Guida di Insight sui fattori umani nella sicurezza

Insight

Introduzione

In Insight siamo consapevoli dell'importanza di un approccio olistico alla sicurezza. Gli autori degli attacchi cercheranno l'area più debole, non quella più forte. Disponiamo di competenze tecniche nei cinque ambiti delle tecnologie (Endpoint, Application, Cloud, Network, Datacenter e IOT, e Data-centric), ma come solution integrator leader nel settore, riteniamo che sia necessario prestare particolare attenzione alle interazioni tra questi ambiti tecnologici (Governance, Risk and Compliance, Identity and Access, Threat Detection and Response e Human Factors). Le falle di collegamento tra i vari ambiti delle tecnologie spesso sono caratterizzate da un valore aggiunto, che contribuisce a migliorare il livello complessivo di protezione in maniera economicamente vantaggiosa.

Il modello olistico di Insight

Che cosa sono i fattori umani e perché sono importanti?

Anche se le infrastrutture, gli strumenti e i controlli di sicurezza vengono costantemente migliorati e si investa in tali attività, le violazioni continuano a verificarsi e non sono facili da identificare e risolvere. Esistono molti controlli di sicurezza specializzati per diversi tipi di minacce, dagli attacchi agli endpoint agli attacchi alle supply chain, ma quando si esamina come si sono verificati questi attacchi, i tre motivi principali sono:

- **Passwords –** una password non sicura è stata violata, una password predefinita è rimasta invariata oppure la stessa password è stata utilizzata in più siti.
- **Phishing –** un utente è stato indotto a divulgare le proprie credenziali, a visitare un sito web compromesso o ad aprire un allegato infetto.
- **Patching –** una vulnerabilità nota è stata lasciata senza patch per troppo tempo ed è stata sfruttata da un malware, oppure un utente ha installato un software rischioso che è stato compromesso.

I team IT possono utilizzare la tecnologia per contribuire a ridurre la possibilità di violazioni, ma gli utenti finali avranno sempre un ruolo nel supportare la sicurezza di un'organizzazione. I team IT: spesso si concentrano sulla tecnologia e talvolta sul processo, per poi dimenticare il lato umano, quando sono queste a determinare il fallimento o il successo di un progetto.

Processo: le politiche scritte che spiegano cosa dovrebbero o non dovrebbero fare gli utenti assumono molte forme, come politiche sulla sicurezza delle informazioni, contratti di lavoro, manuali per il personale, politiche di utilizzo accettabile o piani di risposta agli incidenti.

Technology: gli strumenti, i sistemi e i controlli che forniscono linee guida e restrizioni su ciò che gli utenti possono fare devono essere abbastanza rigorosi da limitare le attività ovviamente rischiose, ma abbastanza ammissibili da consentire una certa flessibilità e non interrompere i processi aziendali.

Persone: quando non esiste un processo documentato o le persone non lo conoscono, devono affidarsi al proprio giudizio personale. Oppure quando una tecnologia non riesce a prevenire una nuova minaccia, le persone spesso rappresentano la prima e l'ultima linea di difesa, contando solo sulle loro competenze e sulla loro formazione.

Entro il 2027, il 50% dei Chief Information Security Officer (CISO) delle grandi aziende adotterà pratiche di progettazione della sicurezza incentrate sull'uomo per ridurre al minimo gli attriti indotti dalla cybersecurity. E massimizzare l'adozione dei controlli.

- Gartner identifica le principali tendenze di sicurezza informatica per il 2023.

Mancanza di competenze

Poiché il divario di competenze informatiche persiste come ostacolo per le organizzazioni, potrebbe essere necessario trasferire le persone da altre parti dell'azienda a ruoli orientati alla sicurezza e dotarle delle competenze di cui hanno bisogno. La formazione e l'affiancamento sul posto di lavoro hanno i loro limiti quando le competenze necessarie per insegnare sono scarse nell'organizzazione. Per le risorse più qualificate, la formazione è spesso considerata essenziale per mantenere esperti tecnici che desiderano aggiornare le proprie competenze.

Fattori umani possono avere un impatto su quasi tutti gli aspetti della tua strategia di sicurezza.

L’importanza delle persone

È necessario adattare una strategia di sicurezza basata sui fattori umani ai diversi tipi di utenti, o persone, all’interno della propria organizzazione. Un approccio generico non sarà molto efficace: le persone devono essere responsabili in relazione al loro ruolo attuale e comprendere come possono contribuire personalmente alla sicurezza dell’organizzazione.

Qui viene mostrato un esempio di come è possibile categorizzare i tipi di utente in un’organizzazione tipica, ma ogni organizzazione è diversa.

