TREE SOLUTION
SECURITY AWARENESS SINCE 2005

Report

Security Culture Code

20 Jahre Security Awareness Radar – Strategische Leitlinien für eine wirksame Sicherheitskultur

Version 1.2, 19. Mai 2026

Ein persönliches Wort des Autors

Als ich vor über zwei Jahrzehnten am international institute of management in technology (iimt) der Universität Fribourg im Rahmen meiner Dissertation den Grundstein für den Security Awareness Radar legte, war Informationssicherheit noch stark technisch geprägt. Firewalls und Antivirenprogramme dominierten; der Mensch galt primär als Fehlerquelle, kaum als strategische Ressource der Resilienz.

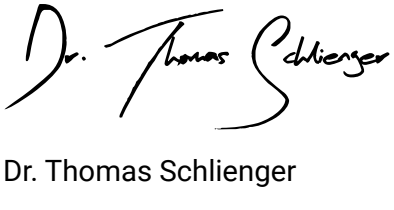
Die Vision war, Sicherheitskultur als bis dahin «weiches» Thema messbar, vergleichbar und damit steuerbar zu machen. Aus dieser wissenschaftlichen Fragestellung ist über 20 Jahre eine der umfassendsten Zeitreihen zur Informationssicherheitskultur im deutschsprachigen Raum entstanden.

Nach 88 Umfragen mit über 100'000 Teilnehmenden zeigt der Datensatz: Einige frühe Hypothesen haben sich bestätigt, andere Ergebnisse haben überrascht. Diese Bilanz ist daher mehr als eine Langzeitauswertung. Sie reflektiert den Reifeprozess einer ganzen Disziplin – und sie verdichtet sich zu dem, was ich heute als den **Security Culture Code** bezeichne.

In den vergangenen zwei Jahrzehnten hat der Security Awareness Radar die Entwicklung der Informationssicherheitskultur in zahlreichen Organisationen begleitet. Die vorliegende Publikation versteht sich nicht als reine Rückschau. Sie dechiffriert jene strategischen Leitlinien, die entscheiden, ob Sicherheitskultur lediglich eine formale Hülle bleibt oder zum wirksamen Betriebssystem einer resilienten Organisation wird.

Der Bericht versteht sich deshalb zugleich als Rückblick und als Roadmap für eine Sicherheitskultur, die einer hochvernetzten und volatilen Zukunft standhält.

Herzlich



Dr. Thomas Schlienger

Management Summary: Der Security Culture Code

Die Ergebnisse aus 20 Jahren Security Awareness Radar zeigen: Technologische und strukturelle Aufrüstung allein genügen nicht. Wirkliche Resilienz entsteht erst durch den **Security Culture Code** – die strategische Dekodierung dessen, was Sicherheitskultur im Kern antreibt.

Die Langzeitauswertung belegt eine breite Professionalisierung; der Anteil an Organisationen mit ungenügender Reife ist deutlich gesunken. Doch der Schritt zu kultureller Exzellenz gelingt nur wenigen. Der Grund: Höhere Reifegrade erklären sich nicht durch mehr Wissen – dieses ist oft bereits auf gutem Niveau –, sondern durch die Verankerung in der sozialen und organisatorischen Struktur.

Der **Security Culture Code** für eine wirksame Sicherheitskultur definiert sich über vier strategische Stellschrauben:

1. Systemlogik vor Geografie: Gemeinsame Frameworks bilden die Infrastruktur für Wirksamkeit.
2. Führung als Katalysator: Vorbildfunktion und Wahrnehmung der Reife entwickeln sich untrennbar zusammen.
3. Konkrete Handhabbarkeit: Motivation steigt dort, wo Sicherheit im Alltag durch klare Prozesse lebbar wird.
4. Aufmerksamkeit statt Wissen: Erfolg wird nicht durch die Menge der Informationen, sondern durch die Steuerung organisatorischer Aufmerksamkeit gemessen.

Fazit für Entscheider: Der nächste Reifeschritt erfordert seltener zusätzliche Schulungen, sondern die sichtbare Integration von Sicherheit in Führung, Kommunikation und Routinen. Das Ziel ist Sicherheitskultur als integraler Bestandteil des organisatorischen Betriebssystems.

Daraus leitet der Bericht eine Roadmap für 2026 bis 2030 ab.

Hohe Reife entsteht dort, wo Führung Sicherheit sichtbar priorisiert, Kommunikation und Befähigung zusammenwirken und Sicherheit in Prozesse sowie Routinen eingebettet wird.

Inhaltsverzeichnis

TREESOLUTION

Abbildungsverzeichnis

Tabellenverzeichnis

1. Warum Kultur heute über Resilienz entscheidet

Informationssicherheit entscheidet sich heute nicht mehr nur an technischen Schutzmassnahmen. Firewalls, Identitätsmanagement und Endpunktschutz bleiben unverzichtbar, reichen für organisatorische Resilienz aber nicht aus. Wirksam wird Sicherheit erst, wenn Mitarbeitende Anforderungen verstehen, priorisieren und im Alltag in Handeln übersetzen. Genau hier wird Sicherheitskultur zum entscheidenden Faktor.

Die zentrale Frage lautet daher nicht nur, ob Organisationen über geeignete Sicherheitsmassnahmen verfügen, sondern wie tief Sicherheit in Führungsalltag, Routinen, Kommunikation und Zusammenarbeit verankert ist. Reife Sicherheitskultur zeigt sich nicht primär in Kampagnen oder formalen Vorgaben, sondern darin, dass sicheres Verhalten im Arbeitsalltag als alltagstauglich, erwartbar und professionell sinnvoll etabliert ist. Der «Faktor Mensch» wird damit vom Risikofaktor zum Gestaltungsfaktor organisatorischer Resilienz.

Was ist der Security Awareness Radar (SAR)?

Der Security Awareness Radar (SAR) ist ein standardisiertes Instrument zur Erfassung von Informationssicherheitskultur in Organisationen. Er misst Sicherheitskultur nicht nur über Wissen, sondern über mehrere Domänen auf Ebene von Individuum, Gruppe und Organisation, darunter Wissen, Werte, Wahrnehmung, Kommunikation, Vorbildfunktion und organisatorische Einbettung. Die Erhebungen erfolgen in der Regel anonym und wiederholt; damit eignen sie sich für Standortbestimmung, Verlaufsmessung und die Ableitung praxisnaher Massnahmen.

Antworten werden zur Vergleichbarkeit in Punktwerte auf einer Skala von 0 bis 100 überführt. Der aggregierte Gesamtwert heisst Security Awareness Indicator (SAI). Zur theoretischen und methodischen Fundierung vgl. Schlienger (2003, 2006) sowie Keller (2026).

88
Erhebungen

100 Tsd.
Teilnehmende

4.5 Mio.
Einzelantworten

20
Jahre

Der vorliegende Bericht stützt sich auf 88 organisationsweite Erhebungen mit über 100'000 Teilnehmenden und rund 4.5 Millionen Einzelantworten aus den Jahren 2004 bis 2025. Ziel ist nicht der Nachweis allgemeingültiger Kausalitäten, sondern die datenbasierte Einordnung typischer Entwicklungsverläufe und praxisrelevanter Unterschiede zwischen Organisationsformen.

Der Bericht verfolgt zwei Ziele:

1. die Entwicklung der Sicherheitskultur über 20 Jahre empirisch und praxisnah einzuordnen;
2. daraus konkrete Handlungsempfehlungen für unterschiedliche Reifestufen und Organisationskontexte abzuleiten.

2. Die Evolution der Reife – Ein Rückblick auf zwei Jahrzehnte

Die Gesamtauswertung von 2004 bis 2025 zeigt ein klares Bild: Die Mehrheit der Organisationen bewegt sich im mittleren Bereich der Reifeskala. 35 % weisen eine ausbaufähige, 30 % eine gute Sicherheitskultur auf. Demgegenüber stehen 23 % mit ungenügender und 13 % mit sehr guter Reife.

Das spricht für eine deutliche Professionalisierung in der Breite, aber auch für Grenzen auf dem Weg zur Exzellenz. Sicherheitskultur ist in vielen Organisationen keine Randerscheinung mehr; eine belastbare Basis führt jedoch nicht automatisch zu einer tief verankerten, bereichsübergreifend gelebten Sicherheitskultur.

Reifegrade als Orientierungsrahmen

Die Stufen wurden theoretisch hergeleitet und empirisch plausibilisiert. Sie sind keine starren Kategorien, sondern belastbare Bezugspunkte, um Unterschiede und Entwicklungen organisatorischer Sicherheitskultur einzuordnen.

Reifegrad	Security Awareness Indicator (SAI)
Ungenügend	<55
Ausbaufähig	55 bis 62.9
Gut	63 bis 69.9
Sehr gut	>=70

Tabelle 1: Reifegrade und ihre Schwellwerte

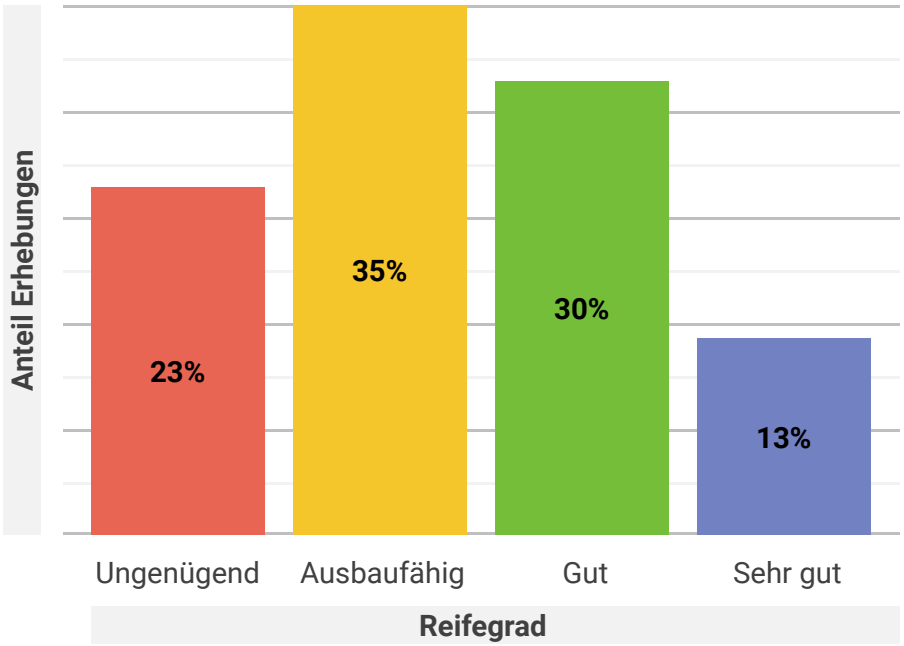


Abbildung 1: Verteilung der Reifegrade 2004–2025

2.1 Differenzierung nach Domänen: Wo liegen die Unterschiede?

Die zwölf Domänen zeigen: Reifegrade unterscheiden sich nicht primär durch Wissen oder allgemeine Wertorientierung. Diese Werte liegen bereits in tieferen Reifestufen vergleichsweise hoch. Die deutlichsten Unterschiede entstehen dort, wo Sicherheit in den organisatorischen Alltag übersetzt wird.

