Resilienz als Schlüsselfähigkeit im Krisenfall

Fazitbericht | 6. FSS Security Talk vom 10. September 2020, Webinar

In der VUCA-Welt (Volatility, Uncertainty, Complexity, Ambiguity) haben sich die Auslöser von Ausfällen und Störungen multipliziert. Resilienz ist als Sicherheitskonzept nebst klassischem Risikomanagement für das Überleben vernetzter Systeme notwendig. Die Referierenden waren sich einig, zum Erhalt und Aufbau von Resilienz in Organisationen sind insbesondere weiche Faktoren entscheidend.

Rund 80 Interessierte fanden sich zum 6. FSS Security Talk ein, der vom FORUM SICHERHEIT SCHWEIZ (FSS) zusammen mit der AWK Group organisiert wurde. Passend zum Thema fand erstmals ein FSS Security Talk online als Webinar statt, die Covid-19-Situation hatte die Verschiebung des Anlasses und Verlegung in den digitalen Raum notwendig gemacht. Nach einer kurzen Begrüssung durch Fredy Müller, Geschäftsführer des FSS, wurde das Wort an die Referierenden übergeben, die aus der Schweiz, Italien und – im Falle von Nationalrätin Judith Bellaïche – gar aus dem Bundeshaus zugeschaltet waren.

Resilienz als Antwort auf die Komplexitätsfrage

In seinem Einstiegsreferat erläuterte **Dr. Benjamin Scharte**, Head des Risk and Resilience Research Team am Center for Security Studies (CSS) der ETH Zürich, die Konzepte von Komplexität und Resilienz und ihren Zusammenhang aus wissenschaftlicher Sicht. Am Beispiel der Bildung eines Staus auf der Autobahn zeigte Dr. Scharte die wichtigste Eigenschaft **komplexer Systeme** auf, **Emergenz**: In komplexen Systemen lassen sich Ergebnisse nicht aus dem Verhalten der einzelnen Bestandteile des Systems erklären, sondern erst auf Ebene des Gesamtsystems. Ein Stau entstehe eben häufig nicht, weil ein einzelner Fahrer einen Unfall verursache, sondern es seien kleine Abweichungen im individuellen Verhalten jedes Fahrers, die sich zum Stau addierten.

Die zweite wichtige Eigenschaft von komplexen Systemen ist **Unsicherheit**. Es braucht daher **Strategien**, wie man mit dieser **Unsicherheit umgehen** kann, womit der Bogen zur Resilienz gespannt ist. Mit Resilienz sei aber nicht die schlichte Rückkehr in einen Ausgangszustand gemeint. Das **Stehaufmännchen** sei daher **kein gutes Bild**, um Resilienz zu erklären. Stattdessen brauche es gemäss Dr. Scharte ein **systemisches Resilienz Verständnis**: Resilienz ist die Fähigkeit, auf **Veränderungen**, besonders unerwartete, **zu reagieren** und sich diesen **anzupassen**.

Quelle: Präsentation Dr. Scharte

Da komplexe Systeme **immer komplexer** werden, müssen wir mit immer mehr unerwarteten, disruptiven Ereignissen umgehen. Resilienz wird immer notwendiger. **Komplexität** sei aber nicht nur Treiber, sondern auch **Voraussetzung für Resilienz**. Denn nur komplexe Systeme können sich anpassen, wenn sie mit unerwarteten Ereignissen konfrontiert werden. Resilienz-erhöhende Systemprinzipien sind dabei Modularität, Diversität, Dezentralität und Redundanz.

Resilienz als Sicherheitskonzept für Organisationen

Dr. Adrian Marti, Leiter Bereich Cyber Security und Privacy bei der AWK-Group, ergänzte diese wissenschaftliche Perspektive im zweiten Einstiegsreferat um Erfahrungen aus der Praxis. Dr. Marti nannte vier Gründe, weshalb Resilienz für Unternehmen und Organisationen der öffentlichen Hand ein immer wichtigeres Thema werde: Erstens sind solche Organisationen immer mehr **in Ökosysteme eingebettet** und abhängig von anderen Organisationen in der Wertschöpfungskette. Zweitens ist Resilienz ein **Marktbedürfnis**, Kunden erwarten in gewissen Segmenten die unterbruchsfreie Leistung einer Dienstleistung. Drittens macht in manchen Segmenten der **Regulator** Vorschriften zur Resilienz. Und viertens nimmt gerade im Cyber-Umfeld die **Qualität der Bedrohungen** zu. Es könne daher nicht mehr darum gehen, einen Angriff abzuwehren, sondern sich möglichst rasch von einem erfolgreichen Angriff zu erholen.

