornire all'hacker informazioni sensibili, ad esempio credenziali di accesso.

Ransomware
Sono attacchi che crittografano i dati sui server di un data center e chiedono all'organizzazione un pagamento in cambio della chiave di decrittografia.

Minacce persistenti avanzate (APT)
Si tratta di attacchi mirati concepiti per ottenere accesso alla rete di un data center e rubare informazioni sensibili in un periodo di tempo prolungato.

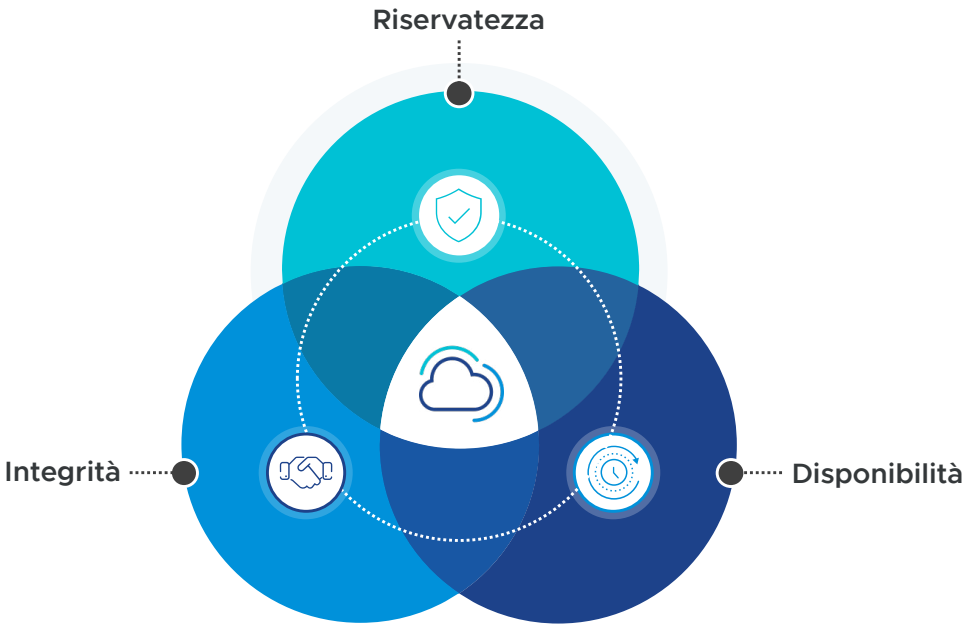
Malware
Si tratta di software malevolo che ottiene accesso alla rete di un data center, ruba informazioni sensibili o interrompe le operation.

Attacchi cloud
Questi attacchi prendono di mira le vulnerabilità dell'infrastruttura cloud che possono portare a un accesso non autorizzato, violazioni dei dati e altre attività malevole.

Attacchi IoT
Questi attacchi prendono di mira le vulnerabilità dei dispositivi Internet of Things (IoT), come le telecamere di sicurezza e i sensori di temperatura, che sono connessi alla rete di un data center.

Attacchi interni
Questi attacchi sono condotti da un dipendente, collaboratore esterno o altro utente fidato che ha accesso alla rete del data center.

Considerazioni per la progettazione di un'architettura di sicurezza a prova di futuro



Un modo efficace per comprendere il livello di sicurezza necessario all'interno delle piattaforme è guardare attraverso le lenti dei tre principi fondamentali della sicurezza delle informazioni: riservatezza, disponibilità e integrità.

1. **Riservatezza dei dati** indica la protezione delle informazioni sensibili dall'accesso o dalla divulgazione a persone o sistemi non autorizzati. La riservatezza dei dati è importante per le organizzazioni poiché le informazioni sensibili possono essere utilizzate per un guadagno finanziario o per recare danno all'organizzazione in caso di accesso o furto da parte di persone non autorizzate.

2. **Integrità di dati** indica l'accuratezza e la completezza dei dati e la garanzia che i dati non sono stati manomessi, alterati o distrutti in modo non autorizzato. L'integrità dei dati è importante perché assicura che i dati utilizzati da un'organizzazione sono accurati, affidabili e attendibili. Dati non accurati o manomessi possono portare a decisioni errate, perdite finanziarie e danno alla reputazione dell'organizzazione.

