Rischio positivo nell'ambito della sicurezza informatica

AWS Linee guida prescrittive

AWS Linee guida prescrittive: Rischio positivo nell'ambito della sicurezza informatica

Table of Contents

Rischio positivo nell'ambito della sicurezza informatica

Greg Bell, Amazon Web Services (AWS)

Maggio 2022 (cronologia dei documenti)

La maggior parte delle persone pensa al rischio da una prospettiva negativa, come l'esposizione a perdite o la gestione di un evento avverso. Tuttavia, l'Organizzazione internazionale per la normazione (ISO) definisce il rischio come "l'effetto dell'incertezza sugli obiettivi". In questo caso, l'effetto può essere positivo o negativo.

I rischi effettivi possono variare da un settore all'altro, ma questa definizione standard si applica a tutti i settori, ognuno dei quali presenta rischi negativi e positivi. Nel settore della sicurezza informatica, il rischio negativo si riferisce alla perdita potenziale e il rischio positivo si riferisce al potenziale guadagno di risorse, conoscenze, miglioramenti o dati.

I settori del project management e dell'IT hanno scelto di valutare i rischi positivi nei report e nelle decisioni aziendali. Per il settore della sicurezza informatica, tuttavia, questa strategia non rappresenta ancora una pratica comune e molte metodologie di gestione del rischio continuano a concentrarsi sui rischi negativi. Quando si parla di rischi positivi, lo si fa solo brevemente.

Tradizionalmente, la sicurezza informatica considera il rischio esclusivamente da un punto di vista negativo. Di seguito sono riportati i due tipi più comuni di rischio negativo nella sicurezza informatica:

- Rischio downside: esposizione a perdite derivante da fattori esterni, come una minaccia. I criminali informatici potrebbero, ad esempio, introdurre o aumentare la probabilità di un incidente di sicurezza.
- Rischio upside: esposizione a perdite che si verifica durante la ricerca di un vantaggio, ad esempio una vulnerabilità derivante dal cambiamento. Ad esempio, quando si implementa una strategia IT, si potrebbe inavvertitamente aumentare il potenziale di un incidente di sicurezza. Il rischio upside non corrisponde al rischio positivo. Anche se si verifica mentre si persegue un guadagno, il rischio upside si concentra sul potenziale di perdita.

Fino a poco tempo fa, la sicurezza informatica considerava solo il rischio negativo e la definizione di rischio si concentrava su un potenziale esito negativo. I rischi positivi si concentrano sul potenziale esito positivo all'inizio dell'identificazione del rischio. L'esclusione del rischio positivo comporta il mancato riconoscimento degli esiti positivi nella sicurezza informatica. A causa dell'attenzione rivolta al rischio negativo, la leadership esecutiva percepisce generalmente la sicurezza informatica come

reattiva anziché proattiva, sottovalutando il suo contributo al conseguimento di risultati aziendali positivi.

Questo documento definisce il rischio positivo per il settore della sicurezza informatica e illustra i vantaggi e l'importanza di includere i rischi positivi nella strategia di sicurezza informatica.

Vantaggi del rischio positivo

Soprattutto in un settore come quello della sicurezza informatica, che si concentra sulla protezione dell'azienda da potenziali perdite, è probabile che il rischio venga interpretato da una prospettiva negativa. Riformulare i rischi di sicurezza informatica in base ai loro potenziali vantaggi può giovare all'azienda, promuovendo risultati positivi, aumentando la sicurezza dell'organizzazione e la fiducia dei clienti.

Promuovere risultati positivi

Un approccio basato sul rischio positivo consente all'organizzazione di valutare e riconoscere il contributo che il dominio dà ai risultati aziendali positivi. Secondo il report Cybersecurity In The C-Suite and Boardroom (di Enterprise Strategy Group):

- Il 69% dei leader aziendali e tecnologici ritiene che la sicurezza informatica appartenga interamente o prevalentemente all'ambito tecnologico, con un legame minimo o nullo con le attività aziendali.
- L'11% dei leader aziendali e tecnologici equipara la sicurezza informatica alla conformità normativa.
- L'82% delle organizzazioni sostiene che i rischi di sicurezza informatica sono aumentati negli ultimi due anni a causa di fattori quali l'aumento delle minacce informatiche, la maggiore integrazione della tecnologia all'interno delle aziende e la crescente superficie di attacco.

