KnowBe4 Research

REPORT ZUR SICHERHEITS-KULTUR FÜR **EUROPA** 2024

Der Report zur Sicherheitskultur 2024 von KnowBe4 beschäftigt sich mit der Wirksamkeit von Sicherheitsmaßnahmen in Organisationen und wie sich die Mitarbeitenden während der Arbeit verhalten und fühlen. Diese tiefgreifende und umfassende Analyse der Sicherheitskultur präsentiert Ergebnisse von tausenden Organisationen weltweit, darunter auch einen aussagekräftigen Vergleich der vergangenen fünf Jahre.

Im Report werden sechs Weltregionen – Nordamerika, Südamerika, Europa, Afrika, Asien und Ozeanien – ausführlich untersucht und es wird der jeweilige Stand der Sicherheitskultur bewertet.

Dieser Leitfaden bietet einen Überblick über die wichtigsten Erkenntnisse für Europa.

Dimensionen der Sicherheitskultur

Die Sicherheitskultur wird anhand von sieben spezifischen Dimensionen systematisch beurteilt:

Einstellungen

Die Gefühle und Überzeugungen der Mitarbeitenden in Bezug auf Sicherheitsprotokolle und -probleme.

Verhaltens-weisen

Die Handlungen und Aktivitäten der Mitarbeitenden, die sich unmittelbar auf die Sicherheit der Organisation auswirken.

Wissen

Das Verständnis der Mitarbeitenden von Angelegenheiten und Aktivitäten in Zusammenhang mit der Sicherheit sowie die entsprechende Kenntnis und das entsprechende Bewusstsein.

Kommunikation

Die Qualität der Kommunikationskanäle für sicherheitsrelevante Themen, die Vermittlung eines Gefühls der Zugehörigkeit und Unterstützung bei Angelegenheiten in Zusammenhang mit der Sicherheit und dem Melden von Vorfällen.

Compliance

Die Kenntnis der schriftlich festgelegten Sicherheitsrichtlinien und das Ausmaß, in dem die Mitarbeitenden diese Richtlinien einhalten.

Normen

Die Kenntnis und Einhaltung von ungeschriebenen Verhaltensregeln in der Organisation.

Verantwort-lichkeiten

Die Wahrnehmung der Mitarbeitenden ihrer Rolle als wichtigem Faktor in Bezug auf die Aufrechterhaltung oder Gefährdung der Sicherheit der Organisation.

Sicherheitskultur Index

Der Sicherheitskultur-Index (Security Culture Index, SCI) ist ein globaler Index zur Bewertung von Organisationen anhand ihres Sicherheitskultur-Scores. Dieser Index wurde vom KnowBe4 Research Team entwickelt. Zur Berechnung wird die Sicherheitskultur von tausenden Organisationen weltweit analysiert.

90 bis 100	**Sehr gut**
80 bis 89	**Gut**
70 bis 79	**Mittelmäßig**
60 bis 69	**Mangelhaft**
0 bis 59	**Schlecht**

Anmerkung: Keine Branche hat in diesem Jahr einen SCI von „Sehr gut“ oder „Gut“ erzielt.

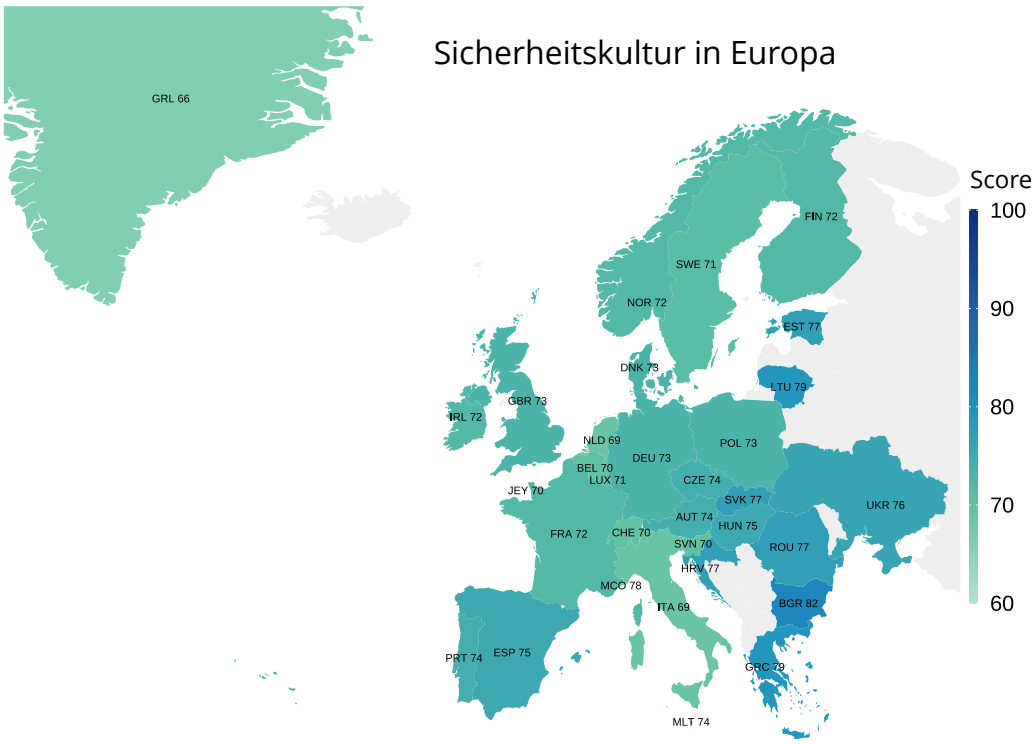
Europa

Von Dr. Martin J. Krämer, Security Awareness Advocate

Anpassung der Unternehmenskultur

Sicherheitskultur wird in Europa und den verschiedenen Branchen unterschiedlich wahrgenommen und verstanden. Sicherheitsfachleute, insbesondere in Branchen mit einem hohen Digitalisierungsgrad wie dem Finanz-, Banken- oder IT-Sektor, greifen das Konzept immer häufiger auf. In anderen Branchen wird der Sicherheitskultur oft erst dann Beachtung geschenkt, wenn die erste Phase einer Cybersicherheitsstrategie mit dem Schwerpunkt Security Awareness abgeschlossen ist.

