kaspersky cybersecurity true to business

Kaspersky Security Awareness

Sicherheitskultur als Fundament für nachhaltigen Erfolg



Warum eine sicherheitsbewusste Unternehmenskultur wichtig ist

Menschliche Fehler

62–80 % der Sicherheitsvorfälle sind auf menschliches Handeln zurückzuführen, darunter Fehler, Missbrauch von Zugriffsrechten und Social Engineering[1,2]

4.99 Millionen US-Dollar

sind die durchschnittlichen Kosten einer Datenschutzverletzung pro Unternehmen[3]

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

Über 85 %

der Mitarbeitenden, die ein Awareness-Training absolviert haben, berichten von erhöhter Wachsamkeit und Vorsicht. Diese Verhaltensänderung trägt dazu bei, Sicherheitsvorfälle zu verhindern[4]

Reduzieren Sie den menschlichen Faktor bei Cyberrisiken mit Kaspersky Security Awareness

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 unterstützt Unternehmen weltweit dabei, die Cyberkompetenz ihrer Mitarbeitenden zu stärken. Fördern Sie eine Unternehmenskultur 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.



90 %

der Benutzer würden Kaspersky Security Awareness weiterempfehlen[4]

3 Millionen

Mitarbeiter haben unsere Schulungsprogramme erfolgreich abgeschlossen.

Über 160

Länder, in denen Unternehmen ihre Mitarbeitenden mit unseren Schulungslösungen schützen

Gründe für Kaspersky Security Awareness

Fast 30 Jahre Erfahrung im Bereich Cybersicherheit

Basierend auf der weltweiten Expertise von Kaspersky erstellen wir praxisrelevante Schulungsinhalte zum Thema Cybersicherheit. Mit dem Auftreten neuer Bedrohungen entwickeln sich auch unsere Inhalte weiter – so sind Ihre Mitarbeitenden jederzeit bestens vorbereitet.

Leicht zugängliches, interaktives Lernen

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

Nachhaltige Verhaltensänderungen

Unsere Methodik festigt neue Kompetenzen, sorgt für kontinuierliche Motivation und hilft, Lerninhalte dauerhaft in den Arbeitsalltag zu integrieren.

Engagement über alle Ebenen

Von Führungskräften bis hin zu Mitarbeitenden mit Kundenkontakt – wir liefern für jede Zielgruppe die richtigen Inhalte im passenden Format.

1 2026 Data Breach Investigations Report, Verizon
2 2026 Cyber Risk Survey, Kaspersky
3 2026 Cost of a Data Breach Report, IBM
4 2024 Security Awareness & Training Data Quadrant, Info-Tech Research Group

Kaspersky Automated Security Awareness Platform

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 Angriffe 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



Minimiert das Risiko von Bußgeldern wegen Compliance-Problemen

durch die Erfüllung regulatorischer Anforderungen



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 ATT&CK

MITRE-Technik	Threat	Kompetenzen und Verhaltensziele
T1566 – Phishing	Schädliche E-Mails	Phishing-Versuche erkennen und melden
T1585 – Kontenein-richtung	Gefälschte Konten/ Profile	Authentizität von Informa-tionen vor der Weitergabe verifizieren
T1199 – Vertrauens-beziehung	Ausnutzung von Ver-trauensbeziehungen	Ungewöhnliche Anfragen kritisch prüfen
T1091 – Replizierung über Wechsel-datenträger	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
- Industrial Cybersecurity
- Social Media und Messenger-Dienste
- Angriffe auf die Lieferkette
- Mobilgeräte
- Sicherheit von Bankkarten und PCI DSS
- Reaktion auf Vorfälle
- Vishing

1 2025 Kaspersky Automated Security Awareness Platform Research

Das Sicherheitsbewusstsein der Mitarbeitenden schulen, testen und stärken mit globaler Expertise und Flexibilität

Kaspersky ASAP ist in drei Tarifen erhältlich. Diese sind für Organisationen jeder Größe und jedes Sicherheitsniveaus geeignet.

		Essential	Proactive	Advanced
		Ideal für kleine Teams	Ideal für wachsende Unternehmen	Ideal für große Unternehmen mit spezifischen Anforderungen und einer ausgereiften Sicherheitskultur
		Compliance-konforme Security-Awareness-Schulungen	Proaktive Security-Awareness-Schulungen und Erfolgsmessung	Maßgeschneiderte, wirkungsvolle Security-Awareness-Schulungen
Phishing	Testet die Aufmerksamkeit der Mitarbeitenden im Umgang mit Cyberangriffen anhand maßgeschneiderter, realistischer Phishing-Simulationen	●	●	●
Schnellkurs	Interaktive Lektionen, die praktische Fähigkeiten für den Umgang mit von Menschen ausgehenden Cyberbedrohungen vermitteln und so die Compliance-Bereitschaft Ihres Unternehmens gewährleisten	●	●	●
Hauptkurs	Vollautomatisierte Security-Awareness-Schulungen, die auf das jeweilige Risikoniveau zugeschnitten sind. Diese umfassen Mikro-Lerneinheiten sowie Wiederholungen		●	●
Anpassbare Inhalte	Anpassbare Module, Tests, Phishing-Seiten und -Domänen und vieles mehr			●
Vor-Ort-Bereitstellung	Möglichkeit der Bereitstellung in Ihrer eigenen Infrastruktur für eine umfassende Kontrolle über sensible Daten, Integrationen und die Einhaltung gesetzlicher Vorschriften			●

Effiziente, einfach zu verwaltende Schulungen für Unternehmen jeder Größe

Einfaches Onboarding

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

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.

