Motivierend
für Mitarbeiter,
effizient für
Manager.

Zur kostenlosen
Testversion
k-asap.com/de

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky bring on the future

Kaspersky
Automated Security
Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

82 % aller Cybersicherheitsvorfälle gehen auf menschliche Fehler zurück und kosten Unternehmen Millionen. Konventionelle Trainingsprogramme sind nicht für dieses Problem geeignet. Ein neuer Ansatz ist erforderlich. Die Lösung: Kaspersky ASAP.

Menschliche Fehler sind das größte Risiko für Cybersicherheit

79 %
der Mitarbeiter
geben zu, dass sie im vergangenen Jahr mindestens eine riskante Aktivität ausgeübt haben, obwohl sie sich der Risiken bewusst waren.*

51 %
der Mitarbeiter
sind der Ansicht, dass ihre IT-Abteilung die volle Verantwortung dafür trägt, dass ihre Arbeitgeber nicht Opfer von Cyberangriffen werden*

55 %
der Unternehmen
berichten von Bedrohungen durch unsachgemäße IT-Nutzung ihrer Mitarbeiter**

51 %
der kleinen Unternehmen
erlitten infolge der Verletzung von IT-Sicherheitsrichtlinien durch Mitarbeiter einen Sicherheitsvorfall**

26 %
der Mitarbeiter
geben an, dass sie für ihre privaten E-Mails dasselbe Passwort nutzen wie für ihr berufliches E-Mail-Konto***

Schwierigkeiten bei der Umsetzung eines funktionierenden Cybersicherheitsprogramms

Unternehmen sehen zwar den Nutzen von Programmen für mehr Sicherheitsbewusstsein, sie sind jedoch häufig mit dem Ablauf und den Ergebnissen nicht zufrieden. Gerade für kleine und mittlere Unternehmen, die in der Regel nicht über die nötige Erfahrung oder die erforderlichen Ressourcen verfügen, stellt das eine große Herausforderung dar.

Ineffizient für Teilnehmer

Wird als kompliziert, langweilig und irrelevant wahrgenommen.

Das Hauptaugenmerk liegt eher auf Verboten als auf Lösungen

Man behält das Gelernte nicht in Erinnerung

Zwischen Lesen und Zuhören fehlt die Praxis

Eine Belastung für Administratoren

Wie erstellt man ein Programm und legt Lernziele fest?

Wie verwaltet man Schulungsaufgaben?

Wie kontrolliert man den Erfolg?

Wie stellen wir sicher, dass sich unsere Mitarbeiter voll engagieren?

* Balancing Risk, Productivity, and Security. Delinea, 2021

** „IT Security Economics 2022", Kaspersky

*** https://www.beyondidentity.com/blog/password-sharing-work

Effiziente, einfach zu verwaltende Schulungen für Unternehmen jeder Größe

Wir stellen vor: Kaspersky ASAP, die Automated Security Awareness Platform, das Kernstück des Trainingsportfolios für Sicherheitsbewusstsein von Kaspersky. ASAP ist ein Online-Tool, das Mitarbeiter das ganze Jahr über in puncto Cybersicherheit sensibilisiert. So kann die **Anzahl der Cybervorfälle, die durch Mitarbeiter verursacht werden, nachhaltig reduziert werden.**

Zur Implementierung und Verwaltung der Plattform sind keine speziellen Ressourcen oder Vorbereitungen erforderlich. Darüber hinaus bietet sie in jeder Lernphase integrierten Support auf dem Weg zu einer sicheren Cyberumgebung im Unternehmen.

Relevante Inhalte, die man nicht ignorieren kann

Eines der wichtigsten Kriterien bei der Auswahl eines Awareness-Programms ist dessen Effizienz, und bei ASAP ist Effizienz fester Bestandteil der Schulungsinhalte und der Verwaltung. Die Inhalte basieren auf **über 25 Jahren Erfahrung im Bereich Cybersicherheit**. Diese sind in ein Schulungsmodell mit über **350 praktischen und unverzichtbaren Grundkompetenzen** eingeflossen.