Quando i responsabili della sicurezza informatica integrano i rischi positivi nelle conversazioni e nei report, contribuiscono a promuovere il valore delle operazioni IT sicure all'interno dell'azienda.

Ad esempio, supponiamo che alcuni anni fa un'azienda abbia subito una violazione dei dati causata dalla mancanza di un processo di gestione delle patch. L'incidente viene ancora riportato dai media e influisce sulla percezione dei clienti e sulle interazioni con l'azienda. L'azienda vuole lasciarsi alle spalle l'incidente ed espandere la propria offerta di servizi, ma la scarsa fiducia dei clienti blocca le vendite. La sicurezza informatica sfrutta il rischio positivo per convincere la leadership a investire in un processo di gestione delle patch che aggiorna continuamente le applicazioni. Il nuovo processo riduce drasticamente il rischio di violazione dei dati, migliorando il livello di sicurezza dell'azienda. Le notizie sul processo di gestione delle up-to-the-minute patch raggiungono i media e i potenziali clienti. che ora si sentono a proprio agio ad acquistare dall'azienda, facendo così aumentare le vendite in modo straordinario.

La mancata considerazione dei rischi positivi durante l'identificazione del rischio può comportare una valutazione incompleta e influenzare le decisioni aziendali. Per esempi concreti di rischi positivi che potrebbero influenzare le decisioni aziendali, vedi Esempi di rischio positivo.

Aumento del livello di sicurezza e della fiducia dei clienti

La sicurezza informatica è parte integrante del livello di sicurezza di un'azienda. Le violazioni dei dati possono influire negativamente sulla fiducia dei clienti, ma un livello di sicurezza elevato e una reputazione solida possono aumentare la fiducia dei clienti e favorire le opportunità commerciali.

Come illustrato in Promuovere risultati positivi, le ricerche dimostrano che i dirigenti comprendono i rischi negativi associati alla sicurezza informatica, ma spesso non ne comprendono i rischi positivi o il valore aziendale. Tuttavia, le ricerche dimostrano che i dirigenti che si occupano di sicurezza informatica sono consapevoli di quanto un livello di sicurezza elevato possa essere vantaggioso per l'organizzazione.

In Cyber Security Research: The Innovation Accelerator (whitepaper di Vodafone), Vodafone ha intervistato 1.434 responsabili delle decisioni in materia di sicurezza informatica a livello mondiale. Secondo i loro dati:

- Il 73% degli intervistati ritiene che una sicurezza elevata crei nuove opportunità commerciali.
- L'89% ha dichiarato che un miglioramento della sicurezza aumenterebbe la fedeltà e la fiducia dei clienti.
- Il 90% ha dichiarato di essere riuscito a migliorare l'immagine dell'azienda, raggiungendo nuovi potenziali clienti e trasformandoli in clienti effettivi.
- L'89% ritiene che avere una sicurezza informatica efficace sia un vantaggio competitivo rilevante, che aiuta a differenziarsi dalla concorrenza.
- Il 24% ha segnalato un aumento dei ricavi grazie all'utilizzo di tecnologie cloud e dell'Internet delle cose (IOT) e all'adozione di controlli di sicurezza IT mirati.
- Quando si comunica con i dirigenti, invece di considerare i potenziali esiti negativi si possono citare anche i rischi positivi per comunicare il valore aziendale del miglioramento della fiducia dei clienti. Spesso i dirigenti possono essere molto cauti quando finanziano i programmi. In alcuni casi, la sicurezza informatica è il requisito minimo per operare. Comunicare internamente i rischi positivi nelle richieste di finanziamento può aiutare i dirigenti a comprendere il valore aziendale della sicurezza informatica. Ciò può comportare un aumento dei finanziamenti per le iniziative di sicurezza informatica e aumentare le entrate per l'azienda.

