AWK Group
Enabling digital performance.

Cyber-Resilienz:
Den Fortbestand von Unternehmen sicherstellen

Studienergebnisse 2020

AWK Cyber-Resilienz Studie 2020

Management Summary

Das Coronavirus hat uns in den letzten Wochen klar vor Augen geführt, wie wichtig es ist, Cyber-Resilienz zu leben, da man in einer Krise stets nur so gut agieren kann wie man darauf vorbereitet war. Jedes Unternehmen agiert heute in einem Umfeld, das zunehmend geprägt wird von nicht bekannten oder vorhersehbaren Bedrohungen und Gegnern. Entsprechend sind Verwaltungsräte und Führungskräfte von Unternehmen jeder Grösse und Branche mehr denn je gefordert, sich mit Cyberrisiken auseinanderzusetzen und sicherzustellen, dass diese systematisch beobachtet, kommuniziert und bewältigt werden.

Adrian Marti, Partner
Cyber Security & Privacy

Der Cyberspace und die damit einherge henden Risiken haben sich in den letzten Jahren stark verändert. Die fortschreitende Digitalisierung führt in vielen Unternehmen zu einer erhöhten Abhängigkeit von unterschiedlichsten Dienstleistern. Das dadurch entstehende Ökosystem und die damit verbundenen Schwachstellen setzen Unternehmen steigenden systemischen Risiken aus und erhöhen das Risiko einer Cyberattacke massiv. Diese Schwachstellen mithilfe eines oftmals nur reaktiv wirkenden Cyber Security Management allumfassend zu überwachen und zu schliessen, ist ein zum Scheitern verurteiltes Unterfangen. Unternehmen müssen die Bedrohungslage fortlaufend analysieren und eine ganzheitliche Abwehrstrategie entwickeln, welche die fortlaufenden Veränderungen ihrer Organisation, ihrer Infrastruktur und ihres Umfelds berücksichtigt. Denn es stellt sich nicht mehr die Frage, ob das eigene Unternehmen getroffen wird, sondern wann.

Resilienz definiert gemäss ISO 22316 als die Fähigkeit, sich einem wandelnden Umfeld anzupassen und die Auswirkungen eines Cyberangriffs auf den Betrieb des Unternehmens zu minimieren. Die Cybersicherheit ist eine tragende Säule der Resilienz. In einem resilienten Unternehmen wird die Cybersicherheit jedoch in den systemischen Ansatz der Cyber-Resilienz integriert. Resiliente Organisationen sind fähig, Risiken und Chancen durch plötzliche oder allmähliche Veränderungen im internen und externen Kontext zu antizipieren und auf diese angemessen zu reagieren. Bei der Cyber-Resilienz geht es also nicht nur um die Identifikation, das Vorbereiten und das Bewältigen von Notfall- oder Krisenszenarien, sondern auch darum, unter herausfordernden Bedingungen weiterzubestehen und sich an das neue Umfeld anzupassen.

Die Ergebnisse unserer Studie unterstreichen, dass die Wichtigkeit einer hohen Cyber-Resilienz für die Sicherung des Fortbestehens bei den Führungskräften breit anerkannt ist. Als Schlüsselelement für den Aufbau und die Verankerung der Cyber-Resilienz im Unternehmen beurteilen 76% der Befragten einen aktiv agierenden Verwaltungsrat, der die Bereitstellung der hierzu erforderlichen Ressourcen tonangebend unterstützt.

Besonders erstaunt hat uns, dass 70% der befragten Unternehmen Cyber Security nicht nur als eine notwendige Voraussetzung für professionelles Handeln, sondern als Differenzierungsfaktor am Markt erachten. Doch obwohl die Relevanz einer

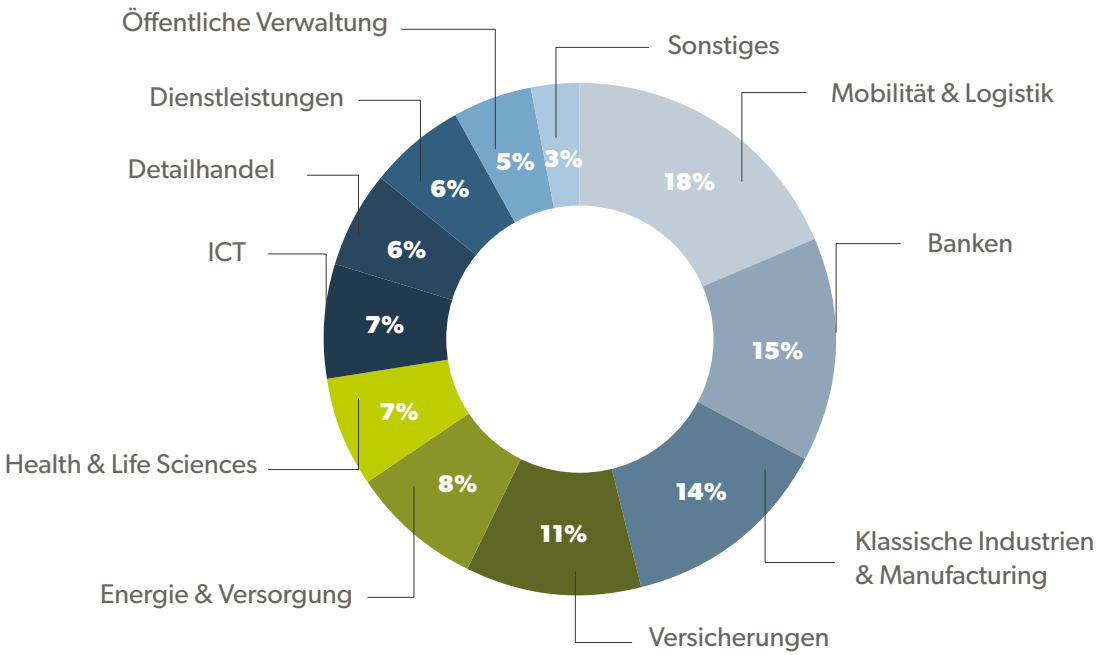
hohen Cyber Security anerkannt und die entsprechenden Budgets in 75% der befragten Unternehmen in den letzten zwei Jahren zum Teil deutlich erhöht wurden, beurteilen lediglich 20% der Teilnehmenden ihren aktuellen Vorbereitungsstand als ausreichend.
Als grösste Hürden zur Verbesserung der Cyber-Resilienz nannten die Teilnehmenden die IT-Architektur und die fehlenden technischen Fähigkeiten für die Umsetzung. Die gute Nachricht ist, dass diese Hürden mit externer Unterstützung und dem entsprechenden internen Engagement überwindbar sind.

AWK empfiehlt Führungskräften, beim Aufbau und Erhalt der Cybersicherheit und -Resilienz einen risikobasierten Ansatz für das Management von Informationsrisiken zu verfolgen. Hierzu müssen sowohl der Risikoappetit des Unternehmens identifiziert als auch die Ownership der Risiken definiert werden. Eigner der Risiken ist typischerweise das Business. Dieses finanziert direkt oder indirekt auch die Massnahmen zur Mitigation der Risiken. Wir empfehlen, die Auswirkungen auf das Business in den Fokus der Risikodiskussion zu stellen. Die Verfahren zur Identifikation, Messung und Bewertung der Risiken sollen nachvollziehbar ausgestaltet werden. Die Ableitung geeigneter Massnahmen wird darauf abgestützt. Zur Nachverfolgung der Massnahmenumsetzung und Überprüfung der damit erzielten Wirkung empfehlen wir ein regelmässiges Reporting.

Verwaltungsräten empfehlen wir, sich als Sparringpartner des Managements zu positionieren und sich aktiv in die Diskussion zum Risikoappetit einzubringen. Wichtig dabei ist, dass sie sich ihrer Vorbildfunktion auch in Bezug auf das Thema Cyber Sicherheit jederzeit bewusst sind.

