„Das Ziel ist immer: Wasser aus der Leitung, Strom aus der Steckdose.“

Interview

Auf dem Weg in eine Welt ohne Cyber-Angriffe?

Ein Interview mit Steve Ritter und Dr. Timo Hauschild vom Bundesamt für Sicherheit und Informationstechnik

Steve Ritter leitet das Referat IT-Sicherheit und Recht, das zentrale Rechtsreferat des Bundesamts für Sicherheit und Informationstechnik (BSI). Er absolvierte zunächst eine Bankausbildung, war während dieser Zeit dort Datenschutzbeauftragter und ist auf diesem Wege mit dem Thema Recht in Berührung gekommen. Anschließend studierte er Jura in Bonn. Da er sich schon während der Schulzeit für Technik interessierte, bewarb er sich nach Abschluss des Referendariats beim BSI.

Dr. Timo Hauschild ist Fachbereichsleiter im Bereich Cyber-Sicherheit für kritische Infrastrukturen und arbeitet seit mehr als 20 Jahren beim BSI. Er hat Journalistik und Physik studiert. Letzteres schloss er mit einer Promotion ab. Im BSI war er bereits in unterschiedlichen Arbeitsfeldern tätig. Sein Weg führte ihn jedoch wieder zurück zum Bereich kritischer Infrastrukturen und Umsetzung der IT-sicherheitsrechtlichen Regulierung.

CTRL: Was sind die Aufgaben des BSI und in welche Bereiche sind diese unterteilt?

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

CTRL: Wie unterscheidet sich denn der Kompetenz- und Aufgabenbereich des BSI im Vergleich zur Bundesnetzagentur und zum Cyber-Kommando der Bundeswehr?

Ritter: Es gibt natürlich immer Berührungspunkte, weil sich alles um IT-Sicherheit dreht. Die Bundesnetzagentur ist eine klassische sektorspezifische Aufsichtsbehörde für den Bereich der Telekommunikation. Wie man sich vorstellen kann – Digitalisierung ohne Telekommunikation – das funktioniert nicht. Das heißt auch dort muss dafür gesorgt werden, dass die entsprechenden Telekommunikationsprovider ihre IT sicher betreiben, damit die Kunden geschützt werden. Das Kommando Cyber-Sicherheit ist demgegenüber eigentlich das genaue Gegenteil, es ist keine Aufsichtsbehörde, es ist keine Regulierungsbehörde, sondern es ist tatsächlich ein rein operativer Arm der Bundeswehr. Es unterscheidet sich vom BSI und der Bundesnetzagentur schon dadurch, dass es gar kein eigenes Gesetz mit Befugnissen und Aufgaben hat. Alles, was das Cyber-Kommando tut, folgt letztlich aus dem Mandat, das die Bundeswehr für ihre Einsätze bekommt.

Das BSI steht irgendwo dazwischen. Wir sind eine allgemeine Cyber-Sicherheitsbehörde. Was uns sehr davon unterscheidet, dass wir früher Kompetenzträger waren; weniger klassische Behörde. Das ändert sich seit 2015 ganz massiv. Erst mit den kritischen Infrastrukturen, jetzt mit den Unternehmen im besonderen öffentlichen Interesse.

Dr. Timo Hauschild (rechts im Bild) und Steve Ritter (2. von rechts) vom BSI gemeinsam mit den Mitgliedern der CTRL-Redaktion Ferdinand Wegener (Mitte), Philipp Beckmann (2. von links) und Clarissa Kupfermann (links im Bild).

Profil: Das Bundesamt für Sicherheit in der Informationstechnik

Das BSI nahm am 01.01.1991 seine Arbeit auf und ging aus der an den Bundesnachrichtendienst (BND) angegliederten Zentralstelle für das Chiffrierwesen (ZfCh) hervor. Hauptaufgabe der ZfCh war die Entwicklung von sicheren Kommunikationstechnologien für die Bundesverwaltung und die NATO im Kalten Krieg. Seit den 1980er-Jahren setzte sich die Erkenntnis durch, dass IT-Sicherheit eine zunehmende gesamtgesellschaftliche Bedeutung hat. Mit der Gründung des BSI rückte daher neben der öffentlichen Verwaltung auch der Schutz von Unternehmen und Bürgern in den Vordergrund. Die Belegschaft des BSI ist in den letzten Jahren enorm gewachsen. Zudem sind mit dem zweiten IT-Sicherheitsgesetz (IT-Sicherheitsgesetz 2.0) neue Aufgabenschwerpunkte wie der Schutz kritischer Infrastruktur hinzugekommen. Aktuell sind ca. 1500 Mitarbeitende beim BSI beschäftigt, das Budget beläuft sich jährlich auf rund 197 Millionen Euro. Neben dem Hauptsitz in Bonn hat das BSI einen großen Forschungsstandort in Freital (Nähe Dresden) und einen kleineren Standort in Saarbrücken. Zudem gibt es eine Außenstelle in Brüssel.

Und gleichzeitig sind wir auch ganz stark operativ tätig, sowohl was die Generierung von Wissen und den Ausbau von Kompetenzen angeht, als auch was die tatsächliche Fallbewältigung betrifft. Man stelle sich vor, dass die gesamten Patientendaten eines Uniklinikums durch einen Cyber-Angriff verschlüsselt wurden. In dieser Situation rückt das BSI mit seinen Mobile Incident Response Teams, quasi als IT-Feuerwehr aus, um vor Ort den Vorfall zu bewältigen.

