Eine Schulungslösung für alle

Unsere Schulungen sind so vielfältig wie die Bedrohungen, mit denen Sie konfrontiert sind.

kaspersky BRING ON THE FUTURE

Kaspersky Security Awareness Training

Minimieren Sie das Risiko von 90 %[1] der Bedrohungen aufgrund menschlicher Fehler

Jeder arbeitet anders und hat andere Fähigkeiten. Wenn es aber um Cybersicherheit geht, kann jeder Mitarbeiter in Ihrem Unternehmen zum Risiko werden.

Dabei genügen schon Grundkenntnisse im Bereich Cybersicherheit, um Unternehmen vor Cyberangriffen zu schützen. Um sich in komplexe Cybersicherheitssysteme zu hacken, nehmen Cyberkriminelle lieber Mitarbeiter mit gering ausgeprägtem Sicherheitsbewusstsein ins Visier als einen komplexen Code zu schreiben. Google hat 2.145.013[2] Phishing-Seiten ausgemacht (Stand: 17. Januar 2021), die es auf diesen „Faktor Mensch" abgesehen haben. Und wenn man sich den durchschnittlichen finanziellen Schaden von Datenschutzverletzungen in Höhe von 1.195.000 US-Dollar[3] pro Unternehmen vor Augen hält, kann niemand den enormen Wert von Schulungen zur Stärkung des Sicherheitsbewusstseins abstreiten.

Nichtsdestotrotz verpflichten nur etwa 60 %[4] der Unternehmen ihre Mitarbeitern zur Teilnahme an formellen Cybersicherheitsschulungen. Und bei 10 %[4] der Unternehmen, die solche Schulungen anbieten, ist die Teilnahme freiwillig.

Wir bei Kaspersky sind der Auffassung, dass der Mangel an geeigneten Lerntechnologien das eigentliche Problem ist. Eine Verhaltensänderung unter den Mitarbeitern herbeizuführen, ist für viele Unternehmen eine große Herausforderung. Gleichzeitig ist die überwiegende Mehrheit der vorhandenen Präsenz- und Online-Schulungsangebote sehr eindimensional und führt nicht zu einer dauerhaften Veränderung des Sicherheitsverhaltens unter den Mitarbeitern.

Bei den Security Awareness-Schulungen von Kaspersky ist das anders. Alle sicherheitsrelevanten Anforderungen eines Unternehmens werden durch eine breite Palette an Lösungen abgedeckt und mithilfe neuester Lernmethoden und -technologien werden Kompetenzen vermittelt, über die jeder verfügen sollte. Die Kursinhalte sind niemals langweilig. Niemals standardisiert. Und geraten nie in Vergessenheit.

[1] „Sorting out a Digital Clutter", Kaspersky, 2019.
[2] Blog: Tessian „Phishing Stastics" (2020)
[3] Kaspersky, 2019
[4] Mimecast Security Awareness Training Statistics, 2018

Flexibles Schulungsangebot für alle

52 %[5] der Unternehmen

sehen Mitarbeiter als größte Bedrohung für die Cybersicherheit in Unternehmen an

60 %[6] der Mitarbeiter

haben vertrauliche Daten auf ihren Firmengeräten (z. B. Finanzdaten, E-Mail-Datenbanken etc.)

Unsere Schulungen zum Sicherheitsbewusstsein sorgen für eine sicherere Arbeitsumgebung im gesamten Unternehmen

Wir bieten Schulungen für jede Unternehmensebene an, von der Führungsebene über IT-Fachleute bis hin zum Sachbearbeiter. Die Lerninhalte sind auf den jeweiligen Bedarf an Weiterbildung im Bereich der Cybersicherheit zugeschnitten und basieren auf unterschiedlichen Methoden der ansprechenden Wissensvermittlung, sei es unter Anleitung eines Referenten oder in eher spielerischen Lernformaten. Mitarbeiter werden motiviert, über die Bedeutung eines erhöhten Sicherheitsbewusstseins nachzudenken.

Und da wir bei Kaspersky den Schulungsbedarf von Mitarbeitern im Bereich der Cybersicherheit gut einzuschätzen wissen, können Sie sicher sein, dass die richtigen Kompetenzen vermittelt werden. Wir helfen Ihnen dabei, die notwendige Verhaltensänderung unter Ihren Mitarbeitern nachhaltig zu festigen.

[5] Forschung: „The cost of a data breach", Kaspersky, Frühjahr 2018.

[6] „Sorting out a Digital Clutter", Kaspersky, 2019.

