eraneos

Cyber-Readiness-Studie 2022/2023

Cyber Readiness.
Die unternehmerische Maturität und die Steuerbarkeit der Digitalisierung sicherstellen

Studienergebnisse 2022/2023

Vorwort

Die Umfrage gewährt vertiefte Einblicke in die Cyber-Readiness von Schweizer Verwaltungen und Unternehmen. Im Zentrum der Befragung standen die Ausrichtung und die technischen Voraussetzungen zur Stärkung der Cyber-Resilienz sowie die Maturität der hierzu bereits etablierten organisatorischen Strukturen.

Die Studie umfasst vier Themenblöcke: Der erste Teil befasst sich mit der aktuellen Cyber-Readiness der Studienteilnehmenden. Der zweite Teil ist der Cyber-Resilienz gewidmet und untersucht die Widerstandsfähigkeit von Unternehmen gegenüber Ereignissen im Cyberumfeld, während im dritten und vierten Teil die Cyber Governance sowie die Herausforderungen auf dem Weg zur Steigerung der Cyber-Maturität im Vordergrund stehen. Die Datenerhebung erfolgte auf Basis eines strukturierten Fragebogens. Zusätzlich haben wir die adressierten Themenbereiche mit ausgewählten Teilnehmenden im Rahmen von Interviews vertiefend diskutiert.

"Um in ihrer Mission einen angemessenen Grad an Informationssicherheit gewährleisten zu können, sind CISOs mehr denn je gefordert. Trotz steigender Komplexität der zu sichernden Infrastrukturen, trotz immer raffinierterer Angriffsmethoden gilt es, sich das eigene Geschäft als Lösungsanbieter bei der Erreichung seiner Ziele zu unterstützen, Compliance sicherzustellen und das eigene Sicherheitsdispositiv zu stärken."

Adrian Marti, Partner, Eraneos Switzerland AG

Die Autoren

Adrian Marti
Partner
Zürich

Ernst Zeller
Managing Consultant
Bern

Management Summary

Zielsetzungen – Ausgangslage

Cyber Security ist ein zentrales Thema – mehr denn je. Die aktuelle Bedrohungslage und die Häufung von Angriffen auf Behörden, die Bevölkerung und die Wirtschaft machen Cybersicherheit zu einem Schlüsselfaktor der Digitalisierung..

Informationssicherheit und Datenschutz konnten dank Schwerpunkt-Themen wie Firewall, Netzwerkgrundsätze, Applikationsrollen und Zugriffsberechtigungs-Steuerungen über Jahrzehnte rein technisch durch IT Fachbereiche gesteuert werden. Eine rein technische Sicht auf die Informationssicherheit deckt die Anforderung einer digitalen Bereitschaft, der «Cyber Readiness», aber bei weitem nicht mehr ab. Eine Energie-Mangellage, ein Cyber-Angriff oder eine Ausspähung können nicht nur digitale Verfügbarkeit betreffen. Nein, solche Ereignisse können auch den Auftrag und die Werterbringung einzelner Unternehmen – oder gar gesamte Industrien massiv beeinträchtigen. Dies erfordert eine ganzheitliche Sicht auf organisatorische sowie technische Abhängigkeiten zur Steuerung und der Bereitschaft gegenüber den aktuellen Anforderungen einer Cyber Readiness.

Mit der Cyber Readiness Studie 2022/23 von Eraneos wurden Führungskräfte und Cyber Experten der Wirtschaft, Forschung und Behörden zur unternehmerischen Maturität und der Cyber Readiness befragt.

Erkenntnisse und Schlüsse

Gegenüber der Studie Cyber Security – Resilienz 2020 sind die Angaben aus technischer Sicht bezüglich Bedrohung und verwendeten Technologien und Massahmen wenig verändert.

Die Studie Cyber Readiness 2022/23 zeigt jedoch deutliche Unterschiede bei der geforderten unternehmerischen Cyber Maturität aus.

Ein deutlicher und sehr hoher Handlungsbedarf besteht im Bereich einer integralen Betrachtung der Cyber Readiness von Behörden und systemrelevanten Unternehmen, damit die Auftragserfüllung in allen Lagen gewährleistet werden kann.

Die heutige, generisch gewachsene, Informations-Technologie Landschaft - mit ihren zahlreichen und unterschiedlichen Applikationen, Systemen und Schnittstellen - prägt auch die betrieblichen Kulturen. Damit einhergehend verständlicherweise auch den Umgang mit der Informationssicherheit und deren Organisationsformen.

Trotz Standards und Normen wie «NIST», «BSI» oder «ISO» oder Governance Standard Frameworks wie «Cobit-19» und «ISMS Richtlinien», Richtlinien und Projektmethoden wie «HERMES» ist die Erfüllung der europäischen und schweizerischen Gesetzgebung bei den wenigsten der Befragten sichergestellt. Darunter fallen auch das totalrevidierte DSG, die neue Datenschutzverordnung (DSV) und die neue Verordnung über Datenschutzzertifizierungen (VDSZ), die alle am 1. September 2023 in Kraft treten.

Die Umsetzung zur Einhaltung mittels einer steuerbaren Informationssicherheit durch Risiko-Eigner zur Gewährleistung der Cyber Resilienz erfordert insbesondere durch zunehmende hybride Systemlandschaften der eigenen Informationsverarbeitung mit Cloud Lösungen und der zunehmenden Verschmelzung der Informationstechnologie «IT» mit Operationellen Technologien «OT» erfordern zwingend Bereichsübergreifende Gesamtkonzepte der Geschäftsarchitekturen.

Der Handlungsbedarf ist beträchtlich und fordert Behörden, Wirtschaft und Anbieter von Services und Lösungen zu einem Umdenken, hin zu einer echten und realistischen Cyber Readiness.

Gliederung

Die Frage nach den Top Cyber-Security-Themen (vgl. Seite 11) zeigt den grossen Handlungsbedarf im Umgang mit Sicherheit bei hybriden Architekturen. Unter Berücksichtigung zahlreicher Abhängigkeiten im gesamten Ökosystemen, in welchem heutige isolierte ISMS Formen unzureichend sind, ist der Handlungsbedarf bei IT- und Cyber-Sicherheit nachvollziehbar.

Auf Seite 13 werden Rückmeldungen zu fehlenden Ressourcen und Kompetenzen gezeigt. Diese lassen eine deutlich mangelnde Gesamtübersicht als eine der grössten organisatorischen Herausforderungen erkennen. In Vertiefungsinterviews wurde noch transparenter, dass es an übergreifenden Abstimmungen, Klarheiten von Abhängigkeiten und der Zusammenarbeit mangelt, damit Cyber Readiness zur Realität wird.

Kontinuitäts-, Notfall- und Wiederaufbaupläne sind nicht übergreifend oder nur rein technisch vorhanden, aber selten mit den Fachbereichen und mit systemrelevanten Abhängigen abgestimmt.

Zusammenfassend wird auf Seite 23 darauf hingewiesen, dass das Engagement des Topmanagements mit einer gesamteinheitlich und Bereichs-Übergreifenden Cyber Readiness gelebt werden muss.

Contents

Die unternehmerische Maturität und die Steuerbarkeit der Digitalisierung sicherstellen

Die fortschreitende Digitalisierung von Geschäftsprozessen erfordert eine harmonisierte und übergreifend abgestimmte Cybersicherheit, die es ermöglicht, den Informations- und Datenschutz jederzeit situationsgerecht zu definieren und auf allen Organisationsebenen wirkungsvoll zu steuern.

Dies setzt eine unternehmerische Maturität im Management der Cyber Sicherheit voraus, die organisationsübergreifend orchestriert und über sämtliche Hierarchieebenen abgestimmt ist. Cyber-Readiness definieren wir als Organisationsform, die Risiken präventiv und effektiv erkentnt und diese durch wirkungsvolle, mit den Stakeholdern des Ökosystems koordinierte Massnahmen vermindert. Entsprechend aufgestellte Unternehmen und Verwaltungen analysieren die Bedrohungslage und die Wirkung ihrer Massnahmen kontinuierlich und verbessern diese in einem kontinuierlichen Lernprozess. Sie verfügen über ein durchgängiges Messsystem, um die erzielten Fortschritte intern und durch externe Audits zu bewerten. Informationssicherheit und Datenschutz bilden einen integrierten Bestandteil bei der Digitalisierung ihrer Prozesse.