Während einige Organisationen ein gutes Verständnis der Sicherheitskultur als Prozess und strategischer Maßnahme haben, stehen andere noch ganz am Anfang. Organisationen, die bereits eine Taktik entwickelt und die ersten Schritte unternommen haben, wissen, dass die Formulierung von sicheren Verhaltensweisen für die Entwicklung einer Sicherheitskultur wesentlich ist. Diese Organisationen wissen auch, dass in einer proaktiven Sicherheitskultur die Mitarbeitenden selbst ein Verständnis dafür entwickeln, dass sicheres Verhalten über das Erkennen und Melden von Phishing-Simulationen hinausgeht. Diese Mitarbeitenden sind von sich aus motiviert, die Sicherheitslage ihrer Organisation zu verbessern.



Die Sicherheitskultur in Organisationen innerhalb Europas ist ganz unterschiedlich ausgereift. In einigen Bereichen wird der Faktor Mensch in der Cybersicherheit kaum oder gar nicht berücksichtigt, sodass sich die Strategie zunächst auf die Ausbildung von Security Awareness konzentriert. Es wird völlig außer Acht gelassen, dass die Mitarbeitenden nach wie vor der größte Angriffsvektor in einer Organisation sind – auch zielgerichtete Angriffe auf einzelne Personen werden kaum thematisiert.

Europa umfasst 44 Länder, in denen 746 Millionen Menschen leben. In Europa werden 287 Sprachen gesprochen, von denen 24 als Amtssprachen der Europäischen Union anerkannt sind.

Allgemeine Einstellungen

Die meisten Organisationen in Europa wissen, dass die Mitarbeitenden in die Verteidigungsstrategie einbezogen werden müssen, um die Widerstandsfähigkeit der Organisation zu erhöhen. Security Awareness Training wird nicht mehr als schnöde Multiple-Choice-Übung verstanden, nur damit Compliance-Anforderungen erfüllt werden. Es findet ein Umdenken statt – hin zu einer strategischen Initiative, um Sicherheitsdenken in der Organisation zu fördern.

Oft wird Sicherheit immer noch als Aufgabe eines einzigen Teams oder einer einzigen Abteilung betrachtet. In Organisationen, in denen ein Bewusstsein für Cybersicherheit fehlt und Abteilungen in Sachen Cybersicherheit nicht kooperieren, können sich Sicherheitsfachleute nur schwer durchsetzen. Es ist vielmehr so, dass viele Organisationen gar keine BISOs (Business Information Security Officers) beschäftigen. BISOs übernehmen eine strategisch wichtige Aufgabe, wenn es darum geht, die Sicherheit einer Organisation dauerhaft zu gewährleisten, da sie Sicherheits- und Geschäftsanforderungen gleichermaßen im Blick haben.

Wichtige behördliche Vorschriften (d. h. Gesetzgebung)

In der Region erlässt vor allem die EU Gesetze und Verordnungen, auch bezüglich der Cybersicherheit. Im Fokus der Gesetzgebung liegt die Wahrung grundlegender Menschenrechte in Zeiten eines rasanten technologischen Fortschritts. Die EU hat sich – wie andere Regionen auch – zum Ziel gesetzt, Unternehmen durch öffentlich-private Bemühungen und immer strengere Cybersicherheitsverordnungen vor Bedrohungen zu schützen. Diese Bemühungen sorgen für mehr Cybersicherheit und Datenschutz in Europa.

Die Einführung der Datenschutz-Grundverordnung (DSGVO) hatte weltweite Auswirkungen. Die DSGVO gilt in der gesamten Europäischen Union und diente als Vorlage für ähnliche Verordnungen in anderen Teilen der Welt. Sie sorgt für ein Gleichgewicht bei der Datenerhebung und -verarbeitung und stellt die Interessen der betroffenen Personen in den Vordergrund. Strenge Cybersicherheitsanforderungen werden auch durch Branchenverordnungen wie die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) durchgesetzt. Bis Oktober 2024 müssen Organisationen mit kritischen Infrastrukturen die NIS2-Richtlinie umgesetzt haben. Diese zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit macht den Vorstand für die Cybersicherheit in der eigenen Organisation verantwortlich. Gemäß der Richtlinie tragen Organisationen auch die Verantwortung für die Sicherheit ihrer Lieferketten.

Die DORA (EU-Verordnung über die digitale operationale Resilienz im Finanzsektor) tritt im Januar 2025 in Kraft und verpflichtet Finanzinstitutionen zur Stärkung ihrer digitalen operationalen Resilienz. Organisationen müssen nachweisen, wie schnell sie sich von einem Cyberangriff erholen können, und Mitarbeitende schulen.