Die Ergebnisse und Erkenntnisse der Cyber-Resilienz Studie 2020

Aufteilung der Studienteilnehmer nach Branche



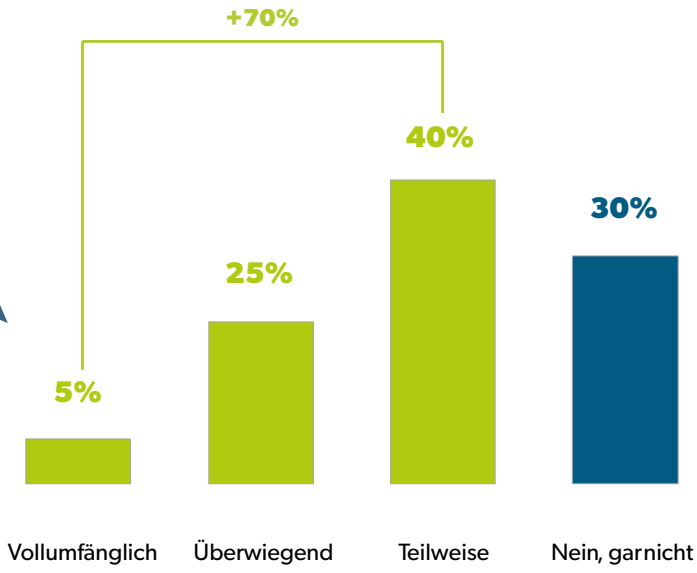
Rund 100 Entscheidungsträger haben an der Umfrage teilgenommen. Befragt wurden wichtige Player am Markt, darunter insbesondere Grossunternehmen und mittelständische Unternehmen, die einen grossen Teil der Schweizer Wirtschaftsleistung erbringen, sowie die öffentliche Hand. 18% der Studienteilnehmer stammen aus den Sektoren Mobilität und Logistik, dicht gefolgt von den Banken, der klassischen und herstellenden Industrie sowie den Versicherungen.

Themenblock Cyber Security

Dieser Themenbereich baut auf einer 2018 durchgeführten Studie mit ähnlichem Inhalt auf.

Erachten Unternehmen Cyber Security als Differenzierungsmerkmal am Markt?

Die Einstufung des Themas als USP ist aus unserer Sicht überraschend hoch.



Seit Jahren steht Cyber-Sicherheit ganz oben auf der Top-Management Agenda. Dies zeigte bereits die 2018 durchgeführte Studie, bei der 87 Prozent der befragten Unternehmen angaben, über eine Cyber-Security-Strategie zu verfügen.

Cyber Security wird in der diesjährigen Studie von 70% der befragten Unternehmen sogar als Differenzierungsmerkmal am Markt wahrgenommen und nicht nur als Voraussetzung für professionelles Handeln.

Dies entspricht einer Steigerung von 7% gegenüber einer Befragung im Jahr 2018. Wir beurteilen dieses Ergebnis als überraschend hoch. Die Einstufung der Relevanz von Cyber Security liegt erwartungsgemäss bei den ICT-Unternehmen (100%) am höchsten, gefolgt von den Banken (92%). Nicht erwartet haben wir, dass auch die öffentliche Hand (80%) dem Thema so hohe Relevanz beimisst. Die tiefste Relevanz hat Cyber Security im Gesundheitswesen, in Industrie- und Dienstleistungsbetrieben.

Welches sind die Top Cyber Security Themen in den verschiedenen Branchen?

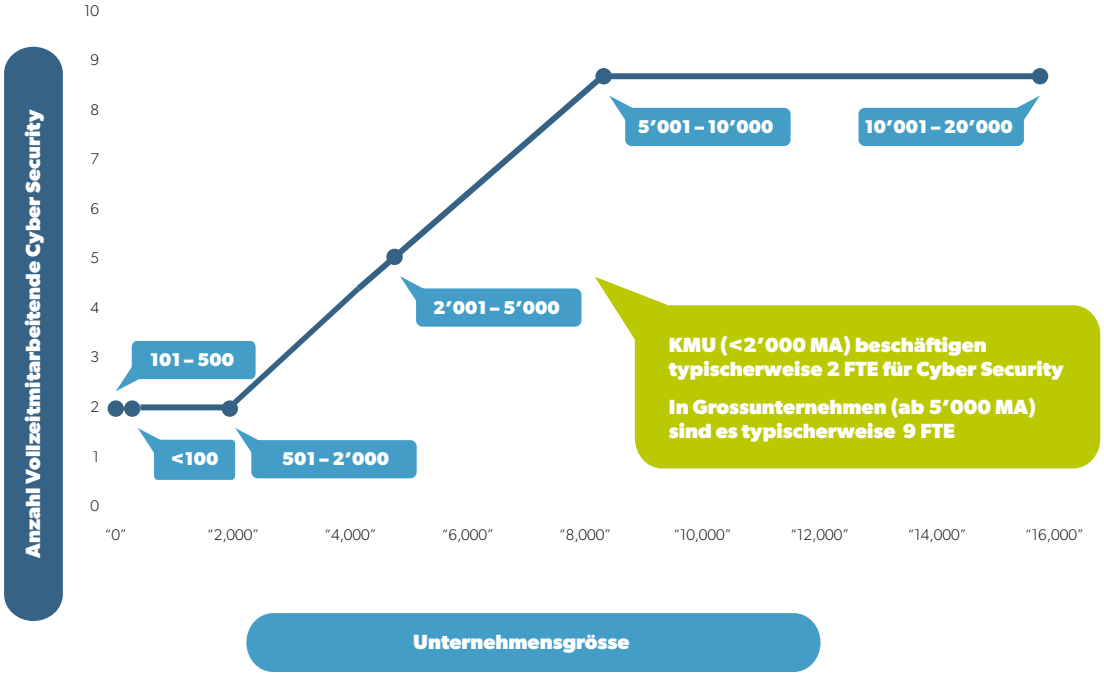
«Die Komplexität der Cyber-Resilienz per se ist die grösste Hürde, da hierzu ein ganzer «Blumenstrauss» von Themen adressiert werden muss.»

Manuel Fäh, Director Business Development/CDO, V-ZUG AG

Die Antworten der Teilnehmenden zeigen, dass für den Aufbau, den Betrieb und die Erhaltung der Cyber Security eine grosse Bandbreite an Themen adressiert wird. Dazu gehören neben Technik, prozessualen und organisatorischen Massnahmen auch benutzerzentrierte Faktoren. Die genannten Top Security Themen passen zu den aktuellen Themen rund um die Digitalisierung. Dazu gehören mobile Endgeräte, Cloud Services sowie die Orchestrierung aller internen Prozesse, die zur Koordination von Sicherheitsmassnahmen zusammengeführt werden müssen. Als wichtige Themen werden ferner die Erkennung von Angriffen, die Verhinderung von Datenverlusten sowie die Sicherheit des ganzen IoT-Umfeldes erachtet.

Interessant ist, in welchen Branchen welche Themen als besonders relevant eingestuft wurden. Mobile Endgeräte sind primär im Gesundheitswesen, in der Mobilität und in der Logistik von grosser Bedeutung. Cloud Services, Sicherheitsmassnahmen, Angriffserkennung und Datenschutz spielen in stark exponierte Branchen und bei Betreibern kritischer Infrastrukturen wie Banken und Dienstleistungsunternehmen eine zentrale Rolle, während IoT-Sicherheit vor allem für die Industrie und die Energieversorger wichtig ist. Die Gewichtung der Top Security Themen widerspiegelt damit den unterschiedlichen Durchdringungsgrad der Digitalisierung und die unterschiedliche ICT-Nutzung in den verschiedenen Branchen.

Wie viele Cyber Security Vollzeitmitarbeitende beschäftigen Unternehmen?

