Bonuskapitel 1

Security Awareness Programme

Security Awareness ist weit mehr als ein jährlicher E-Learning-Klickmarathon oder ein Poster mit Phishing-Warnungen – sie ist das kulturelle Immunsystem der Organisation. In einer Zeit, in der Angriffsflächen exponentiell wachsen, soziale Manipulationstechniken raffinierter denn je sind und technologische Schutzmaßnahmen alleine nicht ausreichen, kommt der menschlichen Komponente eine strategische Schlüsselrolle zu.

Für CISOs, die über rein technische Kontrollmechanismen hinausdenken und eine nachhaltig resiliente Sicherheitskultur etablieren wollen, ist Awareness ein zentrales Handlungsfeld. Sicherheitsbewusstsein ist nicht nur ein »Nice-to-have«, sondern ein entscheidender Risikoreduktionsfaktor – messbar, steuerbar und integraler Bestandteil jeder wirksamen Cybersecurity-Strategie.

Dieses Kapitel zeigt praxisorientiert und evidenzbasiert, wie ein ganzheitliches Awareness-Programm konzipiert, organisatorisch verankert und kontinuierlich weiterentwickelt werden kann. Dabei stehen nicht nur Inhalte und Kanäle im Fokus, sondern auch Change-Management-Aspekte, psychologische Wirkmechanismen und die strategische Verankerung im GRC-Ökosystem. Zudem wird aufgezeigt, wie Awareness-Initiativen nicht nur compliant, sondern tatsächlich wirksam gestaltet und mit geeigneten KPIs gemessen werden – von Click-Raten in Phishing-Simulationen bis hin zu qualitativen Kulturindikatoren.

Psychologische Grundlagen und Verhaltenstreiber

Strategische Relevanz

Security Awareness wird in vielen Organisationen noch immer als klassisches IT-Projekt betrachtet – zeitlich begrenzt, technologiezentriert und vorwiegend auf Wissensvermittlung fokussiert. Doch diese Sichtweise greift zu kurz. In der Realität handelt es sich bei wirksamer Awareness nicht um ein Projekt, sondern um ein dauerhaftes, strategisches Verhaltensänderungsprogramm, das tief in der Unternehmenskultur verankert sein muss. CISOs, die dieses Prinzip erkennen, verschieben den Fokus weg von reiner Wissensweitergabe hin zu einem systematischen Aufbau sicherheitsförderlicher Gewohnheiten im Arbeitsalltag.

Denn Wissen allein reicht nicht aus, um Verhalten nachhaltig zu verändern. Zahlreiche Studien aus der Verhaltenspsychologie belegen, dass es nicht primär der Mangel an Informationen ist, der zu riskantem Verhalten führt. Vielmehr sind es emotionale, soziale und kontextuelle Faktoren, die das tatsächliche Verhalten bestimmen. Ein Mitarbeitender klickt selten auf einen Phishing-Link, weil er nicht weiß, was Phishing ist – sondern weil er unter Zeitdruck steht, einer Autorität gefallen will oder schlicht automatisiert handelt. Die Lücke zwischen Wissen und Handeln lässt sich nur schließen, wenn psychologische Mechanismen bewusst in das Design des Awareness-Programms integriert werden.

Ein wirkungsvolles Modell zur Erklärung und Gestaltung menschlichen Verhaltens liefert hier das Behavior Model von BJ Fogg, Professor an der Stanford University. Es bringt den Kern der Herausforderung auf den Punkt: Verhalten entsteht nur dann, wenn Motivation, Fähigkeit und ein Auslöser gleichzeitig vorhanden sind. In Formel:

```
Behavior = Motivation × Ability × Prompt.
```

Auf den Kontext der Informationssicherheit übertragen bedeutet das: Mitarbeitende müssen nicht nur motiviert sein, sich sicher zu verhalten – sie müssen auch in der Lage sein, es einfach umzusetzen, und sie benötigen konkrete Impulse im richtigen Moment.

Beispiel

Die Nutzung von Multi-Faktor-Authentifizierung wird wahrscheinlicher, wenn der Prozess technisch einfach ist, der persönliche Nutzen deutlich kommuniziert wird, und ein just-in-time Prompt – etwa beim Login – an das richtige Verhalten erinnert. Genau diese Kombination erhöht die Wahrscheinlichkeit sicherer Entscheidungen im Alltag signifikant.

Daraus ergibt sich ein klarer Gestaltungsauftrag für CISOs: Awareness-Maßnahmen müssen entlang dieser drei Achsen konzipiert werden – nicht als Inhalte, sondern als Verhaltensdesign. In der Praxis bedeutet das, gezielt mit Verhaltenstreibern zu arbeiten, die in der Psychologie und Verhaltensökonomie gut erforscht sind. Soziale Normen etwa lassen sich über Peer-Mechanismen, interne Botschafterprogramme oder gemeinsame Challenges stärken. Die individuelle Selbstwirksamkeit kann durch kontinuierliches Feedback, Fortschrittsanzeigen oder Gamification-Elemente gefördert werden. Emotionale Aktivierung wiederum gelingt durch realitätsnahe Simulationen oder persönliche Narrative, die die Bedeutung von Sicherheit greifbar machen.

Entscheidend ist, dass solche Maßnahmen nicht isoliert wirken, sondern systematisch in die täglichen Abläufe eingebettet sind. Microlearning-Einheiten, die exakt auf den jeweiligen Arbeitskontext zugeschnitten sind, wirken weitaus stärker als generische E-Learnings. Visuelle Hinweise oder Default-Sicherheitskonfigurationen im Systemdesign reduzieren Reibungspunkte und erleichtern sicheres Verhalten als Standard. So wird Sicherheit nicht nur erwartet, sondern auch ermöglicht – ein zentraler Unterschied in der Wirkung.

Für CISOs ergibt sich daraus eine strategische Perspektive: Wer Awareness als Behavioural Architecture begreift, gestaltet aktiv mit, wie Sicherheitskultur im Unternehmen entsteht. Dies geht weit über Compliance hinaus. Es stärkt die organisationale Resilienz, reduziert menschliche Risikofaktoren messbar und fördert eine proaktive Sicherheitskultur, in der Mitarbeitende nicht Objekte von Schulungsmaßnahmen, sondern aktive Mitgestalter von Sicherheit sind. Der CISO wird so vom Regelsetzer zum Kulturgestalter.

Letztlich ist dies der Schlüssel zu nachhaltigem Erfolg: Ein Security-Awareness-Programm entfaltet seine volle Wirksamkeit erst dann, wenn es auf der Basis psychologischer Prinzipien gestaltet wird – nicht belehrend, sondern verhaltensunterstützend. Sicherheit wird dadurch nicht zur Pflicht, sondern zur selbstverständlichen Gewohnheit.

Kognitive Verzerrungen als Risikoquelle

Ein weiteres zentrales Element, das moderne Security-Awareness-Programme berücksichtigen müssen, sind sogenannte kognitive Verzerrungen – systematische Denkfehler, die menschliches Verhalten oft unbewusst beeinflussen. Selbst gut informierte Mitarbeitende handeln nicht immer rational oder sicherheitsbewusst, weil ihre Wahrnehmung der Realität durch psychologische Filter verzerrt ist. Diese Verzerrungen stellen ein reales Sicherheitsrisiko dar – gerade weil sie subtil wirken und in nahezu jeder Organisation verbreitet sind.

1. Normalitätsbias (»Mir passiert das nicht«)

Eine der häufigsten Verzerrungen im Sicherheitskontext ist der Normalitätsbias. Menschen neigen dazu, davon auszugehen, dass das, was bisher gut gegangen ist, auch in Zukunft gut gehen wird. Sie unterschätzen Risiken und ignorieren Warnsignale, weil sie glauben, »so etwas passiert anderen, aber nicht mir«. Dieser Denkfehler führt dazu, dass Bedrohungen wie Phishing, Social Engineering oder Ransomware als abstrakt oder irrelevant wahrgenommen werden.

Wirksame Gegenmaßnahme:

Um diesen Bias zu durchbrechen, braucht es Emotionalisierung und Konkretheit. Realitätsnahe Fallbeispiele, insbesondere mit interner Bezugnahme (»Unsere Kollegin aus der Buchhaltung klickte auf eine gefälschte Rechnung und löste eine

interne Eskalation aus…«), schaffen persönliche Betroffenheit. Durch diese Identifikationsmechanismen wird die Wahrscheinlichkeit erhöht, dass Mitarbeitende ihr eigenes Verhalten reflektieren und anpassen.

2. Optimism Bias (»Ich bin sicherer als der Durchschnitt«)

Ein verwandter Denkfehler ist der Optimism Bias. Hierbei überschätzen Menschen ihre eigene Sicherheitskompetenz oder unterschätzen die Wahrscheinlichkeit, Opfer eines Angriffs zu werden. Sie glauben, dass sie klüger, vorsichtiger oder technisch versierter sind als ihre Kolleg:innen – selbst dann, wenn die Statistik das Gegenteil belegt.

Wirksame Gegenmaßnahme:

Dieser Selbstüberschätzung kann mit individualisiertem Feedback entgegengewirkt werden. Tools wie Phishing-Simulationen mit persönlichem Scoring und anonymisiertem Vergleich zur Peergroup ermöglichen eine objektive Rückmeldung. Das schafft kognitive Dissonanz, die zu höherer Lernbereitschaft führt – ein bewährter Mechanismus aus der Verhaltenspsychologie.

3. Overconfidence Bias bei Führungskräften

Ein besonders kritischer Bias zeigt sich häufig bei Führungskräften: der Overconfidence Bias. Aufgrund ihrer langjährigen Erfahrung und Position nehmen viele Executives an, dass Awareness-Schulungen für sie irrelevant seien. Diese Überschätzung der eigenen Immunität ist trügerisch – gerade weil Top-Führungskräfte bevorzugte Ziele für Spear-Phishing, Business Email Compromise (BEC) und andere hochspezialisierte Angriffsformen sind.

Wirksame Gegenmaßnahme:

Für diese Zielgruppe braucht es maßgeschneiderte Inhalte, die nicht belehrend, sondern auf Augenhöhe kommuniziert werden. Awareness-Maßnahmen sollten Business Impact und gezielte Angriffsszenarien thematisieren – etwa anhand realer Beispiele von CEO-Fraud, kompromittierten M&A-Kommunikationen oder Industriespionage. Solche Inhalte schaffen Relevanz und verdeutlichen, dass Awareness kein operatives Thema ist, sondern ein Top-Level-Risikofaktor mit strategischer Tragweite.

Indem Awareness-Programme gezielt mit diesen kognitiven Verzerrungen umgehen, gelingt es, Sicherheit nicht nur als Wissensfrage zu behandeln, sondern als psychologisch fundiertes Verhaltensdesign zu verankern. Es ist diese Tiefe, die den Unterschied macht – zwischen bloßer Compliance und gelebter Sicherheitskultur.

