Cyberbedrohungen – wie gross ist die Gefahr und wie gut sind Staat, Wirtschaft und Gesellschaft davor geschützt?

Fazitbericht | 11. FSS Security Talk vom 17. Oktober 2022, Hotel Schweizerhof, Bern

Wie gehen die EU und weitere europäische Länder mit der wachsenden Cyberbedrohung um? Wie begegnet ihr die Schweiz? Wo steht die «Strategie Cyber 2021-2024» des VBS? Wie können unsere kritischen Infrastrukturen geschützt werden? Wie können sich Staat, Wirtschaft und Gesellschaft vor Cyber-Bedrohungen schützen?

Diese und weitere zentralen Fragen diskutierten namhafte Expertinnen und Experten beim 11. FSS Security Talk in Bern. Die 120 interessierten Teilnehmerinnen und Teilnehmer wurden aus erster Hand informiert. Der Anlass begann mit Inputreferaten von **Dr. Stefanie Frey** (Geschäftsführerin Deutor Cyber Security Solutions GmbH, Advisory Group ENISA), **Oberst i Gst Robert Flück** (Projekt Kommando Cyber, Schweizer Armee) und **Dr**. **Peter Friedli** (Head of Defence AWK Group). Anschliessend folgte ein spannendes Panel mit **Florian Schütz** (Delegierter des Bundes für Cybersicherheit), **Dr. Jörg Mäder** (Nationalrat GLP/ZH, Freischaffender Programmierer), **Alexandra Arni** (Leiterin ICT, Schweizerische Bankiervereinigung, Vizepräsidentin Swiss FS-CSC) und **Dr. Urs Loher** (CEO Thales Suisse SA). Moderiert wurde der FSS Security Talk von **Fredy Müller** (Geschäftsführer FSS).

Die Expertinnen und Experten waren sich grundsätzlich einig, dass Cyber**-Bedrohungen alle betreffen** und deshalb eine **Zusammenarbeit** über alle Ebenen hinweg notwendig ist, um der wachsenden Bedrohung begegnen zu können. Der Anlass machte aber auch deutlich, dass wir noch weit davon entfernt sind, die **Cyberbedrohung in all ihren Facetten zu begreifen und die notwendigen Massnahmen zu treffen**.

Cyberbedrohungen – «Wir kennen zwar den Feind, wissen aber nicht, wie wir ihn bekämpfen und uns schützen sollen»

Den Einstieg in die Referatsrunde machte **Frau Dr. Stefanie Frey, Geschäftsführerin bei Deutor Cyber Security Solutions GmbH**. Sie stellte gleich zu Beginn fest, dass heutzutage zwar überall von Cyber gesprochen werde, die meisten Personen jedoch **keine klare Vorstellung** davon hätten, was **Cyber genau bedeutet**. Drei Feststellungen im Zusammenhang mit dem Begriff Cyber müssten unterstrichen werden: «Cyber ist ein **Mittel zum Zweck** und kein Zweck an sich; Man sollte nicht von Cyber War reden, sondern lieber von **Cyber «in war»**; und Cybersicherheit ist **nicht nur IT-Sicherheit**, es sind davon noch viele andere organisatorische und strategische Komponenten betroffen.»

Anschliessend beleuchtete Frey den aktuellen Trend der **Zunahme von Cyberangriffen**. Dieses starke Wachstum stelle ein grosses Problem dar. Jedes Jahr würden sich die Straftaten verdoppeln und zudem müsse man eine **sehr hohe Dunkelziffer** beachten. Der Schaden für die deutsche Wirtschaft werde beispielsweise allein für das Jahr 2020 auf 223 Milliarden Euro geschätzt. Demnach wurden neun von zehn deutschen Firmen im gleichen Jahr Opfer von Cyberangriffen. Dieser Schaden sei nicht tragbar!

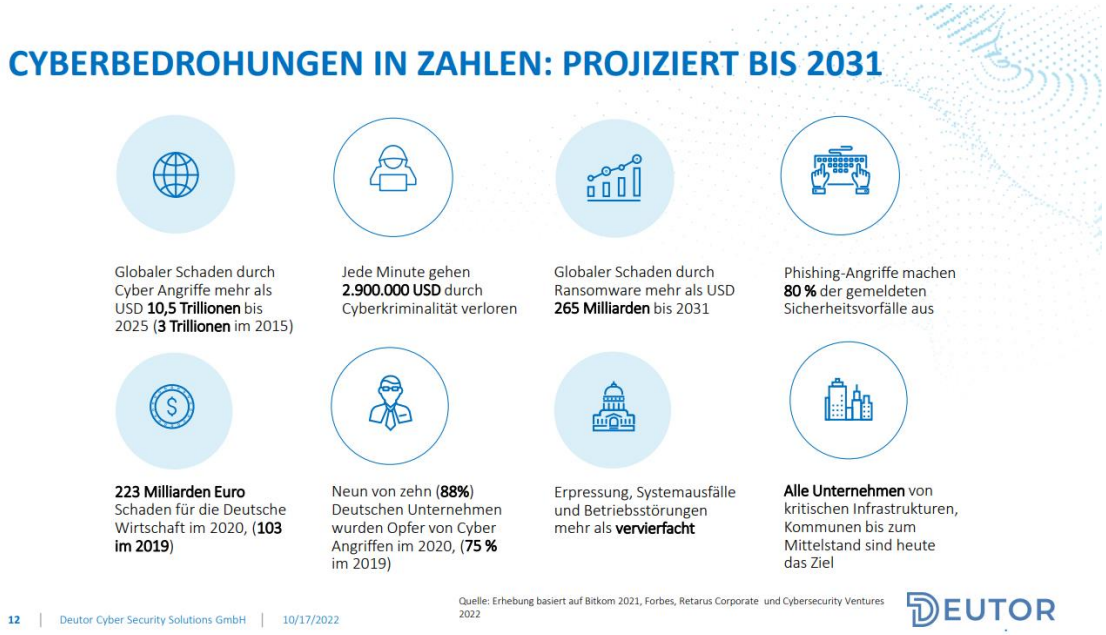


Abbildung 1: Die Zahlen sprechen eine klare Sprache: Die Cyberbedrohungen verursachen schon heute einen enormen Schaden und die Problematik wird sich in Zukunft noch weiter akzentuieren.

Die Frage stelle sich, warum der Schaden durch Cyberkriminalität so gross ist. Die Antwort darauf sei relativ einfach: «Wir kämpfen gegen einen **Feind, den wir zwar kennen**, bei dem wir jedoch nicht wissen, wie wir ihn bekämpfen sollen, da wir das Problem **nicht genügend analysieren und untersucht haben.** Darum wäre es zuerst wichtig, dass wir verstehen **lernen**, welche Lösungen uns gegen die Cyber-Kriminalität schützen.»

