KnowBe4
Human error. Conquered.

# Aufbau eines konformen und widerstandsfähigen Security-Awareness-Programms

# Aufbau eines konformen und widerstandsfähigen Security-Awareness-Programms

## Inhaltsverzeichnis

# EINFÜHRUNG

Internationale Organisationen sind gezwungen, stets neue Cybersicherheitsverordnungen umzusetzen. Denn die in den letzten Jahren immer größer werdende Bedrohung durch länderübergreifende Cyberangriffe hat Regierungen weltweit zum Handeln gezwungen.

Die erlassenen Verordnungen dienen einem wichtigen Zweck: dem Schutz von Daten, Geld und Ruf vor der endlosen Flut von Cyberangriffen.

InfoSec-Beauftragte sind von der Geschwindigkeit des Wandels mitunter überfordert. CISOs (Chief Information Security Officers) und deren Teams müssen ständig neue Richtlinien und Vorgaben wie die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) oder die NIS2-Richtlinie berücksichtigen.

Neben technischen Maßnahmen und verschärften Richtlinien fordern aktuelle Cybersicherheitsbestimmungen immer häufiger Security-Awareness-Training-Programme.

Es ist selbstverständlich gut, dass Security Awareness und Sicherheitskultur stärker in den Fokus rücken, da der Faktor Mensch bei der Cybersicherheit eine wichtige Rolle spielt. Jedoch enthalten die Verordnungen und Vorgaben in der Regel wenig Konkretes dazu, wie sich die Sicherheitskultur einer Organisation durch Security Awareness Training nachhaltig verbessern lässt.

Wie also können Organisationen die eigenen Richtlinien auf die immer strikteren und weitreichenderen Verordnungen und Vorgaben abstimmen? Auch wir haben nicht auf alle Fragen eine Antwort parat. Jedoch wissen wir, wie InfoSec-Teams ein zukunftssicheres und konformes Security-Awareness-Programms entwickeln können.

In diesem Whitepaper finden Sie einen Überblick über das Thema Security Awareness in weltweiten Cybersicherheitsverordnungen und Best Practices für den Aufbau eines Security-Awareness-Training-Programms, damit Ihre Organisation die Anforderungen an Training und Security Awareness heute und in Zukunft erfüllen kann.

# WELTWEITE CYBERSICHERHEITSVERORDNUNGEN

Wir haben für Sie ein halbes Dutzend besonders weitreichender Verordnungen und Vorgaben mit Bezug zu Security Awareness zusammengestellt. In der Tabelle finden Sie Verweise auf die Stellen, an denen Security Awareness in der jeweiligen Richtlinie erwähnt wird und inwieweit sich daraus Anforderungen ergeben. Die Tabelle finden Sie hier.

Was sich nur schlecht tabellarisch darstellen lässt, sind die bei Verstößen fälligen Geldzahlungen. Bei einigen handelt es sich um unverbindliche Vorgaben. Verstöße werden daher nicht sanktioniert. (Jedoch bringt die Nichteinhaltung gängiger Best Practices eigene, weniger konkrete Nachteile mit sich.) Bei anderen müssen Organisationen bei Verstößen mit deftigen Geldzahlungen rechnen.

Bei einem Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) sind bis zu 20 Millionen EUR oder 4 % des gesamten weltweit erzielten Jahresumsatzes fällig, je nachdem, welcher Betrag größer ist. Meta, der Mutterkonzern von Facebook, wurde 2023 auf eine Rekordsumme von 1,2 Milliarden EUR verklagt – das ist mehr als alle Geldzahlungen im Jahr 2022 zusammengenommen.

Auch in den neueren EU-Richtlinien DORA und NIS2 sind Geldzahlungen für Verstöße festgelegt. Finanzunternehmen drohen bei einem Verstoß gegen die DORA-Vorgaben Geldzahlungen von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes. Die DORA-Verordnung erstreckt sich auch auf bestimmte Drittdienstleister für die Finanzbranche. Hier können Geldzahlungen in einer Höhe von bis zu 5 Millionen EUR verhängt werden. Bei einem Verstoß gegen die NIS2-Richtlinie sind sogar Geldzahlungen in einer Höhe von bis zu 10 % des gesamten weltweit erzielten Jahresumsatzes möglich.

