Cyber-Sicherheit in der Digitalisierung – eine Herausforderung für Staat, Wirtschaft und Gesellschaft

Verschriftlichung des Vortrags von Florian Schumacher

Florian Schumacher sprach zum Thema Cybersicherheit und ging dabei auf die drei Felder Staat, Wirtschaft *und* Gesellschaft *ein. Sein Vortrag umfasste zuerst die Gefährdungslage und den aktuellen Lagebericht und im Anschluss das Bundesamt für die Sicherheit in der Informationstechnik (BSI) und zwei konkrete inhaltliche Aufgaben: Schutz von kritischen Infrastrukturen und Cybersicherheit für die Gesellschaft und Dialog. Er selbst arbeitet im Bereich* Cybersicherheit für die Gesellschaft *und kümmert sich um das Thema* Gesellschaftlicher Dialog.

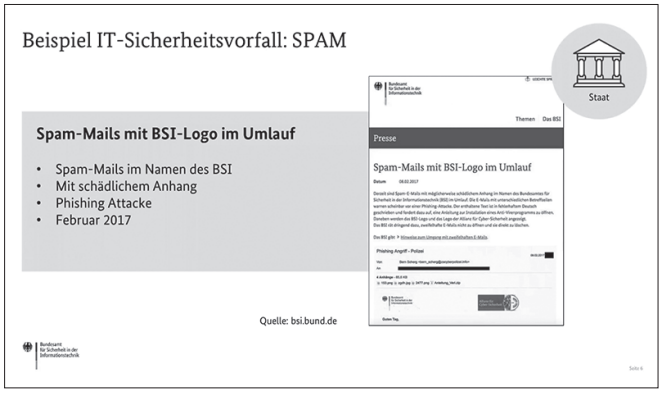
Florian Schumacher beginnt mit der Frage, warum es wichtig ist, sich mit dem Thema Cybersicherheit zu beschäftigen. Er verweist auf Rainer Rehak, der im Rahmen der FIfFkon gesagt hat, Digitalisierung sei kein Thema, das uns jetzt erst seit kurzem beschäftige, sondern sei schon ein lang laufender Prozess. Florian Schumacher weist jedoch darauf hin, dass gerade die Digitalisierungsentwicklung in den letzten Jahren, verkürzt dargestellt durch die drei Begriffe der Vernetzung, der Komplexität und der Allgegenwärtigkeit von IT, es notwendig macht, sich mit dem Thema Cybersicherheit zu beschäftigen. Cybersicherheit stellt eine Voraussetzung für das Gelingen der Digitalisierung dar. Da die Digitalisierung all unsere (sensible) Lebensbereiche durchdringt, sind wir abhängig von der Funktionsfähigkeit und Sicherheit der IT. Sie betrifft uns individuell in unserer Privatheit, in der Sicherheit unserer Daten, aber auch unsere öffentliche Sicherheit.

Cyberangriffe und Cyberkriminalität sind sehr lukrativ, da man damit sehr viel mehr Geld verdienen kann als beispielsweise mit Drogenkriminalität. Florian Schumacher verweist Interessierte explizit auf den BKA-Lagebericht zu Cybercrime. Außerdem sind Cyberangriffe sehr gezielt und oft lange Zeit vom Opfer unbemerkt, wie vergangene APT- (*Advanced Persistent Threat*-) Angriffe zeigen. Und Cyberangriffe verursachen einen großen volkswirtschaftlichen Schaden von durchschnittlich 55 Milliarden Euro im Jahr. Die verwendeten Schadprogramme zeichnen sich durch eine sehr große Varianz und Schnelllebigkeit aus. Begünstigt werden Cyberangriffe durch ein bestehendes Qualitätsproblem der Software, was die Zahl der bestehenden Sicherheitslücken in den zehn meistgenutzten Softwareprodukten zeigt.

Aktuelle Beispiele für Sicherheitsvorfälle

Florian Schumacher nennt nun einige aktuelle Beispiele von Cybersicherheits- oder IT-Sicherheitsvorfällen und beleuchtet einige Phänomene.

Spam



Er beginnt mit dem Thema *Spam*, vor dem auch das BSI nicht gefeit ist. Es gibt Akteure, die sich Vertrauenswürdigkeit zu Eigen machen und dann Logos des BSI oder auch anderer Unternehmen und Institutionen nutzen, um damit kriminell vorzugehen. Beim Thema Spam gibt es eine Verknüpfung von verschiedenen Phänomenen. Es werden beispielsweise Botnetze genutzt, um Spam zu versenden und Spam wird als konkrete Dienstleistung im Darknet angeboten. Um an die Empfänger-E-Mail-Adressen und -Daten zu kommen, werden Datenabflüsse großer Dienstleister oder Kontaktdaten aus E-Mail-Clients von infizierten Systemen genutzt. Teilweise findet auch die Recherche nach konkreten Kontaktdaten statt.