CTRL: Was läuft schon besonders gut im Bereich Cyber-Sicherheit in Deutschland und wo müssen wir noch aufholen?

Dr. Hauschild: In Deutschland läuft schon ziemlich vieles ziemlich gut, was Cyber-Sicherheit angeht. Die Behörden, wie aber auch die Unternehmen, sind sich der Bedrohungslage bewusst und tun eine ganze Menge, um sich zu schützen. Die rechtlichen Anforderungen gehen aber über diese freiwilligen Schutzmaßnahmen hinaus. Wir sind von dem früher gelebten Motto der rein freiwilligen Kooperation in ein Regime der kooperativen Regulierung übergegangen.

Diesen Ausdruck verwenden wir, denn das aktuelle System hat weiterhin etwas Kooperatives, ist aber definitiv mit regulatorischen Vorgaben in gewissen Bereichen unterlegt. Im Kontrast dazu verdeutlicht der diesjährige IT-Lagebericht, dass die Sicherheitslage keine gute ist. Es passiert ständig etwas, es gibt immer wieder erfolgreiche Angriffe, bei denen Behörden und Unternehmen Opfer von Ransomware-Angriffen werden. Das zeigt eben auch: Man darf nicht stehen bleiben. Das Ganze ist ein Prozess. Ich muss ständig wieder meine Maßnahmen überprüfen und erweitern. Um dieser Bedrohung zu begegnen, beinhaltet das neue IT-Sicherheitsgesetz für die Betreiber kritischer Infrastrukturen die Pflicht zum Einsatz von Angriffserkennungssystemen.

Denn wir wissen: Prävention allein reicht nicht. Es wird immer Angriffe geben und wir müssen diese frühzeitig detektieren und dann darauf reagieren können. Diese Reaktion muss vorbereitet sein, damit es dann im Fall der Fälle zu einer guten Lösung kommt. Es kommt darauf an, den Angriff zu stoppen und zwar ohne die Systeme für vier Wochen runterfahren zu müssen und die Daten frei zugänglich im Internet wiederzufinden.

CTRL: Sie haben den Begriff kritische Infrastruktur jetzt schon mehrfach verwendet. Was versteht das BSI unter kritischer Infrastruktur?

Dr. Hauschild: Lange Zeit war unklar, was damit gemeint war, aber 2015 sind kritische Infrastrukturen erstmalig im BSI-Gesetz (***BSIG***) definiert worden. Es handelt sich um Einrichtungen, Anlagen oder Teile davon in ausdrücklich bestimmten, besonders sensiblen Sektoren: beispielhaft Energie, Informationstechnik, Telekommunikation, Transport und Verkehr. Diese Einrichtungen oder Anlagen müssen zudem von hoher Bedeutung für das Funktionieren des Gemeinwesens sein.

Infrastruktur hat erstmal in der Definition keinen direkten Bezug zu IT, sondern kritische Infrastruktur ist die Wasserversorgung, die Gesundheitsversorgung, das Flugzeug, der Zug, die Straße.

„Bei Cyber-Angriffen rückt das BSI quasi als IT-Feuerwehr aus, um vor Ort den Vorfall zu bewältigen“

Erst im Anschluss überprüft das BSI, ob dort IT-Sicherheit eine Rolle spielt und sich daraus eine Zuständigkeit für uns ergibt oder auch eben nicht.

CTRL: Sie haben selbst schon gesagt, dass das BSI hier diese aufsichtsrechtliche Rolle hat, die eher verwaltungsrechtlich ausgeformt ist und eben nicht mehr nur noch auf Kooperationen beruht. Dazu gehört ja auch § 8b BSIG, der Betreiber kritischer Infrastruktur dazu verpflichtet, auch bestimmte Formen von Angriffen zu melden, wenn sie eine gewisse Seriösitätsstufe erreichen. Wir hatten uns daher gefragt: Was sind denn die Konsequenzen einer solchen Meldung?

Dr. Hauschild: Das hängt sehr vom Einzelfall ab, weil die Vorfälle extrem unterschiedlich sind. Es geht los bei einer ausgefallenen Festplatte, bei der man einfach feststellt, dass sie kaputt gegangen ist, wodurch es eine Störung gegeben hat oder hätte geben können. Das wird gemeldet, aber in dem Zeitpunkt, in dem das gemeldet wird, ist die Festplatte längst ausgetauscht und alles läuft wieder. Dann gibt es für uns schlichtweg keinen Handlungsbedarf. Wir nehmen das zur Kenntnis, wir zählen das in irgendeine Statistik und das war es. Aber es gibt auch die Fälle, in denen sich ein Betreiber meldet: „Wir haben hier ein riesiges Problem und wissen eigentlich auch nicht warum.“ Wir als BSI sehen nur, dass kritische Infrastruktur gerade in Teilen nicht funktioniert und wir wissen, dass da IT beteiligt ist, aber nichts Genaueres. Wir haben vielleicht eine Ahnung und dann geht man in engeren Austausch: Wir können Empfehlungspapiere zur Verfügung stellen. Wir können im Extremfall auch mit Notfallteams vor Ort fahren und unterstützen dann hier auf Anfrage der Betreiber der kritischen Infrastruktur. Es besteht eine große Bandbreite an Reaktionsmöglichkeiten.

CTRL: Können Sie ganz kurz auf dieses „auf Anfrage“ nochmal eingehen: Heißt das, dass das BSI nicht von sich aus sagen kann: „Entschuldigung, das ist so kritisch, wir müssen da jetzt mit einem Team reingehen“, unabhängig davon, was zum Beispiel der privatwirtschaftliche Betreiber der Infrastruktur sagt?