**Wichtige Erkenntnis:** Gesetzgeber reagieren mit strikten Verordnungen auf die Gefährdung von Cybersicherheit und Datenschutz und lassen Organisationen bei Verstößen teils tief in die Taschen greifen.

# ENTWICKLUNG DER CYBERSICHERHEITSVERORDNUNGEN

Der Zweck derartiger Verordnungen besteht letztendlich darin, den Schutz vor immer raffinierteren Cyberbedrohungen zu verbessern. Die neueren Vorgaben und Anordnungen sind die Antwort der internationalen Gemeinschaft auf Bedrohungen, die nicht an nationalen Grenzen Halt machen.

Daher zieht die NIS2-Richtlinie im Gegensatz zur Vorgängerversion (NIS1) beispielsweise mehr Organisationen zur Verantwortung. Bisher waren nur die Energie- und Transportbranche betroffen. Jetzt werden auch Branchen mit kritischen Infrastrukturen und wichtigen Dienstleistungen einbezogen, einschließlich der digitalen Netzwerke, die die Weltwirtschaft am Laufen halten. Prominente Cyberangriffe auf kritische Infrastrukturen und Lieferketten weltweit haben zweifellos dazu beigetragen, dass weitere Branchen aufgenommen wurden.

*Die neueren Vorgaben und Anordnungen sind die Antwort der internationalen Gemeinschaft auf Bedrohungen, die nicht an nationalen Grenzen Halt machen.*

Ähnlich wie die NIS2 verlangt auch die DORA-Verordnung bessere Schutzmechanismen. Im Fokus stehen jedoch Finanzunternehmen. Gemäß Reports zu den Kosten von Datenschutzverletzung aus dem Jahr 2023 müssen Finanzunternehmen bei einer Datenschutzverletzung mit einem Verlust in Höhe von 5,9 Millionen USD rechnen; das sind 28 % mehr als der weltweite Durchschnitt. Angesichts dieser Summen und der großen Angriffsfläche ist es kein Wunder, warum Cyberkriminelle häufig Finanzunternehmen angreifen. Zielsetzung der DORA-Verordnung ist eine Reduzierung der Risiken in Zusammenhang mit Informations- und Kommunikationstechnologien (IKT). Ohne Banken und andere Finanzunternehmen steht die Welt still. Europäische Gesetzgeber möchten daher sicherstellen, dass diese Organisationen über eine möglichst hohe operationale Resilienz verfügen.

## Risikomanagement anstelle von Threat Management

Durch diese neuen und erweiterten Richtlinien wird deutlich, dass Risikomanagement innerhalb der Europäischen Union und in anderen Regionen der Welt immer stärker in den Fokus rückt.

Kritische Organisationen sollen vielmehr dabei unterstützt werden, sich heute und in Zukunft vor Cyberangriffen zu schützen. Durch die Aufnahme von Passagen über Security Awareness und entsprechende Trainingsprogramme wird anerkannt, wie wichtig der Aufbau einer soliden Sicherheitskultur ist, die auf einer informierten Belegschaft beruht.

Obwohl die Verordnungen durchaus ausführlich sind, steht dort nicht viel darüber, warum Security Awareness und Training wichtig sind und wie entsprechende Best Practices aussehen. Hier kann KnowBe4 weiterhelfen. Im Folgenden erfahren Sie, wie Sie einen Business Case für Security Awareness erstellen und ein Programm strukturieren, das Ihre Belegschaft mit dem notwendigen Wissen ausstattet, heute und in Zukunft die richtigen Entscheidungen in Bezug auf die Sicherheit zu treffen.

