



Checkliste Lernen für Cyber-Resilienz

Wie Security- und L&D-Teams gemeinsam Cybersecurity-Lernangebote schaffen, die risikorelevant, ansprechend und messbar sind

Bei Cyber-Resilienz handelt es sich um eine gemeinsame Aufgabe.

Security-Teams kennen die Risiken, denen Mitarbeitende ausgesetzt sind, während L&D-Teams das Wissen haben, wie Menschen lernen, sie ihr Wissen behalten und ihr Verhalten ändern. Jedoch ist für ein wirklich effektives Awareness-Programm beides notwendig.

Mit dieser Checkliste bringen Sie CISOs, Security-Awareness-Verantwortliche und L&D-Führungskräfte auf einen gemeinsamen Nenner – für einen effektiven Ansatz für Ihre Cyber-Resilienz.



Lernen für Cyber-Resilienz: Woran man gute Programme erkennt

Ein reines Awareness-Training macht Ihr Team nicht automatisch sicher. Mitarbeitende benötigen praxisnahe Übungen, klare Meldevorgaben, regelmäßige Wiederholungen und Lernerfahrungen, die sie unterstützen, richtig zu handeln, wenn sie etwas Verdächtiges bemerken.

Gemeinsam zu mehr Resilienz

Starke Programme verbinden das Cyber-Risiko mit einem Lernkonzept. Auf diese Weise helfen sie Mitarbeitenden, Bedrohungen zu erkennen und anschließend schnell und angemessen zu reagieren.

Mit dieser Checkliste können Sie einschätzen, ob Ihr aktueller Ansatz beim Cyber-Lernen:

- die aktuellen Bedrohungen Ihrer Organisation abbildet
- ansprechend genug ist, um die Aufmerksamkeit der Menschen zu binden
- auf Verhaltensänderung ausgelegt ist
- über einmalige Schulungen hinaus verankert wird
- so gemessen wird, dass es für Security und L&D wirklich relevant ist
- eindeutige Erwartungen an das Meldeverhalten formuliert
- auch für die Führungsebene überzeugend ist

Das gemeinsame Modell

Security definiert das Risiko

CISOs und Security-Teams sollten definieren:

- welche menschlichen Risikoverhalten am stärksten ins Gewicht fallen
- welche Mitarbeitergruppen am ehesten gefährdet sind
- welche Bedrohungsszenarien immer häufiger werden
- welches Meldeverhalten sich verbessern muss
- welche Nachweise für Gespräche mit der Führung, Audit oder Compliance notwendig sind

L&D gestaltet das Lernen

L&D-Teams sollten definieren:

- wie sich Cyber-Lernen ansprechend und zugänglich gestalten lässt
- wie Mitarbeitende sichere Entscheidungen trainieren können anstatt Informationen passiv aufzunehmen
- wie das Gelernte mit der Zeit gefestigt wird
- wie sich Inhalte in den Arbeitsalltag einfügen
- wie sich Lerntransfer und Verhaltensänderung unterstützen lassen

Checkliste

Lernen für mehr Cyber-Resilienz

Wie viele Aussagen können Sie
mit gutem Gewissen abhaken?

1. Risikorelevanz

- ☐ Haben wir die konkreten menschlichen Risiken benannt, die für die Organisation am wichtigsten sind?
- ☐ Spiegeln unsere Szenarien aktuelle Methoden von Phishing, Identitätsbetrug und Social Engineering wider?
- ☐ Erhalten besonders gefährdete Rollen oder Abteilungen geeignete Beispiele?
- ☐ Bildet unser Training die Realität aus Zeitdruck, Stress und unklaren Situationen ab?
- ☐ Werden KI-gestützte Bedrohungen dort berücksichtigt, wo sie echten Schaden anrichten, ohne das Thema künstlich aufzublähen?

Warum das wichtig ist:

Cybersecurity-Trainings funktionieren am besten, wenn Mitarbeitende Situationen aus ihrem echten Arbeitsalltag wiedererkennen. Allgemeine Ratschläge führen nur selten zu einer realen Verhaltensänderung.

2. Ansprechende Lernerfahrung

- ☐ Ist die Lernerfahrung kompakt und attraktiv genug gestaltet worden für Mitarbeitende mit vollem Terminkalender?
- ☐ Basiert sie auf realistischen Geschichten, Szenarien und Entscheidungen und vermittelt Wissen nicht nur passiv?
- ☐ Wird konsequent auf Angst, Schuldzuweisungen und übermäßigen Fachjargon verzichtet?
- ☐ Sind die Inhalte auch für Mitarbeitende ohne Fachwissen verständlich?
- ☐ Macht sie den Mitarbeitenden bewusst, warum ihr Handeln zählt?

Warum das wichtig ist:

Mitarbeitende merken sich Cyber-Empfehlungen deutlich besser und wenden sie eher an, wenn Lernen relevant, nachvollziehbar und praxisnah gestaltet wurde.