Frey gab weiter zu bedenken, dass heute alles automatisiert und digitalisiert werde, was **ohne genügende Sicherheit** jedoch **sehr gefährlich** sei. Beispielsweise liesse sich auch bei Waffensystemen beobachten, dass diese vernetzt würden, ohne genügend an die Sicherheit zu denken. Cyber sei also nicht immer eine gute Idee, sondern nur mit einem **guten Team und genügend Geld**, um alle **notwendigen Sicherheitsaspekte berücksichtigen** zu können. «Es braucht eine Digitalisierung mit Security und mit Verstand.»

«…wir müssen lernen, wie die Täter zu denken…»

Für einen besseren Überblick über die verschiedenen Facetten der Problematik ging Frey anschliessend noch eine bisschen näher auf die **verschiedenen Cyber-Bedrohungsarten** Cybercrime, Spionage, Subversion und Sabotage ein. «Mit der Cyberkriminalität lässt sich richtig **viel Geld** verdienen! Da sind **schlaue Köpfe** am Werk, die für Geld alles tun, **hochmotiviert** sind und leider viel zu oft Erfolg haben.» Die Motivation sei jedoch nicht immer einfach ersichtlich. Bei einem Fall aus dem Gesundheitssektor, welchen sie selbst mitverfolgt hatte, ging es beispielsweise um die Offenlegung von Patientendaten. Der Täter holte das in Aussicht gestellte Erpressungsgeld jedoch nie ab, was Mutmassungen über die Täterschaft und ihre Motive ausgelöst hat. Ein anderer Fall, den sie erwähnte und bei dem es wiederum um personenbezogene Daten ging, betraf die Conti-Gruppe. Der Fall habe aufgezeigt, dass Firmen ihre eigene **IT-Infrastruktur und deren Sicherheitslücken oft zu wenig kennen** würden. «Wenn aber die Täter vorhandene Schwachstellen finden und ausnützen können, **müssten wir diese auch kennen und beseitigen.** Da gibt es **keine Entschuldigung**: Was die Täter können, können wir auch!» Bei kritischen Infrastrukturen komme öfters die Sabotage über Cyberangriffe zum Zug.

©Daniel Saxer (iOf App, Defence & Security News)

Daraufhin thematisierte Frey wichtige **Probleme** im Zusammenhang mit der **Bekämpfung** von Cyber-bedrohungen. «Wir müssten **lernen so wie die Täter zu denken.**» Wird eine Unternehmung Opfer eines Cyberangriffs, sei jede **Scham und jedes Verschweigen falsch**. Oft bestehe jedoch auch noch das Problem, dass Vieles von oben nach unten verordnet wird, wie beispielsweise die Datenschutz-gesetzgebung, die vieles kompliziert mache.

Dabei wäre es **besser**, die Datensicherheit in einem **Prozess von unten nach oben** zu entwickeln und zu verbessern.

Für Frau Dr. Frey ist klar, dass ein **umfassendes Risiko-Assessment** Standard sein sollte bei jeder Entscheidung im Cyberbereich. Schliesslich lerne man heute in jedem Ausbildungslehrgang, wie eine Bedrohungslage zusammen mit einer Schwachstellen-Analyse zu einem Risk Assessment zusammengetragen werden kann, welches als **Basis für Entscheidungen** herangezogen werden sollte. «Dies wäre **auch im Cyberbereich möglich**, nur tut dies bislang niemand! Wir müssen diese Abfolge leben lernen: Zuerst analysieren wir unsere **Cyber-Bedrohungslage**, dann unsere **Schwachstellen** im Cyberbereich, und dies zusammen erlaubt uns, unser **Risikoprofil** zu erkennen und gezielte Aktionen einzuleiten, um unsere **Cyber-Schwachstellen zu eliminieren.»**

Zudem sollten wir, wie mutmassliche Täter denken, welche sich einen Cyberangriff auf unsere Firma oder Person überlegen. «Durch dieses kritische **Hinterfragen** unserer Cyber-Hardware und -Software könnte schon viel gewonnen werden.» Dafür brauche es aber Zeit und Geld, und kein Digitalisieren von allem und jedem ohne Unterlass. Die Cyber-Sicherheit sei für jede Firma, jedes Land und sogar jede Einzelperson eine zentrale Herausforderung. Nur eben werde die Bedrohung falsch analysiert, was den Boom der Cyber-Kriminalität erkläre, den es dringend einzudämmen gilt. Sonst werde sich die Situation nicht bessern; ganz im Gegenteil.

«Das Cyber-Kommando der Schweizer Armee wird 2024 aktionsfähig!»

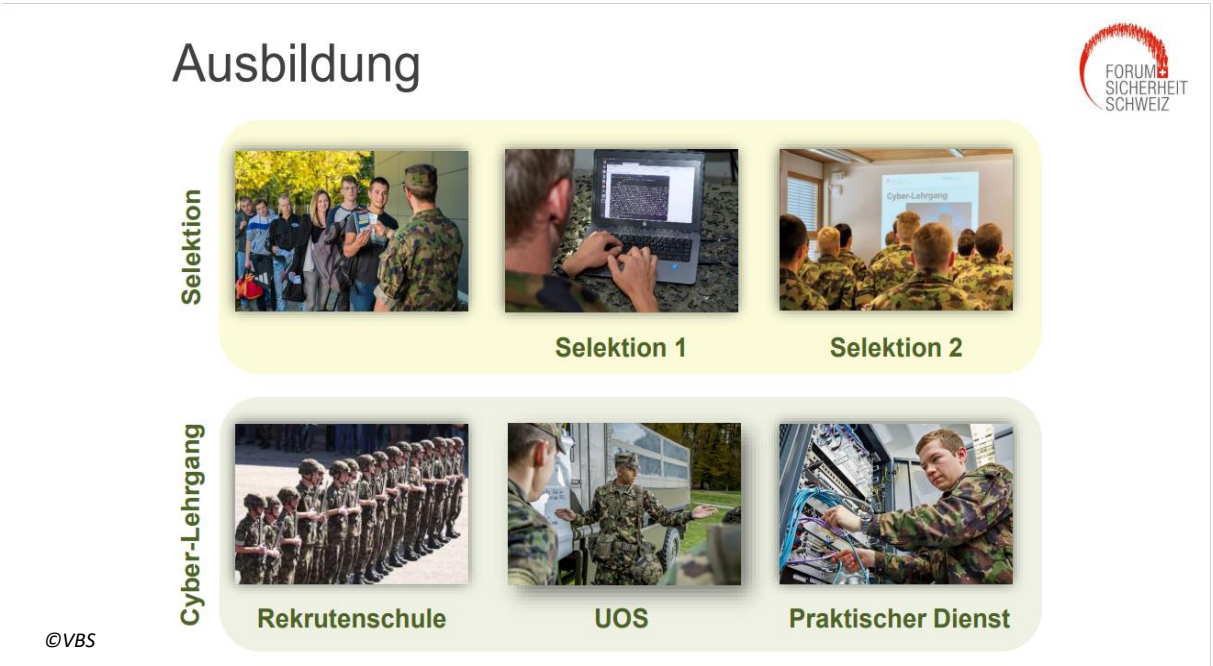
Als zweiter Referent gab **Oberst i Gst Robert Flück** einen Einblick, wie sich die **Schweizer Armee** auf Cyberbedrohungen vorbereitet. Dabei strich er insbesondere die Schaffung des **Cyber-Bataillons 42** heraus, welches **ab 2024** operationsfähig sein soll und eine **wichtige Rolle** im Kampf gegen Cyberbedrohungen einnehmen wird.

