Kaspersky
Security
Awareness

Sicherheitskultur als Fundament für nachhaltigen Erfolg

kaspersky cybersecurity
true to business

Menschliche Fehler

zählen zu den größten Bedrohungen. Im Durchschnitt gehen 64–68 % aller Sicherheitsvorfälle auf unbeabsichtigte menschliche Handlungen zurück.[1]

4,4 Millionen USD

sind die durchschnittlichen Kosten einer Datenschutzverletzung pro Unternehmen[2]

Vorschriften erfordern Security Awareness

als Bestandteil der Compliance: PCI DSS, ISO/IEC 27001, DSGVO, NIS 2 und weitere Regelwerke fordern oder empfehlen ausdrücklich Security-Awareness-Programme zum Schutz sensibler Daten.

Eine sicherheitsbewusste Unternehmenskultur zahlt sich aus

Untersuchungsergebnisse von Kaspersky zeigen, dass über 85 % der Mitarbeitenden, die ein Awareness-Training absolviert haben, von erhöhter Wachsamkeit und Vorsicht berichten. Diese Verhaltensänderung trägt dazu bei, Sicherheitsvorfälle zu verhindern.

92 %

der Benutzer würden Kaspersky Security Awareness weiterempfehlen

3 Millionen

Mitarbeiter haben unsere Schulungsprogramme erfolgreich abgeschlossen.

Über 160

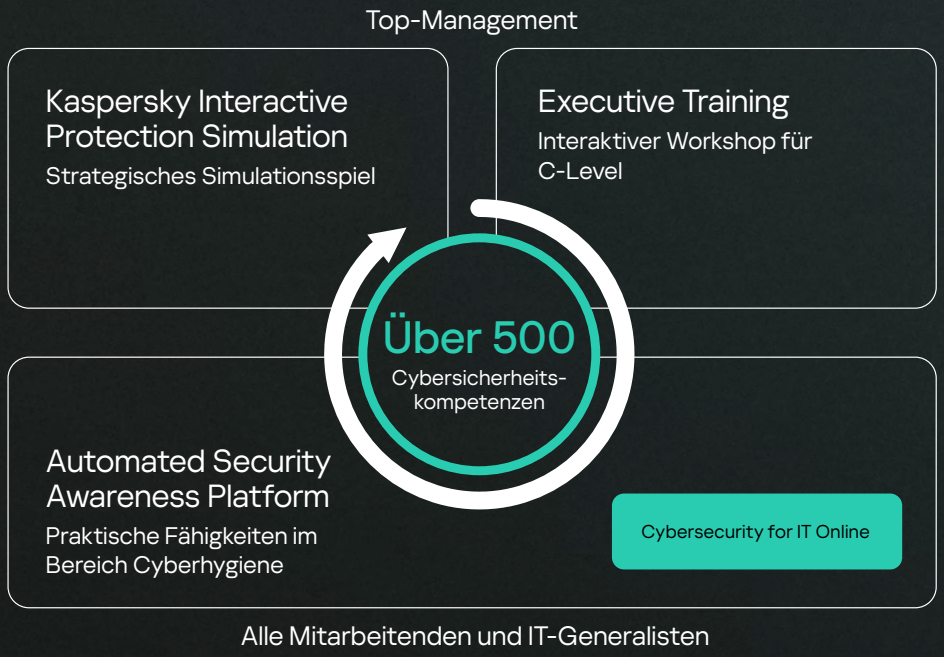
Länder, in denen Unternehmen ihre Mitarbeitenden mit unseren Schulungslösungen schützen

Effektiver Ansatz zur Einschränkung menschlicher Cyberrisiken

Schaffen Sie eine Sicherheitskultur im gesamten Unternehmen, die auf sicherem Verhalten im Umgang mit digitalen Systemen basiert und durch fundiertes Cybersecurity-Bewusstsein sowie praktische Fähigkeiten unterstützt wird. So lässt sich die Zahl der Vorfälle durch menschliche Fehler deutlich reduzieren. Um den menschlichen Faktor erfolgreich zu bewältigen, ist ein strukturiertes Schulungsprogramm, das relevante, aktuelle Inhalte mit modernen Lernmethoden und Technologien kombiniert, der wirksamste Ansatz.

