Computerbasierte Schulungsprogramme für alle Unternehmensbereiche

2019

Kaspersky Security Awareness

kaspersky

Weitere Informationen finden Sie unter
kaspersky.de/awareness

Ein effektiver Weg zum Aufbau von Cybersicherheit im gesamten Unternehmen

Über 80 % aller Cybersicherheitsvorfälle sind auf menschliche Fehler zurückzuführen. Unternehmen verlieren Millionen durch die Wiederherstellung nach Vorfällen, an denen Mitarbeiter beteiligt waren. Herkömmliche Schulungsprogramme zur Vermeidung dieser Probleme sind jedoch oft nicht sonderlich effektiv. Oftmals gelingt es ihnen nicht, Mitarbeitern die gewünschten Verhaltensweisen und die erforderliche Motivation zu vermitteln.

Menschen bilden das schwächste Glied der Cybersicherheitskette:

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** räumen ein, dass sie die Anmeldedaten ihrer Arbeitscomputer an Kollegen weitergeben**

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

Die Lösung:
Machen Sie mithilfe von Schulungen menschliche Schwächen zu Stärken und bilden Sie so mit Ihren Mitarbeiter eine neue erste Verteidigungslinie.

Warum sind Kunden mit vorhandenen Schulungsprogrammen für das Sicherheitsbewusstsein nicht zufrieden?

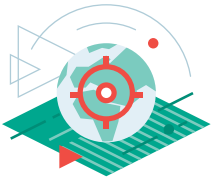
Mangel an Effizienz:
- Die Schulung wird von Teilnehmern als langweilig empfunden, orientiert sich nicht am Arbeitsalltag und das Augenmerk liegt eher auf Verboten als auf Lösungen.
- Zwischen Lesen und Zuhören fehlt die Praxis

Hoher Verwaltungsaufwand:
- Management und Steuerung des Schulungsvorgangs schwerfällig
- Mangel an Anreizen für Engagement und Motivation durch Mitarbeiter

* Studie: „The cost of a data breach", Kaspersky, Frühjahr 2018
** „Sorting out a Digital Clutter". Kaspersky, 2019

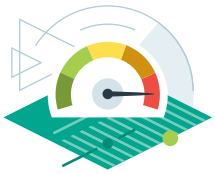
Kaspersky Security Awareness – ein neues Schulungskonzept

Wichtige Alleinstellungsmerkmale des Programms



Rollenbasierte, gezielte Schulungen
- Vermittlung von Fachwissen passend zu Rolle und Risikoprofil von Mitarbeitern
- Praxisnahe Beispiele und Fähigkeiten, die sich unmittelbar umsetzen lassen
- Lernen durch praktische Übungen

Auf natürliche Lernkapazität ausgelegt
- Die Schulungen sind genau passend auf natürliche Denkweisen ausgelegt
- Sichere Verhaltensweisen werden positiv und proaktiv vermittelt
- Einfach verständliche Informationen und Kompetenzen dank Methoden, die speziell auf das menschliche Gedächtnis ausgelegt wurden



Kontinuierliches Lernen in einzelnen Schritten
- Aufbau von leichteren zu komplexen Inhalten
- Fachwissen ausbauen und vorhandene Kenntnisse in neuen Zusammenhängen anwenden

Einfach zu verwalten und zu steuern
- Online
- Automatisiertes Schulungsmanagement
- Automatische Einladungs- und Motivation-E-Mails mit individuellen Empfehlungen für jeden Teilnehmer

Effektives Sicherheitsbewusstsein

Mitarbeiterschulungen auf allen Ebenen sind unerlässlich, um das Sicherheitsbewusstsein im ganzen Unternehmen zu erhöhen und alle Mitarbeiter zu motivieren, auch dann auf Cyberbedrohungen und die jeweiligen Abwehrmaßnahmen zu achten, wenn sie dies nicht als Teil ihrer eigentlichen Aufgaben sehen.

Fehler von Mitarbeitern sind in heutigen Unternehmen die häufigste Ursache für Vorfälle im Bereich Cybersicherheit.

Menschliches Versagen kann zur erheblichen Cyberbedrohung im Unternehmen werden, selbst bei Nutzung herkömmlicher Programme zur Verbesserung des Cybersicherheitsbewusstseins.

