KASPERSKY lab

Cybersafety Management Games

Stimulierende Lern- und Motivationserfahrung zur Förderung
Cyber-sicherer Entscheidungsfindung durch Führungskräfte

www.kaspersky.de
#truecybersecurity

Cybersafety Management Games

Kandidaten

Bereichsleiter als treibende Kraft einer Cyber-sicheren Arbeitsumgebung für das gesamte Unternehmen

Typischer Stand der Cybersecurity in Unternehmen (Nicht-so-schlecht-Szenario):

Unternehmensebene

- Dedizierte IT-Sicherheitsabteilung
- Erkennung des Gesamtproblems
- Allgemeine Cybersicherheits-Strategie implementiert

Mitarbeiterebene

- Jährliche Compliance-Schulung zum Thema Cybersicherheit
- In einigen Büroräumen angebrachte Cybersicherheits-Tipps

Alle Abteilungen führen Maßnahmen durch, um Cyberbedrohungen zu bekämpfen, indem sie IT-Sicherheitsstrukturen einrichten und Compliance-Schulungen durchführen.
Aber reicht dies aus?

- Können die im Training erworbenen Kenntnisse das Verhalten der Mitarbeiter wirklich verändern? Oder ist die Realität einfach anders als ein Training?
- Geht Sicherheit zu Lasten der Effizienz?
- Können dedizierte IT-Sicherheitsmitarbeiter wirklich alle Mitarbeiter eines Unternehmens erreichen?

Diese Herausforderungen können nur überwunden werden, wenn es gelingt, **Führungskräfte dazu anzuhalten, Unternehmen Cyber-sicher zu machen, ohne dafür Effizienz opfern zu müssen. Nur sie** kommunizieren täglich mit den Mitarbeitern und treffen geschäftliche Entscheidungen. Cybersicherheit muss zum obligatorischen Bestandteil der täglichen Entscheidungsfindung werden.

Normalerweise besteht die größte Herausforderung für das Sicherheitsteam darin, das Management zu motivieren.

Aus diesem Grund hat Kaspersky Lab ein spezielles Trainingsprogramm entwickelt, das darauf abzielt, Vorgesetzte und Führungskräfte zu Unterstützern und Fürsprechern der Cybersicherheit zu machen.

Rolle der mittleren Führungsebene in einem gut abgestimmten Cybersecurity-Umfeld:

Unternehmensebene

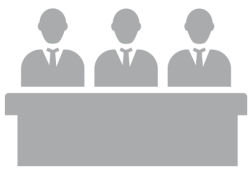
- Engagierte und gut kommunizierende IT-Sicherheitsabteilung
- Umsetzbare Cybersicherheits-Strategie
- Ausrichtung der Geschäftsprozesse an Prinzipien der Cybersicherheit

Führungsebene

- Sicherstellung eines wirksamen Einsatzes von Cybersicherheitsprinzipien in der täglichen Arbeit
- Betreuung, Überwachung und Anweisung der Mitarbeiter

Mitarbeiterebene

- Kontinuierliche Schulung in der Cybersicherheit
- Regelmäßige und effiziente Bewertungen mit automatischer Anpassung der Lernpfades



Schulungsziel

Schulungsziele, durch die Führungskräfte eine treibende Kraft für mehr Cyberhygiene werden

Kaspersky CyberSafety Management Games vermitteln Managern **Kompetenz, Wissen und Einstellungen**, die für die Aufrechterhaltung sicherer Arbeitsumgebungen in ihren Abteilungen unerlässlich sind.

Verständnis

Verinnerlichung der Notwendigkeit von Cybersicherheitsmaßnahmen als wichtige, aber unkomplizierte Aktionen

Führungskräfte erhalten:

- ein Gefühl dafür, warum sie sich um die Sicherheit sorgen sollten
- Einblicke in die Sichtweise von Cyberkriminellen
- ein neues Verständnis von Cyberbedrohungen und Möglichkeiten, sie erfolgreich zu vermeiden/zu verhindern

Überwachung

Untersuchung des alltäglichen Arbeitsprozesses vom Standpunkt der Cybersicherheit

Führungskräfte können:

