Verstärktes Engagement des Bundes im Bereich Cybersicherheit: Wie sicher ist die Schweiz?

Fazitbericht | 16. FSS Security Talk vom 21. Februar 2024, Swiss Cyber Security Days

Als innovativstes Land der Welt stellt die Schweiz ein attraktives Ziel für Cyberangriffe dar. Viele Unternehmen und Organisationen haben die Gefahr erkannt. Auch beim Bund hat das Thema Cybersicherheit einen hohen Stellenwert und so wurden im vergangenen Jahr weitere wichtige institutionelle und legislative Änderungen beschlossen. Auch am 16. FSS Security Talk, welcher erstmals im Rahmen der Swiss Cyber Security Days stattgefunden hat, wurden diese Veränderungen von namhaften ExpertInnen wie **Martin von Muralt** (Delegierter für den Sicherheitsverbund Schweiz SVS), **Maja Riniker** (Nationalrätin, Mitglied der SiK-N und der Parlamentarischen Gruppe Cyber), **Tobias Schoch** (Chief Security Officer, AXA Schweiz), **Gerhard Andrey** (Nationalrat, Mitglied der SiK-N und der Parlamentarischen Gruppe Cyber) sowie **Florian Schütz** (Direktor des Bundesamtes für Cybersicherheit) diskutiert.

Mit welchen Auswirkungen auf die Cybersicherheitsarchitektur der Schweiz darf durch die Schaffung des neuen Staatssekretariats für Sicherheitspolitik SEPOS und dem Bundesamt für Cybersicherheit BACS gerechnet werden? Inwiefern verändert das Informationssicherheitsgesetz die Mindestanforderungen an die Informationssicherheit des Bundes? Inwiefern steht die Privatwirtschaft in der Eigenverantwortung zur Erhöhung der Cyber-Resilienz?

Diese und weitere wichtige Fragen wurden in der Paneldiskussion erörtert, die von **Fredy Müller**, Geschäftsführer des FORUM SICHERHEIT SCHWEIZ, moderiert wurde. Er begrüsste das Publikum und führte aus, dass mit dem Gespräch das Verständnis der jüngsten Veränderungen in der Cybersicherheitsarchitektur der Schweiz gefördert werden soll.

Ein neuer Rekord

Nach dieser kurzen Begrüssung leitete Fredy Müller mit dem Verweis darauf in das Thema ein, dass Anfang November des vergangenen Jahres die Organisation von Florian Schütz, damals noch das Nationale Zentrum für Cybersicherheit NCSC, 2000 gemeldete Cybervorfälle in einer Woche registriert hatte, was ein neuer Rekord war. Er verwies zudem darauf, dass es sich dabei nur um die gemeldeten Vorfälle handle und daneben eine grosse Dunkelziffer existiere. Er wandte sich den beiden PolitikerInnen zu und wollte von ihnen wissen, ob sie über diese Zahl erstaunt seien.

Maja Riniker bekundete, dass sie kaum erstaunt sei, aber es gleichzeitig sehr zu schätzen wisse, dass es das Bundesamt für Cybersicherheit gäbe, an welches man sich einerseits bei Fragen rund um die Thematik Cyber wenden könne und andererseits die Funktion einer zentralen Meldestelle übernehme. Die Sicherheitspolitische Kommission sei auch immer wieder mit dem Thema der Cybersicherheit konfrontiert, sowie auch mit der Sicherheit im Ganzen. Es sei leider die bittere Realität, dass aktuelle geopolitische Entwicklungen dazu führten, dass man nicht mehr so schnell erstaunt sei.

Gerhard Andrey sei ebenfalls nicht überrascht von der genannten Zahl, er vertrete aber die Auffassung, dass es immer zwei Botschaften gäbe, weswegen das Ganze etwas differenzierter angeschaut werden müsse. Zum einen nehme die Anzahl an Cybervorfällen zwar tatsächlich stetig zu, andererseits würden diese aber auch immer konsequenter gemeldet werden. Als Optimist habe er den Eindruck, dass sich einige Dinge verbessern werden. So wurden beispielsweise bereits einige Gesetzesprojekte auf den Weg gebracht, welche mittlerweile in Kraft seien. Jedoch müsse auch er eingestehen, dass es immer noch Bereiche gäbe, wo die Zustände haarsträubend seien. Somit bestehe gleichzeitig Hoffnung und Desillusion.

Keine Revolution sondern eine Evolution

Folgend auf diese beiden Antworten stellte der Moderator fest, dass seit Anfang des Jahres 2024 wichtige institutionelle Änderungen im Bereich Cybersicherheit in Kraft getreten sind. Darauf stellte er dem neuen Direktor des Bundesamtes für Cybersicherheit, **Florian Schütz**, die Frage, weshalb es denn dieses neue Bundesamt benötigte und was sich mit dessen Schaffung verbessern werde.

Dieser entgegnete, dass der Bundesrat im August 2022 über die Organisationform des damaligen NCSC beraten und zum Schluss gekommen sei, dass die Schaffung eines neuen Bundesamst sinnvoll sei. Denn das NCSC stand etwas quer in der Landschaft, die Angestellten waren dem Generalsekretariat EFD unterstellt, Florian Schütz war als damaliger Delegierter für Cybersicherheit aber direkt dem Bundesrat rechenschaftspflichtig, was zu gewissen Spannungsfeldern führte. Entsprechend seien unterschiedliche Organisationsformen diskutiert worden. Die gewählte Organisationsform gebe dem Bundesrat die Möglichkeit, das Bundesamt direkt zu steuern und das ehemalige NCSC habe als Bundesamt zudem mehr Gewicht. Aus diesen Gründen wurde das NCSC am 1.1.2024 in ein Bundesamt für Cybersicherheit im VBS überführt, um eine bessere Nutzung potenzieller und bestehender Synergien zu erreichen. Erste Synergien seien Anfang Jahr bereits manifestiert worden, weitere würden im aktuellen Jahr analysiert werden. Auf die Frage, was besser werden sollte, antwortete Florian Schütz, dass es sich beim BACS nicht um eine Revolution, sondern um eine Evolution handle. Bestehende Arbeiten werden weitergeführt, gleichzeitig sollen die Prozesse aber optimiert werden, um schneller und effizienter zu sein. Parallel müsse man mit den Kantonen und den Gemeinden staatsebenenübergreifend analysieren, welche Leistungen der Bund zusätzlich erbringen sollte. Auch würden Anforderungen aus der Wirtschaft und der Bevölkerung an das BACS gelangen, welche aber über die Politik definiert und entsprechend behandelt werden müssten.

Fredy Müller wandte sich darauf an Maja Riniker und wollte wissen, ob man in der Sicherheitspolitischen Kommission über diese strukturelle Veränderung informiert wurde.

Maja Riniker glaube, dass mit der Schaffung des Bundesamtes die Wichtigkeit des Themas korrekt adressiert wurde. Denn es werde nicht nur die Cybersicherheit isoliert adressiert, da das neue Staatssekretariat für Sicherheitspolitik sich zusätzlich mit der generellen Sicherheitspolitik befasse. Entsprechend sei die Bedeutung erkannt und die Ressourcen richtig verteilt worden. Zudem führe die Konsolidierung unter einem neuen Titel international zu einer verbesserten und veränderten Wahrnehmung, was insbesondere bei Themen, welche nicht an einer Kantons- oder Landesgrenze aufhören, von immenser Bedeutung sei, denn Austausch und Visibilität seien zentral.