Die Studienteilnehmenden

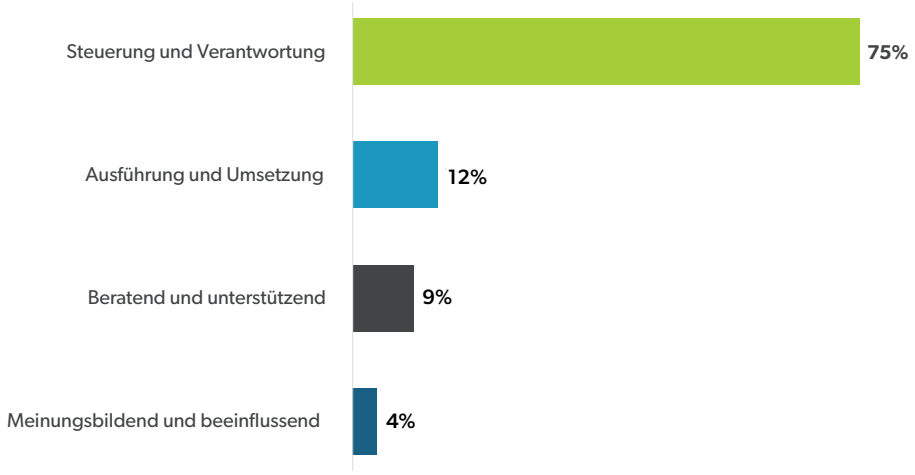


Abb. 1: Funktionsbezogene Aufteilung der Studienteilnehmenden

Die nachstehend erläuterten Ergebnisse basieren auf der Auswertung der Antworten der befragten Unternehmen und öffentlichen Verwaltungen aus der Schweiz. Erfreulich ist, dass mit einem Anteil von 75 % drei Viertel der Antworten durch die Sicherheits-Steuerungsverantwortlichen erfolgten.

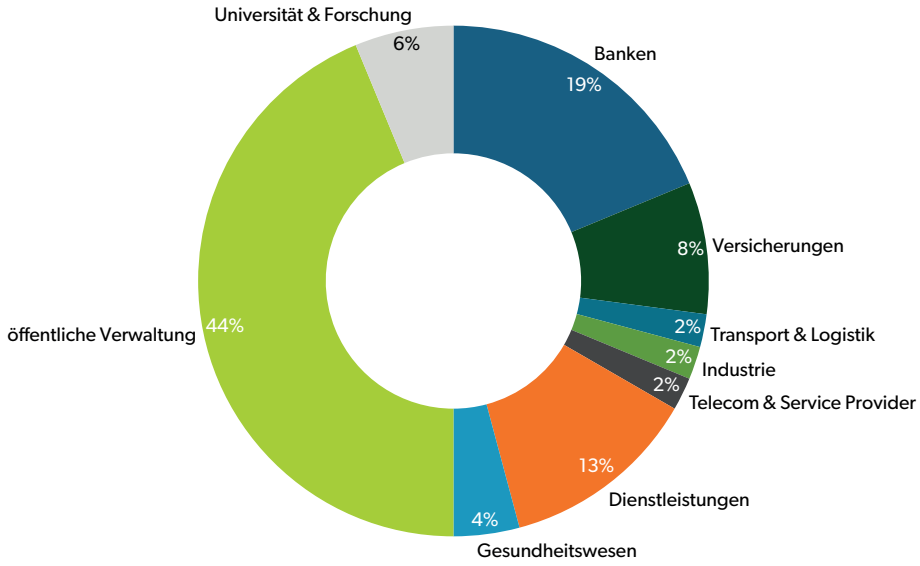


Abb. 2: Branchenbezogene Verteilung der Studienteilnehmenden

Befragt wurden wichtige Player am Markt, darunter neben Grossunternehmen und mittelständische Betrieben insbesondere auch die öffentliche Hand, die 42 % der Studienteilnehmenden ausmachte. Bei den Unternehmen stammen 17 % der Befragten aus dem Bankensektor, gefolgt von den Dienstleistern mit 11 % und der Versicherungsindustrie mit 10 %.

> **"Das Nationale Kompetenzzentrum des Bundes für Cybersicherheit (NCSC) verfolgt den Cyber-Readiness-Ansatz als Chance. Zum Thema Cyber Sicherheit stehen wir in einem kontinuierlichen Dialog mit der Öffentlichkeit. Ein proaktiver Umgang mit dem Thema Cyber Sicherheit fördert das Vertrauen der Bevölkerung in die Sicherheit der Bundesverwaltung."**
>
> **Interviewpartner*in**
> **Bundesverwaltung**

Kapitel

Ergebnisse und Erkenntnisse der Studie

Themenblock 1: Aktueller Status der Cyber-Readiness

Ein solides Management der Cyber-Readiness umfasst massgeschneiderte, proaktive Präventionsmassnahmen, die den Ruf, den Betrieb und die finanzielle Leistungsfähigkeit eines Unternehmens wirkungsvoll schützen.

Jede Organisation ist heute anfällig für Risiken im Bereich der Cybersicherheit und sollte proaktive Massnahmen ergreifen, um Bedrohungen zu entschärfen, bevor sie zu erfolgreichen Angriffen werden.

Inwiefern wird Cyber Security als kritischer Erfolgsfaktor erachtet?

Obwohl Cyber Security heute in den Führungsetagen zum grössten Teil als unverzichtbar erachtet wird, herrscht nach wie vor eine gewisse Ratlosigkeit, wie den zunehmenden Cyberbedrohungen zu begegnen ist und welche Investitionen am schnellsten und effektivsten greifen. Konkret erachteten in dieser Studie 78 % der Befragten Cyber Security als kritischen Erfolgsfaktor. Dies entspricht einer Steigerung von 8,43 % gegenüber unserer Befragung im Jahr 2020.

Der Aufbau und die Umsetzung einer wirksamen, unternehmensweit greifenden Cyber-Readiness ist für die Mehrzahl der Befragten auch weiterhin eine grosse Herausforderung. Ein etabliertes Informations-Sicherheits-Management-System ist vielerorts immer noch nicht in der Organisation verankert und auf allen Ebenen umgesetzt.

Wer sind die Eigner der Cyberrisiken?

Bei zwei Drittel der Befragten sind der Verwaltungsrat (19 %) resp. die Geschäftsleitung (47 %) die Eigner der Cyberrisiken. Demgegenüber wird die Steuerung der Cyberrisiken aber immer noch bei mehr als einem Viertel der Studienteilnehmenden der Informatik oder einzelnen Fachbereichen zugeordnet.

Da Cyberrisiken heute als grösste Bedrohung für Unternehmen eingestuft werden und einen wesentlichen Anteil der Geschäftsrisiken darstellen, sollten diese jedoch nicht mehr ausschliesslich an die IT delegiert werden. Sie gehören vielmehr zwingend auf die Agenda der Unternehmensführung. Unsere Befragung hat ergeben, dass viele Unternehmen davon noch weit entfernt sind, da Cyber-Readiness nach wie vor nicht einheitlich betrachtet, sondern als rein technische Herausforderung verstanden wird.

Wo ist der Chief Information Security Officer (CISO) organisatorisch eingebettet?

Um sicherzustellen, dass der CISO bei der Wahrnehmung seiner Aufgaben alle Aspekte des Unternehmens berücksichtigen kann und hierzu die nötige Durchsetzungskraft hat, ist es wichtig, dass er frei von Interessenkonflikten an die Geschäftsleitung berichten kann. Eine Einbettung des CISO in die IT kann Interessenkonflikte mit dem CIO oder eine Beschränkung des Fokus auf die Systemsicherheit zur Folge haben.