Advanced Persistent Threat (APT)

Ein Beispiel für einen *APT-Angriff* stellt der Regierungshack dar. Es gab einen Hack der Lernplattform ILIAS (Integriertes Lern-, Informations- und Arbeitskooperations-System) der BAKöV (Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat), die an den IVBB (Informationsverbund Berlin-Bonn), also das Behördennetz, angeschlossen ist. Dort wurde ein Trojaner eingeschleust, und darüber konnten dann Dokumente beim Auswärtigen Amt ausgeschleust werden. Insgesamt sind die Auswirkungen aufgrund guter bestehender Sicherheitsmechanismen gering. Außerdem war die Beobachtung der Tätergruppierung möglich.

Im allgemeinen stellt Florian Schumacher im Bezug auf APT-Angriffe einen Zuwachs an Installer- oder Update-Hijacking in der initialen Phase fest. Das heißt, es findet eine Schadcodeinfizierung auf Webseiten oder Updateservern von Softwareherstellern statt. Dort werden dann Schadprogramme eingeschleust, die vom Nutzer unbewusst heruntergeladen werden. Das Ziel hinter APT-Angriffen ist Spionage oder auch Sabotage.

Distributed Denial of Service (DDoS)

Ein weiteres Phänomen sind sogenannte DDoS-Angriffe. Dabei wird versucht, wie am Beispiel der RWE AG, durch eine Vielzahl von Anfragen ein System in die Knie zu zwingen. Bei diesem Phänomen lässt sich eine steigende Tendenz und eine große Bandbreite beobachten. Aufgrund größerer verfügbarer Bandbreite werden Angriffe auf Systeme mit beispielsweise 1 GBit/s durchgeführt. Im Jahr 2018 wurde vom BSI auch eine Rekordbandbreite bei solchen Angriffen festgestellt. Es gab im Frühjahr einen Angriff mit 1,7 TBit/s. Die Motivation der Angreifer in solchen Fällen sind erneut Sabotage, Vandalismus, Manipulation von Systemen oder die einfache Störung.

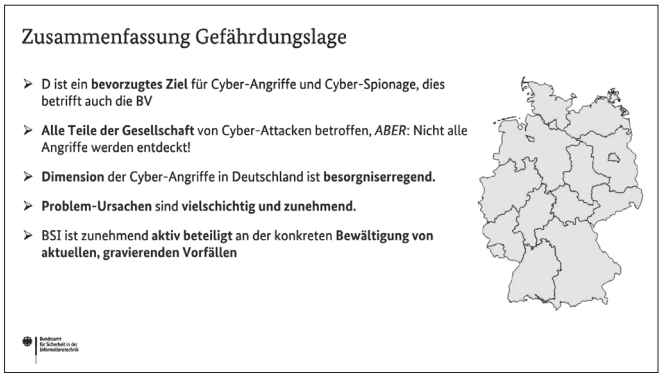
Ransomware

Vom Thema *Ransomware* war im letzten Jahr beispielsweise die Bahn betroffen. Es werden dabei unternehmensinterne Dateien abgegriffen und verschlüsselt und die Angreifer verlangen von den Opfern Geld, um die Dateien wieder zu entschlüsseln. Da einige Opfer kein Backup hatten, gab es manche, die darauf hereingefallen sind und dieses Geld gezahlt haben. Trotzdem haben sie möglicherweise am Ende gar keinen Schlüssel zugesendet bekommen. Das BSI hat generell davon abgeraten, solche Lösegeldzahlungen zu leisten. Generell sind Ransomware-Angriffe meist keine gezielten Angriffe, sondern Massenangriffe, und sehr viele Unternehmen waren davon auch schon betroffen. Eine Umfrage der Allianz für Cybersicherheit, die vom BSI betrieben wird, zeigt, dass 22,5 % der befragten Wirtschaftsunternehmen bereits im Jahr 2017 einen Ransomware-Vorfall hatten. Ein Trend, den das BSI in diesem Fall beobachtet, ist „Ransomware as a service". Das heißt, dass auch weniger technik-bewanderte Nutzer Ransomware-Angriffe mieten und nach dem Baukastenprinzip den Angriff zielgenau auswählen können. Das läuft interessanterweise manchmal in einem Partnermodell ab, bei dem der Dienstleister als Bezahlung einen Teil des Lösegeldes bekommt.