End-user

- Diversi livelli di competenze IT, alcuni possono avere solo conoscenze molto basiche
- Il multilinguismo probabilmente sarà un requisito nelle organizzazioni globali
- Gli argomenti possono riguardare il phishing, il GDPR, la sicurezza fisica, ecc

Sviluppo

- Di solito è tecnicamente avanzato, ma potrebbe non essere a conoscenza delle tecniche di codifica sicura
- È probabile che richieda una formazione di nicchia, utilizzando lo stesso linguaggio di programmazione dello sviluppatore.
- È probabile che la gamification e l’apprendimento pratico abbiano un impatto migliore rispetto a quello non interattivo.

Amministratore IT

- Gli utenti tecnologicamente avanzati vogliono poter sviluppare ulteriormente le proprie competenze esistenti ed essere messi alla prova
- La gamification e la concorrenza possono contribuire a promuovere l’adozione
- Come per i piloti, le competenze pratiche in un ambiente di simulazione sicuro, utilizzate regolarmente, possono aiutare a rispondere a situazioni di sicurezza reali ad alto stress.

Amministratori delegati

- Concentrarsi sulle attività di apprendimento di gruppo basate sul team per testare i processi decisionali e le definizioni di ruoli e responsabilità
- Orientato al business
- Può coinvolgere molti ruoli diversi per testare la dinamica del team

In che modo Insight può essere d'aiuto

Managed Security Awareness per l'end-user

Nell'attuale ambiente digitale, in cui la maggior parte delle operazioni aziendali avviene online, è fondamentale che gli utenti finali siano consapevoli della sicurezza. Le organizzazioni devono assicurarsi che i loro impiegati siano consapevoli dei possibili pericoli degli attacchi informatici e di come possono ridurli. Ciò comporta insegnare agli impiegati come seguire le buone pratiche per la gestione delle password, le abitudini di navigazione sicure e come individuare e segnalare le e-mail sospette.

Gli attacchi di phishing sono uno dei maggiori rischi per la sicurezza informatica di un'organizzazione. Questi attacchi cercano di indurre le persone a divulgare informazioni personali come nomi utente, password o informazioni finanziarie. Le simulazioni di phishing sono un modo utile per insegnare agli impiegati come proteggersi da questi attacchi. Creando false e-mail di phishing che sembrano reali, i dipendenti possono imparare a individuare e segnalare i messaggi sospetti.

Collaboriamo con KnowBe4, un'azienda esperta in formazione sulla security awarenes per gli end-user, che offre una piattaforma completa con moduli di formazione, simulazioni di phishing e altri strumenti che insegnano ai dipendenti a identificare le minacce più recenti e come evitarle. La piattaforma utilizza metodi coinvolgenti, come video, quiz e giochi interattivi, per coinvolgere gli impiegati e rendere più divertente l'esperienza di formazione

La loro metodologia si basa su un ciclo di formazione e test - non una volta all'anno, ma regolarmente in piccoli blocchi in modo che la formazione sia rafforzata e i miglioramenti possano essere misurati. La formazione potrà quindi essere mirata nella giusta quantità e alle persone giuste.

Offriamo una soluzione completa end-to-end che sfrutta la piattaforma KnowBe4 per offrire ai nostri clienti un'efficace formazione sulla security awareness. Il nostro servizio gestito include monitoraggio e reporting continui, consentendoci di identificare le aree in cui potrebbe essere necessaria ulteriore formazione e di fornire un feedback tempestivo ai nostri clienti. Le organizzazioni possono quindi concentrarsi sulle loro attività aziendali principali, mentre noi ci occupiamo delle loro necessità di formazione sulla security awareness, aiutandole a proteggersi dalle minacce informatiche.

Piattaforma di resilienza del personale informatico

Una piattaforma basata su SaaS progettata per esercitare, confrontare, migliorare e dimostrare continuamente la resilienza informatica del personale di un'organizzazione.

Per gli individui:

Un ambiente di apprendimento coinvolgente e gamificato che copre l'intero spettro della formazione tecnica pratica per l'azienda.

- Cyber professionisti offensivi e difensivi
- Sviluppatori ed esperti di sicurezza delle applicazioni
- Professionisti della sicurezza del cloud e delle infrastrutture

Per i team:

Rispondere alle minacce alla sicurezza richiede un lavoro di squadra, dai tecnici ai dirigenti. Coinvolgiamo team provenienti da tutta la tua organizzazione per migliorare le loro capacità decisionali e tecniche di risposta alle crisi per rispondere in modo adattabile ed efficace al rischio informatico.