Zuerst informierte Flück über die zwei grundlegenden Aufgaben der Armee im Cyberbereich: «Um ihre Einsatzfähigkeit und Handlungs-freiheit jederzeit und über alle Lagen sicherzustellen, ist die Armee permanent in der Lage, **Cyber-bedrohungen zu erkennen**, sich vor Angriffen zu **schützen** und diese **abzuwehren**. Im Konfliktfall ist sie zudem in der Lage mit Cyber-Aktionen **militärische Aktionen zu unterstützen**.»

©Daniel Saxer (iOf App, Defence & Security News)

Dann ging er näher auf die Cyber-Organisation der Armee ein. Zu unterscheiden seien die IKT-Systemsteuerung, die Detektion & die Abwehr, die Lage & Operationen, der IKT-Systembetrieb und die Nachrichtenbeschaffung & Wirkungen. Konkret würden zukünftig **fünf Aktionsfelder** vom **Kommando Cyber** wahrgenommen: Zum einen sei dies der **Eigenschutz**, zum anderen die Ausrichtung vom IT-Service Provider zum **militärischen Kommando**, die Schaffung der Voraussetzungen zur **Digitalisierung der Armee**, der elektronischer **Kampf und Cyberoperationen**, sowie die Fähigkeit zur Zusammenarbeit und Unterstützung im **Sicherheitsverbund Schweiz**.

Das Kommando Cyber soll ab 2024 voll operationsfähig sein und sich danach ständig weiterentwickeln. Dafür spiele momentan insbesondere die **Ausbildung des Personals** eine zentrale Rolle. In einer rigorosen Selektion werden Informatiker ausgewählt, die nach einer 42-wöchigen Schulung künftig im Kommando Cyber in verschiedenen Milizfunktionen ihren Dienst verrichten werden.



©VBS

Abbildung 2: "Cyber ist ein People's Business" - Dementsprechend nimmt die Ausbildung des Personals des Kommando Cybers eine zentrale Rolle im Kampf der Armee gegen Cyberbedrohungen ein.

Dies führe zu einem **wechselseitigen Gewinn**. «Einerseits profitieren die betroffenen Personen in ihrem **zivilen Einsatzgebiet** von ihrer **Cybererfahrung in der Armee** und die Armee profitiert von top-ausgebildeten Einsatzkräften.»

Weiter fügte Flück an, dass das Kommando Cyber nur dann gut funktionieren könne, wenn es von der **Kooperation** mit verschiedenen Bereichen, wie beispielsweise in der Kryptologie Nutzen ziehen könne. Ferner könne das Kommando Cyber **zivilen Behörden subsidiär Unterstützung** leisten, wenn die Mittel

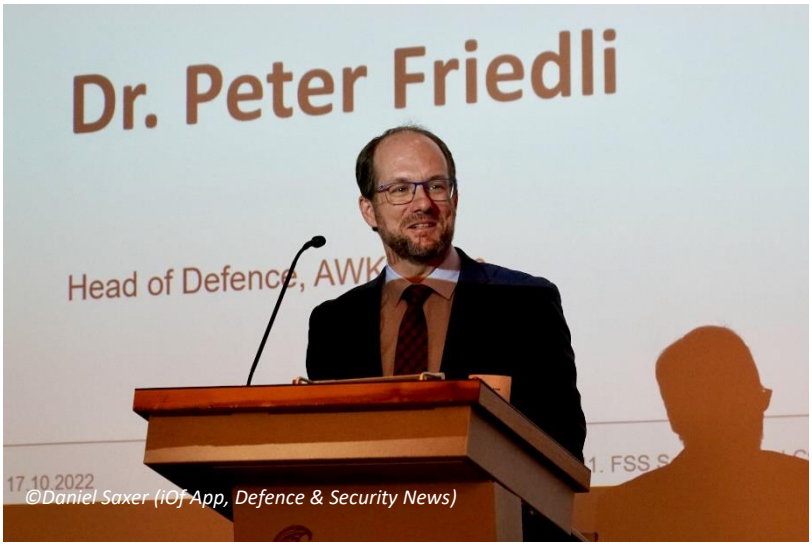
der zivilen Behörden erschöpft oder nicht vorhanden sind und kommerzielle Leistungserbringer nicht im erforderlichen Umfang oder zeitgerecht zur Verfügung stünden.

Anschliessend stellte Flück den Zeitplan und die Organisationsstruktur des Projekts Kommando Cyber noch näher vor. Im Jahr 2021 startete die Initialisierungsphase, 2022 folgte die Konzeptualisierung und im Jahr 2023 die Realisierung. Im Jahr 2024 soll schliesslich die **Einführung des Kommando Cyber folgen** und dieses soll dann in Zukunft **stetig weiterentwickelt** werden. Hervorzuheben in der Organisationsstruktur sei vor allem das Element «langfristige Entwicklung» und das «Einsatzelement Miliz.» Im Zusammenhang mit Cyber sei es sehr wichtig lange in die Zukunft schauen zu können und Trends frühzeitig zu erkennen. Das Milizsystem erlaube zudem Cyber-Fähigkeiten aus der zivilen Welt in die Armee einzubringen und dort weiter auszubauen, was sowohl für die Armee wie auch für Gesellschaft von grossem Vorteil sei.

Zusammenfassend liesse sich festhalten, dass Cyber primär ein **People's Business** sei - «es braucht **Menschen**, Informatik-fachleute, welche Cyberbedrohungen erkennen und damit umgehen können». Ferner brauche es eine **geeignete Organisation innerhalb der Armee**. Diese Rolle werde durch das sich im Aufbau begriffene **Cyber-Bataillon 42** wahrgenommen. Schliesslich stünden wir am Anfang einer Entwicklung, **die Schweizer Armee zu erneuern und auf moderne Bedürfnisse auszurichten.**

«Die zunehmende Konvergenz zwischen IT und OT wird zu wenig beachtet»

Der dritte Referent war **Dr. Peter Friedli, Head of Defence, AWK Group**, der das Bild von bekannten IT-Bedrohungen hin zu Bedrohungen im Bereich der Operational Technologies öffnete. Die Bedrohungen im Informationsraum bzw. in der IT («Information Technology») seien allgegenwärtig und allgemein bekannt. Ein Beispiel dafür sei das bekannte Phishing, also das Stehlen von Passwörtern, um damit den Computer anderer Menschen und Firmen einzudringen und diesen finanziellen und anderen Schaden zuzufügen. **Neben der IT gebe es aber auch die OT**, die «Operational Technology», welche die **Hardware und Software zur Überwachung und Steuerung** von physischen Prozessen, Geräten und Infrastrukturen umfasst. Die produzierende Industrie, aber auch Systeme im Medizinal-Bereich, in der Verkehrslenkung, der Energieversorgung oder der Wasseraufbereitung sind auf die OT angewiesen. Dabei stünden jedoch vor allem die Sicherheit im Betrieb, die Verfügbarkeit und die Produktionszyklen im Fokus. Mit **zunehmender Konvergenz zwischen IT und OT** entstünden aber auch für die OT gewichtige Risiken. «Mit der wachsenden Digitalisierung der OT werden die Möglichkeiten für **Cyberangriffe auch in der OT** immer grösser.» Die fortlaufend leistungsfähigere und komplexere Infrastruktur hat zur Folge, dass Zusammenhänge immer schwerer greifbar werden. Dementsprechend wird es auch vorzu schwieriger nachzuvollziehen, wie sich ein Risiko an einem Ort durch das ganze Geflecht an zusammenhängenden Elementen durchkonjugieren wird.



