So fördern Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter – nachhaltig und aus einer Hand

kaspersky BRING ON THE FUTURE

Kaspersky Security Awareness Training

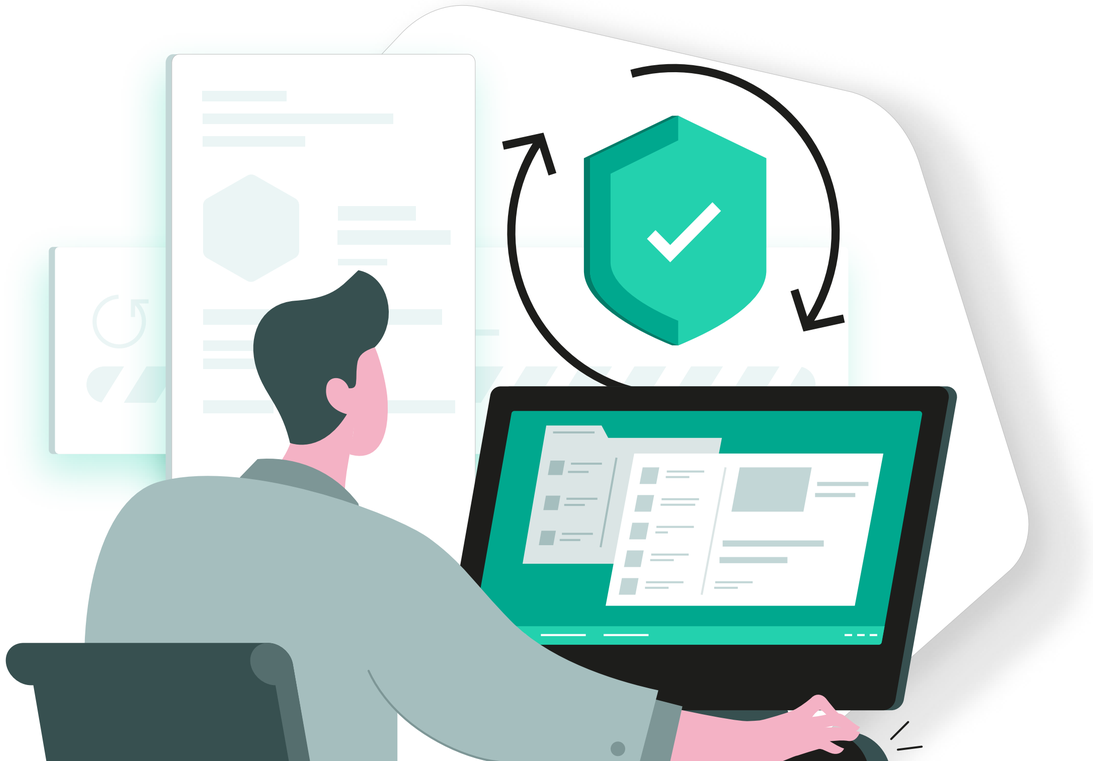
Schutz für das gesamte Unternehmen dank effektiver Sicherheitsschulungen

Die Kosten für eine Sicherheitsverletzung belaufen sich mittlerweile auf durchschnittlich 1.950.000 US-Dollar[1] pro Unternehmen. Mehr denn je müssen Sie in Ihrem Unternehmen für eine sicherere Arbeitsumgebung sorgen.

Tatsächlich sind Mitarbeiter heute die Hauptursache für die meisten Sicherheitsverletzungen.

Mitarbeiter sind der äußerste Schutzwall eines jeden Unternehmens. Daher benötigen Sie eine umfassende Schulungslösung, die auf allen Ebenen des Unternehmens ansetzt, von der Geschäftsführung und den Mitarbeitern bis hin zur IT und Unternehmenskommunikation. Und diese Schulungen müssen zwei Bedingungen erfüllen:

