Kaspersky Security Awareness

Il fattore umano è un aspetto fondamentale per la cybersecurity aziendale

Negli ultimi anni le aziende si stanno organizzando per installare soluzioni avanzate per alzare sempre di più il livello di cybersecurity per bloccare le minacce. Tuttavia, al contempo, i cybercriminali hanno focalizzato la loro attenzione sui dipendenti, utilizzandoli come punto di ingresso nei sistemi IT. Sfruttare le lacune degli utenti in tema di cybersecurity è il modo più semplice per introdursi all'interno dell'infrastruttura IT di un'azienda.

Secondo quanto emerso dal sondaggio di Kaspersky Lab e B2B International*, il **52%** delle imprese riconosce che i dipendenti rappresentano una delle maggiori potenziali debolezze in termini di sicurezza IT dell'azienda, a causa delle lacune di conoscenza in materia di cybersecurity che rischiano di compromettere la strategia di sicurezza aziendale.

Le organizzazioni si preoccupano principalmente dei dipendenti che condividono dati tramite dispositivi mobili (47%) e della perdita fisica degli stessi, che espone l'azienda a rischi (46%) e dell'uso inappropriato delle risorse IT da parte dei dipendenti (44%).

Guardando più da vicino questi risultati, le preoccupazioni circa l'uso improprio delle risorse IT da parte di dipendenti variano notevolmente a seconda delle dimensioni dell'organizzazione, con aziende molto piccole (con 1-49 dipendenti) che si sentono più a rischio rispetto alle aziende con più di mille dipendenti. Ciò potrebbe essere dovuto a diversi fattori, tra cui la presenza di policy aziendali più rigide e una più approfondita formazione del personale sulle best practice.

Fattore umano: la causa principale degli incidenti informatici

Il Cyber Security Intelligence Index di IBM ha rivelato che più del 90% di tutti gli incidenti di sicurezza deriva da una qualche forma di errore umano: utilizzo di link di phishing, visite a siti web dannosi, attivazione di virus e di altre minacce APT (Advanced Persistent Threats).

Il sondaggio di Kaspersky Lab e B2B International* per il 2017 supporta queste conclusioni. Secondo il report, l'uso improprio delle risorse IT da parte dei dipendenti ha contribuito a causare il 39% degli attacchi informatici subiti dalle aziende su un periodo di dodici mesi.

L'aumento nel numero di incidenti informatici causati da errori umani risulta particolarmente evidente per il segmento delle microimprese: in un solo anno la percentuale di piccole organizzazioni (1-49 dipendenti) che ha subito incidenti causati da dipendenti è cresciuta dal 25% al 32%.
Particolarmente preoccupante è il fatto che quasi la metà di tutte le aziende (tra il 44% e il 48%) non si sente sufficientemente protetta dalle minacce legate alla mancanza di competenze e all'ingenuità dei propri dipendenti.

Impatto finanziario medio di azioni inappropriate di dipendenti disattenti/disinformati[1]

Per le PMI

- Condivisione impropria dei dati: $ 88.000
- Smarrimento dei dispositivi mobili che espone l'organizzazione a rischi: $ 99.000
- Smarrimento di dispositivi o supporti contenenti dati: $ 81.000
- Uso inappropriato delle risorse IT da parte di un dipendente: $ 68.000

Per le aziende Enterprise:

- Incidenti che coinvolgono dispositivi IoT: $ 1,6 milioni
- Smarrimento di dispositivi o supporti contenenti dati: $ 1,1 milioni
- Uso inappropriato delle risorse IT da parte di un dipendente: $ 581.000
- Condivisione impropria dei dati tramite dispositivi mobili: $ 464.000

Data breach in numeri [2]**:**

- Il 61% delle vittime di un data breach, nel report del 2017, è rappresentato da aziende con meno di 1.000 dipendenti
- L'81% di violazioni legate ad attacchi hacker ha utilizzato password rubate, deboli o facilmente recuperabili.
- Il 43% delle violazioni è rappresentato da attacchi sui social network
- Il 66% dei malware viene installato tramite allegati e-mail dannosi