Identitätsdiebstahl

Als letztes Phänomen werden *Identitätsdiebstähle* vorgestellt. Dabei ist der *Yahoo-Hack* am bekanntesten. Er stellt den größten öffentlich bekannten Angriff dar, von dem drei Milliarden Nutzerkonten betroffen waren. Sehr bedauerlich war dabei, dass der Angriff aufgrund der intransparenten Vorgehensweise erst mit großem Zeitabstand bekannt wurde. Das BSI hat in dem Fall eine Kooperationsbereitschaft von Yahoo gegenüber den deutschen Behörden erlebt. In Deutschland selbst sind von solchen Angriffen natürlich die Organisationen betroffen, die sensible Daten haben, wie beispielsweise Banken, Online-Bezahlsysteme

oder auch Online-Händler. In diesen speziellen Fällen machen sich die Angreifer gerade die Vertrauenswürdigkeit der Systeme zunutze. Beispielsweise kommt seit Ende 2017 bei Phishing-Webseiten *https* zum Einsatz, um dem Nutzer eine größere Vertrauenswürdigkeit der Seite zu vermitteln. Daneben versucht man die Leute zu erreichen, indem man medienpräsente Themen wie DSGVO oder Blockchain auf solche Fake-Seiten setzt, so dass der Laie sich für dieses Thema interessiert und dann vorschnell darauf hereinfällt.



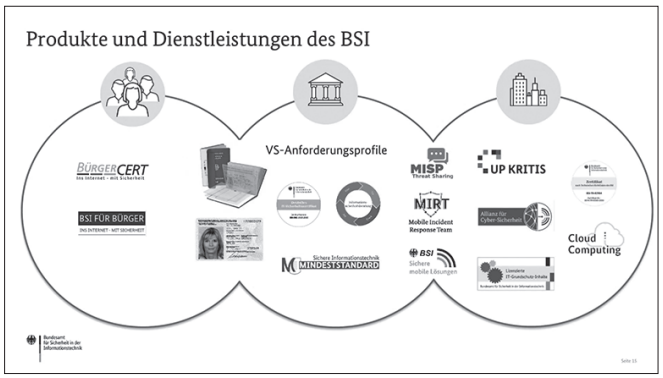
Diese verschiedenen dargestellten Phänomene sollen zeigen, dass von Cyberangriffen und Cyberattacken verschiedene Teile der Gesellschaft betroffen sind, also sowohl staatliche Akteure, wie beispielsweise beim Regierungshack, als auch Wirtschaftsakteure, wie beispielsweise bei RWE, oder natürlich auch kritische Infrastrukturen, wenn Industrieanlagen angegriffen werden, ebenso wie individuelle Nutzer. Das gilt auch für Ransomware- oder Identitätsdiebstahl-Angriffe. Generell lassen sich aus Sicht des BSI viele Angriffe durch einfache geeignete Basismaßnahmen in den Kategorien Prävention, Detektion und Reaktion verhindern oder zumindest in den Auswirkungen minimieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Übersicht dieser verschiedenen Gefährdungen und Risiken, die es in der digitalen Welt gibt, zeigt, dass es eine Stelle erfordert, die sich mit dem Thema beschäftigt und Kompetenzen besitzt, um mit diesen Risiken umzugehen. Das BSI fungiert als diese nationale Cybersicherheitsbehörde und hat dort einen Gestaltungsanspruch in den drei Themenfeldern: präventive Maßnahmen umzusetzen, Detektionsmechanismen zu entwickeln und dann auch reaktionsfähig zu sein. Es versteht sich mit einem ganzheitlichen und kooperativen Ansatz als Dienstleister für die drei Zielgruppen Staat, Wirtschaft und Gesellschaft. Das BSI ist die einzige Behörde mit einem klaren gesetzlichen Auftrag zur Cyberabwehr.