Sensibilisieren Sie Ihr Team für das Thema Cyber-Sicherheit.
Schützen Sie Ihr Unternehmen und Ihre IT-Systeme, indem Sie die Einstellung und das Verhalten Ihrer Mitarbeiter und Mitarbeiterinnen ändern.

Effiziente Schulung

Konsistent	– Gut durchdachte, strukturierte Inhalte – Interaktive Lektionen, laufende Festigung der Kenntnisse, Tests, simulierte Phishing-Angriffe zur praxisorientierten Anwendung der Kenntnisse Inhalte und Struktur des Schulungsmaterials orientieren sich an der Funktionsweise des menschlichen Gedächtnisses und wie wir Informationen aufnehmen und behalten.
Praxisnah und ansprechend	– Relevanz im Arbeitsalltag von Mitarbeitern – Direkt anwendbare Fähigkeiten Beispiele aus dem echten Leben, mit denen sich die Mitarbeiter persönlich identifizieren können, tragen dazu bei, dass sich die Lernenden stärker engagieren und die Informationen besser behalten.
Positiv	– Sichere Verhaltensweisen werden positiv vermittelt – Der Fokus liegt auf dem „Warum“ und „Wie“ anstatt auf Verboten Zu viele Regeln und Verbote führen zu Unzufriedenheit und Desinteresse. Dagegen tragen Erklärungen und Regeln, die an menschliche Denkmuster angepasst sind, ganz natürlich zu Akzeptanz und Verhaltensänderung bei.

Einfache Verwaltung

Einfaches Management	– Durch ein vollständig automatisiertes Schulungsmanagement erlangen Mitarbeiter die für ihr Risikoprofil erforderlichen Kenntnisse, ohne dass der Administrator der Plattform eingreifen muss – Synchronisierung mit AD (Active Directory), SSO (Single Sign-On), Open API (die Möglichkeit, mit Lösungen von Drittanbietern zu interagieren), Online-Onboarding beim ersten Besuch, ein FAQ-Bereich und Tipps erleichtern die Plattformverwaltung und machen sie besonders effizient.
Benutzerfreundliche Steuerung	Umfassendes, zentrales Dashboard und praktisch umsetzbare Berichte: – Bericht über den Fortschritt bei den Lektionen – Berichte über Tests und simulierte Phishing-Angriffe
Ansprechendes Konzept	Die Plattform versendet automatisch Einladungen und Erinnerungen sowie Berichte an Teilnehmer und Administratoren.

Bereitstellungsoptionen

Kaspersky ASAP kann je nach Bedarf in drei verschiedenen Versionen gebucht werden:

- **Komplette in der Cloud bereitgestellte Online-Lösung:** In diesem Fall erfolgt der Umgang mit den Nutzerdaten in voller Übereinstimmung mit den gesetzlichen Vorschriften, die am Standort des gewählten Servers gelten. Wenn Sie sich beispielsweise für Europa entscheiden, werden die Daten in der Europäischen Union (in Frankfurt, Deutschland) gespeichert und alle gesetzlich geschützten Daten werden in Übereinstimmung mit der Datenschutzgrundverordnung (DSGVO) der Europäischen Union verarbeitet.
- **Inhalte im SCORM-Paket:** Mit dieser Option lassen sich die Schulungsmodule in Ihr internes LMS (Learning Management System) integrieren. Bitte beachten Sie, dass Tests oder simulierte Phishing-Angriffe in dieser Option nicht enthalten sind.
- **On-Premise:** Diese Option wurde für Kunden entwickelt, die ein besonders hohes Maß an Vertraulichkeit einhalten müssen. Bei Unternehmen, die aufgrund rechtlicher Vorschriften Einschränkungen unterliegen, sorgt die lokale Bereitstellung für die Einhaltung dieser Vorgaben. Die Schulungsunterlagen werden im Kundennetzwerk bereitgestellt. Sie haben dabei die volle Kontrolle über die Serverhardware, Datensicherheit und Konfiguration. Um auf die Schulungsmaterialien zuzugreifen, ist noch nicht einmal eine Internetverbindung erforderlich.