3. **Disponibilità dei dati** indica la possibilità di individui o sistemi autorizzati di accedere ai dati quando ne hanno necessità. La disponibilità dei dati è importante per le organizzazioni poiché, senza accesso ai dati, i processi aziendali possono subire interruzioni, con conseguente perdita di produttività, perdita di entrate e danno alla reputazione dell'organizzazione. Inoltre, è essenziale per la continuità delle operation, la compliance alle normative e la soddisfazione dei clienti.

Tutte le funzionalità di sicurezza dell'infrastruttura possono essere mappate rispetto a uno o più di questi principi. Ad esempio, la crittografia e il mascheramento dei dati sono funzionalità per la riservatezza dei dati, mentre l'integrità dei dati e l'hashing fanno parte del principio di integrità dei dati.

Ciò rende ogni singola funzionalità una funzionalità di sicurezza, concepita per aiutare le organizzazioni a ridurre ed eliminare i rischi. Tutto questo è estremamente vantaggioso ed è il motivo per cui le organizzazioni attente alla sicurezza scelgono le piattaforme VMware.

Gestione delle principali preoccupazioni in una strategia di sicurezza

Quando si pianifica un programma di modernizzazione dell'infrastruttura cloud, è essenziale che i leader dell'infrastruttura e delle operation comprendano e affrontino i principali requisiti di sicurezza per proteggere l'organizzazione dagli attacchi e istituire un'architettura agile per sventare attacchi futuri.

Visibilità e osservabilità

La sicurezza inizia con la visibilità. Le aziende non possono proteggere ciò che non vedono. Tuttavia, la sola visibilità non è sufficiente. L'osservabilità è visibilità contestuale e intelligente. Le complesse infrastrutture e applicazioni moderne rendono più difficile che mai rispondere alle domande su che cosa è successo, chi è stato colpito e come è possibile rimediare. I sistemi di osservabilità permettono di ispezionare e comprendere lo stack di applicazioni.

L'osservabilità è un elemento chiave della protezione end-to-end. Va oltre la possibilità di vedere e può fornire all'utente informazioni contestuali su cosa accade in un sistema dinamico come il Software-Defined Data Center di oggi.

La visibilità implica la comprensione di quali risorse di elaborazione vengono utilizzate, da chi, per quale motivo e in quale ambito di interesse. Gli amministratori di sistema possono imparare molto sull'infrastruttura osservando tutti gli aspetti al suo interno. Nonostante possa sembrare un requisito ovvio, spesso viene tralasciato nelle politiche e nei processi obsoleti di diverse aziende. È importante visualizzare e ottenere informazioni approfondite su tutti i flussi nell'intero data center con l'ispezione layer 7 di tipo stateful e un contesto del carico di lavoro completo, eliminando così i punti ciechi nella sicurezza e accelerando la correzione degli incidenti.

Implementazione della sicurezza basata su policy

Nelle infrastrutture Software-Defined, l'architettura o la gestione della sicurezza basata su policy è un modo ideale per definire e controllare in modo dinamico l'interazione tra servizi e applicazioni. La gestione della sicurezza basata su policy abilita funzionalità di sicurezza intelligenti e migliora il controllo dettagliato del comportamento degli utenti finali.

Tuttavia, le variazioni dinamiche nella rete, il rapido aumento degli attacchi alla sicurezza, la distribuzione geografica dei nodi e le complesse reti eterogenee possono avere gravi ripercussioni sulle prestazioni delle policy. Più intelligente è la definizione delle policy, maggiori probabilità ha di resistere alle evoluzioni delle violazioni della sicurezza. Pertanto, non appena i leader IT comprendono il flusso delle applicazioni dell'infrastruttura, i tecnici possono definire un modo migliore di proteggere le applicazioni e le risorse fondamentali. L'introduzione di un sistema che richiede il minimo intervento umano possibile equivale a maggiore flessibilità, scalabilità superiore e minore possibilità di errore.

Garanzia di esecuzione delle policy

Le policy di sicurezza hanno un ruolo importante nel modello di sicurezza aziendale complessivo. Tuttavia, in molte organizzazioni esistono tre tipi di sfide:

1. La sfida associata alla comprensione dell'ambito della policy (che affrontiamo con l'osservabilità)
2. La sfida associata alla definizione di una policy di sicurezza completa che tenga conto di tutto
3. La sfida associata all'implementazione iniziale e all'esecuzione

