KASPERSKY lab

Kaspersky Security Awareness

Schulungsprogramme in Form von Planspielen für alle Unternehmensebenen

www.kaspersky.de
#truecybersecurity

Ein effektiver Weg zum Aufbau von Cybersicherheit im gesamten Unternehmen

Über 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. Es kostet Unternehmen Millionen, sich von Vorfällen mit Mitarbeiterbeteiligung zu erholen. Leider ist die Effektivität herkömmlicher Schulungsprogramme zur Vermeidung dieser Probleme beschränkt. Sie führen in der Regel nicht zum gewünschten Verhalten und zur gewünschten Motivation.

Unbeabsichtigte Fehler von Mitarbeitern sind den heutigen Unternehmen die häufigste Ursache für Vorfälle im Bereich Cybersicherheit:

- IBM meldete 2015, dass der Anteil interner **Sicherheitsverletzungen aufgrund menschlicher Fehler bei mehr als 95 %**[1] liegt.
- **75 % der großen Unternehmen in Großbritannien** und 31 % der kleinen Unternehmen **haben** 2015[2] vom Personal verursachte Sicherheitsverletzungen erlebt.
- **Die durchschnittlichen finanziellen Auswirkungen** eines Vorfalls aufgrund von unbedachtem Handeln belaufen sich auf **865 000 Dollar pro Sicherheitsverletzung**[3].
- **Die durchschnittlichen Kosten von Phishing-Angriffen betragen bis zu 400 Dollar pro Mitarbeiter und Jahr** (andere Arten von Cyberbedrohungen sind bei dieser Aufstellung ausgenommen)[4].
- Die Absicherung gegen Vorfälle aufgrund menschlicher Fehler, Irrtümer und Fahrlässigkeit **erfolgt nur zu 25 % durch Cyberversicherungen** (während Risiken durch externe Cyberkriminelle zu 84 % und Risiken durch böswillige oder kriminelle Insider zu 75 % abgedeckt werden)[5].

Analysen haben gezeigt, dass die Mehrzahl der existierenden Cyber Security Awareness-Schulungsprogramme ineffektiv ist:

- Das Lesen von Richtliniendokumenten und Anweisungen ist langweilig, zu technisch und zu skeptisch (zu viele Bedrohungen und Verbote), ohne dass Beispiele für sicheres Verhalten gegeben werden.
- Die Mitarbeiter werden nicht zum Lernen motiviert (nur 22 % glauben, dass sie zum Ziel Krimineller werden könnten).
- Mitarbeiter sehen sich beim Thema IT-Sicherheit nicht als Partner und versuchen ständig, diese zu umgehen.
- Mit Ausnahme der Zählung geschulter Personen erfolgt keine Messung des Sicherheitsbewusstseins.

1 IBM 2015 Cyber Security Intelligence Index.

2 Information Security Breaches Survey 2015. HM Government in Zusammenarbeit mit InfoSecurity Europe und PwC.

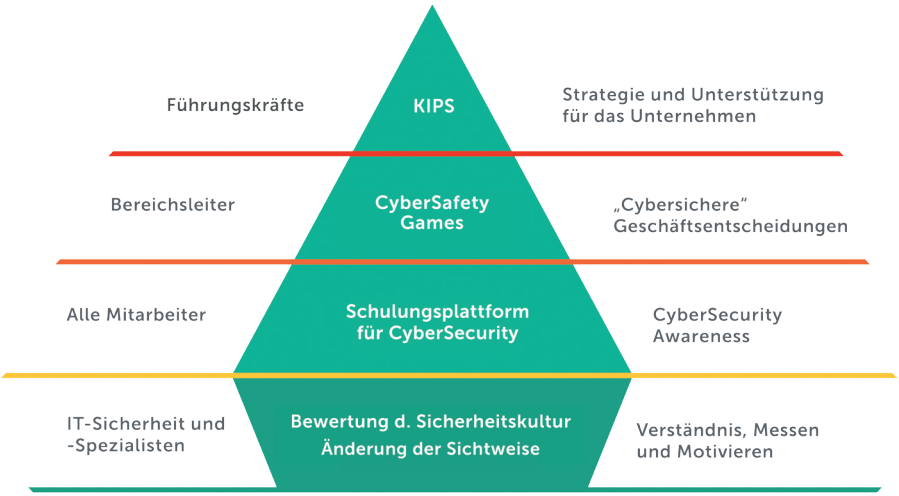
3 „Wahrnehmung der IT-Sicherheit: Der unausweichliche Ernstfall", Kaspersky Lab, 2016.