Kaspersky Security Awareness-Lösungen

Kaspersky Security Awareness unterstützt Unternehmen weltweit dabei, die Cyberkompetenz ihrer Mitarbeitenden zu stärken und eine Kultur zu fördern, in der Sicherheit als gemeinsame Verantwortung gilt. Nachhaltige Verhaltensänderungen brauchen Zeit. Deshalb basiert unser Ansatz auf einem kontinuierlichen Lernzyklus mit verschiedenen Tools und unterstützenden Maßnahmen: Kaspersky Interactive Protection Simulation, Executive Training, Automated Security Awareness Platform sowie Cybersecurity for IT Online.



Warum Kunden sich für Kaspersky Security Awareness entscheiden

Kompetenzen und Sicherheit, um reale Bedrohungen zu erkennen und darauf zu reagieren

Auf Basis von fast 30 Jahren Cybersecurity-Expertise von Kaspersky und aktueller Bedrohungsdaten entwickeln wir hochrelevante Schulungsinhalte. Mit dem Auftreten neuer Bedrohungen entwickeln sich auch unsere Inhalte weiter – so sind Ihre Mitarbeitenden jederzeit bestens vorbereitet.

Nachhaltige Verhaltensänderungen

Unsere Methodik festigt neue Kompetenzen, sorgt für kontinuierliche Motivation und hilft, Lerninhalte dauerhaft in den Arbeitsalltag zu integrieren. Das Ergebnis ist eine nachhaltige Verhaltensänderung: Sichere Verhaltensweisen werden zur Selbstverständlichkeit.

Leicht zugängliches, interaktives Lernen

Unsere Schulungen setzen auf interaktives Lernen mit klarer, logischer Struktur. So können Mitarbeitende die Inhalte leichter mit ihren täglichen Aufgaben in Verbindung bringen. Verständnis und Anwendung in der Praxis verbessern sich.

Engagement über alle Ebenen

Von Führungskräften, die strategische, umsetzbare Einblicke benötigen, bis hin zu Mitarbeitenden an vorderster Front, die praktische Anleitung brauchen: Wir liefern die passenden Inhalte für jede Zielgruppe im richtigen Format.

1 Kaspersky Human Factor 360 Report, Cybersecurity Ventures, Verizon Data Breach Reports
2 Kosten einer Datenschutzverletzung, Bericht von IBM, 2025

Kaspersky Automated Security Awareness Platform: Aufbau einer menschlichen Firewall

Die Kaspersky Automated Security Awareness Platform (ASAP) ist ein Online-Tool für kontinuierliche Schulungen. Es stattet Mitarbeitende mit den notwendigen Kompetenzen und Kenntnissen aus, um reale Angriffsvektoren zu erkennen und zu verhindern.

Entwickelt von führenden Expertinnen und Experten: Kaspersky ASAP unterstützt Ihre Mitarbeitenden und stärkt Ihr Unternehmen.

Reduziert die Zahl menschlicher Fehler sowie daraus entstehende finanzielle und reputationsbezogene Schäden

Minimieren Sie das Risiko von Bußgeldern wegen Nichteinhaltung gesetzlicher Vorschriften, indem Sie die regulatorischen Anforderungen erfüllen.

Reduziert den Zeit- und Arbeitsaufwand für die Verwaltung von Awareness-Trainings und entlastet IT-Teams

Kaspersky ASAP ist mehr als bloß ein Anti-Phishing-Tool. Die Schulungen orientieren sich an den MITRE ATT&CK-Techniken und zeigen, welche menschlich bedingten Angriffsvektoren Mitarbeitende verhindern können. Im Folgenden finden Sie einige Beispiele:

MITRE-Technik	Threat	Kompetenzen und Verhaltensweisen
T1566 – Phishing	Schädliche E-Mails	Phishing-Versuche erkennen und melden
T1585 – Konteneinrichtung	Gefälschte Konten/Profile	Authentizität von Informationen vor der Weitergabe verifizieren
T1199 – Vertrauensbeziehung	Ausnutzung von Vertrauensbeziehungen	Ungewöhnliche Anfragen kritisch prüfen
T1091 – Replizierung über Wechseldatenträger	Wechselmedien	Malware-Gefahren auf USB-Geräten verstehen
T1078 – Gültige Konten	Diebstahl von Zugangsdaten	Zugriff durch Social Engineering verhindern

