Computerbasierte Schulungsprogramme für alle Unternehmensbereiche

Kaspersky Security Awareness

kaspersky BRING ON THE FUTURE

Weitere Informationen finden Sie unter kaspersky.de

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 in der Erwachsenenbildung basiert und nur absolut 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 Unternehmen sehen Mitarbeiter als größte Bedrohung der Cybersicherheit*

60 % der Mitarbeitergeräte beinhalten vertrauliche Daten (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 verwenden 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 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.

* Forschung: „The cost of a data breach", Kaspersky Lab, Frühjahr 2018.

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

Mitarbeiter machen Fehler. Organisationen verlieren Geld...

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

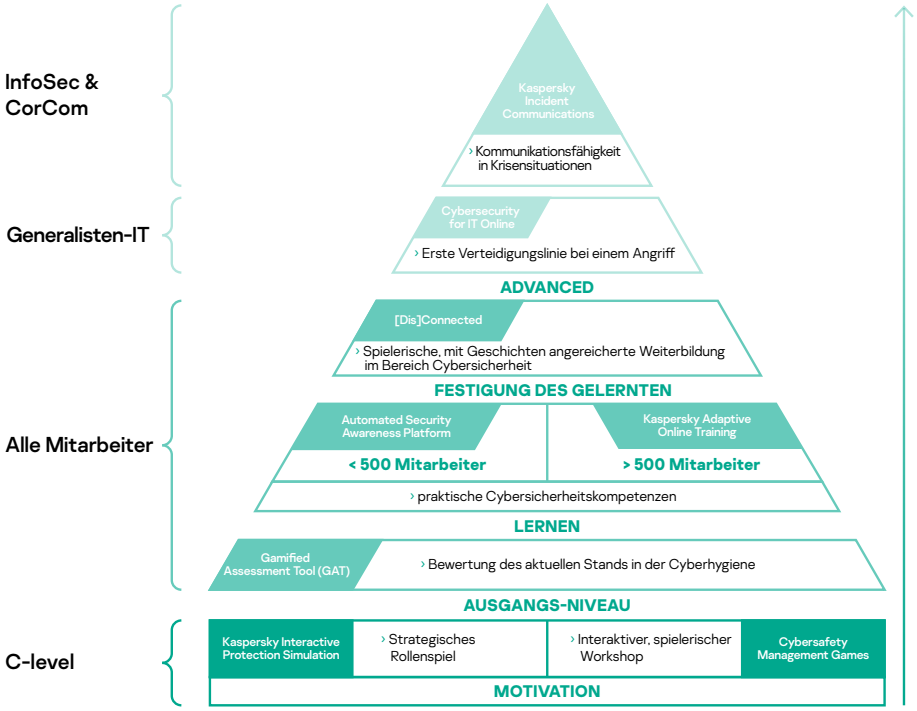
52 %
der Großunternehmen
erlebten einen Cybersicherheitsvorfall aufgrund unangemessener Nutzung von IT-Ressourcen durch Mitarbeiter**

Mehr als 1,7 Mrd. USD
globale finanzielle Verluste
aufgrund von kompromittierten unternehmens-e-mails***

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



* Bericht: „On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives". Kaspersky, 2020

** Bericht: „IT security economics in 2019", Kaspersky

*** FBI „2019 Internet Crime Report"

Kaspersky Security Awareness-Produkte

Einbindung/ Motivation

Ausgangs-Niveau

Lernen

Festigung des Gelernten

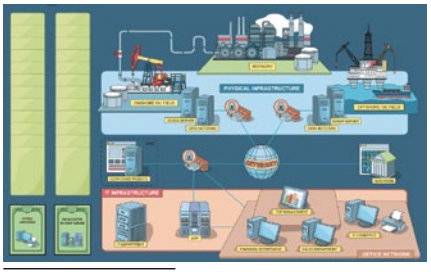
Motivation

Mitarbeiter sind nicht unbedingt begeistert, wenn sie noch mehr 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.



* Die „Vergessenskurve" von Ebbinghaus
** Capgemini „The Digital Talent Gap"

Das Strategiespiel 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.

