Sicherheitsfaktor Mensch

Wie automatisiertes Cybersecurity Training den Mitarbeiter zur ersten Verteidigungslinie gegen Cyber-bedrohungen werden lässt

Kaspersky
Automated Security
Awareness Platform

kaspersky BRING ON THE FUTURE

Zur kostenlosen Testversion:
k-asap.com/de

Einleitung

90 %[1]
aller **Cybervorfälle** gehen auf menschliche Fehler zurück

Wenn Sie, wie so viele andere Unternehmen auch, einem internen Cybervorfall zum Opfer gefallen sind, dann kennen Sie vermutlich bereits das schwächste Glied der Cybersicherheit: den wohlmeinenden, aber unaufgeklärten Mitarbeiter. Seit Phishing-Filter und Firewalls immer ausgefeilter geworden sind, konzentrieren sich Cyberkriminelle zunehmend auf die Mitarbeiter als möglichem Eintrittspunkt in IT-Systeme. Die Folge: Mehr als 90 %[1] aller Cybervorfälle gehen auf menschliches Versagen zurück.

Probleme wie der Verlust vertraulicher Daten, Geschäftsunterbrechungen und Hardware-Ausfälle haben ernsthafte finanzielle Konsequenzen. Die durchschnittlichen Kosten einer Datenschutzverletzung für KMUs durch unsachgemäße IT-Nutzung belaufen sich intern auf 116 000 US-Dollar[2], während die durchschnittlichen weltweiten Kosten einen einzigen Sicherheitsverletzung bei 3,92 Mio US-Dollar[3] liegen. Schätzungen zufolge haben in der ersten Hälfte 2019 nahezu 4000 Datenschutzverletzungen die Daten von mehr als vier Milliarden Nutzern gefährdet[4].

Dieser Umstand weist eindeutig auf ein **fehlendes Bewusstsein bezüglich der Best Practices in der Cybersicherheit unter den Mitarbeitern** hin sowie auf einen Mangel an angemessener Lerntechnologie, um sicherzustellen, dass Schulungen den gewünschten Erfolg erzielen.

In diesem Whitepaper soll dargelegt werden, inwieweit mithilfe von Schulungen sichergestellt werden kann, dass Mitarbeiter mit der Technologie einer Organisation verantwortungsvoll und selbstbewusst umgehen. Insbesondere kann durch stetige, interaktive, interessante, vor allem aber auch *praxisnahe* Schulungen gewährleistet werden, dass der Sicherheitsfaktor Mensch gestärkt wird.

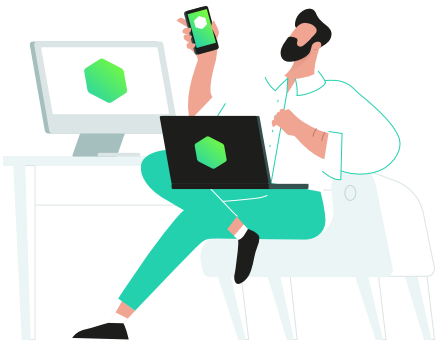
1 Analyse der Berichte zu Datenschutzverletzungen, die der britischen Datenschutzbehörde (ICO) gemeldet wurden

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

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

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

Herausforderung am Desktop, Remote und mobil



Die sich entwickelnde Komplexität unserer IT-Landschaft bedeutet, dass Umfang und Schwere von Cyberangriffen zunehmen. Neue Sicherheitstechnologien helfen die Bedrohung durch Schadprogramme einzudämmen, aber unser Verhalten sowohl als Nutzer von Technologien als auch als Mitarbeiter in einem Unternehmen haben derzeit die größten Auswirkungen auf die Sicherheit von Organisationen.

Wir sind alle stärker vernetzt und immer mobiler geworden, tragen mehr persönliche Geräte mit uns herum und nutzen im täglichen Leben immer mehr kostenlose und weit verbreitete Services. Mobile Geräte sind mittlerweile in 75 % der Unternehmen zu einem festen Bestandteil der Geschäftsprozesse geworden, aber nur 17 % der Arbeitgeber statten ihre gesamte Mitarbeiterschaft mit geschäftlichen Handys aus[1]. Andere lassen bis zu einem gewissen Grad den Einsatz von persönlichen Geräten bei der Arbeit zu, was größere Risiken birgt.

Die zunehmende Zahl an Remote-Arbeitsplätzen tut ein Übriges. Während Unternehmen es meist noch schaffen, Netzwerke und Geräte am Arbeitsplatz umfassend zu schützen, **lassen sich dieselben betrieblichen Standards im privaten Umfeld eher selten umsetzen.** In einer kürzlich durchgeführten Studie zum Thema Heimarbeitsplatz[2] gaben 47 % der Befragten an, mehr Zeit mit dem Anschauen von Videos zu verbringen, wobei etwa jeder zweite (48 %) dazu beruflich genutzte Geräte einsetzt. Überraschenderweise gab die Hälfte (51 %) der Mitarbeiter zu, Inhalte für Erwachsene auf beruflichen Geräten anzuschauen, trotz des damit verbundenen Malware-Risikos von diesen Seiten. Hinzu kommt, dass 73 % der Mitarbeiter von ihrem Arbeitgeber niemals eine Schulung zum Thema IT-Sicherheitsbewusstsein erhalten haben, seit sie von Zuhause aus arbeiten.

„Mit neuen Cyberbedrohungen und neuen Formen der Manipulation konzentrieren sich Cyberkriminelle zunehmend auf Remote-Mitarbeiter."

Mit neuen Cyberbedrohungen und neuen Formen der Manipulation konzentrieren sich Cyberkriminelle zunehmend auf Remote-Mitarbeiter, so dass eine Bewusstseinsschärfung in Bezug auf grundlegende Regeln des sicheren Verhaltens wichtiger ist denn je. Schulungen müssen in diesem Zusammenhang einprägsamer und effektiver gestaltet werden, damit Mitarbeiter unterschiedliche Bedrohungen von der simplen Massen-Mail bis hin zu hochentwickelten Angriffen erkennen können.

1 Studie von Oxford Economics für Samsung, 2018

2 How Covid-19 changed the way people work, Kaspersky, 2020

Warum einmal Gelerntes so schnell in Vergessenheit gerät

Die Zahl der Cybervorfälle lässt sich durch effektive, Computer-gestützte interaktive Weiterbildung erheblich senken

Damit ein radikaler Wandel hin zu einem stärkeren Cybersicherheitsbewusstsein unter den Mitarbeitern gelingt, müssen Schulungen interessant gestaltet sind, damit das Wissen verinnerlicht wird. Eine Lernmethode, die sich auf das Lesen von Texten oder das Anschauen von Videos beschränkt, kann Inhalte nicht nachhaltig vermitteln, weil **viele Mitarbeiter dies als langweilig empfinden und das Gelernte schnell wieder vergessen.**

Um Inhalte zu verinnerlichen, muss eine Schulung die sogenannte Vergessenskurve von Ebbinghaus überwinden, nach der die Erinnerung im Laufe der Zeit verblasst. Lernmethoden sollten auf menschlichem Erinnerungsvermögen und Verhaltenspsychologie beruhen und der Bedeutung der Empathie beim Lernen und Lehren Rechnung tragen. Die folgenden zwei Beispiele sollen veranschaulichen, wo das traditionelle Lernen in dieser Hinsicht versagt. Erstens: Vermitteln von Inhalten, die keinen Bezug zu realen Situationen haben, mit denen die Menschen bei der Arbeit konfrontiert sind. Zweitens: Ein strikter Kursablauf ohne visuelle Anreize und Interaktion für die Teilnehmer führt zu einer geringeren Beteiligungsrate und zu keiner signifikanten Verhaltensänderung hinsichtlich der Cybersicherheit.

Schulungskurse, in denen die Teilnehmer nicht einbezogen werden, sind so schnell vergessen wie die Fähigkeiten, die eigentlich vermittelt werden sollten. Beispielsweise lag die durchschnittliche Klickrate bei Phishing-Mails in einem Unternehmen bei etwa 40 %. Unmittelbar nach der Schulung sank dieser Prozentsatz, um innerhalb weniger Monate wieder zurück auf 40 % anzusteigen[1].

Bei der Kaspersky Automated Security Awareness Platform (ASAP) mit Wiederholungsfragen und interaktiven Online-Schulungen hingegen wird das Gelernte verinnerlicht und es werden solide Fähigkeiten in Sachen Cybersicherheit aufgebaut. Das ist effektiv, weil neben der Wissensvermittlung auch bessere Verhaltensmuster für cybersicheres Arbeiten verinnerlicht werden.

1 Wirtschaftlichkeit der IT-Sicherheit 2019, Kaspersky, Feedback der Befragten

Praxisnah: Rolle der Interaktion und Cybersicherheitsszenarien

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

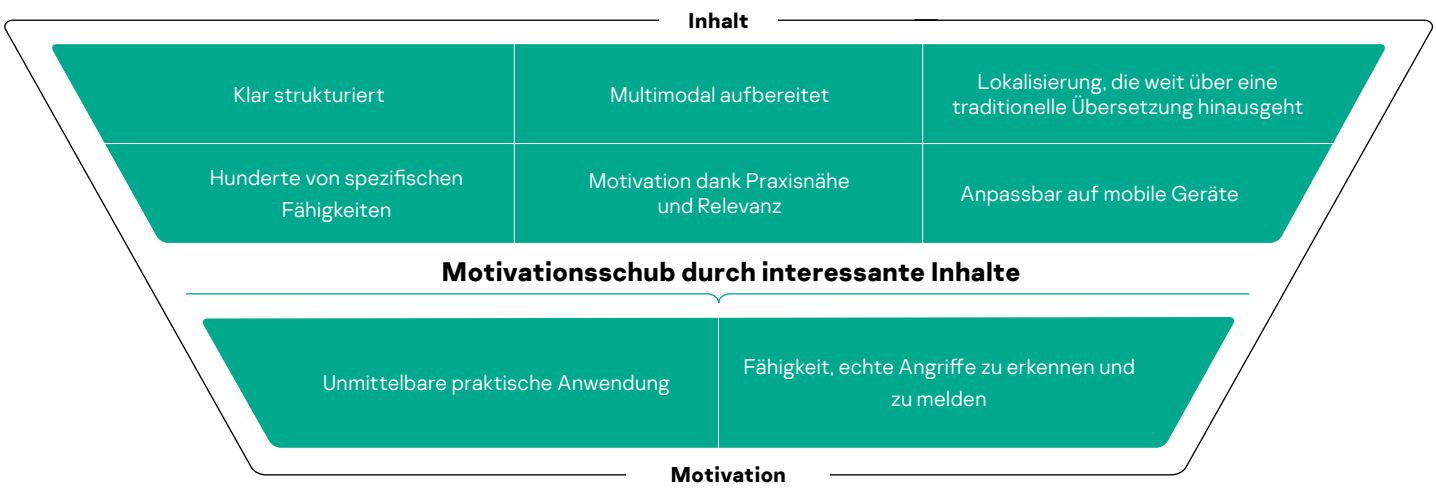
HR Director in der Fertigungsindustrie

Statt theoretischer Abhandlungen zur Cybersicherheit, die man durchliest oder anhört, lassen sich Schulungen mithilfe von multimodalen Inhalten viel interessanter und packender gestalten. Dabei greifen beim Erlernen einer bestimmten Fähigkeit unterschiedliche Schulungselemente ineinander, wie z. B. interaktive Lektionen, Tests, Wiederholungsfragen und simulierte Angriffe.

Realistische Szenarien von Cybervorfällen und simulierte Angriffe sind ein wichtiges Element dieses praxisnahen Ansatzes. Die Mitarbeiter lernen dabei, selbständig zu handeln. **Dadurch wird cybersicheres Verhalten trainiert, wenn während eines tatsächlichen Angriffs schnelle Entscheidungen getroffen werden müssen.**

Werden die multimodalen Inhalte dann noch logisch strukturiert präsentiert, wird die Schulung als leicht verständlich, nachvollziehbar und ausgeglichen wahrgenommen. Das Programm sollte immer auch fordernde Elemente enthalten, um die Motivation zu stärken, und nie „eingleisig" wirken. Kontinuierliches Lernen in einzelnen Schritten – mit Wiederholungsblöcken zu vorangegangenen Themen und das Verinnerlichen von Gewohnheiten – ist am besten geeignet, um sicherzustellen, dass die Mitarbeiter am Ball bleiben und die Inhalte langfristig abspeichern.

Die Schulungsinhalte sollten außerdem von einer Organisation zusammengestellt werden, die über entsprechendes Fachwissen im Bereich Cybersicherheit und nicht nur im Bereich der Pädagogik verfügt. Wir bei Kaspersky können auf mehr als 20 Jahre Erfahrung in der Cybersicherheit verweisen und wissen daher, welche Fähigkeiten Mitarbeiter entwickeln sollten, um sich sicher zu verhalten und das Unternehmen zu schützen. Diese Fähigkeiten sind direkt in die nach Themen und Stufen untergliederten Schulungsinhalte integriert worden.



Unkompliziert dank Automation

Wie bereits erwähnt sollte das Security Awareness Training stetig fortgeführt werden, um die neu angeeigneten Verhaltensmuster zu verfestigen. Dazu sollte in **regelmäßigen Auffrischungskursen das zuvor Gelernte wiederholt werden.** All diese Materialien manuell zuzuweisen, würde vermutlich jeden Administrator an seine Grenzen bringen – vor allem in kleineren Unternehmen mit begrenzten Ressourcen – während die Automation dies mühelos und ohne zeitlichen Aufwand bewerkstelligt.

Dank automatisierter Prozesse bleibt das Programm außerdem benutzerfreundlich und kann für eine Vielzahl von Mitarbeitern mit unterschiedlichem Wissensstand eingerichtet, verwaltet und bereitgestellt werden. Die Schulungen sind in kleinere Lektionen unterteilt, sodass Fortschritte in Bezug auf bestimmte Lernziele leichter nachverfolgt werden können. Das ist auch der Vorteil gegenüber der traditionellen Präsenzschulung, bei der keine großen Teilnehmerzahlen möglich sind und sich der Lernerfolg nur schwer messen lässt.

Gleichzeitig spart eine interaktive Online-Schulung dem Administrator Zeit, und zwar ohne dabei Abstriche bei der Lerntiefe zu machen. Mit Kaspersky ASAP können mehr als 300 praktische Fähigkeiten vermittelt werden, mit automatischen Ausbildungsplänen für jede einzelne Mitarbeitergruppe.

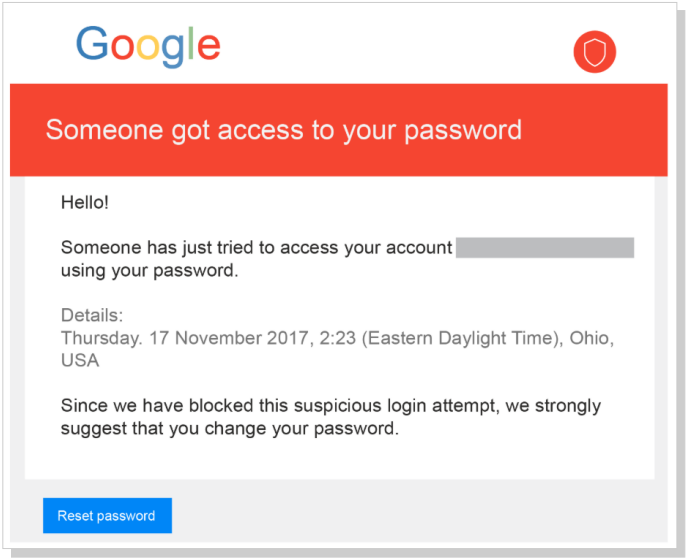
Wegweisend: Beispiel für eine Schulung zu Cyberbedrohungen

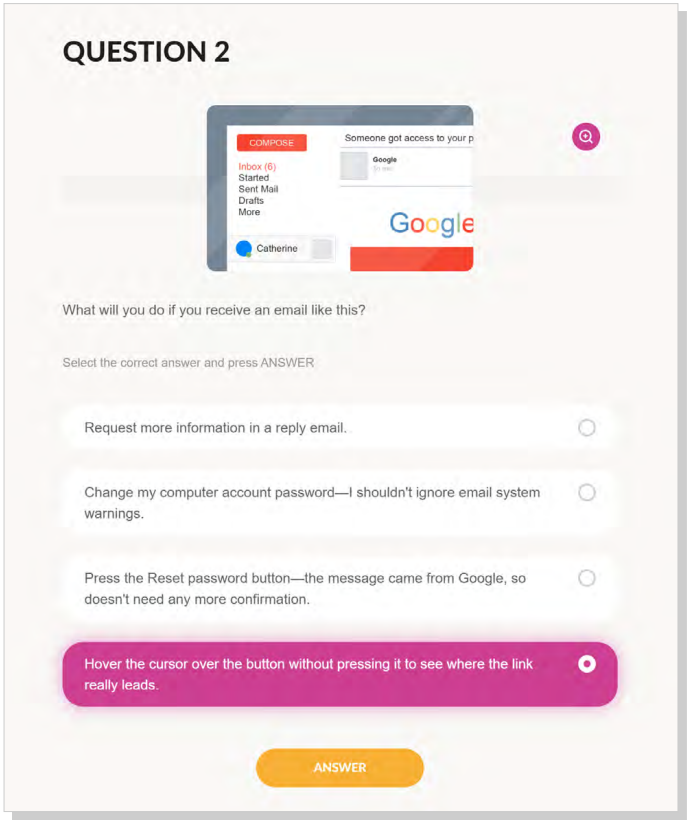
Simulierter Phishing-Angriff

Viele Menschen sind davon überzeugt, dass sie niemals auf einen Phishing-Angriff hereinfallen würden. Deshalb wird im Rahmen von Kaspersky ASAP nach interaktiven Lektionen, Tests und Wiederholungsfragen ein Szenario aus dem wirklichen Leben nachgestellt – in dessen Zentrum der Mitarbeiter steht.

In diesem Beispiel wird überprüft, ob der Mitarbeiter tatsächlich in der Lage ist, eine gefälschte E-Mail zu erkennen. Was sind mögliche Hinweise auf eine Gefahr? Wie überprüft man, ob Name und Adresse des Absenders wirklich echt sind? Was tun, wenn ein Phishing-Verdacht besteht?

Der Inhalt ist bewusst **kurz gehalten, dabei interessant, fordernd und einprägsam.** Das Erfolgserlebnis bei einer richtigen Antwort gibt dem Mitarbeiter einen echten Motivationsschub. Außerdem kann er das Gelernte schon nach einer einzigen Lektion direkt anwenden, um das Unternehmen zu schützen.





Fazit

Entscheidungsträgern im IT- und Sicherheitsbereich wird zunehmend bewusst, wie wichtig Sicherheitsschulungen für ihre Mitarbeiter sind. Jetzt geht es für sie darum, einen Anbieter und eine Schulungslösung auszuwählen, die langfristige Erfolge gewährleistet. Dazu müssen Schulungen auf besseren Lernprinzipien und interaktiven Inhalten basieren, um das Sicherheitsbewusstsein der Teilnehmer in realen Situationen zu fördern. Sie sollten außerdem so angelegt sein, dass das neu angeeignete Wissen verinnerlicht wird und nicht gleich wieder in Vergessenheit gerät.

Die Vorteile eines guten Schulungsprogramms gehen über das rein Finanzielle hinaus und zeigen sich in einer wachen Haltung und dem Selbstvertrauen des Mitarbeiters ebenso wie in einer besseren Arbeitskultur. **Bei einer *praxisnah* ausgerichteten Schulung können die Mitarbeiter den Sicherheitsfaktor Mensch deutlich stärken.**

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

kaspersky BRING ON THE FUTURE

www.kaspersky.de