# ARGUMENTE FÜR EIN PROAKTIVES SICHERHEITSBEWUSSTSEIN

*Wenn Sie als CISO oder InfoSec-Führungskraft mit der Einhaltung der genannten Vorgaben betraut wurden, müssen Sie auch Security Awareness und Training berücksichtigen.*

KnowBe4 begrüßt, dass Security Awareness und Training in Richtlinien und Verordnungen zur Cybersicherheit Erwähnung finden. Das ist ein Anstoß für Organisationen, tätig zu werden, da sich Mitarbeitende andernfalls schnell dazu verleiten lassen, sensible Daten preiszugeben. Sämtliche Technologien und Präventivmaßnahmen einer Organisation sind machtlos gegenüber Social-Engineering-Angriffen. Wenn Sie als CISO oder InfoSec-Führungskraft mit der Einhaltung der genannten Vorgaben betraut wurden, müssen Sie auch Security Awareness und Training berücksichtigen.

Dies wird im Folgenden näher behandelt.

InfoSec-Führungskräfte wie Sie berichten häufig, dass ihnen gute Argumente für Security Awareness Training beim Pitch vor der Geschäftsleitung fehlen. Verweisen Sie am Anfang Ihrer Argumentation am besten darauf, dass Security Awareness Training in Richtlinien wie der DORA-Verordnung oder NIS2 bereits explizit erwähnt wird.

Durch die Nennung von Passagen in Verordnungen mit Bezug zu Security Awareness können Sie der Geschäftsleitung deutlich machen, dass neben den objektiveren, technologischen Anforderungen auch Security Awareness notwendig und genauso wichtig ist.

## Sicherheitskultur statt bloße Compliance

Im nächsten Schritt können Sie auf die Vorteile eingehen, die sich ergeben, wenn mehr als nur die Mindestanforderungen umgesetzt werden. Vielleicht reichen ein oder zwei Trainingskurse pro Jahr aus, um Auditorinnen und Auditoren zu befriedigen. Aber reicht diese Strategie auch aus, um Ihre Organisation über Jahre hinweg zu schützen?

Nein.

Es wäre besser, in Ihrer Organisation eine solide Sicherheitskultur aufzubauen. Damit sind die Konzepte, üblichen Verfahren und sozialen Verhaltensweisen einer Gruppe gemeint, die zur Sicherheit einer Organisation beitragen. Die Sicherheitskultur ist Teil einer breiter gefassten Unternehmenskultur. Für den Aufbau einer Sicherheitskultur müssen jedoch jeweils spezifische Aufgaben, Ziele und Verantwortlichkeiten festgelegt werden.

Indirekt können Cybersicherheitsverordnungen, die auch kurz auf Security Awareness eingehen, als Versuch angesehen werden, den Aufbau einer soliden Sicherheitskultur zu fordern, jedoch mit Argumenten, die die Geschäftsleitung versteht – Geldzahlungen und Risikomanagement. Versuchen Sie es mit einer ähnlichen Argumentation.

*Indirekt können Cybersicherheits-verordnungen, die auch kurz auf Security Awareness eingehen, als Versuch angesehen werden, den Aufbau einer soliden Sicherheitskultur zu fordern, jedoch mit Argumenten, die die Geschäftsleitung versteht – Geldzahlungen und Risikomanagement.*

Betonen Sie, welchen Mehrwert der Aufbau einer Sicherheitskultur für die Organisation hat. Es geht nicht nur um die Abwehr der Bedrohungen von heute, sondern auch um die Vorbereitung auf die Zukunft. Ein starkes Security-Awareness-Programm bringt eine widerstandsfähige, informierte Belegschaft hervor, die sich nicht einfach nur konform verhält, sondern unter Berücksichtigung der Cybersicherheit handelt.