3. Verhalten praktisch trainieren

- ☐ Lernen Mitarbeitende, wie sie reagieren müssen, wenn eine Bedrohung nicht offensichtlich ist?
- ☐ Wurden in das Training interaktive Entscheidungspunkte, spürbare Konsequenzen und direktes Feedback integriert?
- ☐ Regt das Training dazu an, den Kontext zu beurteilen, anstatt nur die Warnzeichen zu erkennen?
- ☐ Fördert das Programm neben reinem Wissen auch das Selbstvertrauen?
- ☐ Sind typische Alltagsszenarien enthalten, z. B. Lieferantenanfragen, geänderte Bankverbindungen, CEO-Fraud oder potenzieller Druck bei der Datenweitergabe?

Warum das wichtig ist:

Theoretisches Wissen über Cyber-Risiken schützt im Ernstfall unter Druck nicht automatisch. Erst die praktische Übung überwindet die Diskrepanz zwischen Wissen und Handeln.

4. Meldekultur

- ☐ Wissen Mitarbeitende genau, wie sie verdächtige Aktivitäten melden?
- ☐ Wird das Melden auch dann gefördert, wenn sich Mitarbeitende unsicher sind?
- ☐ Verzichtet die Organisation auf Schuldzuweisungen?
- ☐ Erhalten Mitarbeitende nach einer Meldung eine zeitnahe Rückmeldung oder eine Bestätigung?
- ☐ Wird das Meldeverhalten gemessen und als Erfolgskriterium des Programms bewertet?

Warum das wichtig ist:

Das Melden von Vorfällen ist eines der deutlichsten Zeichen für die Cyber-Resilienz einer Belegschaft. Mitarbeitende brauchen deshalb absolute Klarheit und Vertrauen in den Meldeprozess, sofern es einen gibt.

5. Kontinuierliche Wiederholung

- ☐ Finden Cyber-Trainings über das gesamte Jahr verteilt statt?
- ☐ Werden zentrale Verhaltensweisen in verschiedenen Formaten aufgegriffen?
- ☐ Orientieren sich die Wiederholungen an aktuellen Bedrohungen oder strategischen Prioritäten der Organisation?
- ☐ Werden Führungskräfte oder Teamleitungen dabei unterstützt, Cybersicherheit regelmäßig zu thematisieren?
- ☐ Werden die Wiederholungen als nützlich empfunden anstatt als lästige Redundanz?

Warum das wichtig ist:

Ein einzelnes Modul pro Jahr verpufft im Alltag schnell. Nachhaltige Verhaltensänderung ist auf Kontinuität angewiesen: Durch regelmäßige Impulse bleiben die zentralen Sicherheitsprinzipien im Kopf präsent und abrufbereit.

6. Messung und Nachweise

- ☐ Werden mehr als nur reine Abschlussquoten und Quizergebnisse gemessen?
- ☐ Wird das reale Meldeverhalten, Engagement und die Entwicklung über Zeit erfasst?
- ☐ Können wir datenbasiert nachweisen, ob Mitarbeitende Bedrohungen selbstsicherer erkennen und melden?
- ☐ Gibt es ein gemeinsames Verständnis zwischen Security und L&D, wie Erfolg definiert ist?
- ☐ Können Fortschritte für die Führungsebene verständlich darstellen werden?

Warum das wichtig ist:

CISOs benötigen Nachweise für ein minimiertes Risiko, während L&D-Führungskräfte den Beleg für die effektive Wirkung des Trainings benötigen. Ein einheitliches Modell für die Messung führt beide Perspektiven zusammen und schafft eine gemeinsame Erfolgsbasis.

7. Governance und Abstimmung der Beteiligten

- ☐ Sind die Schulungsmaßnahmen zur Cyber-Resilienz an die übergeordneten Ziele im Bereich Cyber-Risiko, Compliance und Governance gekoppelt?
- ☐ Ziehen Security, L&D, Risiko und Compliance an einem Strang, was die Ziele angeht?
- ☐ Versteht die Führungsebene, welche Verhaltensziele das Programm verfolgt?
- ☐ Kann das Programm Gespräche über Cyber-Hygiene, KI-Kompetenz und operative Resilienz unterstützen?
- ☐ Gibt es eine klar verantwortliche Person für die kontinuierliche Verbesserung?

Warum das wichtig ist:

Lernen für Cyber-Resilienz überzeugt mehr, wenn es mit Geschäftsrisiken, dem Verhalten der Belegschaft und der Verantwortung der Führung verbunden ist.

Kurzer Bewertungsleitfaden

Zählen Sie für jeden Abschnitt, wie viele Aussagen Sie abgehakt haben.