4 Die Berechnungen basieren auf der Veröffentlichung „Cost of Phishing and Value of Employee Training" des Ponemon Institute vom August 2015.

5 Global Cyber Impact Report 2015. Ponemon Institute LLC.

Vorzüge und Vorteile des Programms

Kaspersky Lab hat eine Reihe von computerbasierten Schulungsprodukten auf den Markt gebracht, die auf modernen Lerntechniken basieren und an sämtliche Unternehmensebenen gerichtet sind. Unser Schulungsprogramm hat seine



Effektivität bereits unter Beweis gestellt.

Das Kaspersky Security Awareness-Portfolio ist ideal auf die Ziele und Anforderungen eines Unternehmens ausgelegt:

- **Entwicklung von Verhaltensweisen statt einer reinen Wissensvermittlung**: Dieser Lernansatz beruht auf Planspielen mit praktischem Lernen, simulierten Angriffen usw. Das Ergebnis sind fest verankerte Verhaltensweisen mit einem langfristigen Effekt.
- Das Programm sorgt für **spezifisches Verhalten auf verschiedenen Unternehmensebenen**: Leitende Manager, Bereichsleiter/mittleres Management, Mitarbeiter – das Programm berücksichtigt die individuellen Anforderungen, sowie die zeitlichen und Formatbeschränkungen.
- **Hochgradig messbar und einfach zu verwalten** durch Computerunterstützung. Kann von der IT-Sicherheit oder von Personalteams verwaltet werden. Kaspersky Lab stellt bewährte Implementierungsmethoden, Best Practices und technischen Support bereit.
- Dieses Angebot ist durch umfassende **Erfahrungen von Kaspersky Lab im Bereich Cybersicherheit und durch Kapazitäten im Bereich Forschung und Entwicklung** abgedeckt.

KIPS als Grundlage für strategische Unterstützung

KIPS richtet sich an Experten für Geschäftssysteme, IT-Personal und Bereichsleiter. Es soll diese Zielgruppe auf Risiken und Sicherheitsprobleme moderner Computersysteme aufmerksam machen.

Kaspersky Interactive Protection Simulation (KIPS) ist ein Übungsszenario, bei dem Teams in eine simulierte Geschäftsumgebung versetzt werden, in der sie einer Reihe unerwarteter Cyberbedrohungen ausgesetzt werden, während die Teams versuchen, den Gewinn zu maximieren und das Vertrauen der Kunden zu erhalten. Die Idee besteht darin, durch Auswahl der besten verfügbaren vorausschauenden und reaktionsschnellen Kontrollmöglichkeiten eine Cyberverteidigungsstrategie zu entwickeln.

Jede Reaktion der Teams auf die eintretenden Ereignisse verändert den Verlauf des Szenarios und damit den Gewinn bzw. den Verlust des Unternehmens. Mit einem ausgewogenen Verhältnis von Entwicklungs-, geschäftlichen und Sicherheitsprioritäten sowie den Kosten eines realistischen Cyberangriffs analysiert das Team Daten und trifft strategische Entscheidungen auf Basis unsicherer Informationen und begrenzter Ressourcen. Dieser Realitätsgrad ist beabsichtigt, da alle Szenarien auf realen Ereignissen basieren.

KIPS ist ein dynamisches Lehrprogramm, das auf praktischem Lernen basiert:

- Unterhaltsam, fesselnd und schnell (2 Stunden)
- Teamwork stärkt die Zusammenarbeit
- Wettbewerb fördert Initiative und Analysekompetenz
- Das Planspiel fördert das Verständnis von Cybersicherheitmaßnahmen

„Mit dieser Übung wird jedoch klar, dass einige der ersten und grundlegenden strategischen Entscheidungen, die man trifft (darunter Sicherheits-Audits und Trainings, Passwortänderungen und Patch Management) spätere Reaktionen auf Vorfälle erheblich vereinfachen."