©Daniel Saxer (iOf App, Defence & Security News)

Die Fälle, wo über Cyberangriffe Industriefirmen lahmgelegt werden oder die Energieversorgung ausfällt häuften sich, wobei gerade im Gesundheitsbereich solche Cyberattacken Leben in Gefahr bringen können. «Was stellen wir aber fest? **Im Bereich der OT ist die Awareness für Security Risks**

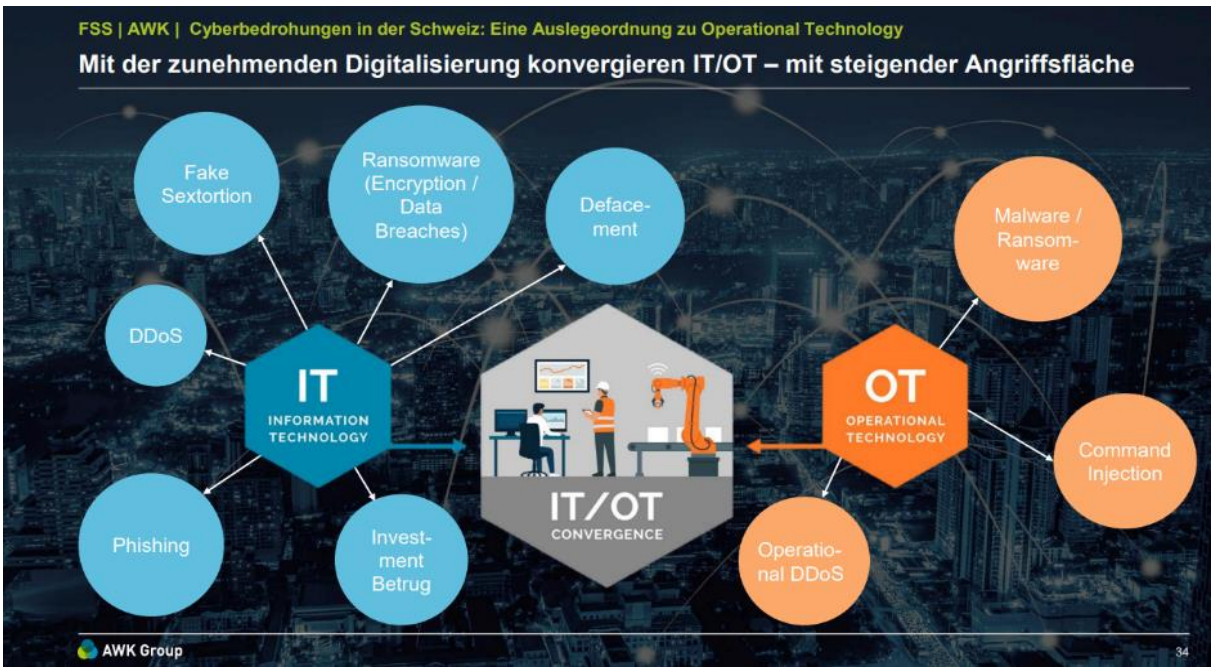


Abbildung 3: IT und OT konvergieren immer mehr - das damit verbundene Risiko ist jedoch Vielen noch nicht ausreichend bewusst.

oft nicht ausreichend vorhanden.» Bekannte **Best Practices aus der IT würden in der OT nicht verwendet** und es fehle eine vollständige Betrachtung der **Wertschöpfungskette End-to-End**. IT und OT seien in vielen Firmen separiert, obschon sie mit der wachsenden Digitalisierung der Produktionsprozesse zunehmend konvergierten. «Gerade in der **Energieverteilung** ist festzustellen, dass **nicht genügend Schutzmassnahmen** gegen mögliche Cyberangriffe vorhanden sind». Dabei sei jedoch interessanterweise keine Korrelation zwischen der Grösse der Energieverteiler und der Cybermaturität, sprich dem Ausbau der Schutzmechanismen, feststellbar.

Glücklicherweise gäbe es jedoch auch im Bereich der OT-Security Best-Practices. Einerseits baue auch die OT-Security auf einer frühzeitigen Risikoerkennung auf, wo man alle zusammenhängenden Elemente und die damit verbundenen Risiken analysieren sollte. Wichtig sei in diesem Zusammenhang auch ein tiefes Verständnis der Schnittstellen zwischen IT und OT. Weiter werde dies auch durch den Miteinbezug von Lieferanten und Herstellern erreicht sowie durch die Schulung des Personals und einen sorgfältigen Betrieb der Anlagen.

Schlussendlich gäbe es **vier Kernaussagen**, die Friedli den Zuhörern mit auf den Weg geben wolle: **Cyberbedrohungen existieren auch im physischen Bereich** und stellen ein grosses Risiko dar; mit der zunehmenden Digitalisierung vermehren sich auch die Angriffsvektoren, **OT und IT konvergieren**; die **operationelle Sicherheit** ist für viele kritische Infrastrukturen **nicht gewährleistet** und stellt daher ein gewichtiges Risiko dar und die OT Security und Supply Chain Security schliessen wesentliche Sicherheitslücken – und müssen **immer Hersteller, Dienstleister und Betreiber involvieren**. «Es muss also noch viel getan werden, um die OT Security zu verbessern und gegen mögliche Cyberangriffe zu schützen.»