1. "Global IT Security Risks Survey 2017". Kaspersky Lab e B2B International
2. "2017 Data Breach Investigations Report" Verizon

Le organizzazioni hanno inoltre menzionato la disinformazione/disattenzione come seconda principale causa di tutti gli incidenti: il 46% degli intervistati ha posto l'accento sulla significativa incidenza di questo fattore in relazione agli incidenti verificatisi.
Abbiamo quindi analizzato come i dipendenti rappresentino il principale punto d'ingresso nell'organizzazione per un attaccante Tuttavia, personale ben formato e informato che segue best practice efficaci e che è consapevole del mondo informatico potrebbe diventare la prima linea di difesa.

*Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", giugno 2017

Programmi di formazione efficace sulla sicurezza informatica

La formazione del personale è fondamentale per accrescere la Security Awareness tra i dipendenti, motivarli a prestare attenzione alla minacce informatiche e alle relative contromisure, anche se ciò non viene percepito come parte specifica delle loro responsabilità sul lavoro.

Purtroppo, molti programmi di formazione sulla sicurezza sono poco efficaci. Vengono applicate tutte le politiche di sicurezza, fornite le informazioni più recenti sui tipi esistenti di malware e sulle tattiche di protezione, ma la formazione continua a non produrre risultati soddisfacenti. Che cosa non funziona? La formazione sulla sicurezza molto spesso viene erogata in una giornata di sessioni obbligatorie di fronte a uno schermo, partecipando a una presentazione PowerPoint mentre furtivamente si continua a lavorare sul proprio telefono. Tale formazione è, naturalmente e di conseguenza, considerata uno spreco di tempo e tutti i partecipanti continuano ad agire come prima. La formazione sulla sicurezza può ugualmente rivelarsi inefficace se i dipendenti vengono sommersi da istruzioni al punto di non riuscire ad assorbire la quantità di informazioni e perdere interesse.

Un programma di Security Awareness efficace deve includere:

L'impostazione degli obiettivi di formazione e del programma
• L'impostazione degli obiettivi misurati su benchmark di medie mondiali/del settore
• La possibilità di definire un bilanciamento accettabile tra il livello di competenza da far raggiungere a ciascun gruppo di dipendenti e il tempo di apprendimento totale necessario per portare i dipendenti a tale livello.

Assicurarsi che tutti i dipendenti siano formati almeno per il livello di rischio correlato alle loro attività quotidiane lavorative
• Possibilità di utilizzare strumenti di gestione automatizzata dell'apprendimento per portare ogni dipendente al livello di conoscenza appropriato ai rischi del proprio profilo
• Accertarsi che le competenze acquisite vengano rinforzate per evitare che siano dimenticate.
• Formare le persone a seconda delle loro capacità individuali e tenendo conto delle loro rapidità di apprendimento

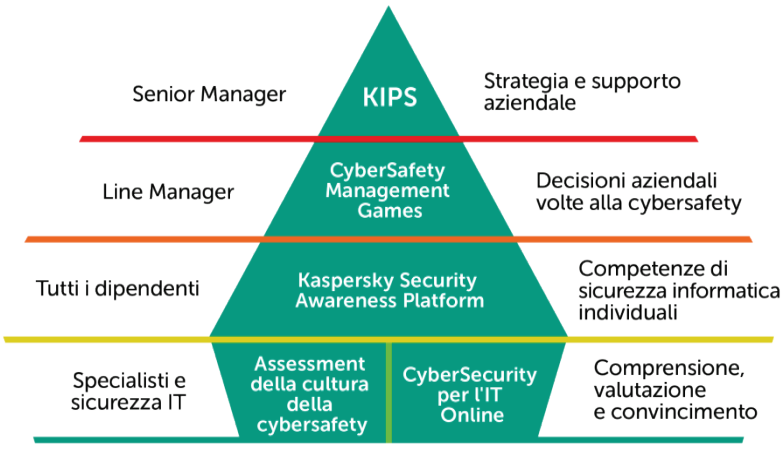
Monitorare i progressi con analisi e report pratici
• Tracciare dati, tendenze e previsioni in tempo reale
• Utilizzare le previsioni in tempo reale per raggiungere gli obiettivi di formazione annuali
• Affrontare le questioni prima che diventino problemi (ad esempio, sapere quali aree dell'organizzazione necessitano di maggiore attenzione e intervenire)
• Generare analisi comparative dei risultati provvisori