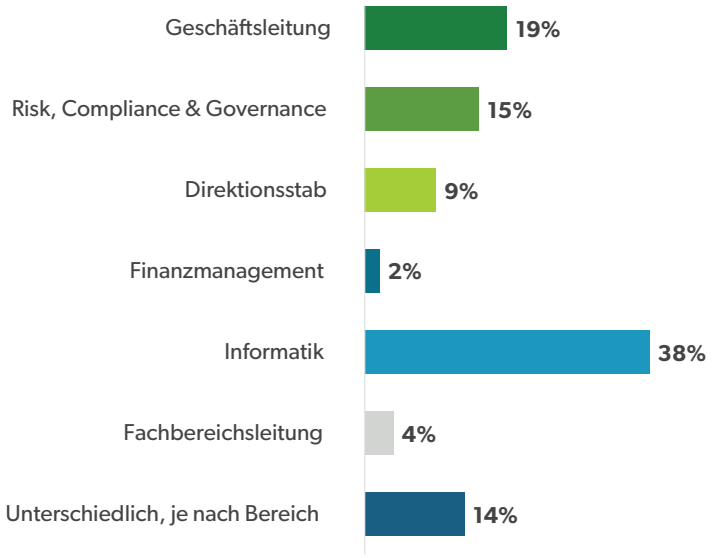


Abb. 3: Einbettung des CISO in der Organisation

Im Rahmen unserer Studie gaben 19 % der Befragten an, dass der CISO organisatorisch in die Geschäftsleitung eingebettet ist. Bei mehr als einem Drittel (38 %) der Studienteilnehmenden ist der CISO in der Informatik angesiedelt. Dies beobachteten wir insbesondere im öffentlichen Sektor.

Was sind die relevantesten Cyberrisiken und -bedrohungen?

Die Verteilung der Relevanz der Cyberbedrohungen hat sich technisch gesehen seit der letzten Befragung im Jahr 2020 wenig verändert. Ransomware bleibt das meistgenannte Cyberrisiko. Erfolgreich durchgeführte Angriffe können Imageschäden und finanziellen Einbussen verursachen sowie gegebenenfalls sogar rechtliche und regulatorische Konsequenzen haben.

Absichtliche oder versehentliche Insider-Bedrohungen machen heute gemäss WEF Global Risk Report 2022 (vgl. Seite 52) 43 % aller Sicherheitsverletzungen aus. Einige Unternehmen reagieren mit einer stärkeren Segmentierung digitaler Systeme, um solche Risiken besser zu berücksichtigen. Massnahmen zur Eindämmung der Risiken sollen so ausgestaltet werden, dass sie sich nicht negativ auf die Effizienz der Mitarbeitenden auswirken.

Akuter Handlungsbedarf besteht im Hinblick auf die Erfüllung gesetzlicher Regelungen, auch beim Datenschutz. Compliance ist heute ein Muss für jedes Unternehmen, um die Gefahr von Rechtsverfahren oder Strafzahlungen wirkungsvoll einzudämmen.

„Unser Unternehmen bewertet alle Risiken auf Basis von einheitlichen Messmethoden. Zudem existiert zur Förderung einer einheitlich steuerbaren Cyber-Readiness eine Gesamtrisiko-Map, die es ermöglicht, die definierten Schwerpunkte strategisch anzugehen."

Interviewpartner*in
Nationales Logistikunternehmen

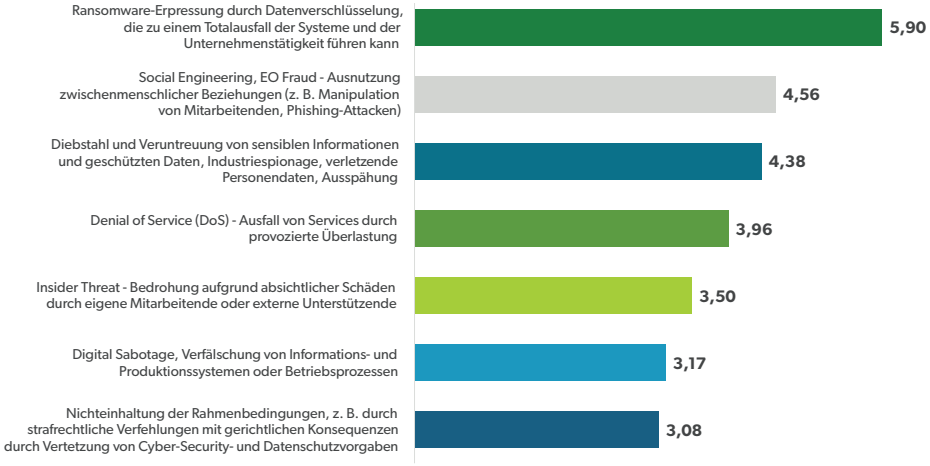


Abb. 4: Relevanteste Cyberrisiken und -bedrohungen (Skala 1-10)

Welches sind die Top-Cyber-Security-Themen?

Gesamthaft betrachtet erachteten in dieser Studie 74 % der Befragten Cloud Security als Security Thema Nummer 1. Dies sind ganze 16 % mehr als in der Umfrage, die wir 2020 durchgeführt haben. Besonders für die Industrien und die Finanzdienstleister ist die Gewährleistung sicherer Cloud-Anwendungen das meistgenannte Thema zur Gewährleistung der Informationssicherheit. Zu den weiteren Top-Cyber-Security Themen gehören mit 66 % (gegenüber 46 % in 2020) die Verhinderung des Abflusses von sensitiven Informationen und schützenswerten Daten sowie die organisatorische Cyber-Maturität, also die effiziente und wirkungsvolle Steuerung der Informationssicherheit innerhalb der Organisation und des dazugehörenden Ökosystems.

Erstaunliche Entwicklungen zeigen sich auch bei der sicheren Nutzung von mobilen Endgeräten. Diese war 2020 noch für 63 % der Befragten ein Top-Thema, während dieses Jahr nur noch 30 % der Studienteilnehmenden das Thema als hohe Priorität einstuften. Stark nach hinten gerückt ist zudem die

IoT-Sicherheit, die 2020 für 45 % der Befragten grosse Bedeutung hatte, während die Sicherheit der eigenen digital vernetzten Produkte in der aktuellen Studie lediglich bei 14 % der Teilnehmenden zu den Top-Themen gehört.

Wie bereits aus unserer Cyber-Resilienz-Studie 2020 hervorging, spielen mobile Endgeräte primär im Gesundheitswesen, in der Mobilität und in der Logistik eine zentrale Rolle. Cloud Services, Sicherheitsmassnahmen, Angriffserkennung und Datenschutz haben hingegen vor allem in stark exponierte Branchen und bei Betreibern kritischer Infrastrukturen wie Banken und Dienstleistungsunternehmen grosse Bedeutung, während IoT-Sicherheit in erster Linie für die Industrie und die Energieversorger wichtig ist.

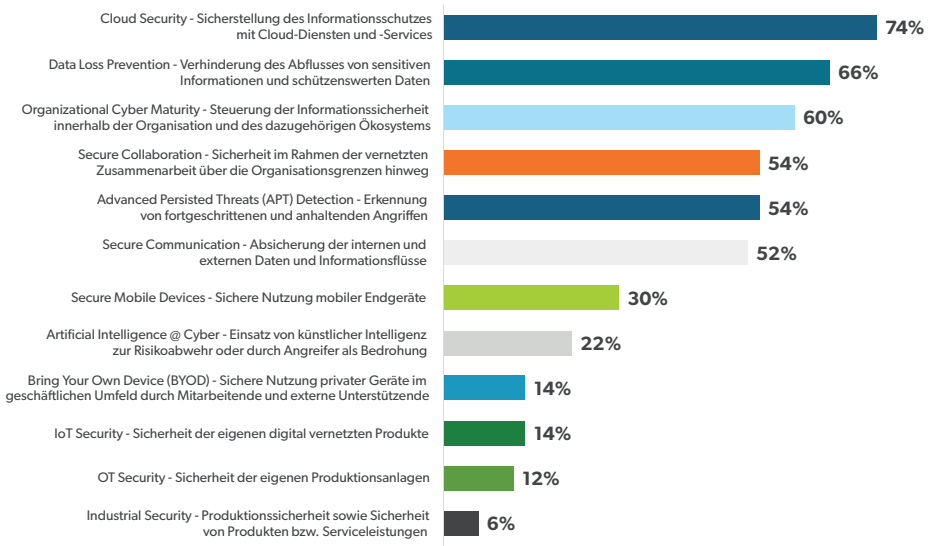


Abb. 5: Top-Cyber-Security-Themen (Mehrfachnennungen möglich)

Themenblock 2: Cyber Resilienz

ISO 22316 definiert Resilienz als die «Fähigkeit, sich einem wandelnden Umfeld anzupassen. Resilientere Organisationen können Risiken und Chancen – aufgrund von plötzlichen oder allmählichen Veränderungen im internen und externen Kontext – antizipieren und darauf reagieren.

Was sind die grössten Herausforderungen bei der Umsetzung der Resilience-Strategie?