Sicherheitsverhalten ist kontextabhängig

Ein weiterer zentraler Erfolgsfaktor für wirksame Security Awareness liegt in der Kontextualisierung von Verhalten. Menschen handeln nicht in einem Vakuum, sondern innerhalb konkreter situativer, sozialer und organisatorischer Rahmenbedingungen. Selbst gut geschulte Mitarbeitende treffen in kritischen Momenten häufig unsichere Entscheidungen – nicht, weil sie nicht wüssten, was richtig wäre, sondern weil der Kontext ihr Verhalten in eine andere Richtung lenkt.

Verhalten ist also nicht konstant, sondern hochgradig kontextabhängig. Awareness-Programme, die diesen Umstand ignorieren, bleiben theoretisch und abstrakt. Wer hingegen kontextsensitiv arbeitet, erhöht die Wirksamkeit seiner Maßnahmen drastisch – weil die Inhalte zur Situation passen, in der sich die Zielgruppe tatsächlich befindet.

Im Folgenden drei typische Alltagssituationen, in denen sicherheitsrelevantes Verhalten verzerrt wird – sowie taktische Gegenmaßnahmen, die CISOs gezielt in ihre Programme integrieren können:

1. Kontext: Hoher Zeitdruck

In dynamischen, stressintensiven Arbeitsphasen – etwa vor Deadlines, unter Last-Minute-Druck oder bei unerwarteten Eskalationen – tritt ein verbreiteter Bias auf: Sicherheit wird als sekundär empfunden. Der Gedanke »Security ist gerade nicht mein Fokus« führt dazu, dass Prüfmechanismen umgangen, Policies übersehen oder riskante Aktionen (z. B. Weiterleitung vertraulicher Informationen) unreflektiert ausgeführt werden.

Taktische Gegenmaßnahmen:

Microlearning statt Langform-Inhalte: Sicherheit muss in kleinen, konsumierbaren Einheiten präsent sein – eingebettet in den Arbeitsfluss, nicht losgelöst davon.

Automatisierung sicherer Defaults: Je weniger Entscheidungen Mitarbeitende selbst treffen müssen, desto weniger können sie im Stress falsch handeln.

Just-in-time Reminder: Situative Prompts – etwa visuelle Hinweise beim Versenden sensibler Daten – bringen Sicherheit zum entscheidenden Moment zurück ins Bewusstsein.

2. Kontext: Remote-Arbeit

Im Homeoffice oder bei mobiler Arbeit verändert sich die Wahrnehmung von Kontrolle und Verantwortung. Die soziale Dichte fehlt, das Gefühl permanenter Beobachtung nimmt ab, und damit auch die Selbstdisziplin. Mitarbeitende fühlen sich weniger eingebunden und entwickeln unbewusst die Annahme: »Was ich hier

tue, sieht sowieso niemand.« Das führt zu Nachlässigkeit, etwa beim Umgang mit privaten Geräten, Passwörtern oder nicht genehmigten Tools.

Taktische Gegenmaßnahmen:

Security Prompts im digitalen Workflow: Awareness-Inhalte müssen dort auftauchen, wo gearbeitet wird – z. B. beim Zugriff auf SaaS-Anwendungen oder beim Öffnen sensibler Dateien.

Konsequente Multi-Faktor-Authentifizierung (MFA): Technische Hürden helfen, sichere Handlungen zu erzwingen – ohne den Nutzer bewusst zu belasten.

Zero Trust UX-Design: Die Benutzeroberflächen sicherheitskritischer Systeme sollten klar kommunizieren, dass Identität und Verhalten kontinuierlich geprüft werden. So bleibt das Bewusstsein für Security auch ohne physische Präsenz erhalten.

3. Kontext: Gruppenverhalten

Ein weiterer Einflussfaktor ist die soziale Dynamik innerhalb von Teams oder Abteilungen. Der psychologische Mechanismus dahinter: Wenn niemand sonst reagiert, erscheint Nicht-Handeln als akzeptabler Standard. Dieser sogenannte Bystander Effect wirkt auch im Cybersecurity-Kontext – etwa, wenn Vorfälle nicht gemeldet oder unsichere Verhaltensweisen nicht hinterfragt werden. Der innere Monolog lautet dann: »Niemand sonst meldet den Vorfall – dann ist es wohl nicht so schlimm.«

Taktische Gegenmaßnahmen:

Social Proof aktiv nutzen: Zeige, dass andere handeln – etwa durch transparente Erfolgsmetriken (»85 % unserer Mitarbeitenden haben Phishing-Versuche erfolgreich erkannt«).

Kollektive Verantwortung kommunizieren: Security ist nicht die Aufgabe einzelner, sondern ein Teamthema. Dies kann durch gruppenbasierte Simulationen, gemeinsame Erfolgsziele oder gamifizierte Challenges gefördert werden.

Belohnungssysteme für positives Verhalten: Auch kollektive Anerkennung (z. B. »Team des Monats« für Sicherheitsverhalten) stärkt die Bereitschaft, aktiv beizutragen.

Diese Beispiele zeigen deutlich: Sicherheitsverhalten ist kein stabiler Zustand, sondern das Ergebnis situativer Kräfte. Ein modernes Awareness-Programm muss diese Kontexte nicht nur kennen, sondern aktiv adressieren – durch adaptive Inhalte, situative Prompts und soziales Design. Nur dann gelingt es, Sicherheit in der Lebensrealität der Mitarbeitenden zu verankern – dort, wo sie tatsächlich handeln.

Behavioral Design: Nudging & Defaults

Ein besonders wirksames Instrument moderner Security-Awareness-Strategien ist der gezielte Einsatz von Behavioral Design-Prinzipien – insbesondere sogenannter »Nudges«. Der Begriff, geprägt durch Richard Thaler und Cass Sunstein (Nobelpreis für Wirtschaft, 2017), beschreibt sanfte, nicht-bevormundende Anstöße, die Verhalten in eine gewünschte Richtung lenken, ohne Entscheidungsfreiheit einzuschränken.

Gerade im Sicherheitskontext – wo Überforderung, Trägheit oder Unsicherheit oft zu riskantem Verhalten führen – kann Nudging helfen, sichere Handlungsoptionen intuitiv und friktionsfrei zugänglich zu machen. Es geht dabei nicht um Kontrolle oder Zwang, sondern um ein intelligentes Umgebungsdesign, das gewünschtes Verhalten zur leichtesten Option macht.

1. Defaults: Die Macht der Voreinstellung

Einer der stärksten »unsichtbaren« Einflussfaktoren auf Verhalten ist die Default-Einstellung. Menschen neigen dazu, Voreinstellungen beizubehalten – sei es aus Bequemlichkeit, Unsicherheit oder implizitem Vertrauen in die Gestaltung. Diese Trägheit kann im Security-Bereich gezielt genutzt werden, um sicherheitsförderliches Verhalten zu etablieren, ohne aktives Zutun der Nutzer.

Beispiele

- Automatisch aktivierte Multi-Faktor-Authentifizierung (MFA)
- Standardmäßige Verschlüsselung von E-Mail-Kommunikation
- »Least Privilege«-Zugriffsrechte als Ausgangspunkt

Durch diese »secure by default«-Ansätze werden Sicherheitshürden nicht erhöht, sondern eliminiert, indem sicheres Verhalten zur einfachsten Wahl wird – im besten Fall zur Voreinstellung, die gar nicht aktiv hinterfragt wird.

2. Nudging durch Framing: Verlust wirkt stärker als Gewinn

Ein weiteres mächtiges Werkzeug des Behavioral Designs ist das sogenannte Framing – also die Art und Weise, wie Informationen präsentiert werden. Die Verhaltensökonomie zeigt, dass Menschen auf Verlustangst stärker reagieren als auf potenziellen Gewinn. Dieses Prinzip lässt sich gezielt in Awareness-Kommunikation übersetzen.

Beispiel

Statt: »Durch Aufmerksamkeit können Sie Angriffe verhindern.«

Besser: »Durch Ihren Klick wären sensible Kundendaten offengelegt worden.«

Diese Form des »Loss Framing« aktiviert emotionale Schutzmechanismen stärker als rein sachliche oder positiv formulierte Appelle. Sie schafft Dringlichkeit, ohne zu dramatisieren – und führt zu höherer Verhaltensänderungsbereitschaft, insbesondere in Simulationen oder Rückmeldungen.

3. Soziale Vergleichswerte: Peer Pressure & Normatives Feedback

Menschen orientieren sich stark am Verhalten ihrer Peers – insbesondere in unsicheren oder mehrdeutigen Situationen. Dieses Prinzip des »Social Proof« kann in Awareness-Programmen strategisch genutzt werden, um sichere Verhaltensweisen als soziale Norm zu etablieren.

Beispiele

- »90 % Ihrer Kolleg:innen haben den Phishing-Versuch erkannt – Sie auch?«
- Gamifizierte Dashboards, die anonymisierte Vergleichswerte pro Team anzeigen
- Team-Challenges mit positiver Verstärkung bei kollektiver Sicherheitsleistung

Solche Rückmeldemechanismen erzeugen einen sanften sozialen Druck, ohne zu stigmatisieren. Gleichzeitig wird sichtbar: Sicherheitsverhalten ist kein individueller Akt, sondern eingebettet in eine kollektive Erwartungshaltung – und damit Teil der Kultur.

Sicherheitsverhalten entsteht nicht durch Appelle – sondern durch Design.

CISOs, die Behavioral Design ernst nehmen, gestalten Sicherheit nicht nur in Policies oder Trainings, sondern in der Architektur der Entscheidungsumgebung. Nudging, Defaults und Framing-Techniken wirken dort, wo klassische Awareness oft ansetzt: im Moment der Handlung.

Indem Sicherheit zur bequemeren, sozial anerkannten und emotional stärker verankerten Wahl gemacht wird, lässt sich Sicherheitsverhalten systematisch beeinflussen – ohne Zwang, aber mit Wirkung.

Feedback & Verstärkung

Ein oft unterschätzter, aber entscheidender Erfolgsfaktor für nachhaltige Verhaltensänderung im Sicherheitskontext ist der gezielte Einsatz von Feedback und Verstärkungsmechanismen. Menschen ändern ihr Verhalten nicht allein durch Wissen oder gute Absicht – sondern durch konsequente, zeitnahe und kontextrelevante Rückmeldungen, die ihre Entscheidungen positiv oder negativ verstärken.

In der Verhaltenspsychologie ist dieses Prinzip gut belegt: Verhalten, das unmittelbar auf eine Reaktion trifft, wird als bedeutsam wahrgenommen – Verhalten, das ohne Rückmeldung bleibt, wird als irrelevant abgetan und meist nicht wiederholt. Für Awareness-Programme bedeutet das: Ohne Feedback keine Lernkurve, keine Konsolidierung, keine Kulturveränderung.

1. Sofortiges Feedback: Lernen im Moment des Handelns

Eine der effektivsten Maßnahmen besteht darin, Mitarbeitenden direkt nach einer sicherheitsrelevanten Handlung Feedback zu geben. Besonders bei simulierten Angriffen – etwa Phishing-Tests – ist der Zeitpunkt entscheidend: Ein Hinweis, der Stunden oder Tage später kommt, verpufft. Dagegen kann eine Rückmeldung in Echtzeit eine tiefe, emotionale Lernerfahrung auslösen.