ASAP-Verwaltung: Einfach & vollständig automatisiert

Programmstart in vier einfachen Schritten

1

Hinzufügen von Nutzern

Einfach per **AD-Synchronisierung** oder in einer xlsx-Datei hochladen bzw. manuell hinzufügen

2

Nutzeraufteilung in Gruppen

Teilen Sie Benutzer entweder manuell oder anhand von Regeln in Zielgruppen auf

3

Schulung starten

Nutzer können manuell oder anhand von Regeln in Zielgruppen aufgeteilt und für jede dieser Gruppen Starttermine festgelegt werden

4

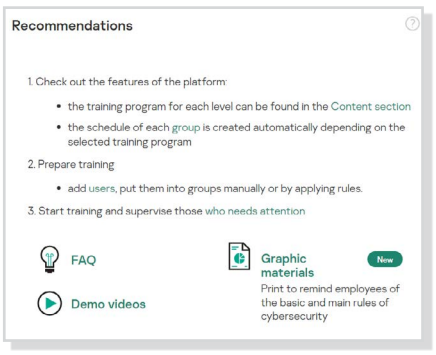
Automatisiertes Schulungsmanagement über ASAP

Auf der ASAP-Plattform wird für jede Gruppe, für Einladungen, Erinnerungen und andere Mitteilungen ein Zeitplan erstellt – und zwar vollautomatisch

Ein neuer und optimierter Trainingsansatz

Kaspersky ASAP verändert die Art und Weise, wie wir Lerninhalte zur Cybersicherheit vermitteln. Jetzt können Sie wählen, ob Sie Ihren Mitarbeitern einen Express-Kurs zuweisen, der Ihnen hilft, die gesetzlichen Anforderungen für Cybersicherheitsschulungen schnell zu erfüllen oder ihr Wissen aufzufrischen, oder ob Sie sich für den Hauptkurs entscheiden, der nach Komplexitätsstufen unterteilt ist.

Onboarding bei der ersten Anmeldung, Empfehlungen, FAQ und Demo-Videos, die zeigen, wie die Plattform für Administratoren oder Nutzer funktioniert – alles, was Sie zum Einstieg brauchen, finden Sie auf der Administrator-Homepage



Behandelte Themen

Behandelte Themen

Hauptkurs	Schnellkurs
E-Mail	E-Mail
Passwörter und Zugänge	Passwörter und Zugänge
Websites und das Internet	Websites und das Internet
Social Media & Messenger	Sicherheit für mobile Geräte
PC-Sicherheit	Social Media
Mobile Geräte	Mein Computer
Schutz vertraulicher Daten	Schutz vertraulicher Daten
Personenbezogene Daten	Doxing
DSGVO	Sicherheit von Kryptowährungen
Industrial Cybersecurity	Informationssicherheit bei Remote Arbeit
Sicherheit von Bankkarten und Datensicherungsstandard für Kreditkartentransaktionen (PCI DDS)	Föderales Gesetz 152-FZ (für Russland)
Physische Datensicherheit	Föderales Gesetz FZ-187 (über die Sicherheit kritischer IT-Infrastruktur in Russland)

Die Themen sind in große Blöcke unterteilt, die zahlreiche IT-Sicherheitskonzepte abdecken.*

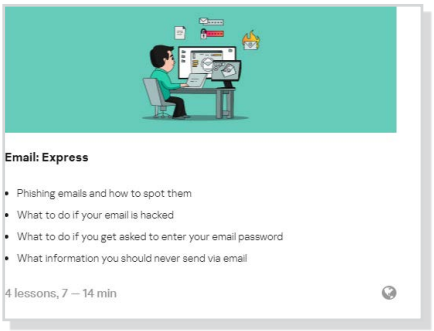
#Passwörter #Phishing #Firmenkonten #Gefährliche Nachrichten #Bankkarten #Ransomware #SocialEngineering #Gefährliche Dateien #Arbeiten mit Browsern #Unternehmensethik #Antivirus #Schadsoftware #Programme #Browser #Vertrauliche Informationen #Informationen speichern #Informationen versenden #Persönliche Daten #Internet und das Gesetz #Europäische Gesetzgebung #Business #Gefährliche Links #Gefälschte Webseiten #Ransomware-Seiten #Datensicherung #Mobile Daten #Verschlüsselung #Cloud-Dienste #Industriespionage #PCI DSS #Zwei-Faktor-Authentifizierung #Digitaler Fußabdruck #Torrents #Catfishing #Gezielte Angriffe #Hashing #Tokens #Pattern Locks #Mining #Kindersicherung