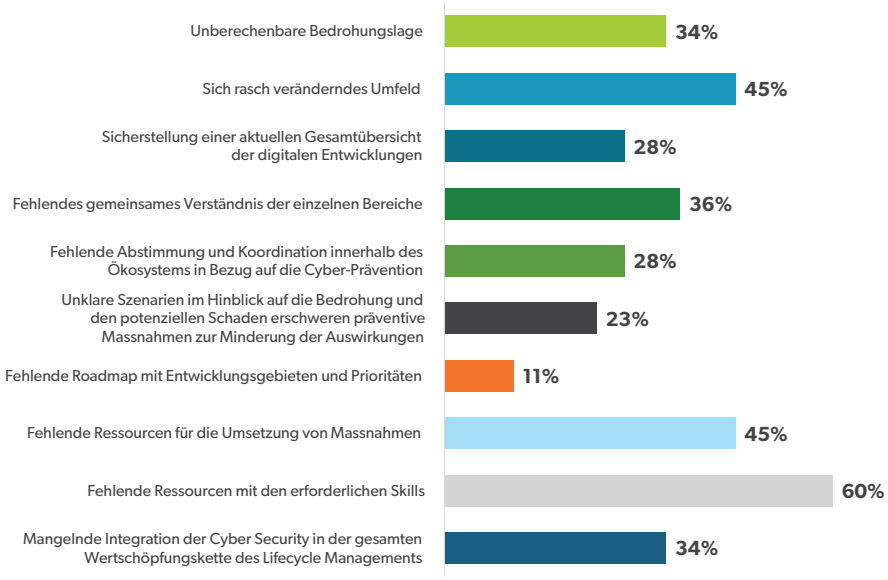


Abb. 6: Herausforderungen Umsetzung Resilience-Strategie (Mehrfachnennungen möglich)

Die Fähigkeit, in einem Umfeld, das sich kontinuierlich verändert, auf unberechenbare Bedrohungslagen und Risiken zu reagieren, gehört für die Studienteilnehmenden zu den grössten Herausforderungen. Neben einer effektiven Cyber-Governance fehlt es hierzu nicht nur an Ressourcen mit den erforderlichen Skills, sondern auch an Ressourcen für die Umsetzung der definierten Massnahmen. In der Praxis gibt es häufig grosse Diskrepanzen zwischen der Anforderung des Business und den verfügbaren Ressourcen mit dem entsprechenden Know-how und der nötigen Erfahrung.

Der vorherrschende Mangel an qualifizierten IT- und Cybersicherheitsexpert*innen, die eine Führungsrolle im Cyberbereich übernehmen, Systeme testen und sichern sowie Menschen in digitaler Hygiene schulen können ist gravierend. Der Fachkräftemangel ist einer der Treiber welche den Trend hin zu Outsourcing und Automatisierung von Cyber Security Tätigkeiten unterstützen.

Gesamthaft betrachtet hat sich hier gegenüber unserer Cyber Resilienz Studie 2020 wenig verändert.

Welchen Stellenwert hat Cyber Resilience bei den befragten Organisationen?

Immerhin etwas mehr als die Hälfte (54 %) der Befragten stufen Cyber Resilience als unternehmenskritisch ein, damit bei einem Angriff nicht die gesamte Organisation betroffen ist und der Auftrag sowie die Geschäftstätigkeit weitergeführt werden können. 23 % der Studienteilnehmer gaben zudem an, dass Cyber Resilience über das gesamte Ökosystem gewährleistet sein müsse. In der Praxis haben dies aber nur 2 % der Befragten umgesetzt. Erstaunt hat uns zudem, dass lediglich 10 % angaben, dass Cyber Resilience Teil der Digitalisierungsstrategie und in der Organisation fest verankert ist.

Sehr überrascht hat uns die Aussage von 7 % der Befragten, dass Cyber Resilience eine vernachlässigbare Anforderung sei und das Thema eine untergeordnete Rolle spiele. Dies umso mehr, als im Rahmen unserer Umfrage vor zwei Jahren keiner der Teilnehmenden angab, dass Cyber Resilience noch nicht im Fokus stehe.

Insbesondere für systemkritische Behörden und Unternehmen wie Versorger und Spitäler ist der Handlungsbedarf sehr hoch, wenn es darum geht, eine koordinierte organisatorische und technisch abgestimmte Cyber-Readiness in allen Lagen sicherzustellen und auf Cyber-Angriffe vorbereitet zu sein.

Werden Vorfälle in der eigenen Organisation beobachtet, um daraus Massnahmen zur Erhöhung der Cyber Resilience abzuleiten und umzusetzen?

62 % der Befragen gaben an, dass aufgrund von konkreten Ereignissen bereits Massnahmen zur Erhöhung der Cyber Resilience definiert und umgesetzt worden sind, während etwas mehr als die Hälfte entsprechende Vorfälle analysiert und in der Geschäftsleitung bespricht, um daraus organisatorische und technische Massnahmen abzuleiten. Erstaunlich ist, dass rund 15 % der Studienteilnehmenden nach wie vor kein Cyber Resilience Management betreiben und diesbezüglich keinen Handlungsbedarf sehen.

Grundsätzlich haben wir bei der Auswertung der Studienergebnisse festgestellt, dass regulierte Industrien und Behörden eher Prozesse und Abläufe installiert haben, um zeitnah auf Ereignisse reagieren zu können und aus Vorfällen lernen zu können. Dies macht solche Organisationen im Vergleich resilienter.

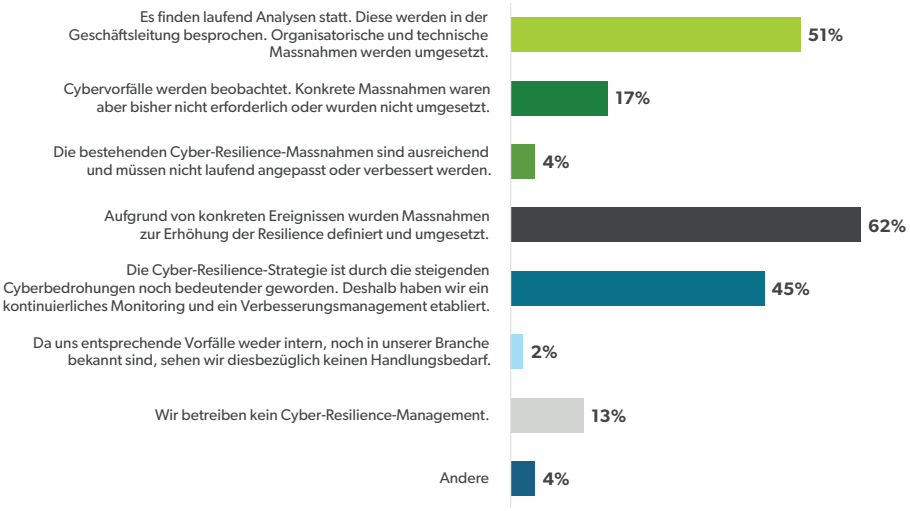


Abb. 7: Massnahmen zur Erhöhung der Cyber Resilienz (Mehrfachnennungen möglich)

Da sich der Eintritt eines Cyberereignisses kaum mehr verhindern lässt, wird die rasche Erholungsfähigkeit zu einem kritischen Erfolgsfaktor. Existieren Kontinuitäts- und Wiederanlaufpläne zur Aufrechterhaltung kritischer Geschäftsprozesse im Ernstfall?

Cybervorfälle können den Betrieb stören, unterbrechen oder vollständig lahmlegen. Dies kann zu markanten Umsatzeinbussen oder in extremen Fällen zur vollständigen Schliessung eines Unternehmens führen. Mit einem Business Continuity Plan (BCP) steigt die Wahrscheinlichkeit um ein Vielfaches, dass sich die Organisation nach einem Cyberereignis schnell wieder erholt. Da der Eintritt eines Cyber-Ereignisses je länger je weniger verhindert werden kann, wird die rasche Erholungsfähigkeit immer mehr zu einem kritischen Erfolgsfaktor. Ein Plan zur Sicherstellung der Business Continuity sollte daher im Rahmen eines sinnvollen Risk Managements zur Grundausstattung gehören.