Beispiele

- Ein Pop-up unmittelbar nach dem Klick auf einen simulierten Phishing-Link, das erklärt, woran der Betrugsversuch zu erkennen gewesen wäre.
- Kontextualisierte Hinweise (»Dieser Link führte auf eine gefälschte Login-Seite – in einem echten Fall wären Ihre Zugangsdaten kompromittiert worden.«)
- Verknüpfung mit Microlearning-Units, die exakt den gemachten Fehler adressieren.

Dieses situationsnahe Lernen transformiert abstrakte Bedrohungen in konkrete, persönliche Erfahrungen – ein Schlüssel zur langfristigen Verhaltensänderung.

2. Positive Verstärkung: Belohnung sichert Wiederholung

Neben korrektivem Feedback ist auch positive Verstärkung ein zentraler Hebel im Behavioral Design. Verhalten, das positiv wahrgenommen und sozial anerkannt wird, hat eine höhere Wahrscheinlichkeit, wiederholt zu werden – insbesondere, wenn es sichtbar und emotional belohnt wird.

Beispiele

- »Security Champion«-Badges oder Zertifikate für Mitarbeitende mit hoher Awareness-Performance.
- Punktesysteme oder Ranglisten im Teamvergleich – gekoppelt an sichtbare, aber nicht beschämende Bewertungskriterien.
- Sichtbare Wertschätzung durch Führungskräfte, etwa in Form von Dankesnachrichten, kurzen Videobotschaften oder öffentlichen Erwähnungen im Intranet.

Diese Maßnahmen wirken nicht nur motivierend auf Einzelpersonen, sondern etablieren sichere Verhaltensweisen als sozialen Standard. Sie erzeugen intrinsische Motivation, weil Sicherheit als Teil des professionellen Selbstbildes erlebt wird – nicht als zusätzliche Belastung.

3. Sichtbarkeit & soziale Verstärkung im Teamkontext

Verhalten wird auch durch das beobachtbare Verhalten anderer beeinflusst. Daher ist es entscheidend, sicherheitskonformes Handeln nicht unsichtbar im Hintergrund ablaufen zu lassen, sondern sichtbar im Team zu machen. Die gezielte Sichtbarkeit schafft soziale Normen und etabliert Sicherheit als Teil des kollektiven Selbstverständnisses.

Beispiele

- Transparente Erfolgsdashboards: z. B. »Unser Team hat in der letzten Phishing-Simulation eine Erkennungsrate von 92 % erreicht.«
- Regelmäßige Team-Feedback-Runden zur Reflexion sicherheitsrelevanter Entscheidungen (z. B. im Rahmen von Retro-Formaten bei DevOps-Teams).
- Peer-to-Peer-Lob für sicherheitsbewusstes Verhalten – z. B. ein einfaches Kudos-System für gemeldete Vorfälle oder identifizierte Schwachstellen.

Diese soziale Rückkopplung sorgt dafür, dass Sicherheit nicht als individuelles, sondern als gemeinschaftliches Ziel wahrgenommen wird – eine Voraussetzung für kulturellen Wandel.

Ein Awareness-Programm ohne Feedback bleibt abstrakt. Eines mit Feedback wird konkret. Und ein Programm mit gezielter Verstärkung wird transformativ. CISOs, die diese Mechanismen konsequent nutzen, erzeugen nicht nur Wissenszuwachs, sondern eine messbare Verbesserung im Sicherheitsverhalten ihrer Organisation – schnell, skalierbar und kulturell wirksam.

Sicherheitskultur als sozialer Referenzrahmen

Sicherheitsbewusstsein lässt sich nicht allein durch Trainings oder Policies verordnen – es muss sich in der Kultur einer Organisation verankern. Kultur ist dabei mehr als ein Schlagwort. Sie bezeichnet das System aus geteilten Überzeugungen, informellen Regeln und sozialen Erwartungen, das das tägliche Verhalten der Mitarbeitenden steuert – oft stärker als jede Richtlinie.

Im Kontext von Security Awareness ist es daher entscheidend zu verstehen: Kultur ist der Referenzrahmen, in dem sicherheitsrelevante Entscheidungen getroffen werden. Ein Awareness-Programm, das nicht auf diese kulturelle Dimension einzahlt, bleibt taktisch – und wird nie strukturelle Wirksamkeit entfalten.

Drei kulturelle Voraussetzungen sind dabei zentral für den Erfolg sicherheitsförderlicher Initiativen:

1. Sicherheit muss sozial erwünscht sein

Verhalten wird in Organisationen stark davon beeinflusst, was als leistungsförderlich, erwünscht und anerkannt gilt. Solange Sicherheit als bürokratische Hürde oder Compliance-Pflicht wahrgenommen wird, bleibt sie ein Randthema. Erst wenn sicheres Verhalten als Bestandteil guter Performance gilt – gleichwertig zu Produktivität, Qualität oder Innovation –, entsteht ein positiver sozialer Druck in Richtung Sicherheitsbewusstsein.

Praktischer Hebel:

- Verknüpfe sicherheitsbewusstes Handeln mit bestehenden Leistungsmetriken.
- Mach sichtbare Anerkennung von sicherem Verhalten zum Bestandteil von Feedbackgesprächen, Team-Dashboards oder Incentive-Modellen.
- Kommuniziere klare Leadership-Botschaften: »Gute Arbeit heißt auch: sicher arbeiten.«

2. Verantwortung muss kollektiv getragen werden

Sicherheitskultur entsteht nur dort, wo Verantwortung nicht delegiert, sondern geteilt wird. Wenn Sicherheit ausschließlich als Aufgabe der IT oder des CISO-Teams gesehen wird, bleibt sie strukturell unterdimensioniert. Erst wenn alle Mitarbeitenden sich als Mitverantwortliche begreifen – vom First-Level-Support bis zum Executive Board – entsteht die notwendige Dichte an Aufmerksamkeit, um Angriffe frühzeitig zu erkennen und Risiken zu minimieren.

Praktischer Hebel:

- Fördere das Prinzip der kollektiven Vorfallmeldung: »Wir alle melden Vorfälle, egal wie klein oder unklar.«

- Nutze teamübergreifende Simulationen oder Incident-Response-Übungen, um das gemeinsame Verantwortungsgefühl zu stärken.
- Betone in der Kommunikation: »Security ist Teamsport – nicht Einzeldisziplin.«

3. Vertrauen muss selbst bei Fehlverhalten bestehen

Einer der stärksten Kulturindikatoren ist der Umgang mit Fehlern. In Organisationen, in denen Fehlverhalten sanktioniert oder stigmatisiert wird, herrscht Schweigen – nicht Sicherheit. Doch gerade im Cybersecurity-Kontext ist es entscheidend, dass Vorfälle schnell und offen gemeldet werden. Dazu braucht es eine Vertrauenskultur, die auf dem Prinzip »No blame, just report« basiert.

Praktischer Hebel:

- Implementieren Sie eine blame-free Reporting-Kultur, gestützt durch klare Kommunikation und Schutzmechanismen.
- Erzählen Sie positive Geschichten über Vorfälle, die rechtzeitig gemeldet und dadurch entschärft wurden – statt über Eskalationen, die Schuldige suchen.
- Integrieren Sie das Prinzip in Ihre Policies: »Melden ist wichtiger als perfekt handeln.«

Tipp - Führungskräfte als kulturelle Verstärker nutzen

Die Wirkung von Sicherheitskultur lässt sich exponentiell steigern, wenn Führungskräfte aktiv eingebunden werden. Denn kulturelle Normen entstehen nicht nur durch Inhalte, sondern vor allem durch Vorbilder. Wenn Manager:innen sich sichtbar sicher verhalten, Awareness-Trainings ernst nehmen und positives Verhalten anerkennen, senden sie starke Signale: »Das ist uns wichtig.«

Beispiele

- Führungskräfte erhalten gezielte Awareness-Inhalte mit Business Impact-Fokus.
- Führungspersonen übernehmen Sponsorship-Rollen für Awareness-Kampagnen, um ihre Reichweite gezielt für Kulturentwicklung zu nutzen.

Alle technischen, prozessualen und didaktischen Maßnahmen der Security Awareness entfalten erst dann ihre volle Wirkung, wenn sie in einer Kultur verankert sind, die Sicherheit sozial legitimiert, kollektiv trägt und vertrauensbasiert lebt. Die Aufgabe des CISO ist es nicht nur, Maßnahmen zu entwerfen – sondern vor allem,

einen Referenzrahmen zu schaffen, in dem sich diese Maßnahmen entfalten dürfen.

Fazit: Vom Wissen zum Verhalten

Ein Security-Awareness-Programm, das menschliches Verhalten nicht systematisch einbezieht, bleibt zwangsläufig begrenzt in seiner Wirkung. Es wird reaktiv statt präventiv, formell statt wirksam, und bleibt oft auf die Rolle eines jährlichen Compliance-Trainings reduziert – mit dem Ergebnis, dass Sicherheit im Alltag nicht stattfindet.

Doch Informationssicherheit ist kein reines Wissensproblem. Sie ist ein Verhaltensphänomen. Die meisten erfolgreichen Angriffe setzen auf menschliche Schwächen, nicht technische Lücken. Wer Sicherheitskultur ernsthaft verändern will, muss daher dort ansetzen, wo Verhalten entsteht: im Zusammenspiel von Motivation, Fähigkeit, sozialem Kontext und situativen Auslösern.

Die Verantwortung von CISOs geht damit über Technik, Prozesse und Governance hinaus. Sie müssen lernen, wie Verhalten gestaltet werden kann – subtil, aber wirksam. Das bedeutet:

- Psychologische Hebel systematisch einbauen: durch Framing, Defaults, Feedback und Nudging.
- Sicheres Verhalten ermöglichen statt fordern: durch einfache, zugängliche Entscheidungen im Alltag.
- Sicherheit sichtbar machen und verstärken: durch soziale Rückmeldung, Anerkennung und kulturelle Normen.

Ein so gestaltetes Awareness-Programm wird nicht als Pflichtübung erlebt, sondern als Unterstützung im Arbeitsalltag. Es verwandelt Sicherheit vom abstrakten Prinzip zur gelebten Gewohnheit, verankert im Mindset der Mitarbeitenden und gestützt durch die tägliche Praxis.

Erst wenn Sicherheit als sozial legitimiertes, emotional verankertes und kognitiv erleichtertes Verhalten verstanden wird, entsteht eine echte Sicherheitskultur. Und genau hier liegt der strategische Hebel für moderne CISOs: Awareness nicht als einmaliges Projekt zu sehen – sondern als kontinuierliche, interdisziplinäre Verhaltensarchitektur, die Sicherheit von innen heraus stärkt.

