10 ASPETTI PRINCIPALI

da considerare in un provider di soluzioni per la sicurezza sul cloud

Cercare un provider per la sicurezza sul cloud può generare confusione. Molti provider sembrano uguali a prima vista: metriche simili, promesse simili. Le informazioni necessarie per fare un vero confronto portano però a porre alcune domande e a richiedere dettagli che i vendor di servizi cloud non forniscono sempre spontaneamente.

Utilizzate questo elenco per assicurarvi di prendere in considerazione tutti gli elementi essenziali nella scelta del giusto provider per la sicurezza sul cloud per proteggere la vostra azienda dagli attacchi informatici pericolosi.

1. **Experience:** da quanto tempo il provider si occupa di sicurezza sul cloud? Quanti clienti conta attualmente in tutto il mondo nell'ambito della sicurezza sul cloud? (È utile un approfondimento sui vettori di attacco globali.) È in grado di supportare la vostra azienda nel modo giusto?

2. **Capacità e scalabilità:** molti vendor di soluzioni per la sicurezza sul cloud hanno una scalabilità sufficiente, ma conta anche il modo in cui misurano tale scalabilità. È opportuno sapere se sono in grado di offrire scalabilità quando serve. Bisogna chiedersi: qual è il più grande attacco DDoS che possono realmente gestire? Possono dimostrare di averlo fatto in caso di attacchi effettivi nella rete?

3. **Performance, distribuzione e disponibilità:** il provider offre soluzioni per la sicurezza sul cloud completamente integrate che incorporano una rete globale di server supportata da automazione e algoritmi basati sui dati? Potete scegliere tra DDoS scrubbing, reti CDN o entrambi?

4. **Intelligence collettiva:** il provider di sicurezza sul cloud ha la scalabilità e il volume di traffico globale necessari per generare intelligence valida? È pronto a sfruttare le competenze accumulate per trarre vantaggio dall'intera base clienti in caso di attacco, durante l'attacco o prima di subirlo? Utilizza un motore di analisi completo dei big data per identificare un singolo autore degli attacchi che può avere un impatto su altri client?

5. **Reputazione IP:** quali origini utilizza il provider di sicurezza sul cloud per assegnare un punteggio di reputazione per gli indirizzi IP? Alcuni prodotti per la reputazione IP hanno livelli di qualità variabili e utilizzano un punteggio di rischio binario per stabilire se si tratta di autori di attacchi o meno, anziché un intervallo di punteggi basato sull'attività pericolosa riscontrata nel corso del tempo.

6. **Accuratezza:** interpretare le rivendicazioni di accuratezza provenienti da diversi vendor WAF (Web Application Firewall) è un aspetto problematico. Il confronto tra due tassi di accuratezza dei vendor non ha alcun valore a meno che non si misurino entrambi con lo stesso test. Scoprite cosa è stato testato, chi è stato testato, e quanti test costituiscono il risultato finale. Assicuratevi di confrontare lo stesso genere di prodotti.

7. **Miglioramento continuo:** la chiave per l'accuratezza è l'ottimizzazione costante delle regole per rimanere aggiornati con il traffico in evoluzione. Con quale frequenza i vendor di soluzioni per la sicurezza sul cloud testano l'infrastruttura di sicurezza: a cadenza mensile, settimanale o giornaliera? Quanto traffico utilizzano per il test?

8. **Tempistiche di mitigazione:** lo SLA (accordo sul livello di servizio) del provider di sicurezza sul cloud è orientato alla velocità e alla qualità di mitigazione o solo ai tempi di risposta? La maggior parte dei vendor può promettere di rispondere in pochi minuti, ma la promessa non può andare oltre l'analisi. Gli SLA (accordi sul livello di servizio) di mitigazione specifici e garantiti a livello di contratto sono una metrica tangibile da utilizzare per confrontare la protezione in modo più accurato.

9. **Il fattore umano (SOC, centri operativi per la sicurezza):** molti vendor rivendicano la protezione attraverso i SOC (centri operativi per la sicurezza) disponibili 24 ore su 24, 7 giorni su 7. Tuttavia, è molto importante scoprire quante strutture conta il proprio vendor per la sicurezza sul cloud, dove si trovano e di che tipo di personale dispongono. Quante persone sono disponibili contemporaneamente? Quali protocolli utilizzano per garantire la copertura fra un turno e l'altro durante un attacco?

10. **Difesa multilivello/Difesa approfondita:** Nessuna soluzione di sicurezza in sé è efficace al 100%. Ma se tutti gli strumenti usati in combinazione si basano sulla stessa tecnologia o hardware, si avranno più livelli con le stesse vulnerabilità e lacune sfruttabili dagli autori degli attacchi. L'approccio migliore consiste nel sovrapporre più livelli di tecnologie all'avanguardia.

Sempre più organizzazioni si affidano al cloud per la sicurezza su Internet. La sicurezza basata sul cloud può offrire a un'azienda maggiore scalabilità, accuratezza e performance migliori rispetto a una singola soluzione in loco. Scegliere una soluzione per la sicurezza sul cloud perfettamente compatibile con l'infrastruttura di sicurezza esistente richiede la reale comprensione dell'offerta.

Ulteriori informazioni sono disponibili nell'ebook gratuito di Akamai, "Why Cloud? The Buyer's Guide to Cloud Security." (Perché il cloud? La guida degli acquirenti alla sicurezza sul cloud.)