95 %

von geschulten Mitarbeitern können nun Phishing-Angriffe erkennen

20-mal

weniger Datenverstöße durch regelmäßige Mitarbeiterschulung[1]

Zu den wichtigsten in ASAP behandelten Themen gehören:

- E-Mail
- Passwörter und Konten
- Websites und Internet
- PC-Sicherheit
- Vertrauliche Daten
- Personenbezogene Daten
- Physische Datensicherheit
- DSGVO
- KI und neuronale Netzwerke
- Angriffe auf Top-Manager
- Mobilgeräte
- Social Media & Messenger
- Angriffe auf die Lieferkette
- Industrial Cybersecurity
- Sicherheit von Bankkarten und PCI DSS
- Reaktion auf Vorfälle
- Vishing

Machen Sie Ihre Mitarbeitenden zu einer weiteren Schutzebene zusätzlich zu Ihren technischen Lösungen.

Testversion starten

1 2025 Kaspersky Automated Security Awareness Platform Research

Inhalte und Methoden, die im Gedächtnis bleiben – damit Wissen erhalten bleibt und Fähigkeiten angewendet werden

Von Experten gesteuert

Die Inhalte basieren auf fast 30 Jahren Cybersecurity-Expertise sowie einem Kompetenzmodell, das grundlegende Cybersecurity-Fähigkeiten aus verschiedenen Themenbereichen praxisnah abdeckt.

Vielfältige Inhalte

Sichert den Lernerfolg durch interaktive Module, Übungen, praxisnahe Beispiele, Tests, Videos sowie Phishing-Simulationen mit mehreren Szenarien

Breite Palette an Optionen

Fügen Sie Ihr Logo und Ihre Zertifizierungen hinzu, ergänzen Sie Schulungen mit internen Präsentationen, Dokumenten und Richtlinien, integrieren Sie eigene SCORM- oder PDF-Module und passen Sie Teststrukturen an.

Auf gehirngerechtes Lernen ausgelegt

Konzipiert nach den Prinzipien der Informationsaufnahme, -verarbeitung und -anwendung

Funktionsweise

Alle in Ihrem Unternehmen benötigen Cybersicherheits-Bewusstsein – doch Umfang und Tiefe des Wissens variieren je nach Rolle und Risikoprofil. Hier scheitert ein One-Size-fits-all-Training. Unsere Plattform unterstützt Ihr Team dabei, mehr als 500 praxisnahe Fähigkeiten aufzubauen. Darüber hinaus können Sie Mitarbeitende effizient gruppieren und mit nur wenigen Klicks die passenden Schulungen zuweisen.

Hauptkurs

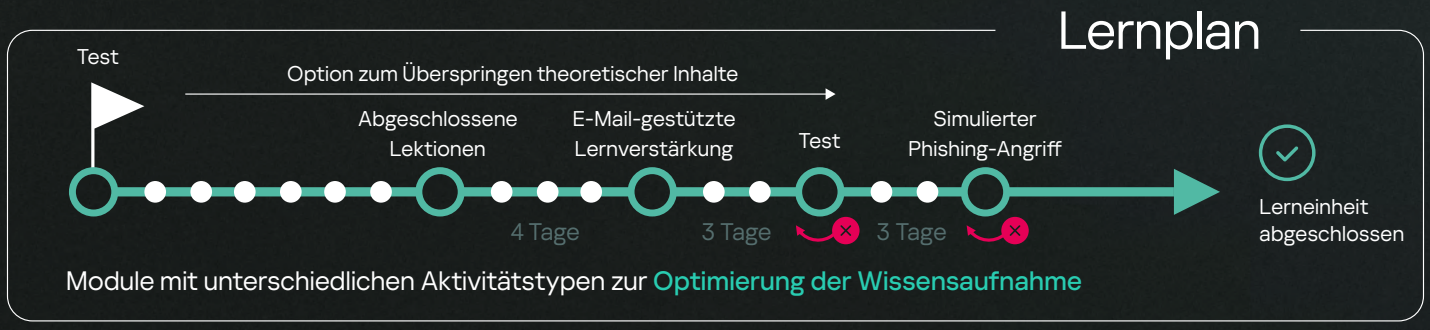
Erwerben Sie fundiertes Wissen durch Mikro-Lektionen, die nach Schwierigkeitsgrad strukturiert sind.