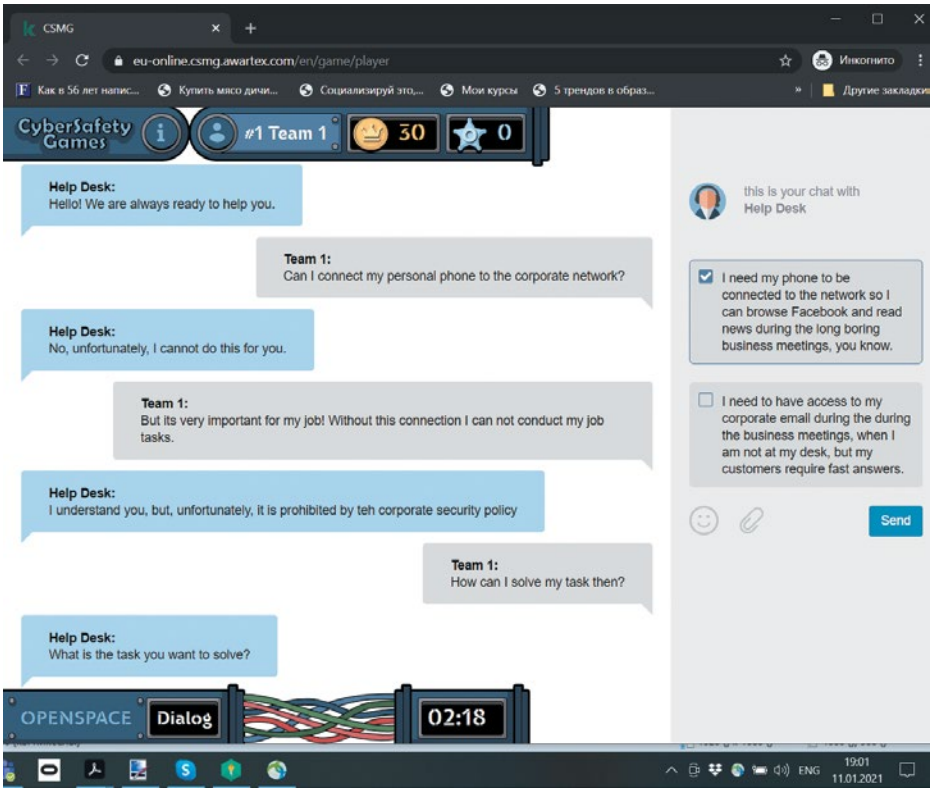
10 branchenbezogene Szenarien (und ständig kommen weitere hinzu)

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

Cybersafety Management Games: So werden aus Geschäftsführern und Abteilungsleitern aktive Botschafter der Cybersicherheit

Cybersafety Management Games ist ein interaktiver Workshop (Kombination aus computergestützter und Präsenzschulung oder vollständig online), in dem Führungskräften Kompetenzen, Fachwissen und die richtige Einstellung vermittelt werden, um in der eigenen Abteilung eine sichere Arbeitsumgebung zu schaffen, ohne dass die Effizienz darunter leidet. Diese Schulung macht Abteilungsleiter und mittleres Management zu Unterstützern und Botschaftern der Cybersicherheit, damit Cybersicherheit zu einem wichtigen Bestandteil der täglichen Entscheidungsfindung wird.

In der Schulung geht es um grundlegende falsche Vorstellungen, die die meisten Menschen haben, und Führungskräfte erfahren, warum Mitarbeiter dazu neigen, Regeln und Prinzipien der Cybersicherheit zu missachten. Mithilfe speziell entwickelter Übungen wird dann aufgezeigt, wie man diese falschen Vorstellungen in positives, cybersicheres Verhalten umwandelt.



Einbindung/ Motivation

Ausgangs-Niveau

Lernen

Festigung des Gelernten

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, wobei die Teilnehmer angeben sollen, 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.

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.

Kaspersky Adaptive Online Training: Cybersicherheitstraining von einem führenden IT-Sicherheitsanbieter auf Basis der adaptiven Lernmethode

Kaspersky Adaptive Online Training (KAOT) ist eine herausragende Lösung, bei der Inhalte aus der über 20-jährigen Erfahrung von Kaspersky im Bereich Cybersicherheit mit einer fortschrittlichen Lern- und Entwicklungsmethode kombiniert werden. KAOT ist das Ergebnis einer Zusammenarbeit zwischen Kaspersky und Area9 Lyceum, einem führenden Unternehmen für adaptive Lernsysteme.

