DELL Technologies

5 Raccomandazioni per soddisfare le esigenze di Zero Trust

1	2	3	4	5
Pianifica il cambiamento di paradigma verso la regola "mai fidarsi, verificare sempre"	**Determina il percorso desiderato**	**È l'organizzazione a guidare l'ambiente Zero Trust, non il contrario**	**Concentrati sui dati**	**Applica la regola "mai fidarsi, verificare sempre", in tutto l'ecosistema IT**
Determina il compromesso accettabile tra mitigazione del rischio e impatto aziendale	Miglioramento incrementale della sicurezza	Crea controlli in base alle esigenze aziendali	Assicurati che tutte le attività di rete, dispositivo e utente siano registrate continuamente	Le attività ZeroTrust come l'autenticazione a più fattori e la gestione delle identità devono essere applicate universalmente per evitare lacune critiche
Considera i costi, l'impatto sulle operazioni e sulle entità interessate, nonché i requisiti richiesti dalle normative vigenti e di conformità	Hyperscaler	Documenta processi, ruoli, responsabilità e classificazioni dei dati	Utilizza l'AI e l'ML per analizzare i dati e identificare anomalie che potrebbero indicare minacce	Includi supply chain fisiche e digitali di terze parti nel framework Zero Trust
Passa dalla sicurezza perimetrale a un modello micro-segmentato e incentrato sui dati	Ambiente dedicato	L'esperienza utente rimane fondamentale	Tieni presente che la protezione di dati e applicazioni è un ruolo chiave dell'architettura Zero Trust	
Se necessario, sfrutta l'aiuto esterno	L'identità è il nuovo perimetro	Miglioramenti alla sicurezza come Zero Trust non possono essere a scapito della fruibilità		
		Gli obiettivi organizzativi, come crescita e innovazione, restano fondamentali		

Zero Trust è ampiamente considerato come la best practice per l'architettura di sicurezza.

I dati dimostrano che la maggior parte delle organizzazioni ha iniziato a considerare o sta implementando Zero Trust[1]. Sebbene il passaggio a Zero Trust sia un fattore importante, esistono alcune considerazioni pratiche e utili nel guidare la transizione.

Gli esperti in materia di Dell Technologies, Tracy Emmersen, Director of Solution Adoption per Project Fort Zero e Justin Vogt, Principal Security Engineer, hanno condiviso le loro raccomandazioni e informazioni con Ash Lakshmanan, Security Services Product Manager. I loro suggerimenti principali sono riepilogati di seguito, oppure puoi guardare la loro intera conversazione all'indirizzo dell.com/cybersecuritymonth.

> "Quando consideriamo Zero Trust da un punto di vista olistico, quando facciamo un passo indietro, ci accorgiamo che tutto riguarda i dati".
>
> ***Tracy Emmersen***
> *Director of Solution Adoption per Project Fort Zero, Dell Technologies*

Pianifica il (grande) cambiamento di paradigma verso la regola "mai fidarsi, verificare sempre"

Per quanto riguarda i fondamentali, il passaggio a un ambiente Zero Trust rappresenta un importante passaggio da modelli di sicurezza storici a un modello basato sui principi di mai fidarsi, verificare sempre e accesso con meno privilegi. "Dobbiamo osservare il nostro profilo di sicurezza in modo diverso da quello passato, allontanandoci dalle tradizionali soluzioni di sicurezza di rete perimetrali e avvicinandoci a un'architettura micro-segmentata e incentrata sui dati", sottolinea Emmersen.

Determina il percorso desiderato

Emmersen ha spiegato tre percorsi distinti per ottenere i vantaggi di Zero Trust:

- **Incrementale:** un approccio iterativo che porta i principi chiave di Zero Trust nell'ambiente attuale
- **Hyperscaler:** sfruttare le funzionalità Zero Trust dei principali provider di cloud
- **Ambiente dedicato e completamente conforme:** Ambiente privato, on-premise, costruito interamente da zero e conforme agli standard Zero Trust

Oltre a questi tre percorsi, le aziende virtualizzate, di piccole e medie dimensioni possono adottare un approccio chiamato "L'identità è il nuovo perimetro". Questa metodologia si concentra sulla gestione delle identità e degli accessi e sfrutta gli strumenti SaaS per ottenere una protezione basata su Zero Trust. Una componente fondamentale di questo metodo è l'implementazione dell'autenticazione a più fattori (MFA) ovunque, che illustra l'impatto di questa funzionalità Zero Trust.

