Computerbasierte Schulungsprogramme für alle Unternehmensbereiche

Kaspersky Security Awareness

kaspersky BRING ON THE FUTURE

Weitere Informationen finden Sie unter kaspersky.de/awareness

Kaspersky Security Awareness

Ein effektiver Weg zum Aufbau von Cybersicherheit im gesamten Unternehmen

Mehr als 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. Eine Kultur des cybersicheren Verhaltens zusammen mit grundlegenden Kompetenzen und einem geschulten Bewusstsein in Sachen Cybersicherheit im gesamten Unternehmen sind der Schlüssel zur Reduzierung der Angriffsfläche und der Zahl der Vorfälle, die Sie abarbeiten müssen. Organisationen tun sich oft schwer, die richtigen Tools und Methoden für effektive Schulungen zu finden, mit denen sich das Mitarbeiterverhalten dauerhaft verbessern lässt. Der Schlüssel zu diesem Ziel ist ein Schulungsangebot, das auf den neuesten Techniken und Technologien basiert und nur relevante und aktuelle 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 wenden sie sich dem schwächsten Glied der Kette zu: dem Menschen.

52 % der Führungskräfte auf C-Level nennen Mitarbeiter als die größte Bedrohung für die Betriebssicherheit*

43 % der kleinen Unternehmen erlitten infolge der Verletzung von IT-Sicherheitsrichtlinien durch Mitarbeiter einen Sicherheitsvorfall*.

60 % der Mitarbeiter haben vertrauliche Daten auf ihren Firmengeräten (z. B. Finanzdaten, E-Mail-Datenbanken, etc.)***

30 % der Mitarbeiter geben zu, dass sie die Anmeldedaten ihrer dienstlichen Computer an Kollegen weitergeben***

23 % der Unternehmen haben keine Cybersicherheitsrichtlinien für den Unternehmensdatenspeicher***

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

Kaspersky Security Awareness bietet eine Vielzahl von ansprechenden und effektiven Schulungslösungen, die das Bewusstsein Ihrer Mitarbeiter schärfen, damit jeder seinen Beitrag zu mehr Cybersicherheit im Unternehmen leisten kann. Weil nachhaltige Verhaltensänderungen Zeit brauchen, sieht unser Ansatz den Aufbau eines kontinuierlichen Lernzyklus vor, der aus mehreren Komponenten besteht.

Kontinuierlicher Lernzyklus

Einbindung/ Motivation	Ausgangs-Niveau	Lernen	Festigung des Gelernten
– Wozu brauche ich das? – Erkenntnis	– Handle ich bewusst? – Was weiß ich und wo habe ich Lücken?	– Mikrolernen – Kontinuierliches Lernen – Anpassungs-fähigkeit	– Habe ich das richtig verstanden? – Habe ich mir das gemerkt? – Handle ich entsprechend?

Wichtige Alleinstellungsmerkmale des Programms

Umfangreiches Fachwissen im Bereich Cybersecurity

Mehr als 20 Jahre Erfahrung im Bereich Cybersicherheit, die in eine Cybersicherheitskompetenz umgewandelt wurde und das Herzstück unserer Produkte bildet.

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: "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure", 2020

** Report "IT Security Economics 2021", Kaspersky.

*** Sorting out a Digital Clutter". Kaspersky, 2020

Mitarbeiter machen Fehler. Organisationen verlieren Geld...

1.315.000 $
pro Unternehmen
Durchschnittlicher finanzieller Schaden einer Datenschutzverletzung aufgrund unangemessener Nutzung von IT-Ressourcen durch Mitarbeiter*

50 %
der Unternehmen
berichteten von Bedrohungen, die direkt durch unangemessenes Verhalten von Mitarbeitern verursacht wurden, was dies zur häufigsten Bedrohung der IT-Sicherheit macht*.