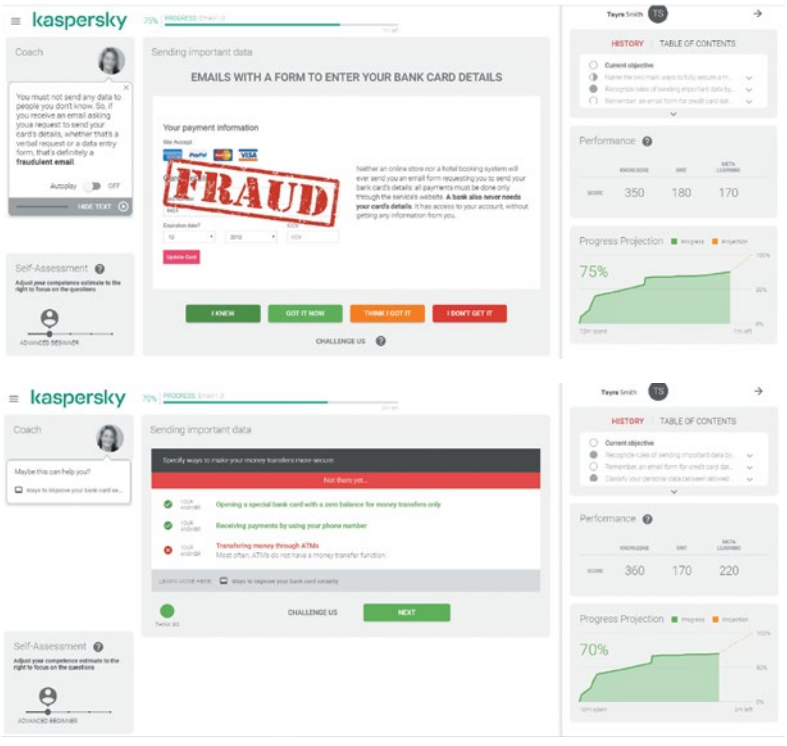
Als Teil einer innovativen adaptiven Lernmethode sorgt der kognitive Ansatz für eine personalisierte Lernerfahrung, die die Vorkenntnisse und Bedürfnisse jedes einzelnen Teilnehmers berücksichtigt.

Hauptvorteile

- **Adaptive Lernmethode ermöglicht** eine Form des persönlichen Einzelunterrichts
- **Darin werden unbewusste Inkompetenz aufgedeckt und behoben,** die Motivation zum Lernen und zu einem nachhaltigen Cybersicherheitsverhalten gefördert. Wenn man weiß, was man nicht weiß und woran man arbeiten muss, kann man Lücken schneller und effizienter schließen.
- **Kampfansage an Langeweile und Frust** dank eines persönlich zugeschnittenen Lehrplans Jede Lektion beginnt mit einer Frage, die nur dann zu einer theoretischen Erläuterung führt, wenn die Antwort es erfordert. Weiterbildung mit Fokus auf realen Problemen bindet den Teilnehmer ein und stärkt sein Interesse an der Cybersicherheit.
- **Dank lernfähiger Algorithmen wird die** automatische, gewohnheitsmäßige Anwendung der Fähigkeiten eingeübt, Teilnehmer schreiten im eigenen Lerntempo voran, wobei identische Themen bei Bedarf mit unterschiedlichen Ansätzen vermittelt und die Fortschritte des Teilnehmenden ständig überprüft werden. Kompetenzlücken werden geschlossen und umfassendere Kenntnisse schnell und effektiv aufgebaut. Bei einem hohen Kompetenzniveau wird bestimmtes Wissen zur Gewohnheit, Handlungen werden automatisch und ohne Nachdenken durchgeführt, regelmäßig verstärkt durch „Auffrischungsübungen", wenn die Gefahr besteht, dass das Gelernte wieder in Vergessenheit gerät.