Mark Jenkins · 16. Dezember 2015, ICT Qatar

Verfügbare Szenarien (als KIPS Live und KIPS Online in 10 Sprachen)

Unternehmen	Schutz des Unternehmens vor Ransomware, APTs und Fehlern in der Automatisierungssicherheit
Bank	Schutz von Finanzinstituten vor ausgefeilten APTs, die Geldautomaten, Verwaltungsserver und Geschäftssysteme angreifen.
E-Government	Schutz öffentlicher Webserver vor Angriffen und Exploits
Industrial	Schutz industrieller Steuerungssysteme und wichtiger Infrastrukturen

Jedes der Szenarien konzentriert sich auf die jeweiligen Bedrohungsvektoren. Auf diese Weise lassen sich die typischen Fehler beim Aufbau der Cybersicherheit ermitteln und analysieren und Reaktionsverfahren je Industriezweig entwickeln.

CyberSafety Games zur Gewährleistung sicherer Entscheidungen

Dieser hochgradig interaktive Workshop (eine Kombination aus computerunterstütztem und Frontalunterricht) motiviert die Manager hinsichtlich der Bedeutung von Cybersicherheit für ihre Aufgabenbereiche und bietet ihnen Kompetenz, Wissen und Verhaltensweisen, die für die Schaffung einer sicheren Arbeitsumgebung in ihren Abteilungen von grundlegender Bedeutung sind.

Unternehmen ergreifen Maßnahmen zur Abwehr von Cyberbedrohungen, indem sie IT-Sicherheitsstrukturen einrichten und Compliance-Schulungen abhalten. Aber reicht dies aus?

- Lässt sich das Verhalten der Mitarbeiter wirklich durch Wissen verändern, das in einer Schulung vermittelt wurde? Gibt es Alternativen?
- Muss die geschäftliche Effizienz zugunsten der Sicherheit geopfert werden?
- Haben die Sicherheitsbeauftragten das Gefühl, zu wenige zu sein, um Jahr für Jahr Cybersicherheit zu erzielen?

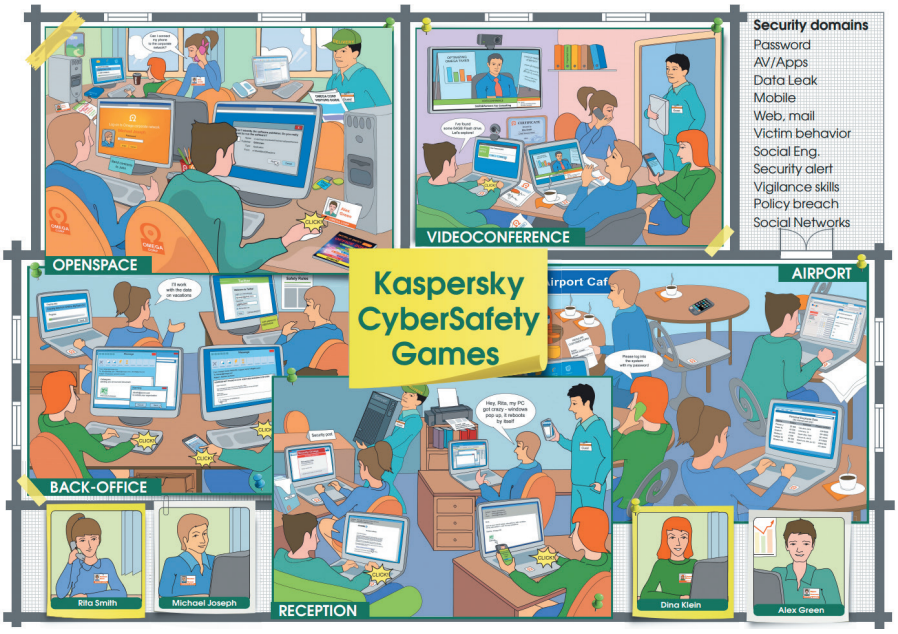
Diese Herausforderungen lassen sich nur bewältigen, wenn die **Bereichsleiter dafür gewonnen werden können, das Unternehmen cybersicher zu machen, ohne die Effizienz zu beeinträchtigen. Nur sie** interagieren täglich mit den Mitarbeitern und treffen geschäftliche Entscheidungen. Die Antwort liegt darin, Cybersicherheit zu einem unverzichtbaren Bestandteil der täglichen Entscheidungsfindung zu machen.