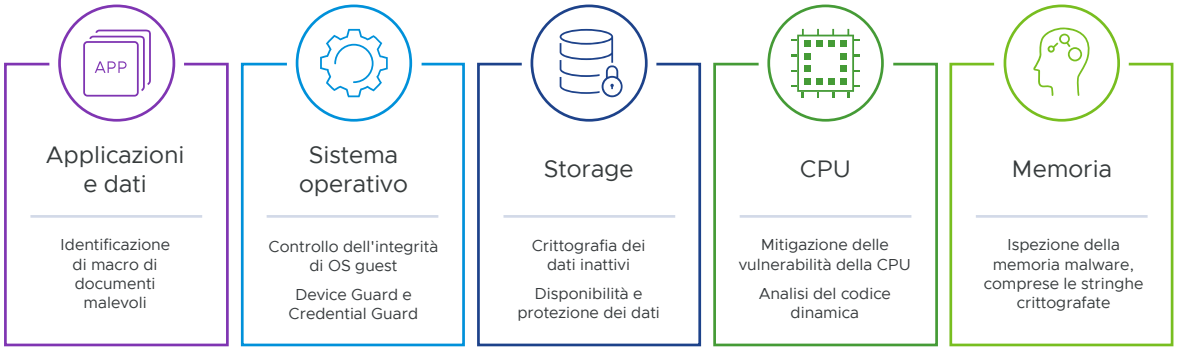
Le organizzazioni dovrebbero assicurare la presenza di solidi processi che supportino i requisiti delle policy di sicurezza. L'automazione e i sistemi intelligenti, come quelli forniti da VMware NSX® o il prodotto Advance Threat Analyzer, aiutano a eseguire questi processi in modo coerente e con maggiore affidabilità rispetto all'intervento umano, che ha una maggiore probabilità di errore di esecuzione.

Implementazione di architetture di sicurezza moderne con VMware Cloud Foundation

La sicurezza in VMware Cloud Foundation™ (VCF) non si limita a router e switch virtualizzati. I servizi di rete e sicurezza sono distribuiti in modo programmato su ciascuna macchina virtuale, indipendentemente dalla topologia o dall'hardware di rete sottostante. In questo modo, i carichi di lavoro possono essere aggiunti o spostati in modo dinamico e tutti i servizi di rete e sicurezza collegati alla macchina virtuale si spostano con essa, in qualsiasi parte del data center.

Utilizzando NSX, VCF riproduce l'intero stack di networking nel software in ogni rete virtuale. Offre un'architettura logica distribuita per servizi L2-7, tra cui switch logico, router, firewall, bilanciamento del carico e VPN.

Sicurezza in VMware Cloud: più di un semplice firewall



Oltre ai classici servizi di networking, i tecnici possono sfruttare funzionalità di sicurezza approfondite:

Nel layer delle applicazioni:
Si identificano le macro di documenti malevoli.

Nel layer del sistema operativo:
I sistemi operativi vengono eseguiti ovunque, pertanto è necessario verificare che siano quanto più sicuri possibile. Questo significa affidarsi non solo al firewall a livello di macchina, ma anche all'infrastruttura per proteggersi dagli attacchi.

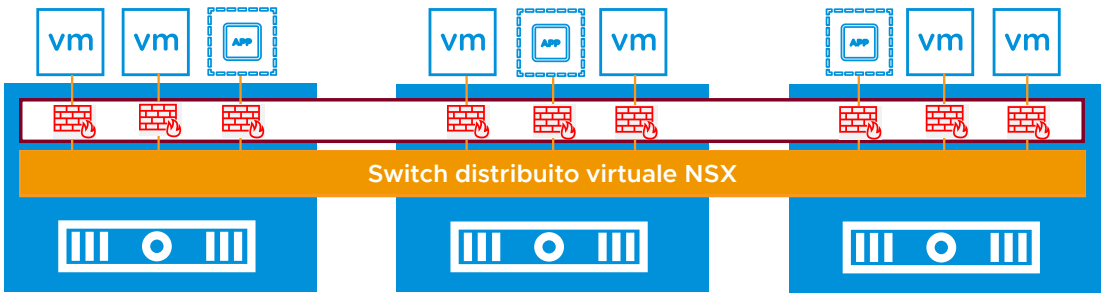
Nel layer dello storage:
VMware Cloud Foundation utilizza VMware vSAN™ per archiviare i dati dei clienti e inoltre, nel processo di storage, li protegge e li crittografa, assicurando così che le policy di protezione dei dati avanzate siano continuamente aggiornate per le minacce di oggi.