Für die Führungsebene

58 %[8] der Vertreter auf Führungsebene

geben an, dass IT-Sicherheit zu komplex ist

42 %[9] sagen,

dass IT-Sicherheit für sie geringe Priorität hat

60 %[10] der IT-Führungskräfte

geben an, dass Vertreter der Führungsebene das wahrscheinlichste Ziel von schädlichen Cyberangriffen sind

76 %[11] der CEOs

geben zu, dass sie Sicherheitsprotokolle umgehen, um etwas schneller zu erledigen, und damit die Sicherheit der Geschwindigkeit opfern

28 %[12] der Vertreter auf Führungsebene

haben beantragt, dass Sicherheitsprotokolle in ihren Organisationen umgegangen werden dürfen

Gängige Wahrnehmung von Cybersicherheit durch Teamarbeit und Simulationen in Frage stellen

Es hat wenig Sinn, Hunderte von Mitarbeitern zu Sicherheitsschulungen zu schicken und gleichzeitig Führungskräfte, Experten für Geschäftssysteme und IT-Experten zu vernachlässigen.

Ein besseres Verständnis des möglichen geschäftlichen und finanziellen Schadens durch Sicherheitsverletzungen wie unbedacht weitergegebene Passwörter oder Phishing muss von ganz oben vorangetrieben werden.

Vertreter der obersten Führungsebene sind außerdem diejenigen, die für die Investition in Schulungen verantwortlich sind. Der Prozentsatz der Mitarbeiter, die in die Cybersicherheitsinitiativen der Unternehmen eingebunden sind, reicht von 85 % bis zu gerade einmal 56 %.[7]

Motivierend und effektiv

Kaspersky vermittelt Ihren Führungskräften ein besseres Verständnis für den Zusammenhang zwischen Cybersicherheit und Unternehmenseffizienz. Im **Executive Training** lernen Führungskräfte und Top-Manager beispielsweise die Grundlagen der Cybersicherheit kennen, und zwar in einem von Referenten geleiteten Kurs, in dem es um ein besseres Verständnis von Cyberbedrohungen und möglichen Schutzmechanismen geht.

Zusätzlich zum **Executive Training**, oder auch komplett separat, bieten wir interaktive Teamspiele wie **Kaspersky Interactive Protection Simulation (KIPS)** an, in denen das Gelernte praktisch angewendet wird. KIPS wurde speziell für Entscheidungsträger entwickelt und ist ein interaktives Teamspiel, das die aktuelle Wahrnehmung der Cybersicherheit in Frage stellt und die Zusammenarbeit zwischen den verschiedenen Ebenen Ihres Unternehmens fördert.

[7] Accenture Cybersecurity Report 2020

[8] Studie: MobileIron „Trouble at the Top"

[9, 10, 11] Forbes „Die größte Insider-Bedrohung für die Cybersicherheit ist die Führungsriege" (2020)