1 057 000 USD
je Unternehmen – durchschnittlicher finanzieller Schaden durch Datenschutzverletzungen aufgrund fehlerhafter Nutzung von IT-Ressourcen durch Mitarbeiter*

101 000 USD
je SMB – Finanzielle Folgen von Angriffen durch Phishing/Social Engineering **(1,3 Mio. je Unternehmen im Enterprise-Segment)****

Bis zu
400 USD
pro Mitarbeiter und Jahr – kosten allein Phishing-Angriffe im Durchschnitt***

Kaspersky Security Awareness Training

Die computerbasierten Schulungsprodukte von Kaspersky vermitteln Fachwissen im Bereich Cybersicherheit mithilfe bewährter Schulungsmethoden und -technologien. Das Konzept fördert ein optimales Anwenderverhalten und gewährleistet Cybersicherheit in allen Unternehmensbereichen.

Spezielle Schulungsformate passend für einzelne Unternehmensebenen

* Bericht: „On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives. Kaspersky, 2018

** Bericht „Human factor in IT security: How Employees are Making Businesses Vulnerable from Within", International, Juni 2017

***Die Berechnungen basieren auf der Veröffentlichung „Cost of Phishing and Value of Employee Training" des Ponemon Institute vom August 2015.

Beschreibung der Produkte für das Sicherheitsbewusstsein von Kaspersky

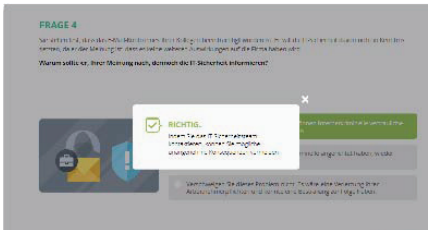
ASAP bietet einfach festzulegende Lernziele, ein ausgeglichenes, vorgefertigtes Schulungsprogramm, Praxisbezug sowie praktisch umsetzbare Berichte. Dadurch sorgen Sie für die Wertschätzung des Programms sowohl durch Mitarbeiter als auch die Führungsebene.

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 Verhaltensweisen im Fall von einfachen oder massenhaften Angriffen. Höhere Levels bauen ein Sicherheitsbewusstsein für besonders durchdachte und zielgerichtete Angriffe auf.

Die Plattform ist in 9 Sprachen verfügbar: Englisch, Deutsch, Italienisch, Französisch, Spanisch, Russisch, Arabisch, Portugiesisch und Niederländisch*.

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 Sicherheitsbewusstsein in Ihrem Unternehmen einrichten und verwalten lässt.



1. Kaspersky Automated Security Awareness Platform (ASAP)

Online-Schulungsprogramme nach einem neuen, umfassenden Konzept, das sich nicht nur auf die einfache Kommunikation von Fachwissen, sondern auch auf „Mustererkennung" stützt, sodass Mitarbeiter sich auch bei komplexen Bedrohungen sicher verhalten können.

Automatisiertes Schulungsmanagement

- Die Plattform kann innerhalb von nur 10 Minuten eingerichtet werden. Laden Sie einfach die Anwenderliste, unterteilen Sie die Anwender in Gruppen und legen Sie gemäß Risikostufe ein Ziel für jede Gruppe fest.
- Die Plattform erstellt dann eigenständig für jede Gruppe einen Schulungsplan. Die Schulung beinhaltet Intervall-Lernen mit laufenden Wiederholungen und wird automatisch über mehrere Schulungsformate bereitgestellt, einschließlich Lernmodule, E-Mails zur Wiederholung, Tests sowie simulierte Phishing-Angriffe.

Jederzeit verfügbare, praktisch umsetzbare Berichte

- Erfassen Sie jederzeit den Lernfortschritt der Teilnehmer im benutzerfreundlichen Dashboard mit Live-Tracking, Trends und Vorhersagen.
- Erhalten Sie Empfehlungen zur Optimierung der Ergebnisse
- Universeller Schulungsplan
- Das umfassende Angebot an Themen der Cybersicherheit eignet sich in Form verschiedener Levels sowohl für Anfänger als auch fortgeschrittene Anwender.

Hauptvorteile:

- **Einfachheit dank vollständiger 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.

- **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 eine verbesserte Aufnahme und spätere Anwendung der Kenntnisse.

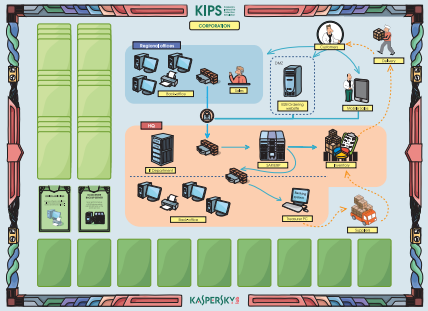
- **Flexibles Lizenzmodell:** Das anwenderbasierte Lizenzmodell ist bereits ab 5 Lizenzen erhältlich.