«Lassen Sie uns mehr in Chancen denken als in Risiken» – Das Panel

Nach drei sehr informativen Referaten folgte die Panel-Diskussion. Moderator **Fredy Müller** unterteilte zu Beginn die Diskussion in drei Bereiche: Einerseits den **militärisch-zivilen Bereich** und andererseits den **industriellen Bereich** sowie den **politischen Bereich**. Für die Eröffnungsfrage wendete er sich an **Florian Schütz, Delegierter des Bundes für Cybersicherheit**, und wollte von ihm wissen, was seine Schlüsselerkenntnisse aus den letzten 20 Jahren im Bereich Cyber waren. Für Schütz war klar, dass die Relevanz des Themas klar zugenommen hat. Dies sollte jedoch aufgrund der zunehmenden Digitalisierung und Vernetzung niemanden erstaunen. Leider habe die Gesellschaft in der politischen Diskussion und in den Führungsebenen bisher noch zu wenig beachtet, dass es sich um ein technisches Thema handle. Daher sei es ein Fehler, **dass man die IT-Fachkräfte nicht in die Management-Ebene befördere**. «Sie haben ja auch keinen CFO, der nichts von Finanzen versteht» fügte Schütz hinzu, um seinen Punkt zu verdeutlichen. Dabei bestünde durch die exzellente Ausbildung in der Schweiz ein **grosses Potenzial**. **Schütz stellte ebenfalls fest, dass sich die Geschichte wiederhole**: «Auch die Fliegerei und die Autos waren einmal neu und man musste erst herausfinden, wie man damit umgeht. Hier können wir jedoch sagen, dass wir die Entwicklung erkannt haben. Wir gehen voran, wir haben zwar noch Verbesserungspotenzial aber ganz so schlecht sind wir nicht.»

Daraufhin wandte sich der Moderator an **Dr. Jörg Mäder, freischaffender Programmierer und Nationalrat GLP/ZH**, mit der Frage, wie diese Thematik im Bundeshaus wahrgenommen werde. Mäder bestätigte zwar, dass Cyber durchaus ein Thema in der Politik sei, jedoch **nicht in dem Masse, wie es wünschenswert wäre**. Die ganze Digitalisierung sei bisher eher als **Mittel zum Zweck** betrachtet worden. Man will die IT zwar nutzen, aber gross über Risiken nachdenken wolle niemand.

Alexandra Arni, Leiterin ICT der Schweizerischen Bankiervereinigung und Vizepräsidentin des Swiss FS-CSC unterstrich, dass der Banken- und Finanzsektor einer der ersten war, welche die Bedeutung des Thema Cyber erkannt habe. Arni erklärte, dass Banken stets ein **beliebtes und starkes Angriffsziel von Cyberattacken** seien.

Auch im militärischen Sektor bzw. in der Rüstungsindustrie ist Cyber schon lange ein Thema, betonte **Dr. Urs Loher, CEO von Thales Suisse SA**, und meinte, dass er es falsch fände, wenn heute alles als komplexer dargestellt würde. **Auch früher musste man Informationen schützen, heute passiere dies einfach auf einer anderen Ebene**, welche von vielen Leuten nicht mehr ganz verstanden werde: «Wir müssen wieder zurückkommen und die Dinge so vereinfachen, dass man wieder versteht, was man macht.» Es gehe um **Schutz von Informationen** und darum, wer zu was Zugriff hat. Dieser Grundsatz habe sich nicht verändert.

Cyberattacken auf Unternehmen als lukrative Einnahmequelle

Moderator Fredy Müller erwähnte, dass **Cyberkriminalität heute mehr Geld generiere als der Drogenhandel** weltweit. Deshalb wollte er von **Florian Schütz** wissen, ob man sich mehr in die **Perspektive der Täter** hineinversetzen solle. Schütz entgegnete, dass die Expertinnen und Experten bereits sehr gut verstehen würden, wie die Täter funktionieren. Diese wollen **mit minimalem Aufwand einen maximalen Ertrag** rausholen. Organisierte Cyberkriminalität sei oft ähnlich **wie eine Firma mit regionaler oder globaler Aufteilung strukturiert**. Operationen würden dabei zum Beispiel aus Afrika durchgeführt, weil es dort viele Talente und einen kleinen Arbeitsmarkt gebe. Support finde man hingegen eher in Nordeuropa, weil dort viele Sprachen gesprochen werden. Auf diesem Verständnis könne aufgebaut werden, man müsse aber dranbleiben. Dafür habe man in der Schweiz den NDB und die Strafverfolgung. Aber natürlich gäbe es immer noch **Verbesserungspotenzial im Lagebild**.

Müller spricht anschliessend **Jörg Mäder** an, welcher **Vorstandsmitglied bei der Digitalen Gesellschaft** ist. Dort gäbe es viele Bastler und Entwickler, der Sicherheitsaspekt ginge jedoch oft vergessen. **Jörg Mäder** entgegnete, dass aufgrund des **Internet of Things** durch physische Grenzen keine Sicherheit mehr gewährleistet sei, da alles miteinander vernetzt werden könne. Solange die Basteleien nur zum Spass gemacht werden, sei das Schadenspotenzial klein. Wenn diese jedoch **für produktive Systeme** eingesetzt werden sollen, werde es schwieriger. Jedoch sei die Awareness in diesem Bereich mittlerweile sehr hoch und Sicherheitsstandards existieren. Man müsse sich einfach auch wirklich daranhalten und **regelmässige Patches und Updates** verfolgen und umsetzen.

©Daniel Saxer (iOf App, Defence & Security News)

Cyber-Angriffe im Alltag eines Unternehmens

Dies verleitete Fredy Müller zur Frage an **Urs Loher**, wie Thales mit Cyberangriffen umgehe. Dieser bestätigte, dass **Thales fast täglich angegriffen werde**. Nur seien sie bisher gut durchgekommen. Für ein Rüstungsunternehmen sei die Sicherheit natürlich sehr wichtig, da sie direkt mit der Glaubwürdigkeit des Unternehmens zusammenhänge. Es werde sehr viel in die betriebliche Sicherheit investiert. 100% sicher sei man jedoch nie. Der Moderator wollte deshalb wissen, warum die Hemmschwelle so gross sei, über Cyberangriffe zu sprechen. Auch Loher sieht dieses Phänomen als grosse Krux: Jeder möchte solche Attacken stillschweigend regeln. Dies sei jedoch der falsche Ansatz. Innerhalb eines Konzerns funktioniere der Austausch hervorragend, **aber zwischen den Konzernen und auch mit den Behörden werde wahrscheinlich zu wenig kommuniziert**.

Alexandra Arni erklärte daraufhin, dass das Swiss FS-CSC deshalb daran sei, eine **Krisenorganisation aufzubauen, welche im Falle eines Bank- Angriffs zum Einsatz komme**. Arni illustrierte die Wichtigkeit dieser Organisation mit einem Beispiel: «Wenn eine systemrelevante Bank von einer DDoS-Attacke heimgesucht würde, dann hat dies einen Einfluss auf den ganzen Zahlungsverkehr in der Schweiz und damit auf die gesamte Volkswirtschaft. In einem solchen Fall braucht es eine stringente Krisenorganisation, welche dann mit den Policies, welche jetzt erarbeitet werden, entscheiden kann,

wie die Systeme schnellstmöglich wieder hochgefahren werden können». Die Kunden müssten in einem solchen Fall natürlich auch ab dem Zeitpunkt, an welchem die Bank nicht mehr funktioniert, entsprechend informiert werden. Diese **Kommunikationsstrategie** werde nun in der noch sehr jungen **Swiss FS-CSC** erarbeitet.

