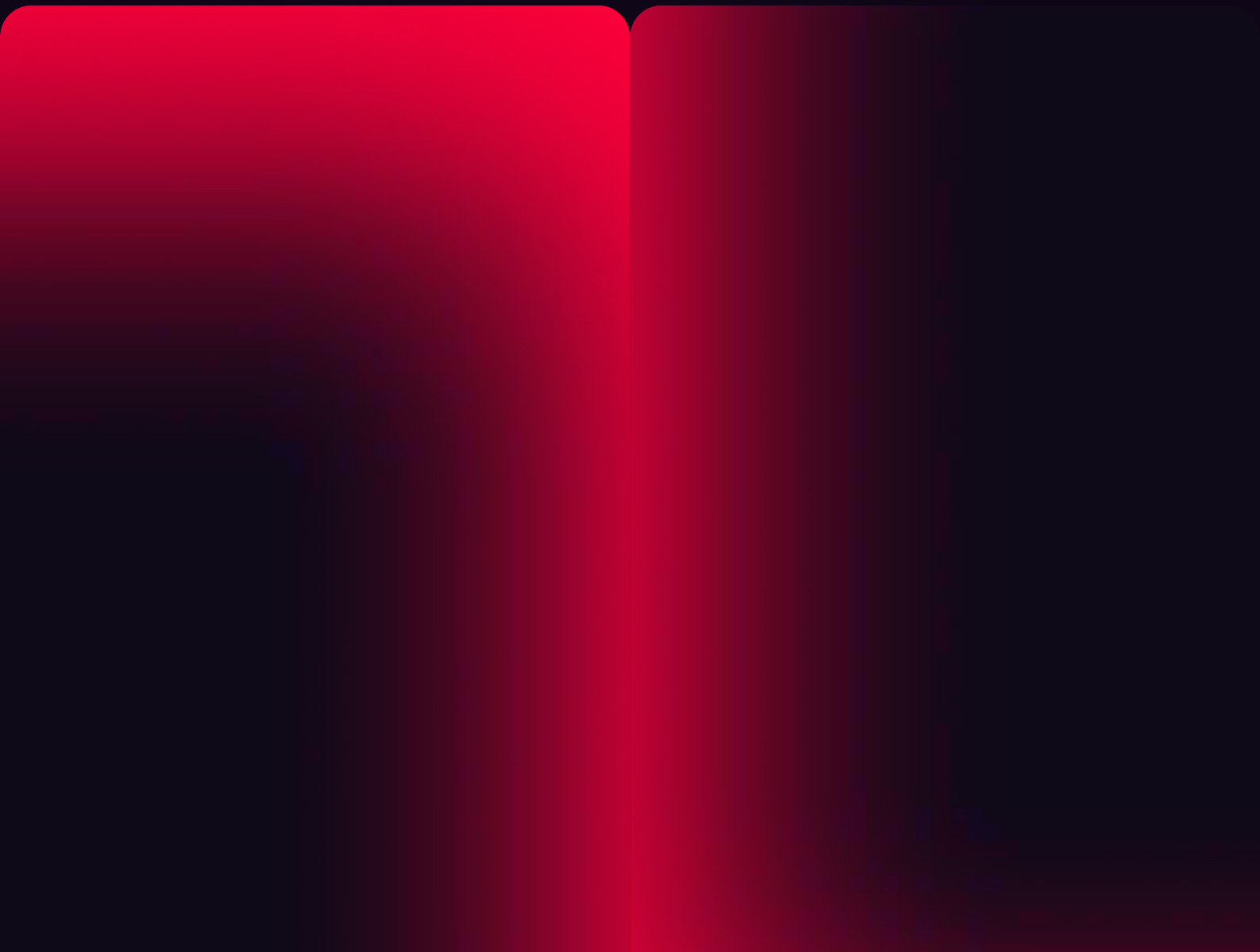
HADRIAN

GUIDE

Oltre il ROI: una guida al valore della prevenzione delle perdite



Una metrica migliore per la sicurezza informatica offensiva

Si tiene costantemente sotto controllo il ritorno sull'investimento (ROI) dei propri strumenti. Tuttavia, quando si tratta di sicurezza informatica offensiva, il modo migliore per dimostrarne il valore è confrontarlo con il costo di una violazione dei dati. Il ROI, pur rimanendo prezioso in determinati contesti, non racconta tutta la storia. Questo documento illustra come utilizzare una nuova equazione per determinare il valore dei propri strumenti di sicurezza informatica offensiva.