- zwischen sicherem und unsicherem Verhalten unterscheiden
- tägliche Ereignisse an typischen Arbeitsplätzen „scannen", um auf potentiell bedrohliche Situationen zu achten und die Mitarbeiter auf Sicherheitsmaßnahmen hinzuweisen

Cyber-sichere Entscheidungen fällen

Überlegungen zur Cybersicherheit zu einem integralen Bestandteil normaler Geschäftsprozesse machen

Führungskräfte können:

- ein optimales Gleichgewicht zwischen Sicherheitsvorkehrungen und Geschäftseffizienz finden
- Geschäftsprojekte planen und umsetzen, dabei aber in jeder Phase und für jedes beteiligte Team die Cyber-Risiken abschätzen
- den erforderlichen Zeit- und Kostenaufwand abschätzen, um cyber-sichere Entscheidungen in jeder Projektphase zu gewährleisten
- effizient mit dem Sicherheitsteam zusammenarbeiten

Führungskräfte werden davon überzeugt, dass Sicherheitsmaßnahmen nicht kompliziert und zeitaufwendig sein müssen, und helfen gleichzeitig, potentiell enorme Unternehmens- und Personalverluste zu vermeiden.

Bestärkung und Inspiration

Vorbildliche Führung und hilfreiche Beratung der Mitarbeiter

Führungskräfte können:

- die Fragen der Mitarbeiter zu Cybersicherheitsthemen richtig beantworten oder passendes Feedback zu Themen geben, bei denen sie sich nicht sicher sind (z. B. den Anfragenden an IT-Sicherheitsspezialisten weiterzuleiten oder selbst um weitere Details zu bitten)
- sicherstellen, dass Mitarbeiter die Cybersicherheits-Werte und -Verfahren einhalten und Skepsis in Bezug auf diese Werte vermeiden
- Mitarbeiter dazu motivieren, Cybersicherheitstechniken täglich aktiv zu erlernen und anzuwenden
- letztlich selbst für die Cybersicherheit motiviert sein – und wissen, dass dies ihre Geschäftsziele, persönlichen Prioritäten und Zeiteinteilung nicht beeinträchtigt

Bedrohungen aus 10 Sicherheitsbereichen:

AV/Apps, Datenleck, Mobile, Web, Mail, Verhalten von Opfern, Social Engineering, Sicherheitswarnungen, Wachsamkeits-Skills, Verstoß gegen Richtlinien

Referentenausbildung verfügbar

In den Fällen, in denen der Kunde CyberSafety Management Games zur Schulung einer größeren Anzahl von Mitarbeitern, Managern und Experten aus verschiedenen Abteilungen oder Standorten nutzen möchte, kann es hilfreich sein, die Lizenz zu erwerben, interne Schulungsleiter auszubilden und Schulungen (vor Ort oder online) im eigenen Tempo und je nach Bedarf des Kunden durchzuführen. Eine solche Lizenz ist bei Kaspersky Lab erhältlich und beinhaltet:

- das Recht zur Nutzung des CyberSafety Management Games-Schulungsprogramms
- Schulungsmaterialien und das Recht, sie zu verwenden/vervielfältigen
- Benutzername/Passwort für den Software-Server der CyberSafety Management Games
- Leitfaden für Schulungsleiter und Moderationsschulung für Programmleiter
- Wartung und Support (Updates und Support für Software und Schulungsinhalte)
- Optionale Anpassung des Szenarios (gegen Gebühr)

Schulungsformat

Ansprechendes computergestütztes Programm mit kurzen Schulungsmodulen

CyberSafety Management Games sind speziell auf die Bedürfnisse und Prioritäten von Managern zugeschnitten und konfrontieren sie mit umfangreichen, komplexen und glaubwürdigen simulierten Arbeitssituationen.

Das Training basiert auf der **eigens entwickelten CyberSafety Management Games-Software**, die Gamification mit umfassender Behandlung von Sicherheitsthemen kombiniert. Beispiele, Erklärungen und Übungen sind in die Software integriert, um dem Schulungsleiter die Präsentation der Schulungen zu erleichtern.

Dadurch kann die Schulung statt von einem Sicherheitsexperten von einem Business-Trainer durchgeführt werden (alle sicherheitsrelevanten Inhalte sind in der Software enthalten).