Programmaufbau: Governance, Ownership und Ressourcen

Ein wirkungsvolles Security-Awareness-Programm erschöpft sich nicht in ansprechendem Content, unterhaltsamen Phishing-Simulationen oder interaktiven Trai-

ningsmodulen. Solche Elemente sind notwendig – aber nicht hinreichend. Was häufig fehlt, ist eine strukturierte Verankerung des Programms in der Governance der Sicherheitsorganisation: mit klaren Zuständigkeiten, definierten Budgets, messbaren Zielgrößen und einem organisatorischen Mandat, das Awareness als gleichwertige Sicherheitsfunktion neben Disziplinen wie Incident Response, Identity & Access Management oder Detection Engineering positioniert.

Die strategische Herausforderung besteht darin, Awareness aus dem Schattenbereich der »weichen Faktoren« zu holen und als eigenständige Domäne zu behandeln – nicht als Kommunikationskampagne, nicht als HR-Initiative, sondern als Teil der sicherheitskritischen Gesamtarchitektur.

1. Governance: Awareness als gleichwertige Sicherheitsfunktion etablieren

In einer ausgereiften Sicherheitsorganisation ist Awareness nicht Teil der internen Kommunikation, sondern Teil der CISO-Strategie. Das bedeutet: Es gibt definierte Steuerungsgremien, ein kontinuierliches Reporting, KPIs und eine Anbindung an die Risikosteuerung.

Konkret heißt das:

- Einbindung ins Information Security Management System (ISMS) gemäß ISO/IEC 27001 oder NIST CSF 2.0
- Regelmäßiges Reporting an das Security Steering Committee, inklusive Metriken wie Klickrate, Meldeverhalten, Awareness-Maturity-Score
- Verknüpfung mit Risikomanagementprozessen: z. B. Bewertung des Human Layer als Angriffsfläche in Risikobewertungen oder Szenarioanalysen

Nur so entsteht formale Sichtbarkeit und Priorität im Sicherheitsbudget und in der strategischen Ressourcenplanung.

2. Ownership: Klar definierte Zuständigkeiten schaffen

Einer der häufigsten Fehler bei Awareness-Initiativen ist die diffuse Verantwortlichkeit. Wenn sich niemand wirklich verantwortlich fühlt, bleibt das Programm fragmentiert und ineffizient. Die zentrale Frage lautet daher: Wer »besitzt« Awareness – fachlich, operativ und strategisch?

Best Practices für Ownership-Strukturen:

- Fachliche Verantwortung liegt beim CISO bzw. einer dedizierten Awareness Lead-Funktion im Security-Team.
- Operative Umsetzung kann interdisziplinär erfolgen – etwa mit HR, Communications, Legal und IT – aber unter zentraler sicherheitsfachlicher Steuerung.
- Rollenprofile definieren klar: Wer erstellt Inhalte? Wer misst Wirkung? Wer priorisiert Zielgruppen? Wer verantwortet Simulationen und Audits?

Awareness braucht damit denselben professionellen Steuerungsanspruch wie jede andere sicherheitsrelevante Funktion.

3. Ressourcen: Nachhaltige Planung statt Nebenprojekt-Logik

Ein weiteres häufiges Defizit liegt in der fehlenden oder unzureichenden Ressourcenplanung. Awareness wird oft als »Nebenprojekt« betrieben – ohne dedizierte Budgets, Tools oder personelle Ausstattung. Das ist riskant, denn nachhaltige Verhaltensveränderung ist kein Einmalaufwand, sondern ein kontinuierlicher, skalierbarer und adaptiver Prozess.

Erforderliche Ressourcen-Elemente:

- Menschliche Ressourcen: Mindestens eine halbe FTE im Security-Team, mittelfristig eine eigene Rolle oder Unit je nach Unternehmensgröße
- Technologische Ressourcen: Awareness-Plattformen, Simulationstools, Behavioral Analytics
- Kreative Ressourcen: Storytelling, Content Creation, UX/Design-Kompetenz – idealerweise in Zusammenarbeit mit Corporate Communications

Change-Management-Kompetenz: Um Lernimpulse nicht nur zu verbreiten, sondern auch in Abläufe und Kultur zu integrieren

Ohne diese Ressourcen bleibt Awareness ein kosmetischer Bestandteil des Sicherheitsprogramms – mit wenig Hebelwirkung im realen Verhalten.

Wer Awareness organisatorisch als Kommunikationsprojekt oder HR-Aufgabe abstempelt, verkennt das enorme Risiko- und Wirkpotenzial des Human Layers. Menschen sind keine »lückenhafte Firewall«, sondern entscheidende Sensoren und Schutzmechanismen im Sicherheitsdispositiv – wenn sie gezielt aktiviert, unterstützt und befähigt werden.

Dazu braucht es nicht nur Inhalte – sondern Strukturen, Prozesse, Budgets und Leadership-Mandate. Nur so wird Awareness von der guten Idee zur messbaren Sicherheitsdisziplin.

Governance: Wo Awareness organisatorisch verankert sein muss

Ein wirksames Awareness-Programm braucht mehr als gute Inhalte und engagierte Kommunikation – es braucht eine klare Verortung innerhalb der Governance-Struktur der Organisation. Denn Awareness ist kein weiches Begleitthema, sondern ein integraler Bestandteil des übergeordneten Risiko- und Sicherheitsmanagements. Genau wie Incident Response, Access Control oder Business Continuity muss auch Awareness formell eingebunden sein – in das Information Security Management System (ISMS), das unternehmensweite GRC-Modell oder die Risikomanagement-Architektur.

Die Frage lautet daher nicht mehr ob, sondern wo und wie Awareness in der Sicherheitsgovernance verankert wird.

In modernen Sicherheitsorganisationen wird das »Human Layer« – also die Schnittstelle zwischen Mensch, Information und digitalem Verhalten – als vollwertige Risikodimension behandelt. Das bedeutet konkret: Awareness ist nicht mehr nachgelagert, sondern wird von Anfang an als strategisches Steuerungselement in der Sicherheits- und Risikostruktur berücksichtigt.

Die ideale Einbettung erfolgt über das ISMS, etwa gemäß ISO/IEC 27001, NIST CSF 2.0 oder einem GRC-Modell, das organisatorische Risiken systematisch aggregiert. Damit wird Awareness steuerbar, messbar und gegenüber internen wie externen Stakeholdern prüfbar und auditierbar.

Ein funktionierendes Awareness-Programm braucht klar zugewiesene Verantwortlichkeiten auf allen Ebenen. Im Folgenden eine strukturierte Darstellung der zentralen Stakeholder und ihrer Funktionen:

Governance-Ebene	Verantwortung
CISO / Security Leadership	Strategische Gesamtverantwortung, Zielvorgaben, Budgetfreigabe, Risikointegration
Awareness Owner / Program Lead	Operative Steuerung des Programms, Kampagnenplanung, KPI-Management, Tool-Auswahl
HR / People / L&D	Integration in Onboarding, kontinuierliche Mitarbeiterentwicklung, Trainingsdesign
Legal / Compliance	Sicherstellung regulatorischer Anforderungen, Richtlinienabgleich, Auditfähigkeit
Kommunikation / Change	Messaging-Strategie, Storytelling, interne Kanalkoordination, kulturelle Einbettung

Diese Aufteilung sichert, dass Awareness nicht in Silos betrieben wird, sondern funktionsübergreifend eingebettet ist – mit klarer Linienführung, aber kollaborativer Umsetzung.

Tipp - Awareness Steering Committee als Steuerungsgremium

Ein effektiver Weg zur Operationalisierung dieser Governance-Struktur ist die Einrichtung eines Awareness Steering Committees – eines fachübergreifenden Steuerungsgremiums, das als Bindeglied zwischen Strategie, Umsetzung und Business fungiert.

Aufgaben und Struktur dieses Gremiums:

- Teilnehmer: Vertretung aus Security, HR, Legal, Comms, Business Units, ggf. Betriebsrat

- Taktung: Quartalsweise Sitzungen, bei Bedarf ad hoc Reviews
- Funktion: Strategische Abstimmung, Review laufender Kampagnen, KPI-Analyse, Freigabe neuer Initiativen, Eskalation sicherheitskritischer Trends
- Verbindung zum Enterprise Risk Management: Einspeisung von Awareness-bezogenen KPIs in Risikoberichte, Management-Reviews und GRC-Dashboards

So wird Awareness nicht nur betrieben, sondern gesteuert, validiert und kontinuierlich weiterentwickelt – mit direkter Sichtbarkeit auf Führungsebene.

Ein Awareness-Programm, das nicht sauber in die Sicherheitsgovernance eingebettet ist, bleibt reaktiv, ad hoc und isoliert. Nur durch klare Verantwortlichkeiten, formelle Strukturen und funktionsübergreifende Steuerung entsteht ein Ordnungsrahmen, der Skalierung, Verbindlichkeit und strategische Relevanz sicherstellt.

CISOs sollten daher darauf achten, Awareness nicht in der Kommunikation, sondern im Risikomanagement zu verankern – und damit das Thema aus der Sphäre der freiwilligen Beteiligung in den Bereich der organisationalen Notwendigkeit zu überführen.

Budgetierung und Ressourcen

Ein Security-Awareness-Programm, das nicht angemessen finanziert ist, bleibt zwangsläufig unter seinen Möglichkeiten – und verfehlt oft seinen eigentlichen Zweck: die nachhaltige Veränderung von Verhalten in sicherheitsrelevanten Kontexten. In der Realität vieler Unternehmen ist Awareness jedoch nach wie vor unterfinanziert, unterpriorisiert und unterstrukturiert – oft als Restposten in Kommunikations- oder HR-Budgets geführt.

Für CISOs ergibt sich daraus ein klarer Handlungsauftrag: Awareness muss wie jede andere sicherheitskritische Domäne behandelt werden – mit eigenem Budgettrack, klar definierten Investitionszielen und einer belastbaren Ressourcenplanung, die auf strategischen Risiken und nicht auf Restmitteln basiert.

1. Warum Budget kein »Nice-to-have«, sondern strategische Notwendigkeit ist

Die Angriffsrealität hat sich verändert. Der menschliche Faktor ist heute Angriffsfläche Nr. 1 – sei es durch Phishing, Social Engineering, Credential Stuffing oder CEO Fraud. Zugleich zeigen zahlreiche Studien, dass sich durch gezielte Awareness-Maßnahmen das Risiko menschlichen Fehlverhaltens signifikant reduzieren lässt.

Die Budgetierung für Awareness ist deshalb kein weicher Kulturbeitrag, sondern Risikomitigation auf strategischer Ebene – vergleichbar mit Investitionen in SIEM,

EDR oder IAM. Wer hier spart, spart am falschen Ende – und lässt die größte Schwachstelle im Sicherheitsdispositiv offen.

