Zscaler Risk360™: più vantaggi per il business, meno rischi per la sicurezza

Quantificare, visualizzare e correggere il rischio

Sfida per le aziende

I responsabili della sicurezza non dispongono di un metodo affidabile, ripetibile e basato sui dati per quantificare, mitigare e comunicare il rischio di sicurezza informatica. Al momento non esiste uno standard generale per quantificare il rischio di sicurezza o l'impatto finanziario, né esistono approcci uniformi per raccogliere i dati, normalizzarli e creare un punteggio di rischio concreto; questo è causato dall'utilizzo di molteplici strumenti terzi, come soluzioni per la gestione delle vulnerabilità, strumenti per il rischio di sicurezza, portali di gestione della superficie di attacco, CMDB, sistemi di GRC e controlli di sicurezza. Tutto ciò porta a intraprendere attività incoerenti per la quantificazione e la mitigazione del rischio informatico, che con il tempo finiscono per compromettere le misure dell'organizzazione.

Soluzione: Zscaler Risk360 per quantificare e mitigare efficacemente il rischio informatico

Zscaler Risk360 è un potente framework per la quantificazione e la visualizzazione del rischio che consente di mitigare i rischi legati alla sicurezza informatica. Il suo sistema elabora i dati reali dell'azienda provenienti da fonti esterne e dall'ambiente di Zscaler e genera un dettagliato profilo di rischio.

Il modello di Risk360 impiega oltre 100 fattori basati sui dati e relativi alle quattro fasi di un attacco.

Come funziona Risk360?

Risk360 impiega oltre 100 fattori all'interno dell'ambiente di sicurezza informatica dei clienti per aiutare a comprendere le stime sulle perdite finanziarie, i principali fattori di rischio informatico, i flussi di lavoro investigativi consigliati, i trend e i confronti tra realtà analoghe.

Fornisce inoltre presentazioni utili da mostrare al consiglio di CISO. Questo modello copre i quattro elementi di un attacco, ossia la superficie di attacco esterna, la compromissione, la propagazione laterale e la perdita di dati, oltre a tutte le entità presenti nell'ambiente aziendale, come risorse, applicazioni, forza lavoro e terze parti.

Le funzionalità principali di Risk360

Punteggio di rischio completo e standardizzato per definire il rischio complessivo aziendale relativo alla sicurezza informatica, ottenuto con i controlli di Zscaler e strumenti di sicurezza di terze parti.

Stima dell'esposizione finanziaria potenziale derivante dal rischio informatico, valutando inoltre gli intervalli di risultati del metodo Monte Carlo.

Misurazione del rischio nel tempo per rilevare e mostrare il modo in cui l'organizzazione gestisce il rischio e come quest'ultimo si evolve rispetto ad altre realtà analoghe nel settore.

Il punteggio di rischio aziendale è suddiviso in base alle quattro fasi di un attacco:

- **Superficie di attacco esterna:** traccia l'esposizione della superficie di attacco esterna e visualizza le vulnerabilità sfruttabili, i livelli di gravità e i server e le risorse che si interfacciano con l'esterno esponendo l'impresa a potenziali attacchi.
- **Rischio di compromissione:** comprendi il rischio di subire una compromissione a causa di file dannosi, dell'esposizione a un paziente zero e di utenti che hanno subito un'infezione.
- **Potenziale movimento laterale:** valuta il livello di efficacia del controllo della segmentazione all'interno della azienda.
- **Rischio di perdita dei dati:** misura il rischio di subire un'esfiltrazione di dati a causa di utenti, dispositivi e applicazioni.

Analisi del rischio in base a tutte le entità che contribuiscono a generarlo, come utenti, terze parti, applicazioni e risorse.

Consigli concreti con flussi di lavoro guidati per mitigare rapidamente il rischio di subire attacchi e compromissioni.

Report, mappatura dei rischi e linee guida da presentare al CdA, grazie alla funzionalità "presentazioni per il CdA", che consente di esportare report sui rischi informatici, valutazioni della maturità della sicurezza informatica basate sull'IA e mappature rispetto ai framework di rischio per la sicurezza, come MITRE Attack e NIST CSF, da presentare al consiglio di amministrazione, supportando inoltre la conformità rispetto all'articolo 106 del regolamento S-K della SEC.

Vantaggi principali

- **Potente quantificazione del rischio** per tenere traccia dell'esposizione informatica e finanziaria che mette a rischio l'azienda.
- **Analisi dei principali fattori di rischio informatico** con la possibilità di approfondire quelli che contribuiscono a generarlo.
- **Misurazione automatizzata del rischio informatico** per evitare che i team aziendali debbano districarsi tra fogli di calcolo e strumenti di terze parti.
- **Profilo di sicurezza più efficace** grazie alla mitigazione proattiva delle principali cause di rischio per dispositivi, sistemi, dati e utenti in pochi clic.
- **Conversazioni più produttive con la dirigenza riguardo alla gestione dei rischi**, grazie al punteggio coerente del rischio, alla mappatura del framework di rischio, al supporto della conformità alla SEC e alla reportistica semplificata per il consiglio di amministrazione.

Visita **la nostra pagina web** per scoprire di più su Risk360.

zscaler™ | Experience your world, secured.™

Zscaler, Inc. (HQ)
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
zscaler.it