eraneos

FOKUS

Resilienz

Von links nach rechts: **Dr. Christian Mauz,** Partner; **Adrian Anderegg**, Head of Financial Services; **Dr. Pascal Bettendorff,** Senior Manager; **Dominik Moser,** Senior Consultant; **Dr. Adrian Marti,** Head of Cyber Security & Privacy; **Stephan Gerber,** Consultant; **Johannes Vamos**, Consultant; **Dr. Thomas Rhomberg**, Head of Security Operations & Transformation

Inhalt

Risiken auf unserer Reise in die Digitalisierung meistern

Die VUCA[1]-World beschreibt unsere neue Realität aus Unbeständigkeit, Unsicherheit, Komplexität und Mehrdeutigkeit. Wie damals zu Beginn der Neuzeit die grossen Entdecker, müssen wir uns in dieser neuen Welt zurechtfinden und unsere Organisationen darauf ausrichten. Die ersten Segler stachen in See, ohne zu wissen, was sie erwartet. Mit der Zeit haben wir uns Hilfsmittel erarbeitet, um Risiken beherrschbar zu machen. Für Christoph Kolumbus war die Reise nach Amerika ein lebensbedrohliches Abenteuer. Heute ist diese für uns nichts Besonderes mehr.
Dr. Christian Mauz

Mit der Digitalisierung und der VUCA-World befinden wir uns in einer ganz ähnlichen Situation. Wir kennen die Bedrohungen und Gegner nicht genau und das Umfeld ändert sich konstant. Wir wissen nur, dass auf unsere Organisationen neben vielen Chancen auch ernste Bedrohungen zukommen. Das klassische Risikomanagement und die Zukunftsplanung stossen hier an ihre Grenzen. Um sich in einem solchen Umfeld erfolgreich zu behaupten, müssen Organisationen robust sein.

Die Natur und biologische Systeme sind gute Vorbilder für resiliente Systeme. Konzepte wie Redundanz, Kapselung, Dezentralität, Autonomie oder Polyvalenz unterstützen den Menschen dabei, sich in unterschiedlichsten Umgebungen erfolgreich zu etablieren und selbst schwerste Krankheiten und Unfälle zu überleben.

Im vorliegenden Eraneos Fokus möchten wir Ihnen Ansätze an die Hand geben, wie Sie Ihre Organisation fit für diese neue Welt machen und resilient werden.

Wir wünschen Ihnen eine spannende und aufschlussreiche Lektüre

„Resilienz ist zwingend für Organisationen, um in der VUCA-World zu überleben."

Dr. Christian Mauz
Partner

1
Volatility, Uncertainty, Complexity, Ambiguity

Resilienz Unser Verständnis

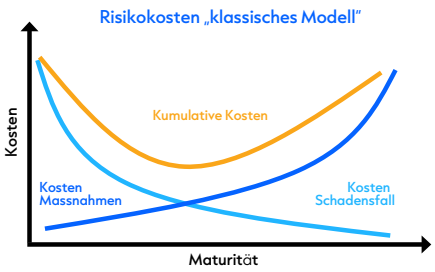
Zurzeit ist das Schlagwort Resilienz im unternehmerischen Kontext allgegenwärtig. Zwar sind sich nicht einmal Experten über seine Definition und Ausprägungen einig. Klar ist jedoch, dass mittels Resilienz die Widerstandsfähigkeit eines Unternehmens gegenüber noch unbekannten, meist negativen Ereignissen erhöht werden soll. Die hohe Bedeutung des Themas Resilienz kann unter dem Sammelbegriff VUCA (Volatility, Uncertainty, Complexity und Ambiguity[1]) zusammengefasst werden: Es wird immer schwieriger, die Zukunft konkret vorherzusehen.

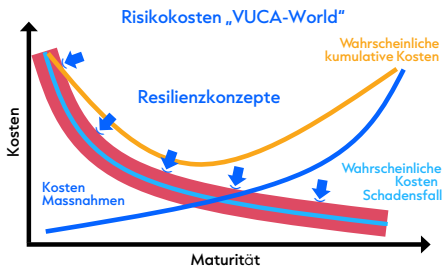
Dr. Pascal Bettendorff, Johannes Vamos

Mit der zunehmenden Digitalisierung und Vernetzung von Unternehmen werden die Identifikation und das Beherrschen von Risiken immer komplexer. Das klassische Risikomanagement misst Risiken einen finanziellen Wert bei, indem es die Schadenshöhe und die Eintrittswahrscheinlichkeit bewertet. Es wird versucht, den Aufwand für die getroffenen Massnahmen im Schadensfall und die dadurch anfallenden Kosten zu optimieren. In einer vielschichtigen und volatilen Bedrohungslandschaft können aber nicht mehr alle Risiken identifiziert werden. Zusätzlich ist es aufgrund der zahlreichen Abhängigkeiten schwierig, die Folgekosten von Risiken zu quantifizieren. Das Schadensausmass verschwimmt zu einem Schadensbereich.

Resilienz hat nicht zum Ziel, sich gegen einzelne, klar abgegrenzte Risiken zu schützen. Vielmehr versuchen sogenannte Resilienzkonzepte, den potenziellen Scha densbereich aller Risiken – bekannte und unbekannte – zu verkleinern. Anstatt sich auf einzelne Risiken zu fokussieren, wird das Schadensausmass für bestimmte Risikogruppen geschätzt und mit den Kosten für die notwendigen Massnahmen verglichen. Ausgangsbasis für die Definition der Risikogruppen sind die Bedrohungslandschaft, welche laufend aktualisiert werden muss, und gewonnene Erfahrungen im Unternehmen. Der klassische Kosten-Nutzen-Vergleich zwischen Risiko und Massnahmen verschiebt sich auf eine noch abstraktere Ebene.

Bei 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.





Risiken sind im Zeitalter der Digitalisierung und Vernetzung immer schwerer greifbar

1 Deutsch: Unbeständigkeit, Unsicherheit, Komplexität, Mehrdeutigkeit

Operationelle Resilienz

als Schlüsselfähigkeit von Unternehmen Der Fall des kanadischen Fintech QuadrigaCX, einer ehemals grossen kanadischen Börse für Kryptowährungen, verdeutlicht, warum klassisches Risikomanagement unzureichend ist. Als technologisch modernes Unternehmen hielt das Fintech die kryptografischen Schlüssel in einem sogenannten Cold Wallet[2]. Im Dezember 2018 verstarb der CEO überraschend in Indien. Mangels berechtigter Stellvertreter waren die Zugangsdaten nicht mehr verfügbar und das Unternehmen verlor mit dem Zugangsschlüssel den Zugriff auf fast 200 Millionen Dollar. Es hatte die organisatorische Resilienz vernachlässigt.