Unklarheiten in den Verantwortungsbereichen der neuen Verwaltungseinheiten

Der Moderator fasste zusammen, dass einerseits das Staatssekretariat für Sicherheitspolitik, das SEPOS, sowie das Bundesamt für Cybersicherheit, BACS, neu geschaffen und somit eine adaptierte Sicherheitsarchitektur im Cyberbereich erreicht wurde. Weiter wollte er von **Gerhard Andrey** wissen, wie wichtig es sei, dass diese Strukturen geschaffen wurden, sowohl als Zeichen nach innen sowie wie auch nach aussen.

Dieser begrüsste die Schaffung des Bundesamtes sehr und erinnerte sich an die entsprechende Ankündigung durch den damaligen Bundesrat Ueli Mauer. Auch erwähnte er, dass er bereits vor der offiziellen Ankündigung im Parlament die Frage gestellt habe, ob ein solches Bundesamt geschaffen werden soll. Der Bundesrat hätte damals aber noch sehr zurückhaltend reagiert. Auch wenn es das BACS jetzt gäbe, sehe er nach wie vor grosse Fragezeichen, insbesondere bezüglich der Organisation. Denn kaum sei das BACS gegründet, werde bereits ein neues Staatssekretariat geschaffen, mit welchem es zu Überlappungen im Tätigkeitsbereich käme. Es bestehe daher der Bedarf, dass mehr Klarheit geschaffen werde. Er fügte an, dass generell etwas Altes richtig funktionieren müsse, bevor etwas Neues begonnen werde. Denn momentan habe man die Situation, dass der Bundesrat noch mit der genauen Umsetzung und Organisation der des Bundesamtes beschäftig sei, obwohl dieses bereits operational war.

Der Moderator spielte **Florian Schütz** darauf die Frage zu, ob es denn nicht zu Kompetenzstreitigkeiten oder zu einem Informationswirrwarr zwischen dem SEPOS, dem Kommando Cyber und dem BACS komme und wie dieser gordische Knoten gelöst werden könne.

Der Angesprochene entgegnete, dass es sich seiner Ansicht nach nicht um einen gordischen Knoten handle. Er sei der Meinung, dass in den vergangenen viereinhalb Jahren in der Zusammenarbeit mit der Armee sehr viel Klarheit geschaffen wurde. Denn die Armee sei für Armeeaufgaben zuständig, währenddem zivile Aufgaben den polizeilichen Behörden auf Stufe Kanton oder Bund zufallen würden, wobei man hier eng zusammenarbeite und sich gegenseitig unterstütze. Das Staatssekretariat nehme primär strategische Fragen der Sicherheitspolitik auf, wovon Cyber lediglich ein Teilstück sei. Es gäbe gewisse Überlappungen, welche man zukünftig abgrenzen wolle und müsse. Durch die Verschiebung der Fachstelle für Informationssicherheit und der Ansiedlung der Betriebssicherheit sowie

Personensicherheitsprüfung im SEPOS, bestehe dort mittlerweile ein Schwerpunkt für interne Sicherheit. Dadurch könne sich das BACS stärker auf seine Kernaufgaben – dem Umsetzen der nationalen Cyberstrategie und dem verbesserten Schutz von Wirtschaft, Bildung, Gesellschaft und Behörden – konzentrieren. Der Bund als Behörde bleibt wichtiger Nutzer der Dienstleistungen des BACS und profitiert von direktem Schutz – präventiv und reaktiv. Als letztes fügte Florian Schütz an, dass es immer verschiedene Modelle gäbe, mit welchen eine solche Zusammenarbeit organisiert werden könne. Daher müsse nun das aktuelle Modell weiter ausgearbeitet und Ende Jahr überprüft werden, ob die Funktionsweise sinnvoll sei.

Der Moderator hackte nach und wollte wissen, was die Fachstelle für Informationssicherheit sei und was deren Ansiedlung im SEPOS bedeute.

Florian Schütz antwortete, dass bevor das ISG in Kraft trat, die Instrumente beim Bund limitiert waren. Damals hätten zwei unterschiedliche Stellen existiert, einerseits die Informatiksicherheitsvorgaben im NCSC und die Informationsschutzvorgaben im Generalsekretariat VBS. Diese Trennung sei schwierig umsetzbar gewesen, zudem konnten beide nur auf den Bund wirken. Mit dem neuen ISG werden die Vorschriften für alle gelten, die Daten des Bundes verarbeiten. Der Bund erhalte dementsprechend zum Beispiel auch Auditrechte, welche davor nicht wahrgenommen werden konnten. Ein Beispiel dafür sei das Third Party Supply Chain Management.

Der Sicherheitsverbund Schweiz – Ein Unikum

Fredy Müller leitete zu einem neuen Thema über und forderte **Martin von Muralt**, den Delegierten des Sicherheitsverbund Schweiz (SVS) auf, dem Publikum zu erläutern, was dessen genauer Aufgabenbereich sei.

Als erstes stellte dieser richtig, dass er nicht der Delegierte des Bundesrates, sondern von Bund und Kantonen sei. Dass sei wichtig, um zu verstehen, was sein Auftrag genau umfasse. Der SVS sei nämlich ein Unikum, dass nur in einem föderalen Staat Sinn mache. Der SVS habe die Verantwortung für die guten Dienste innerhalb der Schweiz, zwischen den drei Staatsebenen im Bereich Sicherheit. Cyber spiele ein wichtige Rolle dabei, sei jedoch nicht der einzige Teil. Die Stärke des SVS liege darin, dass man paritätisch unterwegs sei und die Gemeinden ebenso in jeweilige sicherheitsbezogene Themen eingebunden werden würden. Der Verbund sei agil und nehme die Themen auf, welche zum jeweiligen Zeitpunkt aktuell und gleichzeitig von strategischer sowie politischer Bedeutung seien. Cyber beispielsweise wäre vor zehn Jahren beim SVS noch kein Thema gewesen, habe sich zwischenzeitlich aber zu einem zentralen Element entwickelt, welches auch zukünftig von Bedeutung sein werde. Der SVS stelle einen Mechanismus dar, welcher in der Eidgenossenschaft dafür sorge, dass korrekte Rahmenbedingungen geschaffen werden und dass Bund, Kantone und Gemeinden bei sicherheitsrelevanten Themen miteinander sprechen. Es werde nach Konsens und Gebieten mit Handlungsbedarf gesucht und dafür Massnahmenkataloge sowie Strategien erarbeitet. Der SVS sei demnach heute sowohl im Extremismus und Radikalismus, als auch im Menschenhandel, Cyber und Krisenmanagement tätig sowie bei anderen, zukünftigen Themen, welche bereits in der Pipeline stünden. Der Verbund sei ein Konstrukt, welches den Dialog zwischen den Staatsebenen im Sicherheitsbereich agil und themenbezogen ermögliche. Die Themen seien heute andere, wie sie es in fünf bis zehn Jahren sein werden. Im Cyberbereich habe der SVS heute zwei Rollen. Die erste sei vor ca. fünf Jahren entstanden, als die nationale Cyberstrategie eingeführt wurde und man die bestehenden kantonalen Strategien anpassen musste. Die Erarbeitung der nationalen Cyberstrategie NCS durch das NCSC sei in enger Zusammenarbeit mit den Kantonen erfolgt. Für die Umsetzung der NCS vorgesehen sei eine Fachgruppe Cybersicherheit mit allen beteiligten Partnern auf Bundes-, Kantons- und Gemeindeebene, sodass die Fragen der Selbstbefähigung, der Resilienz und des Incident Managements gemeinsam angegangen und behandelt werden könne.