- Sie müssen unterschiedliche Techniken der Einbeziehung und Weiterbildung nutzen, wie Personalisierung, adaptives und spielerisches Lernen und Simulationen
- Sie müssen auf umfassender Sicherheitsexperte basieren. Kaspersky verfügt über mehr als 20 Jahre Erfahrung im Bereich der Cybersicherheit, so dass Sie sicher sein können, dass auch die wirklich notwendigen Kompetenzen vermittelt werden
- Unsere Lösungen liefern schnelle und kosteneffiziente Ergebnisse, vermitteln Kompetenzen, die von den Teilnehmern verinnerlicht und für den langfristigen Schutz Ihres Unternehmens eingesetzt werden können



[1] Wirtschaftlichkeit der IT-Sicherheit 2019, Kaspersky

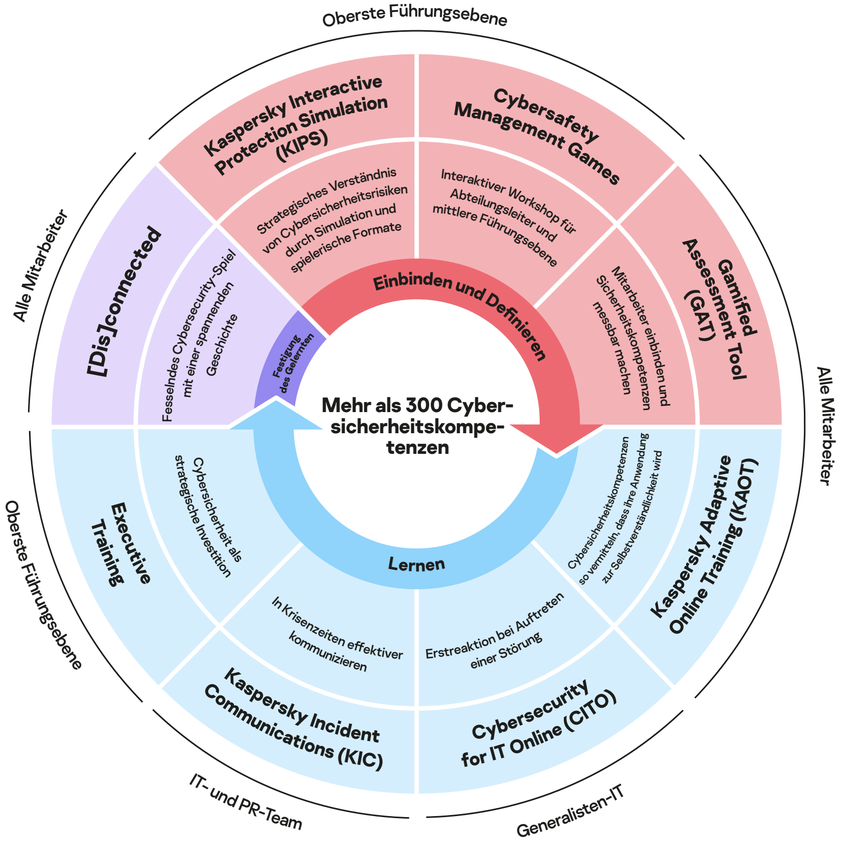
Flexible Gestaltungsmöglichkeiten

Unser einheitliches Schulungskonzept erleichtert Ihnen den Einstieg und die Ausrichtung der Weiterbildung an dem, was für Sie Priorität hat

So umfasst unser Schulungsangebot beispielsweise immersive Schulungen speziell für die oberste Führungsebene **(KASPERSKY INTERACTIVE PROTECTION SIMULATION)**; Mitarbeiterschulungen, die eine adaptiven Lernansatz verfolgen **(KASPERSKY ADAPTIVE ONLINE TRAINING)**; und Schulungen, die eine Brücke schlagen für Mitarbeiter, die zwar über mehr IT-Kenntnisse verfügen als andere, aber keine IT-Sicherheitsexperten sind **(CYBERSECURITY FOR IT ONLINE)**.

Mit Kaspersky können Sie sich für eine einzelne, effektive Lösung entscheiden, die den spezifischen und unmittelbaren Bedarf an Schulungen zum Thema Sicherheitsbewusstsein deckt – oder wir schnüren Ihnen ein Schulungspaket, das auf verschiedene Disziplinen in Ihrem Unternehmen zugeschnitten ist.

