KASPERSKY lab

Kaspersky ASAP: Automated Security Awareness Platform

Effizienz und einfache Verwaltung für Unternehmen jeder Größe

www.kaspersky.de/awareness
asap.kaspersky.com
#truecybersecurity

Kaspersky ASAP: Automated Security Awareness Platform

Mehr als 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. 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.

Menschliche Fehler als größtes Cybersicherheitsrisiko unserer Zeit

83 000 $ pro KMU
Durchschnittliche finanzielle Folgen des Fehlverhaltens von unachtsamen/unwissenden Mitarbeitern[1]

101 000 $ pro KMU
Finanzielle Auswirkungen von Angriffen durch Phishing/Social Engineering[1]

400 $ pro Mitarbeiter und Jahr
Durchschnittliche Kosten von Phishing-Angriffen (andere Arten von Cyberbedrohungen sind von dieser Berechnung ausgenommen)[2]

52 % aller Unternehmen
nannten fahrlässiges Verhalten von Mitarbeitern/Benutzern als größtes Problem in ihrer IT-Sicherheitsstrategie[1]

Hindernisse für die Einführung eines effizienten Programms zur Erhöhung des Sicherheitsbewusstseins

Heutige Unternehmen sind zwar bestrebt, Programme zum Sicherheitsbewusstsein umzusetzen, viele von ihnen sind aber mit dem Verfahren und den Ergebnissen nicht zufrieden. Ein besonders großes Problem ist dies für kleine und mittlere Unternehmen, die in der Regel keine Erfahrung und dedizierten Ressourcen haben.

Wissen nicht, wie man Ziele setzt und Schulungen plant

Verwaltung von Schulungen ist zu zeitaufwendig

Berichte helfen nicht bei der Verfolgung von Zielen

Mitarbeiter nehmen das Programm nicht an → erlernen somit keine Fähigkeiten

Selbst Unternehmen mit engagierten Teams im Bereich Sicherheitsbewusstsein tun sich oft schwer, mit Schulungen zum Sicherheitsbewusstsein eine echte Verbesserung des Benutzerverhaltens zu erreichen.

Viele Unternehmen treffen eine Wahl zwischen einer einmaligen Schulung (wie „Alles zum Thema Cybersicherheit in 1 Stunde") und gut strukturierten Schulungsprogrammen, von denen sie aber nur einige grundlegende Funktionen und Tools nutzen. In der Regel besteht dies aus einer Reihe von simulierten Phishing-Angriffen pro Jahr plus ein paar Übersichtslektionen, weil andere Programmelemente zu schwer durchzuführen und zu verwalten sind. In beiden Fällen erhalten die Mitarbeiter nicht die erforderlichen umfassenden Fähigkeiten, um für anhaltend gute Sicherheit in ihrem Unternehmen zu sorgen.

[1] „Der menschliche Faktor in der IT-Sicherheit: Wenn Mitarbeiter zum Risikofaktor werden", Kaspersky Lab und B2B International, Juni 2017.

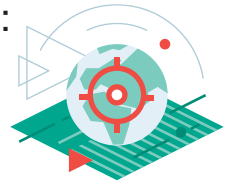
[2] Die Berechnungen basieren auf der Veröffentlichung „Cost of Phishing and Value of Employee Training" von August 2015.

Effizienz und einfaches Bewusstseinsmanagement für Unternehmen jeder Größe

Kaspersky Lab führt die Automated Security Awareness Platform ein, das Kernstück des Schulungsportfolios „Kaspersky Security Awareness“.

Die Plattform ist ein Online-Tool für Mitarbeiter zur Förderung umfassender und praktischer Kenntnisse zur Cybersicherheit im Laufe eines Jahres. Zur Implementierung und Verwaltung der Plattform sind keine spezifischen Ressourcen und Vorbereitungen erforderlich und sie bietet dem Unternehmen integrierte Hilfe bei allen Schritten auf dem Weg hin zu einer sicheren Cyberumgebung im Unternehmen:

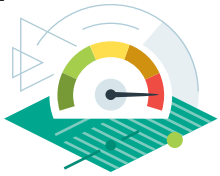
Schritt 1:



Legen Sie Schulungsziele fest und schaffen Sie Relevanz für ein Programm

- Legen Sie Ziele im Hinblick auf den weltweiten Benchmark fest
- Schaffen Sie ein Gleichgewicht zwischen dem angezielten Niveau an Sicherheitskompetenz für jede Mitarbeitergruppe und der gesamten Zeit, die von den Mitarbeitern benötigt wird, um dieses Niveau zu erreichen

Schritt 2:



Stellen Sie sicher, dass alle Mitarbeiter das erforderliche Niveau erreichen

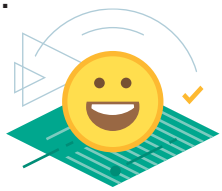
- Verwenden Sie das automatisierte Schulungsmanagement, mit dem alle Mitarbeiter auf den Sicherheitskenntnisstand hinarbeiten können, der für ihr jeweiliges Risikoprofil erforderlich ist
- Stellen Sie sicher, dass die erworbenen Kenntnisse gefestigt werden, um zu verhindern, dass die Mitarbeiter sie vergessen
- Schulen Sie Mitarbeiter individuell und in ihrem eigenen Tempo, um eine übermäßige Vermittlung von Inhalten und Ablehnung zu vermeiden

Schritt 3:

Überwachen Sie den Fortschritt mit praktisch umsetzbaren Berichten und Analysen

- Rufen Sie Daten, Trends und Prognosen in Echtzeit ab
- Verwenden Sie Echtzeitprognosen für die Erreichung des jährlichen Schulungsziels
- Gehen Sie auf Schwierigkeiten ein, bevor diese zum Problem werden (Sie wissen z. B., welche Organisationseinheiten mehr Aufmerksamkeit benötigen, und Sie können Einfluss auf deren Ergebnisse nehmen)
- Vergleichen Sie Ihre vorläufigen Ergebnisse mit den globalen KL-Daten

Schritt 4:



Schaffen Sie ein Umfeld, in dem Schulungen gern angenommen werden, was wiederum zu einer höheren Effizienz führt

- Motivieren Sie Ihre Mitarbeiter mit praktischen, interaktiven Übungen
- Stellen Sie Lernszenarien bereit, die für den Arbeitsalltag der Teilnehmer relevant sind
- Vermeiden Sie Informationsüberflutung und Weiterbildungsmüdigkeit

Programmmanagement: Unkompliziertheit durch Automatisierung

Programmstart in 10 Minuten

- Zielvorgaben anhand weltweiter/Branchendurchschnittswerte
- Schulung beginnen
- Zahlung nur für aktive Benutzer (die Lernenden)

Plattform passt sich dem individuellen Tempo und den Lernfähigkeiten jedes einzelnen Mitarbeiters an

- Plattform sorgt automatisch dafür, dass Benutzer vor dem Fortfahren grundlegende Tests über das Gelernte bestehen müssen
- Manager brauchen keine Zeit für die Analyse individueller Fortschritte und manuelle Anpassungen aufzuwenden

Vorteile spezifischer Lernwege für alle Risikoprofile

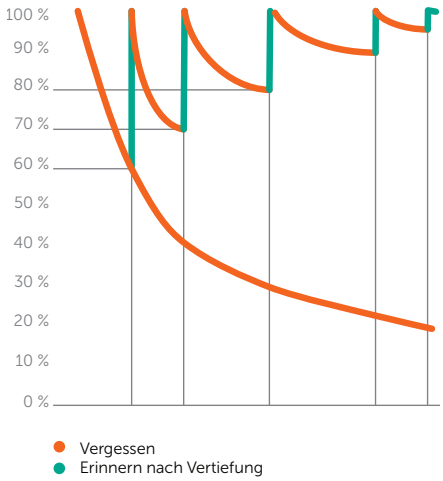
- Automatisierte Regeln verwenden, um Mitarbeiter je nach gewünschter Schulungsebene einer bestimmten Gruppe zuzuweisen. Das Ziel hängt von der Gefahr ab, die der Benutzer für das Unternehmen darstellt. Je höher das Risiko, desto höher sollte die Zielebene für die Schulung sein. IT oder Buchhaltung stellen typischerweise ein höheres Risiko als die meisten Büromitarbeiter dar.
- Jede Gruppe von Benutzern erlernt das Material nur in dem Umfang, in dem es wirklich benötigt wird, ohne zu viel Zeit für die Schulung aufzuwenden.

Jederzeit umsetzbare Berichte

- Nützliche Dashboards mit allen erforderlichen Informationen zur Einschätzung des Fortschritts
- Einholen von Vorschlägen, was zur Verbesserung der Ergebnisse erforderlich ist
- Vergleich der Ergebnisse mit weltweiten/Branchen-Benchmarks

Die ebbinghaussche Kurve

Regelmäßige Wiederholung trägt zu umfassenden Fähigkeiten bei.



Schulungseffizienz: kontinuierliches Mikrolernen

Die Fähigkeiten von Mitarbeitern erhöhen sich Ebene für Ebene, von der einfachsten bis hin zur fortgeschrittensten. Mitarbeitern, die eine vorherige Ebene nicht erfolgreich abgeschlossen haben, werden automatisch weitere Lerneinheiten zugewiesen. Dies sorgt für langfristig vertiefte Fähigkeiten, die nicht leicht vergessen werden.

Mikrolernen

- Der Inhalt ist speziell für Mikrolernen strukturiert (2 bis 10 Minuten), sodass langweilige und ermüdend lange Lektionen vermieden werden.

Umfassende Tools für jedes Sicherheitsthema

- Jede Ebene umfasst: interaktive Lektionen und Videos → Tests → Festigung des Wissens (Test oder simulierter Phishing-Angriff)

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 reicht in der Regel als Schutz vor einfachen und Massenangriffen aus. Zum Schutz vor komplexen und zielgerichteten Angriffen müssen die nächsten Levels abgearbeitet werden.

Schulungsthemen*

- E-Mail
- Surfen im Internet
- Passwörter
- Soziale Netzwerke und Messenger
- PC-Sicherheit
- Mobile Geräte
- Vertrauliche Daten
- Persönliche Daten/DSGVO
- Social Engineering
- Sicherheit zu Hause und unterwegs

Beispiel: im Thema „Webbrowser" vermittelte Fähigkeiten

Einsteiger Vermeiden von Massen-angriffen (billig und einfach)	Grundlegend Vermeiden von Angriffen auf ein bestimmtes Profil	Fortgeschrittener Vermeiden von gut vorbereiteten, gezielten Angriffen	Advanced Vermeiden von gezielten Angriffen
13 Fähigkeiten, einschließlich: – Einrichten des PC (Updates, Virenschutz) – Ignorieren offensichtlich schädlicher Websites (die Sie auffordern, Software zu aktualisieren, die PC-Leistung zu optimieren, SMS zu senden, Player zu installieren usw.) – Niemals ausführbare Dateien von Webseiten aus öffnen	**20 Fähigkeiten, einschließlich:** – Anmelden/ Einloggen nur bei vertrauenswürdigen Webseiten – Vermeiden numerischer Links – Eingabe von vertraulichen Informationen nur auf vertrauenswürdigen Webseiten – Erkennen von Anzeichen für eine schädliche Webseite	**14 Fähigkeiten, einschließlich:** – Erkennen gefälschter Links – Erkennen schädlicher Dateien und Downloads – Erkennen schädlicher Software	**13 Fähigkeiten, einschließlich:** – Erkennen raffiniert gefälschter Links (einschließlich Links, die wie Ihre Unternehmens-Webseiten aussehen, Links mit Umleitung) – Vermeiden gefälschter SEO-Webseiten – Abmelden nach Beendigung der Arbeit – Erweiterte PC-Einrichtung (Java, Adblock und Noscript usw. deaktivieren)
	+ Vertiefung der grundlegenden Fähigkeiten	+ Vertiefung der bisher erlernten Fähigkeiten	+ Vertiefung der bisher erlernten Fähigkeiten

Wichtigste im Thema vermittelte Kenntnisse: Links, Downloads, Software-Installation, Anmelden und Einloggen, Zahlungen, SSL

* Änderungen an den endgültigen Schulungsthemen vorbehalten.

Sprachen

Ab Herbst 2018 ist die Plattform in den folgenden Sprachen verfügbar:*
- Englisch
- Deutsch
- Italienisch
- Russisch

Als Nächstes folgen:
- Arabisch
- Französisch
- Spanisch

Neue Sprachen werden regelmäßig hinzugefügt, um eine tief greifende und effiziente Schulung für alle Regionen zu gewährleisten.

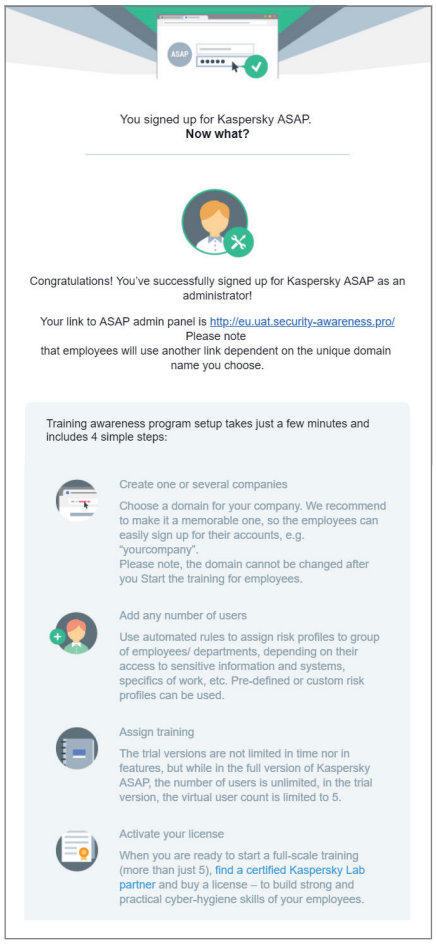
Spielerisches Lernen und Relevanz für das echte Leben gewährleisten höhere Effizienz

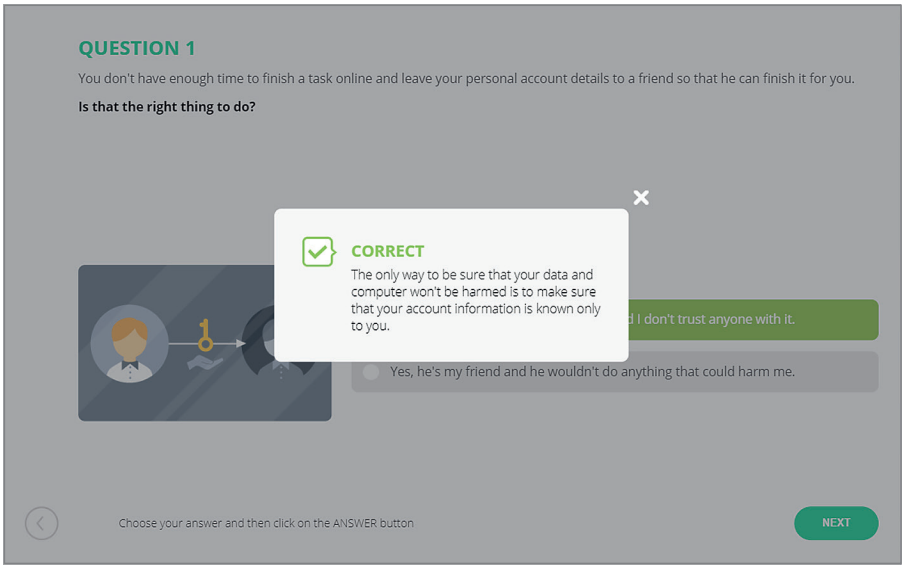
Der Inhalt der Plattform beruht auf Simulationen realer Ereignisse unter Hervorhebung der persönlichen Bedeutung der Cybersicherheit für Mitarbeiter. Der Schwerpunkt liegt dabei auf der Vermittlung von Fähigkeiten, nicht lediglich theoretischem Wissen. Daher stehen praktische Übungen und Aufgaben im Mittelpunkt der einzelnen Module.

Die Module enthalten unterschiedliche Kombinationen von Aufgaben, damit Interesse und Aufmerksamkeit der Benutzer nicht nachlassen und sie motiviert werden, sicheres Verhalten zu erlernen.

Der visuelle Stil und die Texte werden nicht nur in verschiedene Sprachen übersetzt, sondern auch auf die jeweilige Kultur und die lokalen Gegebenheiten angepasst.

Simulationsbasierte Aufgaben und Übungen zum Erlernen praktischer Fähigkeiten und um die Schulung unterhaltsam und motivierend zu gestalten





* Änderungen an der endgültigen Reihenfolge und dem Zeitpunkt der Lokalisierung vorbehalten.

Kaspersky® Security Awareness

Kaspersky Lab hat eine Reihe von computerbasierten Schulungsprodukten mit spielerischem Lernen auf den Markt gebracht, die auf modernen Lerntechniken basieren und an sämtliche Unternehmensebenen gerichtet sind. Dieser Ansatz trägt dazu bei, eine gemeinsame Kultur der Cybersicherheit aufzubauen, wodurch im gesamten Unternehmen eine sich selbst tragende Ebene der Cybersicherheit entsteht.

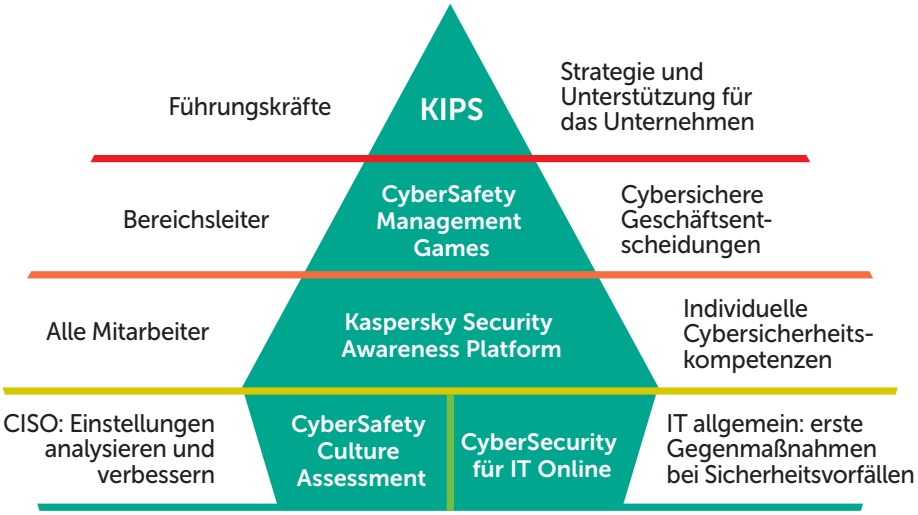
bis zu
90 %
weniger Vorfälle insgesamt

mindestens
50 %
geringere finanzielle Einbußen durch Vorfälle

bis zu
93%ige
Wahrscheinlichkeit, dass das Wissen bei der täglichen Arbeit angewendet wird

mehr als der
30-fache
ROI aus Investitionen in Sicherheitsbewusstsein

ganze
86 %
der Teilnehmer sind bereit, die Schulungsprogramme weiterzuempfehlen



Ziele festlegen und ein Programm auswählen

- Festlegen von Zielen anhand globaler Daten
- Benchmarking anhand von globalem/ Branchen-durchschnitt

Schulungs-management

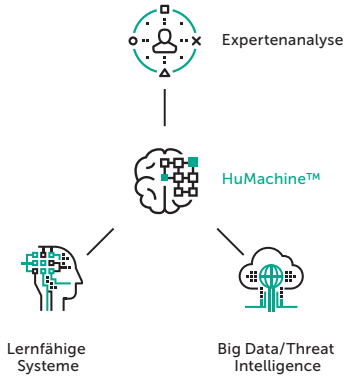
- Automatisiertes Lernen
- Automatisch angepasster Lernpfad
- Berechnung der benötigten Zeit

Berichte und Analysen

- Jederzeit umsetzbare Berichte
- Direkte Analyse des Verbesse-rungspotenzials

Programm-effizienz und -annahme

- Praktische, motivierende Übungen
- Verhindern von Überbelastung und Weiter-bildungsmüdigkeit
- Verinnerlichung von Kenntnissen und Fähigkeiten erreichen



Kaspersky Lab
Security Awareness: www.kaspersky.de/awareness
Enterprise Cybersecurity: www.kaspersky.de/enterprise
Neues über Cyberbedrohungen: www.de.securelist.com
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/

#truecybersecurity
#HuMachine

www.kaspersky.de