Eraneos versteht unter Resilienz die Fähigkeit von Organisationen, geschäftsgefährdende Ereignisse über einen gewissen Zeitraum tolerieren zu können und sich flexibel an sich ändernde Umstände anzupassen. Resilienz betrachtet die ganzheitliche Belastbarkeit der Organisation sowie ihre Reaktionsfähigkeit und nicht nur einzelne Geschäftsprozesse. In diesem Fokus-Artikel gehen wir näher auf die operationelle Resilienz ein, da Unternehmen in diesem Bereich häufig grossen Herausforderungen gegenüberstehen.

Operationelle Resilienz stellt sicher, dass das Erbringen von internen und externen Dienstleistungen auch bei Ausfällen von Teilprozessen oder Zulieferern gewährleistet wird. Obwohl sie sich an das Operational Risk Management anlehnt, werden nicht nur explizite Risiken behandelt. Resilienz orientiert sich sehr stark an der sich ändernden Bedrohungslandschaft und verfolgt das Ziel, auch nicht identifizierte Risiken zu beherrschen, die aufgrund der Komplexität der heutigen Leistungserbringung bestehen.

Teilweise müssen zur Steigerung der operationellen Resilienz bewusst finanzielle Ineffizienzen in Kauf genommen werden. So wird z. B. durch Überdimensionierung, Redundanz oder Rückfallebenen auch unter erschwerten Bedingungen ein stabiler Service aufrechterhalten.

Resilienz im Operating Model

Um Resilienz zu schaffen, wirken wiederkehrende Resilienzkonzepte auf das Operating Model in den Domänen Menschen und Skills, Organisation und Governance, Technologie und Information, Partner und Ökosysteme sowie Geschäftsprozesse. Ein resilientes Unternehmen besitzt in allen genannten Domänen ein ähnlich hohes Maturitätsniveau. Wird eine Domäne vernachlässigt, kann die fehlende Maturität nicht durch Maturität in den anderen Domänen kompensiert werden. Genauso kann eine sehr ausgereifte Domäne die Schwächen in den anderen Domänen nicht kompensieren.

Menschen und Skills sowie **Organisation und Governance** miteinzubeziehen, ist für ein resilientes Unternehmen essenziell. Mitarbeitende müssen angemessen ausgebildet und ausgestattet werden. Die Rollen und Verantwortlichkeiten innerhalb des Unternehmens müssen klar definiert sein. Zugleich müssen die benötigten Rollen zu den Geschäftszeiten verfügbar und vollwertige Stellvertretungen stets sichergestellt sein. Häufig wird Stellvertretung

2
Cold Wallet: eine virtuelle Geldbörse für Kryptowährungen, die nicht mit dem Internet verbunden ist

in der Praxis als Ferienvertretung missverstanden. Dadurch ist die organisatorische Resilienz weniger ausgeprägt, als angenommen. Für ein resilientes Unternehmen ist es besonders wichtig, sich zügig anzupassen. Dies verlangt eine etablierte Kultur, die Änderungen willkommen heisst und eine zu stark zementierte Experten- und Silokultur vermeidet.

Technologie und Information weisen vielerorts einen grossen und teuren Aufholbedarf in Bezug auf die Resilienz auf. Häufig wurde Resilienz mit redundanter Infrastruktur gleichgesetzt, während der applikatorische Teil vernachlässigt wurde. Dabei können bereits einfache Massnahmen, wie etwa regelmässige Updates und ein systematisches Lifecycle-Management, die Maturität signifikant erhöhen. In dieser Domäne gibt es viele Möglichkeiten. Da diese jedoch mit hohen Kosten verbunden sind, ermöglicht nur ein systematisches Herangehen an die Planung und Umsetzung von Massnahmen zur Steigerung der Resilienz den optimalen Ressourceneinsatz.

Partner und Ökosysteme sind im Zeitalter der Digitalisierung ein wesentlicher Bestandteil des Unternehmens. Dies erfordert ein Partnermanagement, das für strategische, taktische oder operationelle Partner gleichermassen etabliert ist. Gut gemanagte und gepflegte Partner können zu einem der stärksten Treiber der Resilienz werden und die Kosten zugleich massiv reduzieren. Schlecht gemanagte Partner bergen hingegen ein hohes Risiko für das eigene Unternehmen und können eine finanzielle Last bedeuten.

Geschäftsprozesse, die im Zusammenhang mit den Kernkompetenzen des Unternehmens stehen, müssen im Zuge der Resilienz-Steigerung berücksichtigt werden. Es ist entscheidend, dass Resilienz bereits beim Design von Prozessen berücksichtigt wird, z. B. durch redundante Unterstützungssysteme oder Kollaborationen mit Unternehmenspartnern. Resilienz darf die Effizienz eines Prozesses nicht beeinträchtigen. Vielmehr muss die Prozesseffizienz auch unter schwierigen Bedingungen gewährleistet sein.

Alle genannten Domänen sind gekoppelt. Gute technologische Lösungen sind wertlos, wenn die Lösung nicht eingesetzt wird, und gute Kernprozesse sind wirkungslos, wenn sich die Mitarbeitenden nicht an diese halten.

Target Operating Model

Mechanismen wirken auf das Target Operating Model und erzeugen Resilienz im Unternehmen

Konzepte zur Steigerung der Resilienz

Aus der Praxis kennt man wiederkehrende Muster (Resilienzkonzepte), die eingesetzt werden können, um die Maturität der Resilienz des Operating Model zu erhöhen. Beispiele für einfache Konzepte sind Redundanz, Kapselung, Skalierung, Dezentralität und Autonomie. Alle diese Konzepte können in jeder Domäne eingesetzt werden. Redundanz in der Technologie bedeutet duplizierte Systeme, während es in der organisatorischen Domäne um vollwertige Stellvertretungen geht. Darüber hinaus existieren auch komplexere Konzepte wie etwa Know-how-Management, Automatisierung und Kollaboration.

Ein resilientes Unternehmen schafft selektiv effiziente Mechanismen, um möglichst gut gegen die Bedrohungslandschaft gerüstet zu sein. Dabei sind nicht alle Resilienzkonzepte für jedes Unternehmen in jeder Domäne sinnvoll anwendbar. Die Konzepte bieten jedoch eine gute Ausgangsbasis, um die Resilienzmaturität im Unternehmen weiter zu verbessern und Lücken in der operationellen Resilienz aufzuspüren. Während das Fehlen solcher Resilienzkonzepte in einzelnen Domänen auf eine niedrige Resilienzmaturität hinweisen kann, ist es nicht sinnvoll, Resilienzkonzepte ohne ganzheitliche Steuerung willkürlich zu kombinieren.