Es wird davon ausgegangen, dass die Teilnehmer bereits über ein gewisses Maß an Cybersicherheits-Fachwissen verfügen und vorzugsweise mehrere Module der Schulungsplattform für CyberSecurity Trainings bestanden haben. Falls nicht, können CyberSafety Management Games mit einer kurzen theoretischen Einführung ergänzt werden.

Standard-Schulungsprogramm

Das empfohlene Schulungsprogramm besteht aus 3 Modulen, die von kurzen technischen Erläuterungen und Erörterung der Fehler der Teilnehmer begleitet werden. Module können je nach Wunsch des Kunden hinzugefügt oder entfernt werden.

Programm und Einstellung können (gegen Gebühr) entsprechend Ihren Bedürfnissen angepasst werden. Die meisten unserer Kunden sind jedoch mit einem einheitlichen Kursplan zufrieden, der Punkte und Situationen abdeckt, die jedes Unternehmen und jede Führungskraft betreffen.

Sitzung 1: „Gefahr geht auch von Menschen aus, nicht nur von infizierten Computern“

2 Stunden

1. Identifizieren von Cyberbedrohungen – „Großraumbüro“
2. Risikominimierung:
   - Verdächtige und normale Links
   - Schwache Passwörter.
     Übung *„Erstellen von starken, einfach zu merkenden Passwörtern und Passwort-Familien“*
   - Verdächtige und normale Anhänge
   - Unbefugter Zugriff auf vertrauliche Informationen.
     Übung *„Was kann ich tun, um Risiken zu mindern“*
   - Unangemessene Verbreitung von vertraulichen Informationen
   - Mitnahme vertraulicher Informationen außerhalb des Unternehmens.
     Übung *„Abwägen von geschäftlicher Notwendigkeit und bestehenden Risiken“*
   - „Herrenloses“ Flash-Laufwerk.
     Übung *„Was kann ich tun, um Risiken zu mindern“*
   - Installieren nicht-signierter Software
   - Phishing-E-Mails.
     Übung *„So erkennen Sie betrügerische E-Mails“*
3. Übung „Cyberkriminelle“
4. Fazit der Sitzung
   - **Denken Sie daran:** „Gefahr geht auch von Menschen aus, nicht nur von infizierten Computern“
   - **Tun:** „Berücksichtigen Sie immer, wer Ihre Online-Aktivitäten missbrauchen könnte“

Sitzung 2: „Sie müssen nicht das Ziel sein, um zum Opfer zu werden“

2 Stunden

1. Identifizieren von Cyberbedrohungen – *„Unterwegs“*
2. Risikominderung – Übungen
   - Weitergabe von E-Mails – persönliche und berufliche
   - Ignorieren von Sicherheitsupdates
   - Posten in sozialen Netzwerken – neutral mit Informationsleck
   - Weitergabe von Passwörtern.
     Übung *„Abwägen von geschäftlicher Notwendigkeit und bestehenden Risiken“*
   - Installation von Spielen auf beruflich genutzten Smartphones
   - Nicht gesperrter PC.
     Übung *„Was kann ich tun, um Risiken zu mindern“*
   - Verdächtiger Link.
     Übung *„Verdächtige URLs“*
   - Verwendung vertraulicher Informationen an öffentlichen Orten
   - Schwache Authentifizierung in öffentlichen WLAN-Netzwerken
3. Übung „Opferprofil“
4. Fazit der Sitzung
   - **Denken Sie daran:** „Sie müssen nicht das Ziel sein, um zum Opfer zu werden“
   - **Tun:** „Ein schwierigeres Ziel als die anderen sein“