Argumentieren Sie mit Risikomanagement und sinnvollen Investitionen. Riskante Verhaltensweisen von Mitarbeitenden müssen wie jede andere Bedrohung für die Organisation behandelt werden. Eine Investition, die riskanten Verhaltensweisen entgegenwirkt, ist nicht nur sinnvoll, sondern im Grunde unerlässlich. Es gibt einfach Bereiche, in denen Minimalansätze nicht ausreichen. Auch Risikomanagement kann durch Security Awareness Training erleichtert werden. Eine Investition in Security Awareness schützt Ihre Organisation und trägt dazu bei, dass Sie den Herausforderungen von morgen gewachsen sind.

Wenn Sie mit Ihrem Pitch erfolgreich waren, finden Sie im Folgenden nun einige Best Practices für ein Security-Awareness-Programm, das die Sicherheitskultur in Ihrer Organisation positiv verändert.

# AUFBAU EINES UMFASSENDEN SECURITY-AWARENESS-PROGRAMMS

Ein Security-Awareness-Programm muss selbstverständlich organisationsspezifisch abgestimmt werden. Eine Einheitslösung gibt es nicht.

Daher ist es von Vorteil, dass in Verordnungen und Vorgaben keine detaillierten Anforderungen an das Security Awareness Training festgelegt sind. Ein robustes und ansprechendes Security-Awareness-Programm, das auf den Aufbau einer soliden Sicherheitskultur ausgerichtet ist, erfüllt daher mit hoher Wahrscheinlichkeit sämtliche Bestimmungen. Es kann auch sein, dass Sie neben einem allgemeinen Programm zur Cybersicherheit auch branchenspezifische Trainingsinhalte anbieten müssen (z. B. Sicherheitstraining zum PCI DSS-Standard).

Ein umfassendes Security-Awareness-Programm stützt sich dabei auf drei Säulen:

- Anforderungen der Organisation
- Content/Kommunikation
- Messung der Wirksamkeit

Diese Säulen werden im Folgenden eingehend behandelt.

## Anforderungen der Organisation

Zunächst muss ermittelt werden, welche Risiken und Anforderungen für Ihre Organisation relevant sind. Das angebotene Training und die Verhaltensweisen Ihrer Mitarbeitenden, die Sie ändern möchten, sollten auf die wichtigsten Risiken Ihrer Organisation abgestimmt sein.

Risiken werden häufig nach folgender Formel berechnet: Risiko = Wahrscheinlichkeit × Auswirkung. Bei den Risiken und Verhaltensweisen, auf die Sie eingehen müssen, handelt es sich also mitunter nicht um die häufigsten, sondern um diejenigen mit den größten Auswirkungen.

*Bei den Risiken und Verhaltensweisen, auf die Sie eingehen müssen, handelt es sich mitunter nicht um die häufigsten, sondern um diejenigen mit den größten Auswirkungen.*

Einige allgemeine Themen gehören in jedes Security-Awareness-Programm. Sie müssen jedoch auch branchenspezifisches Training anbieten. Hierzu lohnt sich ein Blick in die Verordnungen, in denen Security Awareness erwähnt wird.

Sie sollten auch die größten Risiken für Ihre Organisationen berücksichtigen. Die Auswahl der Risiken und Verhaltensweisen ist abhängig vom Bedrohungsmodell und von der Risikobereitschaft Ihrer Organisation. In Berichten wie dem Verizon Data Breach Investigations Report (DBIR) finden Sie ebenfalls Informationen über aktuelle Bedrohungen, die für Ihre Organisation oder Ihre Branche zu beachten sind. Umfragen zum Thema Cybersicherheit unter Mitarbeitenden und Gespräche mit dem IT-Team helfen Ihnen dabei, den Kenntnisstand und den Bedarf an Training zu ermitteln.

Sie sollten sich nicht mit den Mindestanforderungen zufriedengeben. Sie haben sich zum Ziel gesetzt, die Sicherheitskultur zu verbessern. Sie möchten Verhalten ändern. Das ist nur durch kontinuierliches Training möglich.

## Content/Kommunikation

Inhalte müssen ansprechend sein und wiederholt werden, damit sich das Verhalten ändert. Ein einmaliges Training reicht dafür nicht aus. Behandeln Sie ein Security-Awareness-Programm so wie eine laufende Marketing-/PR-Kampagne.

