Kaspersky® Security Awareness

Der Faktor Mensch in der Cybersecurity eines Unternehmens

In den letzten Jahren haben die meisten Unternehmen moderne Phishing-Filter und Firewalls installiert und nutzen Expertentools zur Abwehr von Cyberbedrohungen. Deshalb konzentrieren sich Cyberkriminelle vermehrt auf die Mitarbeiter eines Unternehmens als potentielle Schwachstelle. Denn das Ausnutzen verbreiteter Wissenslücken bei vielen Benutzern ist oft der einfachste Weg, in die IT-Infrastruktur einzudringen.

Einer Umfrage[1] von Kaspersky Lab und B2B International zufolge sehen **52 %** der Unternehmen in ihren Mitarbeitern das größte Risiko für ihre IT-Sicherheit, da sie die IT-Sicherheitsstrategie durch fahrlässiges Handeln oder mangelnde Kenntnisse gefährden.

Unternehmen befürchten vor allem, dass Mitarbeiter unangemessene Daten über ihre mobilen Geräte weitergeben (47 %), durch den physischen Verlust mobiler Geräte das Unternehmen Risiken aussetzen (46 %) sowie IT-Ressourcen unsachgemäß nutzen (44 %).

Bei näherer Betrachtung dieser Ergebnisse variieren diese Bedenken hinsichtlich einer unsachgemäßen Nutzung von IT-Ressourcen durch Mitarbeiter je nach Unternehmensgröße erheblich: Sehr kleine Unternehmen (1 bis 49 Mitarbeiter) fühlen sich durch diesen Punkt stärker bedroht als Unternehmen mit mehr als 1000 Mitarbeitern. Dies könnte mit verschiedenen Faktoren zusammenhängen, etwa, dass Großunternehmen striktere Richtlinien definieren und ihre Mitarbeiter besser schulen.

Menschliche Fehler: die Hauptursache von Cybervorfällen

Aus dem Cyber Security Intelligence Index von IBM geht hervor, dass mehr als 90 % aller Sicherheitsvorfälle auf menschliche Fehler zurückzuführen sind. So werden beispielsweise Links angeklickt, die zu Phishing-Seiten führen, oder bösartige Webseiten aufgerufen, hinter denen Viren und andere hochentwickelte, hartnäckige Bedrohungen lauern.

Die Umfrage von Kaspersky Lab und B2B International aus dem Jahr 2017[1] stützt diese Erkenntnisse. Diesem Bericht zufolge spielte die unsachgemäße Nutzung von IT-Ressourcen durch Mitarbeiter – ein bekannter Faktor menschlichen Versagens bei 39 % aller Angriffe, von denen Unternehmen weltweit über einen Zeitraum von 12 Monaten betroffen waren, keine unerhebliche Rolle.

Die Zunahme der Cybervorfälle, die sich auf menschliches Versagen zurückführen lassen, ist vor allem bei sehr kleinen Unternehmen deutlich: In nur einem Jahr stieg der Anteil kleiner Unternehmen (1–49 Mitarbeiter), deren Mitarbeiter Opfer von Angriffen wurden, von 25 auf 32 %.

Besonders besorgniserregend ist, dass fast die Hälfte aller Unternehmen (44–48 %) der Meinung ist, nicht ausreichend vor Risiken durch Unwissenheit, Naivität und Arglist ihrer eigenen Mitarbeiter geschützt zu sein.

Unternehmen nannten zudem unvorsichtige und unwissende Mitarbeiter als zweitwichtigste Ursache von Vorfällen: 46 % der Befragten nannten diesen Punkt als Hauptfaktor bei Sicherheitsvorfällen. Ja, Mitarbeiter sind für Angreifer das wichtigste Einfallstor ins Unternehmen. Doch gut informierte und geschulte Mitarbeiter, die über Cybersicherheitskompetenzen verfügen und sich der Cyberbedrohungen bewusst sind, können einen wichtigen Beitrag zur Abwehr leisten.