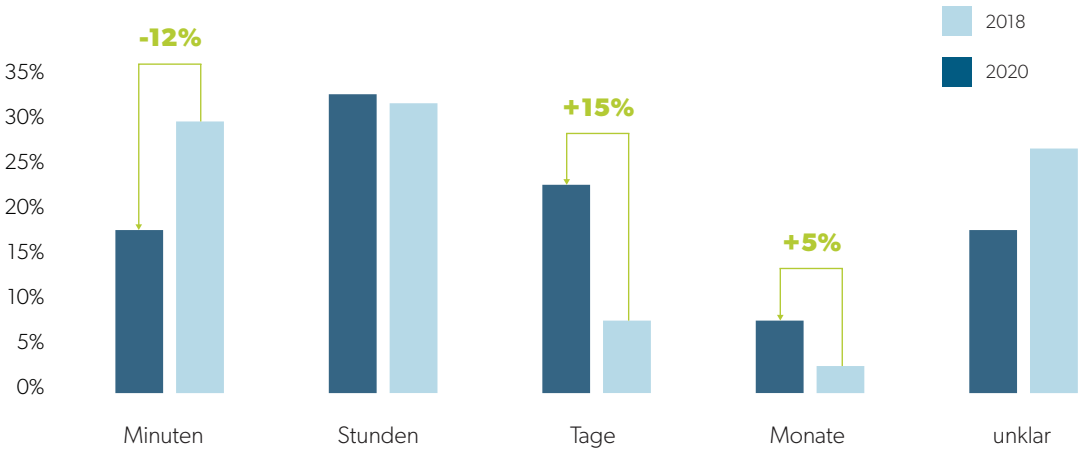


Eine Frage, die besonders in den Interviews auf grosse Resonanz stiess, ist das Verhältnis der Unternehmensgrösse in Bezug auf die Anzahl dedizierter Cyber-Security-Fachkräfte. Die Frage nach diesem Betreuungsverhältnis hat so etwas wie Benchmark-Charakter. Mittelständische Unternehmen mit bis zu 2000 Mitarbeitenden beschäftigen typischerweise 1-3 Security Fachkräfte. Bei Grossunternehmen ab 5000 Mitarbeitenden sind es 6-12. Danach steigt die Anzahl der internen Cyber-Security-Spezialisten erst bei wesentlich grösseren Unternehmen wieder an. Daraus ergibt sich, dass sich in der Regel nur ein Promille der Belegschaft mit Cyber Security befasst.

Da 70% der Befragten Cyber Security als Differenzierungsmerkmal beurteilen, stellt sich die Frage, warum ein so geschäftskritisch eingestufter Erfolgsfaktor mit so geringen personellen Ressourcen ausgestattet wird.

Wie lange dauert die Erkennung eines verdeckten Angriffs?

75% der befragten Unternehmen geben an, einen Cyberangriff innerhalb von Tagen zu erkennen

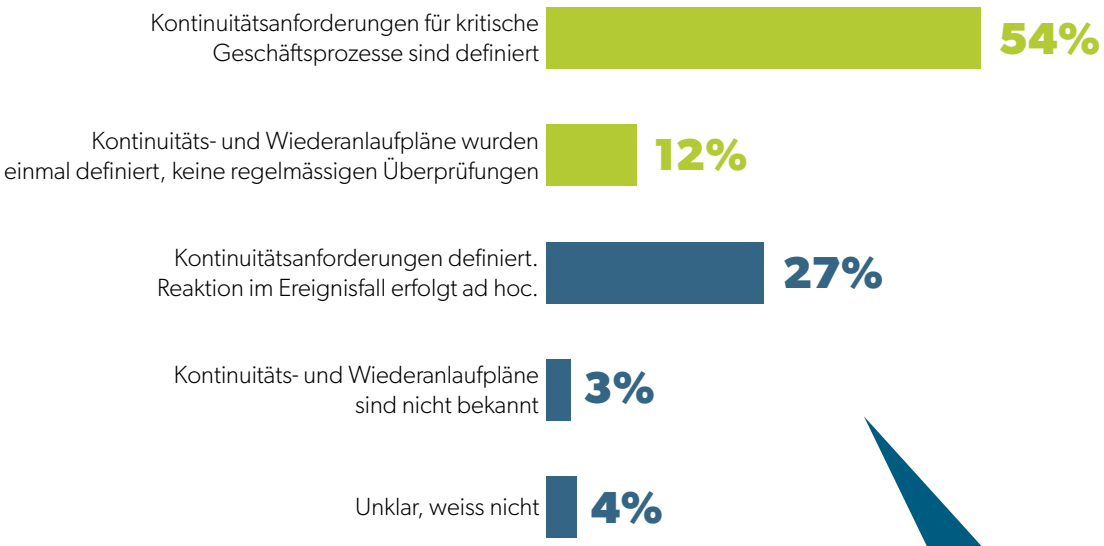


Cyberangriffe verlaufen nicht immer spektakulär und bleiben häufig über längere Zeit unentdeckt, da es im Interesse der Angreifer liegt, nach einem ersten Eindringen zunächst die Systemlandschaft seines Opfers zu erkunden und möglichst ungestört zu den digitalen «Kronjuwelen» vorzudringen. Deshalb ist es für die angegriffenen Unternehmen von grösster Wichtigkeit, eine Attacke so zeitnah wie möglich zu erkennen und Gegenmassnahmen einzuleiten.

Die erwartete Zeitspanne bis zur Erkennung eines verdeckten Angriffs wird heute etwas pessimistischer beurteilt als vor zwei Jahren. Zwar gaben 75% (gegenüber 70% in 2018) der Befragten an, einen Angriff innerhalb weniger Tage zu erkennen. Die Antworten zeigen jedoch eine Verschiebung hin zu längeren Zeiten, bis ein Angriff entdeckt wird: 12% weniger als 2018 erwarten, einen Angriff innerhalb von Minuten entdecken zu können, während 15% mehr als 2018 erwarten, dass es heute mehrere Tage dauert, bis ein Angriff erkannt wird. Andere Studien zeigen, dass es im Durchschnitt mehr als 200 Tage dauert, bis ein Unternehmen einen Cyberangriff bemerkt. Warum dauert die Erkennung so lange? Mögliche Gründe dafür sind sowohl die höhere technische Raffinesse als auch die verschobene Taktik der Angreifer, die so lange wie möglich unentdeckt bleiben wollen. Im Falle von Spionage und Datendiebstahl wird ein Angreifer grundsätzlich so geringe Spuren wie möglich hinterlassen.

Monitoring ist ein wichtiges Instrument für die Erkennung von Angriffen. Wir fragten deshalb, ob sich dazu passend auch der Scope der Cyber Security vom eigenen Unternehmen auf das ganze Ökosystem ausweitet. 38% der Befragten antworteten, dass sie ein umfassendes Security Logging und Monitoring der eigenen Infrastruktur betreiben. 23% gaben an, dass sie zusätzlich auch den Cybersicherheitszustand ihrer Service Provider, Zulieferer und Partner beurteilen. Bei den Banken und Versicherungen haben sogar 53% der Antwortenden die Cyber Sicherheit Ihres Ökosystems im Blick, nicht zuletzt wohl auch getrieben durch entsprechende Finanzmarktregulierungen zum Outsourcing.

Erholungsfähigkeit im Falle eines Angriffs



Wenn der Eintritt eines Cyber-Ereignisses nicht verhindert werden kann, wird die rasche Erholungsfähigkeit immer mehr zu einem kritischen Erfolgsfaktor.

Während Unternehmen ihre Sicherheitsmassnahmen immer wieder verbessern, zeigen auch Cyber Angriffe eine immer grössere Raffinesse. Wer dieses Wettrüsten schlussendlich gewinnen wird, ist heute unklar. Im gegenwärtigen Rüstungswettlauf stellt sich leider immer weniger die Frage, ob das eigene Unternehmen getroffen wird, sondern mehr denn je wann dies der Fall sein wird.

Mehr denn je muss deshalb die Erholungsfähigkeit einer Organisation in den Fokus treten. Unternehmen müssen sich auch für den Fall eines erfolgreich verlaufenen Cyber Angriffs vorbereiten.

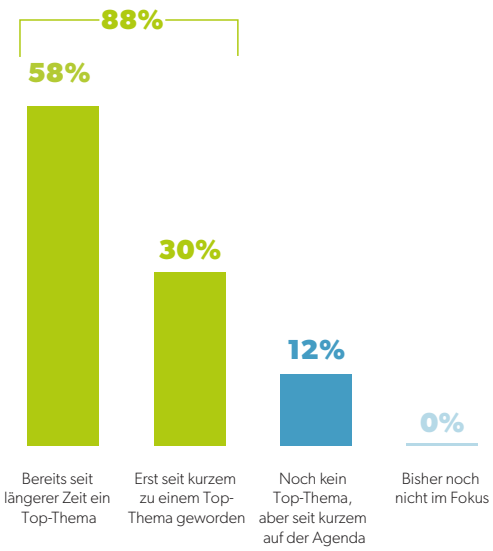
54% der befragten Unternehmen verfügen über definierte Kontinuitätsanforderungen, 12% davon überprüfen diese jedoch nicht regelmässig. Alle anderen Befragten verlassen sich auf ihre Improvisationsfähigkeit im Ereignisfall oder den Befragten sind etwaige getroffene Vorbereitungsmassnahmen nicht bekannt.