>25

Der Großteil wurde abgehakt

Ihr Programm bewegt sich wahrscheinlich schon über reine Awareness hinaus und sorgt für echte Cyber-Resilienz im gesamten Team. Konzentrieren Sie sich als Nächstes darauf, wie Sie die Messung und die Wiederholungen im Alltag weiter optimieren können und das gesamte Training Schritt für Schritt besser machen können.

>15

Einige Lücken sind noch da

Ihr Programm scheint auf einem soliden Fundament zu stehen, verlässt sich aber wahrscheinlich noch zu sehr auf die Schulungen selbst statt auf die echte Verhaltensänderung. Setzen Sie sich am besten zuerst mit den Bereichen auseinander, bei denen Security und L&D noch am wenigsten abgestimmt sind.

<10

Das Meiste ist noch offen

Nutzen Sie die Chance, den Ansatz Ihrer Organisation grundlegend zu überdenken. Definieren Sie zuerst die relevantesten menschlichen Risikofaktoren und gestalten Sie anschließend Lernangebote, die Ihren Mitarbeitenden helfen, sichere Verhaltensweisen zu trainieren und zu festigen.

Diskussionsfragen für Security- und L&D-Teams

Nutzen Sie diese
Fragen als Grundlage
für eine gemeinsame
Planungssitzung:

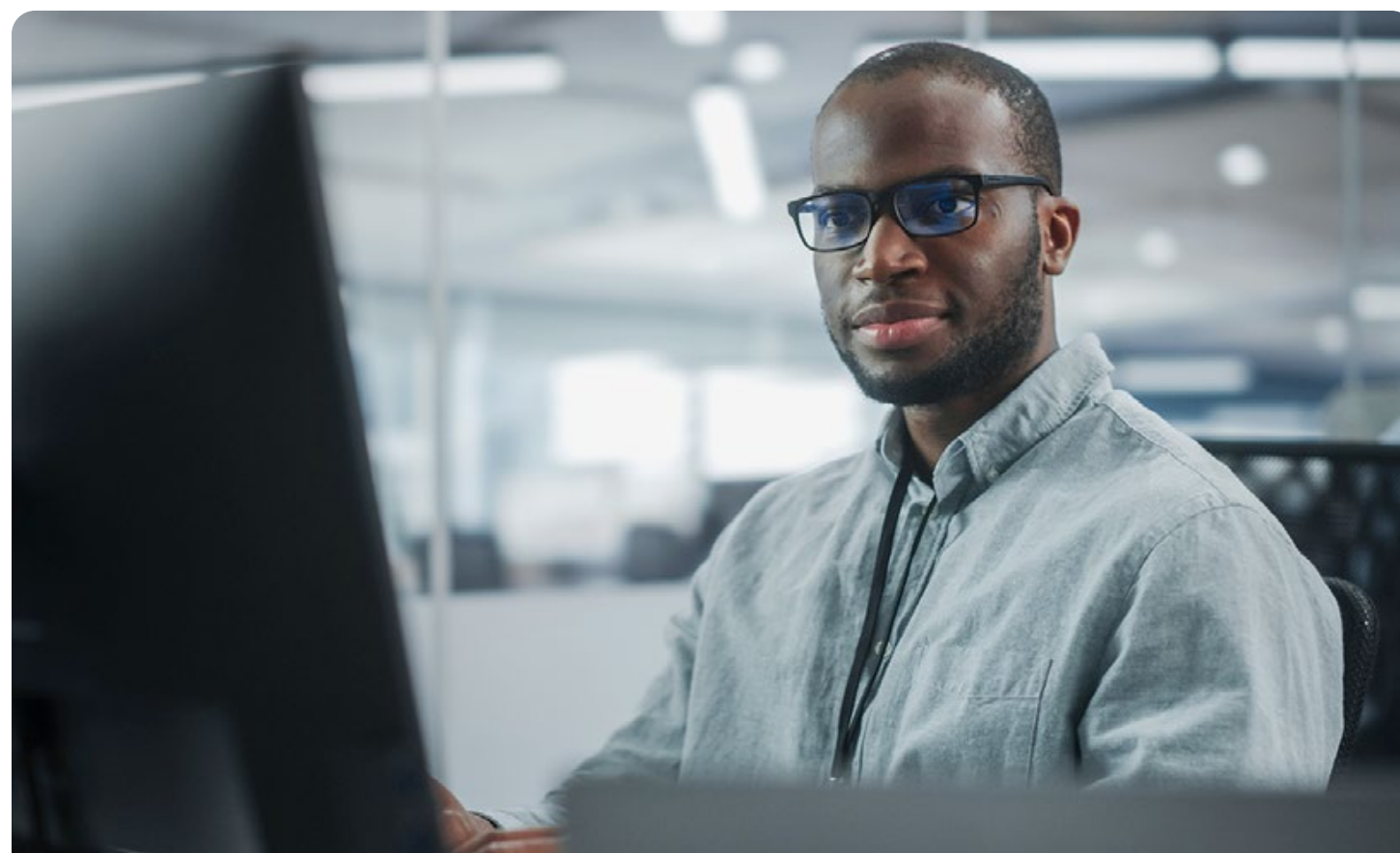
1. Welche drei menschlichen Risikofaktoren möchten wir besonders reduzieren?
2. Welche Mitarbeitergruppen sind in der Praxis am ehesten gefährdet?
3. An welchen Stellen zögern Mitarbeitende, missverstehen die Richtlinien oder versäumen die Meldung von Vorfällen?
4. Wie sieht das richtige Verhalten bei einem echten Sicherheitsvorfall aus?
5. Wie können wir es den Mitarbeitenden so leicht wie möglich machen, sicheres Verhalten im Training zu üben?
6. Was sollten wir über die reine Abschlussquote hinaus messen?
7. Wie halten wir Cyber-Resilienz das ganze Jahr über präsent?