Die EU reguliert den Einsatz von KI auf ähnlich umfassende Weise. Sie hat sich im Dezember 2023 auf die Grundzüge eines Gesetzes geeinigt (Gesetz über künstliche Intelligenz, engl. EU AI Act). Dieses tritt jedoch nicht vor 2025 in Kraft. Das Gesetz über künstliche Intelligenz sieht einen risikobasierten Ansatz vor. Künstliche Intelligenz wird in verschiedene Risikokategorien eingestuft (inakzeptables Risiko, hohes Risiko, begrenztes Risiko und kein/niedriges Risiko). Organisationen, die gegen das Gesetz verstoßen, drohen Strafen von bis zu 35 Millionen Euro oder 3 % des Bruttoumsatzes (je nachdem, welcher Betrag höher ist).

Organisationen sind vielleicht schnell in der Lage, neue Anforderungen in internen Richtlinien zu berücksichtigen. Nach der Dokumentation, Genehmigung und Verbreitung stellt sich jedoch eine viel größere Herausforderung: die Steuerung. Es ist wichtig, dass Organisationen und deren Führungskräfte eine einheitliche Strategie und Zielsetzung im Bereich Cybersicherheit verfolgen. Standardisierte Verfahren, eine solide Durchsetzung, klare Verantwortlichkeiten und Kontrolle durch die Führungsebene sowie geeignete Ressourcen sind erforderlich. Für eine nachhaltige Stärkung der Cybersicherheit benötigen Organisationen eine umfassende Steuerung. Andernfalls verkommt Compliance zu einer schnöden Multiple-Choice-Übung.

Sicherheitsereignisse/ drängende Probleme

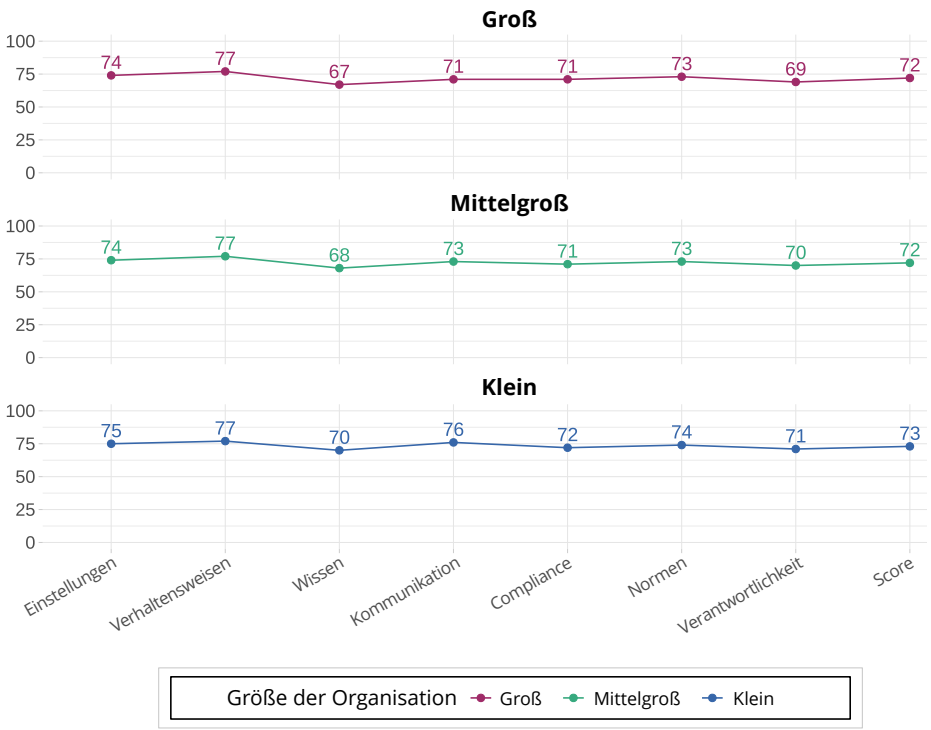
Die Agentur der Europäischen Union für Cybersicherheit ENISA weist in ihrem Bericht darauf hin, dass Cyberangriffe in Qualität und Quantität zunehmen und die Folgen von Cyberangriffen schwerwiegendere Konsequenzen haben. 2023 wurden darüber hinaus mehr Ransomware-Angriffe sowie Einflüsse aus dem Konflikt zwischen Russland und der Ukraine verzeichnet. Die drei größten Bedrohungen waren Ransomware, Malware und Social Engineering. 2023 wurde Cyberkriminalität auch vermehrt als Dienstleistung angeboten, wobei immer vielfältigere Taktiken und Methoden zur Manipulation der Opfer und zur Erpressung von Geld eingesetzt werden. Social Engineering hat erheblich zugenommen. Phishing ist weiterhin der wichtigste Angriffsvektor, aber auch Angriffe in der physischen Welt nehmen zu.

Wie der Krieg von Russland gegen die Ukraine gezeigt hat und zeigt, nehmen Fehl- und Desinformation wieder zu. Mit einer gezielten Verbreitung von Desinformationen, die mithilfe generativer KI-Tools immer schwieriger als Fälschung auszumachen sind und eine Bedrohung für die Gesellschaft darstellen, ist auch bei den bevorstehenden Wahlen im Jahr 2024 zu rechnen. Generative KI erleichtert Cheap Fakes und Voice Phishing, bei denen vor allem Unternehmen erfolgreich um Geld gebracht werden.

Von der kritischen Schwachstelle bei MOVEit waren Versicherungen, Banken und Kontowechselservices in ganz Europa betroffen. Mehr als 100 Organisationen wurden über eine Zero-Day-Sicherheitslücke beim File-Sharing-Dienst angegriffen. Während die SEC (United States Securities and Exchange Commission) in den USA die Richtlinien für das Melden von Vorfällen verschärft hat, wurde Kundinnen und Kunden in Europa von Unternehmen wie Experian empfohlen, Kreditsummen einzufrieren. Banken haben die Offenlegung von Daten einschließlich Kontonummern eingeräumt.