Nachverfolgung der Ergebnisse

Der Fortschritt einzelner Mitarbeiter kann anhand umfassender Statistiken verfolgt werden: Leistungsübersichten und Berichte für Gruppen und Einzelpersonen. Der Administrator kann Mitarbeiter mit hoher Leistung und solche erkennen, die zusätzliches Coaching benötigen. Darüber hinaus gibt es Berichte zu Fortschritten des Nutzers, der Klassen, Details der Aufgabenverteilung mit detaillierter Analyse von Kompetenz und Metaverständnis der Teilnehmer.



Lernen

Unsere Online-Lernplattformen sind das Herzstück des Awareness-Programms. Sie vermitteln **mehr als 300 Fähigkeiten und Fertigkeiten im Bereich Cybersicherheit**, die alle wichtigen IT-Sicherheitsthemen abdecken, wie Passwörter u. Konten, E-Mail-Sicherheit, Soziale Netzwerke u. Messenger-Dienste, PC-Sicherheit, DSGVO etc.

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.

Im Sinne der maximalen Effizienz nutzen wir anpassbare Technologien und automatisierte Lernpfade, wobei berücksichtigt wird, welchen Wissensstand jeder Teilnehmer zu Anfang hatte und welcher angestrebt wird (der Wissenstand am Ende hängt von der Rolle ab, die der jeweilige Teilnehmer im Unternehmen wahrnimmt). Wir arbeiten mit praktischen Beispielen, vielen Erläuterungen, WARUM etwas wichtig ist, sowie zahlreichen unmittelbaren Assessments zu den Aktivitäten der Nutzer.

„Unwissenheit erzeugt viel häufiger Selbstvertrauen als Wissen."
Charles Darwin, „Die Abstammung des Menschen"

In KAOT behandelte Themen:
Passwörter
- E-Mail-Sicherheit
- Surfen im Internet
- Soziale Netzwerke und Messenger
- PC-Sicherheit
- Mobile Geräte
- DSGVO

KAOT ist für folgende Sprachen verfügbar: Englisch, Deutsch, Italienisch, Französisch, Spanisch, Arabisch, Russisch.

Weitere Informationen: kaspersky.com/kaot

Kaspersky Automated Security Awareness Platform: ein benutzerfreundliches Online-Tool, mit dem sich Ihre Mitarbeiter Stufe für Stufe im Bereich Cybersicherheit weiterqualifizieren können.

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

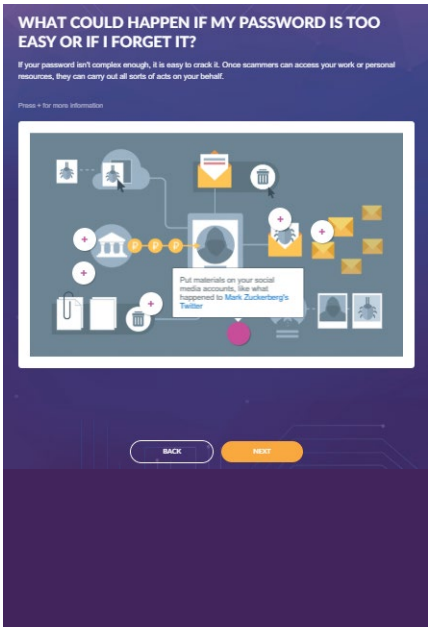
Die Schulung ist ideal für kleine und mittelständische Unternehmen, insbesondere solche ohne eigenen Ressourcen für die Verwaltung von Schulungsprogrammen.

Hauptvorteile:

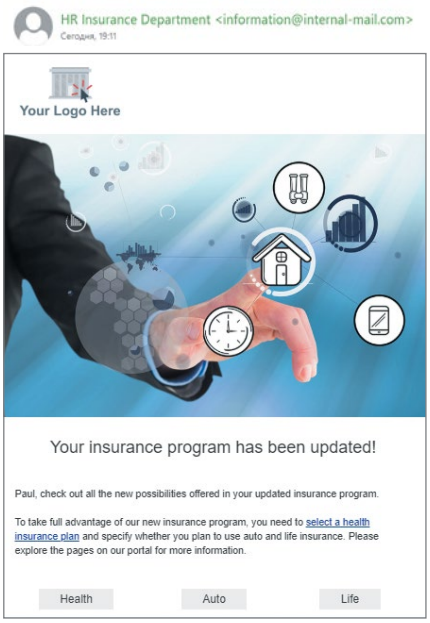
- **Benutzerfreundlich dank kompletter Automatisierung:** Das Programm lässt sich sehr einfach starten, konfigurieren und überwachen, wobei das Management im Verlauf vollständig automatisiert ist und kein Eingreifen durch den Administrator erfordert. Die Plattform erstellt eigenständig für jede Mitarbeitergruppe 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 Lizenzmodell** (für Managed Service Provider): Das anwenderbasierte Lizenzmodell ist bereits ab 5 Lizenzen erhältlich.

