„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 15, 30.11.2021:
Weihnachtsshopping – Ransomware gleich mitbestellt?

Moderation: Ute Lange, Michael Münz
Gäste: Katharina Sook Hee Koch, BSI, und Robert Formanek, BSI
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Lange: Hallo und herzlich Willkommen zu „Update Verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz*:* Ich bin Michael Münz. Für diese Folge hatten wir uns vorgenommen, mit zwei Hackern zu sprechen. Aber seit der vergangenen Folge zum Thema Ransomware sind uns so viele Fälle von digitaler Erpressung untergekommen, da wollten wir das Thema noch einmal aufgreifen. Was macht man, wenn jemand die Daten verschlüsselt und nur gegen ein Lösegeld freigibt? Diese Frage haben sich zuletzt auch MediaMarkt und Saturn stellen müssen, denen genau das passiert ist.

Lange: Ja, und gerade mit Blick auf die anstehende Hochphase des Onlineshoppings, so kurz vor Weihnachten, wollten wir noch einmal bei unseren Expertinnen und Experten des BSI nachhorchen, wie die digitale Gefahrenlage für unseren digitalen Alltag gerade ist und was wir Nutzerinnen und Nutzer sowie Verbraucherinnen und Verbraucher tun können, um nicht Opfer von Ransomware zu werden und um Hacker von unseren Systemen und Netzwerken fernzuhalten.

Münz: Weil das Thema Ransomware so viele unterschiedliche Facetten hat, gibt es in dieser Folge eine Premiere: Wir haben heute nämlich gleich zwei Experten dabei: Katharina Sook Hee Koch und Robert Formanek.

Münz: Hallo ihr beiden und schön, dass ihr da seid.

Formanek: Hallo, schönen guten Tag.

Münz: Bevor wir tiefer in das Thema einsteigen, stellt euch doch mal kurz vor: Was macht ihr im BSI und wie war jeweils euer Werdegang?

Sook Hee Koch*:* Ja, Dankeschön für die Einführung! Ich habe tatsächlich vor knapp 20 Jahren bei der Polizei angefangen, weil ich gerne Menschen helfen wollte und weil ich etwas Sinnvolles tun wollte. Wie jeder habe ich im Streifendienst angefangen. Ich habe dann

meinen Weg gemacht über die Einsatzunterstützung und auch im Führungsstab. Später war ich auch selbst Ausbilderin für den Kommissars-Lehrgang. Irgendwann habe ich mich auch weitergebildet im Bereich internationale Strafjustiz und bin damit zum LKA gewechselt in den Bereich Interpol und Europol-Angelegenheiten. Weil mich IT und Cyber und Big Data Analysis schon immer interessiert haben, bin ich irgendwann in den Bereich Cybercrime des LKA gewechselt. Bevor ich letztendlich den Wechsel zum BSI vollzogen habe, war ich zuletzt im Untersuchungsausschuss Kindesmissbrauch Lüchte. Im BSI bin ich mittlerweile Referentin im Cyber-Abwehrzentrum, weil ich das Verständnis habe für die Sicherheitsbehörden, insbesondere Justiz und Polizei, aber jetzt auch das BSI kennenlerne. Ich bin der Mediator zwischen vielen unterschiedlichen Sicherheitsbehörden und da hilft mir mein Verständnis.

Münz: Und bei uns im Podcast! Wir freuen uns sehr, dass du da bist. Robert, wie war denn dein Weg zu uns in den Podcast?

Formanek: Mein Name ist Robert Formanek. Ich bin jetzt seit anderthalb Jahren im BSI und dort im Bereich operative Cyber-Sicherheit im OC 2 unterwegs, um genau zu sein, im Team der Vorfallsbearbeitung. Bevor ich ins BSI gewechselt bin, war ich relativ lange bei CERT in Baden-Württemberg. Ich habe dort eine sehr ähnliche Tätigkeit gemacht, wobei die nicht so sehr international war und eben sehr fokussiert auf die Landesverwaltung. Davor war ich lange als IT-Sicherheitsbeauftragter an einer Universität in der Nähe von Stuttgart. Ich habe also die IT-Sicherheit aus verschiedenen Facetten und Blickwinkeln betrachten können. Ich bringe diese Erkenntnisse sozusagen einerseits aus der operativen Seite bei den Anwenderinnen und Anwendern sozusagen ins BSI, gleichzeitig bringe ich noch die Ansicht der Landesverwaltung mit, die sich nicht wesentlich, aber doch im Kern unterscheidet von dem, wie die Bundesverwaltung aufgestellt und organisiert ist. Ich versuche also meinen Lebenslauf, den ich bisher hinter mich gebracht habe, sozusagen in die Vorfallsbearbeitung einfließen zu lassen.