1 Der menschliche Faktor in der IT-Sicherheit: Wenn Mitarbeiter zum Risikofaktor werden – Juni 2017

Durchschnittliche finanzielle Folgen des Fehlverhaltens von unachtsamen/unwissenden Mitarbeitern[1]

Für kleine/mittlere Unternehmen
- Unangemessene Weitergabe von Daten – 88 000 $
- Verlust von Mobilgeräten, durch die Unternehmen Risiken ausgesetzt werden – 99 000 $
- Verlust von Geräten oder Medien, die Daten enthalten – 81 000 $
- Unsachgemäße Nutzung von IT-Ressourcen durch Mitarbeiter – 68 000 $

Für Großunternehmen
- Vorfälle mit „non-computing", angeschlossenen Geräten – 1,6 Mio. $
- Verlust von Geräten oder Medien, die Daten enthalten – 1,1 Mio. $
- Unsachgemäße Nutzung von IT-Ressourcen durch Mitarbeiter – 581 000 $
- Unangemessene Freigabe von Daten über Mobilgeräte – 464 000 $

Datenschutzverletzungen in Zahlen[2]:
- 61 % der Opfer von Datenschutzverletzungen im Jahr 2017 waren Unternehmen mit unter 1000 Mitarbeitern
- 81 % der Hacker machten sich für einen Angriff gestohlene Passwörter und/oder schwache oder leicht zu erratende Passwörter zunutze
- 43 % der Datenschutzverletzungen erfolgten über soziale Netzwerke
- 66 % der Malware wurde über schädliche E-Mail-Anhänge installiert

1. „Global IT Security Risks Survey 2017". Kaspersky Lab und B2B International
2. „2017 Data Breach Investigations Report" Verizon

Effektives Sicherheitsbewusstsein

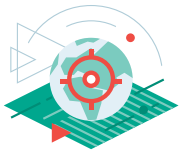
Mitarbeiterschulungen sind essentiell, um das Sicherheitsbewusstsein der Mitarbeiter zu steigern und sie zu motivieren, auf Cyberbedrohungen und Abwehrmaßnahmen zu achten, selbst wenn das nicht Teil ihrer Kernaufgaben ist.

Leider sind viele Sicherheitsschulungen alles andere als effektiv. Alle Sicherheitsrichtlinien wurden umgesetzt, die neuesten Erkenntnisse zu Malware und Schutzmaßnahmen stehen zur Verfügung – und doch führen die Schulungen nicht zu den gewünschten Ergebnissen. Woran liegt das?

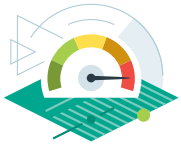
Sicherheitsschulungen werden allzu oft mit halbtäglichen Pflichtveranstaltungen am Computer assoziiert. Man tut so, als würde man aufmerksam zuhören, konzentriert sich aber vor allem auf das eigene Smartphone. Diese Schulungen werden natürlich als reine Zeitverschwendung abgetan und niemand ändert dadurch sein Verhalten.

Sicherheitsschulungen können sich auch dann als unwirksam erweisen, wenn die Mitarbeiter unzählige Anweisungen einhalten und befolgen sollen. Auf diese Weise werden sie sich anschließend nur an wenige Aspekte erinnern und dem Thema keine weitere Aufmerksamkeit schenken.

Für effektive Sicherheitsschulungen sind vier wichtige Punkte zu beachten:



Schulungsziele festlegen und Schulungsprogramme erklären
- Geben Sie Ziele vor, die anhand umfassender Benchmarks überprüft werden.
- Schaffen Sie ein Gleichgewicht zwischen den Sicherheitskompetenzen, über die jede Mitarbeitergruppe verfügen sollte, und der Zeit, die dafür benötigt wird.



Stellen Sie sicher, dass alle Mitarbeiter mindestens ihr persönliches Kompetenzziel erreichen
- Verwenden Sie das automatisierte Schulungsmanagement, mit dem alle Mitarbeiter die Sicherheitskompetenzen erreichen, die für ihr jeweiliges Risikoprofil erforderlich sind.
- Stellen Sie sicher, dass erworbenes Wissen vertieft wird, damit es fest im Gedächtnis verankert ist.
- Berücksichtigen Sie die jeweiligen Anforderungen der Mitarbeiter und schulen Sie sie in ihrem eigenen Tempo.