Kaspersky CyberSafety Management-Planspiele bieten Managern **Kompetenz, Wissen und Verhaltensweisen**, die für den Erhalt einer sicheren Arbeitsumgebung in ihrem Bereich von grundlegender Bedeutung sind:

- **Verständnis:** Verinnerlichung von einfachen, aber dennoch wichtigen Cybersicherheitsmaßnahmen
- **Überwachung:** Untersuchung der alltäglichen Arbeitsabläufe vom Standpunkt der Cybersicherheit
- **Sichere Entscheidungsfindung:** Cybersicherheit als integraler Bestandteil geschäftlicher Prozesse
- **Bestärkung und Inspiration:** Einflussreiche Führung und Unterstützung der Mitarbeiter durch fachlichen Rat

„Train the Trainer"-Lizenzierungen für Schulungszentren im Unternehmen, um wichtige Bereitstellungsvorteile zu erzielen:

- Einfache Bereitstellung: Ausbilder brauchen keine Sicherheitsexperten zu sein.
- Einfache Planung: Modulare, kurze Trainings können in den Zeitplan der Mitarbeiter integriert werden.



Die Plattform steht ab Februar 2017 in 27 Sprachen zur Verfügung.

Anhand der Plattform und basierend auf dem Best-Practices-Leitfaden von Kaspersky Lab kann ein Kunde einen effektiven, beständigen und messbaren Cybersicherheitsplan erarbeiten und umsetzen, bei dem die Mitarbeiter von einfachen zu komplizierten Lektionen geführt werden. Der Plan deckt verschiedene Sicherheitsbereiche ab, die der Bedrohungslandschaft und dem jeweiligen Kenntnisstand entsprechen.

Eine interaktive Demonstration finden Sie unter www.kaspersky.com/demo-sa!

Online-Trainingsplattform zum Aufbau von Fähigkeiten im Bereich Cyberhygiene

Gerade im Bereich der Cybersicherheit ist es sehr wichtig, dass Mitarbeiter regelmäßig geschult werden und typische Szenarien und Situationen potentieller Bedrohungen zu erkennen und mit ihnen umzugehen. Kaspersky Lab bietet Ihren Mitarbeitern dafür ein interaktives Lernportal.

Interaktive Schulungsmodule

- Unterhaltsam und kurz
- Basierend auf Übungen mit langfristigem Effekt
- Automatische Anmeldung zur Stärkung von Kompetenzen
- Mehr als 20 Module zur Abdeckung aller Sicherheitsbereiche

Skills Assessment

- Mit vordefinierten oder zufälligen Bewertungen, kundendefinierten Fragen und anpassbarer Länge
- Abdeckung verschiedener Sicherheitsbereiche
- Umfassende Fragenbibliothek und zufällige Fragenauswahl zur Vermeidung von Täuschversuchen

Simulierte Phishing-Angriffe

- Drei Arten von Phishing-Angriffen mit verschiedenen Schwierigkeitsstufen, basierend auf realen Fällen
- Praktischer Bezug bei jedem Öffnen einer Phishing-E-Mail
- Anpassbare Vorlagen
- Automatische Zuweisung zu Schulungsmodulen bei Nichtbestehen eines simulierten Angriffs

Berichte und Analysen

- Bereitstellung von Statistiken für das gesamte Unternehmen oder nach Abteilung, Standort, Position und individuell
- Überwachung der Mitarbeiterfähigkeiten und ihrer Dynamik
- Datenexport in verschiedene Formate oder auf das LMS des Kunden

Schwerpunkt

Die Bewertung beleuchtet die Sicherheitskultur aus verschiedenen Perspektiven:

- Organisationsebene (Management)
- Persönliche Ebene (Mitarbeiter)
- Verfügbares Fachwissen
- Sicherheitsmaßnahmen als Prozess