Jedes Thema umfasst verschiedene Levels und bietet jeweils spezifische Kenntnisse im Bereich Sicherheit. Die Levels sind je nach dem Grad des Risikos definiert, das vermieden werden soll: Level 1 bezieht sich auf das korrekte Verhalten im Fall von einfachen oder massenhaften Angriffen. In höheren Levels soll ein Sicherheitsbewusstsein für besonders raffinierte und zielgerichtete Angriffe aufgebaut werden.

Interaktive Lektionen



Simulierte Phishing-Angriffe



Nachverfolgung der Ergebnisse

Über das Dashboard können Sie die Fortschritte der Mitarbeiter, aber auch sämtlicher Gruppen bis hin zum gesamten Unternehmen verfolgen und auswerten. Weitere Details bis hin zu einer individuellen Ebene sind ebenfalls zugänglich.

Automatisierter Lernpfad, damit einmal Gelerntes nicht wieder in Vergessenheit gerät

In ASAP behandelte Themen:
Passwörter und Konten
- E-Mail-Sicherheit
- Surfen im Internet
- Soziale Netzwerke und Messenger
- PC-Sicherheit
- Mobile Geräte
- Schutz vertraulicher Daten
- DSGVO

Kaspersky ASAP ist eine mehrsprachige Lösung, die derzeit auf Englisch, Deutsch, Italienisch, Französisch, Spanisch, Russisch, Arabisch, Portugiesisch, Niederländisch, Tschechisch, Polnisch, Kasachisch, Slowenisch, Rumänisch, Türkisch und Ungarisch* verfügbar ist.

ASAP eignet sich ideal für MSPs und xSPs – Schulungs-Services für mehrere Unternehmen lassen sich über ein einziges Konto verwalten und Lizenzen können auf Basis monatlicher Abonnements gekauft werden.

Testen Sie eine voll funktionsfähige Variante von Kaspersky ASAP unter asap.kaspersky.com/de und erleben Sie, wie einfach sich ein Schulungsprogramm für Cybersicherheits-Bewusstsein in Ihrem Unternehmen einrichten und verwalten lässt.

Einbindung/ Motivation

Ausgangs-Niveau

Lernen

Fortschrittliche Lernmethode

Festigung des Gelernten

Advanced

Die meisten Unternehmen bieten zwei verschiedene Ausbildungsstufen zum Thema Cybersicherheit an: eine Expertenschulung für IT-Sicherheitsteams und eine Schulung zum Sicherheitsbewusstsein für Mitarbeiter, die nicht im IT-Bereich arbeiten (Kaspersky bietet ein umfassendes Produktpaket für beide Gruppen). Was fehlt also? IT-Teams, Service Desks und andere technisch ausgebildete Mitarbeiter. Standardmäßige Programme zur Verbesserung des Cybersicherheits-Bewusstseins reichen für sie nicht aus. Unternehmen müssen diese Mitarbeiter aber trotzdem nicht zu Cybersicherheitsexperten ausbilden:

Die CITO-Schulung erfolgt zu 100 % online – die Teilnehmer benötigen lediglich eine Internetverbindung mit Zugang zur Lernplattform (LMS) des Unternehmens und einen Chrome-Browser.

Jedes der 4 Module besteht aus einem kurzen theoretischen Überblick, praktischen Tipps sowie 4 bis 10 Übungen. Mit jeder dieser Übungen wird demonstriert, wie IT-Sicherheitstools und -Software bei der täglichen Arbeit genutzt werden sollten.