Themenblock Cyber-Resilienz

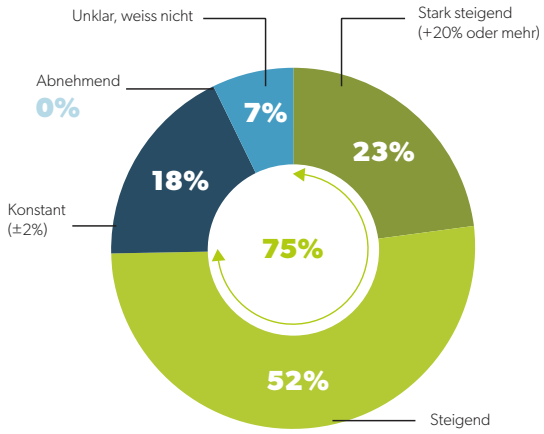
ISO 22316 definiert Resilienz als die Fähigkeit, sich einem wandelnden Umfeld anzupassen. Resiliente Organisationen sind fähig, auf Risiken und Chancen durch unvermittelte oder allmähliche Veränderungen in ihrem Umfeld situationskonform zu reagieren und diese zu antizipieren.

Mit diesem Themenblock wollten wir mehr über die Widerstandsfähigkeit von Unternehmen gegenüber Ereignissen im Cyberumfeld erfahren.

Welchen Stellenwert hat Cyber-Resilienz in den befragten Unternehmen?



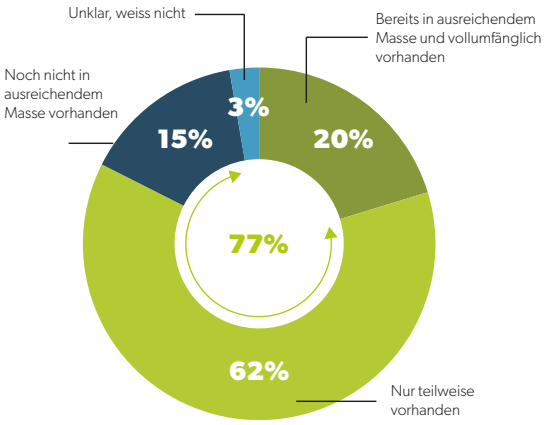
Stellenwert der Cyber-Resilienz



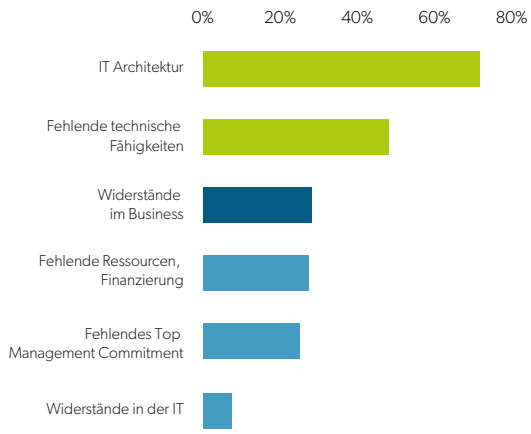
Cyber-Resilienz Budgetentwicklung seit 2018

Cyber-Resilienz rückt auf der Agenda von Führungskräften signifikant nach oben. 88% der befragten Unternehmen erachten Cyber-Resilienz als Top Thema und 75% der Befragten gaben an, dass ihr Budget seit 2018 angestiegen ist. Bei rund einem Viertel der Teilnehmenden erfolgte sogar ein starker Anstieg des Budgets.

Was sind die zentralen Herausforderungen in Bezug auf die Cyber-Resilienz?



Verfügbarkeit der notwendigen Cyber-Resilienz Fähigkeiten

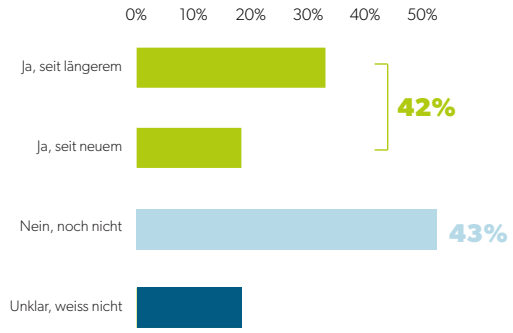


Grösste Hürden für den Aufbau der erforderlichen Cyber-Resilienz

Trotz höherer Budgets zeigen die Antworten der Teilnehmenden jedoch, dass lediglich 20% ihr Unternehmen als ausreichend resilient beurteilen, während 77% der Befragten bekundeten, dass die erforderlichen Cyber-Resilienz-Fähigkeiten nur teilweise oder noch nicht vorhanden sind.

Mögliche Gründe dafür sind beispielsweise Herausforderungen im Bereich der IT-Architektur wie Schnittstellenprobleme oder mangelndes technisches und fachliches Know-how. Die gute Nachricht: Diese beiden Herausforderungen sind sachlicher Natur und können mit entsprechendem Einsatz gemeistert werden. Schwieriger wird es bei den weiteren aufgeführten Hürden für den Aufbau von Cyber-Resilienz. Dazu gehören Widerstände im Business sowie fehlende personelle und finanzielle Ressourcen. Eher nachdenklich stimmt, dass von 9% der Befragten Widerstände in der IT als Herausforderung genannt wurde.

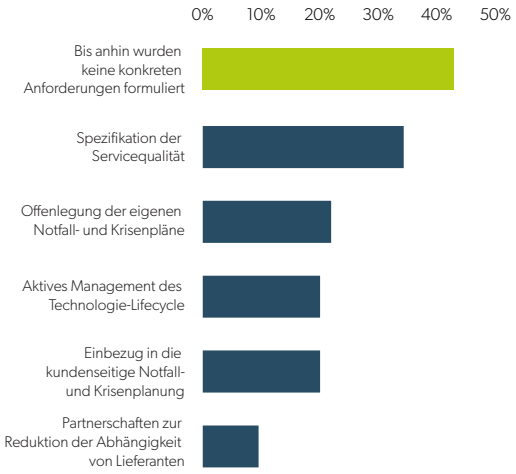
Wird Cyber-Resilienz über die gesamte Wertschöpfungskette von der Kür zur Pflicht?



Übernahme von Verantwortung für die Cybersicherheit von Kunden und Partnern, um die Resilienz der gemeinsamen Wertschöpfungskette zu steigern

Die Frage, ob sie die Verantwortung für die Cybersicherheit ihrer Kunden oder Partner übernehmen, um die Resilienz der gemeinsamen Wertschöpfungskette zu steigern, beantworteten 42% der Befragten mit ja. 43% der Befragten beabsichtigen dies in Zukunft an die Hand zu nehmen.

Ein analoges Bild zeigt sich bei der Frage, ob Resilienz von den Leistungsbezügern und/oder Kunden gefordert werde. 45% der Befragten gaben an, dass bisher von Kundenseite keine Resilienz-Anforderungen formuliert wurden.



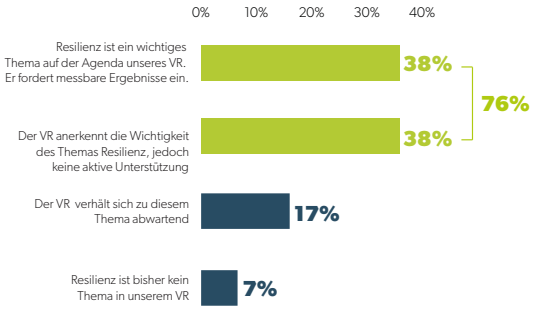
Konkrete Anforderungen von Kunden und/oder Leistungsbezügern an eine resiliente Ausgestaltung der Geschäftsbeziehung

Aufgrund der Erfahrungen aus der Corona-Krise wird eine organisationsübergreifende Sicht auf das Thema Resilienz stark an Bedeutung gewinnen.

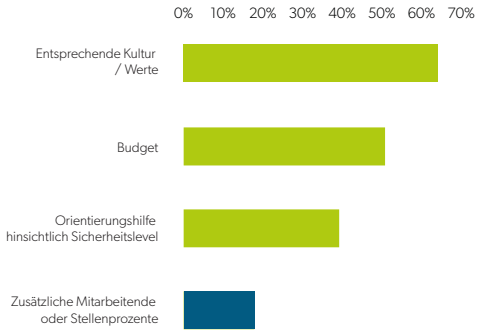
Wir erwarten hier eine Entwicklung hin zu einer gesamtheitlichen Sicht in Bezug auf die Sicherung dieses Ökosystems. Dabei liegt der Handlungsbedarf nicht nur bei den Leistungserbringern, sondern auch bei Leistungsbezügern, die offensichtlich bis heute kaum Anforderungen an die Resilienz ihrer Partner formulieren.