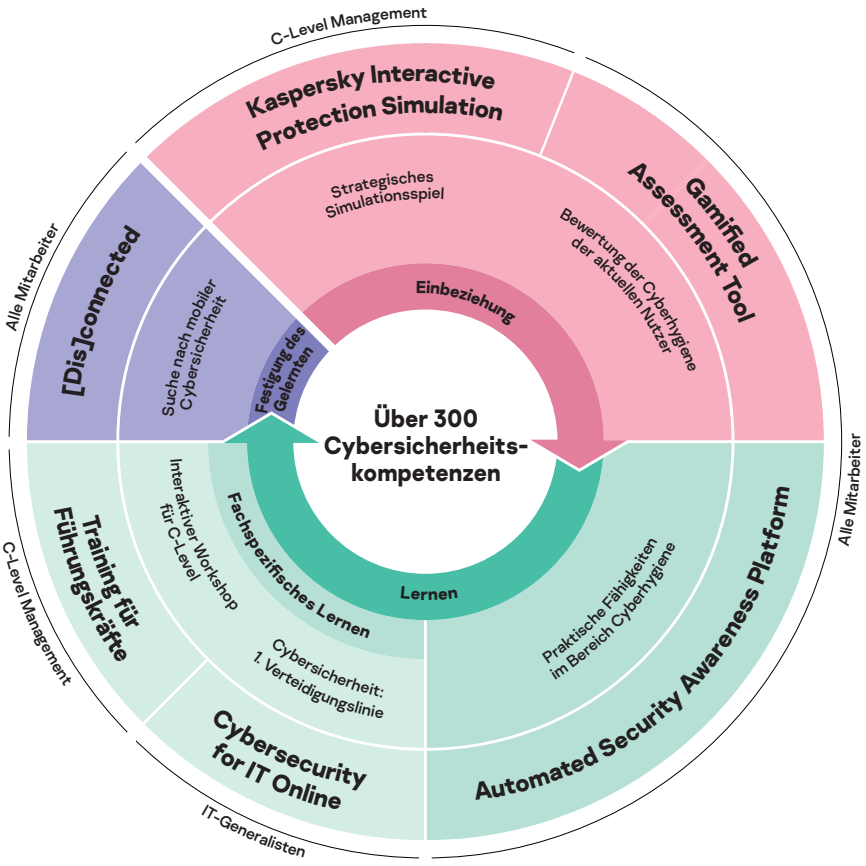
86 %
der Unternehmen
geben an, dass mindestens eine Person auf einen Phishing-Link geklickt hat**

5,01 Mio. US-Dollar
durchschnittliche Kosten pro Datenschutzverletzung
durch BEC-Angriffe (Business Email Compromise – eine Art von Phishing, bei der Angreifer die E-Mail-Konten von legitimen Firmen übernehmen oder fälschen)

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



* Report "IT Security Economics 2021", Kaspersky
** Bedrohungstrends in der Cybersicherheit 2021, CISCO
*** Kosten einer Datenschutzverletzung, 2021. IBM

Kaspersky Security Awareness-Lösungen

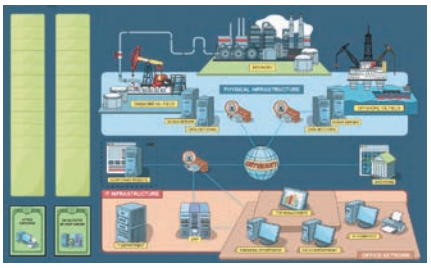
Motivation

Mitarbeiter sind nicht unbedingt begeistert, wenn sie verpflichtende Schulungen absolvieren sollen, und gerade den Bereich Cybersicherheit halten viele für zu kompliziert oder langweilig bzw. glauben, dass das nichts mit ihnen zu tun hat. 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.

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

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

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 unternehmerischer Perspektive

KIPS ist ein zweistündiges interaktives Teamspiel, das ein Verständnis unter Entscheidungsträgern (Geschäftsführung, IT und CISO) aufbaut und deren Wahrnehmung bezüglich 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 stetig erweitert)

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

Individuelle Anpassung von Szenarien

Ab dem 3. Quartal 2022 werden Unternehmen für ausgewählte Branchen eigene Szenarien mit verschiedenen Angriffen erstellen können. Durch unterschiedliche Angriffskombinationen können Unternehmen mit einer KIPS-Unternehmenslizenz dasselbe Branchenszenario mehrfach durchspielen.

KIPS Virtual Reality

KIPS Power Station VR ist ein neues immersives und realistisch gestaltetes Erlebnis, das dem realen Betrieb eines Kraftwerks sehr nahe kommt. Manager können als IT-Sicherheitsspezialisten fungieren. Die Rolle der Cybersicherheit und ihre Auswirkungen auf das Business werden dabei so ansprechend dargestellt, dass sie die Folgen ihrer IT-Entscheidungen nicht mehr nur rein abstrakt, sondern in äußerst realistischen 3D-Grafiken erleben können.

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.

Lernen

Unsere Online-Lernplattform bildet das Herzstück unseres 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 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 & Messengers
- PC-Sicherheit
- Mobile Geräte
- Schutz vertraulicher Daten
- DSGVO
- Industrial Cybersecurity

ASAP Schnellkurs

Eine Kurzfassung der Schulung im audiovisuellen Format.