Mit dem Einsteigerpaket **Essential** wird beispielsweise allen Mitarbeiter solides Basiswissen vermittelt, wenn Unternehmen durch das Angebot von Cybersicherheitsschulungen gesetzliche Anforderungen erfüllen müssen. Es gibt ein **Enterprise**-Paket mit den wichtigsten Produkten, damit Mitarbeiter auf allen Ebenen des Unternehmens spezifische Kompetenzen erwerben und ihr Verhalten in Bezug auf Cybersicherheit verbessern können. Und schließlich gibt es noch das **Expert**-Paket mit spezialisierten Kursen für weiter gefasste IT- und Notfallteams.



Flexible Gestaltungsmöglichkeiten

28 % der Mitarbeiter[2]

sehen sich nicht in der Lage, Phishing-E-Mails zu erkennen

20 % der Führungskräfte[3]

wissen nicht, was sie im Falle einer Datenschutzverletzung zu tun ist

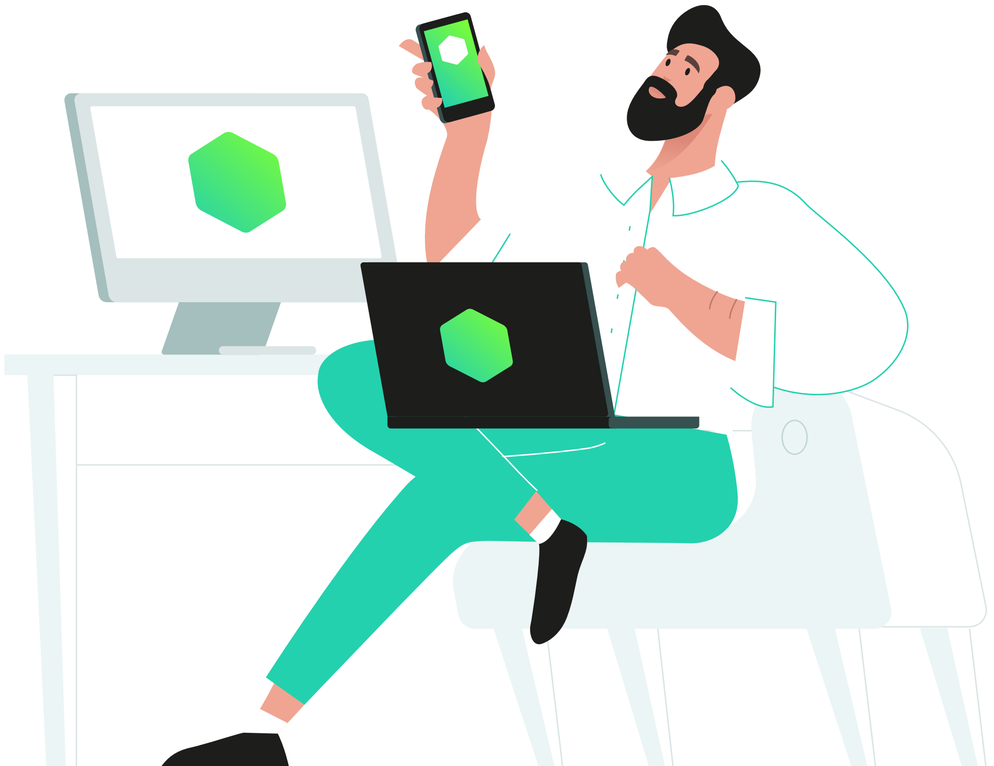
Nur 60 % der Organisationen[4]

bieten ihren Mitarbeitern formale Cybersicherheitsschulungen an

Ist Ihr Unternehmen geschützt?

Zu häufig wird stillschweigend davon ausgegangen, dass Mitarbeiter über die Sicherheitskompetenzen verfügen, die sie benötigen. Anhand dieser Checkliste können Sie erkennen, weshalb Sie die Security Awareness-Schulungen von Kaspersky benötigen. Je mehr Fragen Sie ehrlicherweise mit „Nein“ beantworten müssen, desto größer ist der Bedarf für diese Schulungen.