Entwicklung und Aufgaben

Florian Schumacher beschreibt das BSI mit den drei Schlagworten *Veränderung*, *Attraktivität* und *Vernetzung*. Das BSI wurde 1991 gegründet und war ursprünglich nur zuständig für die Absicherung der Regierungskommunikation. Grundaufgaben waren die Verschlüsselung und die Sicherung vertraulicher Regierungskommunikation. Über die Jahre hat sich das geändert und es wurden Informationen und Sensibilisierungsangebote für Bürgerinnen und Bürger bereit gestellt. Hinzu kamen der Schutz von kritischen Infrastrukturen und Aufbau von Austauschformaten für Wirtschaftsunternehmen, Austausch von Erfahrungen und Best Practices etc. In den letzten Jahren ist das BSI stark gewachsen. 2015 hatte das BSI knapp über 600 Mitarbeiter, aktuell sind es ca. 940 und es wird einen weiteren Wachstumstrend geben. Das ist auch ein Indiz dafür, dass das Thema Cybersicherheit stark an Relevanz gewonnen hat und und in der öffentlichen Wahrnehmung präsent ist. Das BSI gehört laut Umfragen zu den Top-Arbeitgebern, das gilt auch im Vergleich zu anderen Behörden. Es verfügt über einen im Vergleich zur Branche überdurchschnittlich hohen Frauenanteil. Das BSI ist eine technische Behörde mit 80 % MINT-Hintergrund. Bei Vernetzung geht es nicht nur um die nationale Vernetzung. Das BSI möchte auch in der Fläche präsenter sein und hat dazu ein Verbindungswesen mit Schwerpunktregionen aufgebaut. Aber auch international ist es sehr anerkannt. Es vertritt die Bundesrepublik in vielen internationalen Gremien der Organisationen, in denen die Bundesrepublik vertreten ist, beispielsweise bei der NATO als verantwortlicher Stelle für das Thema Cybersicherheit und Cyberabwehr oder bei ENISA (European Union Agency for Network and Information Security) als Mitglied im Management-Board. ENISA ist die europäische Organisation, die sich mit dem Thema Cybersicherheit beschäftigt.



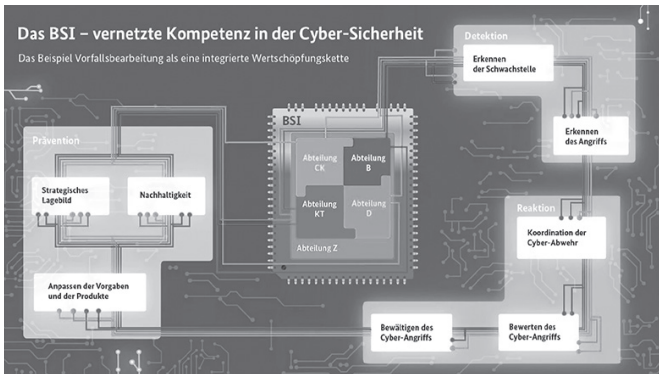
Zielgruppen

Für die drei genannten Zielgruppen, Staat, Wirtschaft und Gesellschaft gibt es ein Produktportfolio und eine Produktübersicht, wovon Florian Schumacher einige Produkte vorstellt, um einen Gesamtüberblick darüber zu geben, was das BSI macht. Angefangen bei der Gesellschaft sind die Angebote zu nennen, die den Bürger direkt adressieren. Es gibt das BürgerCERT (Computer Emergency Response Team), welches Warnmeldungen über aktuelle Sicherheitsvorfälle herausgibt, auf die Bürger und Bürgerinnen achten müssen, oder Informationen zu Updates bereitstellt. Außerdem existiert *BSI für Bürger* mit verschiedenen Informationsmaterialien und konkreten Checklisten und Broschüren, Onlineauftritten, einer Hotline und einem Servicecenter, bei dem man sich melden kann, wenn es Probleme gibt.

Dann gibt es den Übergang zum Bereich Staat. Das BSI ist bei der Entwicklung von Anforderungen zur Sicherheit elektronischer Identitäten dabei oder entwickelt diese maßgeblich. Sei es beim neuen Personalausweis als auch beim Reisepass. Daneben gibt es dann Angebote, die sich direkt an den Staat richten. Wie bereits gesagt: Das BSI kommt aus dem Bereich der Sicherung der Regierungskommunikation. Da ist das Thema VS-Anforderungsprofile zu nennen. Also wie sichere ich Verschlusssachen?

Was ist dort bei der elektronischen Bearbeitung zu beachten? Dann aber auch das Thema ISMS (Informationssicherheits-Managementsystem). Wie baue ich ein ISMS für meine Behörde auf? Dort gibt es Kollegen, die konkret beraten. Als auch das Thema Mindeststandards. Dort gibt es einen Bereich im BSI, der konktret auch Mindeststandards für bestimmte Themen der Bundesverwaltung entwickelt.