Am Beispiel der Kapselung möchten wir dies noch vertiefen. In der Technologiedomäne bestehen gekapselte Systeme aus Teilkomponenten, die während des Lebenszyklus ausgetauscht werden können. So können unterschiedliche Komponenten ersetzt, an Partner vergeben und besser skaliert werden. Auch in der Domäne Prozesse führt Kapselung zu Resilienz. Klare und einfache Schnittstellen erlauben den Ausfall von Teilprozessen und alternative Vorgehensweisen. In der Personendomäne wird bereits durch eine klare Aufgaben- und Kompetenzverteilung Kapselung erzeugt, während klar definierte Verträge und SLA der Partnerdomäne eine gekapselte Struktur vermitteln.

Die Kombination verschiedener Resilienzkonzepte erhöht die Maturität weiter. Modernste Ansätze, wie etwa das von Netflix geprägte „Chaos Testing", funktionieren unter der Prämisse, dass Systeme mittels Kapselung so modular aufgebaut sind, dass sie kurzfristig neu gestartet oder durch eine neue Instanz ersetzt werden können. Netflix setzt einen zentralen Service, den „Chaos Monkey", ein, welcher im laufenden Betrieb zufällig ausgewählte Systeme in Bedrängnis bringt. Durch etablierte Konzepte in der Skalierung und eingespielte Teams können solche Situationen bewältigt werden, ohne dass der Kunde im täglichen Betrieb Auswirkungen spürt. Zusätzlich werden Informationen zu Abhängigkeiten gesammelt, die aufgrund der Komplexität der Systeme schwer abzuschätzen sind. Mit „Chaos Testing" werden die eigene Bereitschaft permanent getestet und die Maturität der Resilienz laufend erhöht.

Erfolgsfaktoren für ein resilientes Unternehmen

Um ein Unternehmen resilient zu gestalten, muss das Unternehmen sowohl sich selbst als auch sein Umfeld verstehen. Dies wird aufgrund der zunehmenden Vernetzung und Dezentralisierung immer schwieriger. Daher ist der Ansatz einer zentralen Stelle, von der alle Resilienz ausgehen soll, immer weniger praktikabel. Erfolgsentscheidend ist vielmehr, dass jeder Bestandteil und jeder Mitarbeitende im Unternehmen zur Resilienz beiträgt. Bei jedem Vorhaben muss Resilienz von Anfang an berücksichtigt und im Produktivbetrieb getestet werden.

Die Umsetzung von Resilienz in etablierten Prozessen und Systemen ist häufig sehr aufwendig. Nach einer unternehmensweiten Analyse hinsichtlich sogenannter „Quick-Wins" sollte geschäftsorientiert vorgegangen werden. Die wichtigsten Kundenservices sollten vorrangig geprüft und widerstandsfähiger gemacht werden. Neben spezifischen Analysen muss also auch nach fehlenden Resilienzkonzepten in den Domänen gesucht werden. Diese sind ein guter Indikator für eine niedrige Maturitätsstufe. Da wenig widerstandsfähige Unterstützungsprozesse eine Gefährdung für widerstandsfähige Kernprozesse darstellen, sollten nicht ausschliesslich auf Kernprozesse fokussiert werden.

Wie gut und schnell die Resilienzmaturität erhöht werden kann, hängt von den folgenden Erfolgsfaktoren ab:

Kultur ist ein Grundpfeiler für Resilienz, da im Zeitalter der Digitalisierung und Vernetzung Änderungen zum Alltag gehören. Mitarbeitende müssen befähigt und unterstützt werden, solche Änderungen aktiv mitzugestalten. Auch das Management muss umdenken: Resilienz steigern bedeutet, bewusst finanzielle Ineffizienzen in Kauf zu nehmen. Operationelle Prozesse, die bereits unter Normallast ihre Kapazitäten voll ausschöpfen, sind sehr anfällig für Störungen und gefährden damit das Unternehmen.

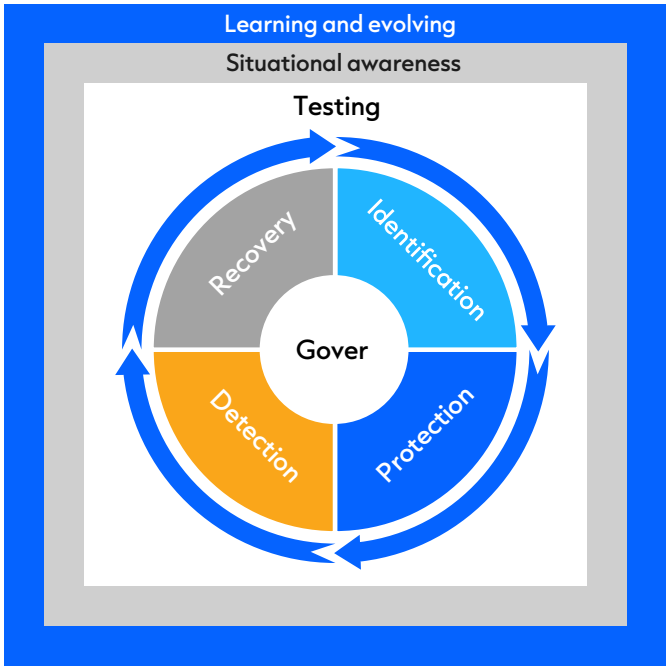
Führungsunterstützung ist aufgrund der weitreichenden Konsequenzen essenziell. Das Enterprise Risk Management bietet dafür einen direkten Anknüpfungspunkt. Angesichts der bewussten finanziellen Ineffizienzen müssen Massnahmen zur Steigerung der Resilienz durch die oberste Führung getragen werden.

Bei neuen **Vorhaben** muss die Resilienz von Anfang miteinbezogen werden. Schwächen in einzelnen Bereichen können sich aufgrund der engen Zusammenarbeit und komplexer Abhängigkeiten schnell auf das gesamte Unternehmen auswirken. Deshalb sind klare, unternehmensweite Kompetenzregelungen von zentraler Bedeutung. Mit langen Entscheidungswegen lässt sich die Resilienz oft nicht mehr gewährleisten.

Tests, Übungen und Überprüfung der Massnahmen sind wichtige Instrumente, um Resilienz im Ernstfall sicherzustellen. Vielfach werden Massnahmen nur formell erfüllt. Auf Stellvertretungen, die nur die notwendigsten Aufgaben erledigen können, oder Ersatzserver, die nicht auf dem aktuellsten Stand sind, kann im Ernstfall nicht zurückgegriffen werden. Der finanzielle Aufwand für entsprechende Tests lässt sich durch Automation und eine angemessene Periodizität reduzieren.