«Die klare Zuordnung von Kompetenzen ist elementar»

Auch Firmen wie Zalando werden regelmässig von Cyberattacken bedroht, erwähnte Fredy Müller und fragte deshalb **Florian Schütz** als ehemaligen Verantwortlichen **bei Zalando,** wie der **Online**-Händler damit umgegangen sei. Schütz erklärte, dass Angriffe bei Zalando an der Tagesordnung waren. Bei Angriffen waren teilweise Betriebsausfälle die Folge, welche in Minuten fünfstellige Schadensbeträge verursachten. Deshalb seien **schnelle Entscheidungen** und eine **klare Zuordnung von Kompetenzen** elementar bei der Cyberabwehr. Schütz betonte daraufhin, dass aus Risiken auch **neue Opportunitäten** entstehen können. Als Beispiel nennt er einen Fall, bei dem auf der Webseite ein Formular aufgesetzt wurde für die «blockierten» Kunden, damit diese trotzdem ihre Bestellung aufgeben konnten. Daraus sei **Market Intelligence** bzw. eine neue Marketingidee entstanden und die Kosten für solche Sicherheitsmassnahmen seien nun auch nicht mehr so ein grosses Thema.

Angesichts der grossen Bedeutung eines raschen Krisenmanagements bei Cyberangriffen, wollte Fredy Müller von **Alexandra Arni** wissen, ob die Swiss FS-CSC bereits ein Logbuch für solche Fälle vorbereitet habe und **Krisenszenarien auch aktiv geübt werden**. Arni bestätigte, dass es elementar sei, dass für solche Fälle **operative Cyberübungen** stattfänden und alle Beteiligten Ihre Rollen sehr genau kennen und entsprechend handeln.

Auf die Frage, ob es im Bundeshaus ebenfalls Cyberrisiko-Vorkehrungen gebe, erläuterte Nationalrat **Jörg Mäder**, dass das Bundeshaus «leider» noch relativ gut aufgestellt sei, da die **Digitalisierung noch nicht so weit fortgeschritten** sei. Im Notfall könne man auf altbewährte Methoden wie Stimmenzähler zurückgreifen, um den Parlamentsbetrieb aufrecht zu erhalten. Viel wichtiger erscheint ihm jedoch, dass man vermehrt über solche Vorfälle und Risiken reden müsse. «Es ist wie bei einer Geschlechtskrankheit: Es betrifft viele Menschen, aber die wissen nichts voneinander, obwohl gerade das helfen würde. Um Angriffe sauber abwehren zu können, muss man seinen Gegner kennen und je mehr Fälle bekannt sind, desto besser wäre dies möglich.» **Die Realität sei jedoch gegenläufig**, fuhr Mäder fort. Man wolle seinen Ruf nicht verlieren aber im Falle der Fälle wolle man auch nicht allein dastehen.

Was tun bei einem Cyberangriff?

Was passiert bei einem konkreten Cyberangriff auf ein Unternehmen? Soll man das Nationale Center Cybersicherheit (NCSC) oder den Cyberdelegierten des Bundes direkt anrufen? **Florian Schütz** erklärte dazu die **Aufgabenteilung des Bundes**, welche vielen Unternehmen nicht bekannt sei. Bei einem kriminellen Akt, was je nach Statistik ca. 95% der Fälle ausmache, sei die **Strafverfolgung** zuständig. Bei Sabotage übernimmt der Nachrichtendienst des Bundes (**NDB).** Jeden Vorfall kann man beim NCSC melden. Das NCSC bietet Ersthilfe und informiert die richtigen Partner. Schütz fügte an, dass die heutige Unterscheidung zwischen kritischer und nicht-kritischer Infrastruktur immer weniger Sinn ergebe. Viel eher sollte man **nach Wirtschaft und Bevölkerung unterscheiden** und erst dann nach Kritikalität abstufen. Grundsätzlich empfehle er daher bei Straftaten immer auch **die Polizei einzuschalten**. Das NCSC fungiere dann immer noch als **technische Unterstützung**. Bei Sabotage versorge das NCSC den NDB dann vor allem mit Analysen. Die Anschlussfrage war, wie mit **Lösegeldforderungen** umgegangen werden sollte. Schütz machte klar, dass **Lösegeld nie bezahlt werden sollte**, denn so würden die Machenschaften der Angreifer nur unterstützt. Wichtig sei jedoch, dass man sich Hilfe hole. Die Polizei könne oft mit Tätern verhandeln und dadurch wertvolle Zeit

gewinnen. Ein Punkt war Schütz jedoch besonders wichtig: «Eigentlich sprechen wir über den falschen Zeitpunkt. Im Falle eines Angriffes bin ich schon zu spät. **Man könnte das System auch sicher bauen**, dann müssten wir nicht darüber diskutieren. Glauben Sie mir: Sie würden auch nicht über eine Brücke gehen, welche so unsicher gebaut ist, wie viele IT-Systeme». Deshalb ist IT für Florian Schütz auch eine klare **Ingenieursdisziplin**. Da sollte der Fokus liegen und weniger auf Angriff und Verteidigung. **Jörg Mäder** ergänzte und unterstrich, dass es wichtig sei, eine Strategie für ein schnelles Herunterfahren und einen Restart von Systemen zu haben. Da brauche es definitiv eine höhere Awareness.

Besondere Cyberabwehrsysteme für Armeen und Staaten

Fredy Müller wollte von **Urs Loher** wissen, welche Systeme Thales baue, **um Staaten und auch Armeen die nötige Sicherheit – auch im Cloud-Bereich – zu bieten**. Loher machte klar, dass Thales Systeme so baut, dass sie einem **Angreifer das Leben möglichst schwer machen**, falls sie bereits ins System eindringen konnten. Das Ziel und die erste Priorität sei natürlich, dass Angreifer **gar nicht erst in Systeme hineinkommen**. Dies wird unterstützt, indem man getrennte Systeme baue sowie mit Firewalls oder mit Schutzmechanismen betrieblicher Natur, wie das Einschränken von Zugriffsrechten arbeite. Dazu seien ebenfalls **regelmässige Updates** nötig, um mögliche Lücken zu schliessen. Loher erklärte, dass der Kryptographie zudem eine zentrale Rolle zukomme. Hier sei Thales führend im Schutz und in der Verschlüsselung von Daten, Datenübermittlung sowie von Cloud-Lösungen für Staaten oder der NATO. Bereits heute werde in diesen Bereichen in Systeme der Zukunft, wie zum Beispiel in die **Quanten-Kryptografie,** investiert. Es sei jedoch wichtig, dass man stets verschiedene Sicherheitswege gleichzeitig einsetze und zum Beispiel eine Zwei-Faktor-Authentifizierung habe.