Dr. Hauschild: Exakt, also bei kritischer Infrastruktur ist es definitiv so, dass der Betreiber damit einverstanden sein muss. Wir können nicht hingehen und sagen: „Wir übernehmen hier“. Wir würden sowieso nicht die Kontrolle übernehmen, sondern nur beraten, unterstützen und analysieren. Es wäre auch ein Irrglaube, anzunehmen, dass wir die IT des Betreibers besser betreiben könnten als er selbst. Denn wir kennen sie nicht, wir können nur mit unserer Expertise helfen zu verstehen, was da gerade vor sich geht. Letztlich muss der Betreiber selbst wissen, was mit seiner IT los ist und wie er damit umgeht. Das muss in eigener Verantwortung geschehen.

CTRL: Das heißt, dass trotz der gesetzlich ausgestalten Meldepflicht ein sehr kooperatives Verhältnis besteht: Sie kooperieren sehr eng mit den relevanten Akteuren, ohne dass es für ihre Arbeit entscheidend auf diese gesetzlichen Pflichten ankommt?

„In Deutschland läuft schon ziemlich vieles ziemlich gut, was Cyber-Sicherheit angeht.“

Ritter: Genau, aber natürlich muss man ab einem gewissen Punkt einschreiten. Die meisten Betreiber wollen tatsächlich auch ihre IT absichern, das muss man an dieser Stelle klar betonen.

Aber es gibt natürlich immer Betreiber, welche die zusätzlichen Kosten und den Compliance-Aufwand

scheuen. Hier schreitet das BSI ein und setzt die gesetzlichen Regelungen durch.

Das Gesetz enthält dazu auch Bußgelder, die mit dem IT-Sicherheitsgesetz 2.0 signifikant erhöht wurden. Allerdings ist es in der Regel so, dass die Betreiber von sich aus die Expertise des BSI einholen. Sie wissen, wie sie ihre IT betreiben und wir als BSI wissen, wie man IT-Sicherheit macht. Dieser kooperative Ansatz hat sich in der Praxis bewährt, sodass es kein Problem ist, dass wir nur auf Anfrage aktiv werden. Die Betreiber profitieren von unserer Expertise und schätzen unsere hoheitlichen Befugnisse zur Durchführung spezifischer Untersuchungen bei der Reaktion auf Angriffe.

Dr. Hauschild: Ich würde vielleicht noch einen Punkt einwerfen: In der Diskussion zum ersten IT-Sicherheitsgesetz war von großem Aufwand für die Wirtschaft die Rede und es bestand große Angst vor der Meldepflicht. Das wurde hoch und runter diskutiert. Was demgegenüber kaum zur Sprache kam, war § 8a BSIG, der aus unserer Sicht viel mehr Aufwand erzeugt und viel mehr Wirkung entfaltet.

Dieser verpflichtet Betreiber kritischer Infrastruktur den Stand der Technik umzusetzen, verkürzt dargestellt. Das muss alle zwei Jahre durch eine externe Prüfung nachgewiesen werden. Da stellt sich natürlich die Frage, ob diese Pflicht bei den Betreibern auf Gegenliebe stößt. Dazu kann man sagen, dass diese Pflicht bei den dort für die IT-Sicherheit Verantwortlichen jedenfalls sehr begrüßt wurde, weil sie endlich im eigenen Unternehmen einen Hebel haben, um weitreichende Sicherheitsmaßnahmen implementieren zu können. Bei den Verantwortlichen, welche die Maßnahmen finanzieren müssen, ist diese Pflicht wohl weniger beliebt. Jedoch versuchen wir auch hier insofern kooperativ vorzugehen, als dass wir nicht konkret vorschreiben, wie sie IT-Sicherheit umzusetzen haben. In vielen Branchen gibt es Verbände, die einen Standard für IT-Sicherheit, den sogenannten branchenspezifischen Sicherheitsstandard, entwickelt haben. Dieser wird bei uns zur Eignungsprüfung eingereicht. Wenn unsere Anforderungen erfüllt sind, setzen wir einen Stempel drunter und geben unser OK. Das Ziel ist immer: Wasser aus der Leitung, Strom aus der Steckdose. Das ist unser Ziel, deswegen machen wir das Ganze.

CTRL: Sie prüfen den Standard, den die Industrie festlegt. Aber prüfen Sie, ob die Unternehmen diesen Standard auch tatsächlich einhalten?

Dr. Hauschild: Die Prüfung des Standards erfolgt in Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie mit gegebenenfalls zuständigen Aufsichtsbehörden auf Bundesebene. Die Prüfung vor Ort, ob die IT-Sicherheit an den kritischen Infrastrukturen ausreichend umgesetzt wurde, machen externe Dritte, die von den Unternehmen beauftragt werden. Diese Prüfer werden auch von den Unternehmen bezahlt und fertigen dann darüber einen Nachweis an, den sie bei uns einreichen. Wir prüfen nur noch, ob der Nachweis gewissen Grundanforderungen entspricht: Etwa ob der Prüfer die Grundeignung hat, dass das, was attestiert wurde, richtig ist und wir schauen uns die Liste der Mängel an, die mitgeliefert werden muss. Insbesondere prüfen wir, inwiefern diese Mängel akzeptabel sind und ob ein Umsetzungsplan vorliegt, der uns glauben lässt, dass die Mängel zeitnah behoben werden. Sollte ein schwerwiegender Mangel vorliegen, hätten wir auch die rechtlichen Mittel, anzuordnen, den Mangel zu beseitigen. Das wäre aber schon ein sehr hartes Schwert, dass wir ungern zücken. Auch hier wieder ganz viel Kooperation vorne weg, wo wir in den Austausch treten und hinterfragen: Warum sind diese Mängel da? Warum kommt es zu diesen und wie kommen wir aus der Situation schnell raus? Meistens, gerade bei den schwerwiegenden Mängeln, haben die Betreiber ein sehr großes Eigeninteresse, diese auch schnellstmöglich abzustellen.

