Cybersicher-
heitskompetenz
für Mitarbeiter
auf allen Ebenen

Kaspersky Security Awareness

kaspersky bring on the future

Weitere Informationen finden Sie unter
kaspersky.de/awareness

Kaspersky Security Awareness

Aufbau einer Cybersicherheitskultur in Ihrem Unternehmen

Mehr als 80 % aller Cybersicherheitsvorfälle werden durch menschliche Fehler verursacht. Indem Sie in Ihrem Unternehmen eine Kultur des cybersicheren Verhaltens sowie grundlegende Kompetenzen und ein Bewusstsein für Cybersicherheit aufbauen, können Sie die Angriffsfläche und die Zahl der Vorfälle, mit denen Sie sich befassen müssen, verringern. Der beste Weg, Verhaltensänderungen zu bewirken, die das Problem des „menschlichen Faktors" in der Cybersicherheit lösen, ist eine Schulung, die die neuesten Techniken und Technologien in der Erwachsenenbildung nutzt und die relevantesten und aktuellsten Inhalte vermittelt.

Der menschliche Faktor – das schwächste Glied in der Cybersicherheit

Cybersicherheitslösungen werden ständig weiterentwickelt und an immer komplexere Bedrohungen angepasst. Das macht Cyberkriminellen das Leben schwer, deshalb konzentrieren sie sich auf das schwächste Glied in der Kette – den Menschen.

55 % der Unternehmen berichten über Verstöße gegen IT-Sicherheitsrichtlinien durch ihre eigenen Mitarbeiter*

43 % der kleinen Unternehmen geben an, dass Verstöße gegen die IT-Sicherheitsrichtlinien durch Mitarbeiter zu Sicherheitsvorfällen führen **

Datenlecks sind das am weitesten verbreitete Sicherheitsproblem, das am häufigsten **von Mitarbeitern** (22 %) und Angreifern (23 %) verursacht wird

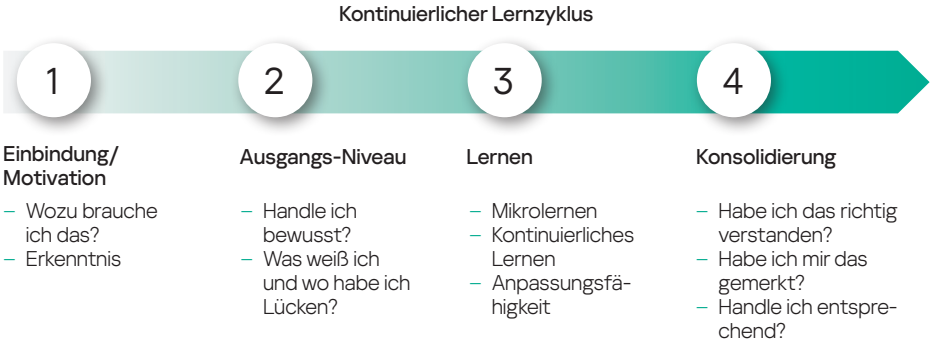
30 % der Mitarbeiter geben zu, dass sie die Anmeldedaten für ihre Dienstcomputer an Kollegen weitergeben***

23 % der Unternehmen haben keine Cybersicherheitsrichtlinien für die Speicherung von Unternehmensdaten***

Kaspersky Security Awareness – ein neues Konzept für die Vermittlung von IT-Sicherheitskompetenz

Kaspersky Security Awareness ist eine bewährte, effiziente Lösung mit langjähriger internationaler Erfolgsgeschichte. Die Lösung wird von Unternehmen jeder Größe genutzt, um über eine Million Mitarbeiter in mehr als 75 Ländern zu schulen. Sie verbindet über 25 Jahre Expertise von Kaspersky im Bereich Cybersicherheit mit umfassender Erfahrung in der Erwachsenenbildung.

Die hochgradig motivierenden und effektiven Schulungslösungen steigern das Bewusstsein Ihrer Mitarbeiter für Cybersicherheit, sodass sie ihren Teil zur allgemeinen Cybersicherheit im Unternehmen beitragen. Nachhaltige Verhaltensänderungen brauchen Zeit. Deshalb sieht unser Ansatz den Aufbau eines kontinuierlichen Lernzyklus vor, der aus mehreren Komponenten besteht.