CROE Inspiration nicht nur für Finanz-marktinfra-strukturen

Hohe Sicherheitsstandards sind im Finanzmarkt Pflicht. In der Vergangenheit war es in der Regel ausreichend, Sicherheitsvorkehrungen auf regulierte oder kommerzielle Anwendungen zu beschränken, wie z. B. im Fall von SOX 404 oder der Zahlungskartenindustrie (Payment Card Industry, PCI).
Dominik Moser



Struktur CROE

Finanzmarktinfrastrukturen (FMI) bilden mit ihren Dienstleistungen für den Handel sowie die Abrechnung, Abwicklung und Verwahrung von Effekten das Rückgrat für einen effizienten und funktionsfähigen Kapitalmarkt. Zudem sind sie ein wesentliches Bindeglied für die internationale Vernetzung der Kapitalmärkte und des Kapitalverkehrs.

Aufgrund zahlreicher Attacken, die weit über den Diebstahl von Finanzzahlen und Zahlungskartendaten hinausgingen, wurden die Anforderungen an die operative Belastbarkeit und Integrität auf alle Systeme ausgeweitet. Abwehrmassnahmen, die sich auf den Perimeter beschränken, sind angesichts der zunehmenden Nutzung von Cloud- und IoT-Lösungen immer wirkungsloser. Ein ganzheitlich ausgerichtetes und nachhaltiges Cyberrisikomanagement wird dadurch unabdingbar. Bestehende Industriestandards und Best Practices unterstützen Unternehmen zwar beim Management von Cybersicherheitsrisiken.

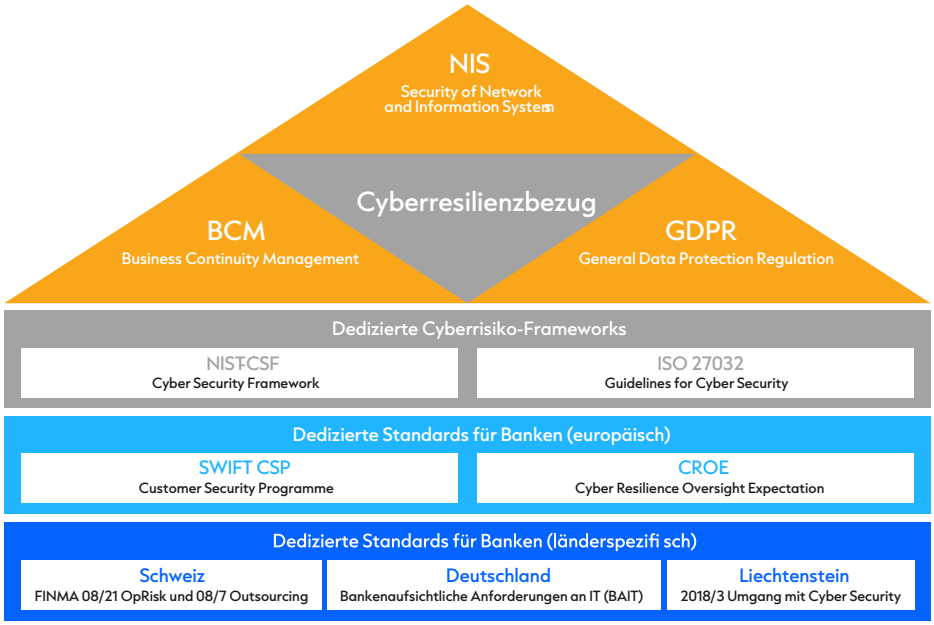
Das Kernproblem liegt jedoch in der Implementierung dieser Frameworks, da diese auf die Sicherheitsanforderungen der eigenen Branche und des eigenen Unternehmens abgestimmt werden müssen. Vor diesem Problem standen auch die Finanzmarktinfrastrukturen (FMI) im Eurosystem, als sie mit dem Leitfaden „Guidance on Cyber Resilience for Financial Market Infrastructures" konfrontiert wurden. Dieser wurde im Juni 2016 vom Ausschuss für Zahlungsverkehr und Marktinfrastrukturen (CPMI) und der International Organization of Securities Commissions (IOSCO) veröffentlicht. Das Europäische System der Zentralbanken reagierte auf den Wunsch nach konkreten Umsetzungshinweisen mit der Formulierung der Cyber Resilience Oversight Expectations (CROE). Dieses Framework definiert die Erwartungen der Aufsichtsbehörden an die Cyberresilienz.

CROE verfolgt im Wesentlichen drei Ziele:

- Konkrete Anleitungen, wie die formulierten Erwartungen umzusetzen sind, um zu einer nachhaltigen Cyberresilienz zu führen.
- Orientierungshilfen für die Aufsichtsbehörden, wie die FMI in ihrem Zuständigkeitsbereich zu beurteilen sind.
- Grundlagen für einen fundierten Dialog zwischen den FMI und ihren jeweiligen Überwachungsinstanzen.

CROE ist ein umfassendes, auf die kritischen Infrastrukturen im Finanzsektor ausgerichtetes Framework auf dem neuesten Stand. Es orientiert sich am NIST Cyber Security Framework (NIST-CSF). Das NIST-CSF hat einen generischen, branchenübergreifenden Charakter und erfordert deshalb eine branchen- und unternehmensspezifische Anpassung. Im Rahmen der Konkretisierung legt CROE grossen Wert auf Governance und Kulturwandel, welche im Bankensektor einige Besonderheiten aufweisen.

Allgemein kann man den Bezug zwischen dedizierten Frameworks wie CROE in einer hierarchischen Ordnung sehen: Von allgemeinen globalen Anforderungen mit gemeinsamen Bezug zu Cyberresilienz (CRS) über dedizierte globale Cyberrisiko-Frameworks (NIST-CSF und ISO-27032) bis hin zu branchen- und länderspezifischen Ausprägungen der Cybersicherheit, welche schlussendlich in die unternehmensspezifische Umsetzung münden.



Verschiedene neue Regularien sind in Bearbeitung bzw. in den letzten Jahren in Kraft gesetzt worden. In der Schweiz beispielsweise das FINMA-Rundschreiben 08/21 „Operationelle Risiken - Banken" Umgang mit Cyberrisiken (unter dem Grundsatz 4, Technologieinfrastruktur). Das ist nur der Anfang. Es ist davon auszugehen, dass kurzund mittelfristig nationale und internationale Behörden den Rahmen zur Anwendung noch enger stecken werden. Die Folge sind regelmässige Prüfungen zur Einhaltung durch behördliche Instanzen.

Schlüsselstandards der Cyberresilienz

Wer sollte CROE umsetzen und was können andere aus diesem Framework lernen?

CROE ist die konkrete Ausgestaltung verschiedener Frameworks für das (kleine) Segment der Finanzmarktinfrastrukturen, wie z. B. NIST-CSF. Daher ergibt eine komplette, dogmatische Umsetzung von CROE für andere Branchen wenig Sinn.