CTRL: Einer der Hauptansätze, mit denen das BSI versucht, möglichst hohe Sicherheitsstandards zu etablieren, ist es, die Eigenmotivation der Unternehmen zu nutzen, da die IT-Sicherheit auch dem Schutz ihrer

„Es wäre auch ein Irrglaube anzunehmen, dass wir die IT des Betreibers besser betreiben könnten als er selbst.“

wirtschaftlichen Interessen dient. Bestehen auf dieser Ebene größere Probleme bei der Verwaltung und der öffentlichen Hand, da dort kein Gewinninteresse besteht, sondern die Motivation anders erzeugt werden muss?

> „Das Ziel ist immer: Wasser aus der Leitung, Strom aus der Steckdose.“

Dr. Hauschild: Das Problem besteht bereits bei kritischen Infrastrukturen. Die Verwaltung ist letztlich auch eine kritische Infrastruktur. Die Unternehmen schützen sich, soweit, wie es für ihren „eigenen Gewinn“ notwendig ist.

Für kritische Infrastrukturen brauchen wir jedoch mehr Schutz. Als Bürger reicht es mir nicht, dass mein Wasserversorger sich gut versichert hat und nicht in die Insolvenz rutscht, wenn er fünf Wochen kein Wasser liefern kann. Sondern für mich als Bürger ist es essentiell, dass das Wasser läuft und zwar in guter Qualität. Darum ist da die Notwendigkeit, sich abzusichern, größer, als rein betriebswirtschaftlich betrachtet und das gilt für Behörden natürlich genauso. Da gibt es keinen wirtschaftlichen Gewinn, da steht nur das Gemeinwohlinteresse dahinter.

Das ist genau der Punkt, der den Unterschied zwischen kritischen Infrastrukturen und einem ganz normalen Unternehmen ausmacht. Dieser Umstand hat uns letztlich auch dazu veranlasst, regulatorische Maßnahmen zu ergreifen und zu sagen „OK, in diesem Bereich brauchen wir Vorschriften, weil es hier keine intrinsische Motivation mehr gibt“.

CTRL: Aber diese Normen sind doch häufig eigene Standards, welche die Industrie sich selbst auferlegt…

Ritter: In den großen Normungsgremien ist die Industrie stark vertreten. Dort hat sie auch ein starkes Eigeninteresse, weil sie durch gemeinsame Standards viel weniger Probleme im internationalen Vertrieb hat. Das macht es viel einfacher, das Geschäft mit den entsprechenden Produkten zu skalieren, wenn man weiß, dass es sich um Normen handelt, die international anerkannt sind. Dasselbe gilt natürlich auch bei IT-Sicherheit, wenn es gelingt, die Standards international zu etablieren, dann wird es besser skalierbar. Dadurch wird IT-Sicherheit dann auch plötzlich viel bezahlbarer, weil man nicht für jeden einzelnen Staat beziehungsweise für jede einzelne Verkaufsregion etwas Eigenes entwickeln muss. Deswegen haben die Unternehmen natürlich ein unmittelbares Interesse. Jedoch ist es nicht so, dass die Unternehmen da minimale Standards durchsetzen können. Dadurch, dass staatliche Organisationen wie das BSI mit am Tisch sitzen, wird hart verhandelt, damit im Ergebnis mehr als nur das Minimum rauskommt.

CTRL: Wie geht das BSI mit künftigen technologischen Entwicklungen und deren Angreifbarkeit um, besonders bezogen auf KI, IoT und 5G?

Ritter: Das BSI ist in einem sehr dynamischen Umfeld tätig. Das betrifft einerseits das, was täglich anliegt, das betrifft aber andererseits auch die Technik, die sich stetig weiterentwickelt.

Vor 15 Jahren hat sich niemand etwa mit KI oder 5G im operativen Einsatz beschäftigt, aber nach und nach wurden diese Entwicklungen immer wichtiger. Deswegen beobachtet das BSI innovative Technologien, um zu erkennen, welche Aspekte der IT-Sicherheit künftig beachtet werden müssen. Beispielsweise im Bereich KI haben Kollegen einen Katalog mit Anforderungen an die Cloud-Infrastruktur von KI entwickelt, um einen Rahmen für Entwickler setzen zu können. Es handelt sich dabei um einen dynamischen und kontinuierlichen Prozess, der keinen Endpunkt hat, sondern auf die Entwicklungen reagiert.

Dr. Hauschild: Gerade solche besonders wichtigen Themen wie KI und 5G werden dann vom BSI gesondert organisatorisch aufgegriffen. Für Künstliche Intelligenz haben wir zum Beispiel unseren Standort in Saarbrücken aufgemacht. Dieser befindet sich in der Nähe von Forschungsstandorten, sodass das BSI dieses Thema an der Spitze der Entwicklung mitverfolgen kann. Für 5G gilt das Gleiche in Freital. Dort versuchen wir eine “***Thought Leadership***” über diese Themen zu erhalten.