Wichtige Alleinstellungsmerkmale des Programms

Umfangreiches Fachwissen im Bereich Cybersecurity

Mehr als 25 Jahre Erfahrung sind in unser Angebotspaket an Cybersicherheitsschulungen eingeflossen

Für Verhaltensänderungen auf jeder Ebene Ihrer Organisation

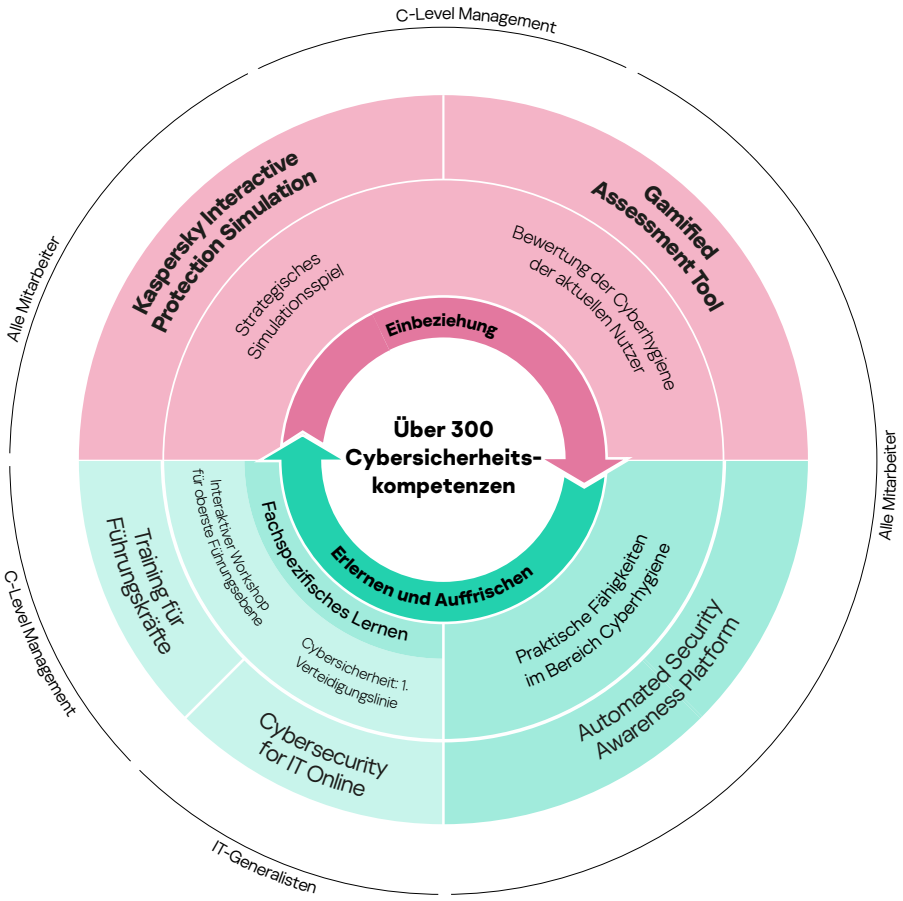
Durch Edutainment werden die Schulungsteilnehmer spielerisch einbezogen und motiviert, während Lernplattformen dafür sorgen, dass die neu erworbenen Kompetenzen verinnerlicht werden und das Gelernte nicht wieder in Vergessenheit gerät.

* Bericht „IT Security Economics 2022", Kaspersky
** Bericht „IT Security Economics 2021", Kaspersky
*** „Sorting out a Digital Clutter". Kaspersky, 2019.

Effektives Sicherheitsbewusstsein dank motiviertem Lernen

Das Verhalten der Mitarbeiter zu ändern, ist die größte Herausforderung für die Cybersicherheit In der Regel sind Menschen schwer dazu zu bewegen, Neues zu erlernen und Gewohnheiten zu ändern. Deshalb werden so viele Weiterbildungen zu einer reinen Pflichtübung. Effektive Schulungen bestehen aus unterschiedlichen Komponenten, berücksichtigen die menschlichen Natur und sorgen dafür, dass erworbene Fähigkeiten verinnerlicht werden. Als Experte in Sachen Cybersicherheit weiß Kaspersky, wie cybersicheres Benutzerverhalten aussieht. Wir haben unser Fachwissen und unsere Erkenntnisse durch Lernpraktiken und -methoden ergänzt, damit die Mitarbeiter unserer Kunden Risiken und Angriffe erkennen und richtig reagieren, während sie gleichzeitig ungehindert arbeiten können.

Spezielle Schulungsformate passend für einzelne Unternehmensebenen



Mitarbeiter machen Fehler. Organisationen verlieren Geld...

