kaspersky BRING ON THE FUTURE

Kaspersky Security Awareness

Programma di formazione sulla cybersecurity per i dirigenti

Le tecnologie digitali hanno un profondo impatto su ogni aspetto della nostra vita, offrendo maggiori opportunità, efficienza dei costi, scalabilità a livello globale e numerosi altri vantaggi. Tuttavia, per ottenere il massimo da questi vantaggi, ora più che mai è fondamentale essere consapevoli dell'importanza della protezione e di un uso corretto delle competenze in materia di cybersecurity.

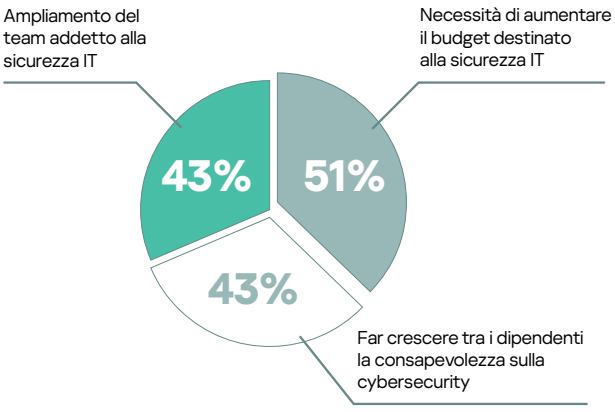
Quando violazioni e cyberattacchi vanno a segno, nella migliore delle ipotesi possono comportare qualche grattacapo per il reparto IT e malfunzionamenti di minore entità dei sistemi interni dell'azienda colpita. Nella peggiore delle ipotesi, ci possono essere conseguenze più gravi per tutta l'organizzazione aziendale. Per essere sempre aggiornati relativamente alle minacce alla sicurezza è necessario il coinvolgimento attivo non solo dei CISO e del personale IT, ma anche dei dirigenti non tecnici, con un impegno condiviso per costruire una cultura della sicurezza informatica in tutta l'organizzazione.

Avendo accesso al livello più elevato della sicurezza e a informazioni riservate, i top manager rappresentano un obiettivo particolarmente ambito per i cybercriminali. Scarse conoscenze, competenze di base lacunose in fatto di cybersecurity e, persino, gli errori commessi in buona fede da questi dirigenti possono costare molto caro alle aziende.

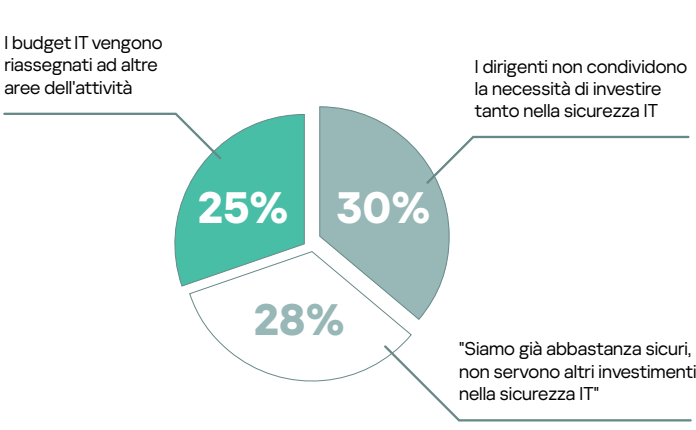
Dirigenti di alto livello e responsabili della sicurezza IT sono sulla stessa lunghezza d'onda?

Sebbene la cooperazione tra i team addetti alla sicurezza IT e il consiglio di amministrazione sia vantaggiosa per tutte le aziende, solo il 50% dei responsabili IT ritiene che i senior manager comprendano appieno i rischi informatici. Secondo il 90% dei decision maker IT, inoltre, i dirigenti delle aziende per cui lavorano sarebbero disposti a scendere a compromessi sulla cybersecurity a favore della trasformazione digitale, della produttività o di altri obiettivi*. A causa di questa mentalità, per il personale IT spiegare l'importanza di allocare un budget per la sicurezza IT rappresenta uno dei tre argomenti più difficoltosi da affrontare con i dirigenti di alto livello.

I tre argomenti più difficoltosi da affrontare includono:**



I tre motivi principali per cui i budget per la sicurezza IT delle aziende vengono ridotti*:**



Il 62% dei manager ammette che questa disconnessione della dirigenza rispetto alla sicurezza IT ha portato ad almeno un incidente di cybersecurity**

---

* Una ricerca globale **"Business friction is exposing organizations to cyber threats"**, Trend micro

** "Fluent in Infosec", Kaspersky 2023

***"Managing the trend of growing IT complexity", Kaspersky

Coinvolgere il top management nella cybersecurity: una sfida per i docenti

Le aziende dove i manager contribuiscono attivamente alle discussioni e alle decisioni sulla protezione dell'attività di business dalle cyberminacce sono meglio preparate a far fronte agli attacchi e meglio attrezzate per riprendersi rapidamente. Il coinvolgimento del CEO come figura maggiormente influente è fondamentale per garantire una consapevolezza della sicurezza coerente ed efficace nell'intera organizzazione. In genere, tuttavia, si tratta di persone sempre molto impegnate, con altre priorità e con l'agenda sempre piena. Pertanto, in che modo è possibile incoraggiarle a dedicare del tempo alla formazione?