„Als Bürger reicht es mir nicht, dass mein Wasserversorger sich gut versichert hat und nicht in die Insolvenz rutscht, wenn er fünf Wochen kein Wasser liefern kann.“

CTRL: Kürzlich wurde der Lagebericht zur IT Sicherheit 2021 vorgestellt. Sehr prominent war darin der Bereich Ransomware-Angriffe auf die Privatwirtschaft und die öffentliche Hand, vor denen gewarnt wurde. Da hat das BSI generell dazu geraten, die Lösegeldforderung von Angreifern nicht wahrzunehmen und nicht darauf einzugehen. Lässt sich das wirklich so pauschal sagen? Selbst wenn für Betroffene sehr sensible Daten auf dem Spiel stehen, die entweder dauerhaft verloren gehen können oder die dann an die Öffentlichkeit geraten?

Dr. Hauschild: Ja! *(lacht)*

Ritter: Es ist sogar relativ leicht begründbar, weil das BSI schon seit den ersten Vorfällen gesagt hat, dass das Wichtigste, was man haben sollte, Backups sind, die nicht am Netzwerk hängen. Wenn man diese hat, dann ist es zwar schade, wenn ein System neu aufgesetzt werden muss und die Daten wieder neu eingespielt werden müssen, aber sie können nicht verloren gehen. Die Grundproblematik besteht darin, dass die kriminelle Infrastruktur immer stärker wird, solange diese Lösegelder gezahlt werden. Sie können immer mehr Ressourcen aufwenden, um noch ausgefeiltere Angriffe zu entwickeln und noch mehr Leute anzugreifen. Das heißt, die Einzigen, die davon profitieren, sind die Angreifer. Auch wenn ich natürlich verstehen kann, dass es unglaublich weh tut, wenn man die Basismaßnahmen nicht ergriffen hat, muss man festhalten, dass im Sinne des Gesamtsystems auf keinen Fall Lösegelder gezahlt werden sollten.

Dr. Hauschild: Und die Nichtverfügbarkeit ist natürlich nur der eine Aspekt. Seit zwei bis drei Jahren ist die Drohung mit der Veröffentlichung der Daten dazugekommen. Das Bezahlen schützt nicht davor, dass die Daten nicht dennoch veröffentlicht werden können. Natürlich kann ein Angreifer sagen, ich tue es dann nicht, aber wer glaubt schon dem, der einen gerade erpresst hat.

CTRL: Inwieweit spielen Kryptowährungen eine signifikante Rolle bei diesen Ransomware-Angriffen? Wie geht das BSI bei der Nachverfolgung von diesen Krypto-Zahlungen im Gegensatz zu traditionellen Zahlungsmitteln um, insbesondere im Hinblick auf die Transaktionsdaten auf der Blockchain?

Ritter: Also man muss an der Stelle unterscheiden zwischen unseren Aufgaben und denen der Strafverfolgungsbehörden. Für Letztere ist es natürlich unglaublich wichtig, herauszufinden, wohin das Geld geflossen ist. Das machen die Strafverfolgungsbehörden auch und ich habe da nie so richtig verstanden, warum alle gedacht haben, mit Bitcoin wären sie total sicher. Auf der Blockchain werden alle Transaktionen dokumentiert. Das ist eigentlich fast das Beste für die Strafverfolgung. Das ist so ein bisschen, als ob jemand bei der Übergabe des Lösegeldkoffers noch eine Quittung mit seiner eigenen Adresse darauf ausstellt. Aber das ist keine Baustelle des BSI. Wir schauen, ob es vielleicht schon Tools gibt, um diese konkrete Ransomware-Angriffe unschädlich zu machen. Uns geht es darum, am Schluss wieder Sicherheit herzustellen. Völlig angreiferagnostisch, also egal ob dieser jetzt ein Staat, ein Cyber-Krimineller oder ein Sonstiger ist.

CTRL: Was ist die Motivation dieser Ransomware-Angriffe? Ist es wirklich nur Geld?

Ritter: Das ist tatsächlich der entscheidende Punkt. Weil es unglaublich gut funktioniert, um Geld zu erpressen. Es gibt da ein System, was es potenziellen Angreifern sehr einfach macht. Man kann sich schnell und unkompliziert die nötigen Werkzeuge besorgen, man kann sich sogar von dem Ausspähen von Zielen bis zur Abwicklung der Zahlung alles als Dienstleistungen buchen. Das ist alles *‚Cyber-Crime as a Service‘*. Da sich leider immer noch sehr viele nicht ausreichend absichern, ist dieses Modell weiterhin lukrativ. Das heißt, man hat gute Chancen, mit einem Schrotschuss auf alle Systeme in Deutschland eine signifikante Menge Treffer zu bekommen. Das ist vergleichbar mit Spam. Man schickt 1.000.000 Nachrichten raus und wenn nur 1.000 Empfänger da drauf klicken hat man zwar prozentual unglaublich wenig Treffer, aber eben immer noch 1.000 zahlende Kunden.

Dr. Hauschild: Der wichtigste Punkt ist, dass jeder sich auch selber davor schützen kann. Natürlich nicht

> „Das ist so ein bisschen, als ob jemand bei der Übergabe des Lösegeldkoffers noch eine Quittung mit seiner eigenen Adresse darauf ausstellt.“

vollumfassend, nicht gegen alles und nicht gegen den versiertesten Angreifer, aber Basisschutz ist immer möglich. Relevante Daten, also vertrauliche Daten, die man wirklich nirgends lesen möchte, sollte man verschlüsselt ablegen. Insbesondere, wenn man verschlüsselte Backups in die Cloud lädt, können die Daten zwar gestohlen, aber nicht so leicht entschlüsselt werden, wenn es ein ordentlicher Schlüssel und ein ordentlicher Algorithmus war. Und damit habe ich den Basisschutz, sodass es, selbst wenn es mich nachher erwischt, nicht umhaut, sondern ich weiterhin gut schlafen kann und mein Backup einspiele, ich weiter arbeiten kann und ich nicht Sorge haben muss, dass meine Gehaltsauszüge der letzten 10 Jahre auf einmal online stehen.

