Weiterbilden, schützen und bestärken

Leitfaden zum Aufbau eines Cybersicherheits-bewusstseins unter Ihren Mitarbeitern

Kaspersky
Automated Security
Awareness Platform

kaspersky BRING ON THE FUTURE

Zur kostenlosen Testversion:
k-asap.com/de/

Das Überleben der eigenen Systeme sichern...

78 %[3]
der Unternehmen geben an, dass Mitarbeiter in den letzten 12 Monaten Daten aus Unwissenheit **gefährdet** haben

116 000 US-Dollar[4]
jährliche Kosten für KMUs wegen **unsachgemäßer IT-Nutzung**

3,92 Mio US-Dollar[5]
durchschnittliche **weltweite Kosten** einer einzigen Datenschutzverletzung

90 %[1] aller Cybersicherheitsvorfälle sind auf menschliches Versagen zurückzuführen.

Dank fortschrittlicher Phishing-Filter und Firewalls sind viele Organisationen mittlerweile besser geschützt. Damit stellen für Unternehmen heutzutage die eigenen Mitarbeiter das schwächste Glied in der Cybersicherheitskette dar. Sie sind der wesentliche Einfallspunkt in IT-Systeme: Mittlerweile ist menschliches Versagen für die Mehrzahl aller Cybervorfälle verantwortlich.

Ihre Organisation könnte durch einen einfachen Mangel an Sicherheitsbewusstsein erhebliche Umsatzeinbußen erleiden. Tatsächlich berichten 82 %[2] der Arbeitgeber von einem Mangel an Fachwissen im Bereich Cybersicherheit.

Wenn Sie jetzt in die Weiterbildung Ihrer Mitarbeiter investieren, um ihr Verhalten und ihre Einstellung zum Thema der Cybersicherheit zu ändern, schützen Sie damit Ihr Unternehmen und Ihre IT-Systeme. Mit der Kaspersky Automated Security Awareness Platform (ASAP) profitieren Sie von einem interaktiven, Computer-gestützten Schulungsprogramm, das die Zahl der von Menschen verursachten Cybervorfälle im Unternehmen signifikant reduziert.

... während Ihre Mitarbeiter als Sicherheitsfaktor überzeugen

Sicherheitsfaktor Mensch

In vielen Unternehmen gibt es großartige Technologien, aber die Menschen brauchen Kenntnisse im Bereich Cybersicherheit, um sie verantwortungsvoll nutzen zu können. Mit dem richtigen Schulungsangebot werden diese Kenntnisse vermittelt und neben dem Sicherheitsbewusstsein und der allgemeinen Haltung der Mitarbeiter wird auch die Arbeitskultur gestärkt.

Wie bei jeder anderen Weiterbildung auch wird der Lernerfolg allerdings beeinträchtigt, wenn die Kurse langatmig oder zu technisch sind. Schulungen zum Thema Sicherheitsbewusstsein sollten kontinuierlich stattfinden, eine klare Struktur aufweisen und in kleinere Abschnitte unterteilt sein, um das gewünschte Verhalten zu fördern und Mitarbeiter zu motivieren, echte Angriffe zu erkennen und zu melden.

Den Mitarbeiter als Sicherheitsfaktor zur stärken ist für jedes Unternehmen ein Gewinn. Gut ausgebildete Mitarbeiter führen zu weniger Sicherheitsvorfällen sowie optimierter Geschäftskontinuität und Effizienz für die gesamte Organisation.

1 Analyse der Berichte zu Datenschutzverletzungen, die der britischen Datenschutzbehörde (ICO) gemeldet wurden

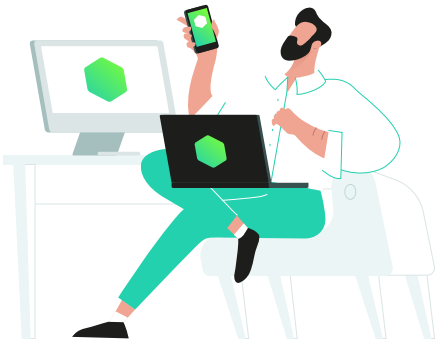
2 The Cybersecurity Workforce (2019), CSIS