- Treten Ihre Führungskräfte vehement für die Vermeidung von Sicherheitsrisiken ein?
- Wissen Ihre Mitarbeiter, woran sie Cyberangriffe erkennen, und reagieren sie darauf instinktiv und automatisch?
- Sind Sie sicher, dass Ihre Mitarbeiter Passwörter nicht weitergeben und keine Schadsoftware auf Firmengeräte herunterladen?
- Hat Ihr Kommunikationsteam einen Notfallplan für den Umgang mit Cyberbedrohungen erstellt?
- Ist eine formale Schulung zum Thema Sicherheitsbewusstsein für alle Mitarbeiter Pflicht?



[2] 2020 State of Privacy and Security Awareness Report. MediaPRO.
[3] 2020 CrowdStrike-Berich
[4] 2020 „State of the Phish"-Bericht.

Schulungen zum Thema Sicherheitsbewusstsein auch für Vertreter der Führungsebene

84 % der Vertreter auf Führungsebene[5]

geben an, dass sie im vergangenen Jahr mindestens einmal Ziel eines Cyberangriffs waren, wobei Phishing-Angriffe (54 %) am häufigsten genannt werden

58 % der Vertreter auf Führungsebene[6]

geben an, dass IT-Sicherheit zu komplex ist, um sie zu verstehen

„Die Kaspersky Simulation war ein echter Augenöffner und sollte für alle Sicherheitsprofis zur Pflichtveranstaltung werden“

Warwick Ashford, Computer Weekly

Sicherheitsbewusstsein muss als Konzept von der obersten Führungsebene vorangetrieben werden, damit Ihr Unternehmen geschützt bleibt.

Daher müssen Schulungen auf Führungskräfte zugeschnitten sein. Sie können nicht einfach einem beliebigen Standard folgen, sondern müssen mit branchenspezifischen und immersiven Szenarien zum Nachdenken und – vor allem – zum Handeln anregen.

Mit KIPS wird Kaspersky diesem Anspruch gerecht, indem beispielsweise anfängliche Widerstände mit neuen, ansprechenden Lernmethoden überwunden werden. KIPS wurde speziell für die wichtigsten 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. Die Schulung kann mit oder ohne speziell auf die Führungsebene zugeschnittene Produkte gebucht werden. Zur Auswahl stehen zum Beispiel CYBERSAFETY MANAGEMENT GAMES – ein interaktiver Workshop – oder das EXECUTIVE TRAINING, ein Einführungskurs in die wesentlichen Grundlagen der Cybersicherheit für Führungskräfte, der von einem Referenten geführt wird.

Kaspersky Interactive Protection Simulation (KIPS)

Ansprechende Simulationen bringen Führungskräften auf anschauliche Weise die Besonderheiten der Cybersicherheit in unterschiedlichen Branchen nahe. Zur Auswahl stehen Szenarien für Konzerne, Versorgungsunternehmen, die kommunale Verwaltung sowie das Banken- und Transportwesen. Anhand dieser Beispiele wird eingeübt, wie man ein Unternehmen leitet, Gewinne macht und gleichzeitig real anmutende Cyberangriffe abwehrt.

Cybersafety Management Games

Mit diesen interaktiven Workshops und spielerischen Elementen sollen Führungskräfte zu Botschaftern der Cybersicherheit in Ihrem Unternehmen ausgebildet werden.

Executive Training

Mit diesem Format soll Führungskräften ein besseres Verständnis für vorhandene Cyberbedrohungen und Sicherheitsrichtlinien vermittelt werden. Sie lernen, wie sie die Widerstandskraft eines Unternehmens stärken und Cybersicherheit als strategische Investition einsetzen können.

Geeignet für Vertreter der Führungsebene

[5,6] MobileIron-Studie „Trouble at the Top“

Nach einer allgemeinen Einstufung wird jeder Mitarbeiter so ausgebildet, dass er in puncto Cybersicherheit ein Kompetenzniveau von 100 % erreicht

42 %[7] der Befragten

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

Sie sollten sich einen Überblick verschaffen, wie stark (oder schwach) die Cybersicherheitskompetenzen in Ihrer Organisation ausgebildet sind. Die größte Herausforderung besteht sicherlich darin, die Mitarbeiter für das Thema Cybersicherheit zu begeistern – weil sie entweder unmotiviert oder sich der eigenen Wissenslücken nicht bewusst sind.