CTRL: Teilweise wurde in den Medien kritisiert, dass die Nähe des BSI zum Innenministerium zu Vertrauensdefiziten bei den Unternehmen führen würde. Spielt das in der Praxis eine Rolle für Sie?

Ritter: Nein, der Punkt, der da ja immer wieder diskutiert wird, ist, dass das BMI natürlich ein unglaublich breites Spektrum an Behörden unter sich hat, mit sehr unterschiedlichen Aufgaben. Bei dieser Diskussion wird immer wieder insinuiert, dass eine Vermischung stattfindet und dass das BSI jede Schwachstelle, die es kennt, mal an den Hersteller, mal an eine andere Behörde weitergibt, die sie dann für ihre Zwecke ausnutzen kann. Das findet nicht statt. Lücken meldet das BSI dem Hersteller. Sofern diese Lücken kritische Infrastruktur betreffen, meldet es diese

> „Das ist alles *Cyber-Crime as a Service*.“

auch den Betreibern dieser Systeme und klärt über bekannte Abwehrmaßnahmen auf.

Also unser einziges Ziel – und deswegen gibt es da auch keinen Zielkonflikt – ist es, diese Systeme sicher zu machen. Die Vorstellung, dass das BSI zunächst beim Bundesverfassungsschutz und beim BKA nachfragt, ob eine gefundene Schwachstelle von Nutzen sein könnte, bevor sie diese dem Hersteller meldet, ist albern.

Dr. Hausschild: Das würde insbesondere auch dem gesetzliche Auftrag des BSI widersprechen.

Es ist nicht nur ein Ziel, sondern gesetzlicher Auftrag und das ist in einer Behörde ja schon etwas wert.

CTRL: Cyber-Sicherheit betrifft alle Staaten. Seit kurzem gibt es jetzt das European Cybersecurity Competence Centre (ECCC). Kann man da schon von einer gesamteuropäischen Strategie auf EU-Ebene sprechen?

Ritter: So eine Strategie bildet sich jedenfalls langsam, jedoch sind die Länder der EU unterschiedlich weit fortgeschritten. Gerade bei der Umsetzung der NIS-Richtlinie (hier abrufbar) traten viele europäische Staaten an uns heran und fragten: „Mensch Deutschland, wie macht ihr das eigentlich?“. Wir haben da sehr unterschiedliche Geschwindigkeiten und das setzt sich quasi bei allen Kooperationen fort. Auf der operativen Ebene existiert der ***CERT***-Verbund innerhalb der EU schon sehr lange. Den gab es auch schon vor der NIS-Richtlinie. Ich würde aber noch nicht sagen, dass es eine Situation ist, in der alle an einem Strang ziehen, sondern es gibt sicherlich noch einen Weg zu gehen. Ob das auch überall sinnvoll ist, das muss man hinterfragen. Es kommt immer darauf an, in welchen Bereichen man wie zusammenarbeitet.

CTRL: Stichwort CERT: Können Sie darauf noch einmal kurz eingehen und erklären, was es damit auf sich hat und wie sich das entwickelt hat?

Ritter: Computer Emergency Response Teams, kurz *CERTs*, beschäftigen sich mit den konkreten Vorfällen und arbeiten an deren Bewältigung mit. In der vernetzten Welt ist es unumgänglich, dass die Akteure sich hierbei austauschen. Das war die grundsätzliche Idee des European Government ***CERT***. Die ***CERTs*** der jeweiligen Mitgliedstaaten arbeiten operativ zusammen, schieben sich zum Beispiel Samples hin und her. „Wir beobachten gerade einen Angriff, wir haben bisher über den Angreifer und über seine Technik Folgendes rausgefunden. Habt ihr dieselben Informationen?“ Auf diese Weise kommt man einfach viel schneller, wie man das bei den Kollegen von ***CERT*** sagt, „vor die Lage“. Das heißt, man rennt nicht jedem Angriff und jedem Vorfall hinterher, sondern kommt Vorfällen zuvor und kann durch den aktiven Austausch schneller auf Angriffe reagieren.

Wenn in einem Mitgliedstaat etwas passiert, aber in einem anderen noch nicht, dann gibt es schon ***Indicators of Compromise***.

Das sind Hinweise, mithilfe derer man entdecken kann, wie ein Angreifer arbeitet und ob er in einem System drin ist. Diesbezüglich besteht eine stark ausgeprägte Zusammenarbeit und das seit vielen Jahren.

CTRL: Im Zuge dieser europäischen Zusammenarbeit finden also regelmäßig Treffen zwischen den Beteiligten statt?

Ritter: Es gibt Treffen, aber das darf man sich nicht als feste Termine vorstellen, sondern es ist wirklich ein täglicher Austausch. Man beobachtet einen Vorfall, man hat seine etablierten Kanäle und informiert sich gegenseitig darüber, was für einen Erkenntnis-

„Also unser einziges Ziel – und deswegen gibt es da keinen Zielkonflikt – ist es, diese Systeme sicher zu machen.“

stand man gerade hat und hilft sich so wirklich Tag für Tag. Das ist gar nichts stark Formalisiertes, sondern das ist Hands-on-Zusammenarbeit.