> "Die kritischen Prozess müssen definiert werden. BCM spielt dabei eine entscheidende Rolle und muss je nach Lage auf die systemrelevanten Aufträge reduziert werden können. Wichtig ist zudem, BCM-Massnahmen über alle Departemente hinweg integral zu betrachtetn und einheitlich zu festzulegen."
>
> **Interviewpartner*in**
> **Kanton**

Im Rahmen unserer Studie gaben 28 % der Befragten an, dass entsprechende Kontinuitäts- und Wiederanlaufpläne definiert sind sowie regelmässig überprüft und trainiert werden. Die Kontinuitätsanforderungen für kritische Geschäftsprozesse sind bei 89 % der Studienteilnehmenden zwar definiert. Trotzdem verzichten nach wie vor 11 % (gegenüber 12 % in 2020) auf eine regelmässige Überprüfung. Auch gaben immer noch 22 % (gegenüber 27 % in 2020) der Befragten an, dass sie im Ereignisfall ad hoc handeln.

Am meisten erstaunt hat uns bei dieser Frage, dass satte 11 % der Befragten nicht wissen, ob entsprechende Vorbereitungsmassnahmen in ihrer Organisation getroffen wurden. Im Jahr 2020 gaben lediglich 3 % der Umfrageteilnehmenden an, dass ihnen etwaige Kontinuitäts- und Wiederanlaufpläne nicht bekannt seien.

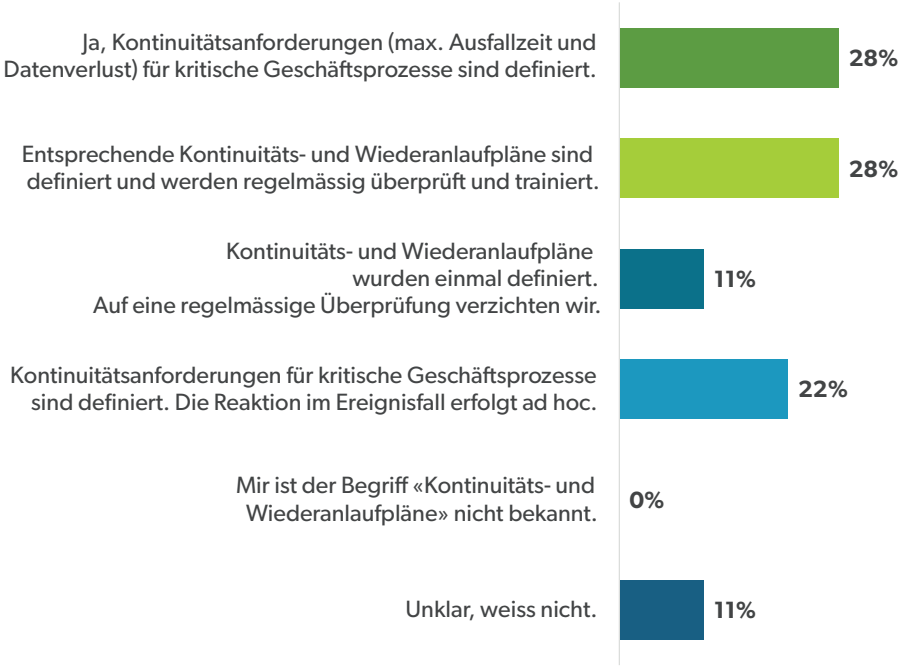


Abb. 8: Vorbereitungsstand Business Continuity

Annahme: Sie wurden angegriffen. Wie reagiert Ihr Unternehmen?

Bei 25 % der Befragten ist die Geschäftsleitung informiert und steuert die Massnahmen mit den internen Verantwortlichen und den Service Providern. 11 % haben Massnahmen zur Eindämmung eines möglichen Schadens aufgrund eines Vorfalls definiert und in Szenarien festgehalten, die auf Basis des entwickelten Notfallkonzepts umgesetzt werden können. Demgegenüber verfügen aber lediglich 2 % der Studienteilnehmenden über ein klares Kommunikationskonzept für das gesamte Ökosystem, das durch die Geschäftsleitung ausgeführt wird, während bei 13 % zurzeit noch gar keine Szenarien für einen überraschenden Angriff existieren.

Grundsätzlich zeigt sich damit, dass eine übergreifende Steuerung der Cybersicherheit in Ökosystemen und in grösseren Unternehmen vielerorts (noch) nicht umgesetzt ist.

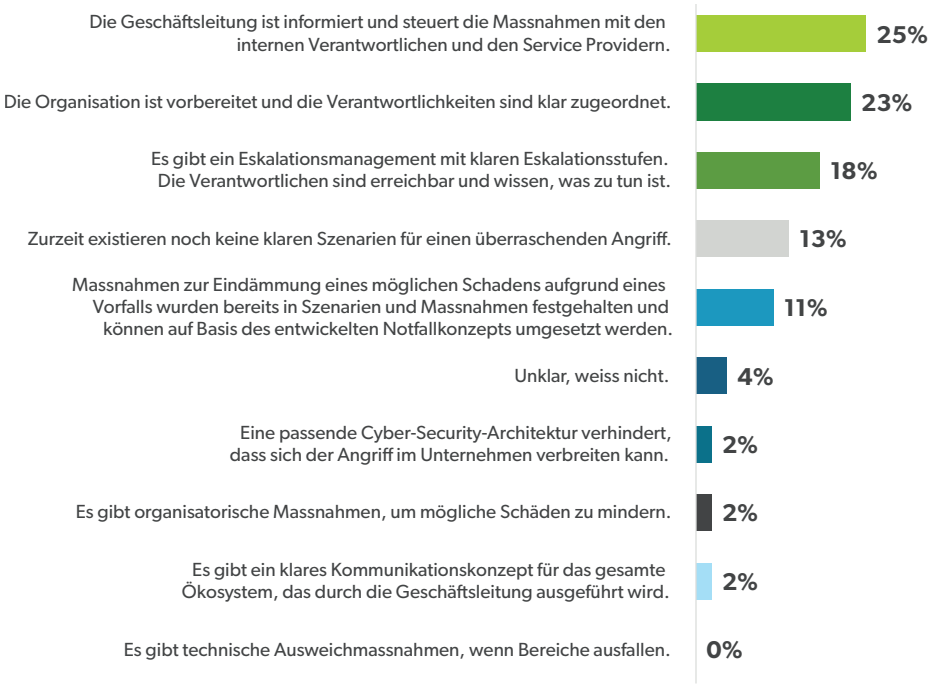


Abb. 9: Reaktionsbereitschaft im Ernstfall

Themenblock 3: Cyber Governance

Eine wirksame Governance der Cybersicherheit fokussiert auf das Risikomanagement und das Sicherheitsbewusstsein, um den Umfang der Risikolandschaft zu verringern. Sie hilft der Organisation, ihre Risikobereitschaft zu definieren und die Aktivitäten zur Risikominderung zu überwachen. Ein starkes Governance-Programm schafft auch einen Rahmen für die Rechenschaftspflicht und legt fest, wer für die Entscheidungen zur Gewährleistung der Risikominderung verantwortlich ist.

Welcher Anteil des IT-Budgets zur Digitalisierung wird für die Cyber Security verwendet?

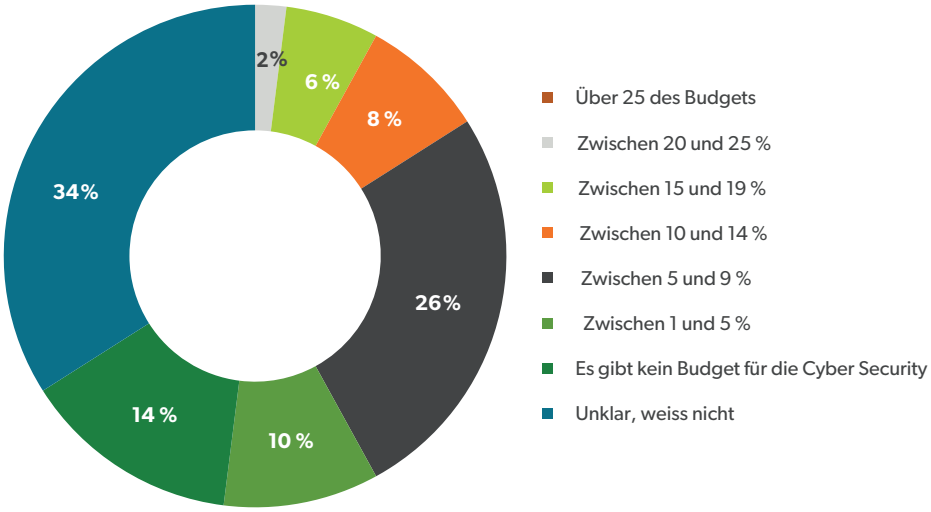


Abb. 10: Verfügbares Budget für die Cyber Security

34 % der Studienteilnehmenden ist das Budget für die Cybersicherheit nicht bekannt, während 14 % angaben, dass ein entsprechendes Budget nicht existiert.