Fredy Müller zeigte sich sichtlich erstaunt von der Fülle an Aufgaben des SVS und wollte von **Martin von Muralt** wissen, wie viele Mitarbeiter er denn zur Verfügung habe und auf wie viele er als Unterstützung in den Arbeitsgruppen zurückgreifen kann.

Dieser unterstrich erneut, dass der SVS ein Mechanismus oder ein Label sei, welches paritätisch und neutral miteinbinde. Eigene Ressourcen und Entscheidungsbefugnisse habe er dementsprechend, abgesehen von seiner eigenen Geschäftsstelle, keine. Darum falle das Personal des SVS eher gering aus, sie hätten lediglich 5,4 FTE (Vollzeitstellen). Es bestünden jedoch sechs Mitglieder auf Bundes- und weitere sechs auf kantonaler Ebene, welche schliesslich für die Umsetzung verantwortlich seien. Der SVS sei lediglich für die Koordination zuständig, durch welche Handlungsbedarf und Massnahmenkataloge identifiziert und Strategien erarbeitet werden. Die Umsetzung liege dann bei den jeweiligen Partnern. Der SVS könne allenfalls im Nachhinein strategisches Monitoring betreiben und das Ganze begleiten. Man sei aber strategisch und politisch angegliedert und könne daher nicht direkt auf die Personalressourcen zurückgreifen.

Koordination zwischen den verschiedenen Staatsebenen

Der Moderator wollte mehr über die Koordination zwischen den drei Staatsebenen erfahren und fragte, wie die Reaktion auf einen brisanten Cybervorfall aussehen würde.

Florian Schütz war der Ansicht, dass sich die Herangehensweise bei einem Vorfall relativ einfach gestalte. Vorfälle erhielten viel Aufmerksamkeit, da sie spannend anzuhören seien und eine gewisse Dramatik inne hätten. Die Behandlung sei aufwändig und das Finden von Schwachstellen könne herausfordernd sein. Viel schwieriger sei es jedoch, sichere System zu bauen. Wir sollten den Fokus mehr auf die Schaffung von Systemen legen, welche Vorfälle vorbeugen. Dies sei der viel spannendere

Aspekt. Bezüglich eines Cyberangriffes auf einen Kanton antwortete er, dass wenn nur ein Kanton betroffen sei, dieser selbst handle. Wenn dieser dazu nicht in der Lage sei, gelange er an das BACS und erhalte entsprechende Unterstützung. Komplizierter würde es werden, wenn mehrere Kantone betroffen seien und es sich um Vorfälle handle, die eine weitreichende Auswirkung haben, wie das beispielsweise bei Xplain der Fall war. Damals seien nämlich sehr viele Kantone und Firmen betroffen gewesen. Die Koordination in diesem Vorfall habe noch nicht optimal funktioniert. Entsprechend wurde klar, dass ein gewisses Instrumentarium fehle, beispielsweise wie Vorfälle staatsebenenübergreifend gleich eingestuft, koordiniert werden würden und wie mit strategischen Fragen umgegangen werden sollte. Deshalb arbeite das BACS mit KDK, KKJPD, mit den verschiedenen Stellen beim Bund, mit dem SVS aber auch der Politik zusammen, sodass jene Prozesse vereinheitlicht werden können, ohne die Autonomie des föderalen Systems zu beeinträchtigen.

Fredy Müller fragte weiter nach, wie eine solche Zusammenarbeit erfolge, ob es einen regelmässigen Austausch gäbe.

Schütz führte weiter aus, dass man sich von der Vorstellung eines Raumes, in dem regelmässig alle paar Stunden Sitzungen zur aktuellen Situation stattfinden, verabschieden müsse. Das funktioniere in der Praxis und insbesondere im Vorfallmanagement nicht. Es laufe heute alles übers Telefon, verschlüsselte Messanger-Services und digitale Plattformen, auch das BACS betreibe einen digitalen Raum für kritische Infrastrukturen und Kantone. Daneben würden punktuell Abgleichsitzungen gehalten. Wichtig für die Vorbereitung seien die in der Schweiz existierenden Gremien auch auf Kantonsebene.

Wie es denn um das Bewusstsein bezüglich einer erhöhten Cyber-Resilienz gegenüber Cyberangriffen in den Kantonen und Gemeinden sei, wollte Fredy Müller anschliessend von **Martin von Muralt** wissen.

Er vertrete die Ansicht, dass dieses immer grösser werde. Er machte die ergänzende Bemerkung betreffend der Zusammenarbeit der Schweizer Sicherheitsorgane, dass der Austausch im Cybersicherheitsbereich zwischen Bund und Kantonen über die Plattformen des SVS laufen sollte. Das sei kürzlich ermöglicht worden. Denn seit Jahren habe er vorgebracht, dass Florian Schütz Mitglied der operativen Plattform des SVS werden sollte, was nun bewilligt wurde. Nun befinde man sich in einer Pilotphase. Beim SVS seien auch die Gemeinden vertreten, wie bei der obligatorischen Meldepflicht von Vorfällen auf kritische Infrastrukturen ersichtlich werde. Zu dieser Thematik habe man die Gemeinden gefragt, ob sie sich betroffen fühlten und ob je nach Grösse der Gemeinde die Meldepflicht unterschiedlich wahrgenommen würde. Alle Gemeinden hätten aber die Gleichstellung begrüsst. Das zeige auf, dass das Bewusstsein für Cyberrisiken auch bei kleinen Gemeinden vorhanden sei. Er war positiv überrascht, dass die kleinen Gemeinden ohne eigene IT-Fähigkeiten, also jene Gemeinden, die ihre IT an Unternehmen der Privatwirtschaft outgesourced haben, sich des Risikos bewusst seien. Die Herausforderungen in einem föderalen Staat mit unterschiedlichen Strukturen blieben aber weiterhin gross. Zürich könne nämlich nicht mit einer Kleinstgemeinde gleichgestellt und verglichen werden.

Maja Rinker ergänzte, dass diese Befähigung von Personen, von Unternehmen oder Gemeinden, der untersten Staatsebene, sehr wichtig sei. Angriffe oder Missbräuche könnten immer auftreten und es sei daher zentral, dass das Wissen vorhanden sei, wie man damit umgehen müsse. Ein Beispiel aus der Sicherheitspolitischen Kommission veranschauliche diesen Sachverhalt. Es ging darum, dass Asylanträge auch bei den Gemeinden gemacht werden können, welche unterschiedlich organisiert seien. Jedoch seien alle Gemeinden mit Anträgen konfrontiert, welche mit einem gefälschten Pass gemacht würden. Um das zu erkennen, werde ein spezielles Gerät benötigt, wobei nicht die Preisfrage der ausschlaggebende Punkt sei, sondern einerseits die Verfügbarkeit dieser Geräte sowie das ausgebildete Personal. Sie glaube daher, dass der SVS eine sehr wertvolle Aufgabe ausübe. Sie teile dabei auch die Meinung von Florian Schütz, dass durch das System Angriffe vermieden werden müssten und der Staat mehr Schutz bieten sollte.