Besonders gross sind die Abstände in:

- Kommunikation: von 30 auf 68 Punkte
- Vorbildfunktion: von 39 auf 62 Punkte
- Schulung: von 29 auf 67 Punkte
- Arbeits- und Technologiegestaltung: von 46 auf 74 Punkte

Höhere Reife entsteht damit vor allem dort, wo Sicherheit nicht nur thematisiert, sondern strukturell unterstützt, sichtbar gemacht und von Führung mitgetragen wird.

Für die Praxis heisst das: Nicht das Wissen allein entscheidet, sondern ob Sicherheit verständlich kommuniziert, im Führungsalltag vorgelebt und in Prozesse, Werkzeuge und Routinen eingebettet wird.

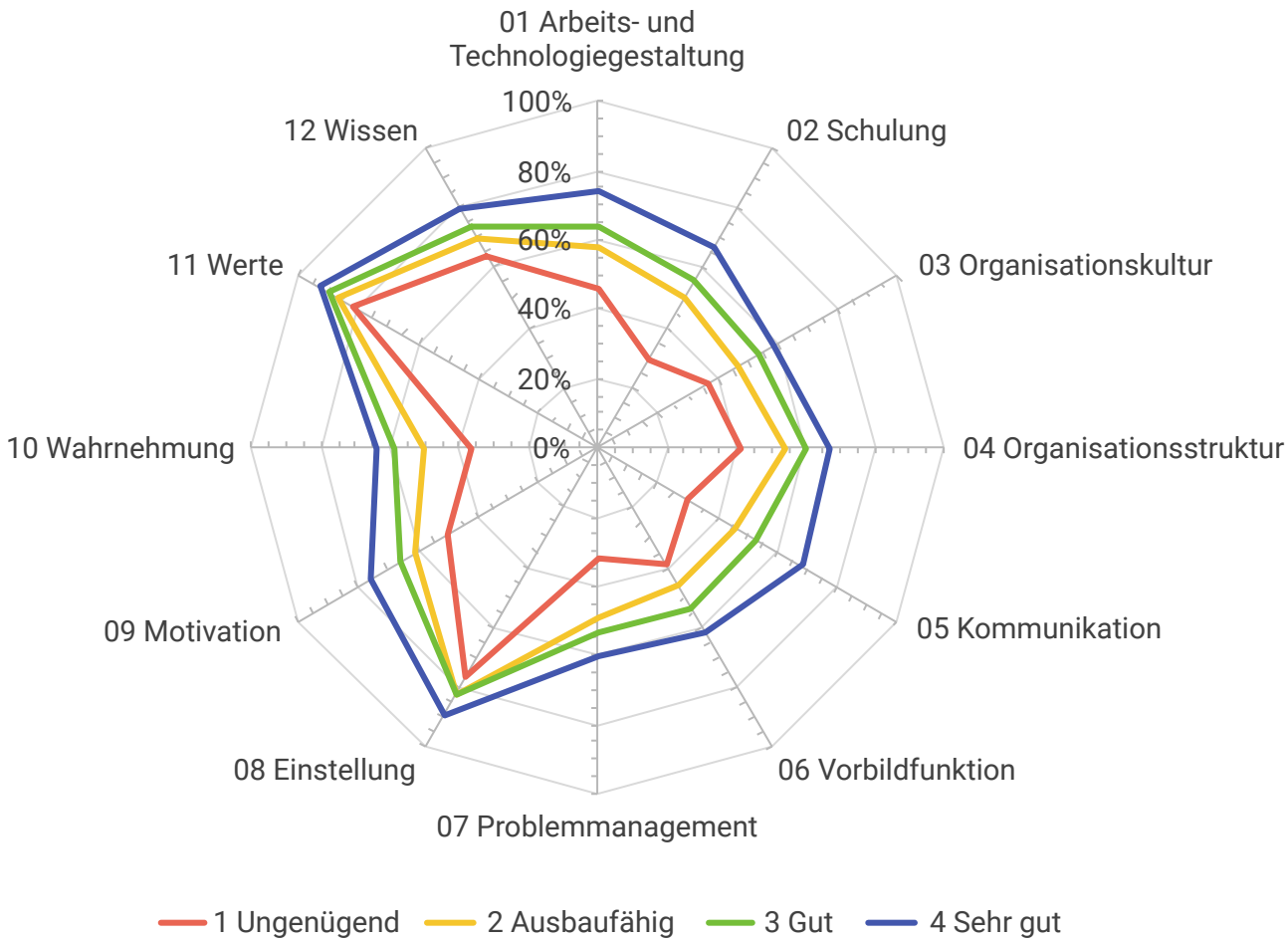


Abbildung 2: Domänenzustimmung 2004–2025 nach Reifegrad

2.2 Die drei Epochen der Sicherheitskultur

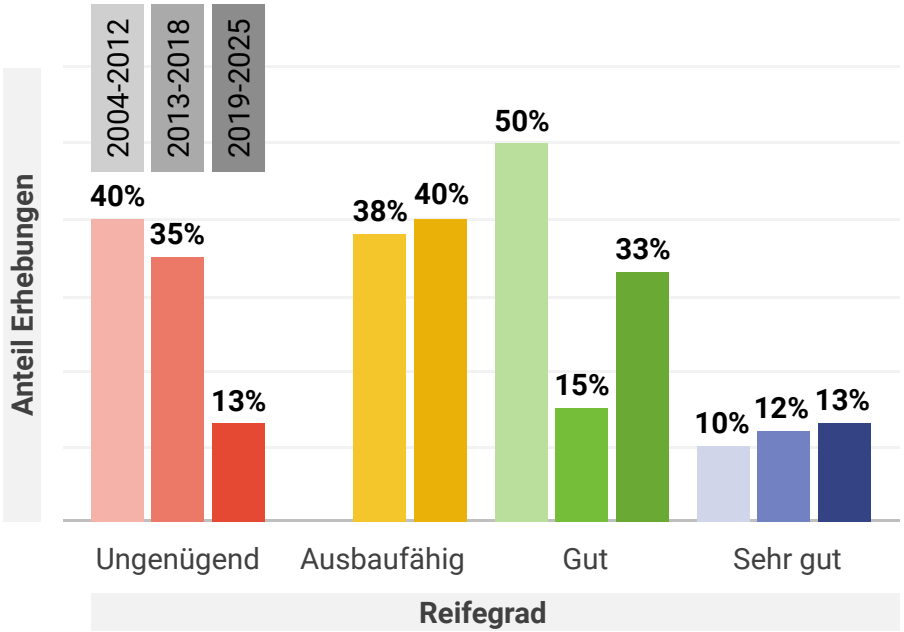


Abbildung 3: Verteilung der Reifegrade nach Epochen
Hinweis: Prozentwerte gerundet; Summen ergeben deshalb nicht immer exakt 100 %. In der Epoche 2004–2012 gab es keine Erhebung mit Reifegrad «2 Ausbaufähig»

Die gläserne Decke zur Exzellenz

Über den gesamten Beobachtungszeitraum bleibt der Anteil von Organisationen mit sehr hoher Reife bemerkenswert stabil und bewegt sich nur in einem Bereich von rund 10 % bis 13 %. Grundlegende Fortschritte sind heute für viele Organisationen erreichbar; deutlich anspruchsvoller bleibt aber der Schritt zu einer tief verankerten, bereichsübergreifend getragenen Sicherheitskultur.

Zur Einordnung der Langzeitentwicklung wurden die Daten in drei Zeitcluster gegliedert:

1. 2004–2012: Pionierphase

Security Awareness war vielerorts noch von technischen Schutzlogiken und formaler Compliance geprägt. Rund 40 % der Organisationen wiesen eine ungenügende Sicherheitskultur auf. Awareness-Massnahmen waren oft punktuell und selten als kontinuierliche Führungs- oder Steuerungsaufgabe verankert.

2. 2013–2018: Professionalisierung

Mit Phishing, digitalisierten Arbeitsformen und internationalen Sicherheitsstandards rückte der Faktor Mensch stärker in den Fokus. Der Anteil ungenügender Sicherheitskulturen sank auf 35 %. Gleichzeitig blieb ein grosser Teil der Organisationen im Bereich ausbaufähig. Das Thema gewann an Breite, ohne dass sich hohe Reifegrade bereits flächendeckend durchsetzten.

3. 2019–2025: Moderne & Resilienz

Der Anteil ungenügender Sicherheitskulturen sinkt markant auf 13 %, während ein Drittel die Stufe «gut» erreicht. Getrieben durch regulatorischen Druck (NIS2, DORA, revDSG) und die Erkenntnis, dass Cyber-Resilienz Chefsache ist, wird Sicherheitskultur zum integralen Bestandteil der Gesamtsteuerung, statt nur technisches Beiwerk zu sein. Damit rückt die organisatorische Resilienz endgültig in das Zentrum der strategischen Aufmerksamkeit.