Die Erpressung der Ransomware-Gang Clop hat die Diskussion um Versicherungsschutz und Zahlungsbedingungen weiter angeregt. Bei Ransomware-Angriffen werden Daten in der Regel verschlüsselt. Clop hingegen droht mit der Veröffentlichung der Daten. Selbst bei Zahlung des geforderten Lösegelds, um deren Offenlegung zu verhindern, müssen Datenschutzverletzung den Behörden gemeldet werden. Ein Datenleck kann den Ruf einer Organisation erheblich schädigen.

Sicherheitskultur aus der Perspektive von Organisationen in Europa



Europa im Vergleich mit der Welt

Größe der Organisation	Einstel-lungen	Verhaltens-weisen	Wissen	Kommunikation	Compliance	Normen	Verantwort-lichkeiten
Groß	75	77	68	72	73	74	69
Europäische Abweichung	-1	0	-1	-1	-2	-1	0
Mittelgroß	75	75	69	74	73	73	69
Europäische Abweichung	-1	2	-1	-1	-2	0	1
Klein	75	75	71	77	73	74	71
Europäische Abweichung	0	2	-1	-1	-1	0	0

Dimensionen

Der europäische Datensatz für das Jahr 2023 umfasst insgesamt 673 Organisationen und 162.688 Personen. Der allgemeine Sicherheitskultur-Score in Europa beträgt wie auch im Jahr davor 73 (unterer mittelmäßiger Bereich).

Für Europa gilt weiterhin: Je kleiner die Organisation, desto höher der Sicherheitskultur-Score. Kleinere Organisationen profitieren von einer persönlicheren und effizienteren Kommunikation. Kommunikationskanäle werden besser wahrgenommen. Es gibt ein stärkeres Zugehörigkeitsgefühl und mehr Unterstützung bei Angelegenheiten in Zusammenhang mit der Sicherheit. Auch in den Dimensionen Wissen und Compliance erzielen kleinere Organisationen einen besseren Score.

Allgemein haben die Teilnehmenden in Europa weniger Verständnis für Sicherheitsrichtlinien und die Mitarbeitenden befolgen diese in einem geringeren Ausmaß (Dimension Compliance). Es gibt auch weniger Verständnis von Angelegenheiten und Aktivitäten in Zusammenhang mit der Sicherheit sowie die entsprechende Kenntnis und das entsprechende Bewusstsein (Dimension Wissen). Diese Dimensionen können wohl am besten durch eine verbesserte Kommunikation positiv beeinflusst werden, an der es in Europa ebenfalls mangelt. Den Organisationen würden bessere Kommunikationskanäle und eine offenere und direktere Kommunikation helfen.

Interessanterweise wird das Verhalten der Mitarbeitenden in Europa in mittleren und kleinen Organisationen als sicherer bewertet als im weltweiten Durchschnitt. Es ist wahrscheinlicher, dass die Mitarbeitenden direkt oder indirekt zur Verbesserung der Sicherheit ihrer Organisation beitragen. Gründe hierfür sind: verschärfte Gesetzgebung und Steuerung, die anhaltende Bedrohung durch den Krieg zwischen Russland und der Ukraine sowie die intensivierten Bemühungen von Behörden für mehr Cybersicherheit und Sensibilisierung.

Verfügbarkeit in verschiedenen Sprachen und Lokalisierung

Die Verfügbarkeit in verschiedenen Sprachen bleibt ein wichtiger Faktor in Europa, wo mehr als 200 Sprachen gesprochen werden. Darüber hinaus gelten auf europäischer und nationaler Ebene spezifische Anforderungen bezüglich Compliance und der Einhaltung von Rechtsvorschriften. Inhalte müssen lokalisiert werden. Eine einfache Übersetzung reicht nicht aus, da jeweils spezifische Anforderungen gelten. Die Bemühungen müssen den aktuellen kulturellen Unterschieden in Europa gerecht werden.

Einfluss von KI

In Europa sind ähnliche Einflüsse von künstlicher Intelligenz zu erkennen wie im Rest der Welt. Die Bedrohungslage im Bereich Cybersicherheit verschärft sich. Phishing-Angriffe nehmen in Quantität und Qualität zu. Auch Fehl- und Desinformation werden durch generative KI verstärkt verbreitet. KI wird von der ENISA bereits als Bedrohung für die Cybersicherheit angesehen. Nach der Verbreitung von Fehlinformationen erfolgen oft Angriffe anderer Art.

Die mögliche Bedrohung durch KI-gesteuerte Cyberangriffe, wie z. B. Phishing- oder Vishing-Angriffe mit Deepfake-Inhalten, ist zwar noch relativ klein, könnte in der Region aber die Aufmerksamkeit für die Themen Security Awareness und Sicherheitskultur erhöhen. Die Zugänglichkeit von KI-Technologie, allen voran generative KI, eröffnet Möglichkeiten für eine noch nie dagewesene Steigerung der Komplexität und Effektivität von Angriffen. Organisationen müssen sich intensiv mit diesem Thema beschäftigen, da künstliche Intelligenz weiter an Relevanz zunehmen wird.