Eine bessere Übersicht über die aktuellen Cyberbedrohungen dank der neuen Meldepflicht für kritische Infrastrukturen

Mit der Revision des neuen Informationssicherheitsgesetz müssen Betreiber kritischer Infrastrukturen systembeeinträchtigenden Cyberangriffe melden. Was sich dadurch für die Allgemeinheit verbessere, wollte Fredy Müller vom Direktor des BACS wissen.

Florian Schütz erklärte, dass es in der Schweiz seit 2004 für sämtlichen kritischen Infrastrukturen möglich sei, freiwillig Cybervorfälle zu melden. Solche Meldungen hätten zugenommen, aber einige Firmen und Organisationen hätten das Melden ernster genommen als andere. Der Bund und das Parlament seien daher der Meinung gewesen, dass es eine Meldepflicht brauche, um Parität herzustellen, da man auf korrekte Statistiken angewiesen sei. Weil Steuergelder investiert würden, müssten die Statistiken transparent die grössten Problemzonen aufzeigen. Cyber sei leider eine sehr marktschreierische Angelegenheit, was bei den Denial of Service Angriffen vom letzten Jahr offensichtlich wurde. Zeitungen seien plötzlich voll gewesen mit Experten, die den grossen russischen Angriff propagierten. Dabei handelte es sich in Wirklichkeit um einen DDoS-Angriff, welcher nicht einmal einen Einfluss aufs Bruttoinlandsprodukt gehabt hätte. Man habe damit eigentlich nur die Angreifer erfolgreich gemacht, da man ihnen eine grössere Plattform und somit Reichweite gab. Gleichzeitig habe man mit dem Hackerangriff auf Xplain ein schwerwiegendes Problem gehabt. Aufgrund der Meldepflicht sei das BACS verpflichtet, betroffenen Betreibern von kritischer Infrastruktur im Falle eines Angriffs zu helfen. Bislang sei das auf freiwilliger Basis erfolgt. Das werde zukünftig eine Herausforderung werden, denn eine 30% Zunahme der Vorfälle sei gleichbedeutend mit mehr Arbeit. Das BACS bekomme aktuell alle vierzig Minuten eine Information über eine Infektion mit Malware, das betreffe zwar nicht nur die kritischen Infrastrukturen, sondern alle Unternehmen. Er sei der Meinung, dass das BACS zukünftig auch Hilfe für nicht kritischen Infrastrukturen – welche keiner Meldepflicht unterliegen - anbieten sollte. Bezüglich den kritischen Infrastrukturen definiert das Gesetz eine Maximalschranke, wer meldepflichtig sei. Das BACS sei daran, die Verordnung auszuarbeiten und plane eine Vernehmlassung in diesem Jahr, welche die effektive Schwelle definieren werde.

Die Interdependenz von Daten

Aufgrund des Angriffs der chinesischen Hackergruppe „Volt Typhoon“ auf kritische Infrastrukturen in den USA kam der Moderator mit der Frage auf, ob es denn eine Liste mit kritischen Infrastrukturen in der Schweiz gäbe.

Florian Schütz bejahte dies und verwies diesbezüglich auf das Bundesamt für Bevölkerungsschutz, welches zuständig für diese Liste sei. Er vertrete die Ansicht, dass es zentraler sei, dass man sich die Frage stelle, ob es zielführend ist, wenn immer nur von kritischen Infrastrukturen gesprochen werde. Denn Cybersicherheit betrifft alle Unternehmen. Im Rahmen der Meldepflicht sei die Einschränkung auf die kritischen Infrastrukturen sinnvoll, denn es gibt im ISG auch eine klare Definition der kritischen Infrastrukturen. Ein Auftrag des Bundesamtes für Cybersicherheit bestehe heute darin, kritische Infrastrukturen bei einem Vorfall zu unterstützen. Sollte nun aber ein KMU in Schwierigkeiten geraten, könne ihnen nicht direkt vom BACS geholfen werden, die KMU seien etwas überspitzt gesagt auf sich alleine gestellt. Diese Unterscheidung zwischen kritischer und nicht kritischer Infrastruktur sei daher etwas problematisch. Zudem würden rund 75 % der Schweizer Unternehmen weniger als eine halbe Million CHF Umsatz im Jahr machen. Da verbleibe je nach Branche ein Budget für Cybersicherheit von wenigen Tausend Schweizer Franken. Damit könne möglicherweise eine Antivirenlizenz gekauft werden. Wenn entsprechend passieren würde, dass alle Apotheken der Schweiz Opfer eines breitangelegten Ransomware-Angriffs werden, der eine Schwachstelle im System der Apotheken ausnutzt, liege ein systemisches Problem vor, auch wenn eine einzelne Apotheke nicht zwangsläufig

systemrelevant sei. Es ist daher wichtig, dass das BACS auch nicht kritischen Infrastrukturen – wo sinnvoll – helfen kann.

Gerhard Andrey fügte an, dass auch er die Unterscheidung zwischen kritischer und nicht kritischer Infrastruktur gerne etwas hinterfragen möchte. Er wies im gleichen Zug auf die Gefahr hin, dass gewisse Unternehmen einen Betriebsausfall aufgrund eines Cyberangriffes zu einfach akzeptieren würden. Das Problem an dieser Perspektive sei, dass in den allermeisten Vorfällen auch noch andere betroffen seien. Als Beispiel bediente er sich einer Arztpraxis, bei der einige tausend Patientenakten entwendet werden, das habe schliesslich Auswirkungen auf die betroffenen Personen, denn deren Personaldaten wurden veruntreut und könnten weiter missbraucht werden. Genau dieses Betroffenheit von anderen werde in seinen Augen noch viel zu häufig auf die allzu leichte Schulter genommen. Solche Vorfälle hätte es auch bei CH-Media oder der NZZ gegeben, wo plötzlich über die eine Tür die andere aufging. Es sei zentral, dass die Gewichtigkeit der entwendeten Daten beachtet werde und diese nicht als etwas Einzelnes angeschaut würden. Er habe, wie bereits erwähnt, den Eindruck, dass einige Unternehmen etwas fahrlässig damit umgingen.

Was denn die Konsequenzen von gestohlenen Daten seien, fragte der Moderator in die Runde.