3 Opinion Matters, Insider Data Breach Survey 2020

4 Kaspersky-Bericht zur Wirtschaftlichkeit der IT-Sicherheit, 2019

5 Cost of a Data Breach, Bericht von IBM, 2019

Arbeitsplätze sicherer machen



So überwindet das richtige Training Hindernisse

Anders als „gewöhnliche" Schulungsprogramme basiert Kaspersky ASAP auf mehr als 20 Jahren Erfahrung und unserem geballten Fachwissen im Bereich Cybersecurity. Wir wissen genau, über welche Fähigkeiten Mitarbeiter verfügen sollten, um sich sicher zu verhalten und das Unternehmen zu schützen. Und genau diese Themen fließen, unterteilt nach Themen und Wissensstand, direkt in die Schulungsinhalte ein. Damit erhalten Teilnehmer jeder Stufe umfassendes, aber auch interessantes Wissen, was hilft, eine Reihe von wichtigen Lernhindernissen auszuräumen:

Das Hindernis	Die Lösung
Schulungen sind langweilig	Wir lernen am Besten, wenn die Inhalte einen Bezug zu unseren täglichen Aufgaben haben. Ein Cybersecurity Training sollte sich daher direkt auf die vom Mitarbeiter genutzten Technologien und Online-Aktivitäten beziehen – und realistische, aktuelle Beispiele enthalten. Ähnliches gilt für die Lektionen und Tests, die die Mitarbeiter absolvieren. Sie sollten sich am echten Leben orientieren und nicht nur rein theoretisch sein. So wird die Motivation der Mitarbeiter gestärkt, nach dem Motto: Jetzt weiß ich, wie ich es richtig mache. Und schlussendlich wird der Lernprozess im Rahmen eines interaktiven Online-Trainings mit dauerhaften Zielen und sofort anwendbaren Fähigkeiten am Laufen gehalten.
Themen geraten schnell in Vergessenheit	Nach strikten Regeln oder Videos zu lernen, ist keine effektive Methode, um neues Wissen zu verinnerlichen. Daher macht sich Kaspersky ASAP moderne Prinzipien und Lernmethoden zunutze. Sie helfen die so genannte Vergessenskurve von Ebbinghaus zu überwinden, nach der die Erinnerung im Laufe der Zeit verblasst. Wiederholungsblöcke mit Kaspersky ASAP auf Basis von Wissenstests und Interaktion sind einprägsam und helfen beim Aufbau solider Fähigkeiten im Bereich der Cybersicherheit.
Schulungen sind nicht länderspezifisch	Großunternehmen erhalten mit Kaspersky ASAP durchgängige Lernpfade über die Landesgrenzen hinweg. Die visuelle Aufbereitung und die Texte werden nicht nur in verschiedene Sprachen übersetzt, sondern auch auf die jeweilige Kultur und die lokalen Gegebenheiten angepasst.
Schulung ist nicht umfassend	Zu den Themen der Kaspersky ASAP-Schulungen gehören Passwörter und Konten; E-Mails; Sufen im Internet; soziale Netzwerke und Messenger-Dienste; PC-Sicherheit und mobile Geräte; DSGVO und der Schutz vertraulicher Daten. Zu jedem Thema gibt einen eigenen Lernpfad mit unterschiedlichen Stufen vom Anfänger bis zum Fortgeschrittenen. Das Programm ist ideal geeignet für Unternehmen, die umfassend weiterbilden möchten, aber auch für solche, die nur bestimmte Themen herausgreifen und an die entsprechenden alltäglichen Arbeitsanforderungen anpassen möchten.
Der Lehrplan ist schwer zu verwalten	Das Schöne an einem automatisierten Onlinekurs ist, dass man den Umfang leichter steuern kann. Von den Einladungsmails an die Mitarbeiter über den zeitlichen Rahmen für die einzelnen Lektionen bis hin zum Berichtwesen mit Handlungsaufforderungen ist alles integriert und der kontinuierliche Lernfortschritt lässt sich völlig automatisch verwalten. Nutzer, die ein Risiko darstellen, Lektionen schwänzen oder Tests nicht bestehen, werden automatisch hervorgehoben, so dass der Administrator rechtzeitig aktiv werden kann.