Modifica del linguaggio legato al rischio nella sicurezza informatica

Parte della sfida legata all'integrazione del rischio positivo nella sicurezza informatica consiste nel fatto che la terminologia tecnica e specifica del settore è incentrata sul rischio negativo, come minacce, vulnerabilità e controlli di sicurezza. Il settore della sicurezza informatica deve sviluppare ed espandere il proprio vocabolario per includere un linguaggio in grado di enfatizzare i risultati aziendali positivi (o rischi positivi) apportati dalla sicurezza informatica alle aziende. Termini come vantaggio aziendale, benefici e valore aziendale evidenziano il contributo della sicurezza informatica all'organizzazione.

La modifica del linguaggio relativo alla sicurezza informatica comporta il cambiamento nell'idea che tale settore sia un'area tecnologica incentrata esclusivamente su minacce e vulnerabilità e che sia indipendente dal business. La leadership aziendale spesso sottovaluta il contributo della sicurezza informatica ai risultati aziendali positivi. Per ulteriori informazioni sulla percezione della sicurezza informatica da parte dei dirigenti, consulta Promuovere risultati positivi.

Adozione crescente in settori correlati

In molti campi c'è un crescente interesse per l'inclusione del rischio positivo, in quanto riconosce i contributi che il dominio apporta ai risultati aziendali. Il concetto di rischio positivo è stato recentemente adottato nei processi e nelle definizioni comuni di project management.

Nel 2013, il Project Management Institute (PMI) ha integrato la definizione di rischio positivo (denominato anche opportunità) nella quinta edizione della Project Management Body of Knowledge (PMBOK). La guida PMBOK definisce il rischio individuale come "un evento o una condizione incerta che, se si verifica, ha un effetto positivo o negativo su uno o più obiettivi del progetto". Definisce il rischio totale di progetto come "l'effetto dell'incertezza sul progetto nel suo insieme... maggiore della somma dei singoli rischi di un progetto, poiché include tutte le fonti di incertezza del progetto... rappresenta l'esposizione degli stakeholder alle variazioni dei risultati del progetto, sia positive che negative".

Sfortunatamente, l'inclusione di esiti positivi nelle definizioni di rischio del PMI non si applica ancora al settore della sicurezza informatica.

Esempi di rischio positivo

Di seguito sono riportati alcuni esempi di rischio positivo per la tecnologia, la gestione dei progetti e la sicurezza informatica.

Rischio positivo per la tecnologia

Un esempio di rischio positivo in ambito tecnologico è il fatto che l'implementazione di una tecnologia potrebbe portare a una riduzione del costo dei salari. Ad esempio:

1. l'implementazione di una tecnologia potrebbe portare a una maggiore efficienza aziendale,
2. la quale potrebbe portare a una riduzione della manodopera
3. che, a sua volta, potrebbe portare a una riduzione del costo dei salari.

Rischio positivo per la gestione dei progetti

Un esempio di rischio positivo per la gestione dei progetti è il fatto che un errore nel calcolo del budget di un progetto potrebbe portare a risparmi sui costi o al finanziamento di progetti aggiuntivi. Ad esempio:

1. l'implementazione anticipata di un progetto tecnologico potrebbe portare il project manager a calcolare male i costi del progetto.
2. Un errore nel calcolo dei costi del progetto potrebbe portare a fondi eccessivi per il progetto,
3. e questo eccesso di fondi potrebbe portare a un risparmio sui costi o al finanziamento di progetti aggiuntivi.

Rischio positivo per la sicurezza informatica

Un esempio di rischio positivo per sicurezza informatica è il fatto che l'implementazione della gestione delle patch potrebbe aumentare la fiducia dei clienti. Ad esempio:

1. L'implementazione della gestione delle patch potrebbe ridurre le vulnerabilità dell'applicazione.
2. La rimozione delle vulnerabilità potrebbe ridurre i rischi delle applicazioni e renderle più sicure.
3. Una maggiore sicurezza delle applicazioni potrebbe ridurre la perdita di dati.