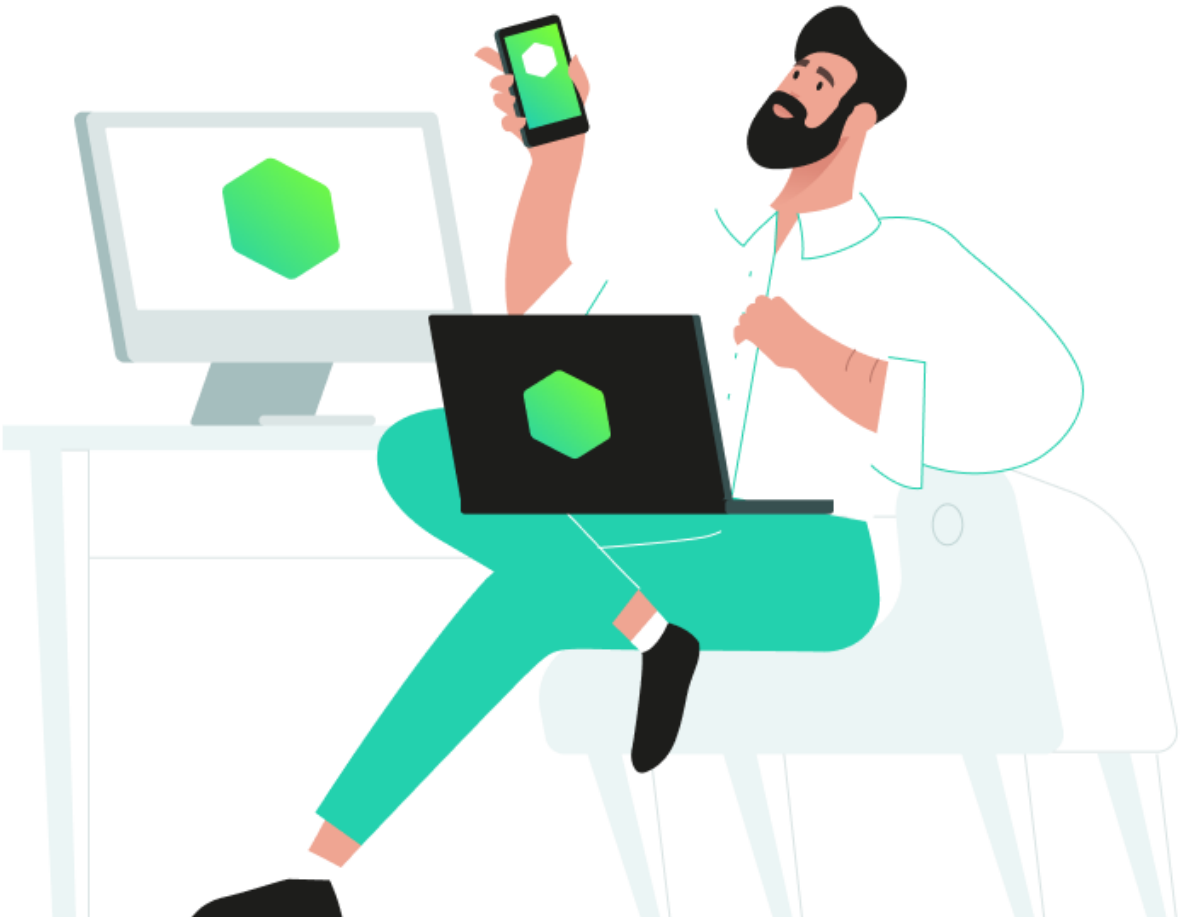
[12] Studie: MobileIron „Trouble at the Top"

In dieser Schulung lernen Ihre Führungskräfte, die Folgen eines Angriffs zu antizipieren, innerhalb zeitlicher und finanzieller Grenzen zu reagieren und sich auf die branchenspezifischen Szenarien einzustellen, die Kaspersky aufgestellt hat – von Sicherheitsrisiken für das Bankenwesen und in Unternehmen bis hin zum Logistik- und zu Versorgungsunternehmen.

Ein weiteres Element von KIPS ist das **CyberSafety Management Game** für Abteilungsleiter und mittleres Management. In diesem Spiel geht es darum, diese Personengruppe zu Unterstützern und Botschaftern der Cybersicherheit auszubilden und Cybersicherheit zu einem wesentlichen Aspekt ihrer täglichen Entscheidungen zu machen.

Geben Sie Ihren höchsten Führungskräften die Gelegenheit zur Teilnahme an diesem neuartigen Weiterbildungsformat.

Screenshot KIPS-Schulung:



Für alle Mitarbeiter

42 %[13] der Befragten

aus Unternehmen mit mehr als 1.000 Mitarbeitern geben an, dass die meisten der von ihnen besuchten Weiterbildungen unnütz und uninteressant waren

12 Länder

nutzen unser Schulungsangebot

Mehr als 500.000
geschulte Mitarbeiter

sorgen dank Kaspersky Security Awareness-Schulung für mehr Sicherheit in ihrem Unternehmen

Personalisiertes Training für eine nachhaltige Kompetenzvermittlung

Organisationen sollten darauf hinarbeiten, dass die Mehrzahl ihrer Mitarbeiter die erworbenen Kompetenzen so weit verinnerlicht, dass deren Anwendung zur Selbstverständlichkeit wird, ganz gleich, wann und wo ein potentielles Sicherheitsproblem auftaucht.

Das ist aus zwei Gründen eine Herausforderung: Zum einen ist der Mensch ein Gewohnheitstier und zum anderen sind die meisten Schulungen nicht darauf ausgelegt, die Teilnehmer mitzunehmen und Kompetenzen auszubauen.

Kaspersky hat seine 20-jährige Erfahrung im Bereich der Cybersicherheit und sein Verständnis von modernen Lernmethoden in einem Format zusammengeführt, das diese Probleme überwindet. Das Ergebnis: ein Schulungsangebot, das effektiver, ansprechender und für Ihr Unternehmen leichter zu verwalten ist.