In der KIC-Schulung werden Ihrem Krisenteam folgende Inhalte vermittelt:

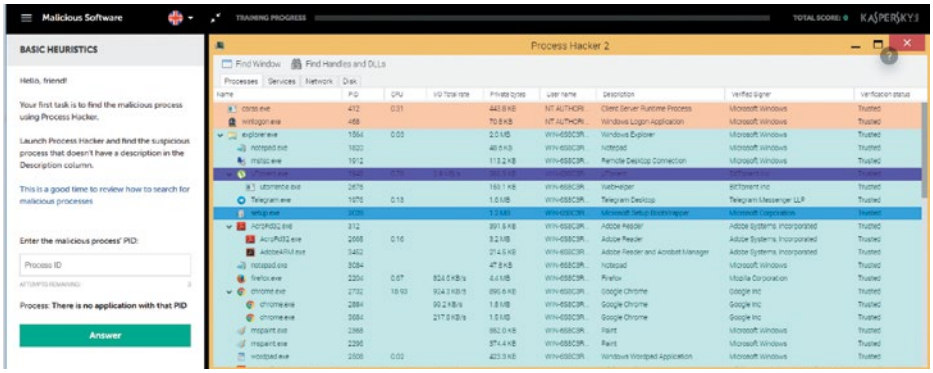
- Kenntnisse über die Cyberbedrohungen, die auf Sie zukommen
- Abschätzen der potentiellen Folgen
- Effektive Koordinierung mit dem IT-Sicherheitsteam
- Praktische Erfahrung mittels Simulation von Cybervorfällen
- Weiß, worauf es in der internen und externen Kommunikation nach einem Cyberangriff ankommt
- Aktualisiert und implementiert Ihren Kommunikationsplan für Cyberkrisen

Cybersecurity for IT Online: Abwehr an vorderster Front

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

Das Programm vermittelt IT-Experten praktische Fähigkeiten, um einen möglichen Angriff unter vermeintlich harmlosen PC-Vorfällen zu erkennen und Vorfallsdaten zur Übergabe an die IT-Sicherheitsabteilung zu erfassen. Außerdem wird der Spaß am Erkennen von Warnsignalen gefördert und damit die Rolle aller IT-Mitarbeiter als erste Verteidigungslinie gefestigt. Die Schulung besteht aus vier Modulen: Schadsoftware, potenziell unerwünschte Programme und Dateien, Grundlagen der Untersuchung sowie Vorfallsreaktion bei Phishing-Angriffen.

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.



Kaspersky Incident Communications: Versetzt Ihr Team für Unternehmenskommunikation in die Lage, auf einen Cyberangriff angemessen zu reagieren.

Sobald ein Cybervorfall entdeckt wird, zählt jede Maßnahme. Ihre externe und interne Kommunikation ist von entscheidender Bedeutung – vor allem dann, wenn Sie es mit unbekannten Angriffsvektoren und APTs (Advanced Persistent Threats) zu tun haben.

Im Rahmen von Kaspersky Incident Communications werden Mitarbeiter der Führungsetagen, aber auch Fachleute aus den Bereichen Informationssicherheit und Unternehmenskommunikation im Umgang mit Krisenkommunikation geschult, wie z. B. in der Erstellung und Anwendung geeigneter Ressourcen. Die Schulung fördert ein starkes Zusammengehörigkeitsgefühl unter den Mitgliedern des Krisenteams und vermittelt Kompetenzen wie die Vorbereitung eines Krisenkommunikationsplans, die Zusammenstellung praktischer Empfehlungen und Verfahren zur Betriebssicherheit sowie Tools zur Verschlüsselung der Kommunikation während eines Cybervorfalls zur Aufrechterhaltung der Geschäftskontinuität.

Einbindung/ Motivation

Ausgangs-Niveau

Lernen

Festigung des Gelernten

Festigung des Gelernten

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

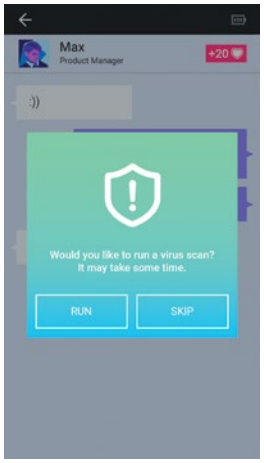
[Dis]connected – Modul für entspanntes, unterhaltsames Lernen

[Dis]Connected ist ein sehr 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.