Wichtig ist die Erkenntnis aus der Praxis, dass das Abstützen auf ein branchenspezifisches Framework gegenüber der Adaption eines Frameworks wie ISO-27032 oder NIST-CSF an das eigene Unternehmen vorzuziehen ist. CROE liefert wertvolle Hinweise, wie eine solche Ausgestaltung aussieht und auf welcher Detaillierungsstufe sie sich bewegt.

In Umsetzungsprojekten hat sich gezeigt, dass viele Diskussionen über den Sinn und Zweck einer Einzelmassnahme vermeidbar sind, wenn diese als Teil eines Frameworks präsentiert wird. Insbesondere das Risiko einer unausgewogenen praktischen Umsetzung, bei der etwa technische Massnahmen überbetont und die Governance vernachlässigt werden, lässt sich so reduzieren. Zudem schafft ein Framework ein ausgewogenes Verhältnis zwischen präventiven und reaktiven Massnahmen. Dies erhöht nicht nur die Schwelle für einen erfolgreichen Angriff, sondern etabliert auch Systeme und Fähigkeiten, um Vorfälle rasch zu erkennen und darauf zu reagieren. Ein weiterer entscheidender Vorteil ist die strategische Steuerung des Umsetzungsprogramms, welche durch das periodische Überprüfen der Gaps zum Framework erreicht werden kann.

Ähnliche Frameworks existieren auch in anderen Branchen, darunter z. B. das Handbuch „Grundschutz für Operational Technology in der Stromversorgung" des Verbandes Schweizerischer Elektrizitätsunternehmen. Ein Standard mit dem Konkretisierungsgrad von CROE fehlt jedoch in vielen Branchen nach wie vor. Hier könnten unternehmensübergreifende Initiativen – eventuell unterstützt durch Branchenorganisationen oder Regulatoren – schnell Abhilfe schaffen. Anstelle einer unternehmensspezifischen Ausgestaltung würde dann zunächst ein Branchenstandard wie CROE definiert. Dieser böte aufgrund der breiten Abstützung weniger Angriffsfläche, sobald die Umsetzungsmassnahmen konkret und damit teuer werden.

Empfohlenes Vorgehen bei der Umsetzung von CROE

CROE ist kein „One size fits all"-Ansatz für das Management von Cybersicherheitsrisiken. Unternehmen sind weiterhin einzigartigen Risiken ausgesetzt, da sie unterschiedliche Schwachstellen und unterschiedliche Risikotoleranzen haben. Entsprechend müssen auch die Praktiken im Framework vor der Umsetzung unternehmensspezifisch angepasst werden. Unternehmen können Aktivitäten festlegen, die für das Bereitstellen kritischer Services wichtig sind, und Investitionen priorisieren, um deren Wirkung zu maximieren. Letztendlich zielt das Framework darauf ab, Cybersicherheitsrisiken zu reduzieren und die Cyberresilienz fortlaufend zu verbessern.

Open Banking als Chance Resilienz für den Schweizer Finanzplatz

Von den Banken wird seit jeher eine hohe Resilienz erwartet. Früher stellten dicke Tresortüren die Integrität einer Bank und der ihr anvertrauten Werte sicher, während heute vermehrt aufwändige Massnahmen im Bereich der Cyber Security die digitalen Tresore schützen. Regulatoren stellen ausserdem Vorschriften auf, die darauf abzielen, die Resilienz der Banken auch in Krisenzeiten zu gewährleisten.

Dr. Pascal Bettendorff, Stephan Gerber

Open Banking

Open Banking nutzt ein kollaboratives Modell, das Finanzinstituten ermöglicht, dem Markt über APIs erweiterte Funktionen zum Austausch von Bankinformationen zur Verfügung zu stellen. Diese Funktionen erlauben Drittanbietern, Anwendungen und Dienste rund um das Finanzinstitut zu entwickeln und so nicht nur dem Bankkunden höhere finanzielle Transparenz zu bieten, sondern auch den Finanzinstituten neue Geschäftsmodelle oder Zusatzdienstleistungen bereitzustellen.

Zurzeit werden traditionelle Banken zusätzlich von einer Bedrohung ganz anderer Art unternehmerisch herausgefordert: Technologiekonzerne und Neobanken aus dem europäischen Raum drängen als neue Player mit innovativen Bankinglösungen in den Schweizer Markt und beeinträchtigen das Kerngeschäft. Klassische Banken haben kaum Chancen, mit der Agilität und den Freiheiten dieser neuen Mitbewerber Schritt zu halten, und müssen daher neue Ansätze finden, um wettbewerbsfähig zu bleiben.

Open Banking bietet Banken eine Chance, ihre hochkomplexen und spezialisierten IT-Landschaften zu öffnen und gemeinsam mit Drittanbietern zukunftsweisende digitale Services anzubieten. Auf diese Weise können traditionelle Banken neue Geschäftsfelder erschliessen, von den Stärken ihrer neuen Mitbewerber profitieren und zugleich eigene Stärken einbringen.

Was verändert sich durch Open Banking?

Die Entwicklung digitaler Dienstleistungen und Ökosysteme führt häufig zu einer Zusammenarbeit mit neuen Partnern, nicht selten auch mit jungen, innovativen Startups. Dabei kollidieren unterschiedliche Unternehmenskulturen, was sich negativ auf die operative Resilienz auswirkt. Betrachtet man die Dimensionen der Operating Models der beiden Partner, werden diese Unterschiede deutlich.

Menschen und Skills

Ein Start-up beschäftigt andere Menschen mit anderen Skills als eine Bank. Das Produkt und die Technik stehen hier klar im Vordergrund. Wichtig ist, die Kunden mit innovativen Ideen zu begeistern. Weitere Kundeninteressen werden diesem Ziel rigoros untergeordnet. Flexibilität und hohe Anpassungsfähigkeit sind für ein innovatives Unternehmen selbstverständlich, können Bankmitarbeitende und -kunden jedoch überfordern. Kleine Start-ups können nicht nachvollziehen, wie massiv minimale Anpassungen an internen Tools die Effizienz Hunderter oder Tausender Mitarbeitender beeinträchtigen und zu unverhältnismässigen Einführungskosten führen können. Im Gegensatz dazu kann sich eine Bank nicht erlauben, auf grosse bestehende Kundengruppen einfach zu verzichten, indem sie breite Zugangskanäle oder umsatzstarke Produkte ohne Alternative einstellt. Am Ende zeigt der durchschnittliche Kunde viel weniger Toleranz für falsche Kontoauszüge, Fehlbuchungen oder Kontosperrungen, als das Start-up annimmt.