2. Typische Budgetposten für ein wirkungsvolles Awareness-Programm

Ein modernes Awareness-Programm umfasst weit mehr als Schulungen. Es ist ein kontinuierlicher Kommunikations- und Verhaltensprozess, der gezielte Investitionen in verschiedene Ressourcentypen erfordert:

Kategorie	Typische Ausgaben
Technologie / Plattformen	Learning Management System (LMS), Phishing-Simulationstools, Analytics-Plattformen
Content-Produktion	Interaktive Lernmodule, Videoformate, Erklärgrafiken, Podcasts, Story-basierte Lernstrecken
Kommunikation & Change	Agenturleistungen für Kampagnendesign, internes Messaging, Behavioral Design-Beratung
Incentives & Recognition	Belohnungssysteme, Gamification-Preise, Merchandise, Zertifikate
Personelle Ressourcen	Awareness Manager:in, Content Designer, externe Fachkräfte, Redakteure, Schulungspartner
Monitoring & Evaluation	KPI-Dashboards, Wirksamkeitsstudien, Awareness-Audits, Benchmarking

Diese Budgetkategorien müssen nicht alle auf einmal abgedeckt werden – aber ohne eine strukturierte Ressourcenzuordnung bleibt das Programm reaktiv und beliebig.

3. Personalressourcen: Awareness braucht dedizierte Kapazitäten

Neben finanziellen Mitteln ist personelle Kapazität der kritische Engpass. Awareness-Programme dürfen nicht als Nebenaufgabe im Security-Team mitlaufen. Eine eigene Rolle – intern oder extern besetzt – ist ab mittlerer Unternehmensgröße zwingend erforderlich.

Tipp – Empfehlung nach Unternehmensgröße

- <500 MA: Awareness als Teilrolle (z. B. 0.25–0.5 FTE)
- 500–2.000 MA: Dedizierte Awareness-Funktion (1 FTE)
- Ab 2.000 MA / regulierte Branchen: Awareness-Team mit Spezialisierungen (Content, Kampagnen, Analytics)

So wird aus Awareness ein programmatisch geführter Veränderungsprozess – nicht eine lose Abfolge von Einzelmaßnahmen.

4. Faustregel für die Budgetplanung

Zur Orientierung empfiehlt sich folgende Daumenregel, abgestimmt auf Reifegrad und Bedrohungslage der Organisation:

2–5 % des gesamten Security-Budgets sollten für Awareness- und Kulturmaßnahmen reserviert werden.

Diese Spanne berücksichtigt:

- Regulatorische Anforderungen (z. B. ISO 27001, DORA, HIPAA)
- Risikoprofil (z. B. stark phishbare Rollen, hoher Remote-Anteil, hohe Third-Party-Exposure)
- Kulturelle Reife (z. B. hohe Fluktuation, geringer Meldegrad, fehlende Sicherheitsroutinen)

Beispiel

Ein Unternehmen mit 5 Mio. € Security-Budget sollte 100.000–250.000 € p.a. für Awareness-Programme einplanen – als kontinuierlichen Invest, nicht als einmalige Kampagne.

Security Awareness ist keine Nebensache. Sie ist ein integraler Bestandteil der Sicherheitsarchitektur – und muss entsprechend finanziell unterlegt und professionell betrieben werden. Ein strukturiertes Awareness-Budget signalisiert nach innen wie außen: Sicherheit ist nicht nur Technik, sondern auch Verhalten – und beides ist gleich wichtig.

Zielgruppenanalyse: Personas & Risikobasierte Segmentierung

Ein zentrales Prinzip erfolgreicher Awareness-Programme ist die Differenzierung nach Zielgruppen. Denn Sicherheitsverhalten ist nicht generisch – es ist rollen-, kontext- und risikobasiert. Mitarbeitende in verschiedenen Funktionen, mit unterschiedlichen Zugriffsrechten, Arbeitsweisen und Exposure-Leveln benötigen spezifische Inhalte, Formate und Impulse, um wirksam adressiert zu werden.

Einheitliche Schulungen nach dem Gießkannenprinzip – z. B. einmal jährlich für alle dieselbe Präsentation – sind aus verhaltenspsychologischer und risikotechnischer Sicht ineffizient und oft kontraproduktiv. Ziel muss es sein, risikobasierte, rollenorientierte und kontextadaptive Lernpfade zu etablieren – im Sinne einer Security-Awareness-Persona-Strategie.

1. Differenzierte Zielgruppenmodelle: Personas statt Massenansprache

Ein erster Schritt besteht darin, die Belegschaft in funktionale und verhaltensrelevante Personas zu segmentieren. Diese orientieren sich weniger an Organigrammen, sondern an sicherheitsrelevanten Merkmalen, wie z. B. Zugang zu kritischen Systemen, typisches Angriffsprofil oder Remote-Exposition.

Typische Awareness-Personas sind:

Persona	Sicherheitsrelevanz
Entwickler	Zugang zu Quellcode, CI/CD-Pipelines, Geheimnissen, Schnittstellenrisiken
IT-Admins	Hohe Rechte, Infrastruktursicht, Ziel für Privilege Escalation & Lateral Movement
Führungskräfte	Hohe Relevanz für CEO-Fraud, Business Email Compromise, Datensensibilität
Vertrieb / CRM	Umgang mit Kundendaten, externe Kommunikation, Phishing-Exposure
Finance / Legal	Zahlungsströme, Verträge, besonders attraktiv für gezielte Angriffe
Allgemeine Nutzer	Standardnutzung, aber häufiges Ziel für Phishing, Social Engineering

Jede dieser Gruppen erfordert maßgeschneiderte Inhalte, die ihre konkrete Bedrohungslage und Alltagssituation reflektieren.

2. Bedrohungsspezifische Inhalte und Szenarien: Realismus erzeugt Relevanz

Die Effektivität von Awareness steigt erheblich, wenn Inhalte szenarienbasiert und bedrohungsspezifisch gestaltet sind. Mitarbeitende erkennen sich in realistischen Fallbeispielen eher wieder und bewerten das Gelernte als relevant – was eine zentrale Voraussetzung für tatsächliche Verhaltensänderung ist.

Beispielhafte Szenarien nach Zielgruppe:

- Entwickler:innen Supply Chain Attacks via Package Manager, Hardcoded Secrets, Git-Leaks
- Führungskräfte → Spear Phishing mit M&A-Tarnung, Fake-Investoren, CEO-Fraud
- Vertrieb → Phishing mit CRM-Fakes, manipulierte Kundendokumente, Kollaborationstools
- Finance → Zahlungsumleitungen durch BEC, manipulierte Rechnungen mit Echtbezug

Inhalte, die diese Bedrohungen situativ, sprachlich und visuell aufgreifen, erzeugen höhere Aufmerksamkeit und stärkere kognitive Verankerung.

3. Rollenbasierte Maßnahmen: »Least Privilege meets Least Effort«

Die risikobasierte Segmentierung sollte sich nicht nur in den Inhalten, sondern auch in der Lerntiefe, Frequenz und methodischen Ausgestaltung widerspiegeln. Hier gilt das Prinzip: Je höher das Risiko, desto höher die Awareness-Anforderungen – aber immer mit geringstmöglicher Friktion.

Best Practices für rollenbasierte Awareness-Aussteuerung:

- Hohe-Risiko-Gruppen (Admins, Executives): Häufige, kurze Microlearnings, simulationsbasierte Szenarien, Just-in-Time-Nudges
- Mittleres Risiko (Finance, Vertrieb): Kombinierte Lernpfade mit Tests, Social Proof, Rollenspiele
- Standard-User:innen: Grundsensibilisierung, anlassbezogene Prompts, visuelle Hinweise im Workflow

Ziel ist es, Awareness nicht als Belastung, sondern als passgenaue Unterstützung im jeweiligen Arbeitskontext zu positionieren – »Least Privilege meets Least Effort«.

Ein modernes Awareness-Programm unterscheidet sich vom Standardtraining durch Relevanz, Präzision und Differenzierung. Wer Personas definiert, Inhalte risikobasiert zuschneidet und Methoden adaptiv einsetzt, erhöht nicht nur die Lerneffizienz – sondern auch die tatsächliche Verhaltenswirkung im Arbeitsalltag.

CISOs, die Awareness als »Human Risk Management« verstehen, gestalten ihre Programme datengetrieben, zielgruppenspezifisch und taktisch flexibel – und sichern damit den entscheidenden Layer moderner Sicherheitsarchitekturen: den Mensch im Kontext seines Handelns.

Kampagnendesign: Formate, Frequenz, Kanäle

Ein Awareness-Programm ist nur dann wirksam, wenn es nicht nur strategisch durchdacht, sondern auch kommunikativ wirksam umgesetzt wird. Die besten Inhalte nützen nichts, wenn sie ihre Zielgruppen nicht erreichen – oder im falschen Moment, über die falschen Kanäle oder im falschen Format ausgespielt werden. Entscheidend ist daher ein bewusst designtes Kampagnenmodell, das Inhalte so verteilt, dass sie wahrgenommen, verstanden und erinnert werden – und im besten Fall: Verhalten verändern.

CISOs und Awareness-Verantwortliche müssen dabei zunehmend interdisziplinär denken: Inhalte, Formate, Mediennutzung und psychologische Trigger verschmelzen zu einem multimodalen Lern- und Kommunikationsprozess.

1. Multimodale Inhalte: Diversität erzeugt Wirkungstiefe

Ein zentrales Element erfolgreichen Kampagnendesigns ist die Nutzung verschiedener Inhaltsformate, die unterschiedliche kognitive und emotionale Kanäle ansprechen. Menschen lernen unterschiedlich – durch Text, Bild, Ton, Interaktion oder spielerische Elemente. Ein modernes Awareness-Programm nutzt daher multimodale Formate, um maximale Reichweite und Wirkung zu erzielen.

Die folgende Tabelle stellt typische Formaten und ihre jeweiligen Stärken dar:

Format	Stärken
Video-Clips	Emotionalisierung, Storytelling, schnelle Rezeption
E-Learning-Module	Vertiefung, Prüfungen, Dokumentation
Simulationen	Realitätsnähe, aktivierende Handlung, nachhaltiger Lerneffekt
Gamification	Motivation, soziale Vergleichbarkeit, Relevanz durch spielerische Elemente
Podcasts / Audio	Nebenbei-Konsum, besonders wirksam bei mobilen Zielgruppen oder Führungskräften
Infografiken / OnePager	Visualisierung komplexer Zusammenhänge, geeignet für Print und digitale Kommunikation

Ein abgestimmter Medienmix erhöht die Wahrscheinlichkeit, dass Inhalte nicht nur gesendet, sondern auch internalisiert werden – und adressiert gleichzeitig unterschiedliche Lernpräferenzen.

2. Phishing-Simulationen: Realismus schlägt Routine

Phishing-Simulationen sind ein zentraler Baustein in vielen Awareness-Programmen – zurecht. Sie ermöglichen verhaltensorientiertes Lernen im Realformat, mit direktem Feedback und hoher emotionaler Relevanz. Doch ihr Lernpotenzial hängt stark von der Ausgestaltung ab: Wiederholte Standard-Templates führen schnell zu Abstumpfung und operativer Ignoranz.