- Direzione aziendale
- Team di crisis management
- Team tecnici informatici

Per l'organizzazione:

Esercizi di sviluppo delle competenze che guidano il cambiamento comportamentale trasformativo in tutta l'organizzazione.

- Amministratori delegati
- Impiegati di prima linea
- Obiettivi ad alto rischio degli attacchi informatici

Tutti questi elementi sono accessibili da qualsiasi luogo con un semplice browser web, quindi possono essere utilizzati anche da persone esterne alle organizzazioni, ad esempio nell'ambito di una valutazione delle assunzioni preliminari.

In qualità di azienda, sarai in grado di:

- Dimostrare continuamente la capacità informatica
- Migliorare la velocità e la qualità della risposta.
- Migliorare il reclutamento e lo sviluppo della carriera.
- Ridurre le vulnerabilità del cloud e delle applicazioni.
- Ridurre i costi di sicurezza informatica.

Adoption and Change Management

L'adozione e la gestione del cambiamento svolgono un ruolo cruciale nel supporto dei fattori umani nella sicurezza informatica, garantendo che le misure, le politiche e le tecnologie di sicurezza siano adottate e integrate efficacemente nella cultura e nelle pratiche di un'organizzazione. I fattori umani, come il comportamento, la consapevolezza e le abitudini degli utenti, sono spesso gli anelli più deboli della sicurezza informatica, in quanto possono essere sfruttati dai malintenzionati.

Ecco come l'adozione di Insight e la gestione del cambiamento possono essere utili nell'affrontare questi fattori umani::

Consapevolezza e formazione del personale: L'adozione e la gestione del cambiamento implica la formazione degli utenti sulle minacce alla sicurezza informatica, sulle best practice e sull'importanza della sicurezza. Fornendo formazione e comunicazioni chiare, gli utenti diventano più consapevoli dei potenziali rischi e sono in grado di prendere decisioni informate che migliorano la sicurezza..

Cambio di comportamento: La gestione del cambiamento mira a modificare il comportamento degli utenti in linea con le pratiche di sicurezza desiderate. Stabilendo nuove routine e abitudini, gli utenti possono essere incoraggiati ad adottare comportamenti sicuri, come l'aggiornamento regolare delle password, essere cauti nei confronti delle e-mail di phishing e segnalare attività sospette.

Cambio culturale: Iniziative di adozione e gestione del cambiamento efficaci promuovono una cultura della sicurezza all'interno dell'organizzazione. Quando la sicurezza informatica è ben radicata nella cultura organizzativa, i dipendenti sono più propensi a dare priorità alla sicurezza nelle loro attività quotidiane, con il risultato di un ambiente complessivamente più sicuro. Riduzione della resistenza: Spesso le persone resistono ai cambiamenti, soprattutto quando interrompono le loro abitudini familiari. Strategie efficaci di gestione del cambiamento prevedono e affrontano questa resistenza, contribuendo a mitigare la spinta contro le misure di sicurezza e facilitando un'adozione più fluida delle nuove pratiche.

Design incentrato sull'utente: I processi di adozione e gestione del cambiamento implicano la comprensione delle necessità degli utenti e la personalizzazione delle soluzioni di sicurezza per soddisfare tali necessità. Questo approccio incentrato sull'utente aumenta la probabilità di accettazione e riduce l'attrito nell'adozione di misure di sicurezza.

Miglioramento continuo: L'adozione e la gestione del cambiamento sono processi continui che comportano la raccolta di feedback e l'adeguamento delle strategie in base alle esperienze del mondo reale. Ciò consente alle organizzazioni di perfezionare le pratiche di sicurezza in risposta all'evoluzione delle minacce e delle necessità degli utenti.

Canali di comunicazione: Una comunicazione efficace è fondamentale per promuovere fiducia e trasparenza nelle iniziative di sicurezza informatica. L'adozione e la gestione del cambiamento offrono la possibilità di un dialogo aperto tra i team di sicurezza e gli utenti, garantendo che le preoccupazioni vengano affrontate e che i malintesi siano chiariti.

Mitigazione delle minacce interne: Promuovendo un senso di appartenenza e lealtà tra i dipendenti, l'adozione e la gestione del cambiamento possono contribuire a ridurre la probabilità di minacce interne, in cui i dipendenti compromettono intenzionalmente o involontariamente la sicurezza.

Incoraggiare la responsabilità: I processi di gestione del cambiamento enfatizzano la responsabilità individuale e collettiva per la sicurezza. Quando gli utenti si sentono responsabili delle loro azioni, è più probabile che rispettino i protocolli di sicurezza e segnalino tempestivamente potenziali incidenti.