52.887 USD
pro Unternehmen
Durchschnittliche Kosten eines Cyberangriffs aufgrund unsachgemäßer Nutzung von IT-Ressourcen durch Mitarbeiter*

30 %
der Malware-Angriffe
erfolgen über E-Mails mit gefälschten Links und Anhängen**

79 %
der Mitarbeiter
geben zu, dass sie innerhalb eines Jahres mindestens eine riskante Aktivität ausgeübt haben, obwohl sie sich der Risiken bewusst waren***

164 USD
pro Datensatz
Die durchschnittlichen weltweiten Kosten für Verstöße, bei denen zwischen 2.200 und 102.000 Datensätze betroffen waren****

42 % der Befragten,
die in Unternehmen mit mehr als 1 000 Mitarbeitern arbeiten,
gaben an, dass die Mehrzahl der von ihnen absolvierten Schulungen nutzlos und uninteressant war*****

* Bericht „IT Security Economics 2022", Kaspersky
** Data Breach Investigation Report, 2022
*** Bericht „Balancing Risk, Productivity, and Security", Delinea 2021
**** Kosten einer Datenschutzverletzung, 2022. IBM
***** Capgemini „The Digital Talent Gap"

Kaspersky Security Awareness-Lösungen

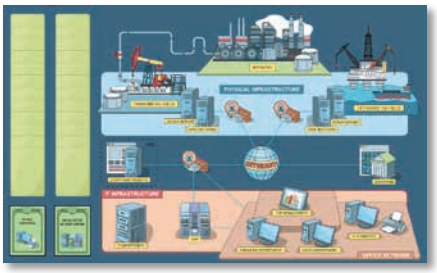
Engagement & Motivation

Teams sind nicht unbedingt begeistert, wenn sie an Pflichtschulungen teilnehmen müssen. Insbesondere das Thema Cybersicherheit wird von vielen als zu kompliziert oder langweilig empfunden oder als etwas, das sie nicht betrifft. Ohne die Motivation zu lernen, wird sich aber kaum ein Lernerfolg einstellen. Eine weitere Herausforderung für die Verantwortlichen im Bereich Weiterbildung besteht darin, auch Führungskräfte zu Schulungen zu motivieren, denn gerade deren Fehler können ein Unternehmen viel Geld kosten. Hier können Online-Planspiele helfen: Wenn sie spannend gemacht sind, gelingt es eher, Mitarbeiter zu Schulungen zu motivieren.

76 % der CEOs geben zu, dass sie Sicherheitsprotokolle umgehen, um etwas schneller zu erledigen, und damit die Sicherheit der Geschwindigkeit opfern*.

62 % der Manager geben zu, dass es in ihrem Unternehmen mindestens einen Cybersicherheitsvorfall gab, der auf eine mangelhafte Kommunikation über IT-Sicherheit zurückzuführen ist**

Die KIPS-Schulung richtet sich an Führungskräfte, Experten für Business-Systeme sowie IT-Experten. Sie fördert deren Sicherheitsbewusstsein hinsichtlich der eigenen Risiken und Herausforderungen beim Arbeiten mit vielen verschiedenen IT-Systemen und -Prozessen.



Kaspersky Interactive Protection Simulation (KIPS): Cybersicherheit aus Unternehmensperspektive

KIPS ist ein zweistündiges interaktives Teamspiel, das Verständnis von Entscheidungsträgern (Management, IT und CISOs) fördert und ihre Wahrnehmung von Cybersicherheit verändert. Es handelt sich um eine Software-Simulation, die die tatsächlichen Auswirkungen von Malware und anderen Angriffen auf die Unternehmensleistung und den Umsatz aufzeigt. Die Teilnehmer sind angehalten, strategisch zu planen, die Folgen eines Angriffs vorauszusehen und innerhalb der zeitlichen und finanziellen Grenzen entsprechend zu handeln. Jede Entscheidung wirkt sich auf alle Geschäftsprozesse aus ... das Hauptziel besteht in der Aufrechterhaltung des reibungslosen Geschäftsablaufs. Das Team, das am Ende des Spiels den höchsten Umsatz generiert hat, weil es alle Fallstricke im Cybersicherheitssystem gefunden und analysiert sowie angemessen reagiert hat, gewinnt.

13 branchenbezogene Szenarien (wird fortlaufend erweitert)

In jedem Szenario wird die Rolle der Cybersicherheit für Geschäftskontinuität und Geschäftserfolg aufgezeigt. Außerdem werden neue Herausforderungen und Bedrohungen sowie typische Fehler, die Organisationen beim Aufbau ihrer Cybersicherheit machen, hervorgehoben. Darüber hinaus wird die Zusammenarbeit zwischen kaufmännischen und Sicherheitsteams gefördert, um einen stabilen Betrieb und Nachhaltigkeit gegenüber Cyberbedrohungen zu gewährleisten.

KIPS ist in zwei Versionen erhältlich

Die sehr beliebte KIPS Live-Option schafft durch den besonderen Anreiz des persönlichen Wettbewerbs eine spannende und anregende Atmosphäre. Dies ist ein hervorragendes Instrument, um in einem Unternehmen eine Kultur der Cybersicherheit zu etablieren.

In der KIPS Online-Version können Nutzer standortunabhängig mit einer großen Anzahl von Teilnehmern interagieren. KIPS Online ist ideal für weltweit tätige Unternehmen oder Einrichtungen und mit KIPS Live kombinierbar. So können auch Remote-Teams in eine Veranstaltung vor Ort eingebunden werden.

