SCHEDA TECNICA

Valutazione dell'architettura cloud e della sicurezza

Migliora la protezione dai ciberattacchi attraverso una migliore architettura e configurazione del cloud

VANTAGGI PRINCIPALI

- **Comprensione** delle minacce all'architettura dello specifico ambiente cloud
- **Mitigazione** degli errori di configurazione dell'architettura cloud comunemente sfruttati
- **Riduzione** della superficie di attacco dalle comuni tecniche di sfruttamento
- **Maggiore visibilità** dei principali rischi per la sicurezza legati alle configurazioni esistenti
- **Migliore** monitoraggio, visibilità e rilevamento nel cloud
- **Maggiore priorità** ai giusti miglioramenti di sicurezza per l'ambiente cloud

Perché FireEye Mandiant
FireEye Mandiant è in prima linea nello sviluppo di soluzioni per la sicurezza e l'intelligence informatica dal 2004. I nostri esperti di sicurezza contrastano le violazioni più complesse in ogni angolo del mondo. Conosciamo in dettaglio gli attori di minaccia esistenti ed emergenti, così come la rapida evoluzione delle loro tattiche, tecniche e procedure.

Panoramica
Per ridurre i costi e migliorare la scalabilità, le aziende stanno migrando sempre più le loro risorse on-premise verso il cloud. Come risposta, gli aggressori stanno riallineando le loro tattiche e tecniche, compresa l'ingegneria sociale e lo sfruttamento di configurazioni errate, per mirare agli ambienti cloud.

La valutazione dell'architettura cloud e della sicurezza di FireEye Mandiant valuta l'attuale stato di sicurezza e raccomanda priorità di protezione avanzata per le risorse sulle piattaforme cloud più popolari: Microsoft Azure, Amazon Web Services e Google Cloud Platform.

Questa valutazione aiuta le aziende a comprendere le minacce e i controlli di sicurezza unici per lo specifico ambiente cloud, migliora la protezione dell'ambiente contro le minacce mirate e aumenta la capacità di rilevare, investigare e rispondere alle attività degli aggressori in tutte le fasi del ciclo di vita dell'attacco.

Questi servizi sono progettati per le aziende che utilizzano fornitori di servizi cloud che supportano un modello di infrastruttura distribuita come servizio (*infrastructure as a service*, IaaS) o di piattaforma distribuita come servizio (*platform as a service*, PaaS). Questi modelli si basano su responsabilità condivise tra il fornitore di servizi cloud e il cliente per proteggersi contro gli incidenti informatici. La nostra valutazione si concentra sulle responsabilità del cliente che rafforzeranno la sua posizione di sicurezza.

Il nostro approccio

La valutazione consiste in quattro fasi, durante le quali gli esperti di Mandiant mappano l'ambiente cloud esistente del cliente e determinano il funzionamento dell'attuale programma di sicurezza per proteggerlo:

1ª settimana: revisione documentale iniziale delle strategie di migrazione, diagrammi di architettura, documentazione di protezione avanzata, politiche e standard di gestione dell'accesso, SOP/playbook e standard di registrazione, condotta fuori sede in collaborazione con gli stakeholder del cliente.

2ª settimana: workshop in loco per esplorare l'ambiente cloud del cliente, l'attuale modello di sicurezza in vigore e i potenziali concetti e controlli di sicurezza da implementare in futuro per soddisfare le sue esigenze aziendali.

3ª e 4ª settimana: revisione della configurazione dalla piattaforma cloud per garantire che i controlli di sicurezza siano implementati in modo efficace, identificare i potenziali punti deboli e confermare gli insegnamenti tratti dai workshop in loco per identificare i potenziali punti deboli che potrebbero essere sfruttati dagli aggressori.

5ª settimana: creazione di report che illustrano in dettaglio le raccomandazioni tecniche pratiche per migliorare la protezione dell'ambiente cloud, aumentare la visibilità e il rilevamento e migliorare i processi per ridurre il rischio di compromessi.

RISULTATI FINALI

Il report successivo alla valutazione fornito da Mandiant comprende

- Un'istantanea dell'attuale ambiente cloud, con dettagli sull'architettura esistente e sui controlli di sicurezza.
- Sicurezza per specifici servizi cloud allineati alle attuali configurazioni e ai processi operativi.
- Consigli pratici per migliorare la visibilità e il rilevamento.
- Suggerimenti prioritari e dettagliati per l'ulteriore potenziamento dell'infrastruttura cloud.

Su richiesta sono disponibili briefing di livello tecnico ed esecutivo.

Principali aree interessate durante la valutazione.

Governance, rischi e conformità	Architettura e rete di sicurezza	Gestione delle identità e degli accessi
• Governance e servizi cloud • Criteri e standard del cloud • Valutazioni dei rischi di minacce • Gestione delle vulnerabilità • Requisiti di conformità normativa	• Architettura cloud e controlli di sicurezza • Segmentazione della rete e integrazione on premise • Connettività e gestione remota del sistema • Ripristino di emergenza • Contenitori, configurazioni e controlli di sicurezza	• Infrastruttura di autenticazione cloud, compresa la connettività on premise (ad esempio, ADFS) • Gestione delle identità • Gestione dei privilegi di accesso • Controllo di accesso basato sui ruoli
Protezione dei dati e dei segreti	**DevOps**	**Rilevamento della minaccia e risposta**
• Protezione e prevenzione della perdita dei dati • Sicurezza del database • Gestione delle chiavi e dei certificati • Crittografia	• Configurazioni pipeline • Implementazione del sistema e delle applicazioni • Ciclo di vita sicuro dello sviluppo del software • Controlli di sicurezza dei repository dei codici	• Registrazione di sistema, database e applicazioni • Registrazione di sicurezza e centralizzazione • Controlli di sicurezza degli endpoint e della rete • Processi di risposta agli incidenti cloud

Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Informazioni su FireEye, Inc.
FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.