Wenn wir jetzt hinübergehen zum Bereich der Wirtschaft: Dort gibt es auch Themen, die mehr die Schnittstellen betreffen. Da gibt es Plattformen zum Informationsaustausch, wie eine Plattform zum Austausch über Gefährdungsindikatoren bei Malware, die Malware-Informationsharing-Platform. Dann gibt es MIRT-Teams: *Mobile Incident Response Teams*, die sich bei Cybersicherheitsvorfällen an staatliche Stellen, aber auch an Betreiber kritischer Infrastrukturen richten und dann konkret helfen; im Einzelfall flexibel zusammengesetzt werden nach den Experten, dies es für diesen Vorfall braucht, um dann vor Ort zu helfen. Als dritter Punkt: sichere mobile Lösungen, das heißt Lösungen, auf denen man auch eingestufte Informationen bearbeiten kann, sei es ein Smartphone oder ein Tablet, wo es auch eine konkrete Lösung gibt. In dem Feld Wirtschaft gibt es auch unterschiedliche Angebote, die das BSI vorhält. Da werde ich dann gleich noch einmal konkreter zu sprechen kommen zu dem Thema *UP-KRITIS*, einer Plattform der öffentlich-privaten Kooperation von KRITIS-Unternehmen, Verbänden, die mit KRITIS-Unternehmen zu tun haben, und den zuständigen staatlichen Stellen – das sind ja auch ganz unterschiedliche Stellen und Aufsichtsbehörden – um gemeinsam an einem höheren Sicherheitsniveau für kritische Infrastrukturen zu arbeiten.



Dann die Allianz für Cybersicherheit, die als Netzwerk fungiert, als Plattform, wo es zum Erfahrungsaustausch kommen kann von Wirtschaftsunternehmen, mit inzwischen ca. 3000 Mitgliedern. Und das soll auch ein bisschen als Multiplikator dienen, als Netzwerk für das Netzwerk: Das heisst, einzelne Akteure können dort Vorträge halten, können dort Best Practices vorstellen für andere Netzwerkmitglieder. Darüber hinaus gibt es den IT-Grundschutz, der sicherlich auch manchem bekannt ist. Das heisst, ein Instrument, in dem IT-Sicherheitsmaßnahmen aufgeschrieben sind, als systematischer Katalog. Dort ist es möglich für Unternehmen oder auch andere Akteure, sich diesen Katalog anzusehen und dort zu identifizieren: Welche Sicherheitsmaßnahmen brauche ich speziell in meinem Kontext und wie kann ich sie umsetzen?

Für das Thema Cloud-Computing hat das BSI ebenfalls einen Anforderungskatalog entwickelt, der sich an Cloud-Anbieter richtet. Dies ist ein Katalog von Mindestanforderungen, die es zu erfüllen gilt. Und nach diesem Katalog kann sich dann das Unternehmen testieren lassen von einem Wirtschaftsprüfungsunternehmen.

Organisation

Wie arbeitet das BSI konkret? Das möchte ich an einem Beispiel der Vorfallsbearbeitung darstellen. Das BSI besteht aus fünf Abteilungen:

- der Abteilung CK, die sich um die operative Abwehr kümmert, aber auch um KRITIS,
- der Abteilung B, in der ich arbeite, die sich um das Feld Beratung für Staat, Wirtschaft und Gesellschaft kümmert,
- der Abteilung D, die sich mit Mindeststandards und Zertifizierung auseinandersetzt,
- die Abteilung KT, das sind die Kryptographen,
- daneben die Abteilung Z, die sich mit Organisation und Personal beschäftigt.

Wie läuft das ab? Holzschnittartig beschrieben im Bereich der Vorfallsbearbeitung: Bei der Detektion würde beispielsweise die Abteilung CK überhaupt erst einmal über das Lagezentrum feststellen, dass es zu einem Angriff gekommen ist, das heißt die Erkennung von Schwachstellen und Angriffsmethoden. Dann im Bereich der Reaktion und Koordination über das nationale Cyberabwehrzentrum, welches auch dort angesiedelt ist: Bewerten des Angriffs, vielleicht auch Bewerten, was dieser Angriff für Auswirkungen für Unternehmen hat. Was hat er für Auswirkungen für die Bundesverwaltung? Müssen wir dort gewisse Anforderungen erhöhen? Gibt es vielleicht auch Effekte, die sich dann wieder auf die Prävention auswirken müssen? Müssen irgendwelche kryptographischen Verfahren angepasst werden? So fügt sich das dann zusammen, wo jede Abteilung die eigenen Kompetenzen einbringt, allerdings dann auch das nach außen gegenüber ihren Stakeholdern darstellt.