- Bis zu 300 Teams (= 1000 Teilnehmer) gleichzeitig und von jedem Standort.
- Internationale Teams können eine Spieloberfläche in verschiedenen Sprachen wählen.
- Kunden können die vordefinierten Szenarien individuell anpassen, indem sie die Anzahl und die Art der Angriffe aus der Bibliothek auswählen.
- Die Online-Version bietet noch weitere Vorteile. So können Statistiken über die Entscheidungen der Spieler oder Daten über das Verhalten der Teams in bestimmten Situationen abgerufen und die Aktionen der Teilnehmer mit denen des vorherigen Spiels verglichen werden.

KIPS für Großunternehmen

Kunden, die sich für eine Lizenz entscheiden, mit der sie KIPS beliebig oft spielen können, haben die Möglichkeit, entweder die vordefinierten Einstellungen zu nutzen oder das Spielszenario bei jedem Spiel anzupassen, indem sie verschiedene Angriffe aus der Bibliothek auswählen und kombinieren. Mit dieser Funktion verläuft das Spiel jedes Mal anders, was es noch interessanter macht.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=62d4820c7626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

Ausgangs-Niveau

Den meisten Menschen ist nicht bewusst, wie wenig sie wissen, und das macht sie anfällig. Teilnehmer werden deshalb getestet und ihnen wird erklärt, wo sie aktuell in Bezug auf die Cybersicherheit stehen, damit künftige Schulungen die gewünschte Wirkung zeigen. Damit wird außerdem sichergestellt, dass keine Zeit für bereits bekannte Inhalte verwendet wird.

Gamified Assessment Tool: eine schnelle und spannende Möglichkeit, die Cybersicherheitskompetenz von Mitarbeitern zu bewerten

Mit dem Kaspersky Gamified Assessment Tool (GAT) können Sie sehr schnell den Kenntnisstand Ihrer Mitarbeiter in Bezug auf Cybersicherheit ermitteln. Der interessante, interaktive Ansatz macht Schluss mit der Langeweile, wie sie oft von klassischen Assessment-Tools ausgeht. In nur 15 Minuten durchlaufen die Mitarbeiter 12 alltägliche Situationen, die für die Cybersicherheit relevant sind. Die Teilnehmer sollen angeben, ob sich die dargestellte Person riskant verhält und wie sicher sie sich bei ihrer Antwort sind.

Nach Abschluss erhält jeder Teilnehmer ein Zertifikat mit einer Punktzahl, die den Grad seines Cybersicherheitsbewusstseins widerspiegelt. Darüber hinaus erhält er zu jedem Bereich ein Feedback mit Erklärungen und nützlichen Tipps.

Der spielerische Ansatz von GAT motiviert die Mitarbeiter und zeigt gleichzeitig, wo nach Analyse der dargestellten Situationen noch Wissenslücken bestehen. Das ist auch für IT- und Personalabteilungen interessant. Sie erhalten einen besseren Überblick über den Grad des Cybersicherheitsbewusstseins in der Organisation und können das Ergebnis zum Anlass für eine breitete Aufklärungskampagne nehmen.

Lernen

Unsere Online-Lernplattform ist das Kernelement des Awareness-Programms. Darin werden **mehr als 300 Cybersicherheitskompetenzen** vermittelt, die alle wichtigen IT-Sicherheitsthemen abdecken. Jede Lektion enthält Fallbeispiele aus dem Berufsalltag, damit die Verbindung zum realen Berufsleben gegeben ist. Und sie können diese Fähigkeiten sofort nach der ersten Lektion anwenden.

Kaspersky Automated Security Awareness Platform: effiziente und einfache Trainingsplanung für Unternehmen jeder Größe

Kaspersky ASAP ist ein effektives und benutzerfreundliches Online-Tool, das Mitarbeitern Cybersicherheitskompetenzen vermittelt und sie zu richtigem Verhalten motiviert.

Obwohl sich die Schulung an alle Unternehmen richtet, ist die automatisierte Verwaltung vor allem für solche Unternehmen interessant, die keine speziellen Ressourcen für das Schulungsmanagement haben.

Hauptvorteile:

- **Benutzerfreundlich dank vollständiger Automatisierung:** Das Programm lässt sich sehr einfach starten, konfigurieren und überwachen, wobei die Verwaltung im Verlauf vollständig automatisiert ist und kein Eingreifen durch den Administrator erfordert. Die Plattform erstellt für jede Mitarbeitergruppe einen Schulungsplan. Die Schulung beinhaltet Intervall-Lernen und wird automatisch über mehrere Formate bereitgestellt.