Costo delle violazioni dei dati

COSTO TOTALE MEDIO DI UNA VIOLAZIONE.

4,88 MILIONI DI DOLLARI

CRESCITA MEDIA ANNO SU ANNO DEL COSTO DELLE VIOLAZIONI DEI DATI.

10% E IN AUMENTO

RISPARMIO SUI COSTI GRAZIE ALL'USO ESTENSIVO DELL'INTELLIGENZA ARTIFICIALE NELLA PREVENZIONE.

2,2 MILIONI DI DOLLARI

Fonte: IBM Cost of a Data Breach Report, 2024

Valore della prevenzione delle perdite

Sebbene i costi sostanziali associati a una violazione dei dati siano tangibili, il valore della prevenzione proattiva può apparire astratto, complicando la presentazione di un chiaro caso finanziario a favore degli investimenti nella sicurezza. Le metriche tradizionali del ritorno sull'investimento (ROI), sebbene efficaci in molti settori aziendali, risultano insufficienti nella sicurezza informatica, poiché faticano a quantificare con precisione l'impatto degli incidenti evitati. In questo caso, il **valore della prevenzione delle perdite (Value of Loss Avoidance, VLA)** rappresenta una soluzione superiore, poiché quantifica direttamente l'investimento nella mitigazione delle esposizioni rispetto alle potenziali perdite finanziarie derivanti da incidenti informatici, fornendo così un metodo chiaro per dimostrare come le spese per la sicurezza proteggano attivamente le aziende da violazioni significative.

Il valore della prevenzione delle perdite (VLA) è una semplice iterazione del ROI in cui si sostituisce l'utile netto con le perdite evitate.

Semplice, vero? Non così in fretta.

Per ottenere un calcolo più accurato basato sui dati e non su medie o speculazioni, esiste una tabella utile che può aiutarti a determinare un ambito di costo più preciso.

Intervalli della scala di probabilità di sfruttamento (LES)

La scala di probabilità di sfruttamento (Likelihood of Exploitation Scale o LES) aiuta a valutare la probabilità che una determinata esposizione venga sfruttata con successo. Questa scala, che va da 0 a 10, fornisce un quadro chiaro per comprendere l'urgenza e il potenziale impatto delle varie esposizioni.

Probabilità molto alta (10 – 8)

Queste vulnerabilità sono quasi certamente oggetto di attacchi da parte di malintenzionati e vengono spesso sfruttate attivamente. Questa categoria include vulnerabilità zero-day, difetti resi pubblici con exploit funzionanti e vulnerabilità di esecuzione di codice remoto non autenticato frequentemente utilizzate negli attacchi.

Probabilità alta (8 – 3)

Le vulnerabilità di questa categoria sono altamente suscettibili di essere sfruttate. Gli aggressori prendono comunemente di mira difetti accessibili da remoto, vulnerabilità in tecnologie ampiamente diffuse e problemi che richiedono uno sforzo minimo per essere compromessi.

Probabilità moderata (3 – 1)

Le vulnerabilità in questo intervallo hanno una probabilità ragionevole di essere sfruttate, ma in genere dipendono da condizioni aggiuntive. Gli aggressori possono sfruttare difetti che richiedono l'interazione dell'utente, un posizionamento di rete specifico o configurazioni non comuni per avere successo.

Probabilità bassa (1 – 0,2)

È improbabile che queste vulnerabilità vengano sfruttate senza uno sforzo significativo. Lo sfruttamento richiede generalmente catene di attacco complesse, conoscenze specialistiche o accessi privilegiati, il che ne limita l'attrattiva per gli aggressori.

Probabilità molto bassa (0,2 – 0)

Le esposizioni in questa categoria sono raramente sfruttate a causa di forti mitigazioni, visibilità minima o requisiti di attacco di nicchia. Gli aggressori in genere ignorano i difetti nei sistemi isolati, negli ambienti legacy con controlli di accesso rigorosi o in quelli che richiedono condizioni molto specifiche per essere compromessi.

Calcolo della perdita mitigata sulla base delle esposizioni identificate

Quando si stimano le perdite mitigate, è fondamentale tenere conto della probabilità di sfruttamento entro il periodo di investimento. Per calcolare con precisione la perdita mitigata per ciascuna gravità dell'esposizione, iniziamo mappando il numero di esposizioni identificate insieme a un'ipotesi di impatto della violazione. Si tratta del costo finanziario stimato di una violazione a quel livello di gravità. Successivamente, il LES viene utilizzato per quantificare la probabilità di sfruttamento riuscito per ciascuna gravità dell'esposizione. Il LES rappresenta la probabilità che un'esposizione venga sfruttata entro un periodo di tempo definito.