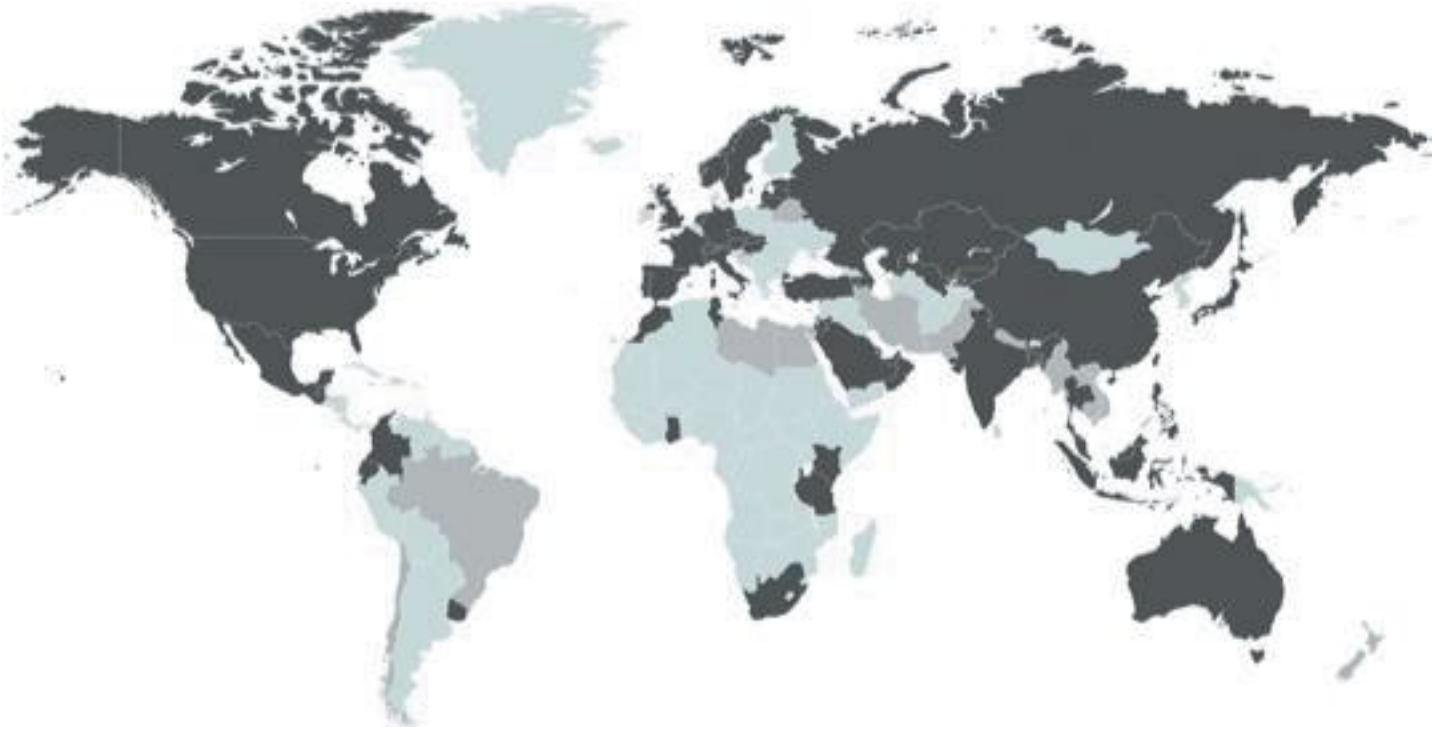
In den Ablauf sind Fragen der Cybersicherheit eingeflochten, die zeigen, wie unsere Entscheidungen in Bezug auf die Cybersicherheit geeignet sind, diese Ziele zu erreichen – oder ein erfolgreiches Ende zu verhindern. Insgesamt sind 18 Fälle zu lösen, mit Themen wie Passwörter und Konten, E-Mail, Surfen 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.



Kaspersky Security Awareness – weltweit



75
Länder

Mehr als 500.000
geschulte Mitarbeiter

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

www.kaspersky.de

kaspersky BRING ON THE FUTURE