Künstliche Intelligenz hat auch weiterhin Einfluss auf Unternehmen. In einer Region, in der Compliance einen hohen Stellenwert besitzt, dürften die Ungewissheit über die Auswirkungen von KI auf Arbeitskräfte und die Art der Arbeit sowie tiefgreifende ethische Fragen die Einführung dieser Technologie verlangsamen. Das Gesetz über künstliche Intelligenz soll zwar einen Rahmen schaffen und Rechtssicherheit bieten, ist aber schon vor dem Inkrafttreten umstritten. Rechtliche und regulatorische Schranken führen in der Regel zu einer langsameren, gezielteren Einführung neuer Technologien. Langfristig werden jedoch nur wenige Unternehmen den Verheißungen hinsichtlich Produktivitätssteigerungen widerstehen können.

Wichtige Erkenntnisse

Kleinere Organisationen in Europa erzielen einen höheren Sicherheitskultur-Score. Dies liegt an einer effektiveren persönlichen Kommunikation, einem stärkeren Gefühl der Zugehörigkeit und einer besseren Unterstützung in Sicherheitsfragen. Daraus ergeben sich ein höherer Wissensstand und eine höhere Compliance. Wesentlich ist eine Verbesserung der Kommunikationskanäle, die im weltweiten Vergleich für ein besseres Verständnis von Sicherheitsrichtlinien und ein proaktives Sicherheitsverhalten sorgen.

Die Sicherheitskultur in Europa weist je nach Branche deutliche Unterschiede in Bezug auf Verständnis und Akzeptanz auf. In stark digitalisierten Sektoren besteht tendenziell ein stärkeres Bewusstsein. Viele Organisationen stehen bei der Entwicklung einer proaktiven Sicherheitskultur jedoch noch ganz am Anfang. Organisationen in Europa erkennen die strategische Bedeutung der Integration von Security Awareness in ihre Kultur, um die Resilienz zu erhöhen. Eine große Herausforderung bleibt, Cybersicherheit endlich auch bereichsübergreifend zu betrachten.

Die EU nimmt bei der Gestaltung globaler Cybersicherheitsstandards eine Führungsrolle ein – durch robuste Gesetze und Verordnungen wie die DSGVO, branchenspezifische Verordnungen wie NIS2 und bevorstehende umfassende Richtlinien wie DORA und das Gesetz über künstliche Intelligenz. Die ENISA sieht für das Jahr 2023 einen drastischen Anstieg der Cyberangriffe, wobei Ransomware, Malware und Social Engineering die größten Bedrohungen darstellen. Diese werden durch Dienstleistungsangebote in der Internetkriminalität und physische Angriffe noch verschärft.

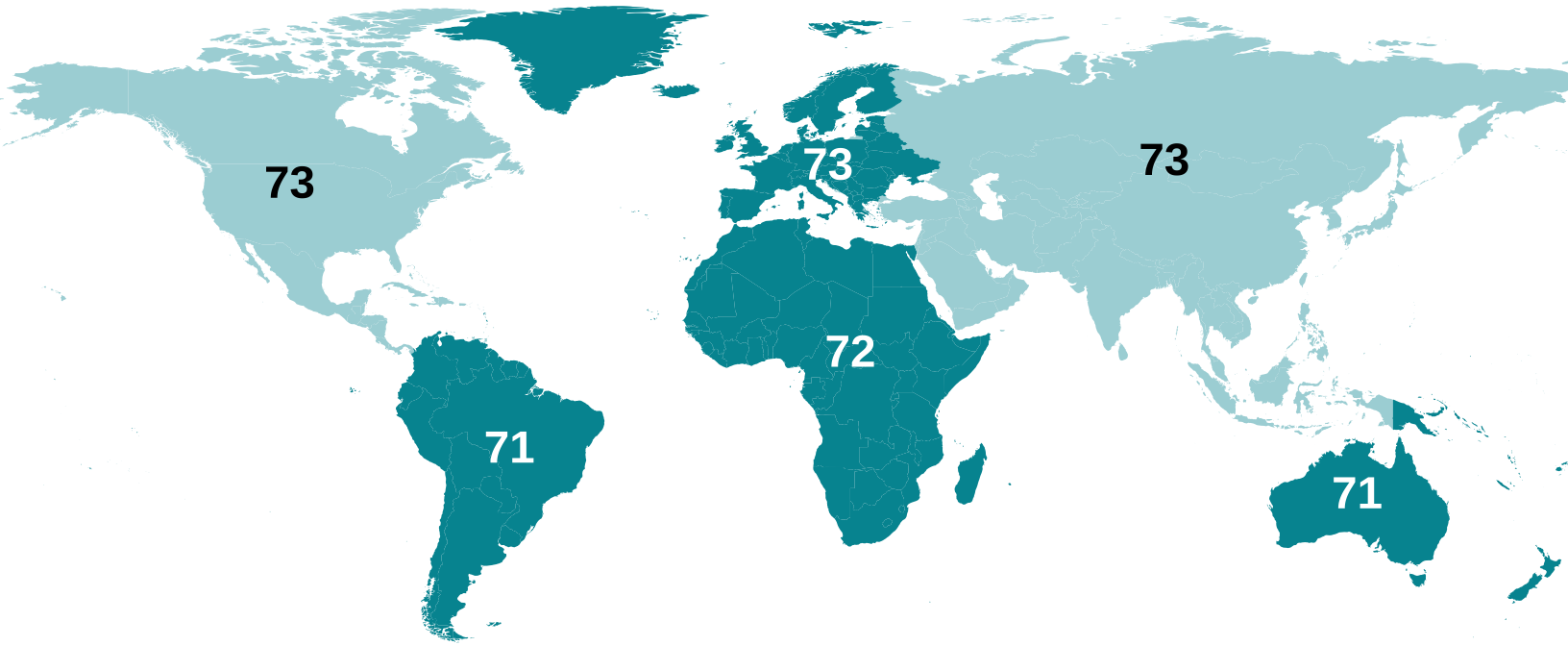
Durch generative KI verbreitete Fehlinformationen werden zu einem immer größeren Problem, während schwerwiegende Datenpannen wie bei MOVEit und Erpressungstaktiken wie bei Clop die Vorschriften für das Melden von Cybersicherheitsvorfällen, Maßnahmen zur Kreditsicherung und Reaktionen der Versicherungsbranche auf Ransomware und Datenlecks beeinflussen.