Als Einstieg in das Kaspersky Security Awareness Training bieten wir Ihrem Team ein schnelles und spannendes Tool, um zu ermitteln, wie viel Sicherheitsbewusstsein in Ihrem Unternehmen bereits vorhanden ist. Im Gegensatz zu klassischen Assessment-Tools ist unser Gamified Assessment Tool niemals langweilig, definiert effektiv das Kompetenzniveau Ihrer Mitarbeiter und motiviert sie nachhaltig.

Ist das Interesse erst einmal geweckt, empfehlen wir als nächstes KAOT, ein Schulungsprogramm, das auf einer adaptiven Lernmethode und einem modernen Lernalgorithmus basiert. Mit diesem Produkt lässt sich das Kompetenzniveau Ihrer Mitarbeiter in der Hälfte der Zeit[8] (gegenüber vergleichbaren klassischen Online- oder Präsenzveranstaltungen) auf 100 % steigern. KAOT ist das Ergebnis einer einzigartigen Zusammenarbeit zwischen Kaspersky und Area9 Lyceum – einem führenden Anbieter von adaptiven Lernformaten. Darin werden mehr als 300 praktische Kompetenzen so vermittelt, dass den Teilnehmern die neuen Verhaltensweisen in Bezug auf die Cybersicherheit in Fleisch und Blut übergehen.

Gamified Assessment Tool (GAT)

Unser Assessment-Tool verschafft Ihnen einen Überblick über den Kenntnisstand Ihrer Mitarbeiter im Bereich Cybersicherheit. Der aktuelle Wissensstand wird auf unterhaltsame Weise abgefragt und der Schulungsbedarf wird ermittelt. Außerdem werden Mitarbeiter zur Weiterbildung motiviert.

Kaspersky Adaptive Online Training (KAOT)

Der Lehrplan wird mit unterschiedliche Aufgaben und/oder Lernpfaden an den Kenntnisstand des jeweiligen Mitarbeiters angepasst. Mit KAOT können mehr als 300 praktische Fertigkeiten so vermittelt werden, dass die richtige Reaktion auf Cyberbedrohungen am Arbeitsplatz zur Selbstverständlichkeit wird.

Für alle Mitarbeiter geeignet

[7] Capgemini „The digital talent gap"
[8] laut Forschungsergebnissen von Area9 zum erstmaligen Wissenserwerb

Aufbau von Kompetenzen für IT- und PR-Teams, um auf einer ersten Ebene richtig auf Vorfälle reagieren zu können

Gerade einmal 30 %[9] der Befragten

geben an, dass ihr Personalbestand im Bereich Cybersicherheit für ein hohes Maß an Cyberresilienz ausreicht

1 Million Dollar[10]

Durchschnittliche Gesamteinsparung im Falle einer Datenschutzverletzung, wenn es dem Unternehmen gelingt, effizient zu reagieren und den Cyberangriff innerhalb von 30 Tagen eindämmen

77 %[11] der Befragten

verfügen nicht über einen Notfallplan für Cybersicherheitsvorfälle

Der Aufbau einer robusten Cybersicherheit im Unternehmen kann ohne systematische Weiterbildung aller Mitarbeiter nicht gelingen. Das ist ein Problem, denn die meisten Unternehmensschulungen sind nicht für IT-Sicherheits- und PR-Teams ohne Expertenwissen gemacht.

Mit seinem umfassenden Schulungsangebot vermittelt Kaspersky IT-Personal wie Service Desk-Mitarbeiter und IT-Support/Admins praktische Kompetenzen zur Erkennung möglicher Angriffsszenarien durch scheinbar harmlose PC-Vorfälle wie Phishing (wie in 54 %[12] der Sicherheitsverletzungen der Fall).

Darüber hinaus wendet sich unsere Schulung an das Kommunikationsteam Ihres Unternehmens, damit auch diese Mitarbeiter helfen können, den Schaden einer Cyberbedrohung gering zu halten.