Automatisierte Benutzergruppierung auf Basis individuell definierter Regeln

Organisation nach Rolle, Abteilung oder Risikoprofil

Flexibles Deployment

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

Vollständige Automatisierung

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

Mandantenfähigkeit und flexible Administratorrollen

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

Übersichtliche und auf Führungskräfte ausgerichtete Berichterstattung

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.

Nahtlose Anmeldung

Integration mit Active Directory und SSO

Kaspersky Interactive Protection Simulation

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. Dazu zählen 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

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

14 branchenspezifische Szenarien, die laufend ergänzt werden

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



KIPS-Anpassungsoptionen

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

Kaspersky Cybersecurity for IT Online

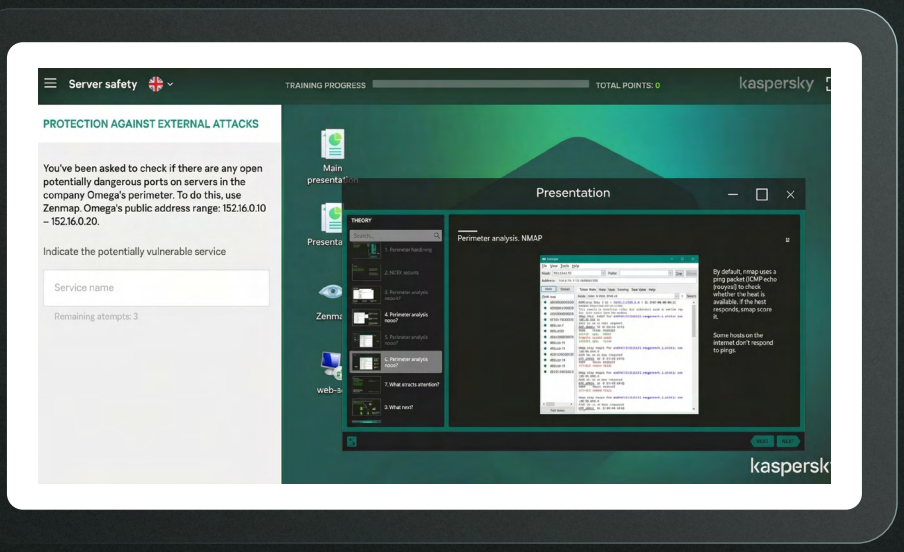
Cybersecurity for IT Online (CITO) ist ein interaktives Schulungsprogramm für Service-Desk-Spezialisten, Systemadministratoren und IT-Mitarbeitende ohne IT-Sicherheitsfokus. Es vermittelt praxisnahe Fähigkeiten, um versteckte Cyberangriffe in alltäglichen PC-Vorfällen zu erkennen, relevante Daten zu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

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

Kompetenzen im Bereich Incident Response und Systemabsicherung:

- 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



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. Wir empfehlen die Kombination dieser Schulung mit KIPS.

Zentrale geschäftskritische Aspekte der Cybersicherheit – klar und allgemeinverständlich erklärt:

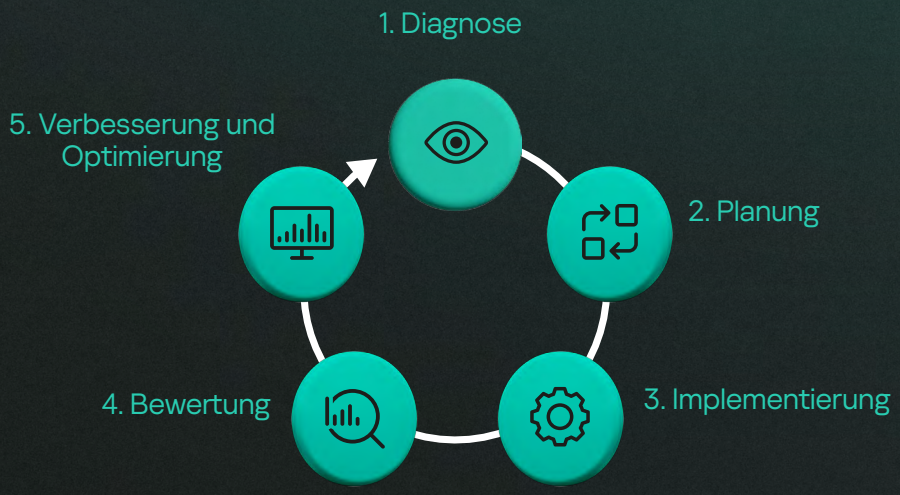
- Verstehen Sie Cybersicherheit als Bestandteil eines Gesamtsystems.
- Lernen Sie, wie Cyberrisiken Geschäftsprozesse gefährden und wie Sie ihnen wirksam begegnen.
- Verstehen Sie die Rolle der Unternehmensleitung in der Cybersicherheits-Governance.

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

Starten Sie jetzt die kostenlose Testversion und bewerten Sie das Niveau Ihrer Sicherheitskultur!



Kaspersky Security Awareness

Seien Sie wachsam.
Bleiben Sie sicher.

www.kaspersky.de

© 2026 AO Kaspersky Lab.
Eingetragene Marken und Servicemarken sind Eigentum ihrer jeweiligen Rechtsinhaber.

#kaspersky
#truetobusiness