CTRL: Ist der Austausch immer Vorfall bezogen und findet damit nicht statt, wenn es keinen Vorfall gibt oder ist es so, dass es ständig Vorfälle gibt und man deswegen täglich zusammenarbeitet?

Dr. Hauschild: Vielleicht muss man hier ein bisschen abgrenzen: Der Austausch im *CERT*-Verbund erfolgt täglich und dabei geht es nicht nur um Vorfälle, sondern auch um potenzielle Schwachstellen, deren Relevanz man einschätzen muss.

Darüber hinaus gibt es formalisierte Kreise, die eingerichtet wurden, um den Austausch zwischen den nationalen Cyber-Sicherheitsbehörden oder den zuständigen Ministerien zu ermöglichen.

Im Vordergrund dieser Treffen stehen präventive Aspekte, wie die Resilienz von Infrastruktur. Das sind aber zwei verschiedene Ebenen, die nebeneinander existieren.

CTRL: Viele Cyber-Angriffe kommen aus dem außereuropäischen Ausland. Gibt es da auch eine starke Zusammenarbeit oder ist die internationale Kooperation des BSI eher auf Europa konzentriert und begrenzt?

Ritter: Digitalisierung und Vernetzung sind ihrer Natur nach weltweit ein Thema. Dementsprechend tauscht sich das BSI auch weltweit aus. In Europa vielleicht ein bisschen enger, da gibt es einfach mehr Foren.

Außerhalb von Europa gibt es zum Beispiel im *CERT*-Bereich unglaublich viel. Dazu gehört das ***Forum of Incident Response and Security Teams*** oder das International ***Watch & Warning Network*** (***IWWN***). Des Weiteren gibt es einen regelmäßigen Austausch etwa mit Australien, dem Vereinigten Königreich, den USA, Israel und anderen Staaten. Das ist auch notwendig, denn Angriffe gibt es von überall, etwa von Staaten oder von Cyber-Kriminellen. Das rein innerhalb von Europa zu betrachten, ergibt gar keinen Sinn.

Ein konkretes Beispiel ist das ***IWWN***, da tauscht man sich nicht nur im operativen Geschäft aus, sondern es gibt auch regelmäßig Übungen.

Wie ein Kollege von *CERT* immer sagt: „Man muss es üben, weil wenn man es schon könnte, dann hieß es ja ‚Könnung'".

CTRL: Gibt das BSI Informationen weiter, wenn es merkt, dass der Angreifer wohl staatlicher Natur ist und an welche Stellen wird das dann weitergegeben?

Ritter: Also es gibt schlicht gesetzliche Regelungen dazu. Wenn es darum geht, dass eine fremde Macht in Deutschland versucht, irgendwelche Umstürze zu starten oder Spionage zu betreiben, dann sieht das Verfassungsschutzgesetz vor, dass jede Stelle in Deutschland, die darüber Kenntnis erlangt hat, dem Bundesamt für Verfassungsschutz dies mitteilen muss.

CTRL: Welche Bedrohungen fallen nicht in ihre Zuständigkeit und in welchen Bereichen besteht aus ihrer Perspektive noch die Notwendigkeit einer weitergehenden Regulierung?

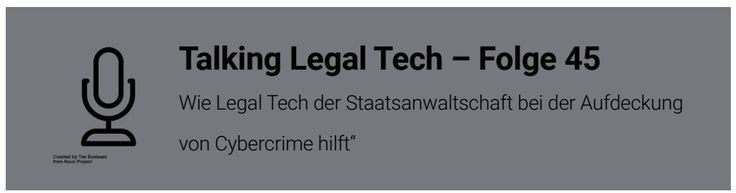
> „Das ist gar nichts stark Formalisiertes, sondern das ist Hands-on Zusammenarbeit."

Ritter: Um nochmal auf die Notwendigkeit weitergehender Regulierung zurückzukommen: Ich glaube, dass es tatsächlich darauf ankommt, was man darunter versteht. Unabhängig von weiteren gesetzlichen Regelungen, ist aus meiner Sicht viel wichtiger, dass wir dahin kommen, IT-Sicherheit als Standard zu etablieren. Das heißt, unsere Kollegen bringen sich unter anderem bei den *ISO*-Gruppensitzungen (***ISO = International Organization for Standardization***) ein.

Es bringt im Zweifelsfall viel mehr, wenn sich alle an einem einheitlichen Branchenstandard orientieren, anstatt dass jeder der 193 Staaten der Welt ein eigenes Gesetz verabschiedet. Diese Standards sind auch

für viele neue Geräte und Geräteklassen etwa im Hinblick auf die Vernetzung durch das ***Internet of Things*** anwendbar. Das hat eine starke Hebelwirkung und da ist das BSI schon gut aufgestellt, weil wir in den entsprechenden Gremien bereits sehr lange aktiv sind.

Zumal man auch sagen muss, dass wir keine Strafverfolgungsbehörde sind. Wir kümmern uns lediglich darum, dass der Vorfall aufhört. Wir sind zwar im Bereich der Gefahrenabwehr tätig und sorgen mit unserer präventiven Arbeit dafür, dass es möglichst selten dazu kommt, dass wir in der Gefahrenabwehr tätig werden müssen. Demgegenüber obliegt die Strafverfolgung in diesem Bereich etwa den Kollegen von der ZAC (***Zentral- und Ansprechstelle Cyber-Crime Nordrhein-Westfalen***) in Köln. Die kooperiert auch international mit anderen Polizeibehörden,



etwa bei dem Telekom-Vorfall, wo ein mutmaßlicher Täter sehr schnell in London festgenommen werden konnte.