Lange: Was für Werdegänge es so im BSI gibt! Wir haben schon mehrere Kollegen und Kolleginnen hier bei uns im Podcast gehabt. Ich persönlich bin immer wieder fasziniert, wie breit ihr ausgebildet seid und aus was für Richtungen ihr kommt. Wir haben eine obligatorische Entweder-oder-Frage zum Einstieg, bevor wir in das eigentliche Thema tiefer gucken. Ihr kennt die Frage, wie alle unsere Gäste, nicht. Wir haben uns heute für euch folgende Frage ausgedacht: Würdest du lieber Gedankenlesen oder Zeitreisen können? Katharina?

Sook Hee Koch: Ich würde lieber Gedankenlesen können. Es gibt so viele vielfältige Menschen auf der Welt. Es macht einfach Spaß, ins Gespräch mit solchen Menschen zu kommen. Man hat aber einfach nicht die Zeit im Leben, alle interessanten Menschen auf der Welt kennenzulernen. Da hilft es dann, Gedankenlesen zu können, und es hätte diesen Zeitvorteil, dass ich mich dafür entscheiden würde.

Lange: Robert, wie ist es bei dir – Gedankenlesen oder Zeitreisen?

Formanek: Lieber Zeitreisen! Um genau zu sein, lieber sogar in die Zukunft hineinreisen! Weniger in die Vergangenheit, um dann irgendwelche Dinge zu ändern, sondern tatsächlich in die Zukunft, weil wir in diesem Vorfallsbearbeitungsumfeld ohnehin sehr prognostisch unterwegs sind! Auch die Lageberichte sind ja immer ein Blick auf das vergangene Jahr, aber mit der Aussicht auf die Zukunft. Manchmal würde ich mir wünschen, ich könnte in die Zukunft reisen, um zu sehen, ob unsere Prognosen, die wir manchmal so erstellen, dann auch eintreffen. Insofern würde ich lieber in die Zukunft reisen.

Münz: Vielen Dank. Wir bleiben aber mal in der Gegenwart. Ich denke, du hast gerade richtig viel zu tun. Vielleicht kommt da auch der Wunsch her, in die Zukunft reisen zu können. Wir haben ja eingangs gesagt, dass wir das Gefühl haben, dass es gerade richtig viele Ransomware-Fälle gibt, die passieren und die auch in den Medien sind. Wir gehen einfach davon aus, dass dich das gerade sehr beschäftigt. Wir würden dich einmal bitten: Könntest du kurz zusammenfassen, was so ein Ransomware-Angriff eigentlich ist und an welchen Fällen du denn gerade arbeitest?

Formanek: Ransomware als solches bezeichnen wir in der Regel als Vorfälle, in denen Tätergruppen oder auch einzelne Täter in ein Unternehmen kommen – auf welche Art und Weise auch immer. Diese breiten sich dann dort aus, um die späteren Lösegeldforderungen, denn nichts anderes ist ja Ransomware, zu untermauern, um dann im Anschluss diese Systeme zu verschlüsseln, sodass das Unternehmen oder die Bertoffenen nicht mehr arbeiten können, weil die Systeme verschlüsselt sind. Die Lösegeldforderung wird durch das das vorherige Ausleiten von Daten untermauert, bei denen gedroht wird, dass sie veröffentlicht werden. Das wird so gemacht, dass das Unternehmen sehr lange und sehr intensiv mit dem Vorfall beschäftigt ist und in Erwägung zieht, die Lösegeldforderung schlicht und ergreifend zu bedienen, weil der Aufwand auf der anderen Seite sehr viel höher wäre. Momentan sind wir tatsächlich intensiv beschäftigt. Man hat den Eindruck, dass die Tätergruppierungen sich jetzt nicht mehr auf bestimmte Zeiten innerhalb des Kalenderjahres berufen, sondern, dass sie die Einfachheit der Lösegeldforderungen, die man damit erreichen kann, ausnutzen. Momentan arbeiten wir im Cybercrime-Umfeld an relativ großen Fällen. Da sind im Grunde drei besonders zu benennen. Das ist einmal der Vorfall bei der Media-Saturn-Holding -GmbH. Der MediaMarkt Fall war ein großer Vorfall. Der war nicht nur so groß, weil er medial begleitet worden war, sondern weil mehr als 3.000 Server verschlüsselt worden sind. Das ganze Unternehmen war deshalb zunächst von Sonntag auf Montag quasi nicht mehr arbeitsfähig. Dann arbeiten wir noch an dem Fall FTI. Das ist Frosch Touristik, ein Unternehmen, das Reisedienstleistungen anbietet. Da sind wir auch sehr intensiv damit beschäftigt, dem Unternehmen unsere Unterstützung zukommen zu lassen. Außerdem sind wir sehr mit dem Fall Eberspächer beschäftigt gewesen – ein Automobilzulieferer, der in Baden-Württemberg auch mit Ransomware zu tun hatte. Auch hier waren nahezu alle Server verschlüsselt und es konnte sozusagen nicht mehr gearbeitet werden.