- **Benutzerfreundlichkeit für Administratoren ...** Automatisierte Plattformverwaltung, Synchronisierung mit AD (Active Directory), SSO (Single Sign-On), Open API (die Möglichkeit, mit Lösungen von Drittanbietern zu interagieren), ein benutzerfreundliches Dashboard, Online-Onboarding beim ersten Besuch, ein FAQ-Bereich und Tipps machen die Verwaltung der Plattform einfach und effizient.

- **... und Lernende:** Eine klare Lektionsstruktur, überschaubare Lektionen, Beispiele aus der Praxis, eine benutzerfreundliche Oberfläche, E-Mail-Erinnerungen, die Möglichkeit, Lektionen bei Bedarf zu wiederholen, eine sowohl mit PCs als auch mit mobilen Geräten kompatible Oberfläche – all das macht das Lernen angenehm, interessant und effektiv.

Kaspersky ASAP: Ein benutzerfreundliches Online-Tool, mit dem sich Ihre Mitarbeiter Stufe für Stufe im Bereich Cybersicherheit weiterqualifizieren können

In ASAP behandelte Themen:

- Passwörter und Konten
- E-Mail
- Websites und das Internet
- Social Media & Messenger
- PC-Sicherheit
- Mobile Geräte
- Schutz vertraulicher Daten
- DSGVO
- Industrial Cybersecurity
- Personenbezogene Daten
- Sicherheit von Bankkarten und Datensicherungsstandard für Kreditkartentransaktionen (PCI DDS)
- Doxing
- Sicherheit von Kryptowährungen
- Informationssicherheit bei Remote Arbeit

ASAP Express-Kurs

Eine Kurzfassung der Schulung in audiovisuellem Format.

- Interaktive Theorie
- Videos
- Tests

Kaspersky ASAP ist eine Mehr-Sprachen-Lösung.

ASAP eignet sich ideal für MSPs und xSPs – Schulungsangebote für mehrere Unternehmen lassen sich über ein einziges Konto verwalten und Lizenzen können als Monatsabonnement erworben werden.

Testen Sie kostenlos eine vollumfängliche Version von Kaspersky ASAP unter asap.kaspersky.com/de – überzeugen sie sich selbst, wie einfach es ist, ein eigenes Schulungsprogramm für Sicherheitsschulungen einzurichten und zu verwalten!

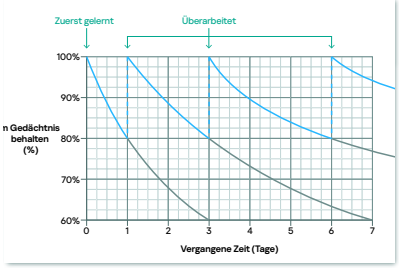
Konsolidierung

Die Festigung des Gelernten ist ein wesentlicher Bestandteil des Lernprogramms. Dadurch prägen sich die Teilnehmer das erworbene Wissen und die neuen Fähigkeiten dauerhaft ein.

Damit Gelerntes zur Gewohnheit wird, muss man es im Alltag anwenden. Gleichzeitig machen Menschen manchmal Fehler und lernen aus persönlichen Erfahrungen. Wenn es aber um Cybersicherheit geht, kann es sehr teuer werden, von den eigenen Fehlern zu lernen.

Mithilfe des spielerischen Lernens können Sie eine Situation und deren Konsequenzen „durchleben", ohne sich oder Ihrem Unternehmen zu schaden.

70 %
des Gelernten
werden bei herkömmlichen Trainingsmethoden innerhalb eines Tages vergessen



- **Vordefinierte Lernziele:** Die Programminhalte sind in einzelne Lernintervalle unterteilt und werden laufend durch Wiederholungen gefestigt. Die Methodik ist speziell auf die Eigenschaften des menschlichen Gedächtnisses ausgelegt und gewährleistet dadurch größere Lernerfolge und nachfolgende Anwendung der Kenntnisse.