- Interaktive Theorie
- Videos
- Tests

Kaspersky ASAP ist eine Lösung, die in mehreren Sprachen angeboten 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, für die Cybersicherheit relevante Situationen. Dabei sollen die Teilnehmer angeben, ob sich die dargestellte Person riskant verhält und wie sicher sie sich 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.

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

Kaspersky ASAP ist ein effektives und benutzerfreundliches Online-Tool, das Mitarbeitern Wissen im Bereich Cybersicherheit vermittelt und zu richtigem Verhalten motiviert.

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

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 Schulungsformate bereitgestellt, einschließlich Lernmodule, E-Mails zur Wiederholung, Tests sowie simulierte Phishing-Angriffe.
- **Effizienz:** 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.
- **Flexibles Lernen:** Wählen Sie die für Sie passende Schulungsoption für Ihre Mitarbeiter: Mitarbeiter können einen Schnellkurs absolvieren, mit dem sie schnell die gesetzlichen Anforderungen für die Weiterbildung in Sachen Cybersicherheit erfüllen oder ihr Wissen auffrischen können. Alternativ kann ein Hauptkurs gewählt werden, der in verschiedene Komplexitätsstufen unterteilt ist und detailliertere und tiefgreifende Cybersicherheitskompetenzen vermittelt.
- **Flexibles Lizenzmodell** (für Managed Service Provider): Das anwenderbasierte Lizenzmodell ist schon ab 5 Lizenzen erhältlich.

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!

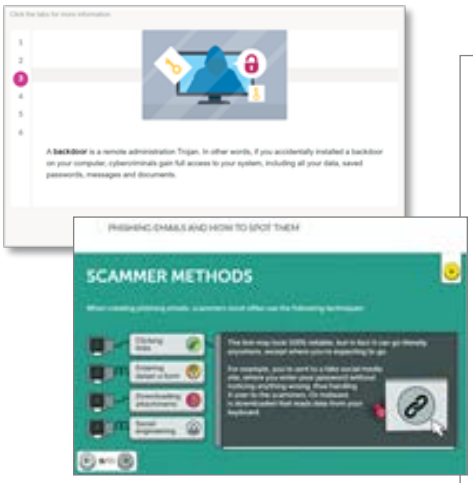
Simulierte Phishing-Angriffe

Simulierte Phishing-Angriffe können vor, während und nach der Schulung eingesetzt werden, um die Kompetenzen der Mitarbeiter im Umgang mit Cyberangriffen zu testen. Gleichzeitig können Mitarbeiter und die Unternehmensleitung einschätzen, wie effektiv die Schulung war.

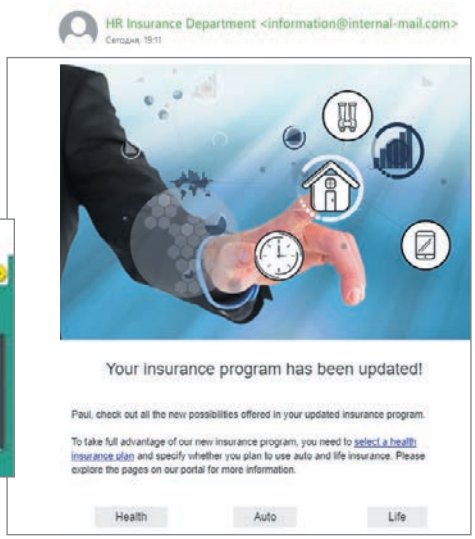
Interaktive Lektionen

Hauptkurs

Schnellkurs



Simulierte Phishing-Angriffe



Ergebnisnachverfolgung

Über das Dashboard können Sie die Fortschritte der Mitarbeiter, aber auch sämtlicher Gruppen bis hin zum gesamten Unternehmen verfolgen und auswerten. Auch eine detailliertere Ansicht für einzelne Mitarbeiter ist möglich.

Festigung des Gelernten

Die Festigung des Gelernten ist ein wesentlicher Bestandteil des Lernprogramms. So prägen sich Schulungsteilnehmer 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.

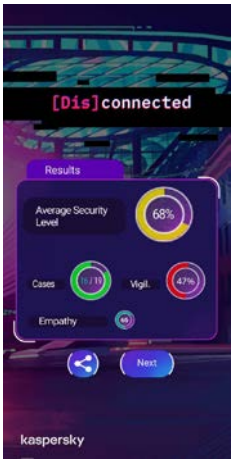
Mithilfe des spielerischen Lernens können Sie eine Situation und deren Konsequenzen „durchleben", ohne sich oder Ihrem Unternehmen zu schaden.