Eine klare Schnittstelle zwischen der Bank und dem finanzfremden Dienstleister ist deshalb sinnvoll. Zusätzlich hilft auch eine laufende Neujustierung der fundamentalen Kerntätigkeiten (Schutz der Kunden-Assets) und des sie umgebenden Mantels von Leistungen mit Added Values, welche viel einfacher durch Partner erbracht werden können. Sowohl die Innovation als auch das klassische Prozessdenken der Bank müssen verstanden und miteinbezogen werden. Innovationsaffine Mitarbeitende in der Bank dienen dabei als Brücke zwischen den beiden Welten.

Organisation und Governance

Organisation und Governance könnten nicht unterschiedlicher sein. Im „Start-up-Groove" entwickeln junge Teams agil und selbstorganisiert innovative Lösungen ohne schwerfälligen organisatorischen Überbau. Das Management ist voll in die Entwicklung integriert und besitzt vielfach ein umfassendes technisches Know-how. Dem gegenüber steht die Organisation etablierter Bankinstitute mit ihren klaren Prozessen und Führungsstrukturen. Regulative, juristische und finanzielle Vorgaben sind omnipräsent und beeinflussen die Prozessabwicklung erheblich.

Um die Stärken beider Organisationen zu vereinen, kann die Governance nicht nur auf Verträgen und SLA basieren, da das Start-up dadurch seiner Vorteile beraubt würde. Den Inhalt des gemeinsamen Kundenerlebnisses soll die Organisation bestimmen. Dabei muss allen Beteiligten bewusst sein, dass die inhaltliche Verantwortung gegenüber dem Kunden bei der Bank bleiben muss. Daraus ergeben sich viele konkrete organisatorische Konsequenzen, wie beispielsweise die Datenhoheit.

Technologie und Information

In der Dimension Technologie und Information sind Schnittstellen ein zentrales Element. Die stark abgeschotteten, teilweise etwas veralteten, aber hochstabilen und effizienten Anwendungen der Banken müssen gegenüber

modernen, oft Cloud-basierten Systemen geöffnet werden. Über technische Schnittstellen lassen sich Daten und Informationen mit den neuen Partnern austauschen. Jede Öffnung birgt jedoch potenzielle Risiken für Cyberangriffe und führt zu neuen technischen Abhängigkeiten.

Häufig kollidieren auch unterschiedliche Entwicklungsprozesse. Innovative Unternehmen bringen Neuerungen so rasch wie möglich zu den Benutzern. Dies kann eine Bank mit komplexem Releasemanagement rasch überfordern. Zudem haben Bankkunden wenig Verständnis für regelmässige wartungsbedingte Ausfälle ihrer digitalen Banking-Services, wie beispielsweise eBanking. Integrationen müssen daher mit dem Bewusstsein entwickelt werden, dass jeder extern bezogene Service grundsätzlich jederzeit ausfallen kann. Ähnlich wie bei den Zero-Trust-Konzepten in der Cyber Security ist deshalb eine Abkehr von Höchstverfügbarkeitsanforderungen sinnvoll. „Chaos Testing" der IT und der Businesskontinuität verankert dieses neue Credo in der Organisation.

Technische Komponenten müssen so konzipiert werden, dass sie ohne Abhängigkeiten von externen Services funktionieren. Verliert ein System etwa den Zugang zu Echtzeitdaten, müssen lokale Daten zur Näherung vorliegen.

Eine übersichtliche Servicearchitektur basiert auf flexiblen Schnittstellen und ermöglicht einen raschen Austausch von technischen Komponenten. Mithilfe von Microservices werden Anwendungen modular gestaltet, bis hin zum Ideal des unterbruchfreien Deployments – obwohl dieser Idealzustand nicht immer gewünscht ist. So dürfen börsenrelevante Informationen oder Finanzdaten im Rahmen eines rollenden Deployments niemals nur einem Teil der Nutzer zugänglich sein. API-Management erlaubt eine einfache Integration von Partnern, mit sauber versionierten Schnittstellen und aufeinander abgestimmten Anpassungen.

Partnerschaften

Jungunternehmen stehen finanziell vielfach auf wackligen Füssen. Sie werden schnell gegründet und bei ausbleibendem Erfolg ebenso schnell wieder liquidiert. Man darf nicht voraussetzen, dass solche agilen Unternehmen als Partner längerfristig zur Verfügung stehen. Gerade in einer Anfangs- oder Wachstumsphase sind Verluste normal. Zudem kommt es vor, dass ein ehemals „heisses" Start-up von noch innovativeren Unternehmen überholt wird.

Entsprechend stellt sich im Open Banking permanent die Frage nach Multi-Vendor-Strategien. Bei jeder Partnerschaft muss sorgfältig evaluiert werden, welche Skills parallel zur Partnerschaft intern oder durch andere Partner aufgebaut werden sollen. Dies gilt es über Know-how-Management und eine entsprechende Ausbildung zu adressieren.

In jeder Zusammenarbeit stellt sich zudem die Frage nach dem geistigen Eigentum. Falls dieses nicht bei der Bank liegt, sollte über Escrow-Mechanismen zumindest der Zugriff auf technische Komponenten oder Schnittstellendokumentationen bei einem Totalausfall im Vorfeld geregelt werden.

Um die Zusammenarbeit zu stabilisieren und partnerschaftlich auszugestalten, empfiehlt sich vor allem bei jungen Unternehmen das Anbieten eines Businesscoachings. Dies ermöglicht eine nähere Steuerung als beispielsweise eine Aufsicht über einen VR-Einsitz.

Geschäftsprozesse

Start-ups ändern erfolglose Geschäftsprozesse und -modelle rasch, da sie nicht entlang etablierter Wertschöpfungsketten funktionieren, sondern bewusst versuchen, diese aufzubrechen oder neu zu gestalten. Genau wie KMU agieren auch Start-ups in anderen Zyklen als traditionelle Banken. Dies erschwert gemeinsame Entscheidungen.

Die Bank muss jederzeit auf geänderte Prozesse ihrer Partner reagieren können. Schlanke, sauber dokumentierte Abläufe und gut geschulte Mitarbeitende erhöhen die Reaktionsfähigkeit in solchen Fällen. Zugleich muss die Bank in der Lage sein, fehlende Beistellungen zu kompensieren, und beispielsweise Schulungen oder die Erstellung von Handbüchern selbst übernehmen. Das Beharren auf vertragliche Abmachungen führt hier grundsätzlich weniger zum Ziel, als spontan die „Ärmel hochzukrempeln".

Möchte eine Bank von den enormen Chancen des Open Banking profitieren, muss sie die aus den Partnerschaften entstehenden Risiken identifizieren und unter Kontrolle bringen. Bereits mit einem funktionierenden Release-Management können beispielsweise technische und prozessuale Risiken angegangen und reduziert werden.