Gemäss **Florian Schütz** können die Konsequenzen sehr vielfältig sein. Diese würden von Identitätsdiebstahl zu Verbesserung von Phishing, usw. reichen. Generell gelte aber, was an die Öffentlichkeit gelange, bleibe öffentlich und könne nicht mehr rückgängig gemacht werden. Schliesslich gäbe es verschiedene Instrumente, um gegen Datendiebstahl vorzugehen. Einerseits müsste dazu aber die Strafverfolgungsbehörden weiterhin befähigt werden, solche Gruppierungen auszuschalten. Kurz vor dieser Paneldiskussion sei in den Nachrichten zu lesen gewesen, dass ein internationaler Schlag gegen Lockbit, auch mit Schweizer Beteiligung, gelungen sei. An dieser Stelle gelte es anzumerken, dass die Schweizer Strafverfolgungsbehörden aktiv und effizient seien. Andererseits, müsse das ganze Thema etwas breiter angeschaut werden. Neben der direkten Verfolgung von Kriminellen und dem Beschlagnahmen ihrer Infrastruktur gibt es noch weitere Instrumente. Kriminelle wollen Geld verdienen. Je schwieriger man es den Kriminellen macht und Finanzflüsse unterbricht, desto weniger rentabel wird es für die Kriminellen. Die Schweiz sei hier relativ aktiv auch im internationalen Dialog , zum Beispiel zusammen mit Singapur, im Bereich Anti-Moneylaundring und Counterterrorism Financing Mechanismen für VSOPs resp. Kryptowährungen. Die Schweiz sei auch in internationalen Gremien, beispielsweise der Counter Ransomware Initiative, welche von den USA initiiert wurden und ca. 50 Staaten umfasse, vertreten. Solche Fälle müssten genau überprüft werden und auch die Geldflüsse gelte es zu tracken. Mehr als 95% aller Cybervorfälle seien krimineller Natur, was Good News sei für alle Zuschauer, denn man müsse nicht der Beste sein in der Cyber Defence, sondern einfach besser als die Anderen, da Kriminelle immer den Weg des geringsten Widerstandes wählen würden.

Austausch zwischen der Privatwirtschaft und dem Bund

Darauf wandte sich Fredy Müller dem Vertreter der Privatwirtschaft im Panel, **Tobias Schoch**, und wollte wissen, ob den eine Versicherungsgesellschaft wie die AXA auch zur kritischen Infrastruktur zähle.

Dieser bestätigte, dass die AXA eine kritische Infrastruktur sei. Es existierte, wie das Florian Schütz bereits im Vorfeld erwähnte, eine Definition von kritischen Infrastrukturen und Versicherungen seinen ein Teil davon. Es sei eine Sparte, die weitgreifenden Schutz benötige. Die AXA selbst sei auch davon betroffen und werde aus diesem Grund stark von der FINMA reguliert. Deshalb habe man klare Anforderungen, die erfüllt werden müssen.

Der Moderator wollte von **Tobias Schoch** weiter wissen, ob es seine Art Gremium oder eine Instanz gäbe, über welche ein Austausch zwischen Privatwirtschaft und Bund stattfinde.

Er meinte, dass der Austausch und die Zusammenarbeit mit dem Bund heute ein Schlüsselelement darstelle. Er habe 20 Jahre Erfahrung im IT-Security-Bereich und konnte daher beobachten, dass die Situation damals noch eine ganz andere war wie heute. Das Thema habe an Fahrt aufgenommen, heute werde diese Möglichkeit der Zusammenarbeit immer stärker genutzt. Ein veranschaulichendes Beispiel sei der wöchentliche Call des BACS am Mittwochmorgen, wo sich Betreiber kritischer Infrastrukturen einwählen können und rund eine Viertelstunde informiert würden, was die neusten Angriffe seien und welche Firmen betroffen waren. Diese Calls seien auch für die AXA sehr wertvoll, denn es handle sich um Informationen, die man vorher so nicht hatte, gerade auch nicht in der Geschwindigkeit, wie man sie heute vorfinde. Diesbezüglich habe auch die Digitalisierung stark geholfen, dass ein solcher Austausch überhaupt möglich sei.

Wie die Rückmeldungen auf dieses Angebot ausfallen würden, wollte Fredy Müller von **Florian Schütz** wissen.

Dieser erwiderte, dass die Rückmeldungen sehr positiv ausfallen würden, er jedoch den Eindruck habe, dass sogar ein breit geteiltes Interesse nach noch mehr Austauschmöglichkeiten bestehe. Neben diesen Calls würden hauptsächlich Informationen gewünscht werden, welchen asynchron abgerufen werden können. Da arbeite das BACS bereits daran und man hoffe, diesen Wünschen möglichst bald nachkommen zu können.

Darauf wandte sich Fredy Müller nochmals der Privatwirtschaft zu und wollte wissen, wie eine grosses Unternehmen wie die AXA mit Cyberangriffen umgeht.

Tobias Schoch sehe die AXA nicht in einer besonderen Position, sie seien mit denselben Problemen konfrontiert, mit welchen andere grössere Unternehmen auch zu kämpfen hätten. Die AXA habe möglicherweise den Vorteil, dass das Thema sehr früh erkannt wurde. Er habe vor fünf Jahren bei der AXA begonnen und war davor im Bankensektor unterwegs. In diesem Sektor sei allgemein massiv in die IT-Sicherheit investiert worden. Im Falle der AXA liege der Hauptsitz in Paris und von dort würden klare Anforderungen an die Niederlassung in die Schweiz gesendet werden. Dabei bestehe nicht viel Verhandlungsspielraum, denn schlussendlich ginge es immer darum, die ganze AXA weltweit zu schützen. Sein Team von rund 30 Leuten sei aber zuständig für die Schweiz. Innerhalb der rund 150‘000 Mitarbeitenden weltweit fokussiere sich ein Teil auf die Sicherheit und die Abwehr von Cyberangriffen. Dabei gebe es unterschiedliche Angriffe, nicht jeder „Ping“ zähle als solcher. Es gäbe natürlich auch die internen Angriffe resp. Incidents, wenn Daten fälschlicherweise rausgehen würden, obwohl sie das eigentlich nicht sollten. Dort spiele dann mehr der Datenschutz eine Rolle.

Ein Appell an die Eigenverantwortung der KMU

Der Moderator dachte diesen Gedanken weiter und verwies auf die Aussage von Florian Schütz, dass 75 % der Schweizer Unternehmen KMU jährliche Umsätzen unterhalb von CHF 500‘000 hätten und wollte von den PolitikerInnen wissen, ob sie diese Tatsache nicht beunruhigen würde.

Gerhard Andrey antwortet mit einer bildlichen Analogie. Viele KMU’s liessen übers Wochenende die Tür offen stehen. An jene müsse man appellieren, sodass diese Unternehmen ihre Verantwortung wahrnehmen würden. Er würde den Druck auf diese Schwachstellen erhöhen, weil sie potenziell andere Akteure damit betreffen. Auch in seiner Firma habe er Fälle verzeichnen können, wo Leistungserbringer Probleme hatten und sich dadurch negative Auswirkungen für seine Firma ergaben. Er habe in der Vergangenheit 130 eingeschriebene Briefe verschickt zum Thema „schliesst doch einmal die Türe“. Das seien Basics und grundsätzlich sei jeder für die eigene Sicherheit verantwortlich. Ihm fehle dieses Delta resp. das Bewusstsein, dass andere auch betroffen sein könnten und man selbst vorsichtiger sein müsse. In dieser Hinsicht müsse die Politik tougher sein. Er sehe deswegen eine Lösung in der Organhaftung. Als Verwaltungsrat beispielsweise habe man nicht-delegierbare Aufgaben, wie die Verantwortung sicherzustellen, dass eine Finanzgovernance bestehe, die den Namen auch verdiene. Er sei ebenso der Meinung, dass im 21. Jahrhundert eine Datengovernance zu den nicht-delegierbaren Aufgaben gehöre. Es sei klar, dass jeder für die eigene Sicherheit verantwortlich ist, aber eben auch für die Supply Chain, die Kunden und Kundinnen, und da müsse noch etwas geschehen.