Bei etwas mehr als einem Viertel der befragten Unternehmen werden fünf bis neun Prozent der IT-Ausgaben für die Cybersicherheit verwendet. Lediglich 2 % verwenden dafür zwischen 20 und 25 Prozent ihres IT-Budgets. Mehr als 25 % des Budget wird in keinem der befragten Unternehmen und keiner Verwaltung für die Cybersicherheit verwendet.

Wer steuert die Cyber Governance im Unternehmen?

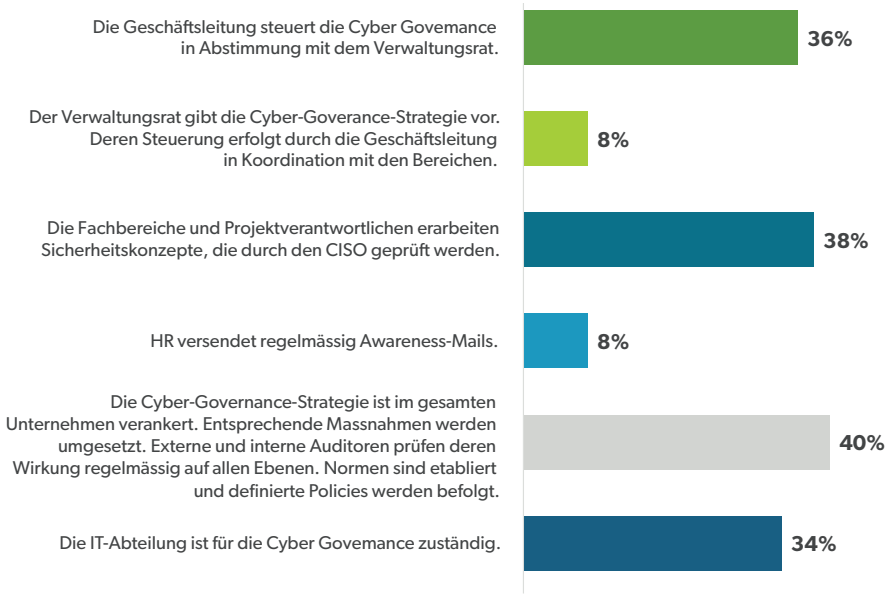


Abb. 11: Verantwortung für die Steuerung der Cyber Governance (Mehrfachnennungen möglich)

Erfolgreiche Cyber Governance erfordert sowohl einen starken Impuls von der Unternehmensspitze als auch eine unternehmensweite Sichtweise. Entsprechend wichtig ist somit, dass die Entscheidungsträger, also der Chief Information Security Officer (CISO), der CEO und der Verwaltungsrat den Ton angeben, wenn es um Entscheidungen geht, welche Massnahmen getroffen und wie diese in der Organisation umgesetzt werden sollen.

Unsere Studie zeigt jedoch, dass eine unternehmensweite Gesamtsteuerung der Cyber Governance durch den Verwaltungsrat und die Geschäftsleitung eine verbreitete Herausforderung darstellt, die viele Organisationen noch nicht gemeistert haben. Erstaunt hat uns insbesondere, dass die Cyber Governance bei mehr als einem Drittel der Befragten immer noch an die IT-Abteilung delegiert wird.

> **"Die Geschäftsleitung schlägt dem Verwaltungsrat die Strategie für das Management der Cyberrisiken vor und verantwortet wie diese umgesetzt werden, während der Verwaltungsrat bestimmt, welche Massnahmen umgesetzt werden sollen."**
>
> **Interviewpartner*in**
> **CISO Versicherungsgruppe**

Wie werden Massnahmen zur Minderung von Cyberrisiken im Unternehmen gesteuert?

Der Glaube, dass die Cyber Readiness mit Hilfe von Sicherheitskonzepten-Konzepten durch Formulare und Dokumente gesteuert werden kann, ist verbreitet. Zudem wird die Wirkung von Massnahmen auch im systemkritischen Umfeld noch zu häufig nicht überprüft.

Erstaunt hat uns vor allem, dass die Cyber Governance für 20 % der Befragten noch kein unternehmerisches Thema ist und ein eigentliches Management von Cyberrisiken bislang nicht etabliert ist. Führend in der Umsetzung entsprechender Massnahmen sind die Banken und die Versicherungen. Da es sich hier um staatlich sehr stark regulierte Branchen handelt, ist dieses dieses Resultat wenig überraschend.

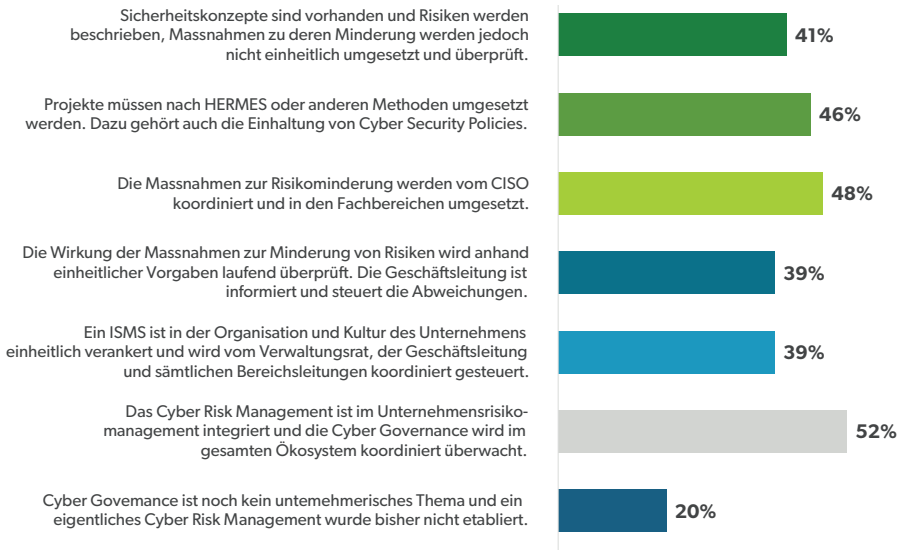


Abb. 12: Massnahmen zur Minderung von Cyberrisiken (Mehrfachnennungen möglich)

Im Cyberumfeld stellt sich je länger je mehr nur noch die Frage, wann ich getroffen werde und nicht mehr, ob ich betroffen sein werde. Welchen Stellenwert hat Cyber Security bei den Teilnehmenden unserer Studie?

Cyber Security ist zwar ein Thema, mit dem sich die Geschäftsleitung seit längerer Zeit intensiv befasst. Der Handlungsdruck für eine effektive Cyber-Readiness in der eigenen Organisation ist aber immer noch tief. Dies zeigt sich insbesondere darin, dass Cyber Security bei 18 % der Befragten erst seit kurzem auf der Agenda steht und bis heute kein Top-Thema ist.

Dass sich bei mehr als einem Drittel (38%) der Studienteilnehmenden namentlich die IT mit dem Thema auseinandersetzt und den Bedarf der IT-Anwenderinnen sowie die Vorgaben der Security Foren koordiniert, bestätigt zudem, dass Cyber Security vielerorts nach wie vor noch nicht als Chefsache traktandiert ist.