Über alle drei Phasen zeigt sich ein doppeltes Muster: klare Professionalisierung in der Breite, aber anhaltende Begrenzung an der Spitze. Schwache Ausprägungen nehmen ab; sehr hohe Reife bleibt selten.

2.2.1 Stabilität innerhalb der Reifegrade

Ein zentraler Befund ist die relative Stabilität der Zustimmungswerte innerhalb der einzelnen Reifegrade. Die Reifegrade beschreiben damit nicht nur Momentaufnahmen, sondern relativ stabile Zustandsbilder organisatorischer Sicherheitskultur. Der Wandel zeigt sich primär in der Verteilung der Organisationen über die Stufen, nicht in einer grundsätzlichen Veränderung der Stufen selbst.

Reifegrad	Security Awareness Indicator (SAI)		
	2004-2012	2013-2018	2019-2025
Ungenügend	48.9	49.7	48.5
Ausbaufähig	-	59.6	60.2
Gut	65.9	66.8	66.5
Sehr gut	74.3	73.9	74.7

Tabelle 2: Durchschnittlicher SAI nach Reifegrad und Epoche
Hinweis: In der Epoche 2004–2012 gab es keine Erhebung mit Reifegrad «2 Ausbaufähig».

Der durchschnittliche SAI steigt von 43.8 Punkte im Jahr 2005 auf 65.2 Punkte im Jahr 2025. Die zwischenzeitlich tieferen Werte in der mittleren Phase lassen sich plausibel durch eine breitere und heterogenere Datenbasis erklären. In den frühen Jahren nahmen eher Organisationen teil, die sich bereits intensiver mit dem Thema befassten. Dass die Werte in der aktuellen Periode trotz grösserer Heterogenität wieder das frühe Niveau erreichen oder übertreffen, spricht für eine substanzielle Professionalisierung in der Breite.

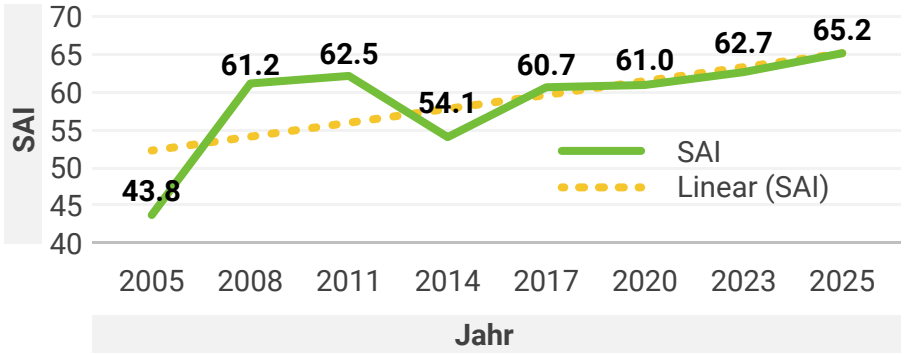


Abbildung 4: Der durchschnittliche SAI von 2004 bis 2025
Hinweis: Es wurden jeweils 3 Jahre zusammengefasst, ausser im letzten Jahr. Die gestrichelte Linie zeigt den Trend.

Domäne	Zustimmungswert		
	2004-2012	2013-2018	2019-2025
01 Arbeits- und Technologiegestaltung	56	56	63
02 Schulung	47	49	53
03 Organisationskultur	55	45	49
04 Organisationsstruktur	56	48	59
05 Kommunikation	47	43	51
06 Vorbildfunktion	49	51	49
07 Problemmanagement	37	44	52
08 Einstellung	81	81	82
09 Motivation	63	61	63
10 Wahrnehmung	57	45	55
11 Werte	88	85	89
12 Wissen	72	70	73

Tabelle 3: Durchschnittliche Domänenzustimmung nach Epoche

2.3 Longitudinale Entwicklungsverläufe (Fallstudien)

Die bisherigen Auswertungen zeigen robuste Muster auf aggregierter Ebene. Für die Praxis ist jedoch ebenso relevant, wie sich Sicherheitskultur in einzelnen Organisationen über Jahre entwickelt. Ergänzend zur Breitenanalyse zeigen nun drei Fallstudien (Keller, 2026), wie unterschiedlich Reifeverläufe ausfallen – von schrittweiser Verbesserung über Reifesprünge bis zu kurzfristigen Schwankungen.

Vergleichbarkeit über die Zeit

Für die Fallstudien wurden pro Organisation nur jene Items in die Berechnung von SAI und Domänenwerten einbezogen, die in allen vier Messungen identisch vorlagen. Dieses Vorgehen folgt der Anker-Items-Methode und verhindert Verzerrungen durch wechselnde Fragensets. Je nach Organisation wurden 17 bis 27 Anker-Items berücksichtigt.

2.3.1 Fallstudie Organisation A

A

Organisationsprofil: National tätige Organisation mit 1'000–5'000 Mitarbeitenden, Sektor 3

Zeitraum: 2012 bis 2025 (13 Jahre, 4 Messzeitpunkte)

SAI-Entwicklung: von 54.6 auf 66.6 Punkte, also +12.0 Punkte bzw. rund +22 %

Organisation A zeigt insgesamt einen klar positiven Verlauf. Nach einer eher seitwärtsgerichteten Entwicklung zwischen 2012 und 2017 steigt der SAI in der zweiten Hälfte deutlich an. Besonders sichtbar sind Fortschritte in Organisationsstruktur, Vorbildfunktion, Kommunikation und Wissen. Gleichzeitig fällt die Domäne Einstellung deutlich zurück. Der Fall zeigt: Substanzielle Reifeschritte sind möglich, verlaufen aber nicht in allen Bereichen parallel.

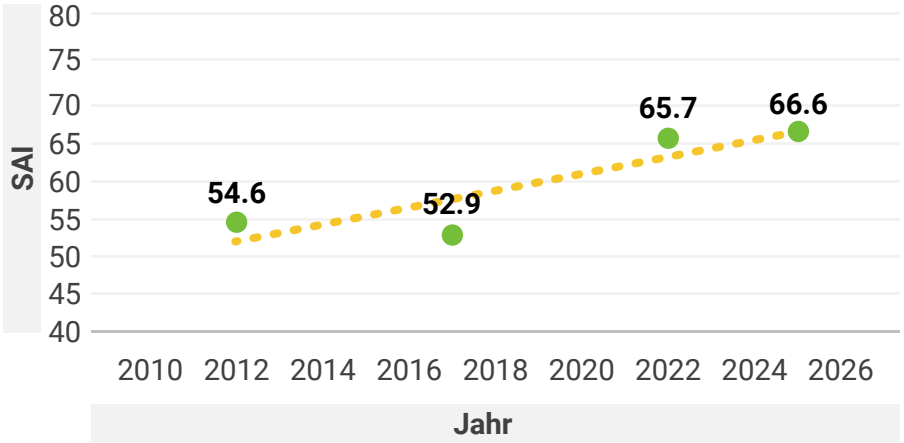


Abbildung 5: Organisation A: SAI-Entwicklung über vier Messungen (gestrichelte Linie stellt den Trend dar)

Domäne	2012	2025	Veränderung
Organisationsstruktur	34	63	+29
Wissen	58	79	+21
Vorbildfunktion	44	64	+20
Kommunikation	49	67	+18
Problemmanagement	41	58	+17
Schulung	56	73	+17
Einstellung	83	50	–33

Tabelle 4: Organisation A: Ausgewählte Veränderungen auf Domänenebene (in Punkten).
Hinweis: Dargestellt sind ausgewählte Domänen mit besonders auffälligen Veränderungen zwischen erstem und letztem Messzeitpunkt. Die Werte sind Punktwerte auf einer Skala von 0 bis 100.

2.3.2 Fallstudie Organisation B

B

Organisationsprofil: Multinationale Organisation mit 25'000–50'000 Mitarbeitenden, Sektor 2

Zeitraum: 2016 bis 2023 (7 Jahre, 4 Messzeitpunkte)

SAI-Entwicklung: von 49.1 auf 71.1, also +22.0 Punkte bzw. +44.8 %

Organisation B zeigt den deutlichsten Reifesprung unter den drei Fällen. Die Entwicklung erfasst mehrere für kulturelle Reife zentrale Domänen gleichzeitig. Besonders stark verbessern sich Schulung, Wahrnehmung, Kommunikation und Problemmanagement; auch die Arbeits- und Technologiegestaltung und Einstellung legen deutlich zu. Der Fall zeigt, dass grosse Reifeschritte besonders dort entstehen, wo mehrere organisatorische und kommunikative Hebel zugleich bewegt werden.

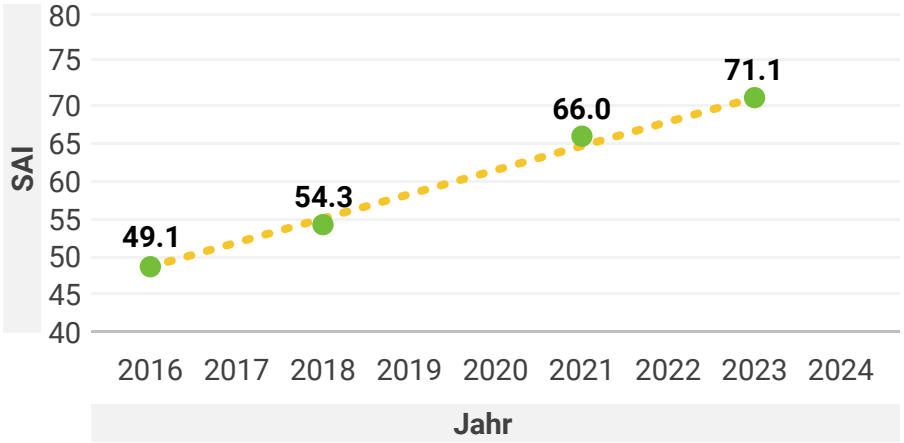


Abbildung 6: Organisation B: SAI-Entwicklung über vier Messungen (gestrichelte Linie stellt den Trend dar)

Domäne	2016	2023	Veränderung
Schulung	20	66	+46
Wahrnehmung	25	61	+36
Kommunikation	28	61	+33
Problemmanagement	42	70	+28
Arbeits- und Technologiegestaltung	47	73	+26
Einstellung	52	76	+24

Tabelle 5: Organisation B: Ausgewählte Veränderungen auf Domänenebene (in Punkten).
Hinweis: Dargestellt sind ausgewählte Domänen mit besonders auffälligen Veränderungen zwischen erstem und letztem Messzeitpunkt. Die Werte sind Punktwerte auf einer Skala von 0 bis 100.