Express-Kurs

Erfüllen Sie Schulungsanforderungen im Bereich Cybersecurity schnell – oder frischen Sie Ihr Wissen mit kurzen, motivierenden Audio-Video-Trainings auf.

Phishing-Simulator

Führen Sie simulierte Phishing-Angriffe vor, während und nach der Schulung durch, um die Fähigkeit Ihrer Mitarbeitenden in Bezug auf die Abwehr von Cyberangriffen zu testen.



Module mit unterschiedlichen Aktivitätstypen zur Optimierung der Wissensaufnahme

Effiziente, einfach zu verwaltende Schulungen für Unternehmen jeder Größe

Einfaches Onboarding

Registrieren Sie sich online und erhalten Sie Demo-Zugriff für bis zu fünf Nutzer für zwei Monate. Umfasst einen Start-Leitfaden und Online-Support

Vollständige Automatisierung

Trainingsmodule, Tests und Phishing-Simulationen werden automatisch zugewiesen – abgestimmt auf die Einstellungen der Trainingsgruppen.

Proaktives Management menschlicher Risiken

Die nahtlose Integration mit Kaspersky SIEM und XDR sowie APIs zur Anbindung von Drittanwendungen ermöglicht eine umfassende Sicht auf das Verhalten der Mitarbeitenden und die direkte Zuweisung von Schulungen auf Basis realer Sicherheitsvorfälle – direkt über die Konsole.

Mandantenfähigkeit und flexible Administratorrollen

Ideal für Organisationen mit Tochtergesellschaften und verteilten Teams: zentrale Steuerung bei gleichzeitiger Delegation der Verwaltung an lokale Administratoren

Automatisierte Benutzergruppierung auf Basis individuell definierter Regeln

Organisation nach Rolle, Abteilung oder Risikoprofil

Übersichtliches Reporting

Dashboards liefern zentrale Kennzahlen mit Drill-down-Ansichten zu Fortschritten, Verzögerungen oder Leistungsdefiziten einzelner Mitarbeitender. Per Klick lässt sich ein PDF-Bericht für das Management erstellen.

Flexibles Deployment

Verfügbar als SaaS-Plattform oder als On-Premises-Installation

Nahtlose Anmeldung

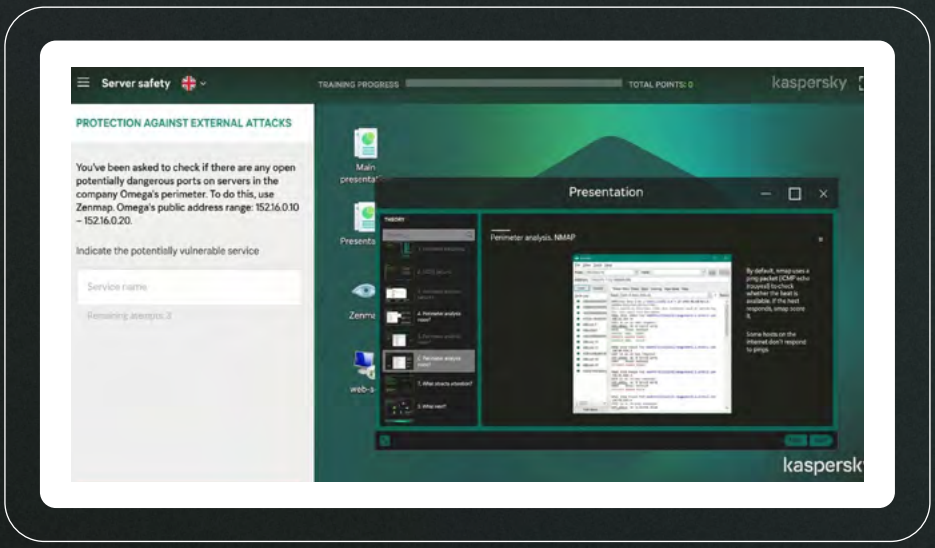
Integration mit Active Directory und SSO

Cybersecurity for IT Online

Cybersecurity for IT Online (CITO) ist ein interaktives Trainingsprogramm für Service-Desk-Spezialisten, Systemadministratoren und IT-Mitarbeitende ohne IT-Sicherheitsfokus. Es vermittelt praxisnahe Fähigkeiten, um versteckte Cyberangriffe in alltäglichen PC-Vorfällen zu erkennen, relevante Daten zu erfassen und als erste Verteidigungslinie zu agieren.