Einbindung von Anfang an

Nachhaltige Veränderungen im Verhalten von Mitarbeitern brauchen Zeit. Das beginnt mit der Einbindung der Menschen und einer exakten Definition des Schulungsbedarfs Ihrer Mitarbeiter.

Mit unserem **Gamified Assessment Tool (GAT)** lässt sich der aktuelle Wissensstand Ihrer Mitarbeiter im Bereich Cybersicherheit schnell ermitteln und bewerten. So können Sie sich ein Bild davon machen, wie gut Ihr Unternehmen auf Cyberbedrohungen vorbereitet ist, und passende Kaspersky-Schulungen anbieten.

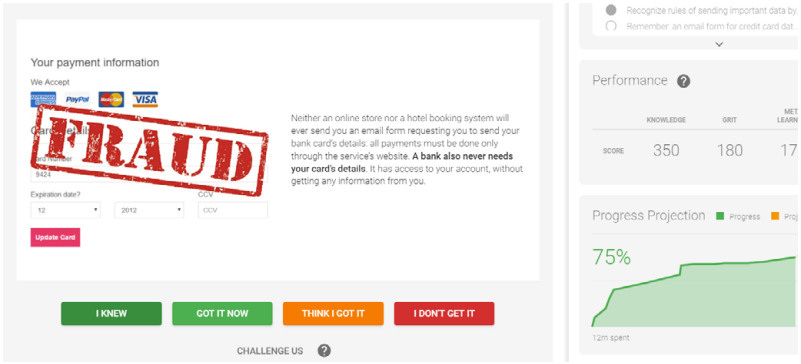
[13] Capgemini „The Digital Talent Gap"

Kompetenzerwerb durch adaptives Lernen

Das Kaspersky Adaptive Online Training (KAOT) basiert auf dem Prinzip des adaptiven Lernens und nutzt einem fortschrittlichen Lernalgorithmus, der die Kursteilnehmer durch die Themen leitet.

KAOT ist das einzige Format, das bei der Vermittlung von mehr als 300 Kompetenzen aus dem Bereich der Cybersicherheit einen wissenschaftlichen Ansatz verfolgt, der dafür sorgt, dass sichere Verhaltensweisen am Arbeitsplatz verinnerlicht und für jeden geschulten Mitarbeiter zur Selbstverständlichkeit werden.

KAOT überwacht den Fortschritt und passt den Kursfortschritt nach Korrektheit der Antworten und der Sicherheit an, das Sie im Laufe der Schulung entwickeln.



Screenshot KAOT-Schulung

Auch Mitarbeiter müssen nicht auf spielerische Lernmethoden verzichten. **Kaspersky [Dis]connected** – ein ebenso unterhaltsames wie lehrreiches Videospiel – ist ein zusätzliches Schulungsformat, mit dem die Inhalte aus den KAOT-Schulungen verinnerlicht werden sollen.

Für Generalisten-IT

Zu 100 % online:

Teilnehmer benötigen lediglich eine Internetverbindung

4 Module

mit kurzem Theorieteil und praktischen Tipps

4 bis 10 Übungen

zu spezifischen Fähigkeiten und zur Nutzung von IT-Sicherheitstools und -programmen

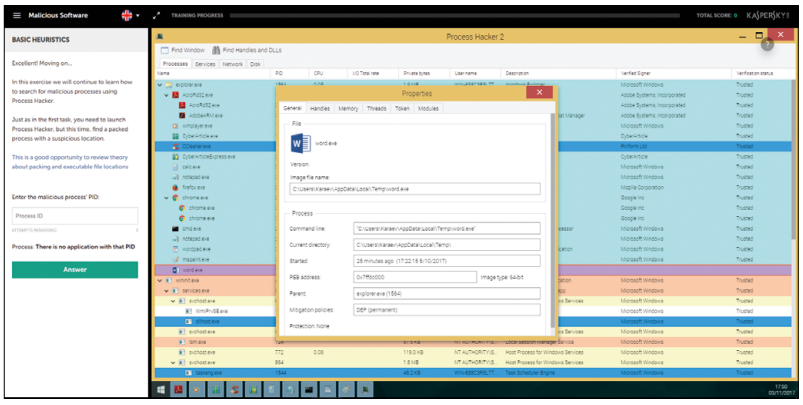
Erstreaktion bei Auftreten einer Störung

IT-Teams, Service Desk- und andere Sicherheitsmitarbeiter, die keine Experten sind, fallen oft durch das Raster gängiger Sicherheitsschulungen. Für allgemeine Unterweisungen sind sie meist zu erfahren, trotzdem brauchen sie – als erste Verteidigungslinie bei Zwischenfällen – spezielle Schulungen.