Garantire uno svolgimento efficace del programma di formazione
• Coinvolgere i dipendenti nella formazione con giochi ed esercizi che stimolano la competizione
• Garantire che la formazione sia rilevante per la vita quotidiana dei partecipanti
• Offrire la possibilità di confrontare i risultati individuali con quelli degli altri
• Prevenire il sovraccarico di lavoro

Conoscere le dinamiche che regolano i processi di apprendimento e insegnamento aiuta a realizzare un efficace programma formativo. Kaspersky Lab ha lanciato una famiglia di prodotti di formazione assistita tramite computer e basata su approccio ludico che utilizza tecniche di apprendimento moderne e si rivolge a tutti i livelli della struttura organizzativa. I nostri programmi non mirano solamente a trasmettere pure e semplici nozioni; l'obiettivo principale è anzi quello di stimolare i partecipanti affinché aderiscano a un nuovo modello comportamentale che tenga costantemente conto delle problematiche legate alla sicurezza informatica.

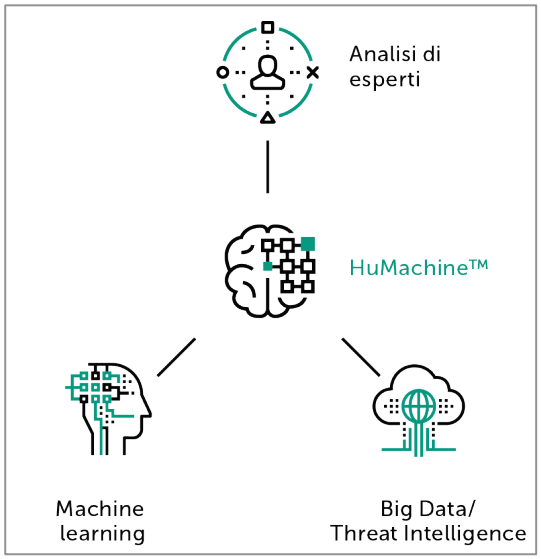
L'approccio a 360° di Kaspersky Lab si basa su moderne tecniche di apprendimento e combina sessioni ludiche, in cui si generano anche interessanti dinamiche di gruppo, apprendimento attraverso attività pratiche e rafforzamento dei concetti. Tra questi, l'approccio ludico rappresenta la chiave per formare l'atteggiamento delle persone e per costruire nuovi modelli comportamentali tramite il confronto e le discussioni durante le attività di gruppo in grado di stimolare l'apprendimento.

Programmi di formazione Kaspersky Security Awareness



Questo approccio ha già registrato risultati:

- Fino al 90%: di riduzione del numero totale di incidenti
- Non meno del 50%: di riduzione dell'impatto finanziario degli incidenti
- Un sorprendente 86%: la percentuale dei partecipanti disposta a consigliare l'esperienza



Kaspersky Lab

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Novità sulle cyberminacce: www.securelist.com
Novità sulla sicurezza IT: business.kaspersky.com/it

#truecybersecurity
#HuMachine

www.kaspersky.it

© 2018 AO Kaspersky Lab.
Tutti i diritti riservati. I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari