KASPERSKY lab

Simply Be Aware

Security Awareness Trainings

Schließen Sie nicht die Augen.

Es ist Zeit für Security Awareness.

Das Ausmaß der Bedrohung

1994
JEDE **STUNDE** EIN NEUER VIRUS

2006
JEDE **MINUTE** EIN NEUER VIRUS

2011
JEDE **SEKUNDE** EIN NEUER VIRUS

2015
325.000 REG. MALWARE JEDEN TAG

2017
360.000 REG. MALWARE JEDEN TAG

Nach wie vor ist der Einsatz von Sicherheitstechnologien eine wichtige Basis beim IT-Schutz. Doch Softwarelösungen allein sind nicht mehr ausreichend, um Unternehmen vor den zahlreichen Gefahren aus dem Internet zu schützen.

Mehr als 80 Prozent aller Cybersicherheitsvorfälle sind auf menschliche Fehler zurückzuführen. Mitarbeiterschulungen sind deshalb eine wichtige Komponente im Security-Konzept.

Erfahren Sie, wie sich die Cyberbedrohungslage in den vergangenen Jahrzehnten zugespitzt hat, welche Bedrohungen heute gezielt auf Mitarbeiter ausgerichtet sind und wie Sie mit Security Awareness Trainings Ihr Unternehmen sicherer machen.

Rückblick: Wandel der Bedrohungslandschaft

Noch vor rund 30 Jahren tauchte Malware nur vereinzelt auf. Heute sieht die Welt der Cyberkriminalität schon ganz anders aus. Ein Blick zurück in die Geschichte der Cyberbedrohungen zeigt: Malware war Mitte der 80er Jahre meist noch das Produkt von „Hobby-Hackern“, die sich einen Spaß daraus machten, einzelne Rechner zu infizieren, um ihr Können unter Beweis zu stellen.

Mit der Verbreitung des Internets wuchs die Gefahr

Einer der ersten größeren Angriffe fand 1988 statt. Der Informatiker Robert Tappan Morris programmierte den ersten Computerwurm. Der sogenannte Morris-Wurm verbreitete sich sehr schnell und legte ca. 6.000 Rechner lahm – das entsprach zur damaligen Zeit mehr als zehn Prozent der weltweit an das Internet angebundenen Computer. Bis Mitte der 90er Jahre schritt die Malware-Entwicklung nur langsam voran. Doch dann hielt das Internet immer mehr Einzug in den Geschäftsalltag und veränderte die Lage radikal.

Die Intervalle, in denen neue Schadprogramme auf den Markt kamen, wurden über die Jahrzehnte immer kürzer. Und nicht nur die Anzahl schädlicher Software stieg kontinuierlich an. Auch wurden die Bedrohungen immer aggressiver und die Folgen eines Angriffs schwerwiegender.

KASPERSKY lab

400 $	83.000 $	101.000 $	52 %
Durchschnittliche Kosten allein durch Phishing-Attacken pro Mitarbeiter im Jahr	Durchschnittlicher Schaden durch unvorsichtiges Verhalten oder Unwissenheit von Mitarbeitern in kleinen und mittelständischen Unternehmen	Folgekosten von Phishing/ Social Engineering in kleinen und mittelständischen Unternehmen	Unternehmen sehen Mitarbeiter als größte IT-Security-Schwachstelle

Der menschliche Faktor in der Cybersicherheit

Heute sind viele Cyberbedrohungen gezielt auf Mitarbeiter ausgerichtet. Als schwächstes Glied in der Sicherheitskette machen sie es Cyberkriminellen oft recht leicht, ins Unternehmensnetzwerk vorzudringen.

Denn viele Mitarbeiter kennen gängige Angriffstechniken und Betrugsmethoden schlicht und einfach nicht. Wenn dann auch noch der Zeitdruck im heutigen Arbeitsalltag hinzukommt, wird manchmal zu schnell und unüberlegt auf schädliche Links geklickt oder vergessen, sicherheitsrelevante Software-Updates durchzuführen. Auch der Einsatz von USB-Sticks und die unabsichtliche Weitergabe von sensiblen Daten an Unbefugte sind typische Sicherheitslücken im Unternehmen.

Top 5 der größten Cybergefahren für Mitarbeiter

Phishing

Phishing ist eine Form von Social Engineering („soziale Manipulation“) und zielt auf die Leichtgläubigkeit und Hilfsbereitschaft von Menschen ab. Phishing-Mails haben zum Ziel, die Benutzernamen, Passwörter oder PIN-Daten von Mitarbeitern abzugreifen.

Auf den ersten Blick sieht eine Phishing-Mail wie eine ganz normale Information beispielsweise einer Bank oder eines Lieferanten aus. Nur Details wie Grammatik- und Orthografie-Fehler oder die Aufforderung, innerhalb kürzester Frist die Daten preiszugeben, weisen darauf hin, dass es sich möglicherweise um einen kriminellen Absender handelt. Allein durch Phishing-Attacken entstehen für Unternehmen durchschnittlich 400 US-Dollar Kosten pro Mitarbeiter im Jahr.

Ransomware

In der Regel wird Ransomware über E-Mails verbreitet. Diese enthalten infizierte Anhänge oder Verknüpfungen, die auf manipulierte Webseiten führen. Öffnet ein Mitarbeiter die angehängte Datei oder klickt auf den Link, wird die Schadsoftware automatisch heruntergeladen und verschlüsselt im schlimmsten Fall sämtliche im Unternehmensnetzwerk gespeicherten Daten.

Eine Entschlüsselung kann nur durch die Angreifer gegen Zahlung von Lösegeld (engl. Ransom) erfolgen. Unternehmen haben allerdings keinerlei Garantie, wieder auf ihre Daten zugreifen zu können. Im Mai 2017 machte die Ransomware-Attacke WannaCry weltweit Schlagzeilen. Auch heute zählt Ransomware zu den größten Cyberbedrohungen.

Top 5 der größten Cybergefahren für Mitarbeiter

Krypto-Miner

Über Mining-Programme können Einheiten (Coins) von Kryptowährungen generiert werden. Dies ist zum Teil allerdings sehr zeitintensiv und nur mit hohem Energieverbrauch möglich. Angesichts der wachsenden Nachfrage nach Kryptowährung nutzen auch Cyberkriminelle verstärkt das Mining für ihre Geschäftstätigkeiten. Sie installieren heimlich Mining-Software auf tausenden von Rechnern, die sie zu einem Botnet zusammenschließen, um mit der Summe an Rechenleistung Kryptowährung zu erzeugen.

Die Gefahr, Opfer eines Kryptowährungs-Miner zu werden, steigt. Laut einer Kaspersky-Analyse zu den Cybergefahren durch USB-Geräte und andere Wechseldatenträger im Jahr 2018 nutzen Cyberkriminelle derzeit vor allem den USB-Anschluss zur Verbreitung von Krypto-Mining-Malware.

Mobile Malware

Mobile Malware ist speziell für die Infektion von Smartphones, Tablets & Co. entwickelt. Da immer mehr Mitarbeiter von unterwegs und im Homeoffice arbeiten und dabei oft ihre privaten Mobilgeräte geschäftlich nutzen (BYOD, Bring Your Own Device), stellt dies eine potenzielle Gefahr für Unternehmen dar.

Es besteht nicht nur das Risiko, dass Geräte verloren gehen oder gestohlen werden. Durch das Herunterladen einer App, aber auch durch die Verbindung zu einem öffentlichen WiFi-Netzwerk können auch unberechtigte Datenzugriffe erfolgen. Erschwerend kommt hinzu: Laut einer Kaspersky-Umfrage wissen 28 Prozent der Befragten nur wenig oder gar nichts über mobile Schadsoftware. Weitere 26 Prozent kennen die Gefahren, ignorieren sie aber weitgehend.

CEO Fraud

Während Phishing-Mails in der Regel von externen Absendern stammen, geben sich Cyberkriminelle beim CEO Fraud als Geschäftsführer (CEO, Chief Executive Officer) oder Vorgesetzter des eigenen Unternehmens aus.

Unter Verwendung dieser falschen Identität bitten sie den Mitarbeiter per E-Mail darum, seinen Benutzernamen und sein Passwort mitzuteilen oder weisen ihn an, hohe Geldbeträge zu überweisen. Solche E-Mails sind nur sehr schwer als „nicht echt“ zu identifizieren, da die Angreifer vorab das persönliche Umfeld der Zielperson äußerst gründlich ausspioniert und Firmeninterna recherchiert haben.

KASPERSKY lab

Simply Be Aware

Security Awareness Trainings

Öffnen Sie die Augen.

Es ist Zeit für Security Awareness.

Die Augen zu schließen, schützt Unternehmen nicht vor Bedrohungen.

Es ist heute wichtiger denn je, aktiv an das Thema IT-Sicherheit heranzutreten und das Bewusstsein für Cybersecurity auf allen Ebenen des Unternehmens zu stärken.

Denn umfassender IT-Schutz geht weit über den Einsatz von Sicherheitstechnologien hinaus. Zudem fällt er längst nicht mehr ausschließlich in den Zuständigkeitsbereich von IT-Abteilungen. Cybersicherheit ist zur Managementaufgabe geworden. Das bedeutet: Die Sensibilisierung aller Mitarbeiter sollte zentraler Teil des Security-Konzepts und der Unternehmensstrategie sein.
Jeder einzelne Mitarbeiter kann einen Teil zu mehr Sicherheit im Unternehmen beitragen.

Wie können Sie Security Awareness aufbauen?

Kaspersky Lab bietet spezielle Security Awareness Trainings an. Diese zeigen Mitarbeitern, wie sie mit den verschiedenen Sicherheitsbedrohungen im Arbeitsalltag richtig umgehen.

Die Online-Schulungen sensibilisieren die Teilnehmer für bestimmte Security-Themen. Ziel ist es, das Interesse an IT-Schutz zu wecken und Mitarbeiter zum aktiven Mitwirken zu bewegen.

1, 2, 3 ... Simply Be Aware

Cybersicherheit ist einfacher als Sie denken!
Das bieten die Online Security Awareness Trainings von Kaspersky Lab:

1 Einfaches Management & effizientes Festlegen von Trainingszielen

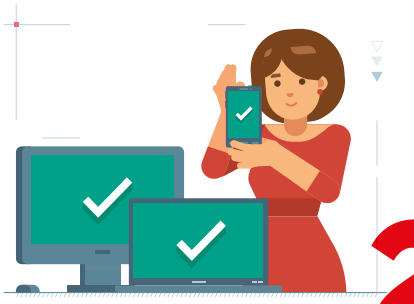
Einfache Implementierung und Verwaltung – auch ohne spezielle IT-Kenntnisse

Interaktive Online-Tools mit Bedrohungsszenarien aus dem Arbeitsalltag

Automatisiertes Lernmanagement mit auf den jeweiligen Mitarbeiter abgestimmten Lerninhalten

Trainingsziele anhand von globalen Benchmarks für individuelle Mitarbeiter, Gruppen oder Abteilungen

Keine Überforderung: Lernen im eigenen Tempo



2 Kurze, interaktive Lernmodule mit Inhalten aus dem Arbeitsalltag

Motivation durch spielerisches Lernen und Wettbewerb mit Kollegen

Verbindung von Lernen mit Spaß an persönlichen Erfolgserlebnissen

Etablierung eines sicheren Verhaltens in der realen Welt

Steigerung der Security Awareness in Unternehmen jeder Branche und Größe

3 Jederzeit Erfolge messen mit Reports und Analysen

Aussagekräftige Assessment-Funktionen zur Darstellung des Schulungserfolgs in Echtzeit

Anpassung von Schulungsmaßnahmen bei Gefahr, Trainingsziele nicht zu erreichen

Flexible Reaktionen auf den Schulungsverlauf einzelner Mitarbeiter

Jetzt Kaspersky Online-Schulungsplattformen testen!

Wählen Sie die passende Lösung aus:

Kaspersky Online Trainingsplattform

- mit bestehenden Trainingsplattformen kombinierbar (z.B. SCORM)
- Lerninhalte unternehmensspezifisch anpassbar
- ideal für Unternehmen mit individuellen Schulungsanforderungen

Kaspersky Automated Security Awareness Platform

- vorkonfigurierte Trainings
- besonders einfaches Management
- ideal für Unternehmen, die sofort starten möchten

www.kaspersky.de

Kaspersky Lab
Cybersicherheit für Unternehmen:
www.kaspersky.de/enterprise
Kaspersky Security Awareness **www.kaspersky.de/awareness**
Simply Be Aware: **www.kaspersky.de/awareness/trendpaper**