Fredy Müller wandte sich an Maja Riniker mit der Frage, ob solche Vorschläge auch in der SiK-N, der Sicherheitspolitischen Kommission des Nationalrats, besprochen werden. Weiter wollte er wissen, wie dort der Tenor sei und ob alles in der Eigenverantwortung der KMUs liege, wenn Daten fälschlicherweise rausgehen.

Maja Riniker stellte die rhetorische Frage, was eigentlich die Aufgabe der Politik sei. Gemäss Riniker ist diese primär für die äussere Sicherheit zuständig, wo über die Armee diskutiert würde, aber ebenso für die innere Sicherheit, die wichtige Aufgaben beinhalte. Es gehe um Geldwäscherei, Kriminalität, Bundespolizei, etc. Sie vertritt die Meinung, dass jeder Unternehmer selbst für die ersten Verantwortungsschritte zuständig sei und auch die Risiken tragen müsse. Riniker, als FDP-Mitglied und Unterstützerin des Unternehmertums, bewundere jeden Unternehmer, aber der Staat sei nicht dafür zuständig, alle Personen und Unternehmen zu versichern und zu unterstützen. Auf dieser Flughöhe würde nicht diskutiert werden in der sicherheitspolitischen Kommission, das wäre ihrer Ansicht nach auch nicht adäquat. Dennoch anerkennt sie es als eine relevante Diskussion, insbesondere solle geklärt werden, ab welcher Grösse eine Unternehmung eine Cyberversicherung benötigt. Im folgenden Schritt gehe es dann darum zu klären, wer das kontrolliert. „Wenn der Unternehmer nicht dafür sorgt, was sind dann die Sanktionen?“, fragte sich Maja Riniker. Es gäbe Bussen und Strafverfolgungen. Die Schweiz sei in der Ahndung von sehr schlimmen Vergehen noch nicht sehr weit. Es könnten mehr Mittel in die korrekte Strafverfolgung investiert werden. Bevor dort aber nicht mehr Mittel gesprochen seien, ist es Rinikers Meinung nach nicht richtig, jeden „KMUler“ zu verfolgen, wenn er nicht die richtige Cyberversicherung abgeschlossen hat.

Da Martin von Muralt oft mit den Kantonen und Gemeinden zu tun hat, spricht ihn Fredy Müller auf die Thematik Eigenverantwortung und KMU’s an.

Martin von Muralt äusserte sich nicht zu den KMU’s, verwies aber auf die Eigenverantwortung, das Subsidiaritätskriterium, welche in der DNA der Schweiz lägen. Die Gemeinden, Kantone und Bevölkerung seien für sich verantwortlich. Der Bund könne nicht bei jedem Angriff zu Hilfe eilen. Man müsse dafür sorgen, dass Kantone und Gemeinden selbstständig sind. Das seien sie auch bereits weitgehend. Aber Gemeinden seien wie KMU’s, sie hätten nicht unbegrenzte Mittel. Deshalb würden Überlegungen, wie man Synergien und Best Practices nutzt, der Austausch zwischen Kantonen gefördert wird, sei es für die Selbstbefähigung oder Incidence-Bewältigung, sinnvoll. Herr von Muralt war einverstanden mit dem, was Maja Riniker gesagt hatte, die Eigenverantwortung gälte auch für KMU‘s auf Staatsebene. Es blieben die Fragen, wann kann eine Gemeinde und ein Kanton die Unterstützung des Bundes erwarten? Wann kommt Unterstützung vom BACS? Das seien Dinge, die seines Erachtens noch der Klärung bedürften.

Florian Schütz verwies noch auf die Sicherheitsperspektive und Ökonomie. Schlussendlich ginge es um die Frage, „kann ich mir eine Leistung am Markt kaufen und weiss ich, was ich mir eingekauft habe?“ Cyber sei ein lauter Markt und man sehe oft nicht, was bei Käufen auf dem Markt eigentlich erworben wird. Das BACS behandle Fälle, wo Betroffene, wären sie bei einem anderen Internetservice-Provider gewesen, keine Vorfälle erlitten hätten. So haben sie einen hohen zweistelligen Millionenbetrag an Schaden erlitten. Das BACS kann jedoch keine Einschätzung zu den verschiedenen Anbietern geben, denn das wäre wettbewerbsverzerrend. Gleichzeitig wäre es in der Verantwortung der Unternehmer, sich die Frage zu stellen, „was bekomme ich von diesem Vertrag und was lasse ich am Markt überhaupt zu?“ Welche Rolle spielen Konsumentenschutzmagazine dabei? Kaufe man beispielsweise einen Teddybären mit giftigem Farbstoff und das würde entdeckt werden, dann müsste dieser vom Markt genommen werden. Allenfalls kämen Schadensersatzforderungen hinzu. Wird hingegen ein IT-Produkt auf dem Markt verkauft, das voller Schwachstellen ist und Daten ins Ausland abtransportiert, hätte dies keine Konsequenzen. Der Hersteller könnte das Produkt weiterhin verkaufen. Herr Schütz ist weder der Meinung, dass man hier mit der Regulierungskeule vorgehen muss, noch dass Regulierung immer das richtige Instrument ist. Aber es brauche ökonomische Incentives, qualitativ gute Produkte und einen sauberen Prozess, um diese Themen zu adressieren. Jedes Produkt habe Schwachstellen, wenn es auf den Markt kommt, aber diese müssten ernst genommen werden und Konsumenten realisieren, für was sie ihr Geld ausgegeben.

Tobias Schoch knüpfte an und lobte das Beispiel des Vergleichs zu anderen Unternehmungen. Die AXA mache das gleich. Man habe das Ziel, im Banken- und Versicherungsbereich unter den Top 25% zu sein. Das sei im entsprechenden Bereich ein gutes Niveau. Der Verwaltungsrat habe das Ziel ebenfalls abgesegnet, sodass genug investiert werden könne, um in die 25% zu erreichen. Die AXA würde mit 37 Banken und Versicherungen verglichen werden und durchlaufe ein Assessment. Im KMU-Bereich sei es sehr relevant, wie viel «Awareness» beim Management zum Thema vorhanden ist. Oft sei diese Awareness erstaunlicherweise gering. Und dann gehe es nicht lange bis etwas passiert. Herr Schoch war schockiert, wie oft fahrlässig damit umgegangen wird.

Sensibilisierung und Entmystifizierung

Fredy Müller sprach Maja Riniker auf das Vorgespräch an, worin sie von Sensibilisierung und Entmystifizierung sowie Ihren Töchtern gesprochen hatte, die bereits in der Schule darauf aufmerksam gemacht würden.