4. La riduzione della perdita di dati potrebbe aumentare la fiducia dei clienti.

Un altro esempio di rischio positivo per la sicurezza informatica è che l'implementazione della risposta agli eventi imprevisti potrebbe aumentare la produttività dei dipendenti. Ad esempio:

1. L'implementazione della risposta agli eventi imprevisti potrebbe portare a rilevare un aumento del traffico di rete.
2. L'aumento del traffico di rete potrebbe portare a rilevare un uso improprio delle risorse da parte dei dipendenti che accedono a contenuti non legati al lavoro, come i servizi di streaming di musica e video. Queste attività consumano la larghezza di banda della rete e possono influire negativamente sulle prestazioni della rete e delle applicazioni.
3. L'individuazione di un uso improprio delle risorse aziendali da parte dei dipendenti potrebbe portare al blocco di questi servizi.
4. Questo potrebbe ridurre il consumo di larghezza di banda della rete, aumentando la produttività dei dipendenti.

Infine, l'ultimo esempio di rischio positivo per la sicurezza informatica è il fatto che l'implementazione di un piano di risposta agli eventi imprevisti potrebbe aumentare le opportunità commerciali e il rispetto delle leggi sulla privacy. Ad esempio:

1. L'implementazione di un piano di risposta agli eventi imprevisti potrebbe portare a rilevare e identificare rapidamente malware e ransomware,
2. riducendo al minimo l'impatto degli eventi imprevisti e mitigando la minaccia per le risorse aziendali.
3. Questo potrebbe portare a nuove opportunità di business e aiutare l'azienda a rimanere conforme alle leggi sulla privacy.

Risposte ai rischi per la sicurezza informatica

Le risposte ai rischi positivi e negativi sono molto diverse. Per i rischi negativi, si adottano misure per ridurre al minimo l'impatto sul risultato, mentre per i rischi positivi si adottano misure per massimizzare l'impatto. La tabella seguente mostra le potenziali risposte ai rischi positivi e negativi.

Tipo di rischio	Risposta	Definizione
Rischio positivo	Sfruttare	Massimizza la probabilità che il rischio si verifichi per realizzarne l'effetto positivo.
	Condividere	Assegna parte della proprietà o della responsabilità del rischio a un'altra parte. Si tratta dello stesso approccio adottato per i rischi negativi e mira a controllare la perdita o il guadagno potenziale.
	Migliorare	Aumenta le condizioni che creano il rischio per sfruttare al massimo l'opportunità.
	Ignorare	Ignora la possibilità del rischio e non intraprende alcuna azione. Questa risposta è comune quando la probabili tà del rischio è molto bassa o quando i benefici di un potenziale risultato positivo sono minimi.
Rischio negativo	Mitigare	Riduce al minimo la probabilità che il rischio si verifichi.
	Trasferire	Trasferisce la responsab ilità del rischio a un'altra

Tipo di rischio	Risposta	Definizione
		parte, ad esempio acquistando una polizza assicurativa per trasferire il rischio a una compagnia assicurativa.
	Evitare	Elimina le condizioni che creano il rischio.
	Accettare	Riconosce l'esistenza del rischio ma non intraprende alcuna azione.

Per quanto riguarda i rischi negativi, le organizzazioni evitano, trasferiscono, attenuano o accettano il rischio, in base alla loro tolleranza e propensione al rischio. Le aziende cercano di prevenire il rischio e, nel caso in cui si verifichi, tentano di minimizzarne l'impatto sulla missione generale.

Il modo migliore per illustrare le risposte relative al rischio positivo consiste nell'utilizzare degli esempi:

- Sfruttare. Un responsabile della sicurezza viene a sapere che un professionista del settore ben qualificato ha recentemente deciso di cercare un nuovo impiego e offre un generoso bonus di assunzione per attirare il potenziale dipendente nel suo team.
- Condividere. Un responsabile di una business unit vorrebbe migliorare la sicurezza utilizzando un prodotto di gestione degli accessi con privilegi, ma non dispone di un budget sufficiente per acquistare gli strumenti e i servizi necessari nell'anno fiscale in corso. Il responsabile collabora con un dirigente di una business unit diversa. Quest'ultimo acquisterà e implementerà lo strumento come progetto pilota e successivamente espanderà l'installazione per supportare entrambe le business unit.
- Migliorare. Un dipendente ha individuato l'opportunità di automatizzare un processo aziendale esistente per ridurre le minacce alla sicurezza informatica, ma ciò richiede un investimento in tempo e attrezzature. Intuendo i vantaggi positivi di tale processo, il manager approva le ore di lavoro straordinario per sviluppare le capacità e riutilizza le risorse hardware e software esistenti che consentono di portare avanti il progetto.
- Ignorare. Un dirigente finanziario scopre che un dipendente del reparto vendite ha sviluppato una nuova applicazione in grado di automatizzare un'attività noiosa e manuale. L'applicazione è stata

recentemente autorizzata per l'uso solo nel reparto vendite. Il responsabile finanziario ottiene una copia della nuova applicazione per raggiungere un vantaggio analogo nel suo reparto, senza autorizzazione esplicita.

Passaggi successivi

I settori della tecnologia e della gestione dei progetti hanno preso in considerazione i rischi positivi nei processi di valutazione del rischio, mentre il settore della sicurezza informatica li ha storicamente esclusi. I rischi positivi possono portare a risultati aziendali favorevoli, motivo per cui il settore della sicurezza informatica deve prenderli in considerazione per sfruttarne i vantaggi.

È possibile iniziare a inserire immediatamente i rischi positivi in tutte le comunicazioni. Ad esempio, le valutazioni dei rischi, le valutazioni della sicurezza o le relazioni sullo stato dovrebbero includere una sezione sui rischi positivi. Le richieste di finanziamento alla dirigenza esecutiva dovrebbero includere i rischi positivi, comunicare i potenziali benefici per l'azienda ed evidenziare i potenziali vantaggi commerciali derivanti dall'approvazione della richiesta.

Domande frequenti

Qual è la differenza tra rischio upside e rischio positivo?

Sebbene i termini rischio upside e rischio positivo possano sembrare sinonimi, in realtà si riferiscono a concetti molto diversi. Il rischio può avere un esito positivo o negativo, mentre l'esito negativo può avere un risvolto favorevole (upside) o sfavorevole (downside).

Il rischio positivo è il potenziale guadagno di risorse, conoscenze, miglioramenti o dati. Si supponga, ad esempio, di implementare la gestione delle patch e adottare un processo per rimuovere rapidamente le vulnerabilità, entro una settimana. Nel corso del prossimo anno, non si verificheranno incidenti di sicurezza.

Il rischio upside è l'esposizione a perdite nel perseguimento di un guadagno. Si supponga, ad esempio, di avere un'azienda che si occupa dell'implementazione di una nuova applicazione e un utente che ha il compito di implementare la gestione delle patch e adottare un processo per rimuovere rapidamente le vulnerabilità, ad esempio entro una settimana. L'esposizione a perdite (il periodo di tempo in cui si rimuovono le vulnerabilità) è finalizzata alla ricerca di un guadagno (un'applicazione più sicura), quindi questo è considerato un rischio upside. È possibile aumentare il rischio upside modificando il processo di rimozione delle vulnerabilità a un giorno oppure ridurre il rischio upside modificando il periodo a un mese. Fondamentalmente, il rischio upside rappresenta l'incerta possibilità di guadagno nel tentativo di minimizzare una perdita.

Perché è importante includere il rischio positivo nell'ambito della sicurezza informatica?

L'integrazione dei rischi positivi nelle valutazioni e nelle conversazioni sui rischi del settore aiuta a promuovere il valore della sicurezza informatica per l'azienda. Per ulteriori informazioni, consulta Vantaggi del rischio positivo.

Risorse

- La sicurezza informatica per vertici aziendali e consigli di amministrazione (rapporto di ricerca di Enterprise Strategy Group)
- Ricerca sulla sicurezza informatica: l'acceleratore dell'innovazione (whitepaper di Vodafone)
- Integrazione della sicurezza informatica e della gestione del rischio aziendale (ERM) (pubblicazione NIST)
- Chiarire i rischi "upside" e "positivi" (post sul blog dell'istituto FAIR)

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	27 maggio 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.