Best Practices für wirksame Phishing-Simulationen:

- Rollen- und kontextspezifische Templates (z. B. für HR, Entwickler, Finance, Vertrieb)
- Integration in Kampagnen (z. B. gekoppelt an Schulungen, Microlearning oder Feedback-Module)
- Differenzierte Auswertung und Peer-Vergleich zur Verankerung des Lerneffekts
- Narrative Koppelung mit echten Bedrohungen (»Diese Simulation basiert auf einem realen Vorfall bei Unternehmen X«)

Simulationen sollten nicht als Test, sondern als Lernimpuls mit Relevanz verstanden und kommuniziert werden.

3. Interne Kommunikation als Awareness-Verstärker

Awareness ist kein »Spezialthema« für Security – es muss in die Gesamtkommunikation des Unternehmens integriert sein. Die Zusammenarbeit mit interner Kommunikation, Employer Branding, HR und Change Management ist entscheidend, um Awareness-Botschaften in vertrauten Kanälen und in passender Tonalität zu platzieren.

Wirkungsvolle Kommunikationskanäle:

- Intranet-Artikel & Kampagnenseiten
- Regelmäßige Awareness-Snippets im Unternehmens-Newsletter
- Interaktive Elemente in Townhalls oder Team-Standups
- Bildschirmschoner, digitale Plakate, Slack-/Teams-Bots

Kampagnen müssen dabei sowohl »Push«- als auch »Pull«-Elemente beinhalten: Einerseits regelmäßige Impulse – andererseits zugängliche Lernangebote, wenn Interesse oder Bedarf entsteht.

4. Microlearning & Security Moments: Lernen im Fluss der Arbeit

Ein besonders wirksames Awareness-Prinzip ist situatives Lernen im Moment der Handlung. Statt lange Trainingsblöcke, die außerhalb des Arbeitskontextes stattfinden, setzen moderne Programme auf Microlearning und »Security Moments« – kurze, kontextspezifische Lernimpulse genau dort, wo sich sicherheitsrelevante Entscheidungen ereignen.

Beispielhafte Security Moments:

- Pop-up beim Öffnen eines Dateianhangs: »Worauf achten bei externen PDFs?«
- Hinweis beim Anlegen eines neuen Passworts: »Nutze passphrases statt Sonderzeichenkombinationen«
- Reminder im Projektboard: »Teile keine Zugangsdaten in Jira-Kommentaren«

Solche just-in-time-Nudges kombinieren Awareness mit realer Handlung – und wirken dort, wo Verhalten entsteht.

Ein wirksames Awareness-Programm lebt nicht von einem Format oder einer Maßnahme – es entsteht durch die Orchestrierung mehrerer Formate, Frequenzen und Kanäle, abgestimmt auf Zielgruppen, Verhalten und Unternehmenskontext. Entscheidend ist, Lernen nicht als Ausnahme, sondern als Teil des Arbeitsalltags zu gestalten – emotional, kognitiv und situativ.

Führungskräfte & Kulturmultiplikatoren

In jeder Organisation gibt es unsichtbare Kräfte, die Verhalten stärker steuern als jede Policy, jedes Training und jede technische Barriere. Eine dieser Kräfte ist das soziale Modelllernen – Menschen orientieren sich an dem, was sie bei anderen beobachten, vor allem bei denen, die Macht, Einfluss oder Vorbildfunktion besitzen. Führungskräfte und »High-Trust-Rollen« wirken dadurch wie Kulturmultiplikatoren: Ihr Verhalten sendet implizite Signale darüber, was akzeptabel, relevant und erstrebenswert ist.

Für ein modernes Awareness-Programm bedeutet das: Ohne aktive Einbindung von Führungskräften bleibt Sicherheitskultur flach. Nur wenn Leadership Security lebt, kann sie auch im Alltag wirksam werden.

1. Das Verhalten von Führungskräften als Referenzrahmen

Führungskräfte definieren durch ihr Handeln implizite Normen. Ob sie E-Mails prüfen, MFA nutzen, Vorfälle melden oder vertrauliche Informationen korrekt klassifizieren – all das wird von ihren Teams beobachtet, bewertet und übernommen. Entsprechend wirkt ihr Verhalten als sozialer Referenzrahmen für Sicherheitskultur – im Positiven wie im Negativen.

Wenn der CEO eine Awareness-Schulung sichtbar ernst nimmt, erhöht das die Teilnahmerate im Unternehmen. Wenn eine Führungskraft jedoch selbst Phishing-Tests ignoriert oder über »übertriebene Sicherheitsvorschriften« lacht, untergräbt das monatelange Aufklärungsarbeit.

Tipps

- Führungskräfte sollten nicht nur »mitmachen«, sondern sichtbar vorangehen: durch Kommunikation, Vorbildverhalten und Sponsorship.
- Fehlverhalten von Führungspersonen darf nicht tabuisiert, sondern im Rahmen eines no-blame-Ansatzes bearbeitet werden – zur Wahrung der Glaubwürdigkeit des Programms.

2. Security als Führungsverantwortung verankern

Awareness und Sicherheitskultur dürfen nicht ausschließlich im CISO-Bereich verortet sein – sie sind auch Teil von Leadership-Exzellenz. Sicherheitsbewusstsein ist damit nicht nur ein »IT-Thema«, sondern ein integraler Bestandteil guter Führung.

Ansätze zur Integration von Security in die Führungsverantwortung:

- Verankerung von Security KPIs in Führungskräfteziele (z. B. Vorfallmeldequote, Team-Teilnahmeraten)
- Inhalte zu Informationssicherheit in Führungskräfteentwicklungsprogramme und Leadership Onboardings
- Strategische Sponsorships von Awareness-Initiativen durch Executives
- »Secure Leadership Playbooks« mit konkreten Handlungsanweisungen für sichere Kommunikation, Vorfallverhalten und Datenschutzführung

So entsteht das Selbstverständnis: Führen heißt auch: für Sicherheit stehen.

3. Schulung und Fokussierung auf High-Impact Roles

Nicht jede Rolle im Unternehmen ist gleich sicherheitskritisch. Es gibt jedoch bestimmte Funktionsgruppen mit hohem Risikopotenzial oder Hebelwirkung, die gezielt und differenziert geschult werden müssen – mit Inhalten, die nicht nur auf technisches Verhalten, sondern auch auf Risiko- und Führungsbewusstsein zielen (siehe dazu auch 26.3).

Als geeignet Maßnahmen haben sich dabei unter anderem, folgende erwiesen:

- Executive Briefings auf Board-Niveau: Keine Schulungen, sondern Risiko-Narrative & Business Impact
- Secure Coding Labs für Entwickler: Hands-on & realitätsnahe Angriffsmodelle
- Incident Walkthroughs für Legal & Finance: Simulationen auf Szenario-Ebene (z. B. Ransomware + Compliance)

Diese Gruppen sind nicht nur Ziel von Angriffen, sondern auch Multiplikatoren für sichere oder unsichere Normen. Ihre Qualifikation ist ein Risikomanagement-Faktor mit strukturellem Impact.

Ein Security-Awareness-Programm, das ohne die aktive Einbindung von Führungskräften operiert, bleibt operativ – nicht kulturell. Erst wenn Security als Teil von Leadership und Verantwortungsverständnis verstanden wird, entstehen verhaltenswirksame, sozial legitimierte Sicherheitsnormen.

CISOs sollten daher bewusst Allianzen mit Führungskräften aufbauen – nicht als Empfänger von Schulungen, sondern als aktive Architekten einer resilienten Unternehmenskultur.

KPIs, Metriken & Wirksamkeitsmessung

Awareness ohne Wirkung ist Kosmetik – und Wirkung ohne Messung ist Behauptung. Für ein modernes, strategisch geführtes Security-Awareness-Programm gilt daher: Transparenz über Effektivität ist essenziell. Wer nicht misst, kann nicht steuern. Wer nicht steuert, kann nicht verbessern. Und wer nicht verbessern kann, verliert Relevanz.

CISOs müssen Awareness deshalb nicht nur inhaltlich und organisatorisch einbetten, sondern auch messbar machen – mit einem strukturierten Set an KPIs, das sowohl technisches Verhalten, kulturelle Reife als auch strategische Steuerung abbildet. Die Kunst liegt dabei in der Ausgewogenheit zwischen quantitativer Präzision und kultureller Aussagekraft.

1. Technische KPIs: Verhalten messen, Trends erkennen

Auf der ersten Ebene geht es um messbare, beobachtbare Reaktionen in Awareness-Maßnahmen – insbesondere im Rahmen von Trainings, Simulationen und Lernformaten. Diese »behavioral signals« liefern eine wertvolle Grundlage für Mustererkennung, Zielgruppenvergleich und Trendanalyse.

Typische technische Metriken:

- Click-Through-Rate (CTR) bei Phishing-Simulationen
- Report Rate: Anzahl korrekt gemeldeter Vorfälle / Simulationen
- Time to Report: Zeit zwischen Simulation und Meldung
- Training Completion Rate: Anteil abgeschlossener Module / Teilnehmerquote
- Quiz Scores: Wissenstransferindikatoren aus Microlearnings
- False Positive Rate: Übervorsichtige Meldungen (zur Kalibrierung)

Diese Kennzahlen liefern harte Daten, um Fortschritt zu belegen, Zielgruppen zu differenzieren und Maßnahmen gezielt zu priorisieren.

2. Kulturelle KPIs: Sicherheitsklima erfassen

Quantitative Verhaltensdaten sind notwendig – aber nicht hinreichend. Denn Sicherheit ist nicht nur Verhalten, sondern auch Haltung. Deshalb müssen Awareness-Programme zusätzlich die subjektive Wahrnehmung und das soziale Klima erfassen – über sogenannte »Cultural Indicators«.

Methoden zur Erhebung kultureller Metriken:

- Security Climate Surveys: Periodische Befragung zu Sicherheitswahrnehmung, Normen und Vertrauen
- Pulse Checks: Kurze, regelmäßige Stimmungstests zu aktuellen Awareness-Themen

- Qualitative Interviews / Fokusgruppen: Tieferes Verständnis für Blockaden, Haltungen, Ideen
- Heatmaps für kulturelle Reife: Visualisierung nach Teams, Regionen, Hierarchieebenen

Fragen könnten lauten:

- »Ich weiß, wie ich einen Sicherheitsvorfall melden kann.«
- »Ich fühle mich verantwortlich für die Informationssicherheit meines Teams.«
- »Fehlverhalten wird bei uns offen, aber nicht strafend angesprochen.«

Solche Daten ermöglichen gezielte Kulturinterventionen und Leadership-Coachings.

3. Strategische KPIs: Awareness als Teil der Unternehmenssteuerung

Awareness muss auf Board-Ebene sichtbar und steuerbar sein. Deshalb sollten die wichtigsten Metriken in das übergreifende Security-KPI-Dashboard integriert werden – idealerweise unter Verwendung einer Balanced Scorecard oder eines Human Risk Index.