2.3.3 Fallstudie Organisation C

C

Organisationsprofil: Multinationale Organisation mit 5'000 bis 25'000 Mitarbeitenden, Sektor 2

Zeitraum: 2022 bis 2025 (4 Jahre, 4 Messzeitpunkte)

SAI-Bandbreite: zwischen 55.3 und 61.4, insgesamt 6.1 Punkte bzw. 11 %

Organisation C wird jährlich gemessen; dadurch werden kurzfristige Ausschläge sichtbarer. Der SAI steigt von 55.3 auf 61.4 und fällt 2025 wieder auf 57.7. Der Verlauf ist deshalb eher als kurzfristige Dynamik, denn als stabiler Langfristtrend zu lesen. Die Bilanz verdeutlicht: Während strukturelle Anpassungen oft nachhaltig wirken, sind Erfolge in der Kommunikation und Führung hochgradig flüchtig und erfordern permanente Steuerung, um nicht innerhalb eines Jahres auf das Ausgangsniveau zurückzufallen.

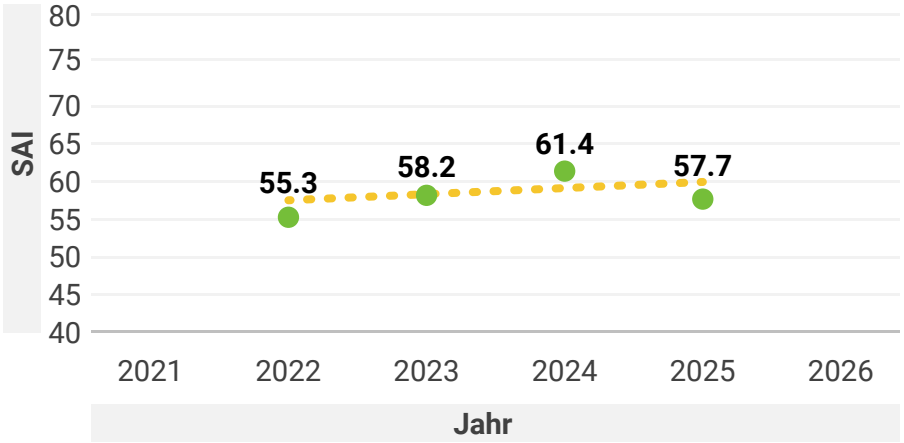


Abbildung 7: Organisation C: SAI-Entwicklung über vier Messungen (gestrichelte Linie stellt den Trend dar)

Domäne	2022	2024 (Peak)	2025	Bilanz
Strukturelle Domänen				
Arbeits- und Technologiegestaltung	58	66	68	+10 (Nachhaltig)
Problemmanagement	58	67	63	+5 (Moderat)
Soziale Domänen				
Wahrnehmung	41	48	42	+1 (Flüchtig)
Vorbildfunktion	48	57	48	0 (Flüchtig)
Kommunikation	46	53	46	0 (Flüchtig)

Tabelle 6: Organisation C: Ausgewählte Veränderungen auf Domänenebene (in Punkten).

Hinweis: Dargestellt sind ausgewählte Domänen, die für den kurzfristigen Entwicklungsverlauf besonders aufschlussreich sind. Die Werte sind Punktwerte auf einer Skala von 0 bis 100.

2.3.4 Fazit aus den Fallstudien

Sicherheitskultur entwickelt sich in Organisationen sehr unterschiedlich. Fortschritte entstehen nicht durch Zeitablauf allein, sondern vor allem dort, wo organisatorische, kommunikative und führungsbezogene Voraussetzungen zusammenwirken. Gleichzeitig verlaufen Entwicklungen nicht immer linear: Neben längerfristigen Verbesserungen können – besonders bei engmaschigen Messungen – auch kurzfristige Schwankungen auftreten, ohne dass daraus bereits auf einen stabilen Trend geschlossen werden sollte.

3. Die Anatomie der Sicherheitskultur (2019–2025)

Kapitel 3 konzentriert sich auf das Zeitcluster 2019 bis 2025, weil diese Periode die heutigen organisatorischen, technologischen und regulatorischen Rahmenbedingungen am besten abbildet. Ziel ist die praxisnahe Einordnung gegenwärtiger Muster und Unterschiede zwischen Organisationskontexten.

3.1 Aktuelles Lagebild der Sicherheitskultur

Die aktuelle Periode zeigt ein differenziertes Bild: Das Grundniveau hat sich verbessert, gleichzeitig konzentriert sich ein grosser Teil der Stichprobe weiterhin im mittleren Reifebereich. Gerade dieses breite Mittelfeld ist für die Praxis entscheidend, weil hier weniger ein Mangel an Grundsensibilisierung als vielmehr die Herausforderung der weiteren kulturellen Verankerung sichtbar wird.

Die Verteilung ist klar: 40 % der Organisationen sind ausbaufähig, 33 % gut, 13 % ungenügend und 13 % sehr gut. Grundlegende Anforderungen der Sicherheitskultur sind also in vielen Organisationen etabliert; der Übergang zur kulturellen Exzellenz gelingt deutlich seltener.

Inhaltlich liegt die Schwelle zur kulturellen Exzellenz weniger bei den Grundhaltungen oder dem Wissen – diese liegen bereits auf den unteren Stufen auf einem hohen Niveau. Die eigentliche Differenzierung findet in den organisatorischen und kommunikativen Domänen statt. Die grössten Abstände zwischen ungenügender und sehr guter Sicherheitskultur zeigen sich bei der Schulung, der Kommunikation sowie der Vorbildfunktion. Auch die Arbeits- und Technologiegestaltung trägt massgeblich zur Steigerung des Reifegrades bei, während das Problemmanagement vor allem beim Schritt in die mittleren Reifestufen an Bedeutung gewinnt.

Für die Praxis heisst das: Wissen bleibt notwendige Basis. Der nächste Reifeschritt entsteht aber vor allem dort, wo Sicherheit sichtbarer kommuniziert, im Führungsalltag vorgelebt und in Prozesse sowie Arbeitsbedingungen eingebettet wird.

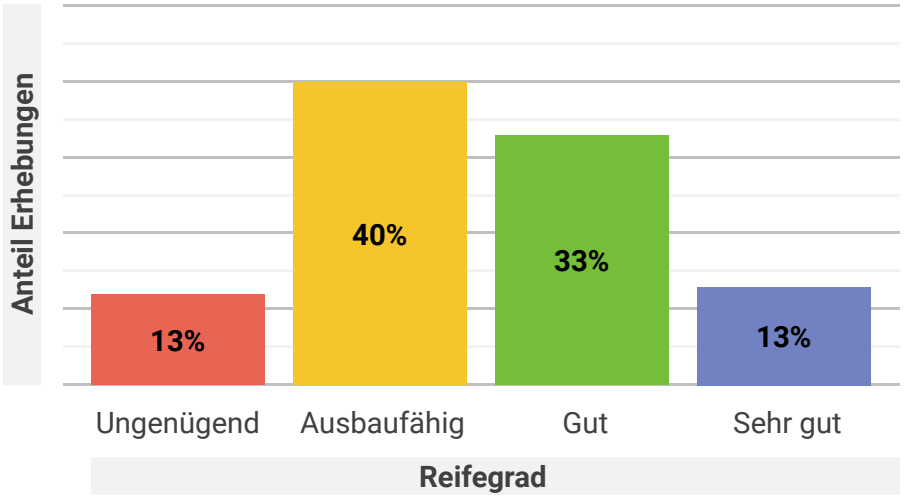


Abbildung 8: Verteilung der Reifegrade 2019–2025

Domäne	Zustimmungswert			
	Ungenügend	Ausbaufähig	Gut	Sehr gut
01 Arbeits- und Technologiegestaltung	49	59	65	76
02 Schulung	28	50	56	69
03 Organisationskultur	33	47	52	58
04 Organisationsstruktur	43	58	62	65
05 Kommunikation	29	48	54	68
06 Vorbildfunktion	32	43	55	63
07 Problemmanagement	35	51	58	61
08 Einstellung	80	80	81	90
09 Motivation	45	62	65	76
10 Wahrnehmung	39	52	59	62
11 Werte	83	88	90	95
12 Wissen	62	70	75	81

Tabelle 7: Durchschnittliche Domänenzustimmung 2019–2025

3.1.1 Was zeigt sich auf Aussagenebene?

Ergänzend zur Domänenanalyse wurden Einzelaussagen betrachtet, die zwischen 2019 und 2025 in mindestens 20 verschiedenen Organisationen in hinreichend vergleichbarer Form vorlagen. Die Aussagenebene illustriert konkrete Stärken und Schwächen des Sicherheitsalltags; die systematische Vergleichsanalyse bleibt bewusst auf Domänenebene.

Aussage	Zustimmung	Perspektive
Keine Passworte weitergeben	94	selbstbezogen
Vorsicht bei verdächtigen E-Mails	93	selbstbezogen
Verantwortung aller	89	Haltung
Nicht (öffentlich) über vertrauliche Dinge sprechen	88	selbstbezogen
Geschäfts-E-Mail nicht für private Zwecke nutzen	83	selbstbezogen

Tabelle 8: Besonders stark ausgeprägte Aussagen

Aussage	Zustimmung	Perspektive
Massnahmen werden durch Vorgesetzten erläutert	39	Führung
Es gibt Vorschriften zur Meldung von Sicherheitsverstössen	46	Organisation
Informationen für neue Mitarbeiter	51	Organisation
Informationen sind verständlich	51	Organisation
Schulung für bestehende Mitarbeitende	53	Organisation

Tabelle 9: Vergleichsweise schwächer ausgeprägte Aussagen

Das Muster ist klar: Hohe Werte finden sich bei grundlegenden sicherheitsbezogenen Verhaltensnormen und persönlich zurechenbaren Erwartungen. Tiefere Werte zeigen sich dort, wo Sicherheit organisatorisch vermittelt, erläutert und im Arbeitsalltag nachvollziehbar gemacht werden muss. Viele Organisationen verfügen somit über eine solide Grunddisziplin, während die kontinuierliche Übersetzung in Führung, Kommunikation und Befähigung anspruchsvoller bleibt.

