

Esercizio di simulazione

Valutare la capacità dell'azienda di eseguire in modo efficace il piano di risposta agli incidenti informatici attraverso uno scenario simulato



VANTAGGI

- Identificare le lacune tra risposte documentate/attese e ciò che effettivamente accade.
- Consigli basati sulle migliori pratiche di risposta agli incidenti reali.
- Valutazione rapida, efficiente e non invasiva



“Essere in grado di rispondere in modo efficace ed efficiente agli incidenti di sicurezza è fondamentale per la nostra attività. Gli esercizi di simulazione sono stati utilissimi perché hanno fornito ai team i mezzi necessari per convalidare le decisioni e partecipare alle discussioni”.

-CISO, azienda globale di distribuzione della tecnologia

Perché Mandiant

Mandiant è in prima linea nello sviluppo di soluzioni per la sicurezza e l'intelligence informatica dal 2004. I nostri esperti di sicurezza hanno dovuto contrastare le violazioni più complesse in ogni angolo del mondo. Conosciamo in dettaglio sia le minacce esistenti che quelle emergenti, così come la rapida evoluzione delle tattiche, delle tecniche e delle procedure utilizzate dagli hacker.

L'esercizio di simulazione sfrutta questa esperienza per fornire uno scenario personalizzato basato sull'esperienza reale e studiato per affrontare le aree di rischio fondamentali in campo commerciale e tecnico.

Panoramica

L'esercizio di simulazione valuta i processi di crisi informatica della vostra azienda, gli strumenti e la professionalità nel rispondere agli attacchi informatici da un punto di vista di risposta agli incidenti sia strategica che tecnica esecutiva. Durante l'esercizio, i consulenti MANDIANT introducono vari scenari basati sull'esperienza reale in una tavola rotonda per osservare le azioni simulate e le decisioni di risposta dell'azienda.



CHE COSA SI RICEVE

Brief esecutivo [PPT]

- Una panoramica di persona del gioco, nello specifico:
 - Interazione dei partecipanti con il Piano di risposta agli incidenti (PRI), i piani di comunicazione e le procedure di escalation
 - Lezioni apprese
 - Consigli strategici

Relazione post-azione dell'esercizio di simulazione [PDF]

- Cronologia degli eventi
 - Tutti gli injects
 - Risposta partecipante/parte interessata
- Analisi della risposta strategica agli incidenti informatici e consigli per il miglioramento in relazione al gioco, classificati in base a:
 - Rilevamento
 - Risposta
 - Contenimento
 - Risoluzione

Approccio

Mandiant inizia dalla comprensione del profilo di minaccia dell'azienda, dell'ambiente operativo e delle specifiche aree di interesse. Svolgiamo un laboratorio in loco con persone chiave, presentando scenari in continua evoluzione in base al comportamento dell'aggressore, tecniche e tattiche osservate durante il nostro lavoro di risposta agli incidenti. Durante l'esercizio, osserviamo il gioco per determinare come le azioni e le decisioni simulate vengono eseguite simultaneamente o divergono dai piani e processi aziendali documentati, e dalle migliori pratiche di risposta agli incidenti di Mandiant.

Dopo il laboratorio, condividiamo le nostre osservazioni con l'azienda in un briefing di persona, seguito da una relazione scritta post-azione con una sintesi passo passo degli input e delle risposte in base a ciascuna fase del ciclo di preparazione: Rilevamento, Risposta, Contenimento e Risoluzione.

Processo dell'esercizio di simulazione



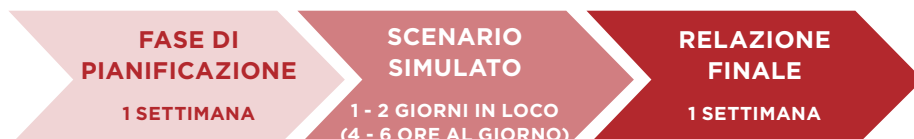
Fase 1:
Fase di pianificazione:
sviluppo scenari e injects



Fase 2:
Laboratorio di simulazione:
presentazione scenari con injects in continua evoluzione e valutazione delle risposte



Fase 3:
Elaborazione e presentazione della relazione: condivisione delle osservazioni e creazione di una roadmap operativa personalizzata.



Per ulteriori informazioni su FireEye, visitare il sito: www.FireEye.com

FireEye, Inc.

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

© 2018 FireEye, Inc. Tutti i diritti riservati.
FireEye è un marchio registrato di FireEye, Inc.
Altri marchi, nomi di prodotto e servizi sono o possono essere rivendicati come proprietà di terzi. DS.TTE.IT-IT-042018

Informazioni su FireEye, Inc.

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Fungendo da estensione semplice e scalabile delle operazioni di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e i servizi di consulenza Mandiant®, rinomati in tutto il mondo. Con questo approccio, FireEye elimina la complessità e il peso della cibersicurezza per le aziende che hanno difficoltà a prepararsi, prevenire e rispondere agli attacchi informatici. FireEye conta oltre 6.600 clienti in 67 Paesi, tra cui più del 45% dei Forbes Global 2000.