Gli approcci all'hyperscaler e all'identità sono in genere più economici, mentre gli ambienti incrementali e dedicati richiedono un investimento maggiore.

È l'organizzazione a guidare l'adozione di Zero Trust, non il contrario

Alla base, l'architettura Zero Trust è progettata per amministrare e proteggere i flussi di lavoro, i ruoli utente e i privilegi correlati, i dispositivi, i dati, le applicazioni e le reti di un'organizzazione. La prima fase dell'implementazione richiede la redazione di una documentazione completa ed esaustiva riguardante questi aspetti e successivamente il piano di gestione e l'infrastruttura vengono progettati in modo tale da applicare le policy che regolano tali aspetti.

Se l'ambiente Zero Trust inibisce o altera in modo significativo le operazioni aziendali a scapito dell'organizzazione, qualunque sia il migliore livello di sicurezza che si ottiene, probabilmente non vale la pena. Come evidenzia Vogt, "Se [la sicurezza]... ostacola la core mission dell'organizzazione... non siamo migliori dei nemici che stiamo cercando di sconfiggere. Abbiamo solo fornito il nostro Denial of Service".

Concentrati sui dati

Come sottolinea Emmersen, "Quando consideriamo Zero Trust da un punto di vista olistico, quando facciamo un passo indietro, ci accorgiamo che tutto riguarda i dati". La protezione dei dati dell'organizzazione è uno dei vantaggi più importanti derivanti dal passaggio a Zero Trust e principi come la verifica e la segmentazione continue proteggono i dati e le applicazioni impedendo alle minacce di muoversi lateralmente all'interno della rete.

La registrazione e il monitoraggio continuo sono componenti fondamentali di Zero Trust e vengono analizzati dati e telemetria per identificare anomalie che potrebbero indicare un rischio o una minaccia. Ad esempio, una modifica dei modelli di utilizzo dei dati può identificare potenziali fuoriuscite di dati o un attacco ransomware.

1. Dallo studio condotto per conto di Dell dall'Enterprise Strategy Group, "Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust", novembre, 2023

DELL Technologies

Data la grande quantità di dati generati dalla registrazione di tutte le attività, i moderni strumenti di analisi devono utilizzare l'AI e l'apprendimento automatico per essere efficaci.

La regola "Mai fidarsi, verificare sempre" deve essere applicata ovunque

Mentre gran parte dell'attenzione su dati, applicazioni, utenti e dispositivi è interna, il controllo inerente a un'architettura Zero Trust deve essere applicato per tutto il ciclo di vita dell'IT. In caso contrario, potrebbero verificarsi delle importanti lacune di sicurezza.

La supply chain è un ottimo esempio e Vogt consiglia di porre domande importanti riguardanti l'hardware e il software di terze parti:

- "Chi altro ha avuto accesso?
- Di cosa è fatto?
- Cos'altro si nasconde sotto la superficie?
- Come è possibile adottare questi principi di non fiducia [e] avere un processo di verifica e un approccio in qualche modo meno privilegiato rispetto alla tecnologia che stiamo usando? Anche se è a un gradino più alto della supply chain tecnologica?

Il passaggio a un'architettura Zero Trust o l'implementazione dei suoi principi rappresenta l'attuale best practice per far progredire la maturità della sicurezza informatica. Molti percorsi presentano diverse opzioni che implicano un compromesso tra il costo, il livello di rischio e l'entità del potenziamento della sicurezza. Il primo passo deve essere quello di determinare la posizione ottimale dell'organizzazione e di guidare le decisioni tecnologiche.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**

DELL Technologies