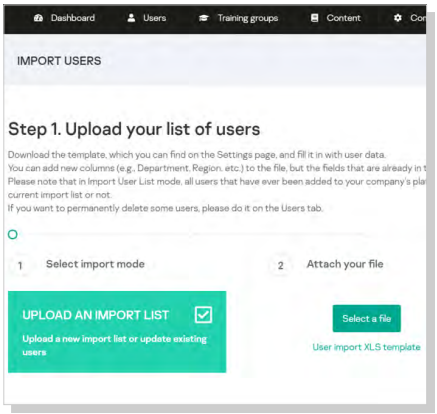
Stärkung des Sicherheitsfaktors Mensch

Automatisiert und einfach zu verwalten

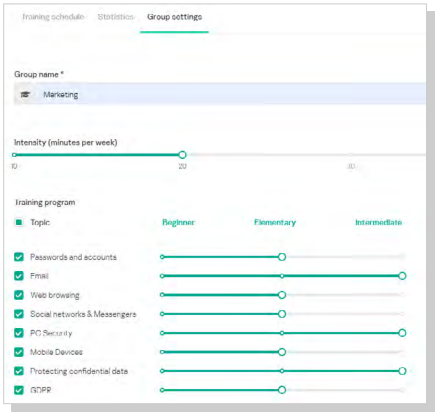
Kaspersky ASAP setzt im Bereich des Cybersecurity Trainings neue Maßstäbe. Damit können Sie ab sofort Online-Lernpfade nutzen, die interaktiv und interessant gestaltet sind.

In der Vergangenheit war es oft schwer, Lernfortschritte und -erfolge der einzelnen Teilnehmer zu messen. Mit dem automatisierten schrittweisen Lernprogramm von Kaspersky ASAP ist alles im Handumdrehen eingerichtet und vorbereitet. Sie können praktisch sofort loslegen und auch der Lehrplan ist komplett individuell steuerbar. So können Sie unterschiedliche Mitarbeiter für unterschiedliche Inhalte zum Thema Cybersicherheit einteilen; können Ziele definieren, automatische E-Mails und Empfehlungen einrichten und Berichte mit Handlungsanweisungen erzeugen.

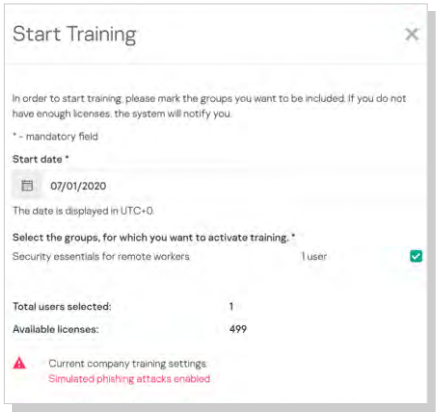
Hier ein Beispiel für die schnelle Automatisierung der Schulungsinhalte, mit denen Sie Ihre IT-Systeme und Ihre Organisation durch ein Mehr an Cybersicherheitsbewusstsein schützen:



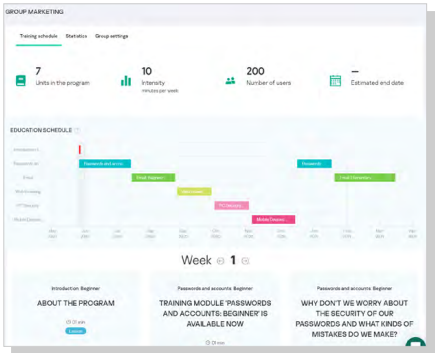
Teilnehmer hinzufügen
Starten Sie Ihr Awareness-Programm mit nur wenigen Klicks



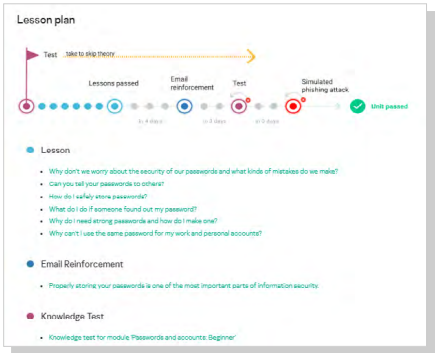
Risikostufen und Intensität des Programms wählen
Mitarbeiter werden entsprechend ihren Lernzielen in Gruppen zusammengefasst



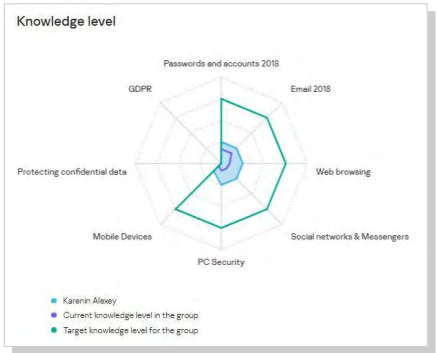
Schulungstermine festlegen
Eingabe eines Startdatums für jede Gruppe



Automatische Lehrplanerstellung
Der Lehrplan wird je nach Lernziel und Vorkenntnissen der Teilnehmer automatisch zusammengestellt



Unterscheidung nach Inhalt/Vorkenntnissen
In jeder Lerneinheit gibt es für jedes Thema unterschiedliche Darstellungsformen



Gruppenstatistik
Überprüfung des Lernfortschritts über eine einfache Oberfläche

Bestehen und wachsen: Beispiele für Fähigkeiten

Einige der mehr als 300 Fähigkeiten, die Ihre Mitarbeiter erwerben können

Passwortgebrauch

Mitarbeiter erstellen für alle Logins ähnlich klingende und vertraute Passwörter und ändern sie nur selten.	Mitarbeiter wissen, wie man Passwörter für persönliche und berufliche Ressourcen erstellt, die komplett unabhängig voneinander sind. Sie aktualisieren ihre Passwörter regelmäßig und wissen, wie man Password Manager verwendet. 