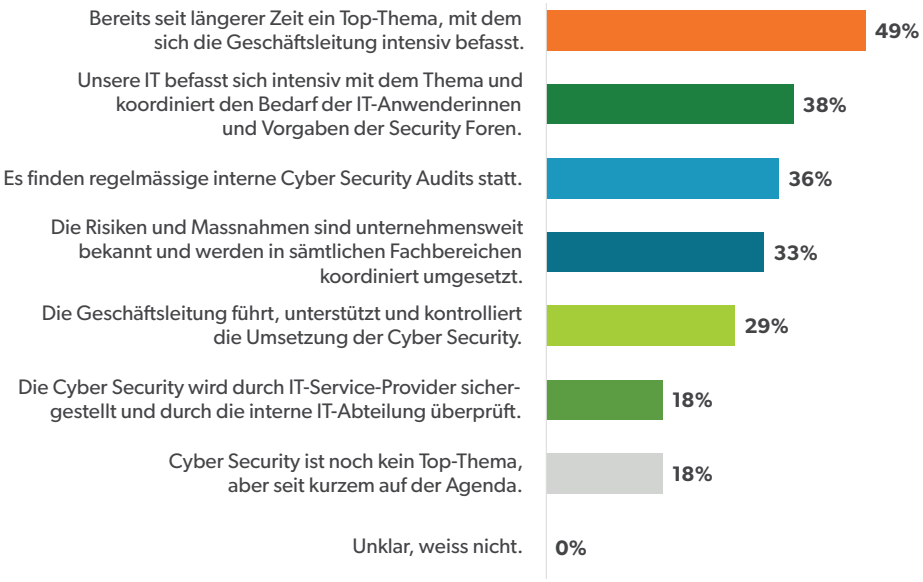


Abb. 13: Stellenwert der Cyber Security in der Organisation (Mehrfachnennungen möglich)

Themenblock 4: Cyber-Security Maturität

Der Grad der Cyber-Maturität einer Organisation hängt massgeblich von unternehmerischen Fähigkeiten und Voraussetzungen ab, die als organisatorische Maturität bezeichnet und gemessen werden. Mit den nachfolgenden Fragen wollen wir die Herausforderungen besser verstehen, mit denen sich Unternehmen auf ihrem Weg zur Steigerung der Cyber-Security Maturität auseinandersetzen müssen.

Die Cyber-Security Maturität unterscheidet in Bezug auf die Organisation folgende Maturitätslevel:

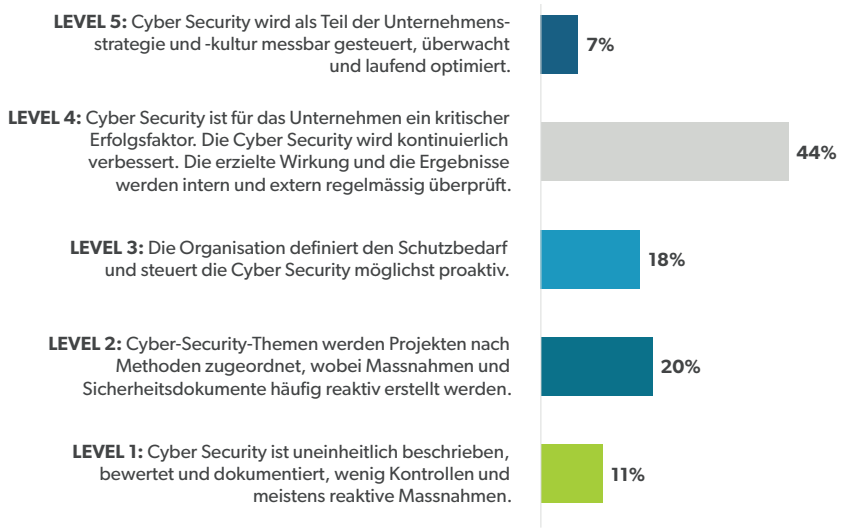


Abb. 14: Selbsteinschätzung Cyber Security Maturität

Ein tiefer Maturitätslevel bezeichnet einen organisatorischen Zustand, in welchem Informationssicherheitsrisiken zwar bekannt sind, jedoch meist keine Massnahmen zur Minderung der Risiken definiert werden oder nicht umgesetzt und kontrolliert werden. Der höchste Maturitätslevel ist erreicht, wenn in der Organisation Massnahmen messbar und zugeordnet umgesetzt werden, dies laufend gelebt und kontrolliert wird und sich die Organisation stetig lernend verbessert.

Sogenannte «intelligente Unternehmen» basieren auf einem Maturitätslevel 5. Sie sind oft resilienter und agiler gegenüber Veränderungen und Bedrohungen. Zugleich sind sie meistens auch kompetitiver und erfolgreicher in ihrem Markt tätig und können ihren Auftrag gegenüber vergleichbaren Organisationen agiler und besser erfüllen.

Mit 31 % bewertete fast ein Drittel der Befragten in unserer Studie den Level ihrer Cyber-Maturität zwischen 1 und 2. Besonders in systemkritischen Unternehmen und Organisationen ist ein Maturitätslevel auf diesen Stufen jedoch ein grosses Klumpenrisiko für die Wirtschaft, die Bevölkerung und das betreffende Land.

Was sind die grössten Hürden, die aus dem Weg geräumt werden müssen, um die Cyber Security in der Organisation erfolgreich voranzutreiben?

Organisationen, welche Risiken präventiv erkennen und bearbeiten und eng mit den Partnern in ihrem Ökosystem zusammenarbeiten zeichnen sich durch eine hohe Cyber Maturität aus. Zentral ist die laufende Weiterentwicklung und Optimierung der definierten Massnahmen sowie eine klare Zuordnung der Verantwortlichkeiten und ein bereichsübergreifendes verbindliches Cybersicherheits-Regelwerk.

Zugleich setzt eine wirkungsvolle Cyber Security Maturiät als kontinuierlicher Prozess voraus, dass sowohl das eigenen digitale Ökosystem wie auch die Ökosysteme der involvierten Drittparteien kontinuierlich überwacht werden. Nur so lässt sich eine akkurate Bewertung der digitalen Widerstandsfähigkeit der eigenen Organisation und die wirkungsvolle Abwehr von Cyberrisiken nachhaltig sicherstellen.

Aufgrund des gravierenden Ressourcenmangels und der zahlreichen weiteren Hürden, die es nach wie vor zu überwinden gilt, liegt eine harmonisierte sowie effektiv gelebte und erprobte Cyber Readiness vielerorts noch in weiter Ferne. Die Hoffnung, dass es nur die anderen trifft, ist immer noch dominant.

> **"Unsere grösste Herausforderung sind zurzeit die steigenden Dimensionen der Cyberbedrohungen, die mit den wenigen zur Verfügung stehenden Ressourcen bewältigt werden müssen."**
>
> **Interviewpartner*in**
> **Stadtwerk**