[Dis]connected: die Suche nach mobiler Cybersicherheit

[Dis]connected ist ein immersiv gestaltetes neues Cybersicherheits-Planspiel, bei dem es darum geht, Beruf und Privatleben in ein gesundes Verhältnis zu bringen und sowohl privat als auch beruflich erfolgreich zu sein.

In den Ablauf sind Fragen der Cybersicherheit eingeflochten, die zeigen, inwiefern unsere Entscheidungen in puncto Cybersicherheit geeignet sind, diese Ziele zu erreichen – oder eben nicht. Insgesamt sind 24 Fälle zu lösen, mit Themen wie Passwörter und Konten, E-Mail, Surfen im Internet, Soziale Netzwerke und Messenger, Computersicherheit und mobile Geräte, Das Gefühl, mitten im Geschehen zu stehen, wird durch emulierte Programme wie Messenger-Dienste, Banking-Apps usw. noch zusätzlich verstärkt.

Am Ende des Spiels gibt es eine Auswertung, wie erfolgreich die Teilnehmer das Projekt gemeistert haben und ob sie über ausreichende Sicherheitskompetenzen verfügen – jetzt und in Zukunft.



Das Spiel läuft auf Smartphones. Eine **kostenlose Demo** ist bei Google Play und im AppStore verfügbar: https://kas.pr/mobilestores

Fortschrittliche Lernmethode

Allgemeine IT-Spezialisten: Helpdesk-Mitarbeiter und andere technisch versierte Mitarbeiter werden oft nicht geschult, weil Standardprogramme zur Sensibilisierung für sie nicht ausreichen. Aber Unternehmen müssen sie auch nicht zu Cybersicherheitsexperten ausbilden: Das wäre teuer, zeitaufwändig und überflüssig.

Unser Schulungsprogramm füllt diese Lücke – nicht so tiefgreifend wie eine Expertenschulung, aber weiterführender als eine Schulung für Mitarbeiter, die nicht im IT-Bereich arbeiten.

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

Testen Sie eines der CITO-Module kostenlos: cito-training.com

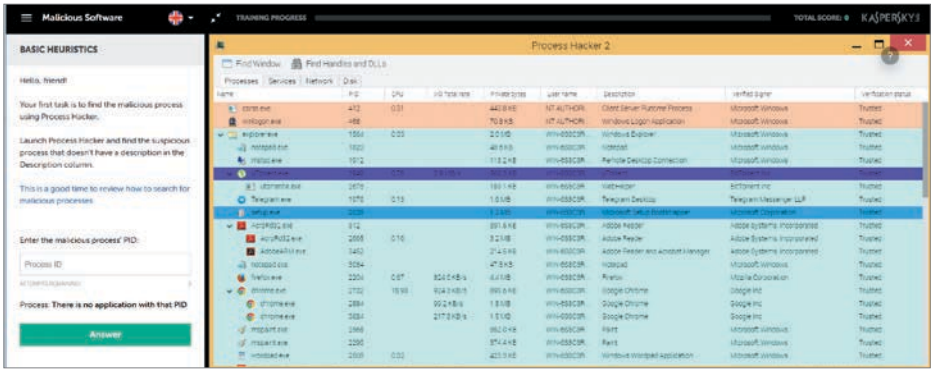
Cybersecurity for IT Online: Abwehr an vorderster Front

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 bei 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.

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.

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.



Cyberkriminelle nehmen zunehmend Top-Manager ins Visier. Für Schulungsreferenten gehören diese aber oftmals nicht gerade zum einfachsten Klientel. Ohne ihre Einbeziehung in verschiedene Initiativen zur Cybersicherheit ist es jedoch unmöglich, eine Cybersicherheitskultur in der Organisation zu schaffen.

Neben dem Projektmanagement, den Finanzinstrumenten und der betrieblichen Effizienz hat die Cybersicherheit einen wesentlichen Anteil an der Umsatzgenerierung. Das bildet den Schwerpunkt unseres Kursangebots für Führungskräfte.

Executive Training: Stärkung der Widerstandsfähigkeit von Unternehmen im digitalen Wandel

Führungskräfte und Top-Manager erlernen die Grundlagen der Cybersicherheit im Rahmen eines von Referenten geführten Kurses. So wird ein besseres Verständnis von Cyberbedrohungen und möglichen Schutzmechanismen entwickelt.

Untersuchungen zeigen, dass ein direkter Zusammenhang zwischen einer schnellen, effizienten Vorfallsreaktion und dem Ausmaß des Schadens besteht, den ein Vorfall verursachen kann. Der Kurs geht vor allem auf die finanziellen Aspekte der Cybersicherheit sowie mögliche Investitionen ein und vermittelt Führungskräften ein besseres Verständnis für den Zusammenhang zwischen Cybersicherheit und Unternehmenseffizienz.