Nel layer dell'hardware:
VMware Cloud Foundation aiuta anche con i problemi associati all'hardware. Esistono non solo opzioni per l'analisi del codice dinamica nei carichi di lavoro, ma anche opzioni per gestire in modo fluido problemi come le vulnerabilità della CPU, con una possibilità di scelta che permette all'organizzazione di allineare la sua risposta ai requisiti aziendali.

Memoria:
VMware NSX Sandbox trova i processi di malware e frammenti di malware che cercano di nascondersi nella memoria e agisce immediatamente per proteggere le infrastrutture.

Firewall di nuova generazione in VMware Cloud Foundation

Il firewall perimetrale, noto anche come firewall di rete, è una misura di sicurezza tradizionale utilizzata per controllare il flusso del traffico di rete tra le reti interne ed esterne. I firewall perimetrali possono offrire un prezioso layer di sicurezza, ma presentano anche dei limiti, come visibilità limitata sul traffico di rete interno, protezione limitata contro le minacce avanzate e protezione limitata per gli utenti dei dispositivi mobili o remoti.



Il firewall distribuito (DFW) è un firewall di tipo stateful, ovvero monitora lo stato delle connessioni attive e utilizza queste informazioni per determinare quali pacchetti di rete lasciar passare attraverso il firewall. Il DFW è implementato nell'hypervisor e applicato alle macchine virtuali per ogni vNIC. Questo significa che le regole del firewall vengono applicate alla vNIC di ogni macchina virtuale. L'ispezione del traffico avviene nella vNIC di una VM quando il traffico sta per uscire dalla VM ed entrare nello switch virtuale (uscita). L'ispezione avviene nella vNIC anche quando il traffico esce dallo switch ma prima che entri nella VM (entrata).

Ogni VM ha il proprio contesto e le proprie regole delle policy del firewall. Durante vMotion, quando le VM si spostano da un host ESXi a un altro host, il contesto del DFW (tabella Rules, tabella Connection Tracker) si sposta con la VM. Inoltre, tutte le connessioni attive rimangono intatte durante vMotion. In altre parole, la policy di sicurezza del DFW è indipendente dalla posizione della VM.

Conclusioni

La sicurezza è un aspetto importante della modernizzazione del data center che aiuta a proteggere le applicazioni e i dati essenziali di un'organizzazione dagli attacchi informatici. Per proteggere i dati sensibili, è importante implementare misure di sicurezza solide come la segmentazione della rete, i firewall, i sistemi di rilevamento e prevenzione delle intrusioni e la crittografia. La modernizzazione dell'infrastruttura complessiva del data center migliora la sicurezza e consente di adottare un approccio più granulare alla prevenzione delle minacce.

- **L'utilizzo di un'architettura Software-Defined Data Center (SDDC)** come VMware Cloud Foundation permette l'automazione e l'orchestrazione dell'infrastruttura e della sicurezza. Questo agevola l'applicazione coerente delle policy di sicurezza in tutto il data center e consente di rispondere velocemente agli incidenti di sicurezza.
- **L'implementazione della virtualizzazione della rete** come VMware NSX, come parte di VMware Cloud Foundation, permette la creazione di più reti virtuali in un'unica rete fisica. Questo abilita il controllo granulare del traffico di rete e la microsegmentazione, contribuendo a ridurre la superficie di attacco e a isolare diversi carichi di lavoro e applicazioni gli uni dagli altri, ostacolando il movimento laterale degli hacker all'interno della rete.
- **Il deployment di una migliore analisi delle minacce** attraverso strumenti come la protezione avanzata dalle minacce può fornire alle organizzazioni ulteriori visibilità e informazioni approfondite sulle minacce alla sicurezza, nonché la capacità di rispondere a queste ultime in modo più rapido e più efficace.
- **L'automazione e l'orchestrazione** offrono rapidità nell'identificare gli incidenti di sicurezza e nel rispondere agli stessi, utilizzando strumenti di sicurezza che possono rilevare e affrontare automaticamente le minacce alla sicurezza.
- **Miglioramento della compliance:** la modernizzazione del data center e l'ottimizzazione della sicurezza possono aiutare le organizzazioni a conformarsi a vari requisiti di compliance normativa, ad esempio HIPAA, PCI-DSS e SOC 2, fornendo un'infrastruttura sicura e compliant.

Il deployment di VMware Cloud Foundation integra tutte queste moderne tecnologie e funzionalità di sicurezza in una piattaforma di modernizzazione del data center sicura, compliant e agile.

Item No: Addressing Key Security Concerns in the Modern Enterprise Data Center_IT 4/23