* Stand: Juli 2019

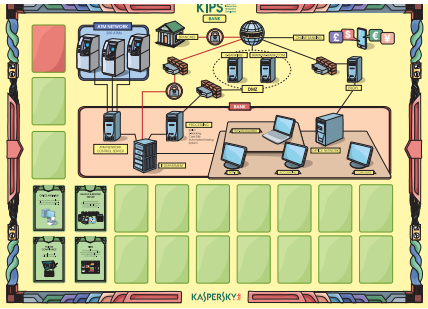
Die KIPS-Schulung richtet sich an Führungskräfte, Experten für Business-Systeme sowie IT-Experten, um deren Sicherheitsbewusstsein hinsichtlich der eigenen Risiken und Sicherheitsprobleme beim Betrieb moderner Computersysteme zu fördern.

KIPS – Beispielszenarien:

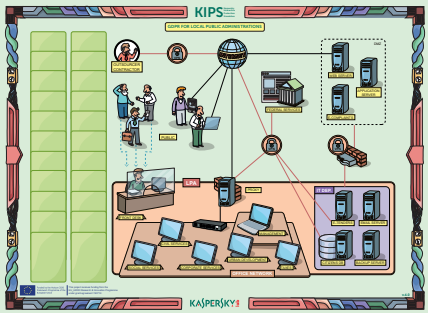
Unternehmen



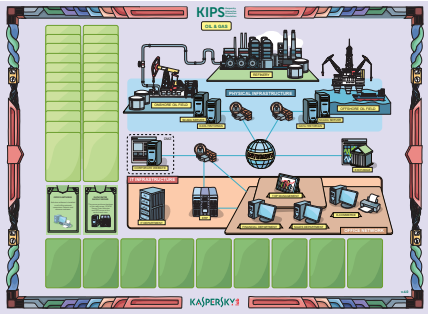
Bank



Lokale öffentliche Verwaltungen NEU



Öl & Gas



KIPS online:

- Ideal für Unternehmen mit weltweiten Standorten
- Gleichzeitige Nutzung durch bis zu 300 Teams
- Die Teams können die Spielschnittstelle in jeweils unterschiedlichen Sprachen nutzen
- Die Sitzungen werden durch einen Schulungsleiter über WebEx betreut

2. Kaspersky Interactive Protection Simulation (KIPS) fördert als Schulung strategische Entscheidungen sowie Kenntnisse

Was ist KIPS?

KIPS ist ein Team-Rollenspiel, in dem eine Unternehmensumgebung simuliert wird, in der die Teilnehmer mit zahlreichen unerwarteten Cyberbedrohungen umgehen und dabei Gewinne und Marktsicherheit optimieren müssen.

Die Idee besteht darin, durch Auswahl der besten verfügbaren, vorausschauenden und reaktionsschnellen Kontrollmöglichkeiten eine Cyberverteidigungsstrategie zu entwickeln.

KIPS ist besonders effektiv, denn es

- bietet einen modernen, leicht umsetzbaren Ansatz zur Sensibilisierung der Mitarbeiter,
- ist unterhaltsam, fesselnd und kompakt (2 Stunden),
- fördert durch Teamwork die Zusammenarbeit,
- baut durch Konkurrenz die Bereitschaft zur Initiative sowie analytische Kompetenzen auf und
- ermöglicht den Aufbau von Cybersicherheit und sicherem Verhalten und dessen Analyse durch Entdeckungen und Fehler in Form eines Spiels.

Das erwartet Sie bei KIPS:

- Machen Sie sich auf fortschrittliche Bedrohungen gefasst und erfahren Sie, wie Kriminelle technisch vorgehen (Threat Intelligence) und welche Ziele sie verfolgen.
- Erfahren Sie, wie Sie Vorfallsreaktion und Vorfallsprävention kombinieren.
- Testen Sie, was passiert, wenn Sie Ihre Sicherheitskontrollen nicht optimal konfigurieren.
- Halten Sie Ausschau nach gleichzeitigen Warnsignalen von Sicherheit, IT und Business.