In Europa gibt es 24 anerkannte Amtssprachen und unterschiedliche gesetzliche Rahmenbedingungen, sodass eine sorgfältige Lokalisierung und kulturell differenzierte Compliance-Strategien erforderlich sind, um Cybersicherheit rund um den Faktor Mensch auf dem gesamten Kontinent effektiv umzusetzen.

Der Einfluss von KI in Europa spiegelt die globalen Trends wider: Die ENISA sieht die Zunahme raffinierter Phishing-Angriffe und die Nutzung generativer KI für die Verbreitung von Fehlinformationen als Bedrohung an. Der traditionell auf Compliance ausgerichtete Markt und die Vorsicht in Bezug auf ethische Implikationen von KI sowie die Auswirkungen auf die Belegschaft könnten die Akzeptanz bremsen, auch wenn KI den Unternehmen letztlich höhere Produktivität verspricht.

Sicherheitskultur weltweit

Von Javvad Malik, Lead Security Awareness Advocate

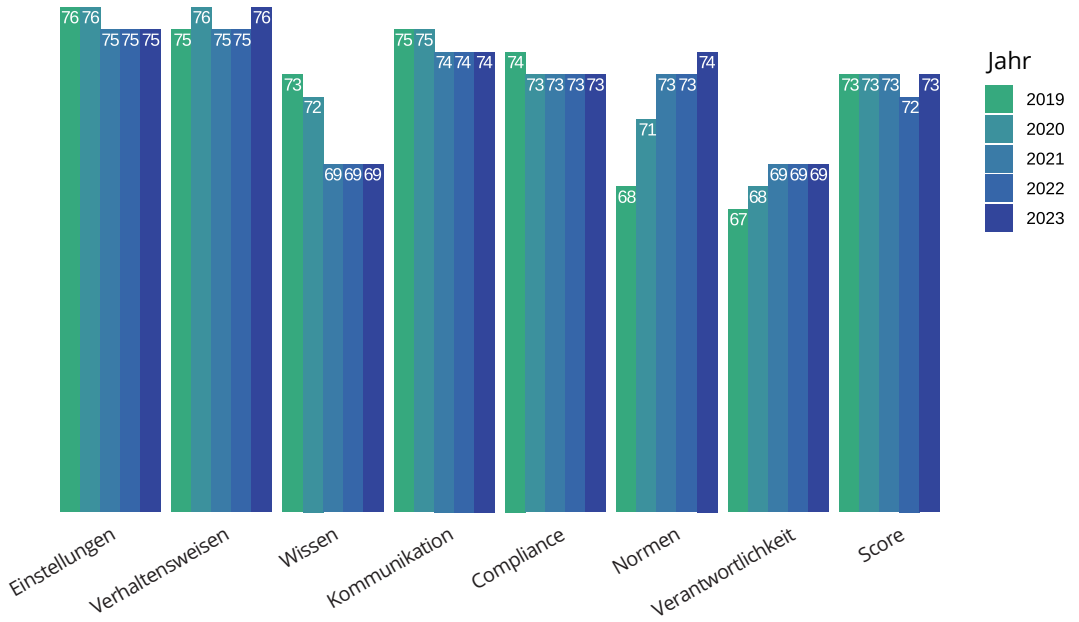


Anpassung der Unternehmenskultur

Möglicherweise liegt Ihnen die Welt zu Füßen. Aber wie gut sind Sie in Sachen Cybersicherheitskultur aufgestellt? Etwa 5,35 Milliarden Menschen haben Zugang zum Internet. Das bedeutet, dass 66,2 % der Weltbevölkerung ein mögliches Ziel von Cyberkriminellen sind. Vor diesem Hintergrund ist die Stärkung der Sicherheitskultur mehr als nur eine unternehmerische Herausforderung. Es ist eine gesellschaftliche Notwendigkeit.