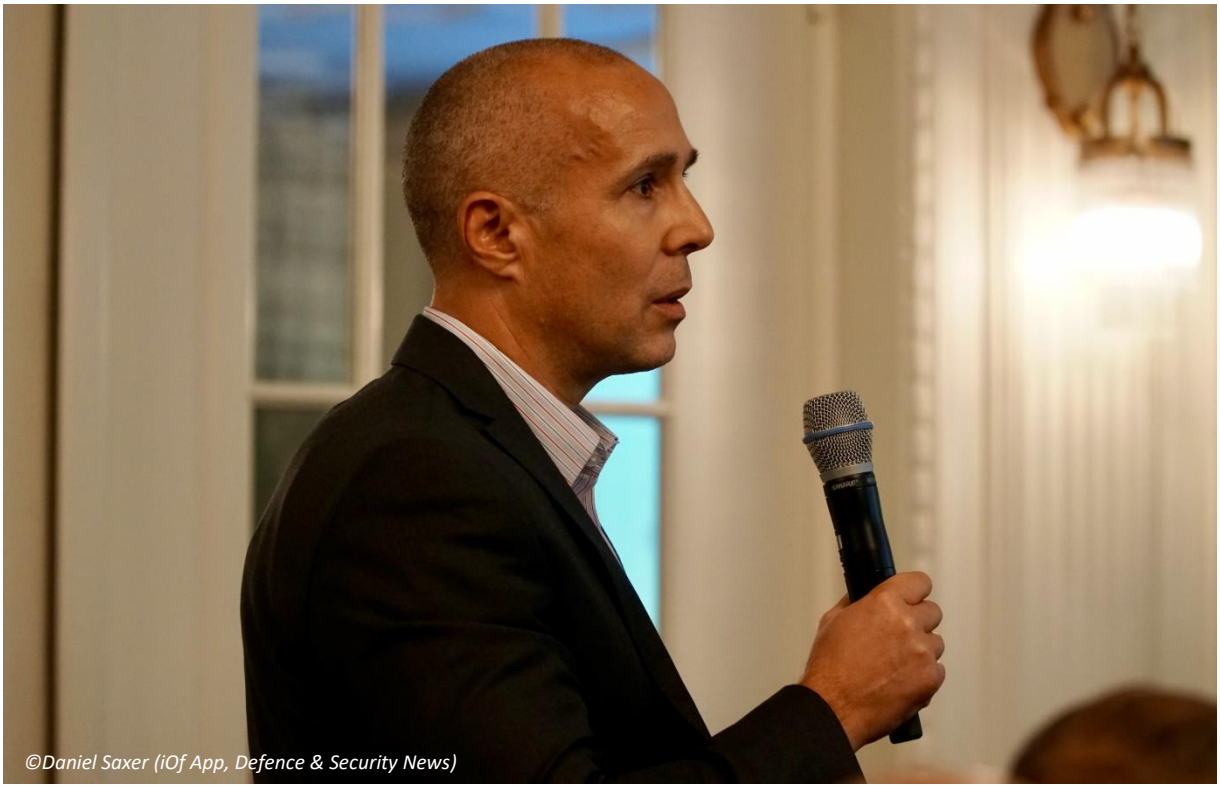
«Cybersicherheit ist ein Prozess, welcher eine permanente Risikoanalyse benötigt»

Anschliessend öffnete Moderator Fredy Müller die Paneldiskussion für das Publikum. **Hans-Peter Steffen, Kadermitglied der RUAG** gab zu bedenken, dass ein Technologiewettlauf stattfinde zwischen Innovation, Totalvernetzung und der Verhinderung von Missbrauch. Daher wollte er wissen, ob es auch **einen anderen Approach** gäbe als die totale Kontrolle sämtlicher Lebensdaten. Als Beispiel nannte er das **Predictive-Policing**, um künftige Bedrohungslagen besser zu erkennen. **Florian Schütz** entgegnete, dass man stets **zwischen Sicherheit und Freiheit** abwägen müsse und dass beides nur in einem begrenzten Masse möglich sei. Für ihn sei jedoch ganz klar, dass man sich von der Vorstellung verabschieden müsse, dass Sicherheit ein Zustand sei. Sicherheit, so auch die Cybersicherheit, sei **vielmehr ein Prozess**, welcher eine **permanente Risikoanalyse** benötige. Ein Social-Credit-System wie in China wäre seiner Meinung nach mit unserem Werteverständnis nicht vereinbar. Dabei verwies Schütz auch auf die Bundesverfassung, welche klar in Artikel 6 festhalte, dass es nicht der Staat sei, der einen schütze, sondern dass **jede Person mit Entscheidungen verantwortungsvoll umgehen müsse**. **Jörg Mäder** fügte an, dass man Risikoabschätzung schon aus anderen Bereichen kenne: «Sie haben vermutlich auch einen Haustürschlüssel und eine Veloschlüssel, welche von unterschiedlicher Qualität sind, weil das Schadensereignis von unterschiedlicher Höhe wäre.» Mäder ergänzte noch, dass beim Predictive-Policing viele Systeme mit künstlicher Intelligenz operieren und dies weitere Probleme verursache.

Die nächste Frage kam von **David Ribeaud, CEO von Helvetia Specialty Markets**. Er führte aus, dass die Helvetia in Bezug auf Cyber zwei Herausforderungen sehe: Einerseits reiche Prävention für eine resiliente Schweiz nicht aus, andererseits gäbe es **keine Versicherungslösungen** für **Cyberbedrohungen**. Die Helvetia schlage deshalb vor, dass die **private Versicherungswirtschaft mit finanzieller Unterstützung des Bundes** ein auf Prävention fokussiertes Unterstützungsprogramm für Gesellschaften entwickle. Die Gesellschaften kämen aber nur in den Genuss solcher Unterstützungen, wenn gewisse Massnahmen zur Erhöhung der Cybersicherheit getroffen werden. Auf diese Ausführungen wollte er von Florian Schütz wissen, wie er zu einer solchen Idee stehe. **Florian Schütz**

fand die Idee Interessant, zeigte sich jedoch **skeptisch gegenüber einer finanziellen Unterstützung** des Bundes. Wenn das Modell ökonomisch interessant wäre, dann sollte es auch finanziell selbsttragend sein. Er würde nicht direkt bei der Unterstützung anfangen, sondern **erst das Modell an sich entwickeln** und dann in einer **zweiten Phase über die Kapitalgeber diskutieren**.