Fortschritte mit praktisch umsetzbaren Berichten und Analysen überwachen
- Behalten Sie den Überblick über Live-Daten, Trends und Prognosen.
- Verwenden Sie Echtzeit-Prognosen, um die jährlichen Schulungsziele zu erreichen.
- Räumen Sie Schwierigkeiten aus dem Weg, bevor daraus Probleme werden (z. B. indem Sie sich einen Überblick darüber verschaffen, welche Unternehmensbereiche besondere Aufmerksamkeit erfordern).
- Unterziehen Sie Zwischenergebnisse anhand von Benchmarks einer eingehenden Analyse.

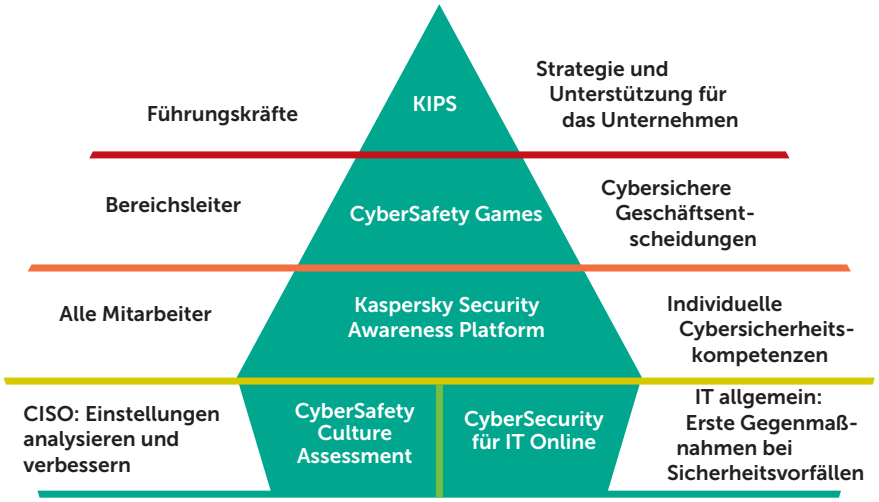
Schulungen attraktiv gestalten, damit vermitteltes Wissen auch wirklich verinnerlicht wird
- Motivieren Sie Ihre Mitarbeiter in Schulungen durch Planspiele und Wettbewerbe.
- Sorgen Sie dafür, dass sich die Schulungen am Alltag der Teilnehmer orientieren.
- Bieten Sie eine Möglichkeit, individuelle Ergebnisse mit den Ergebnissen von anderen zu vergleichen.
- Überschütten Sie die Teilnehmer nicht mit Informationen.

Es ist wichtig, die Grundlagen des Lern- und Lehrprozesses zu verstehen, um ein effektives Schulungsprogramm zu entwickeln.

Wir bei Kaspersky Lab bieten eine Reihe computergestützter Schulungsprodukte an, die moderne Lerntechniken anwenden und sich an alle Ebenen innerhalb der Unternehmensstruktur richten. Unsere Programme vermitteln nicht nur Wissen, sondern etablieren neue Verhaltensmuster – das eigentliche Ziel von Sicherheitsschulungen.

Der ganzheitliche Ansatz von Kaspersky Lab basiert auf modernen Lerntechniken, kombiniert mit Planspielen, Praxisbezug, Gruppendynamik und Vertiefungsübungen. Vor allem der Spielaspekt („Gamification") ist entscheidend, da sich dadurch sowohl Einstellungen als auch Verhaltensmuster verändern lassen. Durch emotionale Assoziationen steigt zudem die Lernmotivation.

Kaspersky Security Awareness-Schulungen



Ein Ansatz, der nachweislich Ergebnisse liefert

Bis zu

90 %

weniger Vorfälle insgesamt

Mindestens

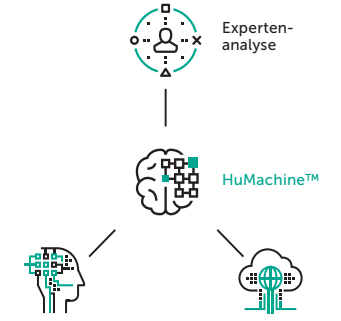
50 %

geringere finanzielle Einbußen durch Vorfälle

Erstaunliche

86 %

der Teilnehmer würden das Programm definitiv weiterempfehlen



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**
Kaspersky Security Awareness **www.kaspersky.com/awareness**

#truecybersecurity
#HuMachine

www.kaspersky.de