In einer neuen Studie der AWK Group zu **Cyber Security** gaben entsprechend **70% der befragten Organisationen** an, dass für sie Cyber Security ein **Differenzierungsmerkmal** am Markt sei. Jedoch betrachteten nur **20% der Organisationen** ihre Cyber-Resilienz **Fähigkeiten als ausreichend**. Es bestehe also, so Dr. Marti, ein **eklatanter Widerspruch** zwischen der Wichtigkeit des Themas und dem erreichten Vorbereitungsstand. Die Frage sei also, wie Organisationen resilienter werden können.

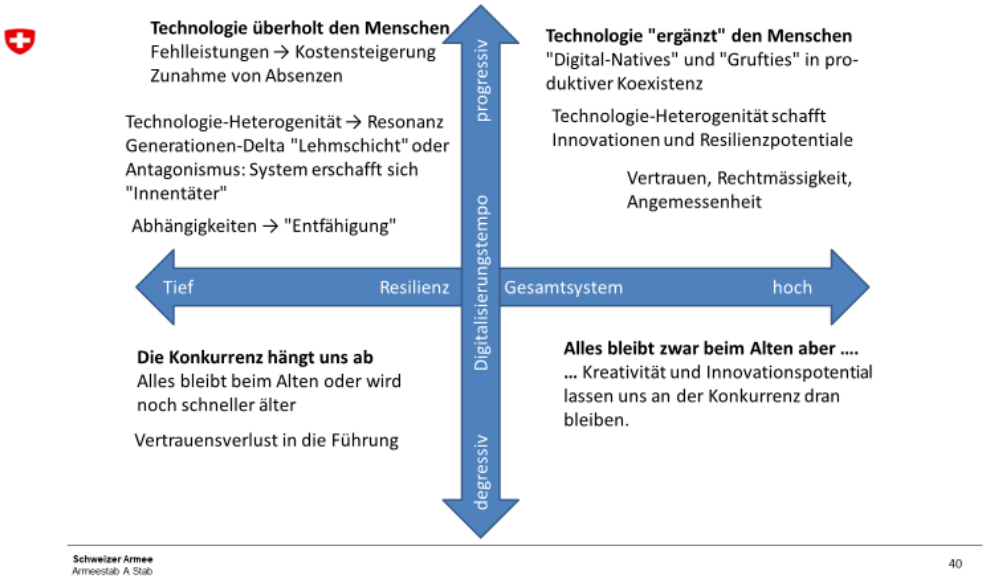
Um Resilienz zu fördern, steht Organisationen laut Dr. Marti ein ganzer **Baukasten an Konzepten** zur Verfügung. Entscheidend für den Aufbau und Erhalt von Resilienz sind dabei insbesondere weiche Faktoren: die **Kultur**, die **Führung** und die **Agilität** der Organisation. Resilienz müsse von Beginn weg bei der Gestaltung von Prozessen und Systemen eingebaut werden und auch **über Unternehmensgrenzen hinweg** aufgebaut werden. Schliesslich bedürften die eigenen Resilienz Konzepte einer **regelmässigen Überprüfung**. Letztlich müsse jede

Organisation aber selbst entscheiden, wie viel Resilienz sie benötigt. Je **zeitkritischer und austauschbarer** die eigenen Dienstleistungen sind und je mehr **öffentliche Aufmerksamkeit** der eigenen Organisation gilt, desto mehr Resilienz werde benötigt. Der wichtigste Erfolgsfaktor sei jedoch, dass Resilienz auf **allen Entscheidungsebenen täglich** thematisiert werde.

Quelle: Präsentation Dr. Marti

Menschliche und soziale Bedürfnisse mit technologischen in Einklang bringen

Im ersten Case der Veranstaltung ging **Dr. Martin Krummenacher,** KPM Doktrinforschung im Armeestab, auf Resilienzpotentiale im soziotechnischen System der **Schweizer Armee** ein. Für Dr. Krummenacher wird Resilienz nicht trotz, sondern **wegen widriger Umstände** entwickelt. Sie entsteht in einem nacheilenden Prozess und hat einen Lerneffekt für die ganze Organisation. Resilienz kann also als **Produkt eines gelungenen Risikomanagements** betrachtet werden. In Bezug auf die Schweiz betrachtete er insbesondere den **Föderalismus als resilienzerhöhende Systemeigenschaft.**