Cybersecurity for IT Online (CITO)

Der Spaß am Erkennen von Warnsignalen wird gefördert und damit die Rolle aller IT-Mitarbeiter als erste Verteidigungslinie gefestigt. Schließt bestehende Wissenslücken, ohne dass Mitarbeiter mit viel Aufwand und Geld zu Cybersicherheitsexperten ausgebildet werden müssen.

Kaspersky Incident Communications (KIC)

In diesem Kurs lernt Ihr Notfallteam, welche realen Cyberbedrohungen es gibt, welche Folgen sie haben können und welche Maßnahmen im Falle eines Falles zu ergreifen sind. Mitarbeiter werden in die Lage versetzt, den möglichen Reputationsschaden zu minimieren und direkte finanzielle Verluste zu begrenzen.

Geeignet für Spezialistenteams

[9,10,11] IBM-Studie, durchgeführt vom Ponemon Institute
[12] MobileIron-Studie „Trouble at the Top"

Neben dem Wissenserwerb ist es genauso wichtig, dass das Gelernte nicht gleich wieder in Vergessenheit gerät

Das ist uns bewusst. Deshalb ist im Lehrplan von Kaspersky auch vorgesehen zu prüfen, ob das Gelernte auch wirklich verinnerlicht wurde. Damit die neuen Fähigkeiten zur Gewohnheit werden, braucht es jedoch Übung und Erfahrung – und die könnte teuer werden.

Hier setzt [DIS]CONNECTED an. In dieser Simulation eines realen Angriffs erfahren Ihre Mitarbeiter in [DIS]CONNECTED, wie sich ein echter Angriff anfühlt. Und sie erhalten die Gelegenheit, ihre neuen Fähigkeiten auszuprobieren und das Gelernte abzurufen. Bei diesem praxisnahen Lernformat werden Situationen aus dem Alltag der Cybersicherheit in die Spielhandlung eingebunden.

Die letzte Lösung im Lernzyklus von [DIS]CONNECTED* kann von allen Mitarbeiter auf allen Ebenen genutzt werden, um die neu erlernten Kompetenzen praktisch anzuwenden und zu verinnerlichen.

[Dis]connected

Ein mobiles Lernspiel, in dem das Gelernte vertieft und die Mitarbeiter zu sicheren Verhaltensweisen motiviert werden. Die Teilnehmer lösen Fälle, die ein breites Spektrum von Cybersicherheitsthemen abdecken, und [Dis]connected hilft dabei herauszufinden, ob die Sicherheitskompetenzen der Mitarbeiter für heute – und in Zukunft – ausreichen.

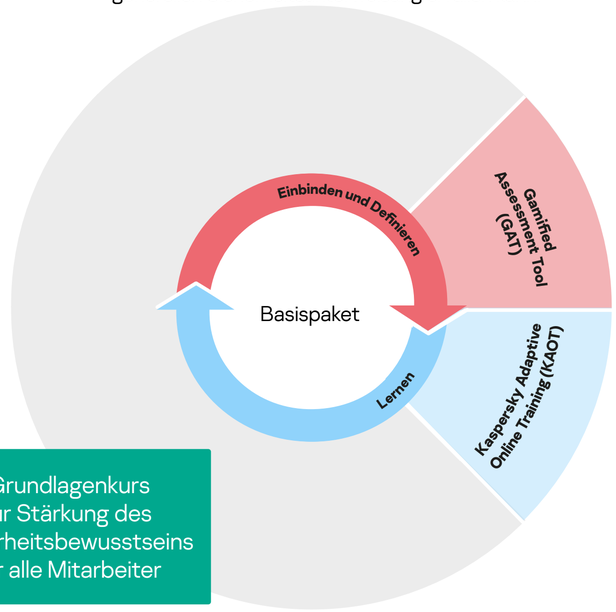
Für alle Mitarbeiter geeignet

* Da es sich bei [Dis]connected um eine mobile App handelt, können für die Bereitstellung besondere Bedingungen gelten – bitte wenden Sie sich wegen weiterer Details an Kaspersky

Individuell auf Sie zugeschnittene Schulungslösung zur Stärkung des Sicherheitsbewusstseins