Dr. Hauschild: Ich muss manchmal ein bisschen lachen, weil ich vor 20 Jahren, als ich hier eingestellt wurde, das Government-Handbuch mitgeschrieben habe und da stand genau das auch schon drin: Denkt IT-Sicherheit von Anfang an mit, überlegt euch wie die Prozesse sind, vereinfacht die Prozesse und denkt das von Anfang an mit, sonst wird es nicht gelingen.

Das gilt heute mehr denn je, da wir die Konsequenzen der Angriffe unmittelbar sehen können. Das war vor 20 Jahren noch anders, da konnten wir noch sagen, wenn wir die Mauer hoch genug ziehen, dann wird es schon gut gehen. Das gilt heute definitiv nicht mehr, aber wenn man die Prozesse gleich richtig und sicher gestaltet, dann hat man die Grundlagen gelegt, um auch die Digitalisierung erfolgreich hinzukriegen.

Das ist eben nicht nur eine Floskel, dass ist wirklich die Grundlage des Ganzen. Beim Datenschutz ist das auch ins Recht eingeflossen. ‚***Privacy by Design***‘ sollte auch dazugehören, da haben wir noch einen kleinen Schritt zu gehen.

CTRL: Wo sehen Sie beide in Anbetracht dieser zunehmenden globalen Vernetzung die Rolle des BSI zukünftig?

Dr. Hauschild: Im Bereich der Regulierung ist vieles tatsächlich eher national möglich, weil wir die Infrastruktur, die zu schützen ist, nur hier in Deutschland haben.

Die EU macht Vorgaben, sodass der Rechtsrahmen einheitlich ist, denn gerade im Bereich der Stromnetze ergibt es wenig Sinn, nur nach Deutschland zu schauen.

Darüber hinaus gibt es internationale Vereinbarungen, die vorsehen, sich über Cyber-Crime-Aktivitäten gegenseitig zu informieren, zu unterstützen.

Nun wissen wir alle, dass nicht jeder Staat das gleiche Verständnis von krimineller Aktivität hat. Insofern wäre es natürlich wünschenswert, dass man hier eine einheitliche Sprache findet, was über UN-Gremien bereits versucht wird.

Das sind allerdings Aktivitäten, die Jahre und Jahrzehnte andauern. Dennoch bestehen von Grund auf verschiedene Weltanschauungen, die so voneinander

„Das war vor 20 Jahren noch anders, da konnten wir noch sagen, wenn wir die Mauer hoch genug ziehen, dann wird es schon gut gehen. Das gilt heute definitiv nicht mehr.“

„Den Tag, an dem es keine Cyber-Angriffe mehr gibt, werden wir alle nicht erleben.“

abweichende Interessen widerspiegeln, dass es vielleicht nie ein gemeinsames Ergebnis geben kann.

Das heißt, wir müssen uns weiter durch Prävention schützen, indem wir uns bei der Detektion stark aufstellen, um überhaupt mitzubekommen, dass Angriffe stattfinden. Wir müssen wissen, wie wir reagieren für den Fall, dass mal was passiert.

Den Tag, an dem es keine Cyber-Angriffe mehr gibt, werden wir alle nicht erleben.

Wir danken unseren Interviewpartnern Herrn Dr. Hauschild und Herrn Ritter ganz herzlich für das Gespräch. Des Weiteren danken wir Herrn Gärtner, dem Pressesprecher des BSI für die Begleitung des Gesprächs sowie Herrn Caspers, der den Kontakt vermittelte und dem BSI für seine Gastfreundschaft.

Das Interview wurde von Philipp Beckmann, Clarissa Kupfermann und Ferdinand Wegener geführt.

Philipp studiert Jura an der Universität Freiburg und hat den Schwerpunkt Grundlagen des deutschen, europäischen und internationalen öffentlichen Rechts absolviert. Er interessiert sich besonders für öffentliches Recht, Rechtstheorie und Rechtsvergleichung sowie Völkerrecht.

Clarissa studiert Jura an der Universität zu Köln und ist als studentische Hilfskraft am Institut für Straf- und Strafprozessrecht tätig.

Ferdinand ist Jurastudent an der Universität zu Köln und Head of CTRL im LTLC. Neben dem Studium beschäftigt er sich insbesondere mit Technologien wie Blockchain, KI und IoT sowie ihren rechtlichen und regulatorischen Implikationen.

Referendariat beim BSI

Wer nach dem Lesen dieses Interviews Interesse daran gewonnen hat, Einblicke in den praktischen Arbeitsalltag zu erlangen, kann sich auf eine Referendariatsstelle beim BSI bewerben. Dabei ist zu beachten, dass eine vorherige Sicherheitsüberprüfung erforderlich ist und nur begrenzte Plätze vorhanden sind, sodass sich eine frühzeitige Bewerbung empfiehlt.

Die Bewerbung kann an **Bewerbung@bsi.bund.de** gerichtet werden.

Zurück zum dynamischen Inhaltsverzeichnis?

Zum dynamischen Inhaltsverzeichnis

1/22

2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

CTRL

Cologne Technology & Law Review

Hier geht es zur ganzen Ausgabe

Dort findest Du in 19 Beiträgen alles von Datenschutz bei Connected Cars über Krypto-Auktionen bis hin zum Artificial Intelligence Act und Legal Tech.

LEGAL TECH LAB COLOGNE