La risposta sta in un tipo di formazione pensato per adattarsi alle esigenze dei dirigenti. Un programma appositamente progettato che aiuta a comprendere il panorama della cybersecurity e l'importanza del modo in cui si connette all'efficienza aziendale, fornendo al contempo approfondimenti sulle realtà operative della costruzione e dell'applicazione di strategie per la cybersecurity a vantaggio dell'intera organizzazione.

Formazione per i dirigenti e Formazione online sulla cybersecurity per i dirigenti: sviluppo della consapevolezza sulla sicurezza per top manager e decision maker

La cybersecurity svolge un ruolo fondamentale nella generazione di entrate insieme alla gestione dei progetti, agli strumenti finanziari e all'efficienza operativa aziendale. È proprio questo il fulcro del nostro corso rivolto ai dirigenti. I leader aziendali e i top manager apprendono le basi della cybersecurity attraverso un corso guidato da tutor grazie al quale impareranno a conoscere meglio le minacce informatiche e a proteggersi da esse.

Vantaggi della formazione

Il corso copre gli aspetti critici della cybersecurity in ambito aziendale, in un linguaggio accessibile e non tecnico. Si concentra sul ritorno sugli investimenti (ROI, Return on Investment) effettuati per la cybersecurity e promuove la reciproca comprensione e la cooperazione tra reparti ai fini della sicurezza.

Sono disponibili due formati: un workshop offline interattivo tenuto da un esperto Kaspersky (**Formazione per i dirigenti**) e un corso online (**Formazione online sulla cybersecurity per i dirigenti).**

Il corso Formazione online sulla cybersecurity per i dirigenti è composto da 6 moduli:

1. Introduzione alla cybersecurity
   a. Che cos'è la cybersecurity
   b. Perché i manager dovrebbero essere coinvolti nella cybersecurity
   c. Intervento di Eugene Kaspersky: dalla sicurezza informatica all'immunità informatica
2. Rischi informatici per le aziende
   a. Perdite aziendali a seguito di un attacco informatico
   b. Misure e approcci alla gestione dei rischi informatici
   c. Casi di successo (e insuccesso): l'importanza della gestione dei rischi informatici
3. Cyberattacchi e strumenti impiegati dagli autori degli attacchi
   a. Gli strumenti impiegati dagli autori degli attacchi: social engineering, malware, exploit, Dark Market
   b. Cyberattacchi: tipologie, fattori di riuscita, attacchi mirati, attacchi di massa, fughe di dati, come proteggersi
4. Protezione dell'azienda e delle attività aziendali dagli attacchi informatici
   a. Igiene informatica per i manager
   b. Formazione del personale per lo sviluppo della consapevolezza sulla cybersecurity
   c. La cybersecurity ai diversi livelli di maturità dell'azienda
   d. Controlli e servizi di cybersecurity
5. Gestione delle conseguenze dei cyberattacchi
   a. Come reagire e rispondere a un cyberattacco
   b. Piano di gestione della crisi informatica
   c. Comunicazione degli incidenti
6. Il futuro della cybersecurity
   a. Cyberminacce: statistiche e vettori di attacco
   b. Industry 4.0. e Internet of Things
   c. Cyber immunity

Il corso è stato creato dai top manager di Kaspersky in collaborazione con i principali esperti di cybersecurity. Include complessivamente 50 lezioni da 3-6 minuti ciascuna. Può essere erogato tramite accesso a una piattaforma cloud oppure in SCORM per essere integrato nell'LMS.

Questi programmi fanno parte del portfolio Security Awareness di Kaspersky, che offre una gamma di opzioni di formazione coinvolgenti per aumentare la consapevolezza del personale sulla cybersecurity e consentire loro di svolgere il proprio ruolo nell'ambito della sicurezza informatica complessiva dell'organizzazione.

Alla fine di ogni argomento è prevista un'attività pratica e 5-10 domande per l'autovalutazione e il rafforzamento delle nuove conoscenze. Una volta completate tutte le attività e le lezioni, i manager dovranno superare il test finale.

Alla fine verrà rilasciato un certificato di completamento.

Principali vantaggi:

- **Semplicità di erogazione:** microlezioni + attività pratiche + test = consolidamento e mantenimento delle competenze
- **Praticità:** il corso online può essere seguito sia da dispositivi mobili che desktop
- **Basato su un'approfondita conoscenza delle specifiche esigenze dei dirigenti:**questo corso è stato creato dai top manager di Kaspersky
- **Linee guida pratiche e liste di controllo:**contiene materiali pronti all'uso

Esito della formazione

Al termine del corso, i manager saranno in grado di:

- Parlare la stessa lingua degli specialisti IT e di sicurezza IT
- Sviluppare un piano di gestione della crisi informatica insieme ai team IT e di sicurezza IT
- Pianificare comunicazioni efficaci sugli incidenti
- Prendere decisioni strategiche sulla base delle valutazioni dei rischi informatici
- Applicare le regole per l'igiene informatica
- Proteggersi dalle minacce informatiche

Per saperne di più, visitate il sito Web all'indirizzo **https://www.kaspersky.it/small-to-medium-business-security/security-awareness-platform**

www.kaspersky.com