Praktische Fertigkeiten für die Erstreaktion bei Sicherheitsvorfällen:

- Lernen Sie, Malware, potenziell unerwünschte Programme, Exploits und Phishing-Angriffe zu erkennen, zu analysieren und darauf zu reagieren
- Nutzen Sie praktische Tools und Techniken zur Verstärkung der Sicherheit Ihrer IT-Infrastruktur und zur effektiven Untersuchung von Vorfällen
- Entwickeln Sie Fähigkeiten für die Analyse von Protokollen, die Erfassung digitaler Nachweise und die Untersuchung von Bedrohungen
- Lernen Sie, Server und Active Directory durch Härtung, Richtlinienkonfiguration und Monitoring abzusichern



Die Teilnehmenden durchlaufen sechs Module. Diese kombinieren kompakte Theorie, praxisnahe Tipps und jeweils 4–13 Übungen. Der Fokus liegt dabei auf auf realen IT-Sicherheitstools und typischen Alltagsaufgaben.

Schadsoftware	Potenziell unerwünschte Programme und Exploits	Server-Sicherheit
Grundlagen der Untersuchung	Phishing und Open Source Intelligence	Active Directory-Sicherheit

Kaspersky Executive Training

Fördern Sie eine Sicherheitskultur top-down. Zeigen Sie, wie Entscheidungen der Führungsebene die Risikolage, die Einhaltung regulatorischer Vorgaben und die langfristige Resilienz Ihres Unternehmens direkt beeinflussen.

Kaspersky Executive Training ist ein Live-Workshop für Geschäftsleitung und Top-Management. Sie erfahren, wie sich die aktuelle Bedrohungslage konkret auf Ihr Unternehmen auswirkt, welche Maßnahmen im Fall eines Cyberangriffs erforderlich sind und vieles mehr. Über die Cybersecurity-Grundlagen hinaus erhalten die Teilnehmenden wichtige Einblicke in die wirtschaftliche Tragfähigkeit von Sicherheitsinvestitionen. So können Entscheider auf C-Level Sicherheitsmaßnahmen gezielt mit Geschäftsergebnissen verknüpfen. Wir empfehlen die Kombination dieser Schulung mit KIPS.

Zentrale geschäftskritische Aspekte der Cybersicherheit – klar und allgemeinverständlich erklärt:

- Verstehen Sie Cybersicherheit als Bestandteil eines Gesamtsystems.
- Lernen Sie, wie Cyberrisiken Geschäftsprozesse gefährden und wie Sie ihnen wirksam begegnen.
- Verstehen Sie die Rolle der Unternehmensleitung in der Cybersicherheits-Governance.

Kaspersky Interactive Protection Simulation (KIPS): Cybersicherheit aus unternehmerischer Perspektive

KIPS schärft das Bewusstsein für die Risiken und Herausforderungen im Umgang mit verschiedensten IT-Systemen und Geschäftsprozessen. Es ist ein zweistündiges interaktives Teamspiel für Führungskräfte, Fachverantwortliche und IT-Experten. Branchenspezifische Szenarien konfrontieren die Teilnehmenden mit modernen Angriffstechniken, die Kaspersky-Experten in aktuellen Kampagnen beobachten – darunter Angriffe auf die Lieferkette, Ausnutzung von Drittzugängen, Social Engineering und Malware. Teams müssen unter Zeit- und Budgetdruck Strategien entwickeln, die Auswirkungen von Sicherheitsvorfällen abschätzen und effektiv reagieren, um Unternehmens-Performance und Umsatz zu schützen

Fördert ein gemeinsames Verständnis unter Entscheidungsträgern

Macht Cybersicherheitsrisiken sichtbar und verknüpft sie direkt mit Umsatz und operativen Abläufen

Bindet Teams aktiv in Cybersecurity-Themen ein und fördert eine sicherheitsorientierte Unternehmenskultur.