Branchenbezogene Szenarien (als KIPS Live und KIPS Online in 10 Sprachen)

- **Unternehmen:** Schutz des Unternehmens, etwa vor Ransomware, APTs und Fehlern in der Automatisierungssicherheit
- **Bank:** Schutz von Finanzinstituten vor ausgefeilten APTs, die Geldautomaten, Verwaltungsserver und Geschäftssysteme angreifen
- **e-Government/Regierungsbehörden:** Schutz öffentlicher Webserver vor Angriffen und Exploits.
- **Kraftwerk/Wasserwerk:** Schutz industrieller Steuerungssysteme und wichtiger Infrastrukturen.
- **Transportwesen:** Schutz von Passagieren und Fracht vor Heartbleed, Ransomware und APTs.
- **Öl- und Gasindustrie:** Lernen Sie die Folgen zahlreicher Bedrohungen kennen – von Website Defacement über aktuelle Ransomware bis hin zu durchdachten APTs.

In den einzelnen Szenarien wird den Teilnehmern die Rolle der Cybersicherheit vor dem Hintergrund von Geschäftskontinuität und Rentabilität vermittelt. Dabei liegt das Hauptaugenmerk auf neu entstehenden Herausforderungen und Bedrohungen sowie gängigen Fehlern von Unternehmen beim Aufbau der eigenen Cybersicherheitsstrategie. Zudem wird die Zusammenarbeit zwischen Business- und Sicherheitsteams gestärkt, die einen soliden Betrieb und nachhaltigen Schutz vor Cyberbedrohungen fördert.

Cybersecurity IT-Training für Service Desk-Spezialisten, allgemeine IT-Sicherheit und lokale IT-Administratoren

Schulungsformat

Die 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 und zwischen 4 und 10 Übungen. Mit jeder dieser Übungen wird eine besondere Kompetenz erlernt und demonstriert, wie IT-Sicherheitstools und -Software bei der täglichen Arbeit genutzt werden sollten.

Die Schulung ist so angelegt, dass sie auf ein ganzes Jahr verteilt wird. Als Lerntempo wird eine Übung pro Woche empfohlen. Jede Übung nimmt etwa 5–45 Minuten in Anspruch.

3. Cybersecurity for IT Online

Diese interaktive Schulung für alle im IT-Bereich baut solide Kenntnisse der Cybersicherheit sowie Fähigkeiten zur ersten Vorfallsreaktion auf.

Für den Aufbau einer robusten Cybersicherheit im Unternehmen ist eine systematisch Schulung aller beteiligten Mitarbeiter erforderlich. In den meisten Unternehmen wird Cybersicherheit in Form von Schulungen auf zwei Ebenen vermittelt: Expertenschulungen für IT-Sicherheitsteams und Sicherheitsbewusstsein für Mitarbeiter außerhalb der IT. Keiner dieser Ansätze eignet sich für die zahlreichen IT-Mitarbeiter, die nicht direkt an der Sicherheit beteiligt sind und dennoch maßgebend zur Cybersicherheit im Unternehmen beitragen können.

Erste Gegenmaßnahmen bei Sicherheitsvorfällen

Kaspersky bietet eine umfassende Online-Schulung für IT-Facharbeiter in Unternehmen.

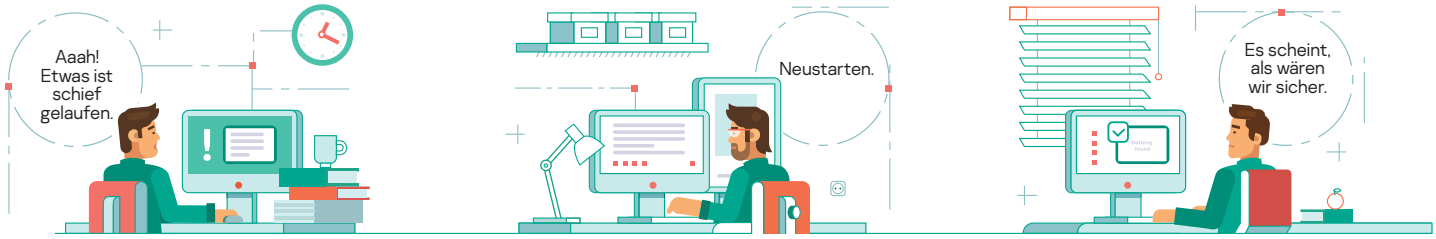
Der Kurs beinhaltet 4 Module:

- Schadsoftware
- Potenziell unerwünschte Programme und Dateien
- Grundlagen der Untersuchung
- Vorfallsreaktion bei Phishing-Angriffen

Mit dem Kurs erlangen IT-Experten praktische Fähigkeiten, einschließlich:

- Aufdecken möglicher Angriffsszenarios hinter vermeintlich harmlosen PC-Vorfällen
- Erfassen von Vorfallsdaten zum Übermitteln an die IT-Sicherheitsabteilung
- Erkennen von Anzeichen: Festigung der Rolle aller IT-Mitarbeiter als erste Verteidigungslinie

Aktuell:



Benutzer | IT-Support/Admins | IT-Sicherheit

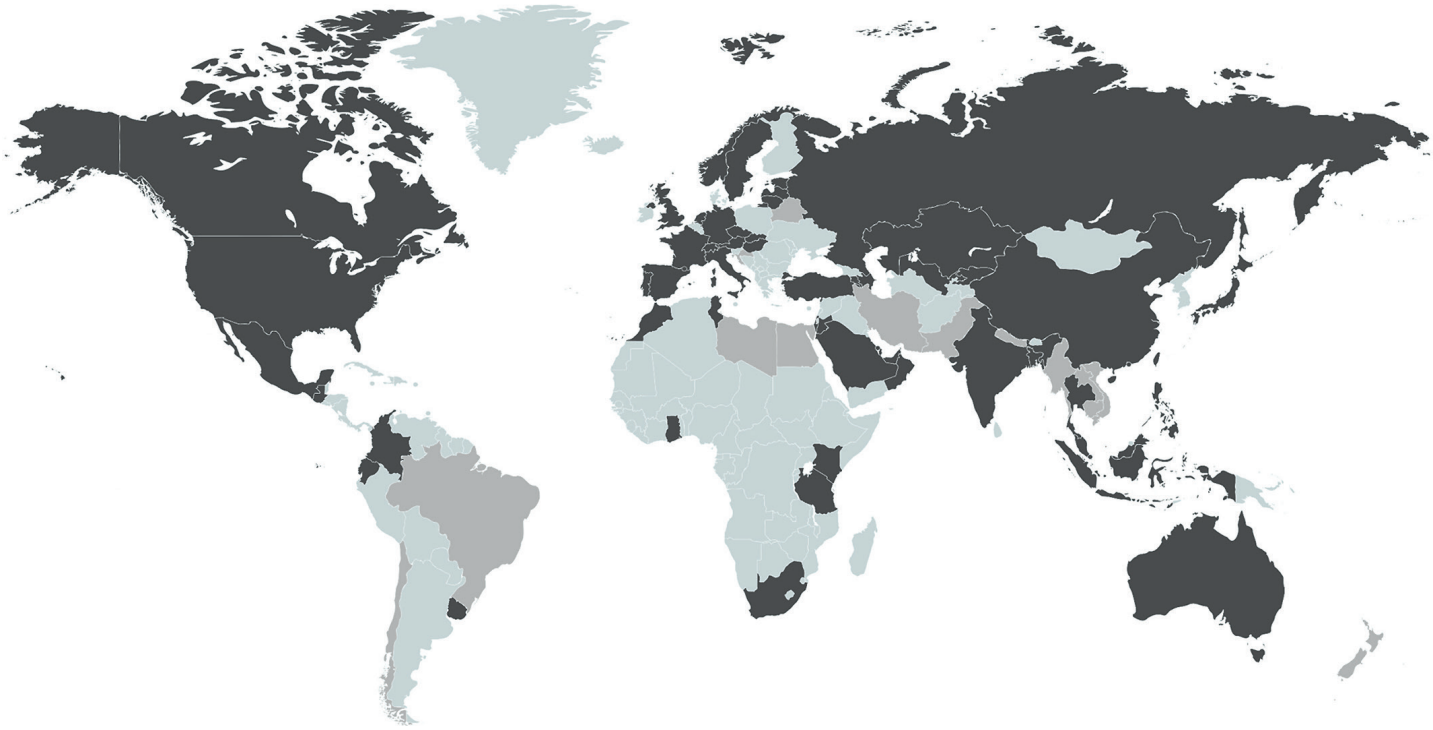
So sollte es sein:

Benutzer | IT-Support/Admins | IT-Sicherheit

75
Länder

250 000
geschulte Mitarbeiter

Kaspersky Security Awareness – weltweit



Stand: März 2019

Kommerzielle Nutzung oder wichtiges Event
An Online-Turnier teilgenommen

Mit mapchart.net erstellt

Cybersicherheit für Unternehmen: www.kaspersky.de/enterprise
Kaspersky Security Awareness www.kaspersky.de/awareness
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b

www.kaspersky.de

kaspersky BRING ON THE FUTURE