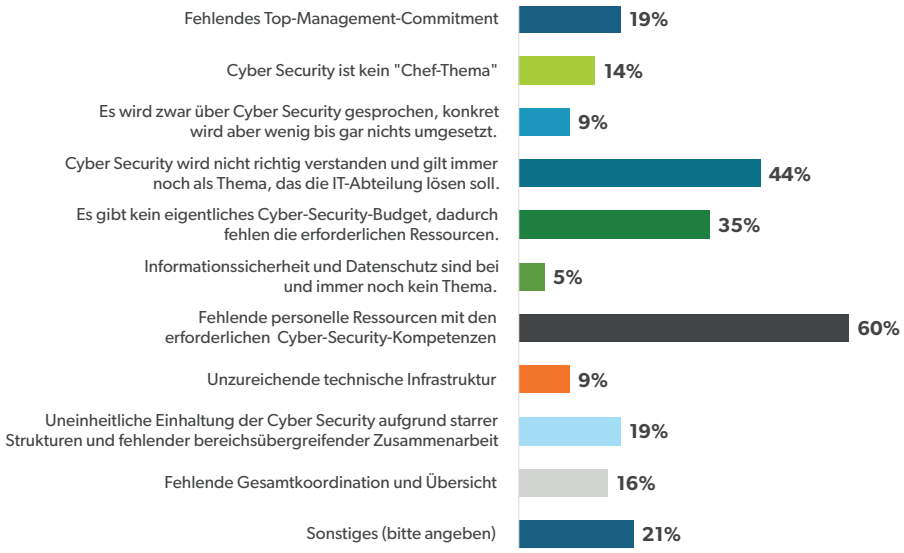
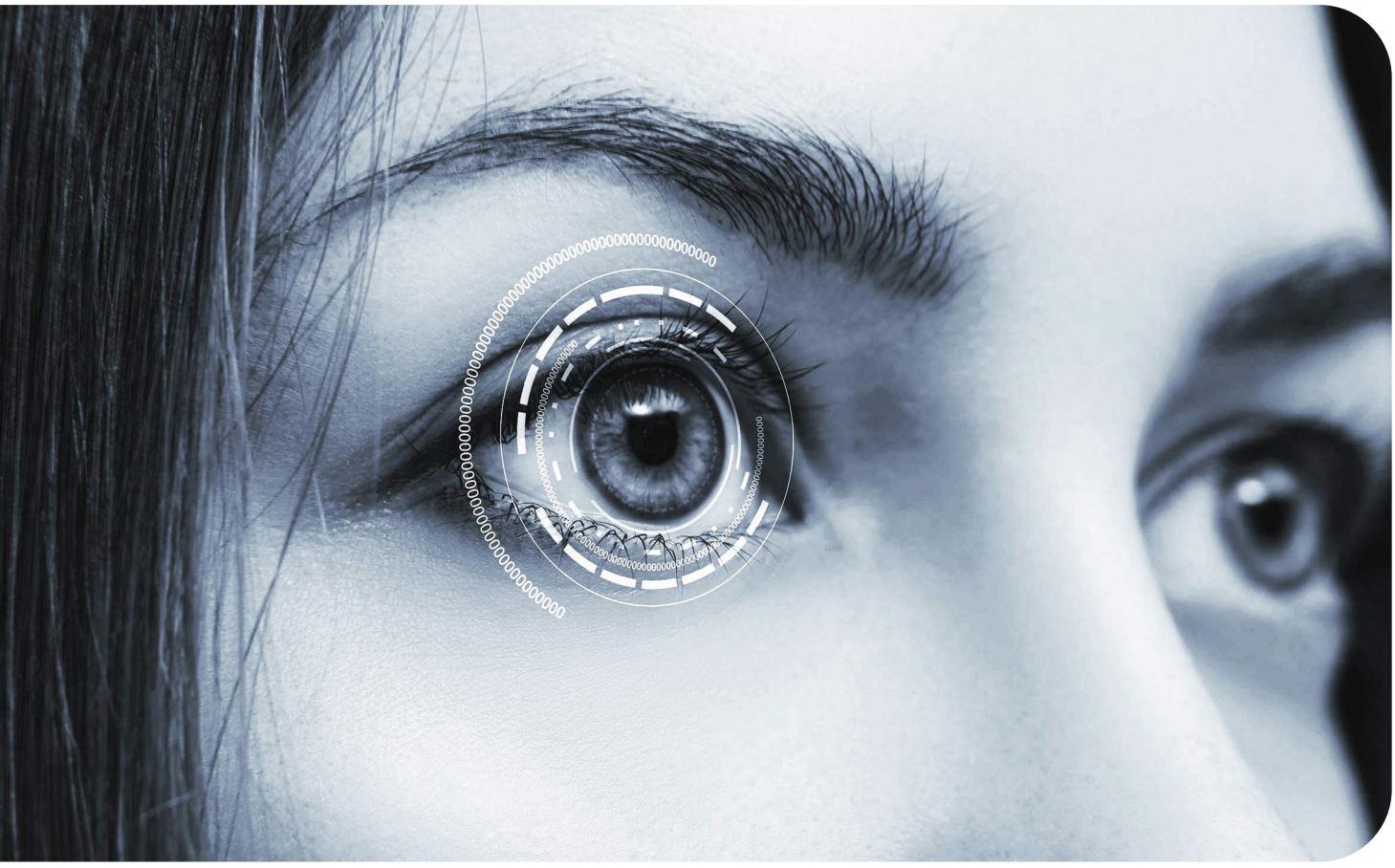
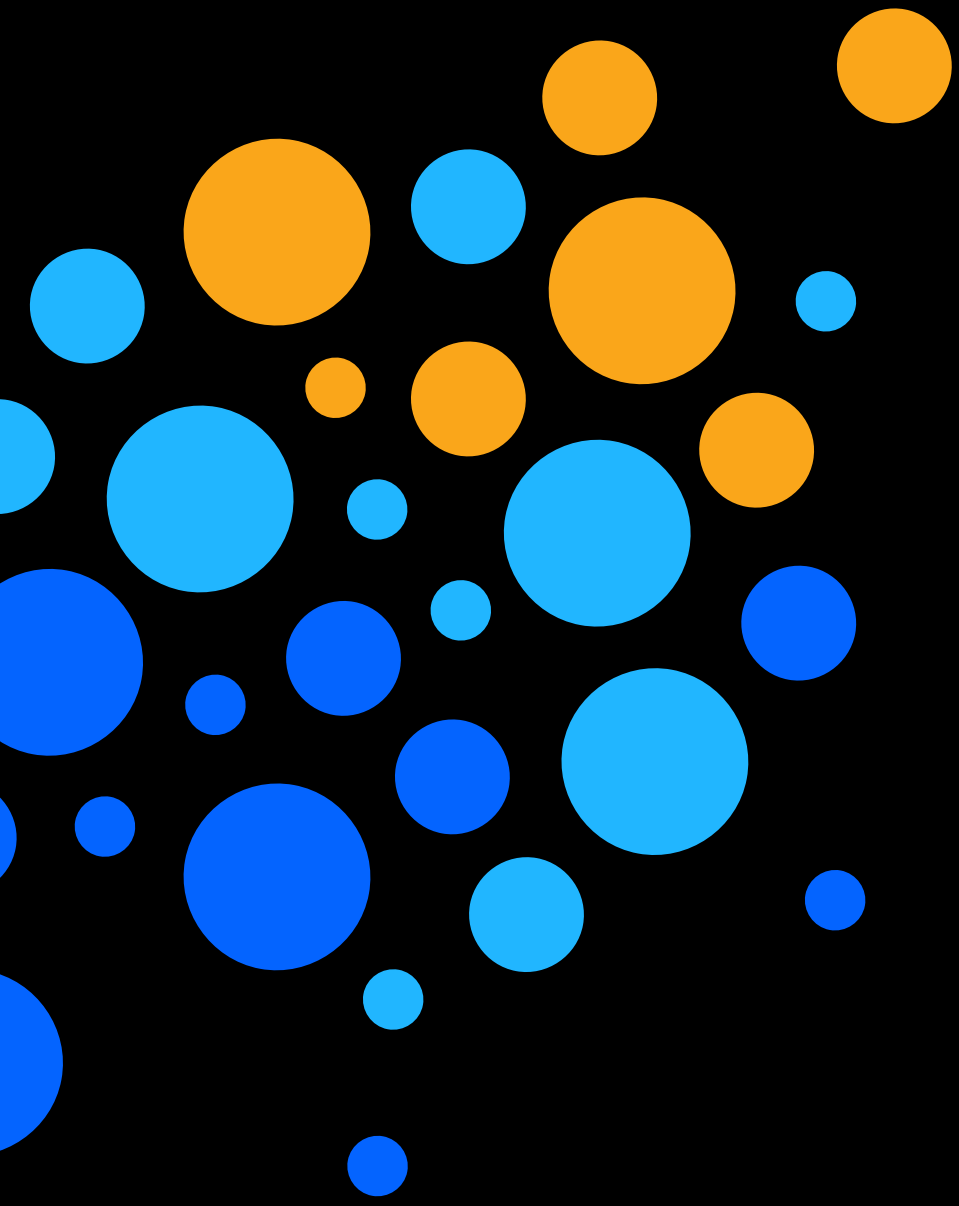


Abb. 15: Hürden für Verbesserung Cyber Security Maturität (Mehrfachnennungen möglich)





eraneos

Experienced in a wide range of industries

Über Eraneos Switzerland AG
Die Eraneos Switzerland AG (vormals AWK Group AG) ist eine internationale Management- & Technologieberatungsgruppe, die Kunden bei der Entwicklung digitaler Geschäftsmodelle und komplexer Transformationsprojekte unterstützt und ihnen hilft, das Potenzial der Digitalisierung voll auszuschöpfen.
Als Teil der international agierenden Eraneos Group, die sich von der Schweiz über Luxemburg, Deutschland, Spanien, die Niederlande, China, Singapur und die USA erstreckt, setzen mehr als 1000 hochqualifizierte Experten ihr Wissen ein.
Die einzigartige Kombination von Kompetenzen in den Bereichen Digital Business & Innovation, Organizational Excellence & Transformation, Data & AI, Cyber Security & Privacy, Sourcing & IT Advisory und Technology & Platforms über alle Industrien ermöglicht es uns, unsere Kunden umfassend zu unterstützen.
An den Schweizer Standorten Zürich, Basel, Bern und Lausanne arbeiten mehr als 550 Mitarbeitende. Eraneos Schweiz (vormals AWK Group AG) wurde wiederholt mit dem "Great Place to Work"-Award ausgezeichnet.

Contact us >

Visit our website >

Join our Company >

---

eraneos.ch