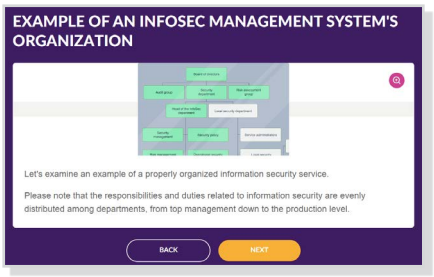
* Die aktuelle Liste der Themen und Konzepte finden Sie unter k-asap.com/de

Jedes Thema besteht aus verschiedenen Levels und bietet jeweils spezifische Kenntnisse im Bereich Sicherheit. Die Stufen sind nach dem potentiellen Risiko definiert, das sie einzudämmen helfen. So reicht Stufe 1 in der Regel aus, um sich vor sehr einfachen oder Massenangriffen zu schützen. Auf den höheren Stufen geht es um den Schutz vor besonders raffinierten und zielgerichteten Angriffen.

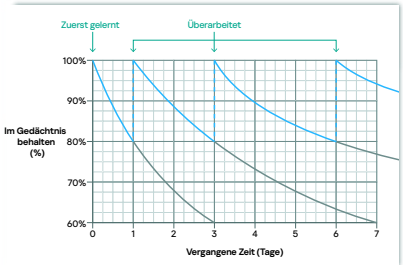
Beispiel: Vermittelte Kompetenzen im Bereich „Websites und Internet“

Einsteiger Vermeiden von Massenangriffen (diese sind kosteneffizient und einfach umzusetzen)	**Basis** Vermeiden von Massenangriffen auf ein bestimmtes Profil	**Mittleres Niveau** Vermeiden von gut vorbereiteten, gezielten Angriffen	**Fortgeschritten*** Vermeiden von zielgerichteten Angriffen
23 Fähigkeiten, einschließlich: – Erkennen gefälschter Pop-ups – Sensibilisierung bei Weiterleitungen – echte Download-Links von gefälschten unterscheiden – ausführbare Dateien aus dem Internet erkennen – Feststellen, ob eine Browsererweiterung echt ist	**34 Fähigkeiten, einschließlich:** – Daten nur auf Websites mit einem gültigen SSL-Zertifikat eingeben – unterschiedliche Passwörter für verschiedene Registrierungen benutzen – Anzeichen für gefälschte Webseiten erkennen – numerische Links vermeiden – ungültige Netzwerkadressen mit gefälschten Subdomains erkennen	**12 Fähigkeiten, einschließlich:** – Freigabelinks vor dem Senden prüfen – für Torrents nur Software von vertrauenswürdigen Herstellern verwenden – legale Inhalte nur von Torrents herunterladen – Browser-Cookies regelmäßig löschen	**13 Fähigkeiten, einschließlich:** – Erkennen raffiniert gefälschter Links (einschließlich Links, die wie Ihre Unternehmens-Websites aussehen, und Links mit Weiterleitungen) – Prüfen von Websites mit speziellen Dienstprogrammen – Erkennen, ob der Browser Mining betreibt – Vermeiden gefälschter SEO-Webseiten
	+ Vertiefung grundlegender Fähigkeiten	+ Vertiefung der bisher erlernten Fähigkeiten	+ Vertiefung der bisher erlernten Fähigkeiten





Die Vergessenskurve nach Ebbinghaus



ASAP Express-Kurs

Eine Kurzfassung der Schulung in audiovisuellem Format. Zu jedem Thema aus dem Bereich Cybersicherheit gibt es mehrere kurze Lektionen, in denen grundlegende Kompetenzen vermittelt werden.