Hinweis zur Interpretation

Die hoch bewerteten Aussagen beziehen sich überwiegend auf eigenes Verhalten oder persönliche Haltungen; die tiefer bewerteten häufiger auf Organisation, Führung oder Unterstützungsstrukturen. Unterschiede sind daher nicht nur als inhaltliche Stärken oder Schwächen zu lesen, sondern auch vor dem Hintergrund sozialer Erwünschtheit, Selbstzuschreibung und kritischerer Beurteilung des organisatorischen Umfelds.

3.1.2 Vertiefende Zusammenhänge zwischen den Domänen der Sicherheitskultur

Sicherheitskultur lässt sich nicht auf isolierte Domänen reduzieren. Die Analysen zeigen wiederkehrende Muster zwischen mehreren Handlungsfeldern:

Führung und Wahrnehmung

Wo Führung Informationssicherheit sichtbar unterstützt, vorlebt und priorisiert, ist auch die Wahrnehmung von Informationssicherheit stärker ausgeprägt. Führung ist damit kein Zusatzfaktor, sondern zentraler Bezugspunkt dafür, wie Sicherheit im Alltag eingeordnet wird.

Kommunikation und Schulung

Beide Domänen treten wiederholt als eng gekoppelter Entwicklungsbereich auf. Kommunikation ohne Lernangebote bleibt oft abstrakt; Schulung ohne kommunikative Einbettung wirkt häufig punktuell. Nachhaltig ist ein integrierter Ansatz aus Kommunikation, Befähigung und regelmässigen Lernimpulsen.

Werte und Einstellung

Diese beiden Domänen bilden einen kohärenten kulturellen Kern. Wo Sicherheit als gemeinsamer Wert getragen wird, ist die Einstellung gegenüber sicherheitsrelevantem Verhalten typischerweise positiver.

Motivation und Problemmanagement

Motivation entsteht durch konkrete Umsetzbarkeit und einen professionellen Umgang mit Vorfällen. Mitarbeitende handeln engagierter, wenn Prozesse im Ernstfall klar sind und sie durch direktes Feedback auf Meldungen die Wirksamkeit ihres Handelns erleben. Entscheidend ist zudem eine ausgeprägte Fehlertoleranz: Diese «psychologische Sicherheit» stellt sicher, dass aus Fehlern gelernt werden kann, statt sie aus Angst vor Sanktionen zu verbergen.

Strukturelle Verankerung

Verbesserungen über die Zeit gehen häufig mit klaren Zuständigkeiten, Prozessen und Strukturen einher. Kulturentwicklung wird tragfähig, wenn sie institutionell eingebettet ist.

Insgesamt verdichten sich die Ergebnisse zu vier **praxisrelevanten Entwicklungsfeldern:**

1. Führung und Wahrnehmung
2. Kommunikation und Befähigung
3. Werte und kulturelle Verankerung
4. Handhabbarkeit und psychologische Sicherheit

3.1.3 Hinweise auf eine kritischere Bewertung der Führungsumsetzung durch Teamleitungen

Die Bedeutung der Führung zeigt sich nicht nur im Domänenzusammenhang, sondern auch in der hierarchischen Perspektive. Teamleitungen (Position 2) bewerten die Umsetzung von Sicherheitsvorgaben durch ihre direkte Führung (Position 3) tendenziell kritischer als Mitarbeitende (Position 1) ihre Teamleitungen und als das mittlere bzw. obere Management die oberste Führung. In zehn von zwölf Fällen liegt Position 2 unter Position 3, in sieben von zwölf Fällen auch unter Position 1.

Für die Praxis ist das relevant, weil Teamleitungen an der Schnittstelle zwischen Vorgabe und operativer Umsetzung stehen. Kritischere Bewertungen weisen auf Reibungsverluste in der Übersetzung von Sicherheitsanforderungen in den Führungsalltag hin.

Perspektive	Bewertete Führungsebene	Zustimmung
Position 1	Mitarbeitende bewerten Teamleitungen	46.1
Position 2	Teamleitungen bewerten mittleres/oberes Management	42.2
Position 3	Mittleres/oberes Management bewertet oberste Führung	50.5

Tabelle 10: Zustimmungswerte in Items aus der Domäne Vorbildfunktion nach Hierarchiestufe

3.2 Sektorspezifische Dynamiken: Wenn Fachnähe kulturelle Reife nicht automatisch erhöht

Die sektorale Betrachtung relativiert die verbreitete Annahme, techniknahe oder informationsintensive Organisationen seien automatisch kulturell reifer. Im industriellen Sektor liegen 94 % der Organisationen zwischen ausbaufähig und gut. Im wissensintensiven Sektor 4 dagegen werden 50 % als ungenügend eingestuft. Das wirkt zunächst überraschend, weil dort ein hohes Sicherheitsverständnis naheliegt. Die Domänenwerte relativieren dies: Der wissensintensive Sektor erreicht beim Wissen 67 Punkte, liegt damit aber unter dem Dienstleistungssektor mit 75 Punkten und leicht unter dem industriellen Sektor mit 70 Punkten. Noch deutlicher fallen die Unterschiede in den kulturellen und organisatorischen Domänen aus: Kommunikation 37, Vorbildfunktion 33 und Organisationskultur 38.

Für die Praxis ist dieser Befund besonders relevant, weil er eine verbreitete Fehleinschätzung korrigiert: Fachliche Expertise ersetzt kulturelle Steuerung nicht. Wo Sicherheit primär als Aufgabe einzelner Spezialisten verstanden wird, bleiben gemeinsame Orientierung, Führungssignale und soziale Verankerung oft schwächer.