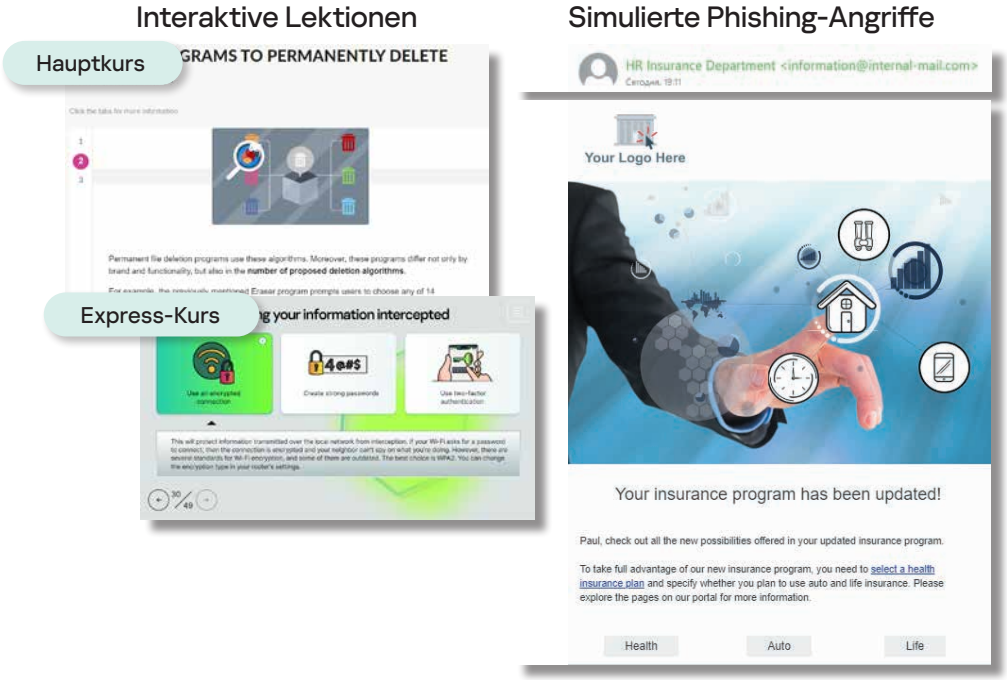
- **Anpassung:** Das Erscheinungsbild des Schulungsprogramms lässt sich im Handumdrehen anpassen: Ersetzen Sie im Verwaltungs- und Lernportal sowie in den E-Mails der Plattform das Kaspersky-Logo durch das Ihres Unternehmens, passen Sie die Zertifikate an und fügen Sie jeder Lektion persönliche Inhalte hinzu.

- **Flexibles Lernen:** Wählen Sie die für Sie passende Schulungsoption für Ihre Mitarbeiter: Mitarbeiter können entweder einen Express-Kurs absolvieren, mit dem sie schnell die gesetzlichen Anforderungen für Cybersicherheitsschulungen erfüllen oder ihr Wissen auffrischen. Oder Sie wählen den Hauptkurs, der in verschiedene Komplexitätsstufen unterteilt ist und in dem detailliertere und tiefer gehende Cybersicherheitskompetenzen vermittelt werden.

- **Flexibles Lizenzmodell** (für Managed Service Provider): Das anwenderbasierte Lizenzmodell ist schon ab 5 Lizenzen erhältlich und mehrere Unternehmen können über ein einzelnes Konto verwaltet werden.

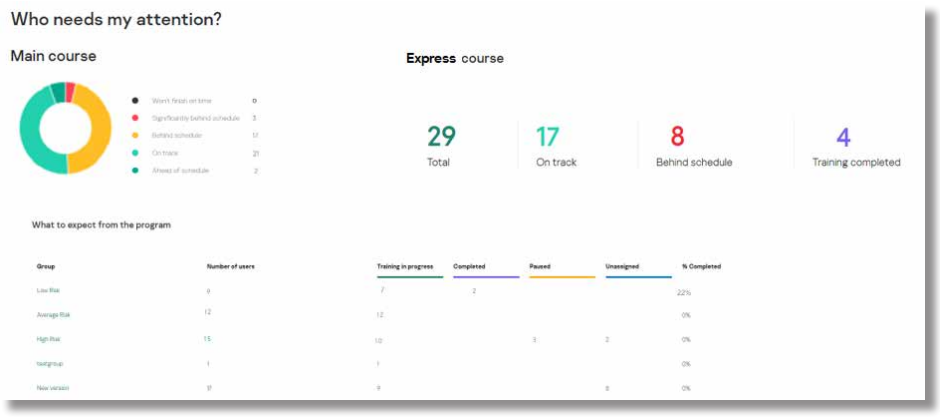
Simulierte Phishing-Angriffe

Simulierte Phishing-Angriffe können vor, während und im Anschluss an das Training eingesetzt werden, um die Kompetenz der Mitarbeiter im Umgang mit Cyberangriffen zu testen. Gleichzeitig können Mitarbeiter und Management dadurch die Vorteile des Trainings erkennen.



Nachverfolgung der Ergebnisse

Über das Dashboard können Sie die Fortschritte der Mitarbeiter, aber auch aller Gruppen bis hin zum gesamten Unternehmen auf einen Blick verfolgen und auswerten. Auch eine Detailansicht für einzelne Mitarbeiter ist möglich.



Fachspezifisches Lernen

Allgemeine IT-Fachkräfte: Helpdesk-Mitarbeiter und andere technisch versierte Mitarbeiter werden oft nicht geschult, weil Standard Awareness Programme für sie nicht ausreichen. Aber Unternehmen müssen sie auch nicht zu Cybersicherheitsexperten ausbilden: Das ist zu teuer, zeitaufwändig und überflüssig.