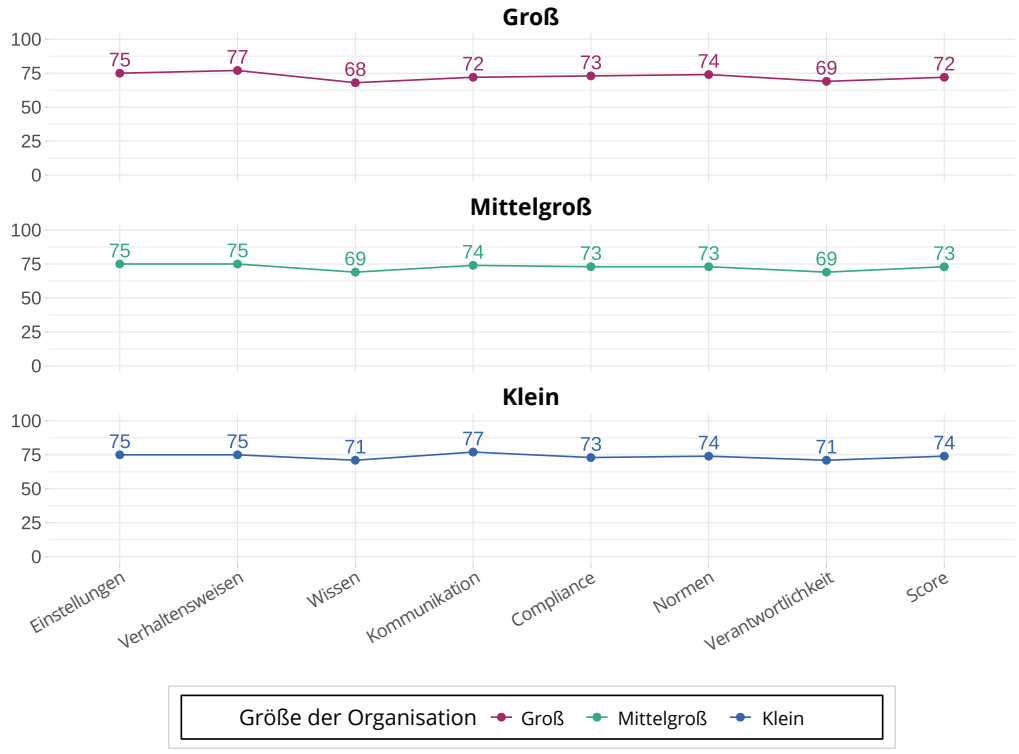
Der Aufbau einer soliden Sicherheitskultur, die auf die Risikotoleranz und die allgemeine Kultur abgestimmt ist, wird von Organisationen auf der ganzen Welt ganz unterschiedlich vorangetrieben. Obwohl sich bereits viele Regierungen und Organisationen darum bemüht haben, eine Cybersicherheitsstrategie zu entwickeln und umzusetzen, sind die jeweiligen Erfolge unterschiedlich.

Trends in der Sicherheitskultur in allen Dimensionen weltweit



Viele Organisationen versuchen, den Aufbau einer Cybersicherheitskultur so umzusetzen wie ein Technologieprojekt. Ein Ansatz, der bei Computern und Netzwerken funktioniert, ist jedoch zum Scheitern verurteilt, wenn der Faktor Mensch ins Spiel kommt. Dieses Problem der Umsetzung kann ein Grund dafür sein, warum konkrete Schritte zum Aufbau einer starken Kultur nur zögerlich erfolgen oder zu einer Compliance-Übung verkommen. Mit Security-Awareness- und Trainingsmodellen aus längst vergangenen Tagen, in denen die Mitarbeitenden einmal im Jahr ein Training absolvieren, kann keine solide Cybersicherheitskultur aufgebaut werden.

Sicherheitskultur aus der Perspektive von Organisationen weltweit



Allgemeine Einstellungen

Die Sicherheitskultur ist in Organisationen auf der ganzen Welt unterschiedlich ausgereift. Mancherorts sind Menschen sicherheitsbewusster und wachsamer gegenüber Bedrohungen auf privater Ebene. Diese Security Awareness wird jedoch nicht automatisch auf Organisationen übertragen. An anderen Orten wird die Abwehr von Bedrohungen als Aufgabe der Organisation betrachtet, um die sich einzelne Personen nicht kümmern müssen.

Erfahrungsgemäß gedeiht die Sicherheitskultur dort, wo sie nicht nur für die Organisation, sondern auch für die Mitarbeitenden relevant ist – wenn Inhalte aus einem Training auch privat sinnvoll angewendet und an Verwandte oder Bekannte weitergegeben werden können.

Positiv ist, dass offenbar immer mehr Organisationen bei Initiativen für Cybersicherheit und beim Aufbau einer soliden Sicherheitskultur nicht nur technologische Kontrollen, sondern auch den Faktor Mensch berücksichtigen.

Wichtige behördliche Vorschriften (d. h. Gesetzgebung)

Weltweit wird mit alten und neuen behördlichen Vorschriften versucht, das Thema Cybersicherheit bei Organisationen in den Fokus zu rücken. Diese konzentrieren sich jedoch meist nur auf technologische Kontrollen, Anforderungen bezüglich der Meldung von Vorfällen oder ein grundlegendes Bewusstsein. Obwohl dies alles Bausteine für den Aufbau einer Sicherheitskultur sind, ist mehr erforderlich.

Sicherheitsereignisse/drängende Probleme

Viele Ereignisse auf der ganzen Welt wirken sich auf die Sicherheitskultur von Organisationen aus. Cyberkriminalität steht bei vielen Organisationen weiterhin im Fokus. Obwohl Probleme wie Ransomware bekannt sind, wird oft vernachlässigt, dass diese meist über Social Engineering verbreitet wird.

Das hat sich 2023 deutlich gezeigt. Bei der Umstellung auf dezentrale oder hybride Arbeitsmodelle wurden Technologien zu schnell eingeführt, ohne auf Cybersicherheit und entsprechendes Training zu achten. Das haben viele Organisationen zu spüren bekommen.