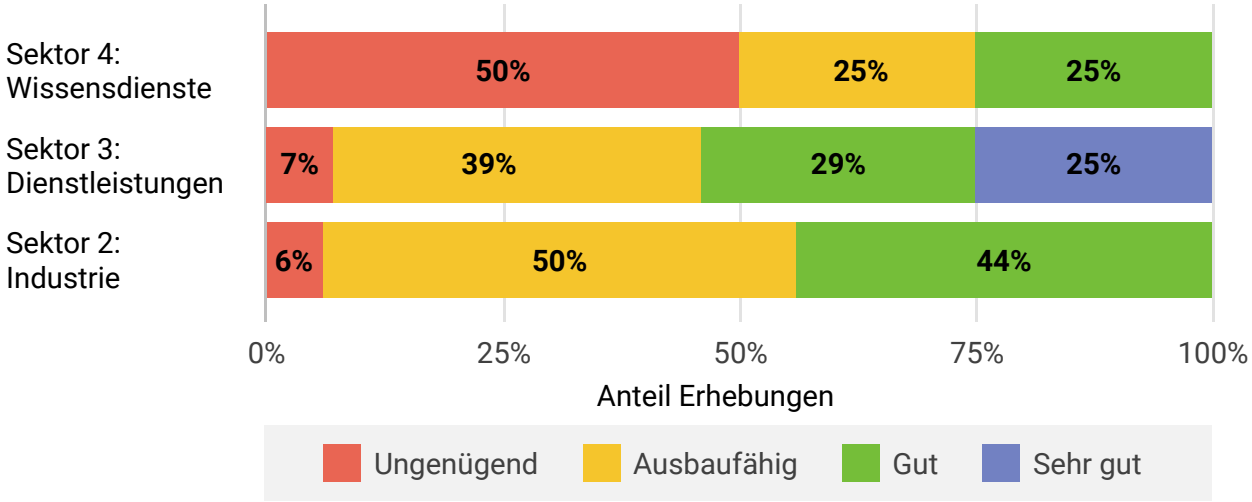


Abbildung 9: Reifegrade nach Sektoren 2019–2025

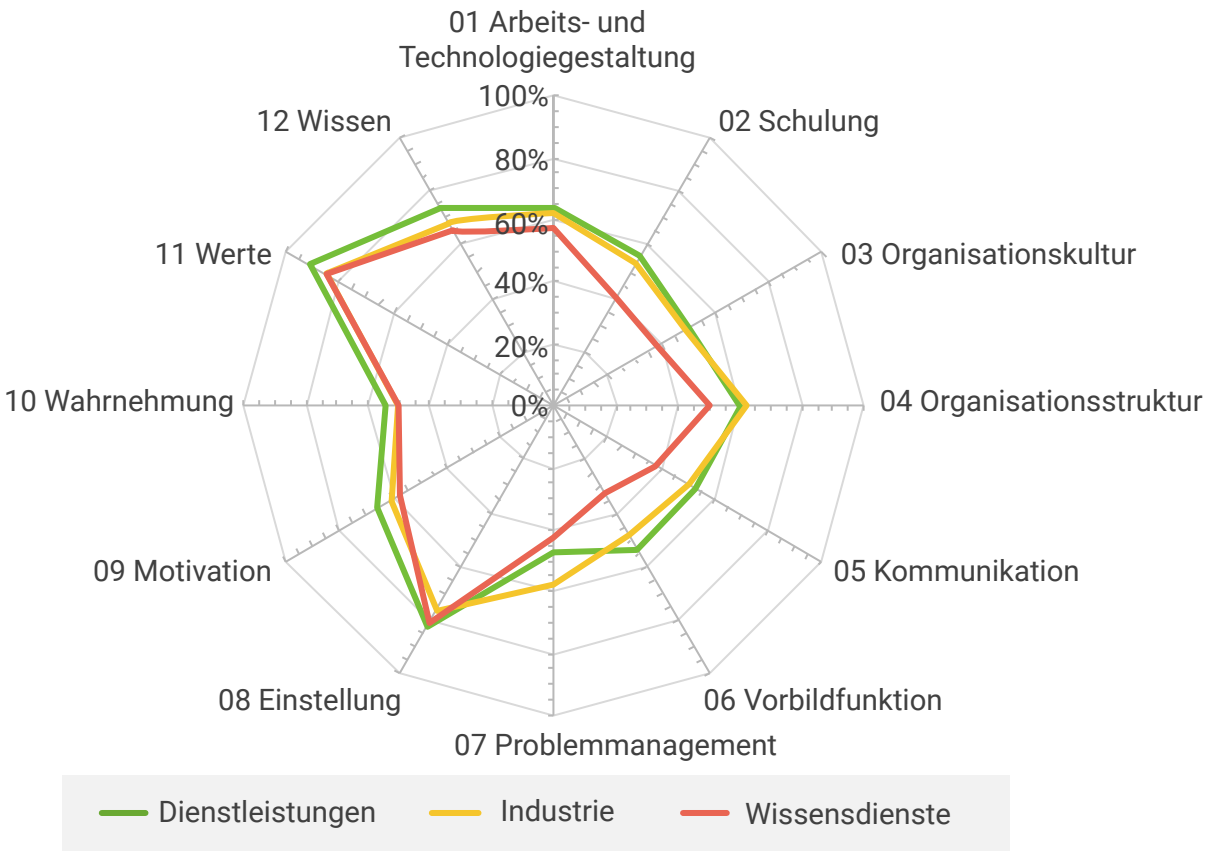


Abbildung 10: Domänenzustimmung nach Sektoren 2019–2025

Sektor 4 ist nicht «schwächer», sondern kulturell anders organisiert

Die niedrigeren Werte in Kommunikation und Führung sind oft Ausdruck einer spezifischen Organisationslogik. In Anlehnung an die Kulturtypen nach Handy (1993) finden sich hier häufiger personen Kontexte, in denen individuelle Autonomie und Expertenstatus über formaler Hierarchie stehen. In solchen Strukturen greifen zentrale Steuerungssignale oft schwächer. Die Herausforderung ist hier nicht fehlendes Wissen, sondern die kollektive Übersetzung dieses Wissens in verbindliche Verhaltensnormen innerhalb einer Experten-Organisation.

3.3 Internationale Aufstellung und kulturelle Reife

Die Unterscheidung nach Multinationalität liefert einen weiteren wichtigen Hinweis. Multinationale Organisationen erreichen häufiger eine hohe bzw. sehr hohe Sicherheitskultur als rein national agierende Organisationen.

Der Vorsprung zeigt sich besonders dort, wo Sicherheitskultur von klaren Prozessen, skalierbaren Massnahmen und konsistenter Umsetzung profitiert – etwa in Arbeits- und Technologiegestaltung, Kommunikation und Wissen. Das spricht weniger für eine generelle Überlegenheit multinationaler Organisationen als für die Wirkung formalisierter Strukturen. Wo Sicherheitsprogramme in Governance-, Reporting- und Standardisierungslogiken eingebettet sind, steigt die Wahrscheinlichkeit, dass Sicherheit systematisch statt punktuell organisiert wird.

Für die Praxis ist nicht Multinationalität entscheidend, sondern die damit oft verbundene Steuerungslogik: verbindlichere Rahmenwerke, höherer Nachweisdruck, standardisierte Roll-outs und die konsequente Übersetzung von Sicherheitsanforderungen in wiederkehrende Prozesse. Kulturelle Exzellenz entsteht daraus jedoch nicht automatisch. Sie entwickelt sich erst dann, wenn diese strukturellen Voraussetzungen durch sichtbare Führung, lokale Verankerung und gelebte Kommunikation wirksam gemacht werden.

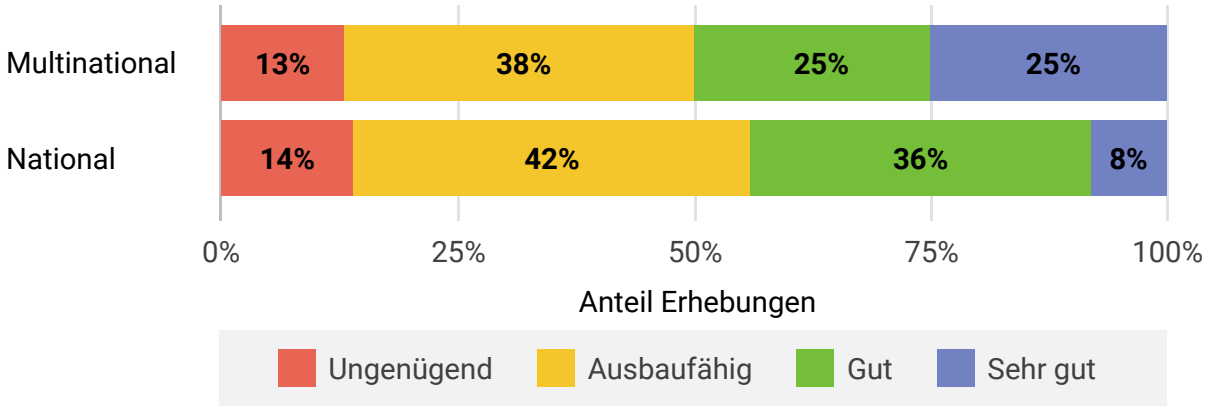


Abbildung 11: Reifegrade nach Multinationalität 2019–2025

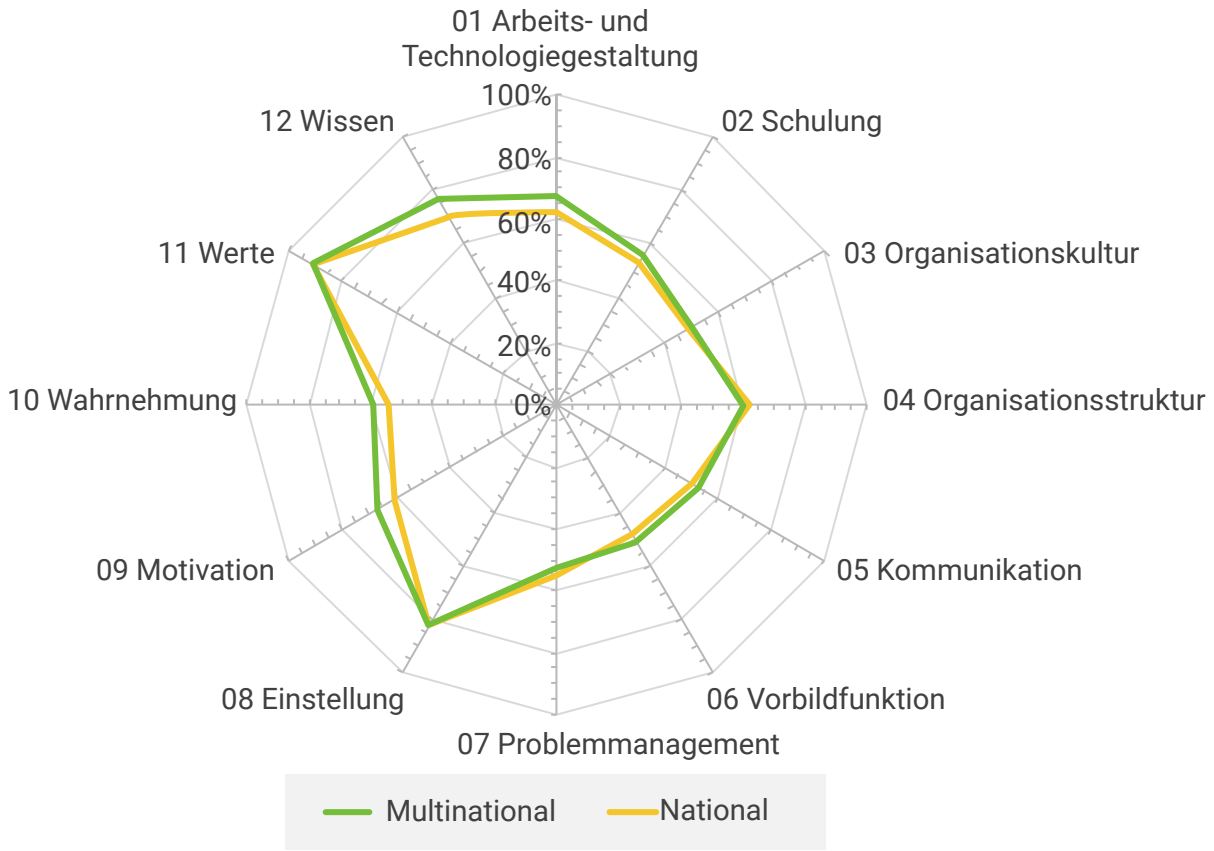


Abbildung 12: Domänenzustimmung nach Multinationalität 2019–2025

Vorsprung durch Systeme, nicht durch Geografie

Der beobachtete Vorsprung beruht primär auf Systemlogik, nicht auf Geografie. Gemeinsame Frameworks, verbindliche Routinen und konsistentes Reporting schaffen die Voraussetzungen, unter denen Führung und Kommunikation kulturell wirksam werden können.

3.4 Spannungsfeld zwischen Strukturstärke und Expertenautonomie

Aus den sektoralen und internationalen Vergleichen ergibt sich ein gemeinsames Spannungsfeld. Der Vergleich zwischen multinationalen Organisationen und wissensintensiven Organisationen des Sektors 4 zeigt zwei unterschiedliche Logiken kultureller Reife. Auf der einen Seite stehen Organisationen, die Sicherheit stark über Systeme, Standardisierung und formalisierte Prozesse steuern. Auf der anderen Seite stehen Kontexte, in denen fachliche Autonomie, Expertenstatus und dezentrale Problemlösung das organisatorische Handeln stärker prägen.

Multinationale Organisationen profitieren davon, dass Sicherheitsanforderungen systematisch ausgerollt, dokumentiert und standortübergreifend vereinheitlicht werden. Das schafft Verbindlichkeit und erleichtert die Übersetzung von Sicherheitszielen in Routinen. Wissensintensive Expertenumfelder zeigen häufiger ein anderes Muster: Sicherheit ist fachlich naheliegend, wird aber eher als Aufgabe informierter Einzelner verstanden, denn als gemeinsame kulturelle Norm. Kommunikation, Vorbildfunktion und organisatorische Verankerung bleiben dadurch oft schwächer.