Jörg Mäder stellte Herr Ribeaud die Frage, wie es um Rückversicherungen und die Einschätzung langfristiger Risiken stehe. Dieser entgegnete, dass man eben **keine Rückversicherung kriege,** weshalb man Massnahmen zurückfahren müsse. Er zog einen Vergleich mit der Pandemie, bei der das Risiko


©Daniel Saxer (iOf App, Defence & Security News)

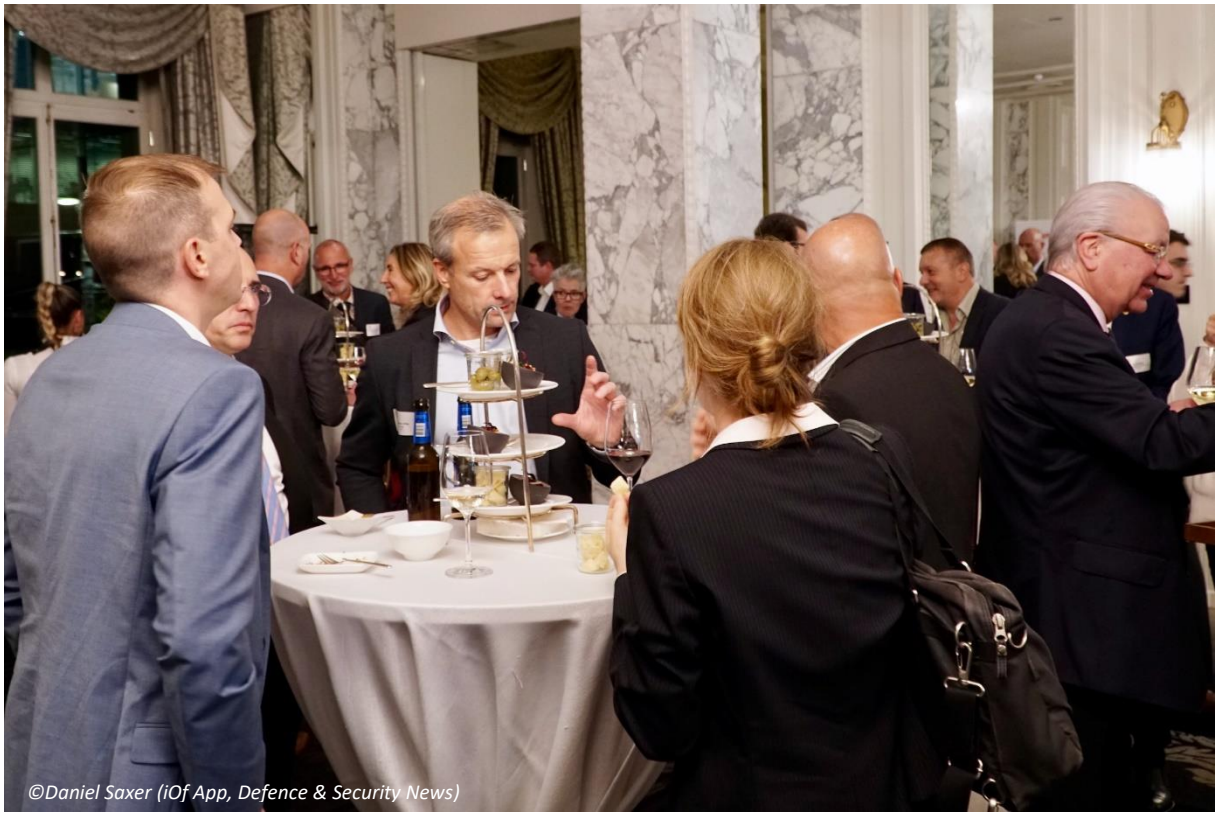
auch schlecht diversifiziert war, weshalb der Bund subsidiär einspringen musste. **Schütz** gab zu bedenken, dass die Frage dabei eigentlich sei, ob man die **Risiken nicht besser verstehen lernen müsse, um sie dann quantifizieren** zu können oder ob dies nicht möglich sei und es tatsächlich eine Substitutionslösung für den Wegfall der Versicherbarkeit brauche. Im Falle Letzteres könne man durchaus Modelle, wie das von der Helvetia vorgeschlagene, diskutieren. Er **verschliesse sich nicht gegenüber dem Modell**, man müsse es nur genau prüfen.

Eine weitere Frage kam von **Yann Schmuki, Mitarbeiter der Führungsunterstützungsbasis der Armee.** Er wollte von den Panel-Gästen wissen, wie der Staat und die Armee sicherstellen können, dass Investitionen in den Cyberbereich sinnvoll seien und den Schutz gewährleisten, den man möchte. Daraufhin verwies **Florian Schütz** auf die Funktionen des privaten Marktes: «Es ist ein Irrglaube, dass der Staat alles selber machen kann. In der Vergangenheit ist der Staat daher auch vermehrt in die Gegenrichtung gegangen und hat verschiedene Bereiche privatisiert.» Die letzte Publikumsfrage kam von der **Studentin Yvonne Aregger**, welche wissen wollte, ob es aufgrund der Cyberrisiken auch **Lösungsansätze gäbe, welche zu einer «Entdigitalisierung»** führen würden. Urs Loher verwies darauf, dass es sich hier ähnlich wie bei den Lieferketten verhalte, wo es ähnliche Überlegungen gäbe. Jedoch müsse man **über den Trade-off nachdenken**, was eine solche Massnahme mit sich bringen würde. Vielleicht werde man in Zukunft gewisse Dinge nicht mehr digitalisieren, welche man ansonsten digitalisiert hätte. Auch **Florian Schütz** hält die Idee für verlockend, sieht aber einen **kleinen Überlegungsfehler** darin. Heute sei es in einem globalen Markt **nicht mehr primär wichtig, sicher zu**

sein, sondern schnell zu sein. Es gäbe eine **Machtverschiebung von Staaten zu Firmen**, welche auf globalen Märkten agieren. Er zeigte dies mit dem Beispiel von Mikrochips auf, deren Bestandteile alle an anderen Orten auf der Welt hergestellt würden. Viele Dinge lassen sich daher gar nicht mehr manuell bzw. «entdigitalisiert» umsetzen.

Learnings und Take-Aways

In der Schlussrunde gaben die Referierenden noch **wichtige Kernbotschaften** an das Publikum weiter. Für **Jörg Mäder** sind eidgenössische Aufklärungskampagnen wichtig, jedoch müsse ein noch **grösserer Fokus auf die Ausbildung gesetzt werden**, damit IT und OT in Zukunft sauber benützt werden können. **Alexandra Arni** stellte klar, dass die **Digitalisierung hier sei und dass diese nicht mehr rückgängig gemacht werden könne**. Daher müsse man lernen, mit ihr umzugehen. Zudem brauche es ein zunehmendes Bewusstsein für **Eigenverantwortung im Cyberbereich**. Cybersicherheit sei nicht nur etwas für Nerds, sondern müsse alle Teile der Gesellschaft erreichen, bis in die Management-Ebene. Für **Urs Loher** ist Cyber viel umfassender als nur Attacken auf IT-Netzwerke. Genau so viel Effort brauche es auch in das **Bauen von Systemen und in das Entwickeln von Massnahmen**. Das Schlusswort erhielt **Florian Schütz**: «Nehmen Sie die Nerds mit Führungsqualitäten und machen Sie daraus Führungskräfte und zweitens: **Lassen Sie uns mehr in Chancen denken als in Risiken und daran, diese Chancen zu nutzen**.» Mit diesem Plädoyer wurde das Panel geschlossen. Das Publikum hatte daraufhin die Möglichkeit, viele weitere spannende Fragen beim anschliessenden Apéro zu diskutieren.



©Daniel Saxer (iOf App, Defence & Security News)

Wir danken unseren Event-Partnern!

….und unseren Jahrespartnerschaften!