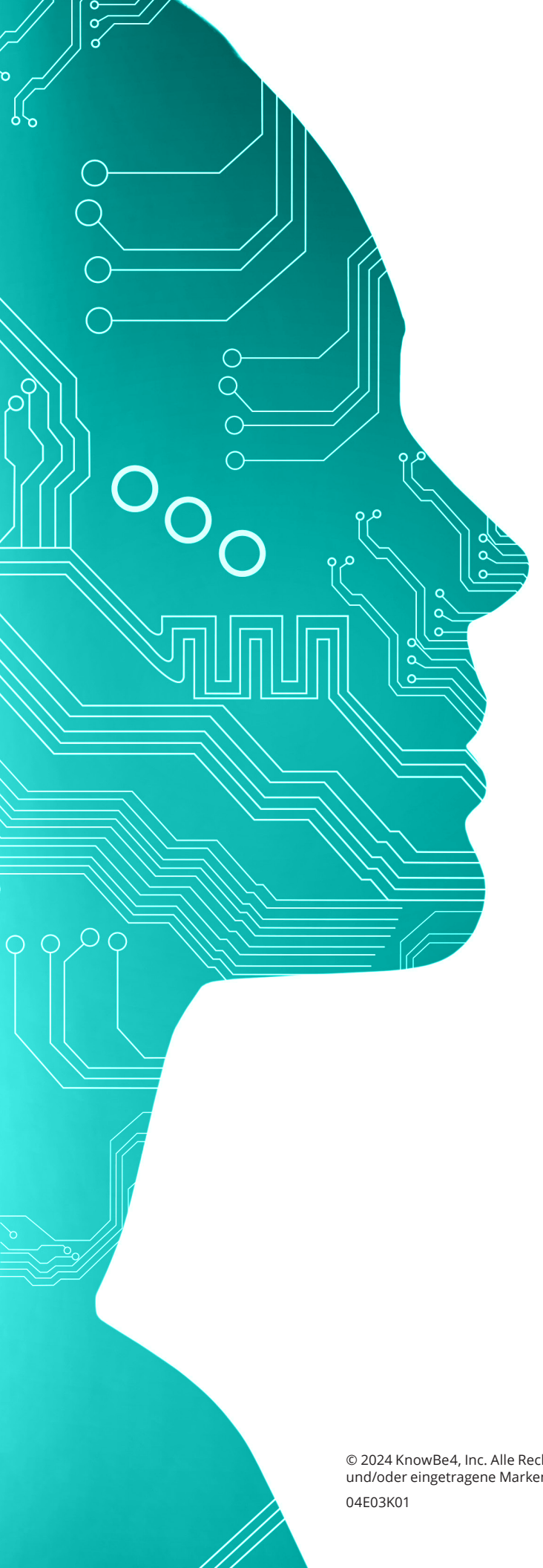
Diesen Problemen während der COVID-19-Pandemie, zu denen auch Hamsterkäufe von Toilettenpapier gehört haben, sind neue globale Ereignisse mit komplexen Risiken gefolgt. 2022 hat Russland mit seiner Invasion in die Ukraine begonnen, im Jahr darauf ist der Nahostkonflikt eskaliert. Cybersicherheit spielt bei all diesen Themen eine bedeutende Rolle. Nicht nur für die direkt Betroffenen, sondern für Menschen auf der ganzen Welt.

Dimensionen

2023 haben wir Daten von 816.733 Mitarbeitenden aus 4.078 Organisationen erfasst. Der allgemeine Sicherheitskultur-Score weltweit beträgt wie auch im Jahr davor 72 (unterer mittelmäßiger Bereich). Wie erwartet haben kleinere Organisationen einen höheren Sicherheitskultur-Score. Es ist viel leichter, die Kultur innerhalb einer kleinen Gruppe als innerhalb einer großen Gruppe zu ändern. Lediglich in der Dimension Verhaltensweisen haben große Organisationen einen höheren Score als andere erzielt.

Weltweit sind die Werte für Kenntnisse, Wissen und Bewusstsein in Bezug auf Sicherheit sowie für Verantwortlichkeit zurückgegangen.

Die Varianz schwankt abhängig von geografischem Standort, Größe der Organisation und Branche stark. Die Zahlen zeigen jedoch deutlich, dass in Sachen Sicherheitskultur noch viel zu tun ist.



Einfluss von KI

Von allen neuen Technologien wird künstliche Intelligenz (KI) wahrscheinlich die tiefgreifendsten Auswirkungen auf die Cybersicherheit von Organisationen und Personen haben. KI wird bereits eingesetzt, um Desinformationen und Fehlinformationen zu verbreiten, Social-Engineering-Angriffe zu verstärken und mehrschichtige und vielschichtige Angriffe in großem Umfang zu automatisieren – selbst wenn die Angreifenden wenig oder kaum technisches Know-how besitzen.

In den kommenden Monaten und Jahren, wenn Wahlen anstehen, sich Kriege ausbreiten oder andere unvorhergesehene Ereignisse passieren, wird KI im Repertoire von Kriminellen immer wichtiger werden. Angesichts des aktuell geringen Bewusstseins und fehlender wirksamer Vorschriften kann es schon zu spät sein, wenn sich Regierungen und Behörden entscheiden, zu handeln.

Wichtige Erkenntnisse

Die Sicherheitskultur ist je nach Region sehr unterschiedlich ausgeprägt. Das ist in unserer voll vernetzten Welt ein Problem, denn Cyberbedrohung kennt keine nationalen Grenzen. Wir benötigen ein ganzheitliches Konzept. Regierungen müssen enger untereinander und mit den Aufsichtsbehörden zusammenarbeiten. Es dürfen nicht nur Vorschriften festgelegt werden, es müssen auch konkrete Schritte für den Aufbau einer starken Kultur definiert werden.

Organisationen müssen den Faktor Mensch berücksichtigen und dürfen Cybersicherheit nicht nur aus technologischer Perspektive betrachten. Computer können mit einem Patch auf den neuesten Stand gebracht werden. Um „Sicherheitslücken“ bei Menschen zu schließen, sind kontinuierliche Sensibilisierung und kontinuierliches Training erforderlich. Ich möchte mit einem Zitat von Nelson Mandela abschließen: „Bildung ist die mächtigste Waffe, um die Welt zu verändern.“

Hier können Sie den kompletten Report herunterladen!

04E03K01