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

Un framework completo per aiutare i responsabili della sicurezza a quantificare e visualizzare il rischio informatico.

La sfida per le aziende

Gli aggressori esplorano costantemente nuovi modi per sfruttare le superfici di attacco delle organizzazioni, muoversi all'interno dell'ambiente e rubare i dati. Per riuscire a reagire efficacemente, i responsabili della sicurezza si ritrovano a dover misurare, quantificare e mitigare incessantemente e accuratamente il rischio.

Con violazioni di alto profilo che ogni giorno vengono riportate sui giornali e perdite che hanno raggiunto i massimi storici, la quantificazione del rischio di sicurezza informatica (Cybersecurity Risk Quantification, CRQ) è diventata una priorità per i consigli di amministrazione. Purtroppo, gli strumenti indipendenti e i processi manuali per la gestione del rischio rendono praticamente impossibile, per i responsabili della sicurezza, ottenerne una visione olistica e un quadro completo.

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

Zscaler Risk360™ è un framework di rischio completo e pratico che offre una potente quantificazione del rischio informatico. Risk360 consente di visualizzare in modo intuitivo i rischi, indica in modo granulare i fattori di rischio, offre dettagli sull'esposizione finanziaria, report pronti da presentare al CdA e informazioni dettagliate e concrete sui rischi legati alla sicurezza che possono essere sfruttate subito per le attività di mitigazione. 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 dei clienti per aiutare a comprendere le stime sulle perdite finanziarie, i principali fattori di rischio informatico, i flussi di lavoro investigativi consigliati, le tendenze e i confronti con altre aziende analoghe.

Inoltre, consente di esportare diapositive chiare da mostrare al consiglio di CISO. Questo modello copre i quattro aspetti di un attacco, ossia la superficie di attacco esterna, la compromissione, la propagazione laterale e la perdita di dati, e tutte le entità presenti nell'ambiente aziendale, come gli asset, le applicazioni, la forza lavoro e le terze parti.

Le funzionalità principali di Risk360

Un punteggio di rischio completo e standardizzato che riflette il rischio complessivo relativo alla sicurezza aziendale, ricavato dai controlli di Zscaler e dagli strumenti di sicurezza di terze parti presenti nel tuo ambiente.

Stima dell'esposizione finanziaria potenziale derivante dal rischio informatico, valutando anche 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 che possono essere colpite, i livelli di gravità e i server e le risorse che si interfacciano con l'esterno ed espongono 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.

Raccomandazioni pratiche per mitigare rapidamente il rischio di subire attacchi e compromissioni.

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

I vantaggi principali

- **Punteggio di rischio:** visualizza un punteggio di rischio consolidato per tutta la tua organizzazione e monitorane l'andamento nel corso del tempo. Risk360 analizza questo punteggio e lo misura rispetto alle quattro fasi principali di un attacco informatico.
- **Fattori che contribuiscono al rischio:** ottieni valutazioni accurate che riflettano i fattori di rischio nel tuo ambiente IT. Risk360 monitora, normalizza e tiene costantemente conto di oltre 100 fattori predefiniti e personalizzati.
- **Visibilità totale:** scopri il profilo di rischio complessivo con una visione globale del tuo ambiente. Risk360 ti consente di esplorare in profondità qualsiasi rischio e di iniziare a mitigarlo all'istante.
- **Approfondimenti concreti:** riduci i tempi che intercorrono tra l'indagine e l'azione grazie a informazioni dettagliate sui problemi che determinano i tuoi fattori di rischio, così da poter mitigare rapidamente le lacune e adeguare le policy.

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

zscaler™ | Experience your world, secured.™

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