Adattamento alle nuove tecnologie: Il panorama della sicurezza informatica è in rapida evoluzione, con l'emergere frequente di nuove tecnologie. L'adozione e la gestione del cambiamento aiutano gli utenti ad adattarsi a questi cambiamenti fornendo formazione e supporto, garantendo che le nuove tecnologie siano utilizzate in modo sicuro fin dall'inizio.

Conclusione

Le persone rappresentano il principale rischio per la sicurezza di un'organizzazione e devono ricevere una formazione regolare ed efficace per diventare validi guardiani della sicurezza di un'organizzazione. Un individuo ben formato può essere l'ultima linea di difesa contro una violazione che è sfuggita ai controlli tecnici e di processo.

La tradizionale formazione annuale sulla security awareness è qualcosa che nessuno si aspetta, e se un'organizzazione dedica un impegno minimo alla sicurezza, ad esempio mettendo insieme un video e una serie di domande a quiz, non sorprende se i dipendenti adottano lo stesso approccio alla sicurezza. Considerare alcune delle seguenti best practice quando si definiscono i fattori umani nella strategia di sicurezza.

Metodi e tecniche di formazione:

- Utilizzare la gamification e la concorrenza per aumentare il desiderio di partecipazione degli individui.
- Gli interventi formativi devono essere regolari e brevi: pensa a 10 minuti alla settimana invece di un'ora all'anno per la formazione generale sulla security awareness.
- Utilizza i test per garantire a livello organizzativo che i tuoi obiettivi di maturità siano stati raggiunti e per fornire ai partecipanti un feedback immediato sull'apprendimento del materiale didattico.
- Considera sia l'abilitazione individuale altamente mirata, incentrata sulle competenze tecniche, sia gli esercizi di gruppo per testare i processi e le competenze del lavoro di team.

Comunicazione e coinvolgimento:

- Parlare con le persone nella loro lingua locale e nel tono giusto può essere importante quanto il contenuto.

Gestione degli incidenti:

- Un solido processo di gestione degli incidenti, sottoposto a stress test, può fare la differenza tra un evento di sicurezza in corso e un incidente critico per l'azienda

Inclusione nei temi di security awareness:

- La tua strategia deve considerare tutti i profili, dall'utente IT occasionale all'amministratore di sicurezza più tecnico della tua organizzazione. Tutti hanno un ruolo da svolgere nel mantenere la sicurezza.

L'aspetto umano della strategia di sicurezza di un'organizzazione non è solo una formalità; è un fattore essenziale che può fare la differenza tra essere sicuri ed essere esposti. Come abbiamo dimostrato, dall'utilizzo di metodi di formazione moderni alla garanzia della diversità, è fondamentale creare un approccio globale che riconosca l'importanza dell'elemento umano. Concentrandoci sull'apprendimento continuo, su una comunicazione efficace, su una solida gestione degli incidenti e sull'inclusione di tutti i ruoli all'interno di un'organizzazione, costruiamo le basi per una postura di sicurezza resiliente. Man mano che la tecnologia cambia e le minacce diventano più avanzate, è l'individuo ben formato, consapevole e coinvolto acostituire in modo affidabile una solida barriera contro le possibili violazioni. L'adozione e la gestione del cambiamento garantiscono che le azioni, le politiche e le tecnologie di sicurezza siano perfettamente integrate nella cultura e nelle pratiche quotidiane di un'organizzazione. Cambia la prospettiva dalla semplice consapevolezza al cambiamento comportamentale pratico, creando una cultura della sicurezza proattiva. Questo cambiamento porta a una minore opposizione, supporta il miglioramento continuo e rafforza la responsabilità tra gli impiegati. Man mano che il panorama della sicurezza informatica cambia, è fondamentale stare al passo con le nuove tecnologie. La gestione del cambiamento garantisce che le organizzazioni non solo si adattino, ma prosperino in mezzo a questi cambiamenti utilizzando nuovi strumenti in modo sicuro ed efficace.

Fasi successive

Comprendendo il rischio organizzativo, scegliendo le tecnologie e le piattaforme giuste per il percorso di apprendimento e integrandole nei processi aziendali, Insight può aiutarti a creare e implementare un fattore umano coerente nella strategia di sicurezza informatica. Possiamo anche monitorare e migliorare l'adozione man mano che l'implementazione progredisce. Contatta i nostri consulenti per la sicurezza o i nostri esperti in gestione dell'adozione e del cambiamento per ulteriori informazioni.

- **it.insight.com**
- **02 21080210**