Falsche Informationen

Mitarbeiter erkennen gefälschte Domänen, Popup-Fenster oder andere manipulierte Inhalte nicht	Mitarbeiter erkennen ungültige Linkadressen von gefälschten Subdomänen und können anhand bestimmter Eigenschaften eine offizielle Seite oder ein legitimes Popup-Fenster unterscheiden. 

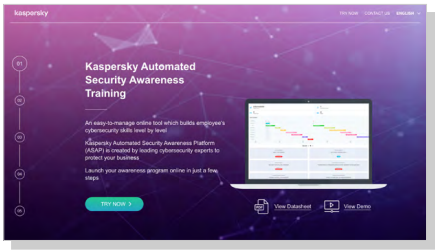
Inhalt der E-Mail

Mitarbeiter sind sich der möglichen Gefahren in Links und E-Mail-Anhängen nicht bewusst und überprüfen nicht die Absenderadressen.	Mitarbeiter sind in der Lage, Anhänge wie zum Beispiel Programmdateien in Nachrichten auf Risiken zu prüfen. Sie erkennen außerdem manipulative Ausdrücke in E-Mails, und ob sich der Absender nur der imitierten Form eines Namens bedient hat. 

Mobile Sicherheit

Mitarbeiter lassen ihre mobilen Geräte mit sensiblen Daten und beruflichen Anmeldedaten auf dem Tisch liegen und wissen nicht, wie man Malware auf Smartphones erkennt.	Mitarbeiter sperren Geräte bei Nichtgebrauch und wissen, wie man Malware auf Smartphones erkennt und vermeidet. Für wichtige Services wird eine Mehrfaktor-Authentifizierung eingerichtet. 

Der Mitarbeiter als Sicherheitsfaktor für Ihr Unternehmen



Starten Sie noch heute das Awareness Training mit der kostenlosen Testversion

Gehen Sie auf: k-asap.com/de

Man hat schon viel von Hackerangriffen gehört, aber eine richtige Schulung zu dem Thema hatten wir vorher nie. Mit dem Erwerb dieser Fähigkeiten bekommt man ein besseres Gefühl dafür, ob etwas gefälscht oder gefährlich ist.

Reservierungsmitarbeiter in der Tourismusbranche

Ein Cybersecurity Awareness Training sollte für den durchschnittlichen Anwender verständlich, interessant und benutzerfreundlich sein. Das ist bei der Lösung von Kaspersky durchweg der Fall. Hier gilt ganz klar die Devise: je einfacher desto besser.

Führungskraft im Bauwesen

Der Phishing-Kurs war sehr hilfreich und interessant. Diese Plattform zeigt uns, wo wir im Bereich Cybersicherheit noch Lücken haben, und man erfährt, wie man sich grundsätzlich verhalten muss, um nicht Opfer eines Cyberangriffs oder eines Virus zu werden.

IT-Berater im Einzelhandel

Ich habe erst zwei Lektionen zum Thema Cybersicherheit durchgearbeitet und habe schon das Gefühl, dass ich beim Arbeiten verantwortungsvoller geworden bin. Die Schulung lässt sich angenehm absolvieren, weil sie in kleinere Abschnitte unterteilt ist.

Buchhalter im Marketing

Ich finde die automatischen Einladungen und E-Mails toll, die man vom Schulungsmodul erhält. Sie helfen mir, am Ball zu bleiben. Ich lerne das, was ich wissen muss, und das hilft mir ganz speziell für meinen Job.

Verkäufer im Einzelhandel

Wir hatten Probleme, eine Schulung zu entwickeln, die als Frontalunterricht wirklich funktionierte. Das automatisierte Training mit Kaspersky war da effektiver und bereits nach 6 Monaten wurden weitaus weniger Cybervorfälle gemeldet.

HR Director in der Fertigungsindustrie

Kostenlose Testversion von Kaspersky ASAP: k-asap.com/de/
IT Security News: www.kaspersky.de/blog/category/business/

kaspersky BRING ON THE FUTURE

www.kaspersky.de