Nächste Schritte für die Praxis

Für Security-Verantwortliche

- Definieren Sie die kritischsten Alltagsszenarien für menschliche Fehler
- Legen Sie das Meldeverhalten und die Eskalationswege fest
- Bestimmen Sie die notwendigen Nachweise für die Führungsebene und Governance
- Teilen Sie den Bedrohungskontext in einfacher, nicht-technischer Sprache mit L&D



Für L&D-Verantwortliche

- Übersetzen Sie die definierten Risiken in konkrete Lernmomente
- Nutzen Sie Praxisbeispiele und -szenarien für nachhaltige Sicherheitsentscheidungen
- Verankern Sie regelmäßige Wiederholungen fest im Lernkalender
- Messen Sie die echte Anwendung im Alltag statt reiner Abschlussquoten



Für beide Teams

- Vereinbaren Sie gemeinsame Erfolgskennzahlen
- Überprüfen Sie das Programm gemeinsam auf vierteljährlicher Basis
- Aktualisieren Sie die Inhalte bei veränderten Bedrohungslagen und Arbeitsweisen
- Behandeln Sie Cyber-Resilienz als dauerhafte Aufgabe anstatt als einmalige Maßnahme



Wo Cyber Crime Time ins Spiel kommt

Cyber Crime Time unterstützt Organisationen beim Wechsel von einmaligen Awareness-Schulungen zu einem immersiven, praxisnahen Lernerlebnis für echte Cyber-Resilienz.

Durch story-getriebene Szenarien und regelmäßige Wiederholung unterstützt Cyber Crime Time Ihren Mitarbeitenden, moderne Cyber-Bedrohungen wie Phishing, Social Engineering, Deepfakes und KI-gestützte Angriffe sicher zu erkennen, angemessen darauf zu reagieren und diese sofort zu melden.

Auf diese Weise minimieren Security-Teams den menschlichen Risikofaktor spürbar im Alltag, während L&D-Teams mit einem motivierenden Tool den Verhaltenswandel begleiten.

Möchten Sie erfahren, wie immersives, spielerisches Training Ihre Security- und L&D-Ziele voranbringt?

[Cyber Crime Time entdecken](#)[Demo buchen](#)

more than technology

**information
multimedia
communication AG**

Scheer Tower
Uni-Campus Nord
66123 Saarbrücken

T. +49 681 9476-0
info@im-c.com

Scheer IMC weltweit

Deutschland (Saarbrücken,
Freiburg, München)
Australien (Melbourne)
Großbritannien (London)
Niederlande (Vianen)
Österreich (Graz)
Rumänien (Sibiu)
Schweiz (Zürich)
Singapur
USA (Dover)

Über Scheer IMC

Scheer IMC ist führender Anbieter von E-Learning-Technologien mit mehr als 25 Jahren Erfahrung. Als Full-Service-Dienstleister bietet das Unternehmen modernste Lernplattformen, Lerninhalte und strategische L&D-Expertise für globale Marken, um komplexe Lernziele zu erreichen. Die imc AG wurde Ende der 1990er Jahre von IT-Pionier Professor August-Wilhelm Scheer gegründet und ging aus einem wegweisenden universitären Bildungsprojekt hervor.

Heute beschäftigt das Unternehmen mit Hauptsitz in Saarbrücken über 400 Mitarbeitende an 12 Standorten weltweit. Als zuverlässiger Partner im Bereich Corporate Learning hat Scheer IMC das Lernen für mehr als 10 Millionen Lernende in über 1.300 Unternehmen und Organisationen revolutioniert. Als innovativer Vorreiter für Lernstrategien bietet Scheer IMC nicht nur preisgekrönte Technologien, sondern schafft mit einzigartigen, nutzerzentrierten Learning Journeys einen echten Mehrwert.

Erfahren Sie mehr unter

scheer-imc.de