Wichtig ist, alle Massnahmen so auszurichten, dass eine graduelle Degradation von Services bei einer Störung in einer Dimension des Operating Model erfolgt. Dadurch kann die gesamte IT-Landschaft ähnlich zuverlässig funktionieren wie ein Bancomat, der im Störungsfall lediglich einzelne Funktionen deaktiviert und dadurch konstant den maximal möglichen Kundennutzen bietet.

Zukunftskompetenz Ein Interview zum Thema Resilienz mit Dr. Thomas Rhomberg

SIX ist das Rückgrat des Schweizer Finanzplatzes und steht als zentrale Infrastrukturanbieterin seit 2008 für Innovation und Stabilität auf den weltweiten Finanzmärkten. Dr. Thomas Rhomberg, Head of Security Operations & Transformation von SIX, erläuterte im Interview mit Adrian Anderegg und Dr. Adrian Marti von Eraneos, wie SIX mit dem Thema Resilienz umgeht und wie das Unternehmen seinen heutigen Status in dieser erfolgskritischen Domäne erreicht hat.

Dr. Adrian Marti, Adrian Anderegg

Herr Dr. Rhomberg, wie grenzt SIX den Begriff Resilienz ab?

Thomas Rhomberg: Resilienz geht bei SIX ganz klar über Business Continuity Management (BCM) hinaus. Ich sehe diese als nächsten Entwicklungsschritt, da Resilienz neben dem planerischen Element des BCM auch weitere Managementdisziplinen integriert, wie beispielsweise das Krisenmanagement. Widerstandsfähigkeit als Begriff gefällt mir in diesem Kontext gut. Ein umfassender Ansatz, um die Domäne Resilienz voranzutreiben, ist das Risikomanagement.

Wichtige Faktoren für die Resilienz sind einerseits das wirtschaftliche Ökosystem eines Unternehmens. Dazu gehören Lieferanten und Kunden ebenso wie Ereignisse, welche die Sicherheit oder Geschäftskontinuität als „Third-Party Risk" beeinträchtigen. Anderseits spielt die Fähigkeit, sich in einem volatilen und disruptiven Geschäftsumfeld weiterzuentwickeln, eine zentrale Rolle. Zudem sollte Resilienz auch aus der Perspektive der Organisationspsychologie des Menschen und damit auf Ebene der Mitarbeitenden betrachtet werden.

Für mich ist Resilienz aber keine reine Sammlung von klassischen Fähigkeiten, sondern vielmehr eine intrinsische Eigenschaft einer Organisation, so wie Compliance, Liquidität oder Governance. Eine Organisation soll nicht resilient aufgestellt werden. Resilienz soll vielmehr der Sinn und Zweck der Organisation sein.

Was tut SIX, um resilient zu sein?

Wir haben in den letzten Jahren ein eigenes Security Operations Center (SOC) aufgebaut. Dabei haben wir von Anfang an den Gedanken verfolgt, die erbrachten Services auch unseren Kunden anzubieten, da nicht jede Organisation selbst einen solchen „Schutzschirm"-Service betreiben kann. So können wir neben unserer eigenen Resilienz auch die Resilienz des Ökosystems, dem SIX angehört, widerstandsfähiger machen und einen klaren Mehrwert für den Finanzmarkt generieren.

Zur Sicherstellung der internen Resilienz haben wir bei der Governance klare Zuständigkeiten und betreiben ein Risikomanagement, das die Oversight-Erwartungen im Hinblick auf die Cyberresilienz berücksichtigt und damit Treiber und Katalysator ist für notwendige Veränderungen im Hinblick auf eine sichere und verfügbare IT. Zusätzlich ist für uns in diesem Zusammenhang auch das Management eines robusten Kontroll-Frameworks sehr wichtig.

Resilienz ist mit viel Aufwand verbunden. Welche Treiber haben die Resilienz von SIX auf den heutigen Stand gebracht?
SIX ist ein Gemeinschaftswerk und eine Infrastrukturdienstleisterin für den Finanzmarkt. Von diesem Grundauftrag leitet sich unser primäres Bestreben ab, die Resilienz weiterzuentwickeln und bestehende Prozesse laufend robuster zu machen. Das ist auch der direkte Mehrwert, den wir generieren. Nur so können wir ein verlässlicher und hochverfügbarer Partner sein, dem man kritische Elemente der gemeinsam Wertschöpfungskette anvertraut. Wir bezeichnen uns auch als kritische Infrastruktur für den Finanzmarkt und wollen als resilientes Unternehmen bewusst zu dessen Stabilität beitragen, da der Finanzmarkt einen Teil unserer Volkswirtschaft darstellt, der nicht ausfallen darf.

Konkret ist das Risikomanagement, also unsere Fähigkeit, Risiken zu identifizieren, zu beurteilen und daraus adäquate Massnahmen abzuleiten, der Haupttreiber. Zudem ist Resilienz in unserem Umfeld eine implizit gehegte Erwartung und manchmal sogar eine konkret adressierte Kundenanforderung. Letztendlich kommt der Antrieb für Resilienz auch aus der Geschäftsstrategie, in welcher Change und Wandel eine zentrale Rolle spielen. Denn Transformation im Sinne der Fähigkeit, die eigene Organisation und das Geschäftsmodell jederzeit flexibel anzupassen, wird in zunehmendem Masse erfolgskritisch. Die treibenden Kräfte hinter der Resilienz sind bei SIX somit ein Zusammenspiel verschiedener Elemente, die gemeinsam zum erreichten, ganzheitlichen Status der Resilienz führen.

Sie haben aus der Pflicht, resilient zu sein, einen Service gemacht, woraus sich dank ihrem SOC auch ein neues Geschäftsfeld für SIX entwickeln kann.
Resilienz ist meines Erachtens keine Pflicht, sondern ein Bestreben, mit dem wir bei SIX proaktiv umgehen. So sind wir auch das Thema Cyber Security vor rund vier Jahren proaktiv angegangen und haben uns gefragt, welche Fähigkeiten wir aufbauen müssen, um für künftige Herausforderungen besser gewappnet zu sein. Das SOC ist ein Beispiel dafür, wie aus diesem Streben letztendlich eine Geschäftsopportunität erwachsen ist.

Wo sollte die Verantwortung für die Resilienz angesiedelt sein?
Sofern die Resilienz von zentraler Stelle getrieben sein soll, ist die Verantwortung dafür am besten in einer Risikoorganisation aufgehoben. Da Resilienz jedoch unterschiedliche Ausprägungen hat, sollte sie vorzugsweise einen dezentralen Ansatz verfolgen. Einzelne Fähigkeiten, Domänen und Organisationsteile mit spezifischen Leistungsmerkmalen, leisten einen Beitrag zur organisationalen Resilienz. Deshalb ist diese für mich eher ein Bottom-up-Approach als ein reiner Top-down-Ansatz.