Der Handlungsbedarf auf Stufe C-Level ist damit erkannt.

Wie kann der Verwaltungsrat die Entwicklung der Resilienz tonangebend unterstützen?



Kenntnisse und Unterstützung von Seiten des Verwaltungsrates



Erwartungen an den Verwaltungsrat in Bezug auf die Cyber-Resilienz

Zu Schluss stellt sich die Frage, inwieweit sich die übergeordnete Ebene der Verwaltungsräte zur resilienten Ausgestaltung des Unternehmens bekennt: Verwaltungsräte sind ein wichtiger Treiber für die Entwicklung der Cyber-Resilienz in ihren Unternehmen.

76% der Verwaltungsräte sind sich dessen bewusst und anerkennen die Wichtigkeit des Themas. Erstaunlich ist jedoch, dass nur die Hälfte davon auch messbare Ergebnisse von ihrer Unternehmensleitung einfordert.

Aus Unternehmenssicht erwarten die Befragten von ihrem Verwaltungsrat insbesondere eine tonangebende Unterstützung in Bezug auf die entsprechende Kultur und Werte, die Freigabe und Zuweisung von personellen und finanziellen Ressourcen sowie Orientierungshilfe hinsichtlich des erforderlichen Sicherheitslevels.

Welche Erkenntnisse haben wir aus dieser Studie gewonnen?

- Obwohl Cyber Security für 70% der befragten Unternehmen ein Differenzierungsmerkmal am Markt ist, beurteilen nur 20% der Teilnehmenden ihren aktuellen Vorbereitungsstand als ausreichend.
- Grosse Hürden zur Verbesserung der Cyber-Resilienz, wie die Ausrichtung der IT-Architektur und Bereitstellung der benötigten technischen Kompetenzen sind mit externer Unterstützung und entsprechendem internem Engagement überwindbar.
- Ein sachkundiger und aktiv agierender Verwaltungsrat ist ein Schlüsselelement für den Aufbau und die Verankerung der Cyber-Resilienz im Unternehmen. Er definiert nicht nur die Kultur und die Werte, sondern sorgt auch für die Bereitstellung der erforderlichen Ressourcen.

Handelsempfehlungen

Der Aufbau von Cyber-Resilienz gelingt nicht von heute auf morgen. Vielmehr muss im Unternehmen zunächst kommuniziert und akzeptiert werden, dass die Vorbereitung auf den Eintritt einer digitalen Krisensituation heute notwendiger ist denn je zuvor.

Cyber Resilienz als Kulturelement ist besonders auf der Verwaltungsrats- und Führungsebene von zentraler Bedeutung und bildet die Basis für die Durchdringung einer resilienten Unternehmenskultur auf allen Ebenen der Organisation.

Cyber-Resilienz ist kein einmaliger Prozess. Die zum Einsatz kommenden Sicherheitstechnologien und -mechanismen müssen regelmässig überprüft, aktualisiert und getestet werden, da sich im Zeitalter der Digitalisierung sowohl die Bedrohungen als auch die Unternehmen selbst kontinuierlich verändern.

Beim Aufbau und Erhalt der Cybersicherheit und -Resilienz sollten die verantwortlichen Führungskräfte einen risikobasierten Ansatz für das Management von Informationsrisiken verfolgen. Hierzu müssen sowohl der Risikoappetit des Unternehmens identifiziert als auch die Ownership der Risiken definiert werden. Eigner der Risiken ist typischerweise das Business. Dieses finanziert direkt oder indirekt auch die Massnahmen zur Mitigation der Risiken. Wir empfehlen, die Auswirkungen auf das Business in den Fokus der Risikodiskussion zu stellen. Die Verfahren zur Identifikation, Messung und Bewertung der Risiken sollen nachvollziehbar ausgestaltet werden. Die Ableitung geeigneter Massnahmen wird darauf abgestützt. Zur Nachverfolgung der Massnahmenumsetzung und Überprüfung der damit erzielten Wirkung empfehlen wir ein regelmässiges Reporting.

Nicht weniger entscheidend ist die menschliche Komponente, ohne die automatisierte Prozesse und ausgefeilte Sicherheitstechnologie nicht die erwartete Wirkung erzielen. Um im Ereignisfall schnell und angemessen zu reagieren, muss Cyber-Resilienz im gesamten Unternehmen verankert und von allen Mitarbeitenden «gelebt» werden.

Corona hat bei vielen Organisationen schlagartig die Wichtigkeit der Sicherung der Wertschöpfungsketten über die Grenzen der eigenen Organisation hinweg aufgezeigt. Denn diese werden immer komplexer und erfordern ein sicherheitsbewusstes Zusammenspiel ganzer Ökosysteme, die immer weniger unter der eigenen, ausschliesslichen Kontrolle sind.

Letztendlich sollten Unternehmen festlegen, wie sie Vorhaben und Attacken im Umfeld der Cybersicherheit kommunizieren. Hierzu gehört neben den gesetzlichen Meldepflichten auch ein themenbezogener Austausch mit Investoren, Partnern, Lieferanten, Kunden und Mitarbeitenden. Unternehmen, die sich proaktiv auf potenzielle Vorfälle vorbereiten und in ihre Cyber-Resilienz investieren, schaffen eine Vertrauensbasis, die im Ereignisfall das eigene Fortbestehen sichern kann.

Verwaltungsräten empfehlen wir, sich als Sparringpartner des Managements zu positionieren und sich aktiv in die Diskussion zum Risikoappetit einzubringen. Wichtig dabei ist, dass sie sich ihrer Vorbildfunktion auch in Bezug auf das Thema der Cyber Sicherheit jederzeit bewusst sind.

Cyber-Resilienz in der öffentlichen Verwaltung

Die grosse Aufgabenvielfalt der Verwaltung und das föderalistische System führen dazu, dass in Bezug auf die Maturität, Innovation und Dynamik eine grosse Bandbreite vorherrscht. Beim Thema Cyber-Risiken zeigt sich dieselbe Situation: Grundsätzlich hat die öffentliche Verwaltung ihre Hausaufgaben hinsichtlich der Cybersicherheit gemacht und konnte sich bisher vor grossen, vertrauenserschütternden Vorfällen schützen.