Beispiele strategischer Kennzahlen:

- »Human Risk Exposure Index«: Kombination aus CTR, Melderate, MFA-Nutzung, Reporting Time
- »Security Culture Score«: aggregierte Bewertung aus Pulse Surveys & Verhalten
- »Awareness Coverage Rate«: Anteil kritischer Rollen mit abgeschlossenen Trainings + Feedback
- »Security Engagement Quotient«: Kombination aus Interaktionen, Feedback, Aktivitätsrate

Diese Kennzahlen erlauben es, Awareness in strategische Risikoberichte einzubinden, mit Zielwerten zu versehen und deren Veränderung über Zeit darzustellen – auch gegenüber Vorstand, Audit oder Aufsicht.

4. Integration mit GRC- und Audit-Prozessen

Die Wirksamkeit von Awareness darf nicht nur intern sichtbar sein – sie muss auch prüfbar und auditfähig sein. Moderne Awareness-Programme sollten daher in GRC-Systeme integriert sein und auf regulatorische Anforderungen (z. B. ISO 27001, DORA, NIS2, HIPAA) abgestimmt sein.

Typische Integrationspunkte:

- Automatisierte Nachweise für Trainingsteilnahmen und Simulationen
- Risikobasierte Zuweisung von Awareness-Inhalten im GRC-Tool

- Verknüpfung mit Controls aus internen Kontrollsystemen (IKS)
- Audit Trails für Awareness-Kampagnen, inkl. Inhalts-, Zielgruppen- und Ergebnisdokumentation

So wird Awareness nicht nur operativ effektiv, sondern auch compliance-fähig und prüfsicher – ein zunehmend kritischer Erfolgsfaktor in regulierten Branchen.

Ein Awareness-Programm ohne belastbare Messgrößen ist blind. Es kann keine Wirkung belegen, keine Ressourcen rechtfertigen und keine Entscheidungen steuern. Wer dagegen ein strukturiertes KPI-Framework aufbaut, schafft die Grundlage für datengetriebenes Lernen, strategische Verankerung und glaubwürdige Kommunikation gegenüber Geschäftsführung und Aufsicht.

CISOs sollten Awareness daher nicht nur als Kommunikationsprogramm führen, sondern als kennzahlenbasiertes Verhaltensmanagementsystem – verbunden mit Governance, Auditfähigkeit und echter Steuerungsfähigkeit.

Kontinuierliche Verbesserung und Innovationsimpulse

Ein modernes Awareness-Programm darf kein starres, jährliches Schulungskonstrukt sein. In einer sich permanent verändernden Bedrohungslandschaft muss es als dynamisches, lernfähiges System konzipiert sein – kontinuierlich angereichert durch neue Erkenntnisse, Feedback, Vorfallanalysen und technologische Entwicklungen. Nur so bleibt es relevant, wirksam und zukunftsfähig.

CISOs, die Awareness als lebendigen Teil des Sicherheits-Ökosystems begreifen, etablieren nicht nur Trainings – sie schaffen einen adaptiven Kommunikations- und Lernkanal, der sich an reale Risiken und organisatorische Reife anpasst.

1. Lessons Learned aus Vorfällen und Near Misses nutzen

Jeder Sicherheitsvorfall – ob realisiert oder »gerade nochmal gut gegangen« – ist eine wertvolle Lernchance. Wenn Awareness-Programme diese Erkenntnisse zeitnah, kontextsensitiv und anonymisiert in Inhalte überführen, entsteht eine tiefe Verbindung zwischen realer Bedrohung und Verhaltenstraining.

Best Practices zur Integration von Lessons Learned:

- »Case-Based Microlearning«: Kurze Lernmodule auf Basis echter Vorfälle (interne oder externe), angepasst an Zielgruppe und Rolle.
- Incident Reviews mit Awareness-Fokus: Was war der menschliche Faktor? Wie hätte sich der Vorfall durch Awareness verhindern lassen?
- »Near Miss«-Analysen als präventives Lerninstrument – auch bei »fast erfolgreichen« Angriffen.

Der Schlüssel liegt in der sofortigen Operationalisierung dieser Erkenntnisse – nicht als Blame, sondern als kollektiver Lernprozess.

2. Threat Intelligence als Awareness-Treiber

Awareness-Content sollte nicht nur auf bekannten Standards beruhen – er muss sich ständig mit der aktuellen Bedrohungslage synchronisieren. Durch die Integration von Threat Intelligence (TI) lässt sich Awareness nicht nur reaktiv, sondern proaktiv und angriffsspezifisch ausrichten.

Beispielhafte TI-Integration:

- Aktuelle Phishing-Kampagnen im Unternehmensumfeld als Vorlage für Simulationen
- Taktiken aus MITRE ATT&CK (z. B. Initial Access, Credential Harvesting) als Szenarienbasis
- Regionale oder branchenspezifische Threat Reports als Narrative für Führungskräfte-Briefings
- OSINT-basierte Beispiele (z. B. geleakte Accounts oder Domains) als Lernimpulse

So wird Awareness zum realitätsnahen Frühwarn- und Trainingskanal, nicht nur zur abstrakten Schutzmaßnahme.

3. Agile Weiterentwicklung: Feedback-Loops und Iteration

Kontinuierliche Verbesserung erfordert strukturierte Feedback-Prozesse und einen agilen Entwicklungsansatz. Awareness-Programme müssen nicht perfekt starten, aber intelligent iterieren – datenbasiert, nutzerzentriert und eng an die Sicherheitsrealität gekoppelt.

Elemente eines agilen Awareness-Feedbacksystems:

- Microfeedback nach jeder Lernintervention (z. B. 2-Fragen-Surveys)
- Monatliche Stakeholder-Retrospektiven (z. B. mit HR, IT, Legal, Comms)
- User Research: Interviews, Fokusgruppen, Heatmaps zur Wirksamkeit
- »Content Sprint Reviews« mit Security Engineers und Awareness-Team
- A/B-Tests bei Kampagnenformaten: Welche Ansprache, Visualisierung oder Frequenz wirkt besser?

Diese iterativen Zyklen fördern eine Kultur der ständigen Verbesserung, in der Awareness-Formate nicht veralten, sondern sich weiterentwickeln wie lebendige Software.

Awareness darf kein statisches Schulungskonzept sein. Es muss ein intelligentes, adaptives System werden, das aus Vorfällen lernt, auf Bedrohungen reagiert, Inno-

vationen integriert und Feedback auswertet – in kurzen Zyklen, mit klarem Fokus auf Wirkung. CISOs sollten es deshalb wie ein agiles Produkt führen: mit Backlog, KPIs, User Research und Release-Zyklen.

Nur so entsteht ein Programm, das nicht nur Wissen vermittelt, sondern Verhalten verändert – dauerhaft, resilient und im Takt mit der Bedrohungslage.

Regulatorische und normative Anforderungen

Ein modernes Awareness-Programm ist nicht nur ein freiwilliger Kulturbeitrag – es ist in vielen Fällen eine verbindliche Anforderung innerhalb von Informationssicherheitsstandards, Datenschutzvorgaben und branchenspezifischen Regulierungen. Die Fähigkeit, Mitarbeiter*innen angemessen und kontinuierlich für Sicherheitsrisiken zu sensibilisieren, ist heute ein formaler Bestandteil regulatorischer Compliance und gleichzeitig ein prüfbarer Kontrollpunkt in Audits und Zertifizierungen.

CISOs müssen daher Awareness nicht nur als Sicherheitsmaßnahme verstehen, sondern auch als Compliance-Baustein mit konkreten Nachweispflichten.

1. ISO/IEC 27001: Awareness als integraler Bestandteil des ISMS

Die internationale Norm ISO/IEC 27001 (in der aktuellen Fassung von 2022) definiert Awareness als einen zentrale Steuerungsbereich (Control Domain) innerhalb des Informationssicherheits-Managementsystems (ISMS).

Relevante Controls:

- A.6.3 – Informationssicherheit in den Rollen und Verantwortlichkeiten
  - Beschäftigte müssen über ihre Sicherheitsverantwortung informiert sein.
  - Awareness-Maßnahmen müssen zielgruppenspezifisch, dokumentiert und nachweisbar sein.
- A.7.2 – Schulung und Awareness
  - Organisationen müssen Prozesse etablieren, um sicherzustellen, dass alle Personen, die unter ihrer Kontrolle arbeiten, auf einem ihrem Informationssicherheitsrisiko angemessenen Niveau geschult und sensibilisiert werden.

Audit-Relevanz:

- Nachweis von durchgeführten Schulungen (Zeitpunkt, Teilnehmer, Inhalte)
- Kontinuierliche Verbesserung (z. B. Lessons Learned, KPI-Entwicklung)
- Risikobasierte Differenzierung der Awareness-Maßnahmen (z. B. für privilegierte Rollen)

2. NIST SP 800-50: Building an Information Technology Security Awareness and Training Program

Der Standard NIST SP 800-50 (US-amerikanischer Kontext) bietet eine strukturierte Methodik für den Aufbau eines Awareness- und Schulungsprogramms. Er unterscheidet klar zwischen:

- Awareness (bewusstseinsbildend, reaktiv, breit gestreut)
- Training (kompetenzaufbauend, rollenbasiert, interaktiv)

Kernelemente laut NIST:

- Zielgruppenanalyse und risikobasierte Priorisierung
- Messbarkeit von Verhalten und Wirkung
- Integration in Sicherheitsstrategie und Management Reviews

Relevanz für global agierende Unternehmen:

Obwohl NIST nicht europäisch reguliert ist, bieten viele seiner Konzepte eine praktische Operationalisierungshilfe für ISO-Umfelder.

3. DSGVO (Privacy by Awareness): Datenschutzschulungen als Verpflichtung

Die Datenschutz-Grundverordnung (DSGVO) schreibt in Artikel 39 explizit vor, dass Datenschutzbeauftragte Sensibilisierungsmaßnahmen und Schulungen für Mitarbeitende durchführen (lassen) müssen.

Konkret bedeutet das:

- Schulung zu Grundprinzipien (Art. 5 DSGVO), Rechte Betroffener, Datenpannenmanagement
- Awareness über den Zweckbindungsgrundsatz, Datenminimierung und Vertraulichkeit
- Zielgruppenangepasste Schulung für Fachbereiche (z. B. HR, Marketing, Sales)

In der Praxis spricht man von »Privacy by Awareness« – dem kulturellen Gegenstück zu »Privacy by Design«. Auch hier ist Dokumentation und Nachweiserbringung bei Aufsichtsbehörden essenziell.

4. NIS-2-Richtlinie (Directive (EU) 2022/2555)

Mit Inkrafttreten der NIS-2 ist Awareness in vielen Unternehmen EU-weit verpflichtend reguliert – insbesondere für sog. wesentliche und wichtige Einrichtungen. Die Anforderungen betreffen sowohl operative Mitarbeitende als auch die oberste Führungsebene.