Für dieses wichtige Segment hat Kaspersky das Modul **Cybersecurity for IT Online (CITO)** entwickelt. In unserer Schulung lernen auch allgemeine IT-Mitarbeiter, woran sie erkennen können, ob es sich bei einem Angriffsszenario um einen gutartigen PC-Vorfall handelt.

CITO vermittelt außerdem Grundlagen zur Untersuchung sowie zum Arbeiten mit IT-Sicherheitswerkzeugen und -programmen. In theoretischen Modulen und praxisnahen Übungen erwerben Ihre IT-Fachleute darüber hinaus Kompetenzen, um im Falle eines Falles die notwendigen Vorfallsdaten zu sammeln und an die IT-Sicherheit weiterzuleiten.

Mit dieser Schulung bauen Sie den Schutz Ihres Unternehmens auf einer wichtigen Ebene der Vorfallsabwehr aus, ohne für die Kosten einer Schulung auf Expertenniveau aufkommen zu müssen.



Screenshot CITO-Schulung

CITO fördert außerdem den Spaß am Erkennen von Auffälligkeiten und festigt damit die Rolle Ihrer IT-Mitarbeiter als erste Verteidigungslinie.

Für Informationssicherheit und Unternehmenskommunikation

In Krisenzeiten effektiver kommunizieren

Weiß Ihr Kommunikationsteam, was es bei einem Cyberangriff tun muss? Diese Kompetenz steht nur selten auf dem Ausbildungsplan. Trotzdem ist sie unerlässlich, wenn ein externer oder interner Cybervorfall oder Advanced Persistent Threat (APT) erkannt wird.

Ihre Mitarbeiter müssen wissen, wie sie intern und extern auf einen Cybervorfall reagieren sollen, und dafür braucht es Führungsstärke und eine geeignete Notfallkommunikation.

Mit Kaspersky Incident Communications (KIC) wird das Kommunikationsteam Ihres Unternehmens anhand von Simulationen darin geschult, was im Falle eines Angriffs zu tun ist. Außerdem wird aufgezeigt, wie Sie sich während eines Cybervorfalls effektiv mit Ihrem IT-Sicherheitsteam abstimmen – einschließlich der Entwicklung und Einleitung von Maßnahmen, um den Schaden für den Ruf des Unternehmens sowie die finanziellen Verluste einzudämmen.

All dieses wertvolle Wissen kann in ein Handbuch für die Notfallkommunikation einfließen: So verbessern Sie Ihre Kommunikationsfähigkeit in Krisensituationen und sichern die Geschäftskontinuität.

Screenshot KIC-Schulung

Durch das Simulieren eines Cybervorfalls im Rahmen der KIC-Schulung wird Ihrem Krisenteam ein besseres Verständnis der möglicherweise bevorstehenden Cyberbedrohungen vermittelt.

Für Informationssicherheit und Unternehmenskommunikation

Praxisnah

Das Schulungsmaterial basiert auf einem realen zielgerichteten Angriff, der abgewehrt und erfolgreich nach außen kommuniziert wurde.

Professionell

Erstellt von renommierten Sicherheitsexperten und erstklassigen PR-Fachleuten.

Gut aufgestellt

Ihr Unternehmen erstellt oder aktualisiert einen Kommunikationsplan für Cyberkrisen, dem Ihr Vorfallsreaktionsteam folgen kann.

Fazit

Cyberbedrohungen sind vielfältig und nehmen mittlerweile ganz gezielt Ihre Mitarbeiter als schwächstes Glied der Cybersicherheitskette ins Visier.

Nicht jede Lösung passt, daher brauchen Sie Schulungen, mit denen auf jeder Ebene Ihres Unternehmens ein sicheres Arbeitsumfeld geschaffen wird – vom einfachen Sachbearbeiter bis zum obersten Management.

Kaspersky Security Awareness umfasst eine breite Palette von Lösungen, die auf die Bedürfnisse von Unternehmen zugeschnitten sind, sowie auf unterschiedliche Rollen angepasste Lerninhalte und ansprechende Lernmethoden bieten.

Sprechen Sie mit einem unserer Experten oder Partner darüber, wie sich Ihre Sicherheitsstrategie mit den Security Awareness-Lösungen von Kaspersky weiter optimieren lässt.

Kontakt