Oliver Spiess, Partner

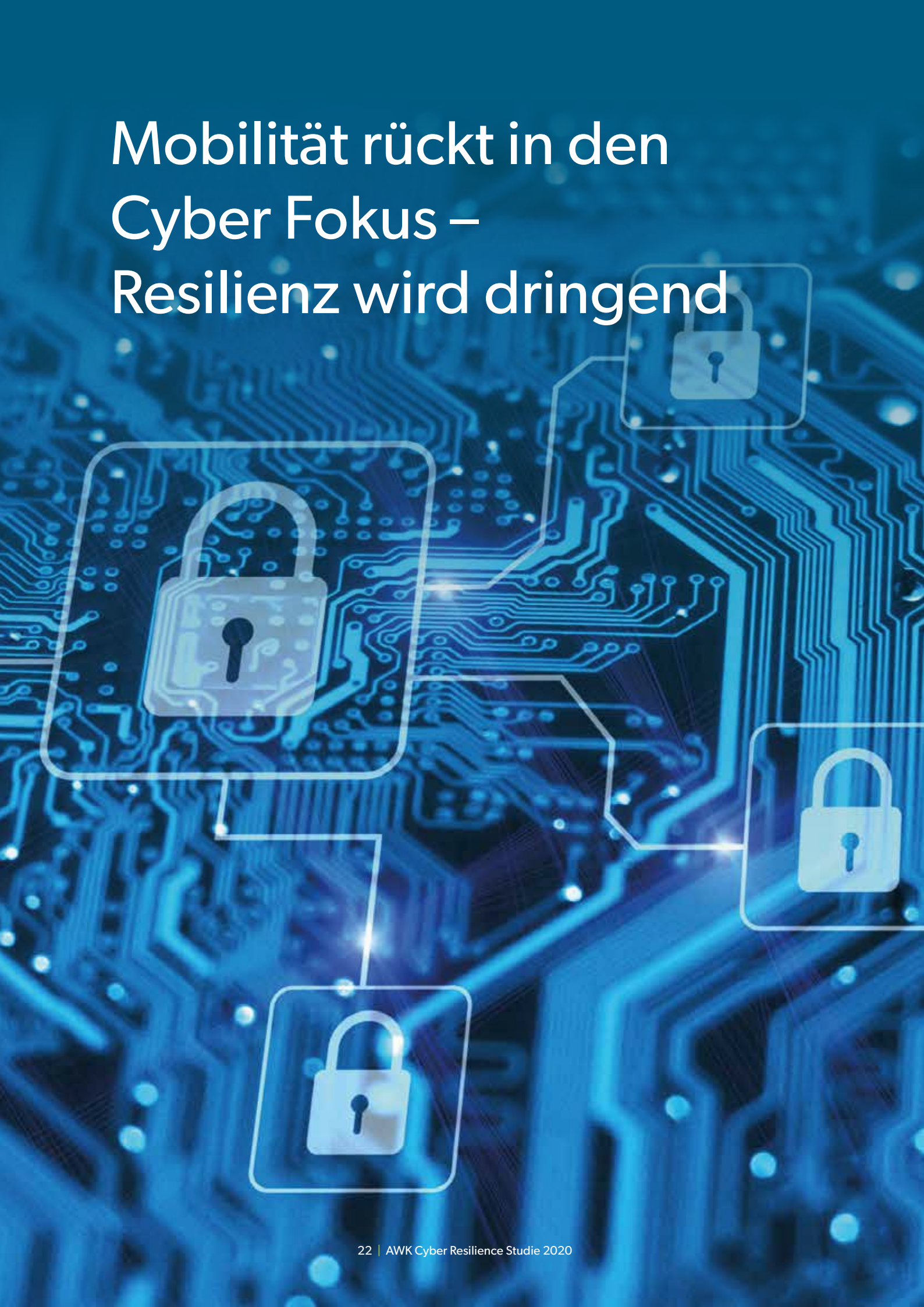
Die Teilnehmer der C-Level Studie aus der öffentlichen Verwaltung haben deutlich zum Ausdruck gebracht, dass Cyberrisiken schon seit längerem sehr weit oben auf der Agenda stehen und angemessene Investitionen in Personal und Systeme getätigt werden. Dies gilt insbesondere für den Perimeter-Schutz.

Das Vertrauen in die Sicherheit scheint ebenfalls vorhanden zu sein. Alle Teilnehmer gehen davon aus, dass sie in der Lage sind, Cyber-Angriffe innerhalb von «Tagen» zu erkennen. Gleichzeitig wird aber auch attestiert, dass Security Logging und Monitoring in der Regel bei der eigenen Infrastruktur aufhört und weder Service Provider, Zulieferer und Partner einschliesst, noch die gesamte eigene Landschaft umfasst. Ein Umstand, der etwas erstaunt und vertieft analysiert werden sollte.

Andererseits ist bezüglich der Cyber-Resilienz definitiv Verbesserungspotenzial vorhanden - insbesondere da Cyber-Resilienz nicht nur mithilfe von IT-Systemen erreicht wird, sondern eine Disziplin für die gesamte Organisation darstellt. Kein Teilnehmer an der C-Level Studie aus dem öffentlichen Dienst hat attestiert, dass die notwendigen Fähigkeiten in seiner Organisation im ausreichenden Masse vorhanden sind oder Resilienz einen Teil der Unternehmenskultur darstellt. Wenn man bedenkt, dass Resilienz die Flexibilität der gesamten Organisation anspricht und erfordert, müssen hier noch einige Hausaufgaben gemacht werden.

Die Herausforderung, die Cyber-Resilienz in ihrer gesamten Breite auch in der öffentlichen Verwaltung auf das heute erforderliche Niveau zu bringen, ist sicherlich beachtlich. Das Thema darf nicht mehr länger aufgeschoben werden, denn sonst besteht die Gefahr, dass die öffentliche Hand den Anschluss verpasst und sich dadurch hohen Sicherheitsrisiken aussetzt. AWK unterstützt die öffentliche Verwaltung als bewährter Partner von der Frage, was «genügendes Ausmass» bedeutet, über die Konzeption und Beschaffung bis zur Optimierung im Betrieb und begleitet entsprechende Projekte mit ihrer umfassenden Expertise und Erfahrung.

Mobilität rückt in den Cyber Fokus – Resilienz wird dringend



Die Sicherheit hat in der Mobilität seit jeher einen hohen Stellenwert, aber das Themenspektrum hat sich deutlich verändert und erweitert.

Während bisher in den Medien vor allem Personenunfälle hohe Aufmerksamkeit erhielten, weil sie betroffen machen und jeder/jedem widerfahren können, sind in den letzten Jahren zusätzliche Themen in den Fokus der Sicherheit gerückt. In der Luftfahrt sind die kritischen Systeme seit langem mehrfach redundant ausgelegt und unterliegen strengsten Vorschriften und Abnahmeverfahren. Auch im Schienen- und Strassenverkehr wird das Rollmaterial auf Herz und Nieren geprüft, bevor eine Zulassung erteilt wird. Die Infrastruktur und die damit verbundenen technischen Systeme bilden die Grundlage der Mobilität. Trotz dieser hohen Standards gibt es immer wieder sicherheitskritische Vorfälle, seien dies einstürzende Brücken, Lawinen oder LKW, die in einem Tunnel in Brand geraten. Einige dieser Vorfälle kann man unter dem Begriff «Unfall» zusammenfassen, während andere definitiv auf fehlerhafte Systeme und Prozesse zurückzuführen sind.

In jüngster Vergangenheit sind es aber nicht mehr nur solche Vorfälle, die den Führungsetagen der Mobilitätsunternehmen und -behörden Kopfzerbrechen bereiten. Die Antworten der Studienteilnehmer aus der Mobilitätsbranche zeigen deutlich, dass die Zahl der Herausforderungen in Bezug auf die Cyber-Security auch in ihrem Umfeld kontinuierlich steigt.

Beispielsweise waren im Strassenverkehr viele Systeme lange nur lokal bedienbar. Seit dem Umstieg auf IP-Technologie werden diese Anlagen über ein Breitbandkommunikationsnetz (BKN) bedient und sind dadurch faktisch zum grössten Teil «im Internet». Obwohl sie mittels demilitarisierter Zonen (DMZ) und Firewalls vor nicht autorisierten Zugriffen geschützt werden, sind sie vom Internet nicht komplett isoliert.