Sitzung 3: „Cybersicherheit geht jeden an“

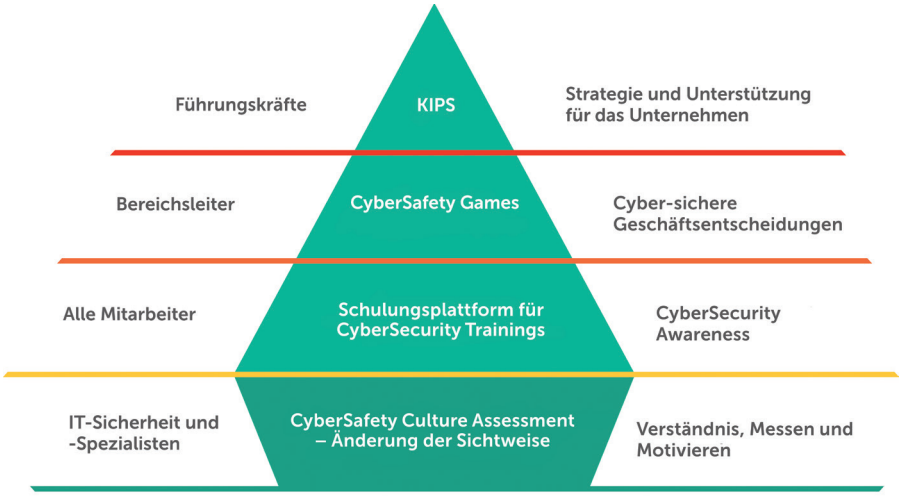
2 Stunden

1. Identifizieren von Cyberbedrohungen – „Konferenzraum“
2. Risikominderung – Übungen
   - Wiederverwendung und Aufbewahrung von Passwörtern
   - Unabsichtliche Weitergabe von vertraulichen Informationen.
     Übung *„Was kann ich tun, um Risiken zu mindern“*
   - Warnungen vor Datenverlust
   - Social-Engineering-Angriff.
     Übung *„So erkennen Sie Social Engineering“*
   - Ignorieren von IT-Sicherheitsrichtlinien
   - Senden von vertraulichen Informationen an Empfänger außerhalb des Unternehmens.
     Übung *„Abwägen von geschäftlicher Notwendigkeit und bestehenden Risiken“*
   - Schädliche Webseiten
   - Mitnahme vertraulicher Informationen außerhalb des Unternehmens
   - Unbefugter Zugriff auf vertrauliche Informationen.
   - Veraltete Virenschutzsoftware
   - Erreichen von geschäftlichen Zielen bei vorhandenen Sicherheitsmaßnahmen.
     Übung *„Dialog mit der IT-Sicherheitsabteilung“*
3. Übung „Sicherheitsplanung als Teil des Unternehmens“
4. Fazit der Sitzung
   - **Denken Sie daran:** „Cybersicherheit geht jeden an“
   - **Tun:** „Kooperieren Sie mit der IT-Sicherheitsabteilung“

Kaspersky-Schulungsprodukte für Security Awareness / Sicherheitsbewusstsein

Das CyberSafety Culture Assessment ist ein Teil des Portfolios von Kaspersky Lab zum Thema Sicherheitsbewusstsein, das auf CyberSafety Culture-Methoden beruht. Die CyberSafety Culture ist eine Reihe von Werten und Ansichten, die das Verhalten von Menschen sowohl auf der individuellen als auch auf der Unternehmensebene steuern.

Wir unterstützen unsere Kunden durch Sicherheitsschulungen unter Leitung der Sicherheits- und Personalabteilung beim Aufbau einer Cybersicherheitskultur. Die Schulungen beruhen auf Planspielen und richten sich an sämtliche Unternehmensebenen.



Umfassend, aber einfach und verständlich

- Zahlreiche Sicherheitsaspekte
- Vertraute Umgebungen
- Fesselnder Schulungsprozess
- Praktische Übungen
- Sprache geeignet für Nicht-IT-Mitarbeiter

Geschäftsvorteile

bis zu
93 %
Wahrscheinlichkeit der Anwendung des Wissens in der täglichen Arbeit

bis
90 %
reduzieren die Anzahl der Vorfälle

50–60 %
reduzieren das monetäre Cyberrisiko

mehr als die
30-fache
Bereitstellung der Investitionsrendite für Sensibilisierung

www.kaspersky.de

Kaspersky Lab
Cybersicherheit für Unternehmen:
www.kaspersky.deenterprise-security
Kaspersky Security Awareness
www.kaspersky.de/enterprise-security/security-awareness
Produkt-Demoversion: **www.kaspersky.de/enterprise-security/cybersecurity-awareness/demo/**