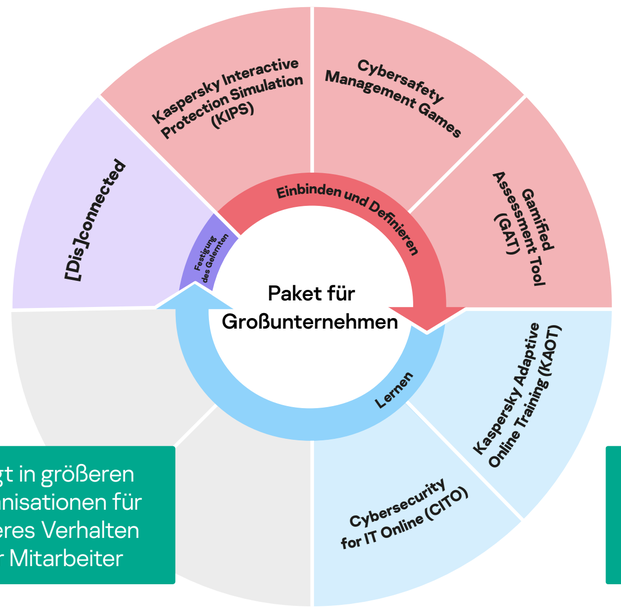
Die Lösungen von Kaspersky decken alle Ebenen Ihres Unternehmens ab und können einzeln oder zusammen gebucht werden. Darüber hinaus erleichtern wir Ihnen den Einstieg mit Paketen, die auf Ihre Bedürfnisse zugeschnitten sind und auf unserem dreistufigen Ansatz basieren: Einbinden und Definieren, Lernen und Festigung des Gelernten.

Vermittlung allgemeiner Grundlagen der Cybersicherheit, damit Ihr Betrieb erfolgreich arbeiten kann, vor verschiedenen Arten von Angriffen geschützt ist und die Anforderungen von Behörden oder Dritten bezüglich einer generellen Sicherheitsunterweisung erfüllen kann.



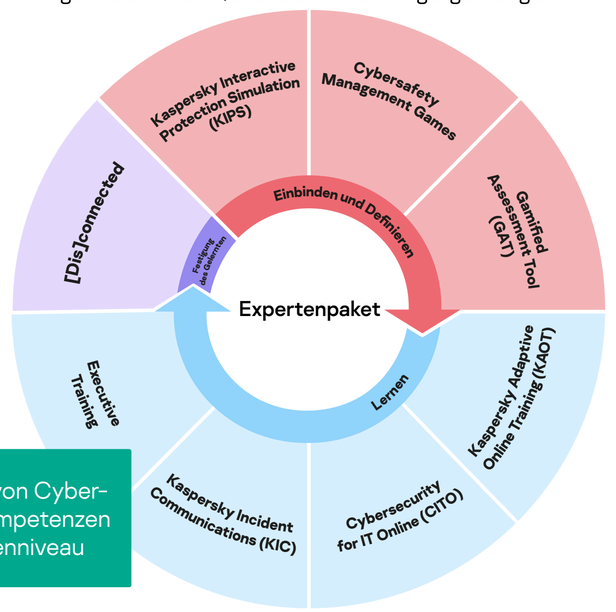
Grundlagenkurs zur Stärkung des Sicherheitsbewusstseins für alle Mitarbeiter

Eine einfache, sofort einsatzbereite Schulungslösung hilft größeren Organisationen, Geschäftskontinuität zu gewährleisten. Führt auf jeder Ebene des Unternehmens zu Verhaltensänderungen, indem alle Phasen des Lernzyklus abgedeckt werden.



Sorgt in größeren Organisationen für sicheres Verhalten der Mitarbeiter

Etabliert umfassende Cybersicherheit in Ihrem Unternehmen dank Führungskräften, die mit Bedrohungsszenarien vertraut sind, Mitarbeitern, die Cybersicherheitskompetenzen verinnerlicht haben, und einem breiter gefassten IT-Team, das als erste Verteidigungslinie agiert.



Vermittlung von Cybersicherheitskompetenzen auf Expertenniveau

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

kaspersky BRING ON THE FUTURE

Kaspersky Security Awareness Training