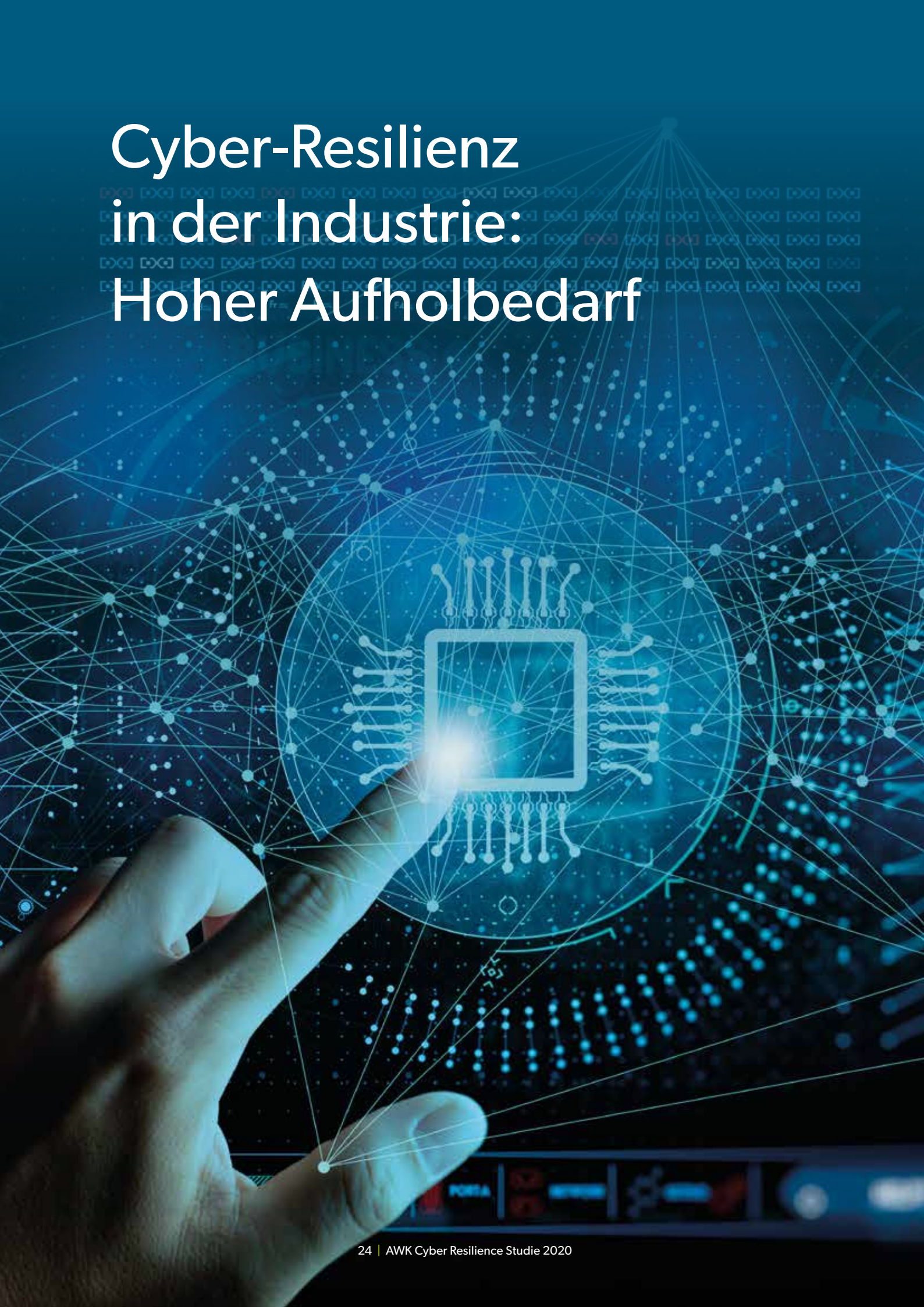
Peter Geissbühler, Head of Smart Mobility

Somit wird konsequente IT- und Netzwerksicherheit auch in diesem Bereich immer wichtiger. Dies konfrontiert Unternehmen und Behörden mit Herausforderungen, denen sie mit ihren eigenen personellen Ressourcen und dem intern verfügbaren Know-how oft nur unzureichend begegnen können.

Auch im öffentlichen Verkehr nimmt die Vernetzung von Fahrzeugen und der Infrastruktur laufend zu. Die Vernetzung von Verkehrswegen und Fahrzeugen wird die Kapazität des Verkehrssystem erhöhen, schafft gleichzeitig jedoch neue Anforderungen, das Gesamtsystem sicher und resilient zu halten. Aufgrund der vielen untereinander vernetzten Systeme von verschiedenen Lieferanten mit unterschiedlichen Lebenszyklen steigt die Komplexität rasch an, was sicherheitstechnisch und kostenseitig neue Herausforderungen schafft.

Resilienz ist auch in der Mobilität gefragt. Unternehmen müssen ihr Risikomanagement im Griff haben, sicherheitsrelevante Vorfälle rasch und sicher entdecken und darauf mit vorgefertigten Prozessen und Abläufen automatisch oder manuell reagieren. Mit der fortschreitenden Vernetzung wächst die Angriffsfläche des Gesamtsystems Mobilität mit hoher Geschwindigkeit. Ein durchdachtes und unter den verschiedenen Akteuren abgestimmtes Konzept wird daher unerlässlich, um die Resilienz des Systems umfassend zu gewährleisten.

Cyber-Resilienz in der Industrie: Hoher Aufholbedarf



Angreifer haben den Covid-19 Lockdown geschickt ausgenutzt, um erfolgreich Cyberattacken auf herstellende Industrieunternehmen zu führen. Die erlittenen Schäden betragen in manchen Fällen Millionen von Schweizerfranken.

Die grossen wirtschaftlichen Verwerfungen aufgrund des globalen Lockdowns hat bei zahlreichen herstellenden Industrieunternehmen dazu geführt, dass Kurzarbeit aufgenommen werden musste und ein Grossteil der weiterhin beschäftigten Arbeitskräfte ins Home-Office verbannt wurde. In manchen Unternehmen war auch die IT-Abteilung von der Kurzarbeit betroffen. Dies schaffte optimale Voraussetzungen für Cyberangriffe.

Zur Bereitstellung der erforderlichen digitalen Infrastruktur infolge der Krise, mussten vielerorts innerhalb von kürzester Zeit die Bandbreiten erhöht und die VPN-Infrastruktur ausgebaut werden. Nachdem diese ersten Hürden gemeistert waren, erhöhte die zunehmende Home-Office Arbeit den Bedarf an IT-Supportdienstleistungen. Im Vordergrund standen dabei die Verfügbarkeit und Funktionalität der Infrastruktur für die operativen Mitarbeitenden.

Gleichwohl führte die physische Distanz und die mit der Kurzarbeit verbundene reduzierte Verfügbarkeit zu einem unzureichenden Meinungs- und Informationsaustausch unter den Mitarbeitenden. Um den Betrieb dennoch aufrechtzuerhalten, wurden Entscheidungen in bester Absicht nicht selten ohne die sonst üblichen Abklärungen getroffen.

Damit entstanden gleich mehrere Opportunitäten für potenzielle Angreifer, die erfolgreich ausgenutzt wurden:

- Reduzierte personelle und finanzielle Ressourcen
- Aufsetzen und Ausrollen von Lösungen innerhalb von kürzester Zeit und unter hohem operativem Druck

André Schmid, Senior Manager Manufacturing

- Aufrechterhalten des Betriebs als Maxime
- Nichteinhalten von Standardprozessen

Aus diversen Studien geht klar hervor, dass die Maturität bezüglich der IT-Sicherheit bei vielen herstellenden Industrieunternehmen tiefer ist als in anderen Wirtschaftssektoren. Erstaunlicherweise gaben 70% der Studienteilnehmer aus der herstellenden Industrie an, dass ein Sicherheitsvorfall in der Regel innerhalb von ein paar Stunden entdeckt wird. Diese Einschätzung führt falsche Annahmen vor Augen. In Wahrheit dürfte die durchschnittliche Dauer vielmehr länger als 200 Tage sein.

Auf diese Einschätzung lässt sich mit hoher Wahrscheinlichkeit auch zurückführen, dass die IT-Sicherheit bei der Mehrheit der herstellenden Industrieunternehmen einen zu geringen Maturitätsgrad aufweist. Es scheint, dass manche Unternehmen die tatsächlichen und potenziellen Risiken nicht kennen oder diese falsche einstufen.

Es bleibt zu hoffen, dass die publik gewordenen IT-Security-Vorfälle der letzten Monate viele Industrieunternehmen veranlassen werden, einen grösseren Fokus auf die Cyber-Resilienz zu legen. Denn durch Cyberangriffe verursachte Schäden gehen nicht nur schnell in die Millionenhöhe. Sie hinterlassen auch bei Investoren und Kunden ein ungutes Gefühl und schaden dadurch der Reputation des Unternehmens.

Vorreiterstellung der Banken – kritische Selbsteinschätzung der Versicherungen

Informationssicherheit gehört spätestens seit dem Aufkommen des E-Bankings Ende der 1990er Jahren zu den zentralen Fähigkeiten von Banken. Mit der fortschreitenden Vernetzung rüsteten alle Institute zudem ihre Cyber Security auf. Diese Anstrengungen wurden durch Regulierungen zum Umgang mit operativen Risiken und Outsourcing zusätzlich verstärkt.

Diese Efforts widerspiegeln auch die Umfrageresultate unserer Studie. Banken attestieren sich im Vergleich zu Unternehmen aus anderen Branchen eine hohe Maturität: 54% verfügen gemäss eigenen Aussagen über eine ausreichende Cyber-Resilienz. Besonders erstaunt hat uns, dass 92% der befragten Banken und 70% der Versicherungen Cyber Security als Differenzierungsfaktor am Markt erachten. Ein Reputationsschaden durch eine nicht abgewehrte Cyber Attacke kann sich niemand leisten. 86% der befragten Finanzinstitute gaben an, dass sie ihre Budgets für Cyber Security in den letzten zwei Jahren zum Teil deutlich erhöht haben. Obwohl Ökosysteme erst in den letzten Jahren zum wichtigen Bestandteil des Geschäftsmodells von Finanzinstituten gehören, beweisen Banken auch hier Weitsicht: 73% betrachten im Rahmen ihrer Aufwendungen für die Cyber Security die ganze Wertschöpfungskette. Im Vergleich zu den übrigen Teilnehmenden erwähnten jedoch auffallend viele Verantwortliche von Banken ein fehlendes Commitment beim Top-Management.