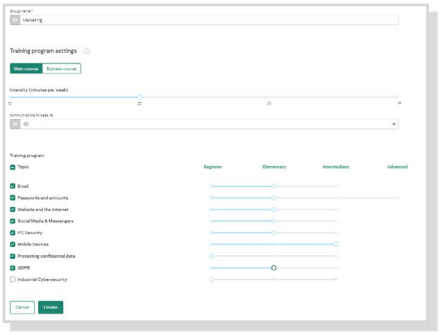
- Interaktive Theorie
- Videos
- Tests

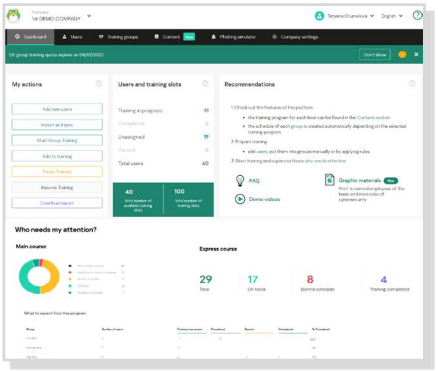
Simulierte Phishing-Angriffe sind nicht Teil des Lernpfades, können aber separat vom Administrator zugewiesen werden.

ASAP-Hauptkurs

Die Schulung orientiert sich an der Funktionsweise des menschlichen Gedächtnisses:

- Multimodale Inhalte:
  - Jede Einheit umfasst: eine interaktive Lektion, Assessments zur Verstärkung (ggf. simulierte Phishing-Angriffe testen)
  - Alle Trainingselemente unterstützen die in jeder Einheit vermittelte Kompetenz, so dass die Kompetenz wirklich verstanden und Teil des neuen, erwünschten Verhaltens wird
- Intervall-Lernen:
  - Schulungseinheiten folgen in bestimmten Abständen aufeinander, damit sich die Teilnehmer nicht einfach durch alle Lektionen klicken. So können sie sich die Inhalte besser merken. Die Intervalle basieren auf der „Vergessenskurve“ von Ebbinghaus
  - Wiederholung fördert sichere Gewohnheiten und lang anhaltendes Fachwissen
- Ausgewogene, strukturierte Inhalte und Praxisbezug sorgen für Effizienz:
  - mit vielen Beispielen aus der Praxis, die den Mitarbeitern die Bedeutung der Cybersicherheit für sie selbst deutlich machen
  - Der Schwerpunkt der Plattform liegt dabei auf der Vermittlung von Fähigkeiten, nicht lediglich theoretischem Wissen. Daher stehen praktische Übungen und Aufgaben im Mittelpunkt der einzelnen Module.





Flexibles Lernen

Der Trainingsumfang der Ausbildung ist flexibel, wobei die Vorteile eines sequentiellen und automatisierten Lernmanagements erhalten bleiben. Je nach Teilnehmergruppe können Sie wählen:

- Haupt- oder Express-Kurs bzw. eine Kombination aus beidem;
- welche Themen im Hauptkurs und/oder im Express-Kurs behandelt werden sollen und für die Teilnehmer der Gruppe relevant sind;
- welche Ziele die Teilnehmer zu bestimmten Themen im Standardkurs erreichen sollen.

Auf der Grundlage dieser Einstellungen wird der Lernpfad für jede Teilnehmergruppe automatisch von der Plattform erstellt.

Komplette Verwaltung über das Dashboard

- Alles, was Sie zur Steuerung und Verwaltung Ihrer Schulungen benötigen, lässt sich über das Dashboard erledigen: Statistiken, Übersichten über die Aktivitäten und Fortschritte der Nutzer, Schulungszeiten, Gruppenschulungen, Vorschläge zur Verbesserung der Ergebnisse. Die Berichte können Sie einfach per Mausklick herunterladen. Sie entscheiden, in welcher Frequenz Berichte erstellt werden.

Sicherheitsfaktor Mensch

- Mit dem für Mobilgeräte optimierten Design von ASAP können Ihre Mitarbeiter von jedem Gerät aus lernen und wann immer es in ihren Zeitplan passt.
- Nutzer können über personalisierte Links in der Schulungseinladung oder, falls vom Administrator eingerichtet, über einen gemeinsamen Link für alle Benutzer per Single Sign-On (SSO) auf das Schulungsportal zugreifen.

Individuelle Anpassung

Administratoren können das Erscheinungsbild des Programms einfach anpassen:

- im Verwaltungsbereich, im Schulungsportal und in den E-Mails der Plattform das Kaspersky-Logo durch Ihr Firmenlogo ersetzen;
- Zertifikate anpassen;
- zu jeder Lektion persönliche Inhalte hinzufügen.

Integration

Sie können Open API verwenden, um mit Lösungen von Drittanbietern zu interagieren – Open API funktioniert über HTTP und bietet eine Reihe von Anfrage-/Antwort-Methoden.

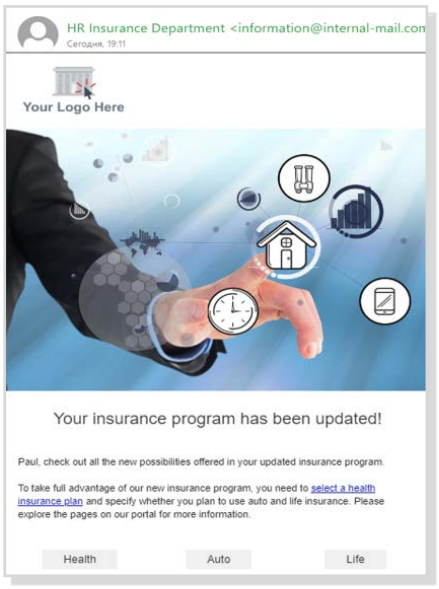
ASAP lässt sich in die Kaspersky-Plattformen KUMA und XDR integrieren:
– Administratoren können ein Ereignis in XDR sehen und die entsprechenden Maßnahmen ergreifen, indem sie zum Beispiel eine Schulung in ASAP zuweisen
– Automatische Anreicherung von Ereigniskarten mit Informationen zum Level der Sicherheitskenntnisse des angegriffenen Nutzers

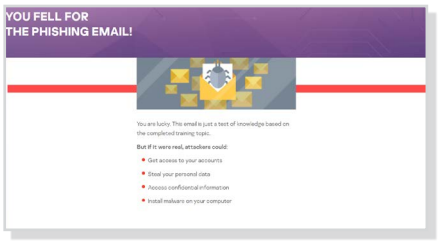
Lokalisierung

ASAP ist in 25 Sprachen verfügbar*. Die Lokalisierung von ASAP geht über die reine Übersetzung hinaus – Texte und Bildmaterial werden nicht nur in verschiedene Sprachen übersetzt, sondern auch an unterschiedliche Kulturen und lokale Gegebenheiten angepasst.

* Eine aktuelle Liste der verfügbaren Sprachen finden Sie unter k-asap.com/de

Beispiel für eine editierbare simulierte Phishing-Vorlage und Feedback

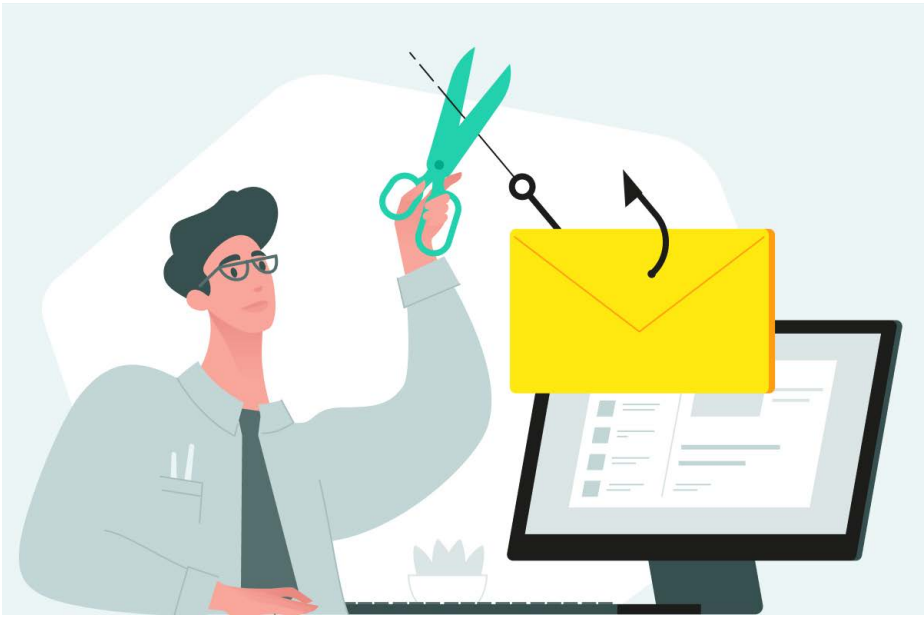




Simulierte Phishing-Angriffe

Als Ergänzung zu den Hauptkursen werden auch Phishing-Kampagnen angeboten. Darin wird getestet, ob Ihre Mitarbeiter wissen, wie sie in der Praxis mit Phishing-Angriffen umgehen müssen. Außerdem helfen solche praktischen Tests den Schulungsverantwortlichen, Wissenslücken bei den Nutzern schnell zu erkennen und problematische Themen zu vertiefen. Die Phishing-Kampagnen sind auch hervorragend geeignet, um Mitarbeitern zu vermitteln, wie sie gefährliche Anzeichen erkennen und wie sie ihr Wissen in die Praxis umsetzen können.

Auf der Plattform finden Sie vorgefertigte E-Mail-Vorlagen mit Phishing-Beispielen. Diese können in allen verfügbaren Sprachen an die Nutzer versendet werden. Die Vorlagen werden regelmäßig aktualisiert und erweitert. Auf Basis der vordefinierten Templates können Sie auch eigene E-Mails erstellen.



Bevor Sie in das Training einsteigen, können Sie einen simulierten Phishing-Angriff starten. So prüfen Sie die Resilienz Ihrer Mitarbeiter! Dies hilft Mitarbeitern und Vorgesetzten, die Vorteile des Trainings zu erkennen.

Mitarbeiter können ihr Wissen unter Beweis stellen, indem sie sich von einem simulierten Phishing-Angriff nicht täuschen lassen und Phishing-Mails über das Phishing Meldetool anzeigen.

Das Phishing Meldetool zeigt, inwieweit die Mitarbeiter sensibilisiert sind, entfernt E-Mails aus dem Posteingang und sendet Nachrichten nicht nur an Plattformadministratoren, sondern auch an die IT- und IT-Sicherheitsteams. So kann das Unternehmen seine Prozesse zur Erkennung und Reaktion auf Phishing verbessern.

Kaspersky ASAP für MSP/MSSP-Partner oder unternehmen mit einer geografisch stark verteilten Strukturen

Die Plattform ermöglicht die Durchführung von Awareness-Schulungen in mehreren Unternehmen. Die Verwaltung erfolgt über eine zentrale, mandantenfähige Konsole, für die keine zusätzliche Software installiert werden muss.

Gute Neuigkeiten! Über eine Verwaltungsfunktion für Lizenzkontingente in Kaspersky ASAP können Sie jedem Unternehmen ein Lizenzkontigent zuweisen und die Gültigkeitsdauer selbst festlegen.

Darüber hinaus können für jedes Unternehmen weitere Administratoren mit jeweils unterschiedlichen Rollen benannt werden.

Kaspersky Security Awareness – ein neuer Ansatz zur Vermittlung von IT-Sicherheitskompetenz

Wichtige Schlüsselmerkmale des Programms

Umfangreiches Fachwissen im Bereich Cybersecurity
Mehr als 25 Jahre Erfahrung sind in unser Angebotspaket an Cybersicherheitsschulungen eingeflossen

Training, welches das Verhalten der Mitarbeiter auf allen Ebenen Ihres Unternehmens verändert
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.