Maja Riniker war der Überzeugung, dass man sich nicht mehr schämen müsste, wenn ein Fehler begangen wird oder ein Angriff erfolgte. In solchen Fällen biete das Bundesamt für Cybersicherheit eine Anlaufstelle. Sie war der Ansicht, dass man früh mit solchen Thematiken konfrontiert werden sollte. Bereits die beiden Teenager Töchter würden in der Schule sensibilisiert werden. Sie sprach ebenfalls eine gute Freundin an, die eine grosse Unternehmung als CEO verantworte und im vergangenen Jahr einen Cyberangriff erlitten hatte. Die Freundin habe in den Medien darüber gesprochen und gesagt, ohne eine gute Versicherung, welche sofort Liquidität zur Verfügung gestellt hatte, wäre es ihr nicht möglich gewesen, die neue Hardware innerhalb von 3 Tagen wieder zu beschaffen. Man müsse darüber sprechen dürfen und sollte sich nicht mehr schämen müssen. Es brauche eine Entstigmatisierung. Angriffe gehörten zum Alltag und man sollte daraus lernen können, ist Maja Riniker der Meinung.

Gerhard Andrey verdeutlichte diesen Standpunkt. Er sprach Riniker auf ein Panel des Industrietags 2023 an, wo beide vertreten waren. Er war beeindruckt, wie dort einige CEO's hingestanden seien und erzählt hätten, wie es gewesen war, ein Opfer von solchen Angriffen zu werden, was ihre persönliche Verantwortung betraf und wo eventuell Fahrlässigkeit Einzug genommen hatte. Dieses Entmystifizieren von solchen Vorfällen sei auch in Andreys Augen wesentlich. Er spannte den Bogen zum Informations- und Sicherheitsgesetz (ISG), wo er sich eine Erweiterung gewünscht hätte. Seiner Meinung nach hätten Schwachstellen, welche noch nicht bekannt waren, ebenfalls dem ehemals NCSC (Nationales Zentrum für Cybersicherheit) heute das BACS, gemeldet werden müssen. Der Nationalrat hätte zu Beginn noch Gehör gehabt für sein Anliegen, aber die Industrie war noch nicht bereit gewesen.

Fredy Müller sprach **Gerhard Andrey** auf Whistle-Blowing an.

Andrey verneinte von Whistle-Blowing zu sprechen, sondern hätte bei seinen Ausführungen eher an Heartbleed oder Lockbit gedacht (zwei konkrete Schwachstellen). Wenn eine Lücke bei einer kritischen Infrastruktur entstehe und jemand das bemerken würde, hätte er sich gewünscht, dass eine Meldepflicht beim BACS bestünde. Aber so weit war man noch nicht. Andrey war sich sicher, dass es nur eine Frage der Zeit sei, bis diese Pflicht kommen sollte. Am Ende des Tages, sei die Erkenntnis „Bei mir brennt es, dann könnte es bei dir auch brennen", sehr zielführend. Dieser Gedankengang sollte das Ziel sein.

Fredy Müller wandte sich an Florian Schütz und fragte, ob sich bei den wöchentlichen Calls auch KMU's einwählen könnten.

Florian Schütz verneinte, dass nicht kritische Unternehmen teilnehmen können. Momentan seien die Calls auf die kritischen Infrastrukturen beschränkt. Es gäbe aber natürlich auch KMUs die als kritische Infrastruktur gelten. Es gäbe allerdings Pläne, diese zu öffnen, jedoch müsse man sich überlegen, ob die aktuelle Form dann noch Sinn ergebe. Es bringe einer Gemeinde beispielsweise nichts, wenn sie etwas über die grossen internationalen Angriffsvektoren erfahren würde, wenn sie mit der Information nicht umgehen kann. Man müsse das stufen- und bedarfsgerecht steuern.

Fredy Müller richtete das Wort an **Tobias Schoch**. Die AXA sei ein Weltkonzern, die viel investiere. Hohe Investitionen komme die AXA günstiger zu stehen, als wenn Sie Lösegeld bezahlen müsste. Die Schweiz sei ein hochinnovatives Land. Deshalb sei die Awareness in der Schweiz im internationalen Vergleich wahrscheinlich auch höher. Fredy Müller wollte wissen, ob die AXA Schweiz denn stärker betroffen sei von Angriffen als andere Länder.

Gemäss Schoch ist dies nicht der Fall. Die Schweiz sei beispielsweise an gewissen Anlässen, wie dem WEF, im Fokus, wo DDoS-Angriffe stattgefunden hätten. Schaue man heute die Weltordnung an, gebe es im Cyberbereich einen starken Zuwachs an Angriffen zu verzeichnen auch aufgrund des Ukrainekriegs, der jetzt dann 2 Jahre dauere. Diesbezüglich stehe die Schweiz auch im Fokus aber nicht stärker als andere Länder. Schoch sieht ein Vorurteil darin, das Angreifer annehmen würden, in der Schweiz sei viel Geld zu erpressen. Die AXA als grösste Versicherung sei wahrscheinlich stärker im Fokus solcher Angriffe als kleine Versicherungen aufgrund der Geldmenge.

Sicherheitsverbundsübung 2025

Fredy Müller forderte Martin von Muralt abschliessend dazu auf, einige Information zur nächste Sicherheitsverbundsübung «strategische Führungsübung 25» zu teilen und wollte wissen, ob die Sensibilisierung und die Prävention gegen solche Angriffe geübt würden.

Martin von Muralt bestätigte, dass es um Sensibilisierung gehe, jedoch nicht um Prävention, denn es sei Krisenbewältigung und Prävention finde im Vorfeld statt. Es handle sich um eine integrierte Übung, da die Sicherheitsverbundsübungen und die strategischen Führungsübungen zusammengeführt

würden. Zum ersten Mal in der Schweiz werde der Bundesrat gemeinsam mit den Kantons- und Regierungsräten, kritischen Infrastrukturen sowie unter Einbezug der Wissenschaft beübt werden. Das Thema sei bekannt und relativ breit aufgestellt: „hybride Bedrohung auf die Schweiz". Es gebe drei Hauptziele für diese Übung. Erstens wolle man prüfen, wie der Einstieg in die Krise läuft, zweitens die Ausdauerfähigkeit, und drittens die Kommunikationskoordination. Cyber beinhalte Cybersicherheit, Resilienz, Incidence Management, aber auch Cyber Warfare. Letzteres mit Bezug zur Kommunikation gehe oft auf Desinformation zurück. Als Antwort darauf, müsse man sich fragen, „wie meistern, wie reagieren, wie koordinieren wir uns, wenn ausländische Desinformationskampagnen eingesetzt werden?" Das werde im Zentrum dieser Übung stehen.

Erkenntnisse für das Publikum

Fredy Müller wollte zum Abschluss von allen wissen, was die wichtigsten Erkenntnisse für das Publikum im Bereich Cybersecurity seien.

Für **Florian Schütz** war die ganze Thematik staatsebenen- sowie Wirtschafts- und Gesellschafts-übergreifend. Man dürfe den Angriff und die Verteidigung nicht isoliert betrachten, das wäre zu kurz gedacht. Gute strategische Ansätze und Umsetzungen würden einen Mehrwehrt unter Berücksichtigung von gesellschaftlichen und ökonomischen Aspekten schaffen.