Ein Training, das einmal im Jahr abgehalten wird und bei dem lediglich Multiple-Choice-Aufgaben gestellt werden, wird das Verhalten Ihrer Mitarbeitenden nicht ändern. Viel besser ist es, die Inhalte immer wieder neu zu präsentieren (normales Training, Poster und Grafiken, „Lunch & Learn"-Events). Nur dann werden die Inhalte verinnerlicht und Ihre Mitarbeitenden treffen irgendwann ganz natürlich smartere Entscheidungen.

*Es ist wichtig, Gründe zu nennen, warum eine Änderung des Verhaltens wünschenswert ist und der Sicherheit der Organisation dient.*

Wir empfehlen in der Regel, jeden Monat mindestens 10 bis 15 Minuten für Security Awareness Training einzuplanen. Zudem sollten Sie Ihre Mitarbeitenden bei einem simulierten Phishing-Test einmal im Monat auf die Probe stellen. Behandeln Sie alle erforderlichen Themen, auch wenn das bedeutet, dass die 15-Minuten-Marke ein oder zwei Monate lang überschritten wird. Bitten Sie sicherheitsbewusste Mitarbeitende, als „Security Champions" aufzutreten und sich persönlich für sicherheitsbewusstes Verhalten in Ihrer Organisation starkzumachen.

Es ist wichtig, Gründe zu nennen, warum eine Änderung des Verhaltens wünschenswert ist und der Sicherheit der Organisation dient. Diese „intrinsische Motivation" ist wichtig, da Mitarbeitende zusätzliche Schritte in ihren Arbeitsalltag integrieren müssen.

Nehmen Sie als einfaches Beispiel, den Computer bei Nichtgebrauch zu sperren. Es ist zwar äußerst trivial, den Computer zu sperren. Dieser muss nach der Rückkehr aber wieder entsperrt werden. Und das bedeutet, dass die Mitarbeitenden mehrmals am Tag ihr Passwort eingeben müssen. Wenn Sie nicht verständlich machen können, warum es wichtig ist, den Computer zu sperren, wird diese Richtlinie möglicherweise nicht befolgt.

Wenn Sie Verhaltensweisen ändern und die Sicherheitskultur verbessern möchten, müssen Sie richtig kommunizieren. Informieren Sie die Mitarbeitenden über bevorstehendes Training und bitten Sie am besten Vorgesetzte, diesbezügliche E-Mails zu senden.

## Messung der Wirksamkeit

Natürlich müssen Sie die Wirksamkeit Ihres Trainings auch mit Daten belegen können. Dazu stehen Ihnen bei KnowBe4 die Ergebnisse der simulierten Phishing-Tests, Tools zur Messung des Risk Scores von Nutzerinnen und Nutzern sowie Assessments zur Abfrage von Lerninhalten zur Verfügung. Abhängig von den Ergebnissen können Sie Schwerpunkte anders setzen oder bei Bedarf weitere Themen einbinden.

*Security Awareness ist ein kontinuierlicher Trainings- und Anpassungsprozess, der letztendlich zu Verhaltensänderungen führt.*

Die Ergebnisse können auch als Nachweis für Auditorinnen und Auditoren in einem Report dokumentiert werden. Diese Reports sind natürlich auch für die Geschäftsleitung interessant, die Sie ab und zu über den Stand der Dinge informieren müssen.

Die Reports müssen nicht ins Detail gehen, sondern sollen eher Bereiche aufdecken, in denen Verbesserungsbedarf besteht, und die Geschäftsleitung von einer fortgesetzten Investition in Security Awareness Training überzeugen. Bestens geeignet sind Vorher-/Nachher-Vergleiche, die die Wirkung des Trainings belegen.

Wenn Sie neue Themen einbinden, vergessen Sie dabei nicht die zurückliegenden Trainingsinhalte. Für eine nachhaltige Änderung des Verhaltens ist es wichtig, bereits behandelte Themen zu wiederholen. Security Awareness ist ein kontinuierlicher Trainings- und Anpassungsprozess, der letztendlich zu Verhaltensänderungen führt.