14 branchenbezogene Szenarien (Liste wird kontinuierlich erweitert)

- Flughafen
- Konzern
- Bank
- Öl & Gas
- Transportwesen
- Kraftwerk
- Wasserwerk
- Kommunalverwaltung
- Petrochemie
- Mineralölkonzern
- Kleine und mittlere Unternehmen
- Telekommunikation
- Technische Zuordnung
- IT

KIPS Live

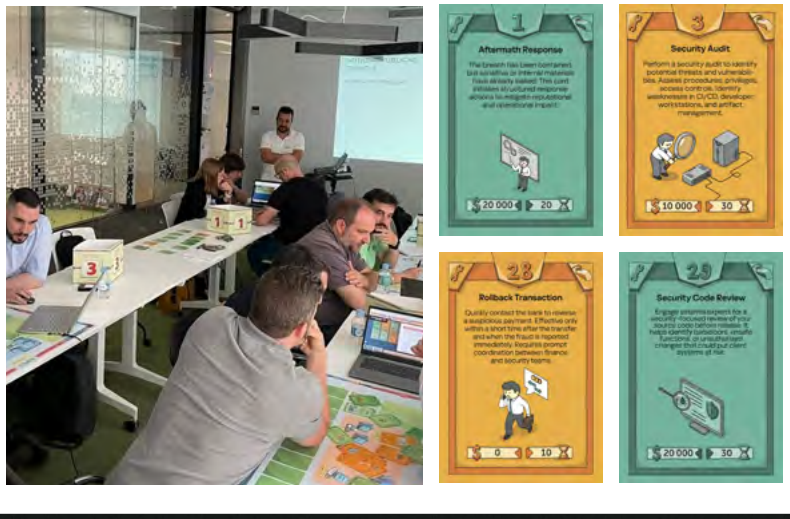
Eine kurzweilige Aktivität, die als separate Veranstaltung oder als Programmpunkt innerhalb einer bestehenden Konferenz, eines Seminars oder eines Unternehmens-Events durchgeführt werden kann.

- Bis zu 100 Teilnehmende, 4–5 pro Team
- Vor-Ort-Moderator und Trainingsassistent

KIPS online

Eine Online-Version eignet sich perfekt für global tätige Organisationen und öffentliche Veranstaltungen. Sie lässt sich auch mit KIPS Live kombinieren, um Remote-Teams in eine Präsenzveranstaltung einzubinden.