Wir freuen uns, ein Training ankündigen zu können, das diese Lücke füllt – nicht so tiefgehend wie eine Expertenschulung, aber weiterführender als eine Schulung für einfache Arbeitnehmer.

CITO Trainingsmodule:

- Schadsoftware
- Potenziell unerwünschte Programme und Dateien
- Grundlagen der Untersuchung
- Vorfallsreaktion bei Phishing-Angriffen
- Server-Sicherheit
- Active Directory-Sicherheit

Methode zur Durchführung der CITO-Schulung:

Cloud- oder SCORM-Format

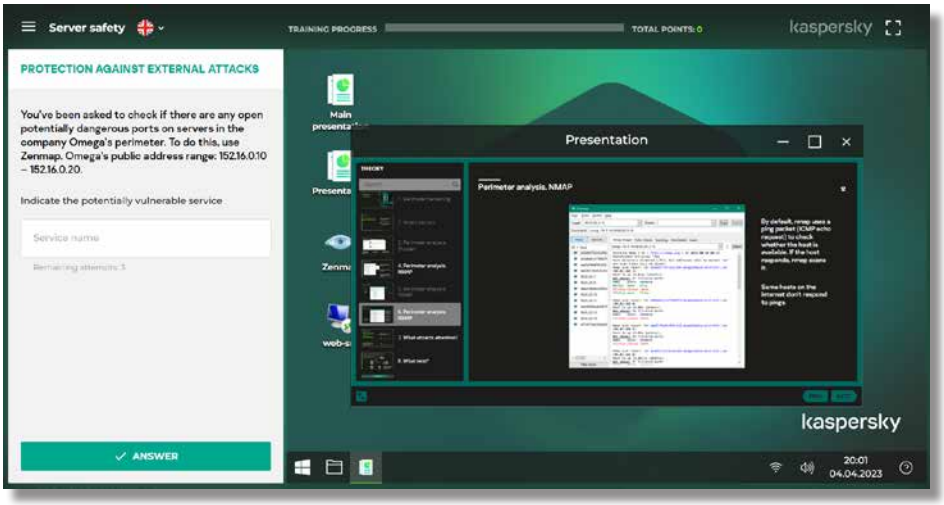
Cybersecurity for IT Online: die erste Verteidigungslinie bei Zwischenfällen

Cybersecurity for IT Online ist eine interaktive Schulung für jeden Beschäftigten im IT-Bereich. Dort werden solide Kenntnisse der Cybersicherheit sowie Fähigkeiten zur ersten Vorfallsreaktion aufgebaut.

Das Programm vermittelt IT-Fachleuten praktische Kompetenzen, um ein mögliches Angriffsszenario hinter einem scheinbar harmlosen PC-Vorfall zu erkennen. Außerdem wird der Spaß am Erkennen von Warnsignalen gefördert und damit die Rolle aller IT-Mitarbeiter als erste Verteidigungslinie gefestigt.

Außerdem vermittelt CITO die Grundlagen für die Analyse und die Arbeit mit IT-Sicherheitswerkzeugen und -programmen. In theoretischen Modulen und praktischen Übungen erwerben Ihre IT-Fachleute zudem die Kompetenz, im Ereignisfall die notwendigen Vorfallsdaten zu sammeln und an die IT-Sicherheit weiterzuleiten.

Diese Schulung wird für alle IT-Experten innerhalb des Unternehmens empfohlen, in erster Linie aber für Service Desks und Systemadministratoren. Der Großteil der Mitglieder in Sicherheitsteams, die keine IT-Experten sind, wird ebenfalls von diesem Kurs profitieren.



Führungskräfte zum Mitmachen bewegen

Top-Manager gehören zu den begehrtesten Zielen von Cyberkriminellen, sind aber nicht die einfachste Zielgruppe für Trainer. Ohne ihre Beteiligung und Unterstützung verschiedener Cybersicherheitsinitiativen ist es jedoch unmöglich, eine Cybersicherheitskultur in der Organisation zu schaffen.

Cybersicherheit ist neben Projektmanagement, Finanzinstrumenten und betrieblicher Effizienz ein wichtiger Aspekt der Umsatzgenerierung. Dies ist der Schwerpunkt unseres Kurses für Führungskräfte.

Training für Führungskräfte:

In unserem Schulungsprogramm für Führungskräfte lernen Unternehmensleitung und Top-Management in einem interaktiven Workshop oder Online-Kurs unter Anleitung eines Tutors die Grundlagen der Cybersicherheit kennen, um Cyberbedrohungen besser zu verstehen und sich davor zu schützen.