# FAZIT

Internationale Cybersicherheitsvorschriften sind notwendig, da sie Angriffe von Akteurinnen und Akteuren mit böswilligen Absichten verhindern sollen. Durch die Erwähnung von Security Awareness in Richtlinien wie der DORA-Verordnung (hier wird auf Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen verwiesen) wird deutlich, dass der Faktor Mensch unbedingt berücksichtigt werden muss.

Es geht in diesen Richtlinien nicht darum, einen Sturm abzuwettern, sondern sich für die Zukunft zu rüsten. Es dauert eine Zeit, bis sichergestellt ist, dass Ihre Mitarbeitenden nicht nur auf dem neuesten Stand in Sachen Cyberbedrohungen sind, sondern sich auch den Herausforderungen von morgen stellen können. Sie tragen wesentlich dazu bei, dass ein Ruck durch Ihre Organisation geht und Verordnungen eingehalten werden.

Resilienz erreichen Sie nicht nur mit robusten Technologien. Durch den Aufbau einer proaktiven und soliden Sicherheitskultur können Sie sich darüber hinaus auf eine informierte und wachsame Belegschaft stützen. Setzen Sie sich für kontinuierliches Lernen ein und bauen Sie eine Sicherheitskultur auf, die Ihr Unternehmen vor dem größten Cyberrisiko schützt: menschlichem Versagen.

## Weitere Ressourcen

**Kostenloser Phishing Security Test**
Wie anfällig sind Ihre Mitarbeitenden für Phishing? Unser kostenloser Phishing Security Test verrät es Ihnen.

**Kostenloses Automated Security Awareness Program**
Erstellen Sie ein auf Ihr Unternehmen, Ihre Institution oder Ihre Organisation abgestimmtes Security Awareness Program.

**Phish Alert Button (kostenlos)**
Mit diesem Tool können Mitarbeitende ab sofort Phishing-Angriffe mit nur einem Klick sicher melden.

**Email Exposure Check (kostenlos)**
Welche Ihrer E-Mail-Anmeldedaten wurden bereits offengelegt? Werden Sie aktiv, bevor es die Kriminellen tun.

**Domain Spoof Test (kostenlos)**
Finden Sie heraus, ob Hacker E-Mail-Adressen Ihrer Domain spoofen können.


## Über KnowBe4

KnowBe4 versetzt Ihre Belegschaft in die Lage, jeden Tag intelligentere Sicherheitsentscheidungen zu treffen. Zehntausende Organisationen weltweit setzen auf die KnowBe4-Plattform, um ihre Sicherheitskultur zu verbessern und menschliche Risiken zu reduzieren. KnowBe4 baut eine menschliche Verteidigungslinie auf, mit der Organisationen das Verhalten der Nutzerinnen und Nutzer durch neuartiges Security-Awareness- und Compliance-Training stärken können.

Mit KnowBe4 sind die Nutzerinnen und Nutzer wachsam und sorgen sich um den Schaden, den Phishing, Ransomware und andere Social-Engineering-Bedrohungen nach sich ziehen. Die Plattform bietet eine umfassende Suite für Awareness- und Compliance-Training, Echtzeit-Coaching für Nutzerinnen und Nutzer, KI-gestütztes simuliertes Social Engineering sowie Phishing-Abwehr via Crowdsourcing.

Mit Inhalten in mehr als 35 Sprachen bietet KnowBe4 die weltweit größte, stets aktuelle Bibliothek mit motivierenden Inhalten für eine starke Human Firewall.

**Weitere Informationen finden Sie auf www.KnowBe4.de**

KnowBe4
Human error. Conquered.

KnowBe4 Germany | Rheinstr. 45/46 | 12161 Berlin – Deutschland |
Tel: +49 30 34 64 64 60 | knowbe4.de | E-Mail: kontakt@knowbe4.com



04E01K01