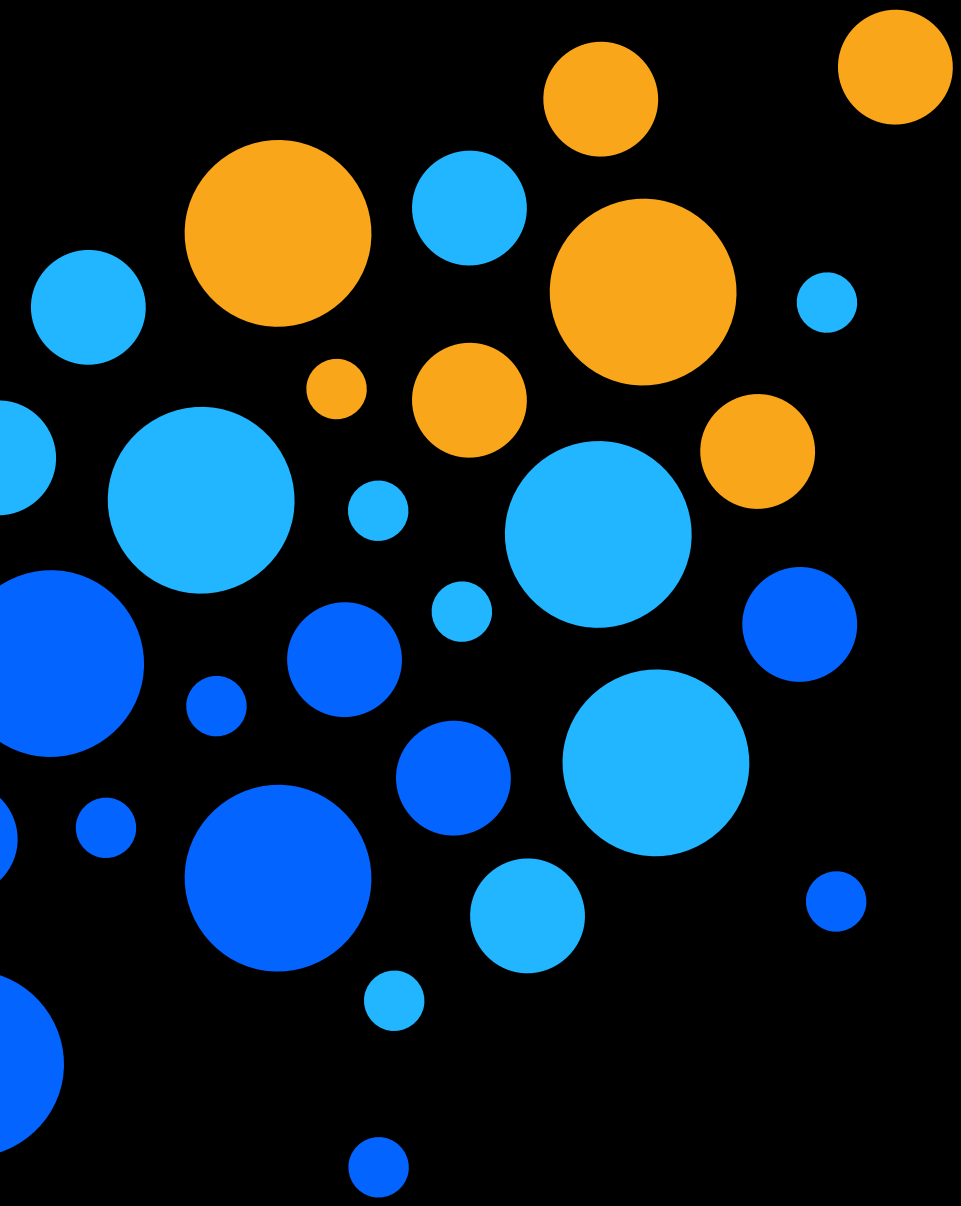
Was möchten Sie der Leserschaft mitgeben zum Thema Resilienz?
Ich empfehle jedem Unternehmen, das in ein Ökosystem von Stakeholdern jeglicher Ausprägung eingebunden ist, im Rahmen der Resilienz auch über die Nachhaltigkeit Überlegungen anzustellen und über die eigene Organisationsgrenzen hinauszudenken. Denn viele Probleme sind heute nur noch gemeinsam über Partnerschaften oder Allianzen lösbar. Das ist die systemische Perspektive hinter dem Thema Resilienz, die mit einbezogen werden sollte. SIX tut dies bereits und hat beispielsweise mit anderen systemrelevanten Organisationen eine Szenarioanalyse zu wichtigen Trends im Bereich der Geschäftskontinuität durchgeführt, um den Resilienzgedanken gemeinsam voranzutreiben.

FinTech „Made in Switzerland"

SIX betreibt und entwickelt systemrelevante Infrastrukturdienstleistungen in den Geschäftseinheiten Securities & Exchanges, Banking Services und Financial Information mit dem Ziel, die Effizienz, Qualität und Innovationskraft entlang der gesamten Wertschöpfungskette des Schweizer Finanzplatzes zu erhöhen. SIX befindet sich im Besitz ihrer Nutzer (120 Banken) und erwirtschaftete 2018 mit rund 2600 Mitarbeitenden und einer Präsenz in 20 Ländern einen Betriebsertrag von über 1,9 Milliarden Schweizer Franken sowie ein Konzernergebnis von 221,3 Millionen Schweizer Franken.

www.six-group.com

eraneos



Experienced in a wide range of industries

Eraneos Group ist eine internationale Management- & Technologieberatungsgruppe, die Dienstleistungen von Strategie bis Implementierung anbietet. Sie ist aus dem 2021 angekündigten Zusammenschluss von Ginkgo Management Consulting, Quint Group und AWK Group hervorgegangen. Die Gruppe betreut Kunden auf drei Kontinenten, wo rund 1.000 engagierte und hochqualifizierte Fachleute gemeinsam daran arbeiten, das volle Potenzial der Digitalisierung auszuschöpfen. Die Dienstleistungen reichen von der Entwicklung digitaler Geschäftsmodelle und Datenanalysen bis hin zu Cybersicherheit, von Sourcing und IT-Beratung zum Management komplexer Transformationsprojekte. Eraneos Group hat Niederlassungen in der Schweiz, Deutschland, Luxemburg, Spanien, den Niederlanden, China, Singapur und den USA. 2021 erzielte die Gruppe einen Umsatz von fast 200 Millionen Euro.

Contact us >

Our offices >

Visit our website >