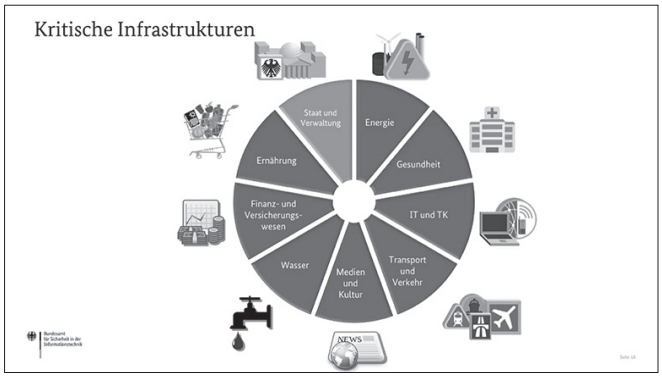
Tätigkeitsfelder des BSI

Um zum konkreten Beispiel zu kommen, zu zwei Feldern in denen das BSI aktiv ist: Ich möchte einmal das Feld KRITIS vorstellen, *Kritische Infrastrukturen* – auch auf konkreten Wunsch der Organisatoren – um zu zeigen, was das BSI macht in diesem Feld, und dann komme ich gleich noch zum Themenfeld *Gesellschaftlicher Dialog*.

Kritische Infrastrukturen (KRITIS)

Kritische Infrastrukturen sind essenziell wichtig für unser tägliches Leben; ihre Betreiber sind essenziell wichtige Dienstleister, sonst hätten wir hier kein Licht, könnten nichts essen, etc. Das Feld wurde in neun Sektoren unterteilt. Wenn wir uns dies ansehen und an unser tägliches Leben denken, stellen wir fest, diese verschiedenen Sektoren sind stark von Informations- und Kom-

munikationstechnologie (IKT) durchdrungen und können auch gar nicht ihre Dienstleistung erbringen, ohne dass sie eine funktionierende Unterstützung durch IKT haben. Seit 2015 gibt es mit dem IT-Sicherheitsgesetz eine gesetzliche Grundlage zum Schutz von kritischen Infrastrukturen und das BSI setzt dieses IT-Sicherheitsgesetz um, das heisst, beim BSI können sich Unternehmen aus dem Bereich der kritischen Infrastrukturen, die unter diese Definition fallen und aus diesen Bereichen kommen, registrieren. Sie werden dort in ein Meldewesen eingebunden, das heisst, wenn sie einen IT-Sicherheitsvorfall haben, wird dieser ans BSI gemeldet, und gleichzeitig überprüft das BSI die Umsetzung von Sicherheitsmaßnahmen dann durch Audits.



Für die verschiedenen Zielgruppen des BSI haben wir eine Dienstleistungspyramide entwickelt, die so zu verstehen ist, dass das, was ganz unten ist, das Thema Information, den geringsten Bereitstellungsaufwand hat. Das steigt dann immer weiter nach oben. Natürlich wäre der höchste Aufwand, wenn das BSI oder Kollegen des BSI konkret technische Schutzmaßnahmen übernehmen. Das ist im Bereich KRITIS nicht vorgesehen. Bei anderen Organisationen oder beim Staat sieht das dann anders aus. Das BSI hat ein ziemlich breites Angebot, wenn man diese Pyramide betrachtet für den Bereich der kritischen Infrastrukturen. Angefangen unten natürlich beim Thema Information. Den IT-Grundschutz hatte ich schon genannt, Es gibt aber auch technische Richtlinien, nach denen man sich richten kann. Es gibt Cybersicherheits-Empfehlungen. Das Thema Abstrahlprüfung könnte auch interessant sein. Es gibt allgemeine Lageberichte und es gibt spezielle Lageberichte, auch für kritische Infrastrukturen.

Das BSI ist aber auch tätig für kritische Infrastrukturen im Bereich der Aus- und Fortbildung, das heisst, wir gehen auf Veranstaltungen von Verbänden etc., wo für Themen der Cybersicherheit sensibilisiert wird.

Und dann in der Mitte eins der wichtigsten Felder: Kooperation. Weil gerade bei KRITIS, aber auch generell, das BSI einen kooperativen Ansatz hat. Es sind keine Alleingänge möglich. Das betrifft sowohl die Unternehmen als auch das BSI selbst. Das heißt, es gibt UP-KRITIS als Plattform, wo 600 verschiedene Akteure (Unternehmen, Verbände, staatliche Akteure) organisiert sind mit Branchen und Themenarbeitskreisen. Die Branchen richten sich nach den verschiedenen Themenbereichen, die ich dargestellt habe. Dann gibt es die Allianz für Cybersicherheit, das heisst, Unternehmen, die nicht unter die KRITIS-Definition fallen, wie beispielsweise Institutionen mit besonderem staatlichem Interesse, können sich auch in dieser Allianz organisieren. Wie ich schon sagte, dies ist eine große Gruppe von Akteueren. Dort gibt es wiederum Themenarbeitsgruppen und andere Angebote, wo man sich auch austauschen oder Informationen einholen kann. Sie veranstalten Cybersicherheitstage, die um ein spezielles Thema gehen. Das heißt, wenn ich Input zu einem speziellen Thema brauche, kann ich dorthin gehen. Das Thema nationales Verbindungswesen habe ich eben schon erläutert.