Quelle: Präsentation Dr. Krummenacher

Anhand eines Szenariokreuzes zeigte Dr. Krummenacher die Auswirkungen eines hohen Entwicklungstempos der Digitalisierung auf Organisationen mit tiefer Resilienz auf. Die Folge waren **Stresserkrankungen** und **Bruchlinien durch Generationen** bis hin zur mutwilligen Sabotage durch Innentäter. Es brauche daher im Zuge der Digitalisierung einen geführten Prozess und eine integrale auf Resilienz ausgerichtete Kultur, die darauf abzielt, dass **Technologie den Menschen ergänzt** und nicht ersetzt. Eine Möglichkeit dazu würden sogenannte **«Offline-Days»** bieten, Tage, an denen ein Teil der Firma gezwungen wird, konventionell zu arbeiten. Dabei wurde sichtbar, dass die Digital Natives auf die **Erfahrung der «Grufties»** angewiesen waren. Oft entstanden an solchen Offline-Days Innovationen und Resilienzpotentiale und Ängste vor der Digitalisierung wurden abgebaut.

Bei der Forschung der Schweizer Armee zu Resilienz in Krisensituationen zeigte sich, dass häufig **weiche, psychologische Faktoren** die **robustesten Elemente** waren, die zur Bewältigung von kritischen Situationen beigetragen haben. Besonders Überreglementierung und die Einmischung der Führung von aussen schienen resilienz-zersetzend zu wirken. Insgesamt zeigte sich in Bezug auf die Digitalisierung, dass **resilienz-zersetzende Elemente digitalisierungsfördernd** sind und umgekehrt resilienz-fördernde Elemente hinsichtlich einer gelingenden Digitalisierung kritisch sind, z.B. Dezentralität und die Selbststeuerung von Gruppen. Dieses Spannungsfeld gelte es zu beachten, so Dr. Krummenacher, und **menschliche und soziale Bedürfnisse mit technologischen in Einklang** zu bringen.

Auch als KMU kann man resilient und sicher aufgestellt sein

Im zweiten Case zeigte **Martin Leuthold,** Leiter der Abteilung «Security & Network» bei Switch, wie Switch Resilienz und Cyber-Security für den Betrieb kritischer Infrastrukturen schafft. Switch wurde als Service-Provider und Selbsthilfeorganisation der Schweizer Hochschulen eingerichtet und ist heute eine gemeinnützige Stiftung getragen von Bund und Kantonen. Als KMU betreibt Switch heute **drei nationale kritische Infrastrukturen**: Die DNS-Infrastruktur für .ch und .li, das Schweizer Forschungsnetzwerk und das nationale Multisektor-Computer Emergency Response Team (CERT).

Quelle: Präsentation Martin Leuthold

Am Beispiel des **Schweizer Forschungsnetzwerks** zeigte Herr Leuthold die vielfältigen Massnahmen auf, die für den sicheren und resilienten Betrieb kritischer Infrastrukturen nötig sind. Switch mietet einzig Glasfaserleitungen und besitzt sonst alle Kompetenzen sowie das technische und Betriebs-Know-how In-House. Der Aufbau des Forschungsnetzwerks ist geprägt von **Redundanzen**. Es bestehen ca. 3'000 km Glasfaserleitungen und mindestens drei unabhängige Webe in die Nord-Süd und Ost-West Richtung, sodass **kein Single-Point-of-Failure** besteht. Die Anbindung ans Ausland ist mit fünf Internet Exchange Points sichergestellt. Alle Hochschulen sind mit zwei geographisch redundanten Glasfaserleitungen ans Netzwerk angeschlossen. Switch betreibt weiter **zwei unabhängige Data Center** in Zürich und Lausanne. Zudem hält Switch grosse **Bandbreitenreserven** auf allen Ebenen bereit, welche selbst den Lastwechsel durch die vollständige Umstellung auf **Fernunterricht** im Frühling bewältigen konnten. Ausserdem hält Switch eine minimale **Autarkie** in Bezug auf Ersatzmaterial aufrecht und schafft über einen **kooperativen Betriebsansatz** mit den Hochschulen organisatorische Resilienz.

Die **DNS-Infrastruktur** stellt das kritische Element für die **Domain-Registry** dar. Sie übersetzt alle Internet-Adressen in IP-Adressen, bei einem Ausfall wäre keine .ch- oder .li-Adresse mehr erreichbar. Die DNS-Infrastruktur nutzt alle diese Resilienzen in der Basis-Infrastruktur und wird von Switch selbst betrieben. Sowohl das Forschungsnetzwerk als auch die Domain-Registry profitieren von der dritten kritischen Infrastruktur, dem **Multisektor-CERT**, welches die interne Fähigkeit für Krisenbewältigung sicherstellt. Insgesamt zeigt sich, dass auch ein **KMU resilient und sicher** aufgestellt sein kann, wenn es **kritische Dienstleistungen** erbringt.