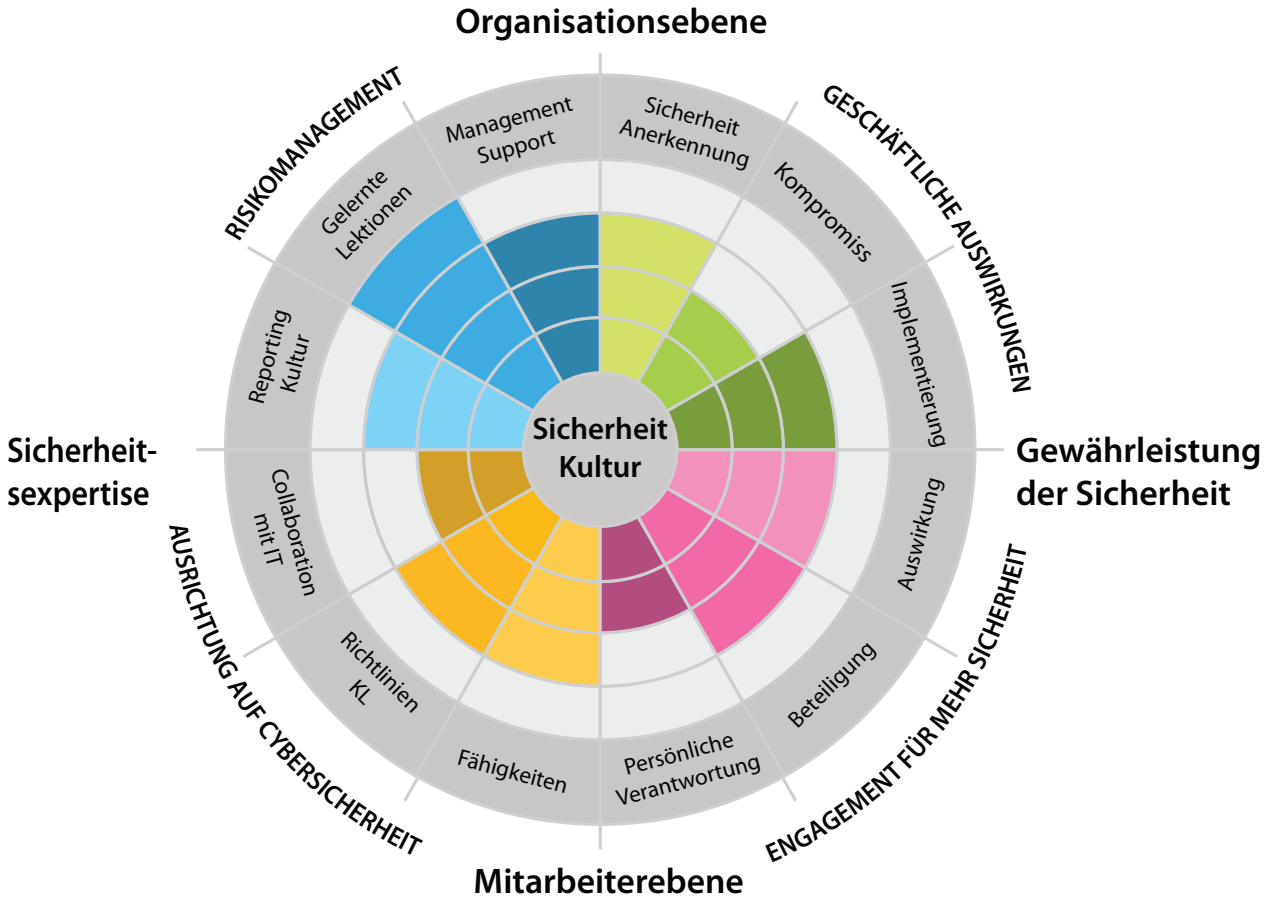
Security Assessment

In der Bewertung der „Cybersicherheitskultur" werden das tatsächliche Alltagsverhalten und die Einstellung zu Cybersicherheit auf allen Unternehmensebenen analysiert und aufgezeigt, wie Mitarbeiter Ihres Unternehmens die verschiedenen Aspekte der Cybersicherheit wahrnehmen.

Mit den Bewertungsergebnissen können Ungleichgewichte und Schwerpunktbereiche ausgearbeitet werden. Weiterhin können Prioritäten der internen und externen Aktivitäten der Sicherheitsabteilung, darunter Bewusstsein und Schulungen, interne PR und Informationsverbreitung sowie Zusammenarbeitsprinzipien im Geschäftsleben, fundiert und ausgerichtet werden.