Dann gibt es aber auch konkrete Beratungsdienstleistungen, die durch das IT-Sicherheitsgesetz reguliert sind. Beispielweise meldet ein Unternehmen einen Vorfall und kann dann auf diese Beratungsdienstleistungen zurückgreifen. Aber es gibt auch vom BSI zertifizierte Dienstleister, die in einem solchen Fall konkrete Hilfe vor Ort leisten können.

Technische Unterstützung und Dienstleistungen: Die Abkürzung B3S bedeutet, es gibt branchenspezifische Mindeststandards, das heisst, die Unternehmen müssen sich nach dem Stand der Technik richten und können dann für sich als Branche einen Stand der Technik definieren. Dieser wird dann vom BSI überprüft. Es gibt schon verschiedene Bereiche, die das für sich getan haben. Wer heute auf die BSI-Webseite klickt, wird sehen, es wurde kürzlich erst aus dem Bereich der Fernwärme ein branchenspezifischer Standard definiert. Dieser wurde beim BSI vorgelegt und bestätigt. Die Unternehmen dürfen sich jetzt nach diesem Stand der Technik richten. Der Sinn dahinter ist, dass sie einen Standard haben, an dem sie sich orientieren können, aber es auch eine Breitenwirkung hat, wenn Unternehmen nicht unter die KRITIS-Definition fallen, dass sie dann darauf blicken können und sagen können, was ist Best Practice, was könnte ich machen in meinem Bereich, um vor Angriffen sicher zu sein und mich dort zu schützen. So viel zum Thema KRITIS.

Cybersicherheit für die Gesellschaft

Ich möchte jetzt als letztem inhaltlichem Punkt noch zum Thema *Cybersicherheit für die Gesellschaft* kommen, in dem ich persönlich arbeite. Ich habe vorhin schon einmal den Überblick gegeben über Produkte und Dienstleistungen, die das BSI anbietet. Dort waren beim Thema *Bürger* eher Angebote, die sich direkt an diesen richten. Wir in unserem Referat sprechen eher die organisierte Zivilgesellschaft an und möchten da eher in einen Austausch kommen, um gemeinsam zu gestalten, denn wir sind der Überzeugung, dass wir nicht im Elfenbeinturm sitzen und selbst alles am besten wissen, sondern dort auch in einen Austausch kommen müssen, um Erwartungen, Bedürfnisse und Ideen identifizieren zu können. Und das nicht nur mit dem Staat, nicht nur mit der Wirtschaft, sondern auch eben auch mit gesellschaftichen Akteuren, und am besten sprechen diese auch noch miteinander.

Und deshalb ist dort unser Ansatz das BSI als gesamtgesellschaftlicher Gestalter von Cybersicherheit. Das heißt, wir möchten zum einen eine Plattform bieten für diesen Austausch. Wie auch schon in der Einleitung gesagt, geht es dort um einen Austausch von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft zu strategischen gesellschaftlichen Themen, um gemeinsam neue Lösungsansätze durch diesen Multi-Stakeholder-Dialog zu erzielen. Wie am Anfang schon sagte, gibt es verschiedene Personen auch hier im Raum, die daran schon teilgenommen haben. Ich möchte darauf auch gleich weiter zu sprechen kommen.

Als zweiten Punkt: mit starken Partnern zusammenarbeiten. Es ist sinnvoll, in verschiedenen Feldern mit Akteuren zusammenzuarbeiten, die vielleicht schon ein spezielles Wissen haben, oder die besondere Befugnis haben. Als Beispiel ist hier die Zusammenarbeit des BSI mit den Verbraucherzentralen zu nennen, weil die Verbraucherzentralen ein sehr gutes Wissen haben, was den Verbraucher angeht, weil sie eine größere Nähe zum Verbraucher haben durch das Beratungsangebot überregional, aber auch bestimmte rechtliche Befugnisse, die das BSI so nicht hat. Und so lassen sich dann diese Befugnisse und Kompetenzen sehr gut kombinieren. Als ein Beispiel der Nutzung dieser Kombination aus Kompetenzen und Befugnissen ist eine Klage anzusehen, die die Verbraucherzentrale NRW erhoben hat, wo es um die Sicherheit von Smartphones geht. Jeder kennt es: Wenn man in einen Elektronikmarkt geht oder online mal nachsieht, was es so für Smartphones im Angebot gibt, beispielsweise Android-Smartphones, dann sieht man, dort gibt es auch noch sehr viele Smartphones mit einem veralteten Betriebssystem, beispielsweise Android 4.1. Als interessierter Nutzer weiß ich: „Veraltetes Betriebssystem! Ich habe da schonmal was von *Stagefright* gehört. Es könnte Probleme mit der Sicherheit des Handys geben!“ Als Laie weiß ich das wahrscheinlich nicht und gehe in den Laden und erwarte ein neues Smartphone, welches funktioniert. Über diesen Umstand informiert der Verkäufer aber nicht: Dass das Smartphone eigentlich ein veraltetes Betriebssystem hat, welches über eklatante Sicherheitsmängel verfügt. Und das, glauben wir, ist ein Umstand, der geändert werden muss und es befindet sich gerade in der gerichtlichen Prüfung, ob der Verkäufer über öffentlich bekannte Sicherheitslücken informieren muss. Und zweitens, ob der Verkäufer auch über den Zeitraum, in dem Sicherheitspatches zur Verfügung gestellt werden, informieren muss.