Technologie ist nur ein Baustein für Resilienz

Zum Abschluss gab **Sandra Hauser**, Head Transformation & Technology bei der Zurich Versicherung, im dritten Case Einblick in die Perspektive des Finanzsektors auf das Thema Resilienz. Aus dessen Sicht bedeute Resilienz, so Frau Hauser, in einem unbeständigen Umfeld Krisen zu bewältigen und weiterhin Werte zu generieren. **Technologie** sei dafür ein wichtiger Baustein, aber es gebe aus dem Blickwinkel des Finanzsektors ganz **viele andere Bausteine**, die für Resilienz notwendig seien. Dazu gehören neben den erwähnten **technologischen Komponenten**, **rechtliche Komponenten**, **People-Komponenten** und **regulatorische Komponenten**.

In der Praxis gilt es in Bezug auf Resilienz die Vorbereitung vom Handeln in der Krise selbst zu trennen. Sandra Hauser betonte besonders **Change-Readiness** als bedeutendes Asset in der Vorbereitungsphase: Eine Organisation, die nicht bereit ist, sich zu verändern, ist im Krisenfall nicht in der Lage auf spezifische Problemstellungen zu reagieren. In der Corona-Krise hiess dies konkret für Zurich **Home-Office für alle** zu ermöglichen, die **Erreichbarkeit für Kunden** sicherzustellen, **Cyber-Risiken** zu managen und mit signifikant **angestiegenen Versicherungsansprüchen** umzugehen. Gleichzeitig lernt eine Organisation aber auch mit jeder Krise dazu. Für Zurich zeigte sich, dass trotz guter Vorbereitung zusätzlich Massnahmen nötig waren, wie der Ausbau der Callcenter-Funktionalität, die Ermöglichung von Kundenidentifikation remote oder die erhöhte Relevanz von Cyber-Bedrohungen.

Quelle: Präsentation Sandra Hauser

Allgemein identifizierte Sandra Hauser vier wesentliche Merkmale von **Cyber-Resilienz**: die resiliente Unternehmensführung, der **Tone-from-the-Top** muss richtig gesetzt werden, eine resiliente Unternehmenskultur, der Informationsaustausch in resilienten Netzwerken sowie resiliente Change-Readiness. Resilienz bezieht offensichtlich **alle Bestandteile** mit ein. Wie auch Dr. Marti betonte Sandra Hauser, dass Resilienz entlang der **ganzen Wertschöpfungskette** sichergestellt werden muss. Gleichzeitig stand auch für sie fest, dem Thema Resilienz muss Raum in der **ganzen Strategieplanung** gegeben werden.

Bewusstsein für Resilienz und Cyber-Security schaffen

An der anschliessenden Panel-Diskussion nahm neben den Referierenden **Nationalrätin Judith Bellaïche** (GLP, ZH), Geschäftsführerin des Wirtschaftsverbands Swico, teil. In Bezug auf die Corona-Krise stellte Judith Bellaïche fest, die Legislative sei etwas unvorbereitet in die Krise geschlittert. Die Exekutive sei besser vorbereitet gewesen, aber was überhaupt nicht funktioniert habe, sei die **Datengenerierung und der Datenaustausch** gewesen. Dieses Problem müsse in Zukunft gelöst werden, egal in welcher Krise.

Zudem habe sie festgestellt, dass für das Überleben, die Erholung und die Normalisierung der Gesellschaft und der Volkswirtschaft als Gesamtsystem die **Aussenbeziehungen** von entscheidender Bedeutung sind. Dies betreffe zum einen die **Kommunikation während der Krise** und zum anderen die wirtschaftliche Erholung. Aufgrund der hohen Abhängigkeit vom Ausland wirken alle inländischen Massnahmen nur, wenn die **Aussenwirtschaft** ebenfalls funktioniert. In diesem Kontext sind für sie insbesondere **belastbare Beziehungen** entscheidend.

Aus Sicht von Swico war für Judith Bellaïche die Schlussfolgerung aus der Krise klar: Es gelte, mehr Fokus auf die **Digitalisierung** zu, **Redundanzen** zu schaffen, die **Digital-Literacy** und

schliesslich die **Cyber-Security** zu erhöhen. Sie zeigte sich überzeugt, dass die Corona-Krise die Verwaltung und Unternehmen aufgerüttelt hat, endlich die bestehenden Defizite in diesen Bereichen anzugehen.

