

Implementare un approccio Zero Trust per la protezione dei bot e la sicurezza di Web e API



L'approccio Zero Trust è una delle tre tendenze più interessanti identificate nello State of Application Strategy 2022 report di F5 e negli ultimi dodici mesi ha sicuramente riscosso un significativo interesse su Google Trends.

Il risultato è che lo Zero Trust è uno degli approcci alla sicurezza più discussi – e travisati – da quando è entrato in scena lo “shift left”. Troppo spesso lo Zero Trust viene equiparato a una tecnologia specifica, come il software-defined perimeter (SDP), o a un segmento di mercato, come l'identity and access management (IDAM).

Abbiamo assistito alla stessa corsa all'equiparazione a tecnologie o prodotti specifici quando è stato introdotto il cloud computing. Il “cloud washing” era un fenomeno che si verificava regolarmente e spesso veniva usato come osservazione dispregiativa sull'effettiva “cloudiness” di qualche nuovo prodotto.

La sicurezza Zero Trust è, in sostanza, una impostazione mentale dalla quale emergono tecniche e tattiche che sfruttano tecnologie specifiche, che possono essere applicate per affrontare un ampio spettro di minacce alla sicurezza.

Questa mentalità si basa su una serie di presupposti: la scelta e l'uso di specifiche tecnologie sono conseguenze di tali presupposti.

L'implementazione di una tecnologia come l'SDP o la sicurezza

delle API non significa che abbiate adottato lo Zero Trust. Non esiste un singolo prodotto che, una volta adottato, consenta di affermare di essere “conformi allo Zero Trust” e quindi immuni da attacchi, violazioni o exploit.

È vero che la sicurezza di SDP e delle API può essere una risposta tattica adeguata all’adozione di un approccio Zero Trust. Ma per arrivarci è necessario partire da alcuni presupposti fondamentali e poi, in base ad un processo logico, decidere quali sono gli strumenti e le tecnologie migliori da adottare per raggiungere l’obiettivo.

Vediamo alcuni esempi che, come suggerisce il titolo, ci portano a concludere che la protezione dai bot e la sicurezza del web e delle API fanno parte della “cassetta degli attrezzi” di un approccio Zero Trust.

1. Un approccio Zero Trust presuppone una compromissione a priori, e cioè che gli utenti legittimi con accesso autorizzato possano essere stati compromessi e quindi costituire una minaccia involontaria e molto costosa. Gli aggressori sanno che di solito è più facile entrare dalle finestre (gli utenti) che dalla porta principale (la rete aziendale). Gli utenti sono costantemente minacciati e quindi l’ipotesi che siano già compromessi è il presupposto più sicuro da cui partire. Le azioni potenziali di un computer portatile o di un telefono cellulare aziendale compromesso sono molteplici e comprendono il lancio di attacchi contro siti Web e applicazioni che tentano di condividere materiale dannoso (tra cui malware, ransomware o la prossima minaccia che arriverà) o di sfruttare le vulnerabilità per ottenere l’accesso. Poiché le API stanno aumentando il modo in cui le applicazioni mobili e basate sul Web accedono alle applicazioni e ai sistemi aziendali, diventa importante ispezionare i contenuti provenienti anche da utenti legittimi e autenticati per determinare se sono dannosi o meno. Per questo motivo, la sicurezza

del Web e delle API è una scelta logica per implementare la protezione contro questo rischio.

2. Un approccio Zero Trust presuppone che le credenziali non siano sufficienti. Che l'utente sia un essere umano, una macchina o un software, un approccio Zero Trust presuppone che anche se vengono presentate credenziali legittime, l'utente effettivo potrebbe non essere legittimo. Il credential stuffing, del resto, è un problema costante che sfrutta credenziali legittime, ma rubate. È risaputo che, in media, ogni giorno un milione di nomi utente e di password viene segnalato come divulgato o rubato. Un'analisi di F5 conclude che lo 0,5%-2% di un elenco di credenziali violate sarà valido su un sito web o un'applicazione mobile presi di mira. Pertanto, un approccio Zero Trust dovrebbe adottare misure per verificare non solo le credenziali, ma l'identità stessa dell'utente. Ciò include la scoperta di bot mascherati da utenti legittimi. Dal punto di vista tattico, questo fa sì che la protezione dai bot, che può essere chiamata anche rilevamento dei bot, svolga un ruolo importante in un approccio Zero Trust.
3. Un approccio Zero Trust presuppone che il cambiamento sia costante. Lo Zero Trust rifiuta l'ipotesi che, una volta verificato un utente e autorizzato l'accesso a una risorsa, non vi siano rischi. Ogni transazione viene considerata rischiosa e valutata in base al contenuto che trasporta e all'utente che la sta inviando. Il dirottamento di sessione è un metodo di attacco reale, dopo tutto. La vigilanza costante è (o dovrebbe essere) il motto dello Zero Trust, che implica la costante ricerca di contenuti dannosi. Per questo motivo, la sicurezza del Web e delle API e il rilevamento dei bot sono componenti fondamentali di un approccio Zero Trust.

Ora, questo approccio porta anche ad altri strumenti e tecnologie, come l'SDP e il controllo dell'identità e dell'accesso, i firewall di rete e i Cloud Access Security

Broker (CASB), e una serie di altre soluzioni che mitigano i rischi noti che derivano naturalmente da questi presupposti. Ma non si può implementare solo uno di questi strumenti e considerare conclusa l'attività Zero Trust. È come prendere un analgesico per curare una gamba rotta invece di andare dal medico. Certo, riduce il dolore, ma non fa nulla per affrontare il resto del problema.

L'adozione dello Zero Trust come cambiamento di mentalità che porta alla mitigazione non è perfetta – nessun metodo lo è – ma vi porterà più avanti sulla strada dell'adattabilità e della capacità di affrontare attacchi nuovi ed emergenti più velocemente e con maggiore successo.

A cura di **Lori MacVittie**, *Distinguished Engineer di F5*

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/implementare-un-approccio-zero-trust-per-la-protezione-dei-bot-e-la-sicurezza-di-web-e-api/>