Questo calcolo produce la perdita mitigata per esposizione. La perdita per esposizione può essere calcolata in base al costo medio di quanto segue:

- **Costi di recupero dati**
- **Spese legali**
- **Sanzioni normative e di conformità**
- **Costi di interruzione dell'attività**
- **Indagini forensi**
- **Aumento dei premi assicurativi**

Ciò trasforma probabilità astratte in dati finanziari quantificabili. Ad esempio, considerando un campione di esposizioni identificate, il calcolo risulterebbe il seguente:

VALUTAZIONE DELL'ESPOSIZIONE	LES	PERDITA PER ESPOSIZIONE
Critica	3	146.400 $
Elevata	1	34.160 $
Media	0.5	4.880 $
Bassa	0.1	195 $

Differenze per settore

Purtroppo, non tutti gli attacchi informatici sono uguali e ci sono alcuni settori che i criminali informatici prendono di mira più di altri a causa dei margini elevati, dei dati preziosi o della proprietà intellettuale riservata.

Qualunque siano le ragioni, alcuni settori dovrebbero essere pronti ad aggiungere un moltiplicatore al loro numero totale di esposizioni per far fronte alle crescenti pressioni che questi settori devono affrontare. È possibile utilizzare questa tabella come riferimento:

SETTORE	Moltiplicatore
PRODUZIONE	x7 numero totale di esposizioni
FINANZA	x7 numero totale di esposizioni
SANITÀ	x5 numero totale di esposizioni
PUBBLICA AMMINISTRAZIONE	x4 numero totale di esposizioni
ENERGIA	x3 numero totale di esposizioni
VENDITA AL DETTAGLIO	x2 numero totale di esposizioni
ALTRO	Nessun moltiplicatore

Calcolo del VLA

Tenendo presente che le esposizioni raramente si verificano in modo isolato e che spesso molte esposizioni si verificano in concomitanza con altre esposizioni, i costi potrebbero aumentare molto rapidamente. In un caso conservativo, se si hanno 3 esposizioni critiche, 5 esposizioni elevate, 8 esposizioni medie e 12 esposizioni basse con gli stessi punteggi LES sopra elencati, si arriva rapidamente a un costo di violazione dei dati pari a **636.380 dollari.**

Torniamo alla nostra equazione del valore della prevenzione delle perdite:
VLA = Perdita totale evitata - Costo dell'investimento nello strumento

E se inseriamo le nostre ipotesi con un costo medio di uno strumento di sicurezza proattivo pari a 70.000 dollari.

Il VLA in questa stima ammonta a oltre mezzo milione di dollari. La perdita causata dalla violazione supera di gran lunga il costo dello strumento che avrebbe potuto prevenirla.

Fornite risparmi finanziari misurabili al vostro consiglio di amministrazione

Il valore della prevenzione delle perdite (VLA) consente ai team di sicurezza di giustificare efficacemente le richieste di budget quantificando il potenziale impatto finanziario delle esposizioni mitigate. Questo approccio dimostra come gli investimenti strategici in strumenti di sicurezza prevengano in modo proattivo incidenti costosi, traducendo esposizioni di sicurezza astratte in metriche finanziarie chiare che risuonano direttamente con i dirigenti e i membri del consiglio di amministrazione.

A differenza delle metriche tradizionali, come il numero di incidenti prevenuti o la percentuale di esposizioni mitigate, che spesso non riescono a trasmettere il loro significato finanziario ai leader aziendali, il VLA sposta l'attenzione sui risultati finanziari misurabili. Ciò illustra con precisione come gli investimenti nella sicurezza informatica migliorino direttamente i profitti di un'organizzazione.

Hadrian è una piattaforma di sicurezza offensiva basata su IA agentica che aiuta i moderni team di sicurezza a prevenire le violazioni valutando continuamente la superficie di attacco esterna, convalidando le minacce reali e dando priorità alle esposizioni sfruttabili. L'IA agentica offre una visibilità 10 volte superiore sui rischi critici, elimina i falsi positivi e fornisce una guida passo passo per la risoluzione dei problemi. Le organizzazioni riducono i tempi di risoluzione dell'80%, recuperano più di 10 ore alla settimana e agiscono prima che gli aggressori possano farlo.