Gerhard Andrey stimmte dem zu und ergänzte mit einem weiteren Aspekt. Er sei gleichzeitig ein Mitglied der Finanz- und Sicherheitskommission. Eine Balance zwischen den zur Verfügung stehenden Mitteln und den Sicherheits- sowie Verteidigungsbedürfnissen zu finden, sei nicht einfach. Er äusserte Kritik an den überwiesenen Beträgen, welche in die Armee fliessen und nicht in die Verteidigung. Seiner Meinung nach bekäme so das Mittel und nicht unbedingt der Zweck das Geld. Viele Dinge seien sicherheitsrelevant, nicht nur die Armee und er wolle sich dafür einsetzen, dass man da eine gute Balance findet. Denn nicht alle Risiken, die heute schon schmerzten und in Zukunft noch zunehmen würden, seien mit Blech, Stahl und Kanonen zu bewältigen. Und an dieser Stelle müsste man schauen, dass es nicht aus dem Lot falle und man in einen Militarismus abrutsche.

Gemäss **Tobias Schoch** sei es für die Privatwirtschaft nicht so schwierig, den unmittelbar notwendigen Schutz aufrecht zu erhalten. Dazu gehöre eine Multifaktorauthentifizierung, Verschlüsselungen sowie Immutable Backups für Ransomware-Angriffe, welche eingebaut sein sollten. Das seien Kernelemente, die man implementiert haben müsste. Er war der Meinung, dass auch KMU's mit diesen Kernelementen gut aufgestellt seien. Es biete keinen 100% Schutz, aber es werde ein Schritt vorwärts gemacht. Wenn man hier ein wenig investierte, wüchse die Schweiz als Ganzes in diesem Bereich.

Martin von Muralt sprach die Komplexität der gesamten Thematik an. Diese Komplexität sei allerdings gegeben. Es gebe Cyber Defence, -strafverfolgung und Security. Daneben sei die Verantwortung auf die drei Staatsebenen verteilt, was gleichzeitig den Koordinationsbedarf erhöhe. Es bringe allerdings auch Vorteile mit sich. Dank diesem föderalistischen System entstünden überall neue Ideen und kleine Laboratorien. Das habe einen kreativen Charakter und könnte gute Ideen sowie eine zielführende Zusammenarbeit hervorrufen. Das Zweite sei die Nähe zur Bevölkerung, welche durch die Kantone und Gemeinden gegeben ist. An dieser Stelle bestünde eine grosse Diversität aber auch ein Risiko durch die verschiedenen Anbieter im Cyberbereich. Nichtsdestotrotz biete es auch Schutz, da nicht alles an einem Ort zentralisiert sei und somit die Schweiz nicht an einem Punkt angegriffen werden könnte. Wolle man von Resilienz der Infrastrukturen sprechen, müssten dafür die unterschiedlichen Mittel koordiniert werden, Prozesse und Minimalstandards vorhanden sein und das sei die Herausforderung.

Maja Riniker schloss mit einer Beruhigung. Man gebe in der Politik nicht nur Geld aus für „Stahl und Artillerie". Es gäbe ein Cyberbataillon, man führe eine Cyber-RS durch und forsche auch auf diesem Gebiet. In diesen Bereich fliesse ebenfalls viel Geld. Man sei sich in der Sicherheitspolitischen

Kommission bewusst, dass das Thema Cyber sehr wichtig ist. Die Kommission bestünde möglicherweise nicht aus den Cracks, wie allenfalls das Publikum der Swiss Cyber Security Days, aber das Thema sei immer wieder auf der Agenda sei es im Austausch mit der Landesversorgung, wenn das Bundesamt für Bevölkerungsschutz, der Direktor des Bundesamtes für Cybersicherheit, Herr Schütz, oder die Direktorin vom fedpol, Frau della Valle, in der Kommission ist. Das Publikum könne heute die Sicherheit mitnehmen, dass die Politik mit dem Thema konfrontiert sei und es sicher ernst nehme. Den kompletten Schutz werde es wahrscheinlich nie geben. Aber das Bewusstsein sei vorhanden.

Die Nachfragen zeigten: Das Interesse im Publikum war gross

Fredy Müller bedankt sich und übergibt das Wort dem Publikum.

Eine Zuschauerin fragte, wie die angesprochene Meldepflicht im Falle von Cyberangriffen ausgeführt resp. kontrolliert werden könne.

Darauf entgegnete **Florian Schütz** den entsprechenden Ablauf. Für die Ausführung werde es ein Meldeformular geben. Je nach Branche bestünden bereits Meldepflichten bei Regulatoren, wie es beispielsweise in der Finanzbranche bereits der Fall sei. Man arbeite aktuell daran, dass es möglichst nur eine Meldestelle geben werde, welche die Meldung in einem zweiten Schritt verteilen soll. Das solle sehr niederschwellig geschehen und es sei nicht erforderlich, ins Detail zu gehen. Man wolle keinen zusätzlichen Aufwand aufbürden. Wenn etwas nicht gemeldet werde und das BACS davon erfahren sollte, dann könne die Firma abgemahnt und darauf hingewiesen werden, dass ein meldepflichtiges Ereignis vorläge, was nachgemeldet werden müsse. Wenn die betroffene Organisation der Meldepflicht nach wiederholtem Auffordern nicht nachkommt sollte, könnte eine Busse verordnet werden.

Ein Zuschauer teilte eine Anregung mit den Panelisten. Es sei in der Runde von Eigenverantwortung der Unternehmen gesprochen worden. Er wollte diesbezüglich auf die Finanzindustrie und den Beirat Brunetti des Bundesrates zur Zukunft des Finanzplatzes verweisen, welcher Auslöser für das Milizsystem und die Zusammenarbeit von Bund und Industrie war. Seiner Meinung nach könne der Bund oder die Politik manchmal der zündende Funke sein, der dann die entsprechende Miliz anrege.

Gerhard Andrey könne das unterstützen. Er sprach eine der von ihm eingereichte Interpellation an, in welcher er den Bundesrat fragte, ob man nicht von Best Practice Beispielen lernen könnte. Er sei selbst auch im Verwaltungsrat einer Bank, der Alternativen Bank und kenne daher ein wenig den Umgang. Die FINMA habe schon vor Jahren Rundschreiben gemacht, welche in einer scharfen Tonalität verfasst seien. Deshalb bestünde wahrscheinlich weniger Angriffsfälle in der Finanzindustrie, jedoch gelte es zu beachten, dass die Branche schon früh scharfe Transaktionen gemacht habe. Er habe in seiner Interpellation den Bundesrat gefragt, ob es bereits Aufsichtsorgane in Industrien gäbe, die ähnlich wie die FINMA für die jeweiligen Bereiche die Aufsicht übernehmen könnten. Die genaue Antwort des Bundesrats könne er nicht mehr wiedergeben. Aber er spreche sich klar dafür aus, auf guten Beispielen aufzubauen.

Fredy Müller schloss darauf das Plenum und bedankte sich beim Publikum für die Aufmerksamkeit sowie bei Jürg Walpen und Nicolas Mayencourt für die Organisation der Swiss Cyber Security Days.