- Bis zu 300 Teams (= 1.000 Teilnehmer) gleichzeitig und standortunabhängig



KIPS-Anpassungsoptionen

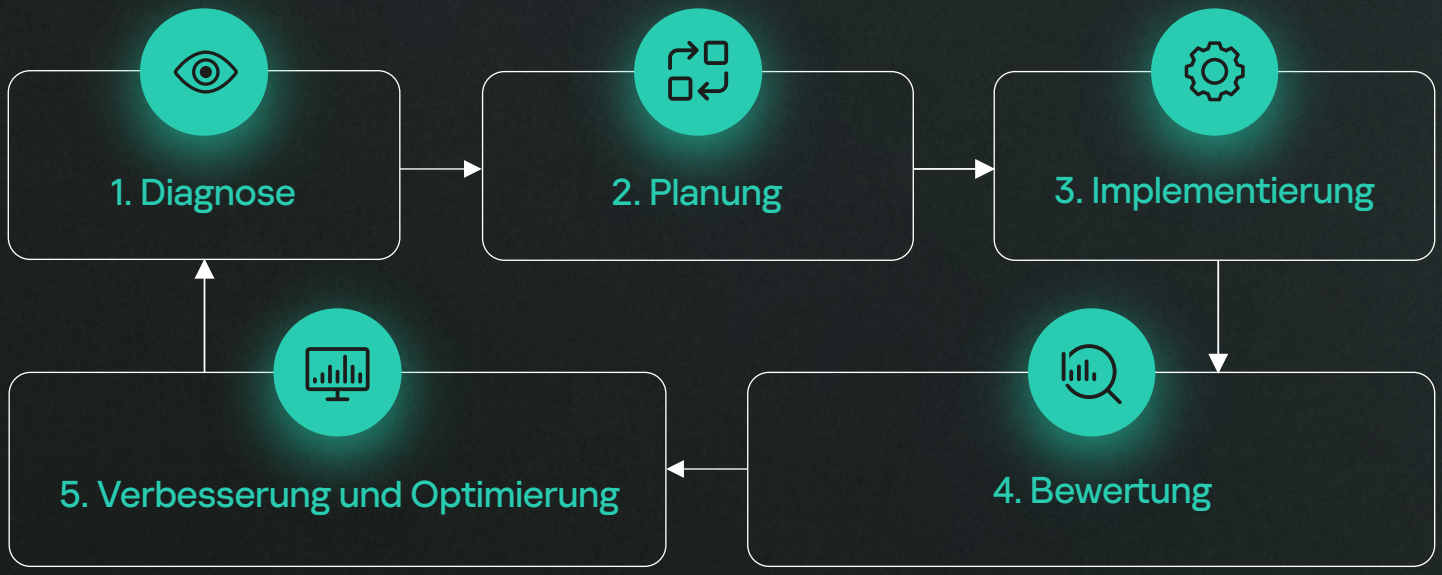
- Co- oder kundenspezifisch gebrandete Spielbretter, Karten und Tischnummern
- Ein einzigartiges Szenario, das in Partnerschaft mit Kaspersky entwickelt wird und Ihr Netzwerk, frühere Vorfälle oder branchenspezifische Bedrohungen widerspiegelt.

Sicherheitskultur als Fundament für nachhaltigen Erfolg

Echte Cyberresilienz entsteht nicht allein durch Richtlinien und Technologien, sondern auch durch die Unternehmenskultur. Und Kultur wird geprägt durch das Verhalten der Mitarbeitenden, die Art der Führung, die Prozesse und den Einsatz von Technologie:

- Menschen und Verhalten
- Leadership und Kooperation
- Operative Integration
- Sicherheitskompetenz und Einsatzbereitschaft

Eine nachhaltige, cybersichere Kultur erfordert ständiges Engagement auf allen Ebenen. Deshalb haben wir für die Kaspersky Security Awareness-Lösungen einen systematischen 5-stufigen Ansatz entwickelt.



Wie hoch ist der aktuelle Reifegrad der Cybersicherheitskultur in Ihrem Unternehmen?

0 Fragmentiert
Risiko: Das Fehlen von grundlegenden Praktiken und Strukturen erzeugt zahlreiche Schwachstellen. Selbst ein geringfügiger Sicherheitsvorfall kann ernsthafte Folgen haben.

1 Wachsam und reaktiv
Risiko: Es werden nur ausdrücklich definierte Regeln befolgt. In nicht standardisierten Situationen handeln Mitarbeitende nach eigenem Ermessen.

2 Managed
Risiko: Die Zahl der Vorfälle geht zurück, aber das System bleibt anfällig für komplexe Szenarien.

3 Integriert
Risiko: Prozesse wirken zwar stabil, doch wenn die Cyberkultur nicht als selbstregulierendes System funktioniert, bleibt ein „Verzögerungsrisiko“ bestehen.

4 Resilient
Ergebnis: Anzahl und Schweregrad der Vorfälle sinken weiterhin. Das Unternehmen kann sich schnell auf neue Bedrohungen einstellen.

> Wenn Sicherheit nicht mehr nur als Kampagne, sondern als fester Bestandteil der Unternehmenskultur verstanden wird, sinkt das Risiko und die Ergebnisse folgen.

CISO
Engagement im Kundenservice

Bauen Sie, eine cyberresiliente Kultur auf! Bringen Sie mithilfe von Kaspersky ASAP Menschen, Prozesse und Technologien in Einklang.

Jetzt testen!

Kaspersky Security Awareness

Seien Sie wachsam.
Bleiben Sie sicher.

www.kaspersky.de

#kaspersky
#cybersecuritytruetobusiness