Für die Praxis ist die Gegenüberstellung aufschlussreich:

- Systemstarke Organisationen riskieren, Sicherheit wirksam zu formalisieren, aber zu stark auf Compliance und Prozessbefolgung zu verengen.
- Expertengeprägte Organisationen verfügen oft über hohe fachliche Kompetenz, unterschätzen aber gemeinsame Verbindlichkeit und sichtbare Führungssignale.

Höhere Reife entsteht in beiden Fällen erst dort, wo formale Anforderungen oder individuelles Expertenwissen in eine gemeinsam getragene, kommunikativ vermittelte und durch Führung gestützte Sicherheitskultur überführt werden.

3.5 Von der Wissensvermittlung zur organisatorischen Aufmerksamkeit

Über alle Reifestufen hinweg zeigt sich ein konsistentes Muster: Hohe Werte bei Wissen und sicherheitsbezogenen Grundhaltungen reichen nicht aus, um kulturelle Exzellenz zu erreichen. Bereits in der Stufe ungenügend liegen Einstellung und Werte vergleichsweise hoch. Auch das Wissen steigt zwar über die Reifestufen, erklärt aber den Unterschied zwischen solider und sehr hoher Reife nicht ausreichend.

Die eigentliche Differenz entsteht stärker in jenen Domänen, in denen Sicherheit sichtbar kommuniziert, durch Führung vorgelebt und im organisatorischen Alltag verankert wird. Für den Übergang von ausbaufähig zu gut oder sehr gut ist daher weniger die Ausweitung von Inhalten entscheidend als die Qualität ihrer organisatorischen Einbettung, besonders in Kommunikation, Vorbildfunktion, Problemmanagement sowie Arbeits- und Technologiegestaltung.

Für die Praxis bedeutet das jedoch nicht, dass Schulung an Bedeutung verliert. Sie bleibt ein notwendiges Basisinstrument für Wissensaufbau, Sensibilisierung und Mindeststandards. Der zusätzliche Fortschritt entsteht ab einem gewissen Reifegrad jedoch seltener durch noch mehr Inhalte allein, sondern häufiger durch sichtbare Führungsaufmerksamkeit, glaubwürdige Vorbilder, lernorientierten Umgang mit Vorfällen und eine bessere Einbettung in Arbeitsprozesse.

Der Reifehebel: Aufmerksamkeit verstärkt, was Schulung vorbereitet

Wissen und Grundwerte liegen in vielen Organisationen bereits auf beachtlichem Niveau. Der nächste Reifeschritt entsteht daher oft nicht durch zusätzliche Inhalte allein, sondern dort, wo Sicherheit im Alltag sichtbarer wird: wenn Führung über Sicherheit spricht, Vorfälle als Lernanlass genutzt werden und sichere Verhaltensweisen in Prozesse und Routinen eingebettet sind. Aufmerksamkeit ersetzt Training nicht; sie erhöht dessen kulturelle Wirksamkeit.

4. Die Roadmap zur kulturellen Reife: Strategische Handlungsempfehlungen für 2026 bis 2030

Die Roadmap zur kulturellen Reife

Die Daten aus zwei Jahrzehnten zeigen: Es gibt keine Einheitslösung für eine starke Sicherheitskultur. Welche Massnahmen den grössten Nutzen bringen, hängt vom Reifegrad und von der organisatorischen Logik ab. Dennoch lassen sich belastbare Entwicklungspfade ableiten.

1 Pfad 1: Das Fundament legen

von **Ungenügend** **zu** **Ausbaufähig**

Organisationen auf dieser Stufe verfügen oft bereits über punktuelles Sicherheitswissen, erreichen aber noch keine verlässliche Übersetzung in den Arbeitsalltag. Sicherheit wird eher als Zusatzaufwand, denn als Unterstützung erlebt. Der erste Entwicklungsschritt besteht deshalb vor allem darin, Reibung zu reduzieren und sichere Verhaltensweisen einfacher in den Arbeitsalltag integrierbar zu machen.

- **Fokus:** Arbeits- und Technologiegestaltung, flankiert durch klare Basiskommunikation
- **Massnahmen:** Reduktion kognitiver Last durch Single Sign-on, Passwortmanager, intuitive Meldewege für Phishing, klare Standardprozesse und leicht verständliche Hilfestellungen im Moment der Handlung
- **Ziel:** Sicherheit von einer individuellen Belastung zu einer organisatorisch unterstützten Selbstverständlichkeit machen

2 Pfad 2: Den «Attention-Gap» schliessen

von **Ausbaufähig** **zu** **Gut**

Dies ist die grösste Gruppe im Datensatz. Basis-Compliance ist meist vorhanden, Sicherheit bleibt aber zu oft in der Fachfunktion verankert und gewinnt im Führungsalltag zu wenig Sichtbarkeit. Der nächste Reifeschritt entsteht weniger durch zusätzliche Inhalte als durch wahrnehmbare Einbettung in Kommunikation, Führung und alltägliche Steuerung.

- **Fokus:** Vorbildfunktion und Kommunikation
- **Massnahmen:** Regelmässige Security-Impulse in Townhalls und Linienformaten, kurze Management-Updates, Integration von Sicherheit in bestehende Führungsroutinen, sichtbare Bezugnahme auf Vorfälle und Lernpunkte statt isolierter Awareness-Kampagnen
- **Ziel:** Sicherheit aus der IT-Nische in die allgemeine Führungskommunikation und den betrieblichen Alltag überführen

3 Pfad 3: Die «gläserne Decke» durchbrechen

von **Gut** **zu** **Sehr gut**

Organisationen auf dieser Stufe haben die Grundstabilisierung erreicht. Der verbleibende Abstand zur kulturellen Exzellenz liegt weniger in zusätzlichen Regelwerken als in der Qualität der sozialen Verankerung. Entscheidend werden lernorientierte Fehlerkultur, glaubwürdige Vorbilder und Motivation über blosse Pflichterfüllung hinaus.

- **Fokus:** Problemmanagement, Motivation und kulturelle Lernfähigkeit
- **Massnahmen:** Aufbau einer positiven Reporting-Kultur, systematische Nutzung von Beinahe-Vorfällen als Lernanlass, Security-Champions-Netzwerke, teamnahe Reflexionsformate und sichtbare Anerkennung erwünschten Verhaltens
- **Ziel:** Sicherheit als Teil organisatorischer Identität, kollektiven Lernens und professionellen Stolzes verankern

4 Pfad 4: Die Strategie für Expertenkulturen

Besonderheit Sektor 4

Für wissensintensive Fachorganisationen greifen die Pfade 1 bis 3 nur dann voll, wenn sie an deren spezifische Organisationslogik angepasst werden. Hohe fachliche Autonomie und ausgeprägter Expertenstatus können Sicherheitskultur stützen, erschweren aber oft zentrale Steuerung und klassische Top-down-Kommunikation.

- **Fokus:** Dezentrale Verankerung, Peer-Kommunikation und fachliche Legitimation
- **Massnahmen:** Einsatz anerkannter Fachmultiplikatoren, Übersetzung von Sicherheitsanforderungen in die Sprache der jeweiligen Profession, teamnahe Diskussionsformate, Communities of Practice und Standards, die als Qualitätsmerkmal statt als externe Bürokratie wahrgenommen werden
- **Ziel:** Sicherheit als Ausdruck professioneller Exzellenz und nicht als administratives Hindernis positionieren

Welcher Entwicklungspfad passt zu Ihrer Organisation?

Die Roadmap ist kein lineares Standardprogramm. Entscheidend ist, welcher Engpass die weitere Reifeentwicklung aktuell am stärksten begrenzt:

- Entsteht Unsicherheit oder Umgehungsverhalten aus hoher Alltagsreibung, stehen Vereinfachung und technische Leitplanken im Vordergrund.
- Ist Basis-Compliance bereits vorhanden, wird sichtbare Führungsaufmerksamkeit zum zentralen Hebel.
- Handelt die Organisation bereits proaktiv, entscheiden Lernkultur, Motivation und glaubwürdige Vorbilder über den nächsten Reifeschritt.
- In Expertenkulturen müssen alle Massnahmen zusätzlich fachlich tragfähig und dezentral legitimiert sein.

5. Schlussbetrachtung: Den Culture Code aktiv gestalten

Die Dekodierung von 20 Jahren Security Awareness Radar macht deutlich: Der **Security Culture Code** ist kein statisches Regelwerk, sondern ein dynamisches Steuerungsmodell. Die Analyse von zwei Jahrzehnten belegt eine deutliche Professionalisierung in der Breite, zeigt aber auch die gläserne Decke zur kulturellen Exzellenz auf.

Die zentrale Erkenntnis: Der nächste Reifeschritt scheitert nicht an fehlendem Wissen, sondern an der Sichtbarkeit und Handhabbarkeit von Sicherheit im Alltag. Wissensgrundlagen sind meist vorhanden; die Differenzierung erfolgt über die soziale und organisatorische Dimension: in der Vorbildfunktion der Führung, der Konsistenz der Kommunikation und der Qualität des Problemmanagements.

Daraus folgt eine differenzierte Steuerungslogik:

- Sicherheitskultur entwickelt sich je nach Organisationskontext unterschiedlich.
- Höhere Reife wird erst dort erreicht, wo Führung, Kommunikation und Befähigung mit systemischer Verankerung verschmelzen.
- Fortschritt entsteht nicht durch isolierte Projekte, sondern durch die gezielte Arbeit an den Bedingungen, unter denen sich sicheres Verhalten im Alltag verstetigt.

Für Entscheidungsträger ist die Messung des Reifegrades kein Abschluss, sondern der Ausgangspunkt. Wer den **Security Culture Code** in seine Strategie integriert, entwickelt eine Resilienz, die weit über das Abhaken von Compliance-Checklisten hinausgeht. Sicherheit wird so zum integralen Bestandteil dessen, wie Organisationen Verantwortung, Zusammenarbeit und Zukunftsfähigkeit organisieren.

