SCHEDA TECNICA

MANDIANT®
A FireEye® Company

Valutazione del rischio assicurativo informatico

Una valutazione del rischio di alto livello per la stipula di polizze assicurative

VANTAGGI

- Individuazione, classificazione e analisi del rischio informatico
- Individuazione dei fattori che potrebbero portare un'organizzazione a subire perdite finanziarie
- Individuazione delle minacce informatiche per l'azienda e per il settore
- Consigli strategici per l'ottimizzazione
- Fornitura delle informazioni necessarie agli assicuratori per valutare il livello di rischio degli assicurati

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 contrastato 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.

Panoramica del servizio
La valutazione del rischio assicurativo informatico si basa sulle conoscenze di Mandiant relative agli aggressori, sull'esperienza nel reagire alle violazioni della sicurezza e su una grande competenza nel valutare il grado di maturità e di reattività dei programmi di sicurezza. Si tratta di uno strumento elaborato specificamente per consentire una valutazione rapida e di alto livello del grado di rischio di un'organizzazione, in base alla tecnologia, ai processi e alle persone di cui si avvale, per agevolare l'individuazione, la classificazione e l'analisi del rischio informatico per la sottoscrizione di polizze assicurative. Il rischio viene valutato in riferimento ai quattro elementi del quadro operativo di sottoscrizione delle polizze assicurative sui beni, noto come C.O.P.E.: costruzione, occupazione, protezione ed esposizione. Il C.O.P.E. è stato esteso in modo da essere applicabile alla valutazione del rischio legato alla tecnologia.

Metodologia
Questo progetto della durata di due settimane combina una valutazione del livello di rischio generale in base al settore di attività dell'organizzazione, alle sue dimensioni e alla situazione geografica, con un punteggio di rischio informatico riferito ai quattro ambiti del C.O.P.E. Sovrapponendo la valutazione del rischio generale nei quattro ambiti e in numerosi sottoambiti, si ricava un punteggio di rischio ponderato per determinare la situazione di rischio di ogni ambito e dell'azienda nel suo insieme.

FireEye

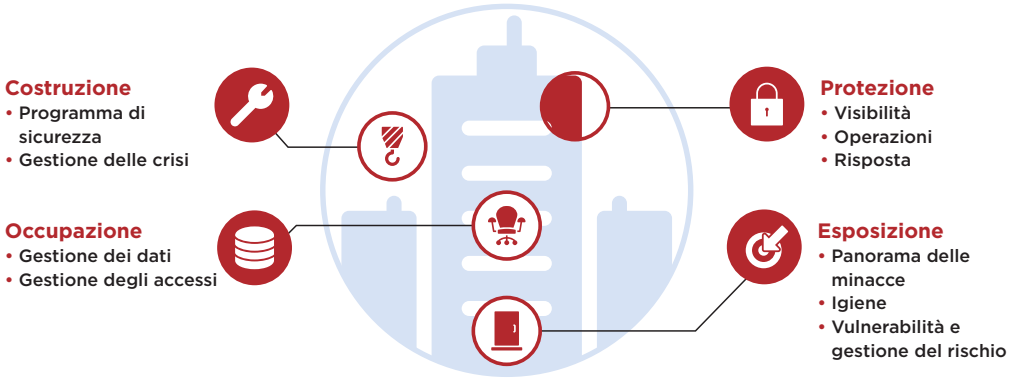

Figura 1. Ambito di rischio assicurativo C.O.P.E.

ELEMENTI FORNITI

- Report sulla valutazione del rischio assicurativo informatico
  - Sintesi
  - Individuazione delle capacità attuali e dei livelli di rischio per i singoli ambiti
  - Consigli strategici per l'ottimizzazione
- Presentazione esecutiva
- Report sulla valutazione delle minacce

Descrizione degli ambiti

Costruzione

Valutazione di come il programma di sicurezza informatica è strutturato, individuando i punti di forza e le aree che presentano opportunità di miglioramento. Le aree esaminate comprendono:

- Politiche e procedure informatiche generali
- Politiche e procedure per la risposta agli eventi, come la notifica delle violazioni e la gestione delle crisi
- Assegnazione del personale
- Consapevolezza degli alti dirigenti e dei manager
- Pratiche di audit e conformità

Occupazione

Processi di revisione dei dati e di gestione delle risorse, comprendenti:

- Politiche di classificazione
- Controlli tecnici per la gestione dei dati
- Requisiti di ricorso alla crittografia
- Politiche di conservazione dei dati
- Politiche di backup e ripristino
- Requisiti standard di generazione e controllo delle risorse per elementi come computer portatili, server e dispositivi mobili

Protezione

Esame del modo in cui l'organizzazione è ben protetta per mezzo di tecnologie, processi e persone dedicate al rilevamento, all'analisi, alla risposta e al contenimento degli attacchi informatici avanzati. Comprende la visibilità delle minacce, le funzionalità di sicurezza operativa e la capacità di risposta agli eventi.

Esposizione

Determinazione dell'esposizione al rischio, valutando il panorama delle minacce in base al settore, al tipo di attività e alle aree geografiche in cui le organizzazioni operano.

- Esame dell'efficacia dei processi e delle politiche in atto per l'individuazione dei rischi relativi alla sicurezza dei dati e dell'attività
- Esame delle politiche di manutenzione del sistema e della rete per determinare l'adeguatezza dei controlli esistenti
- Esame dei processi e delle politiche per valutare le vulnerabilità e risolverle, i requisiti di accesso, la gestione dei log, gli endpoint, la protezione e l'accesso al cloud e ai dispositivi mobili, i test di penetrazione interna ed esterna e la risoluzione delle vulnerabilità individuate

Per maggiori informazioni sui servizi di consulenza di Mandiant, visitare il sito:
www.FireEye.com/services.html

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. 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 sicurezza informatica 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.

FireEye®