Die Cybersicherheitskultur umfasst Bereiche, die unternehmensweit als Ganzes bewertet und gemessen werden. Die Bewertungsergebnisse bilden die Gesprächsgrundlage für die Rolle der Cybersicherheit bei der Unterstützung der Unternehmenseffizienz:

- Einstellung zu Cybersicherheit (Wahrnehmung von Sicherheit und Richtlinien)
- Risikomanagement (Anleitung, Feedback, Verbesserungen)
- Engagement (Einstellung und Verhalten zum Thema Sicherheit)
- Auswirkungen auf das Unternehmen (Gleichgewicht zwischen Sicherheit und Unternehmenseffizienz)



Beachten Sie, dass der Bericht zur Cybersicherheitskultur keine Bewertung des technischen Reifegrads des Unternehmens und kein Maß für die Wirksamkeit der Sicherheitsabteilung ist.

Der Bericht zur Cybersicherheitskultur zeigt auf, wie durchschnittliche Mitarbeiter Cybersicherheit für sich wahrnehmen, was sie über die Kultur, Gewohnheiten und tägliche Vorgehensweisen zu den Aspekten der Cybersicherheit denken und wie sie die verschiedenen Aspekte der Absicherungskultur vor Cyberbedrohungen persönlich wahrnehmen. Diese Wahrnehmung ist das Ergebnis verschiedener Unternehmenspraktiken und -einheiten und nicht nur das Ergebnis der Aktivitäten der Sicherheits- oder Risikomanagementabteilung.

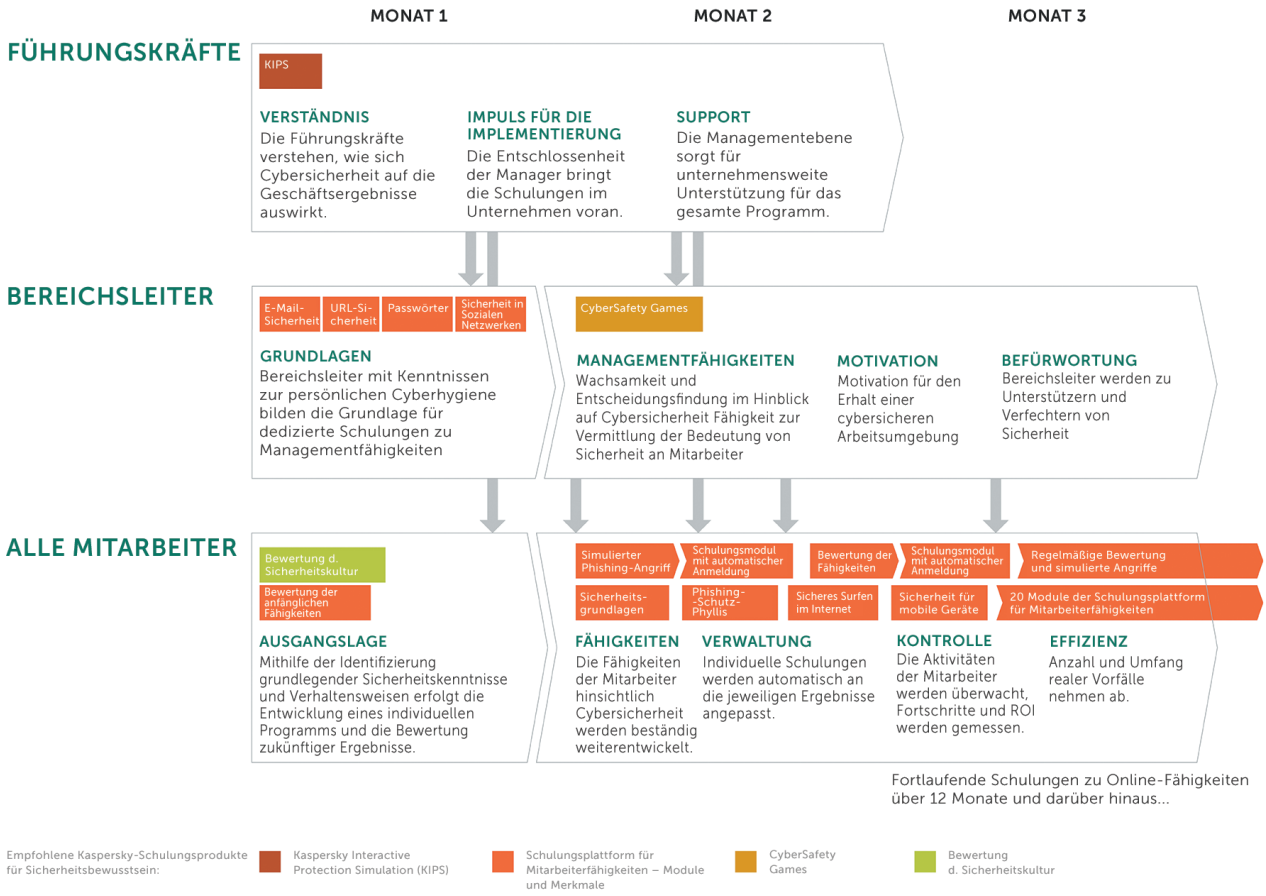
Die Bewertung erfolgt in Form einer Cloud-basierten Umfrage. Ein Mitarbeiter benötigt hierfür ca. 15 Minuten. Die Durchführung der Umfrage für alle Mitarbeiter nimmt im Durchschnitt zwei Wochen in Anspruch.