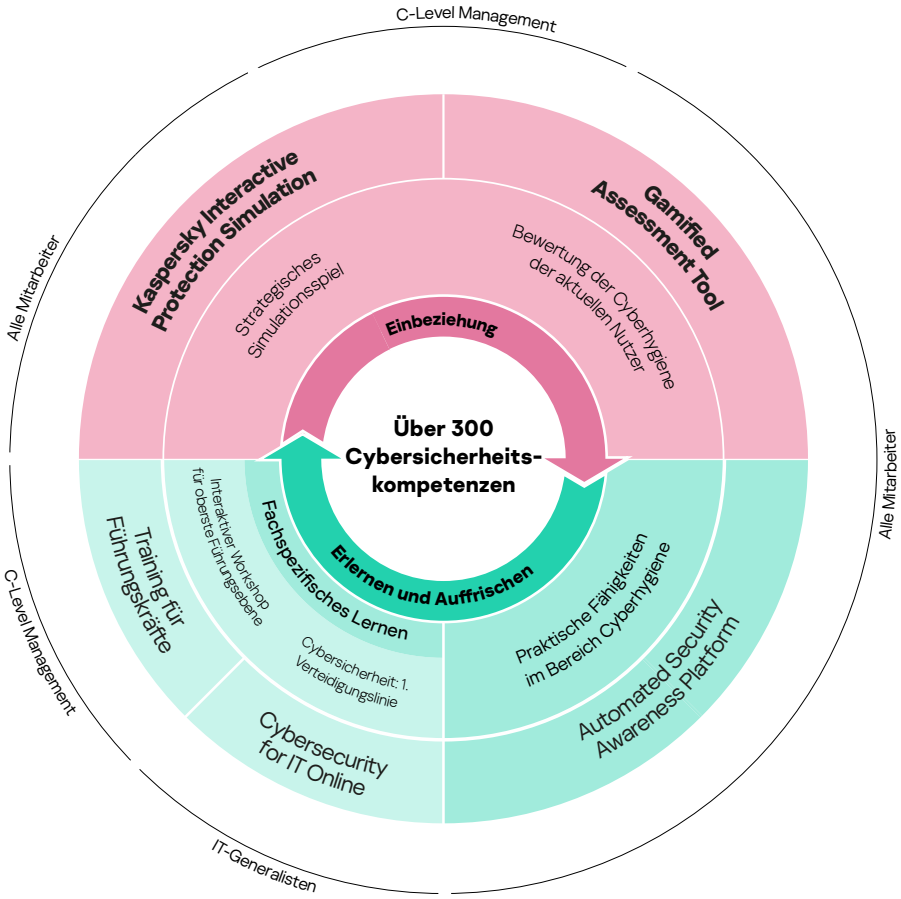
ASAP ist das Kernprodukt im Security Awareness-Portfolio von Kaspersky.

Flexibles Schulungsangebot für alle

Kaspersky Security Awareness ist international seit vielen Jahren erfolgreich. 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.

Das Portfolio bietet eine Reihe interessanter Trainingsoptionen, die das Cybersicherheitsbewusstsein Ihrer Mitarbeiter auf allen Ebenen schärfen und sie in die Lage versetzen, ihren Beitrag zur allgemeinen Cybersicherheit Ihres Unternehmens zu leisten.

Nachhaltige Verhaltensänderungen brauchen Zeit. Deshalb sieht unser Ansatz den Aufbau eines kontinuierlichen Lernzyklus vor, der aus mehreren Komponenten besteht. Spielerisches Lernen bindet Führungskräfte ein und macht sie zu Befürwortern von Cybersicherheitsinitiativen und zu Unterstützern für den Aufbau einer cybersicheren Verhaltenskultur. Spielerisch angelegte Weiterbildungsmaßnahmen decken Wissenslücken der Mitarbeiter auf und fördern kontinuierliches Lernen, während über Online-Plattformen und Simulationen die richtigen Fähigkeiten vermittelt und dauerhaft verinnerlicht werden.



Kostenlose Testversion von Kaspersky ASAP: k-asap.com/de/
Enterprise Cybersecurity: www.kaspersky.de/enterprise
Kaspersky Security Awareness: www.kaspersky.de/awareness
IT Security News: www.kaspersky.de/blog/b2b

www.kaspersky.de

kaspersky bring on the future