Die Bedeutung weicher Faktoren und des Menschen als Schlüsselerkenntnis

Gefragt nach ihren Schlüsselerkenntnissen aus der Veranstaltung, zeigten sich alle Panellisten erfreut über die vielen Gemeinsamkeiten. **Dr. Adrian Marti** betonte die Wichtigkeit von **weichen Faktoren**, um Resilienz zu schaffen: Man müsse von oben herab die Kultur etablieren, den Ton setzen, damit Resilienz ein wichtiges Thema in der eigenen Organisation werde. **Dr. Benjamin Scharte** betonte, Resilienz lasse sich nicht rein technisch umsetzen, der Mensch müsse und sollte immer eine Rolle spielen. Im Endeffekt gehe es darum, wie man die dem Menschen eigene **Improvisationsfähigkeit und Kreativität mit Technologie** unterstützen könne. Für **Dr. Martin Krummenacher** war es zentral, dass alle **Redundanzen, Dezentralität** und **weiche Faktoren** genannt hatten. Letztere seien interessanterweise die robustesten in der Krise. **Martin Leuthold** erachtete es als entscheidend, dass **Resilienz und Cyber Security** in der **DNA eines Unternehmens** verankert seien. Man müsse wegkommen vom Gedanken, dass wir uns mit Technologie allein retten könnten. **Sandra Hauser** betonte es sei entscheidend, sich in der Vorbereitung Gedanken zur ganzen eigenen Wertschöpfungskette zu machen. Für Zurich habe sich gezeigt, dass man besonders bei den **Outsourcing-Partnern** eine grosse Exposure hatte.

Aus dem Publikum nach der Resilienz der Schweizer Gesellschaft gefragt, antwortete **Dr. Benjamin Scharte**, die Schweizer Gesellschaft sei sehr resilient aus Sicht der **sozialen Resilienz**. Diese drücke sich stark in **sozialen Netzwerken** und dem **gebildeten Sozialkapital** aus. Der Schweizer Bevölkerung sei vielleicht nicht einmal bewusst, dass sie resilient ist. Aber wie schnell sich in der Pandemie Bottom-up neue Ideen für die Unterstützung der Mitbürger entwickelt haben, zeige aus Forschungssicht, dass sehr viel soziale Resilienz vorhanden ist.

In Ihrer Schlussmessage ans Publikum betonte **Sandra Hauser** erneut die Wichtigkeit von **Vorbereitung** und des Einbezugs von Soft- und Hard-Factors in diese Vorbereitung. **Dr. Benjamin Scharte** plädierte dafür den **Menschen** nicht als grösstes Risiko und grösste mögliche Schwachstelle, sondern als **grösstes Asset** und eigentliche **Quelle von Resilienz** zu begreifen. **Dr. Martin Krummenacher** strich die Bedeutung von **informellen Strukturen** hervor. Diesen muss Raum offengehalten werden, denn sie würden dafür sorgen, dass es auch dann funktioniere, wenn die Führung ausfällt. **Dr. Adrian Marti** widmete seinen Schlusssatz einem Aufruf: Beginnen Sie dort **Resilienz aufzubauen, wo es Ihnen am wichtigsten** ist.

In seinem Schlusswort dankte **Oliver Spiess**, Partner im Bereich Public Safety and Defense bei der AWK Group, allen Referierenden und fasste den Anlass zusammen. Von Dr. Benjamin Scharte habe er ein neues Fremdwort gelernt, Emergenz. Von Dr. Adrian Marti habe er gehört, dass Resilienz systematisch aufgebaut werden muss, dass der Baukasten ganz wichtig ist und dass Resilienz nicht an der Firmengrenze aufhört. Bei Martin Leuthold habe er beruhigt festgestellt, dass die .ch-Infrastruktur dermassen viele Redundanzen beinhaltet, dass sie fast allem standhält. Er dankte Sandra Hauser für die Schilderung der aktuellen Situation und wie die Zurich Versicherung diese gemeistert haben. Und bei Frau Bellaïche habe er wieder gehört,

dass die Aussenbeziehungen wichtig sind. Resilienz hört nicht an der eigenen Firmengrenze auf, sondern es muss das ganze Ökosystem betrachtet werden. Schliesslich dankte Oliver Spiess **Martin Leuthold und Switch** für das **Event-Sponsoring**.