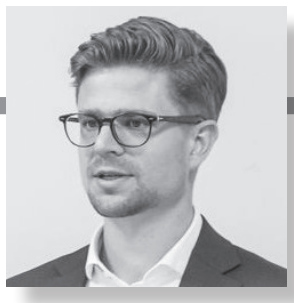
Und drittens wollen wir uns mit Denkfabriken vernetzen, mit Think-Tanks, um auch von außen Input zu bekommen für unsere Arbeit. Um auf diesen Dialog noch einmal konkreter einzugehen, dort haben wir eine Plattform entwickelt: die Denkwerkstatt. Um dort einen vertrauensvollen Dialog zu realisieren, möchten wir uns Zeit nehmen für den Austausch und in einem deliberativen Verfahren gemeinsam neue Lösungsansätze entwickeln. Über diesen breiten Austausch hinaus sind wir gerade dabei, diesen Dialog zu verstetigen, zu vertiefen. Mit einer kleineren Gruppe von Akteuren machen wir uns sehr partizipativ und offen Gedanken, wie wir das gestalten möchten. Nichtsdestotrotz gibt es dieses Modell der Denkwerkstatt weiterhin und läuft im Rahmen eines Projekts.

Desweiteren ist im Kontext der Gesellschaft das Thema des Verbraucherschutzes zu verorten. Dort gab es auch eine Stärkung des Themas durch den Koalitionsvertrag. In diesem wurde konkret dem BSI die Aufgabe des Verbraucherschutzes zugewiesen, und das möchten wir gerne annehmen. Das Ziel ist es, dort Verbraucher so zu unterstützen, dass es eine Sensibilität für diese Themen gibt, sie dann aber auch in ihrer Beurteilungsfähigkeit zu stärken, denn am Beispiel der Smartphones sieht man: der Verbraucher ist oft noch gar nicht in der Lage dazu, Sicherheitsaspekte beurteilen zu können, weil es keine Informationen dazu gibt. Und schließlich, wenn es Unsicherheiten gibt, dann auch Lösungskompetenz zu besitzen, das heißt einerseits, vielleicht zu wissen, wie befreie ich mich aus dieser Unsicherheit oder dann zu wissen, an wen kann ich mich wenden, wer hilft mir. Das ist einerseits natürlich als Beitrag zur individuellen Sicherheit zu sehen, aber auch zur öffentlichen Sicherheit, wenn wir beispielsweise an das *Mirai*-Botnetz denken, das dann auch eine Gefahr für unsere Infrastruktur darstellt.

Schluss

Zum Abschluss zusammengefasst: Cybersicherheit ist eine Bedingung für das Gelingen einer erfolgreichen Digitalisierung. Wir möchten das gemeinsam gestalten für die und mit den verschiedenen Akteuren und wollen für eine sichere digitale Gesellschaft gemeinsam eintreten, dort nicht als Verhinderer angesehen werden, sondern auch als Ermöglicher, denn mit einer sicheren Digitalisierung kann man überhaupt erst diese Digitalisierung bestreiten. Alleingänge sind keine gute Lösung. Es ist eine gemeinsame Verantwortung, und diese Verantwortung gilt es für unterschiedliche Akteure im Dialog und im Austausch wahrzunehmen.

Damit beende ich meine Präsentation und danke für die Aufmerksamkeit und freue mich jetzt auf Ihre Fragen.



Florian Schumacher

Florian Schumacher ist Referent im BSI und leitet dort die Projektaktivitäten im Bereich des gesellschaftlichen Dialogs von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft zu Fragen der Cyber-Sicherheit. Darüber hinaus koordiniert er die Maßnahmen des BSI im Themenfeld Verbraucherschutz und entwickelt diese strategisch weiter.