Nach Abschluss der Umfrage erhält der Kunde einen konsolidierten Bericht.

Implementierungsmethode: Schneller Start und kumulativer Effekt

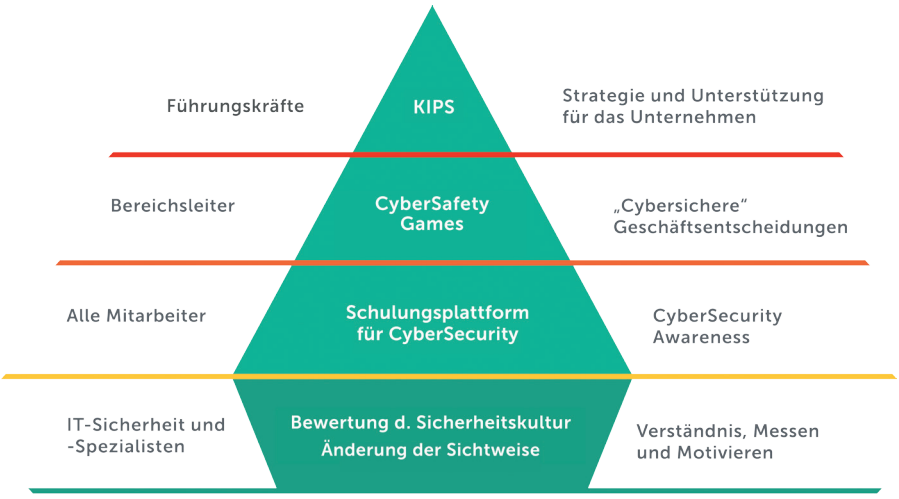
Es folgt eine Beschreibung der empfohlenen Reihenfolge zur Mitarbeiterschulung mit Kaspersky Security Awareness-Produkten (Der „Best Practice-Leitfaden" steht unseren Kunden ebenfalls zur Verfügung). Wir bieten Kunden detaillierte Anweisungen und methodische Unterstützung. Auf diese Weise wird sichergestellt, dass unsere Schulungsprodukte einfach implementierbar und handhabbar sind und Kunden den optimalen Nutzen aus ihnen ziehen können.

Kumulativer Effekt – jedes Training unterstützt die anderen



Kaspersky-Schulungsprodukte für Sicherheitsbewusstsein

Die KIPS-Schulung ist ein Teil des Portfolios von Kaspersky Lab zum Thema Sicherheitsbewusstsein, das auf CyberSafety Culture-Methoden beruht. Cyber Safety Culture-Entwicklung durch verschiedene Trainings mit Spielcharakter für alle Ebenen der Unternehmensstruktur, verwaltet durch Sicherheits- und Personalteams.



Umfassend, aber einfach und verständlich

- Zahlreiche Sicherheitsaspekte
- Vertraute Umgebungen
- Fesselnder Schulungsprozess
- Praktische Übungen
- Sprache geeignet für Nicht-IT-Mitarbeiter

Geschäftsvorteile

ganze
93 %
Wahrscheinlichkeit der Anwendung des Wissens in der täglichen Arbeit

bis
90 %
weniger Vorfälle

50–60 %
geringeres monetäres Cyberrisiko

mehr als
30-fache
Rendite für Investition in Sensibilisierung

www.kaspersky.de

Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Kaspersky Security Awareness: **https://www.kaspersky.de/enterprise-security/security-awareness**
Produktdemo: **https://www.kaspersky.de/enterprise-security/cybersecurity-awareness/demo/**