- Management-Verantwortung (Art. 20)

- Mitglieder der Geschäftsleitung (z. B. CEO, CIO, CISO) müssen regelmäßig geschult werden, um Cyberrisiken zu erkennen, Risikomanagement zu bewerten und wirksam zu handeln. Auch alle weiteren Mitarbeitenden müssen entsprechend sensibilisiert werden.

- Awareness-Themen nach Rollen (Art. 21 § 2)
  - Alle Mitarbeitenden: Grundlagen der NIS-2-Richtlinie, Cyber-Hygiene, Vorfallmanagement, Datensicherung, Business Continuity, Nutzung von MFA
  - IT-/Security-Teams: Sicherheitsrichtlinien, Desaster Recovery, sichere Softwareentwicklung, Verschlüsselung, Zugangskontrollen, Asset Management, gesicherte Kommunikation, Notfallkommunikation
  - Security-Verantwortliche: NIS-2-Konformität, Bezüge zu ISO 27001 / DORA / GDPR, Schulungskonzepte, Risikoanalyse, Lieferantenbewertung, Berichtspflichten, Haftungsfragen

NIS-2 fordert regelmäßige Awareness-Maßnahmen für alle Mitarbeitenden – inkl. Führungskräfte. Awareness wird damit zur gesetzlichen Pflicht, nicht zur freiwilligen Maßnahme.

Die Unternehmensleitung ist persönlich haftbar für die Einhaltung der NIS-2-Vorgaben. Bei Missachtung drohen Sanktionen, Management-Ausschlüsse und Reputationsrisiken.

5. Branchenspezifische Anforderungen

Viele regulierte Sektoren gehen über generische Sicherheitsstandards hinaus und definieren spezifische Anforderungen an Awareness-Programme:

- KRITIS (Deutschland):
  - Betreiber Kritischer Infrastrukturen müssen gemäß BSI-KritisV regelmäßig Awareness- und Schulungsmaßnahmen nachweisen – insbesondere bei IT-Personal, aber auch beim allgemeinen Personal im operativen Bereich.

- BaFin-Rundschreiben (z. B. BAIT / VAIT / KAIT):
  - Versicherungen, Banken und Kapitalverwaltungsgesellschaften müssen Sicherheitskultur und Awareness-Programme nicht nur implementieren, sondern auch regelmäßig evaluieren. Spezifisch gefordert: Awareness für Top-Management, Datenschutz, Outsourcing-Risiken und Incident-Handling.

- HIPAA (USA, Healthcare):
  - Die HIPAA Security Rule fordert regelmäßige Schulungen zum Schutz elektronischer Gesundheitsdaten. Dies umfasst sowohl technische wie auch administrative Sicherheitsmaßnahmen – Awareness ist ein formaler Auditpunkt.

- DORA (EU):
  - Die Digital Operational Resilience Act der EU verlangt für Finanzorganisationen explizit Schulungen zur Erkennung, Meldung und Abwehr digitaler Bedrohungen – mit Nachweispflicht gegenüber Aufsichtsbehörden.

6. Auditfähigkeit und Nachweisführung

In regulierten Unternehmen ist Awareness nicht nur durchführungs-, sondern prüfpflichtig. Das heißt: Die Wirksamkeit muss in Audits belegt und nachvollziehbar dokumentiert werden – mit robusten, strukturierten Nachweissystemen.

Wichtige Elemente für Auditfähigkeit:

- Teilnehmernachweise: Wer hat wann was absolviert?
- Rollenspezifische Zuordnung: Wer benötigt welches Awareness-Level?
- Versionskontrolle: Welche Inhalte wurden wann geschult?
- Wirksamkeitsnachweise: KPIs, Clickrates, Meldequoten, Culture Surveys
- Integration ins ISMS/GRC: Zentrale Nachvollziehbarkeit über das Kontrollsystem

CISOs müssen Awareness nicht nur als Sicherheits-, sondern auch als Compliance-Verpflichtung verstehen – auditierbar, dokumentiert, steuerbar. Wer diese Perspektive frühzeitig in die Programmplanung integriert, schützt nicht nur das Unternehmen, sondern erfüllt regulatorische Anforderungen effizient und resilient.

Fazit

Security Awareness darf nicht länger als jährlicher Pflichttermin im Schulungskalender verstanden werden. Wer Awareness auf eine periodische E-Learning-Maßnahme reduziert, verfehlt die strukturelle Bedeutung von menschlichem Verhalten im Sicherheitskontext. Der Mensch ist heute nicht nur Ziel, sondern oft auch Vektor moderner Angriffsformen – etwa bei Phishing, Business Email Compromise, Social Engineering oder Credential Theft.

CISOs und Sicherheitsverantwortliche müssen Awareness daher als dynamisches, lernfähiges System gestalten – integriert in Risikomanagement, gesteuert über Governance, entwickelt entlang von Verhalten und Kultur. Nur durch kontinuierliche Entwicklung, differenzierte Zielgruppenansprache und messbare Wirkung wird aus Awareness ein strategischer Wirkfaktor für organisatorische Resilienz.

Awareness ist kein Kommunikationsthema, sondern ein strategischer Risikopunkt auf Board-Ebene. Entsprechend sollte das Thema in Sicherheits- und Risikoberichten mit einer eigenständigen Position behandelt werden, insbesondere bei folgenden Schwerpunkten:

1. Risikoperspektive

- Welches Risiko geht vom »Human Layer« realistisch aus?
- Wie effektiv sind aktuelle Awareness-Maßnahmen dagegen abgesichert?

2. Governance-Perspektive

- Gibt es eine dokumentierte Awareness-Strategie?
- Ist die Rolle des Programms im ISMS/GRC verankert?
- Existiert ein Steering Committee mit Interdisziplinärbesetzung?

3. Wirksamkeit & KPIs

- Welche Awareness-Kennzahlen werden erhoben und berichtet?
- Wie ist der Reifegrad verteilt über Zielgruppen, Regionen, Rollen?

4. Compliance-Fitness

- Erfüllt das Programm die Anforderungen aus ISO 27001, DSGVO, NIS-2, DORA, etc.?
- Ist es prüfbar, dokumentiert, differenziert?

Das Audit Committee sollte Awareness in seine jährliche Prüfagenda aufnehmen, inklusive Nachweispflichten, Management-Einbindung und Kulturentwicklung – analog zu anderen Risikodomänen wie Business Continuity oder Third Party Risk.

Ein bewährtes Steuerungsinstrument zur Entwicklung von Awareness ist die Reifegradmodellierung. Sie erlaubt es, systematisch vom Pflichtprogramm zum verhaltenswirksamen Sicherheitsmotor zu wachsen:

Reifegrad	Merkmale
Basic	Einmalige Schulung p. a., wenig zielgruppenspezifisch, geringe Wirkungsmessung
Defined	Strukturierte Lernpfade, Phishing-Simulationen, Zielgruppendifferenzierung, initiale KPIs
Managed	Awareness-Strategie, Budget, Ownership, interne Kampagnen, Feedback-Schleifen
Measured	KPI-Dashboard, Culture Surveys, Integration in ISMS, kontinuierliche Verbesserung
Embedded	Awareness als Teil der Sicherheitskultur, Leadership-Engagement, lernfähige Governance

Tipps

- Führen Sie ein Awareness Maturity Assessment durch (z. B. auf Basis von NIST NICE Framework oder ISO 27004).
- Verknüpfen Sie das Reifegradmodell mit Budgetplanung, Zieldefinition und Personalallokation.
- Integrieren Sie Awareness-Scorecards in Ihre Risikoberichte und Business Impact Assessments.

Security Awareness ist kein Produkt. Es ist kein Training. Es ist ein kontinuierlicher Kulturprozess, der Verhalten, Systeme und Führung verbindet. Es ist das Bindeglied zwischen Strategie und Realität – und damit das Rückgrat einer resilienten Organisation.

Awareness muss aufhören, der »letzte Punkt in der Sicherheitsstrategie« zu sein. Es ist an der Zeit, es zum ersten kulturellen Hebel moderner Security Governance zu machen – durch Leadership, Systematik und messbare Wirkung.

Referenzen

- Advisera. (2025). *ISO 27001 Control 6.3 – Information Security Awareness, Education and Training*. Abgerufen am 21. August 2025, von https://advisera.com/iso27001/control-6-3-information-security-awareness-education-and-training/
- ANSI. (2022). *ISO/IEC 27001:2013 & ISO/IEC 27001:2022 Vergleich*. Abgerufen am 21. August 2025, von https://blog.ansi.org/anab/iso-iec-27001-2013-2022-comparison/
- DataGuard. (2025). *ISO 27001 Controls: Übersicht über Annex A (inkl. 6.3)*. Abgerufen am 21. August 2025, von https://www.dataguard.com/knowledge/iso-27001-controls-annex-a/
- Decision Lab. (o. J.). *Fogg Behavior Model – Reference Guide*. Abgerufen am 21. August 2025, von https://thedecisionlab.com/reference-guide/psychology/fogg-behavior-model
- Fogg, B. J. (2009). A behavior model for persuasive design. *Proceedings of the 4th International Conference on Persuasive Technology*, 1–7. Abgerufen am 21. August 2025, von https://www.habitweekly.com/models-frameworks/the-fogg-model
- Hightable. (2025). *Implementierung von ISO 27001 Annex A 6.3 – Leitfaden & Audit-Hinweise*. Abgerufen am 21. August 2025, von https://hightable.io/iso-27001-annex-a-6-3-information-security-awareness-education-and-training/

- ISMS.online. (2025). *ISO 27001:2022 Annex A 6.3 – Information Security Awareness, Education and Training*. Abgerufen am 21. August 2025, von https://www.isms.online/iso-27001/annex-a/6-3-information-security-awareness-education-training-2022/
- Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2021). *Evaluation of security training and awareness programs: Review of current practices and guideline*. arXiv [Preprint]. Abgerufen am 21. August 2025, von https://arxiv.org/abs/2112.06356
- Microsoft Tech Community. (2024). *NIST CSF 2.0 – Protect (PR) Kategorien inkl. Awareness & Training (PR.AT)*. Abgerufen am 21. August 2025, von https://techcommunity.microsoft.com/blog/microsoft-security-blog/nist-csf-2-0---protect-pr---applications-for-microsoft-365-part-1/4163650
- National Institute of Standards and Technology (NIST). (2023). *NIST Cybersecurity Framework (CSF) 2.0 Reference Tool*. Abgerufen am 21. August 2025, von https://www.nist.gov/document/11032023-sara-r-update-draft-csf20
- National Institute of Standards and Technology (NIST). (2024). *NIST Cybersecurity Framework (CSF) 2.0*. Abgerufen am 21. August 2025, von https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- Navvia. (2025). *The fundamentals of NIST CSF 2.0: What it is and why it's important*. Abgerufen am 21. August 2025, von https://navvia.com/blog/the-fundamentals-of-nist-csf-what-it-is-and-why-its-important
- Stanford Behavior Design Lab. (o. J.). *Fogg Behavior Model – What causes behavior change?* Abgerufen am 21. August 2025, von https://behaviordesign.stanford.edu/resources/fogg-behavior-model