Praxis-Check: Drei Konsequenzen für die Awareness-Strategie

Reife regelmässig messen und Entwicklung sichtbar machen

Reifegradmessungen sollten in sinnvollen Intervallen wiederholt und möglichst mit bestehenden Risiko- oder Governance-Prozessen verbunden werden. So lassen sich Stagnation, Plateaueffekte oder neue Schwachstellen früher erkennen und Massnahmen gezielter nachsteuern.

Führung als kulturellen Verstärker nutzen

Die Auswertungen deuten darauf hin, dass Unterschiede in Vorbildfunktion und Kommunikation besonders relevant für höhere Reifegrade sind. Sicherheit sollte deshalb sichtbar in Führungsroutinen, Management-Kommunikation und bereichsübergreifenden Prioritätensetzungen auftauchen – nicht nur in Schulungsformaten.

Benchmarking als Orientierung, nicht als Selbstzweck einsetzen

Der Vergleich mit ähnlichen Organisationen oder Sektoren kann helfen, den eigenen Entwicklungsstand realistischer einzuordnen. Entscheidend ist jedoch nicht die Platzierung im Ranking, sondern welcher Engpass die eigene Reifeentwicklung aktuell am stärksten begrenzt und welche Massnahme unter den gegebenen Rahmenbedingungen den grössten Fortschritt verspricht.

6 Methodische Einordnung der Ergebnisse

88
Erhebungen

100 Tsd.
Teilnehmende

4.5 Mio.
Einzelantworten

20
Jahre

Die Ergebnisse basieren auf 88 organisationsweiten Erhebungen des Security Awareness Radar (SAR) aus dem Zeitraum 2004 bis 2025. Die Datengrundlage umfasst über 100'000 Teilnehmende und rund 4.5 Millionen Einzelantworten.

Ziel der Auswertung ist nicht der Nachweis allgemeingültiger Kausalzusammenhänge, sondern die datenbasierte Einordnung wiederkehrender Muster, typischer Entwicklungsverläufe und praxisrelevanter Unterschiede zwischen Organisationskontexten. Der Bericht ist damit ein empirisch fundierter Praxisbericht, keine umfassende Wirkungsstudie.

6.1 Datengrundlage und Analysefokus

Mit Ausnahme der Fallstudien erfolgen die Analysen auf aggregierter Organisationsebene. Betrachtet werden Mittelwerte und Verteilungsmuster über Organisationen hinweg, nicht individuelle Einzelprofile.

Für die Fallstudien in Kapitel 2 wurde der gesamte Zeitraum 2004 bis 2025 herangezogen. Es wurden dabei ausschliesslich organisationsspezifische Anker-Items berücksichtigt, also nur jene Fragen, die über alle Messzeitpunkte eines Falls in identischer Form vorlagen.

Für die vertiefte Betrachtung in Kapitel 3 liegt der Schwerpunkt auf dem Zeitcluster 2019 bis 2025 mit 52 Erhebungen, da diese Periode die heutigen organisatorischen, technologischen und regulatorischen Rahmenbedingungen am besten abbildet.

Ergänzend zu den deskriptiven Auswertungen wurden Zusammenhänge zwischen den Domänen vertiefend analysiert – organisationsübergreifend und im Längsschnitt. Ziel war, wiederkehrende Muster sichtbar zu machen und jene Domänen zu identifizieren, die besonders häufig gemeinsam mit positiven Entwicklungen in anderen Bereichen auftreten. Diese Ergebnisse sind keine strengen Kausalnachweise, sondern datenbasierte Hinweise auf stabile und praxisrelevante Zusammenhänge.

Für die hierarchiebezogene Analyse wurden nur jene 34 Erhebungen berücksichtigt, in denen Bewertungen für alle drei betrachteten Hierarchiepositionen eindeutig zuordbar vorlagen.

Die sektorale Einordnung folgt der erweiterten Sektorentheorie. Im Datensatz vertreten sind Organisationen aus dem **industriellen Sektor (Sektor 2)**, dem klassischen **Dienstleistungssektor (Sektor 3)** sowie dem **wissensintensiven Quartärsektor (Sektor 4).** Für den Primärsektor lagen keine Fälle vor.

6.2 Herleitung der Reifestufen

Die Einordnung erfolgt über ein vierstufiges Reifegradmodell auf Basis des SAI, der auf den Zustimmungswerten in zwölf Domänen der Sicherheitskultur beruht.

Die Werte beruhen auf einer zustimmungsbasierten Punktelogik auf Ebene der Einzelfragen. Antwortkategorien werden in numerische Werte überführt; starke Zustimmung erhält den höchsten Punktwert, eher zustimmende Antworten entsprechend tiefere Teilwerte. Domänenwerte ergeben sich aus dem Durchschnitt der zugehörigen Einzelfragen und bilden thematische Profile. Der Security Awareness Indicator (SAI) wird davon getrennt als aggregierter Gesamtwert auf Basis aller einbezogenen Einzelfragen berechnet, nicht als Durchschnitt der Domänenwerte. Dadurch lassen sich thematische Stärken und Schwächen auf Domänenebene sowie die Gesamtausprägung der Sicherheitskultur konsistent abbilden.

Die vier Reifestufen dienen als Orientierungsrahmen:

- **Stufe 1 – Ungenügend:** deutliche Schwächen in zentralen Bereichen
- **Stufe 2 – Ausbaufähig:** grundlegende Sensibilisierung vorhanden, aber lückenhafte Verankerung
- **Stufe 3 – Gut:** Sicherheit ist in wesentlichen Bereichen organisatorisch und sichtbar verankert
- **Stufe 4 – Sehr gut:** hohe kulturelle Reife mit starker Integration in Führung, Kommunikation und Alltagsroutinen

Die Schwellenwerte wurden theoriegeleitet definiert und anhand der Verteilung der Organisationsscores zusätzlich empirisch plausibilisiert. Sie schliessen gut an beobachtbare Verdichtungen im Datensatz an.

6.3 Aussagekraft und Grenzen

Die Stärke des Datensatzes liegt in seiner Langfristigkeit, seiner Grössenordnung und seiner Nähe zur organisatorischen Praxis. Dadurch lassen sich Entwicklungen über zwei Jahrzehnte sichtbar machen und typische Muster zwischen unterschiedlichen Organisationsformen nachvollziehen.

Gleichzeitig sind die Ergebnisse mit der für Praxisberichte angemessenen Vorsicht zu interpretieren. Die Auswertungen beschreiben Zusammenhänge und Unterschiede zwischen Gruppen, erlauben aber keine eindeutige Zuschreibung einzelner Ursachen. Unterschiede zwischen Sektoren oder Organisationsformen sind daher nicht als starre Typologien zu lesen, sondern als Hinweise auf unterschiedliche Ausgangslagen und Steuerungslogiken.

Hinzu kommt, dass einzelne Teilgruppen unterschiedlich gross sind und sich die Zusammensetzung der Stichprobe über die Jahre verändert hat. Der Bericht fokussiert deshalb bewusst auf robuste Muster und konsistente Unterschiede, nicht auf eine maximale statistische Ausdifferenzierung jeder Untergruppe.

6.4 Verweis auf die vertiefte methodische Fundierung

Die ausführlichere methodische Fundierung sowie die detaillierte Ausarbeitung der Fallstudien sind nicht Gegenstand dieses Praxisberichts, sondern werden in den entsprechenden Grundlagen- und Vertiefungsarbeiten dargelegt (Schlienger, 2003, 2006; Keller, 2026).

Für die Einordnung dieses Berichts ist wesentlich: Die zugrunde liegende Messlogik wurde methodisch geprüft und über mehrere Jahre weiterentwickelt. Der vorliegende Beitrag baut auf dieser Fundierung auf, konzentriert sich aber bewusst auf die praxisorientierte Interpretation der Ergebnisse und deren strategische Bedeutung für Organisationen.

7 Referenzen

Handy, C. (1993). Understanding Organizations. Penguin Books.

Keller, D. (2026): Multiple Fallstudien des Security Awareness Radars – Entwicklung, Validierung und Fragenauswahl. Masterarbeit im Rahmen des MAS Business Psychology. Zürich: Kalaidos Fachhochschule Schweiz.

Schlienger, T. (2006): Informationssicherheitskultur in Theorie und Praxis – Analyse und Förderung sozio-kultureller Faktoren der Informationssicherheit in Organisationen. Dissertation Universität Freiburg (CH), iimt University Press.

Schlienger, T. & Teufel, S. (2003): Information Security Culture – From Analysis to Change. In: Eloff, J., Venter, H., Labuschagne, L. & Eloff, M. (Eds.): Information Security South Africa – Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton Convention Center, Johannesburg, South Africa. ISSA: 183-195.

Weiterführende Praxisquelle

TreeSolution Security Awareness AG (o. J.): Die Sicherheitskultur messen und Veränderungen nachverfolgen. Online verfügbar unter: TreeSolution, abgerufen am 07.04.2026.

Über TreeSolution

Bei TreeSolution sind wir überzeugt: Effektive Informationssicherheit ist eine Frage der organisatorischen Kultur. Damit Sicherheit dort wirkt, wo sie gebraucht wird, betrachten wir Technik, Prozesse und Menschen als untrennbare Einheit. Selbst die fortschrittlichsten Systeme bleiben wirkungslos, wenn die Menschen, die sie bedienen, nicht über die notwendige Awareness, das passende Wissen und eine gefestigte Sicherheitskultur verfügen.

Was TreeSolution auszeichnet, ist die operative Verankerung unserer Lösungen: Wir basieren unsere Arbeit auf realen Daten, klaren Fakten und zwei Jahrzehnten systematischer Forschung. Unser Fokus auf die menschliche Dimension der Informationssicherheit macht uns zum führenden Partner bei der Dekodierung und Entwicklung Ihrer Sicherheitskultur.

TreeSolution Security Awareness AG
Bösch 23
6331 Hünenberg
Schweiz

Telefon: +41 58 510 98 00
E-Mail: info@treesolution.com
Webseite: www.treesolution.com

TREESOLUTION
SECURITY AWARENESS SINCE 2005

Rechtliche Hinweise