Dabei geht es vor allem um die finanziellen Aspekte der Cybersicherheit sowie um mögliche Investitionen, sodass Führungskräfte ein besseres Verständnis für den Zusammenhang zwischen Cybersicherheit und Unternehmenseffizienz entwickeln. Sie erfahren, was die aktuelle Bedrohungslage für ihr Unternehmen bedeutet, welche Maßnahmen im Falle eines Cyberangriffs zu ergreifen sind, plus viele weitere interessante, relevante und nützliche Informationen.

Eine KIPS-Schulung ist die ideale Ergänzung zu diesem Kurs. Die Schulung für Führungskräfte kann entweder vor oder nach KIPS absolviert werden, je nach Ihrem Ansatz für das Sicherheitsbewusstsein.

* Die aktuelle Liste der Module finden Sie unter cito-training.com

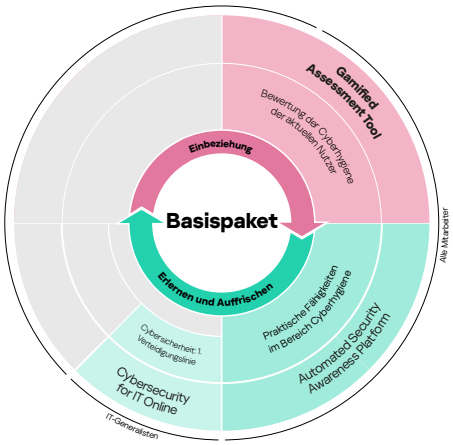
Kaspersky Security Awareness: Flexible Gestaltungsmöglichkeiten

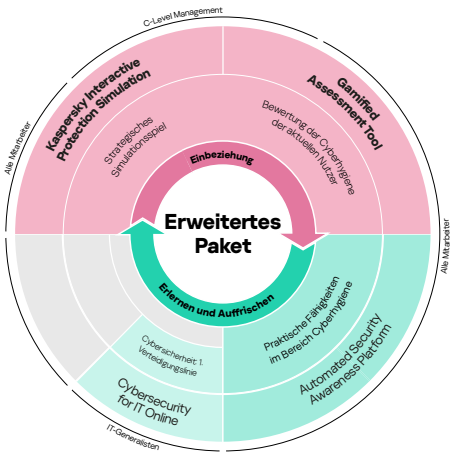
Die Schulungslösungen von Kaspersky decken jede Ebene Ihres Unternehmens ab und können einzeln oder zusammen gebucht werden. Da die Pakete genau auf Ihre Bedürfnisse zugeschnitten sind, ist der Einstieg ganz einfach.

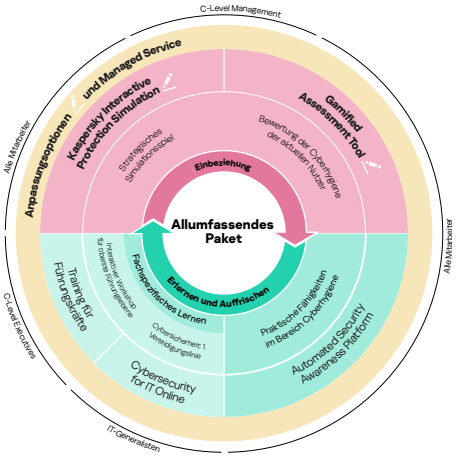
Eine einfache Möglichkeit, das Bewusstsein der Mitarbeiter für Cybersicherheit zu schärfen – einfach einzurichten, einfach zu verwalten. Vermittelt werden allgemeine Grundlagen, damit Sie die Anforderungen von Behörden oder Dritten in Bezug auf allgemeine Cybersicherheitsschulungen erfüllen können.

Eine einfache, sofort einsatzbereite Schulungslösung hilft größeren Organisationen, Geschäftskontinuität zu gewährleisten. Führt zu Verhaltensänderungen auf allen Ebenen des Unternehmens, indem jede Phase des Lernzyklus abgedeckt wird.

Die Lösung lässt sich benutzerdefiniert anpassen, bietet auch Managed Services und etabliert ein umfassendes Verständnis von Cybersicherheit in Ihrem Unternehmen – damit Führungskräfte mit Bedrohungsszenarien vertraut sind, Mitarbeiter über anwendbares Cybersicherheitswissen verfügen und allgemeine IT-Mitarbeiter Sie als erste Verteidigungslinie unterstützen.







Kaspersky Security Awareness Training verwendet die neuesten Schulungsmethoden und fortschrittliche Techniken, um den Erfolg zu gewährleisten. Flexible neue Paketlösungen können auf Ihre Bedürfnisse zugeschnitten werden, so dass mit Sicherheit für jeden das passende Angebot gefunden wird. Weitere Informationen finden Sie unter kaspersky.de/awareness

Kaspersky Security Awareness: kaspersky.de/awareness
IT Security News: business.kaspersky.de/

kaspersky.de

kaspersky