Überraschend sind die Ergebnisse zu den Versicherungen. In der Umfrage zeigten sich die Antwortenden aus der Assekuranz generell kritischer bezüglich ihrer Maturität in Cyber Security als ihre Kollegen aus den Banken. Dies widerspiegelt nur zum Teil unseren Eindruck, da die meisten Versicherungen umfassende und den Banken nur geringfügig nachstehende Massnahmen zur Sicherstellung ihrer Cyber-Resilienz getroffen haben. Möglicherweise sind die tiefer bewerteten Fähigkeiten auf den transparenten Umgang mit Risiken im Versicherungsumfeld zurückzuführen. Dieser gehört zum Kerngeschäft der Versicherer, da eine objektive Beurteilung von Risiken für deren Überleben entscheidend ist.

Adrian Anderegg, Head of Financial Services

Trotz der insgesamt hohen Maturität der Branche ist Ausruhen keine Option. Als grösste Herausforderung erachten die Umfrageteilnehmer aus der Finanzindustrie das sich rasant verändernde Umfeld. Genau hier setzt Cyber-Resilienz an. Sie bereitet Unternehmen im Gegensatz zu reinen Cyber Security Konzepten auch auf unvorhersehbare Ereignisse vor. Eine Krise wie diejenige der letzten Monate zeigte sehr transparent auf, in welchen Bereichen die eigene Organisation instabil wurde. Dies bietet Unternehmen die Chance, ihre Krisenstabseinsätze anhand der «Lessons learned» mit fokussierten Verbesserungsmassnahmen weiter zu optimieren.

Aus unserer Sicht liegt das grösste Potenzial in der Steigerung der Cyber-Resilienz. Unternehmen reagieren bereits heute auf eine Vielzahl von konkreten Bedrohungsszenarien, um deren Eintrittswahrscheinlichkeit zu minimieren. Doch das Umfeld ändert so rasch, dass niemals alle Bedrohungen adressiert und eliminiert werden können. Cyber-Resilienz erhöht die Stabilität des Gesamtsystems und stellt im Falle eines unvorhergesehenen Ereignisses sicher, dass Unternehmen ihren Betrieb aufrechterhalten und Einbussen in Bezug auf ihre Servicequalität massiv reduzieren können.

Cyber-Resilienz als Enabler für hohe Krisenresistenz und Zukunftssicherheit

Die Verlagerung von physischen hin zu digitalen Bedrohungen in den letzten Jahren und die daraus resultierende Verantwortung von Unternehmen ihren Mitarbeitenden, Partnern und vor allem auch ihren Kunden gegenüber, war für uns Cyberexperten schon immer ein guter Startpunkt für Diskussionen. Unsere Studie verdeutlicht, dass Cyber Security in Unternehmen heute branchenunabhängig zu den Grundsatzthemen gehört.

Wolfgang Schurr, Partner

In den letzten Tagen, Wochen und Monaten hat uns die Corona-Krise die Bedeutung der physischen Sicherheit deutlich vor Augen geführt. Die Sicherstellung der Gesundheit der Gemeinschaft – unserer Kollegen, Geschäftspartner und Kunden sowie auch unserer Familien – ist zum Glück immer noch das wichtigste Gut für uns alle! Die Digitalisierung hat uns in dieser Krise geholfen, die Gemeinschaft zu schützen. Die vorhandene IT-Infrastruktur ermöglichte vielen Betrieben, ihre Arbeiten im Home-Office mehr oder weniger unterbruchsfrei fortzuführen.

Die Digitalisierung war somit einmal mehr das richtige Mittel, um unser Leben zu sichern. Ein entscheidender Teil der Digitalisierung ist deren Sicherheit, die Cyber Security oder – für mich noch besser beschrieben – die Cyber-Resilienz. Überraschend oder nicht, zeigt unsere Studie, dass immer mehr Manager die Cyber-Resilienz als Wettbewerbsvorteil erachten. In den Wochen des Lockdowns hat sich dieser Vorteil bereits bestätigt. Unternehmen, die sich während der Krise schnell digital gewandelt und auf die neuen Herausforderungen und Risiken adäquat reagiert haben, konnten ihre Kunden nicht nur halten, sondern sogar das Vertrauen im und in das jeweilige Ökosystem erhöhen und neue Kunden gewinnen. Diese Vorteile und das neue Vertrauen in die Digitalisierung gilt es zu wahren und zu festigen. Cyber-Resilienz bedeutet in diesem Kontext risikobasiertes und flexibles Handeln – von der Identifikation bis hin zur Bewältigung von Cyber-Notfällen. Das Ziel der Cyber-Resilienz ist und bleibt dabei stets die Sicherstellung des Fortbestandes des Unternehmens unter herausfordernden Bedingungen.

Die Eindrücke der letzten Wochen, die Ergebnisse der Studie und insbesondere die Kommentare der Teilnehmer zeigen mir, dass der Schutz des Einzelnen, der Gemeinschaft und des jeweiligen Unternehmens für jeden von uns entscheidend ist. Lasst uns durch eine risikobasierte Sicherheitsanalyse die optimalen Massnahmen ergreifen und die Digitalisierung unserer Unternehmen zielbewusst weiter vorantreiben.

Vorgehensweise bei der Cyber-Resilienz Studie 2020

Die breit abgestützte, in Partnerschaft mit C-LEVEL durchgeführte Studie zeigt auf wie Unternehmen aus allen Wirtschaftssektoren mit den Themen Cyber Security und Cyber-Resilienz umgehen. Ziel der Studie war es, Führungskräfte dabei zu unterstützen, sich schnell und effektiv mit diesen aktuellen Themen auseinanderzusetzen sowie die damit verbundenen Herausforderungen und Potenziale für das eigene Unternehmen zu erkennen und erfolgreich zu nutzen. Zugleich hatten die teilnehmenden Unternehmen die Möglichkeit, von anderen Thought Leadern und Unternehmen zu lernen und die Ausgangslage des eigenen Unternehmens zu vergleichen.

Der erste Teil der Cyber-Resilienz Studie 2020 befasst sich mit dem Thema Cyber Security und zieht auch einen Vergleich zu einer vor zwei Jahren durchgeführten Studie. Der zweite Teil ist der Cyber-Resilienz gewidmet und untersucht die Widerstandsfähigkeit von Unternehmen gegenüber Ereignissen im Cyberumfeld.

Die Datenerhebung erfolgte auf Basis eines strukturierten Fragebogens. Zusätzlich haben wir die adressierten Themenbereiche mit ausgewählten Teilnehmenden im Rahmen von Interviews weiter vertieft.

Der Geschäftsbereich Cyber Security & Privacy von AWK gehört zu den namhaften Playern im Schweizer Security Beratungsmarkt. Unsere Cyber Security & Privacy Spezialisten unterstützen Unternehmen beim Schutz gegen Cyberbedrohungen mit einem vorausschauenden Cyber Security Management und begleiten den Aufbau von Resilienz für den Ereignisfall im Einklang mit den strategischen Geschäftszielen unserer Kunden.

Ziel der AWK Group ist es, dieses strategische Geschäftsfeld bis 2025 auf 150 Mitarbeitende auszubauen.

AWK Group
Enabling digital performance.

Zürich
AWK Group AG
Leutschenbachstrasse 45
CH-8050 Zürich

Bern
AWK Group AG
Laupenstrasse 4
CH-3001 Bern

Basel
AWK Group AG
Centralbahnstrasse 11
CH-4051 Basel

Lausanne
AWK Group AG
Tour Edipresse
Avenue de la Gare 33
CH-1003 Lausanne

Telefonisch erreichen Sie uns
unter +41 58 411 95 00

Kontaktieren Sie uns per
E-Mail an info@awk.ch

www.awk.ch

AWK Cyber-Resilienz Studie 2020

AWK Group
Enabling digital performance.