Die Schulung lässt sich hervorragend mit Kaspersky Interactive Protection Simulation (KIPS) kombinieren, um den Stoff durch praktische Übungen zu vertiefen.

Ziele des Kurses

- Neueste Informationen zu modernen Cyberbedrohungen und deren Risiken für Unternehmen
- Teilnehmer werden auf den neuesten Stand der modernen Cyberbedrohungslandschaft gebracht
- Praxisnahe Vermittlung der Grundregeln einer persönlichen und unternehmerischen Cybersicherheitskultur für Führungskräfte
- Aufklärung über die Auswirkungen der wichtigsten rechtlichen Fragen im Bereich der Informationssicherheit für Unternehmen
- Einführung in die Grundkonzepte der Cybersicherheit und Vermittlung von Methoden zum Schutz vor gezielten Angriffen
- Praktische Empfehlungen für die Implementierung von Unternehmensrichtlinien
- Beratung zur Kommunikation während der Vorfallsreaktion und der Untersuchung von Vorfällen

Kaspersky Security Awareness: Flexible Gestaltungsmöglichkeiten

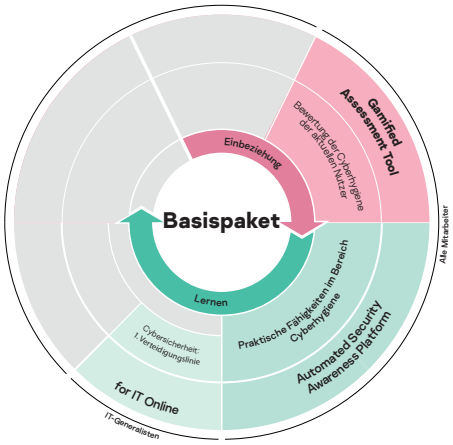
Die Schulungslösungen von Kaspersky decken jede Ebene Ihres Unternehmens ab und können einzeln oder zusammen gebucht werden. Aufgrund der speziell auf Ihre Bedürfnisse zugeschnittenen Pakete ist der Einstieg in unser Schulungsprogramm ganz unkompliziert.

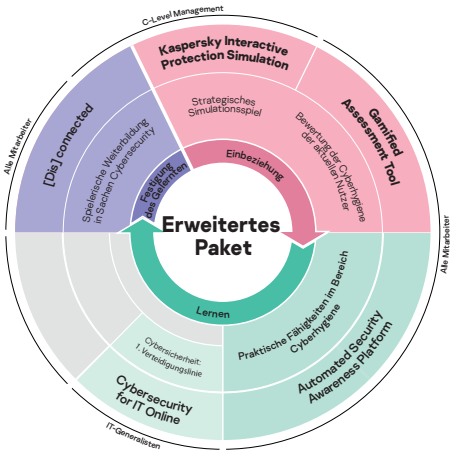
Mit dieser einfach umsetzbaren Option verbessern Sie das Cybersicherheitsbewusstsein Ihrer Mitarbeiter nachhaltig und profitieren von benutzerfreundlicher Konfiguration und Verwaltung.

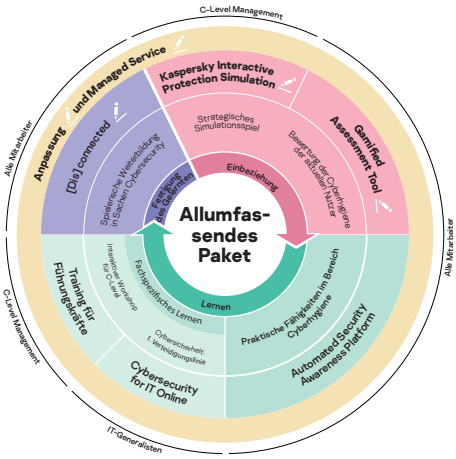
Vermittelt werden allgemeine Grundlagen, damit die Anforderungen von Behörden oder Dritten in Sachen Cybersecurity erfüllt werden können.

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 – mit Führungskräften, die mit Bedrohungsszenarien vertraut sind, Mitarbeitern, die Cybersicherheitskompetenzen verinnerlicht haben, und einem breiter gefassten IT-Team, das als erste Verteidigungslinie agiert.







Kaspersky Security Awareness Training nutzt 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 alle Anforderungen das passende Angebot gefunden wird. Weitere Informationen finden Sie unter kaspersky.de/enterprise-security/security-awareness

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

kaspersky.de

kaspersky BRING ON THE FUTURE