Lange: Das klingt nicht nur nach viel Arbeit, sondern das klingt auch, zumindest im MediaMarkt Fall und bei dem Autohersteller so, dass es auch uns Verbraucherinnen und Verbraucher betreffen könnte. Wir haben beim letzten Mal schon darüber gesprochen, dass

wir bei den Ransomware-Attacken oft nicht direkt betroffen sind, weil nicht unsere Rechner verschlüsselt werden und nicht wir erpresst werden, sondern eben Kommunen oder, wie du jetzt gesagt hast, auch Firmen. Was sind die Folgen? Was war denn zum Beispiel bei MediaMarkt die Folge für Käufer und Käuferinnen?

Formanek: Primär war die Folge für die Käuferinnen und Käufer, die wirklich sichtbar war, dass man zunächst keinen Kassenbon mehr bekommen hat. Das mag jetzt dem einen oder anderen aus ökonomischen oder ökologischen Gründen gar nicht so schlimm erscheinen. Problematisch war aber, dass man dadurch keine Umsatzsteuer ermitteln konnte. Das heißt, die Unternehmen konnten zunächst nicht ihre steuerlichen Verpflichtungen erfüllen. Später geht das natürlich trotzdem, weil diese Kassen die Informationen aufbewahren, aber das sind bis dahin hoch automatisierte Prozesse, die automatisch funktionieren. Auch die Steuergeldzahlung wird sehr schnell erledigt – mit der Problematik, dass man das jetzt nicht noch einmal machen kann und die Verbraucherinnen und Verbraucher keinen Kassenbon bekommen. Eine weitere Problematik bei MediaMarkt war, dass man zum Beispiel keinen Umtausch mehr machen konnte und auch keine Reparaturen. Das heißt, wenn man also zum Beispiel eine kaputte Kaffeemaschine hatte, die man bei MediaMarkt gekauft hatte, und die zurückbringen wollte, war MediaMarkt nicht in der Lage diese zu reparieren. Die Auswirkungen kann sich jetzt jeder vorstellen, der gern Kaffee trinkt.

Münz: Da ich gern Kaffee trinke, mag ich gar nicht mehr weiter darüber nachdenken. Aber natürlich ist das gar nicht so lustig, wie ich es jetzt gerade versuche darzustellen. Was ich mich an der Stelle frage: Wenn so ein Anruf oder so ein Signal bei euch ankommt, dass so etwas passiert ist – wie geht ihr dann vor? Bleibt ihr bei euch in den Büros an euren Arbeitsplätzen oder habt ihr ein BSI-Mobil, mit dem ihr dann vorfahrt?

Formanek: Bei den allermeisten Sachverhalten bleiben wir tatsächlich zunächst mal im Büro und versuchen zu klären, welche Tätergruppierung im Haus ist und was wir vom BSI jetzt leisten können. Wir können zum Beispiel unser Wissen teilen, das wir über die Tätergruppierung haben. Das ist immer essenziell für den späteren Wiederaufbau, wenn ein Unternehmen verschlüsselt ist oder auch eine Privatperson. Das muss ja wieder aufgebaut werden. Das heißt, Systeme müssen irgendwann wieder hergestellt werden – aber immer mit dem Nimbus, dass man möglicherweise damit rechnen muss, dass der Täter oder die Täterin noch weiterhin da ist. Das heißt, die Systeme müssen angemessen wieder aufgesetzt werden. Dazu ist es wichtig zu wissen, wie die Tätergruppierung hineingekommen ist. Das ist eine Kernfrage, die wir uns in der operativen Cyber-Sicherheit stellen. Wenn sich dann der Sachverhalt so darstellt, dass es besser ist, wenn wir vor Ort sind, dann gehen wir hin. Das ist zum Beispiel der Fall, wenn wir nicht sicherstellen können, dass wir die Systeme forensisch analysieren und die dann möglicherweise auch den Ermittlungsbehörden zur Verfügung stellen können im Rahmen eines Zivil- oder Strafprozesses. Dann sind wir tatsächlich mit unserem Automobil vor Ort. Diese Automobile sind Busse, in denen wir ganz viele Materialien mit zum Einsatz nehmen können. Vor Ort können wir Datensicherung machen, aber auch Analysen der Systeme, die dann forensisch untersucht werden: Welche Schadsoftware war installiert? Wie ist der Täter im Netzwerk vorgegangen? Da werden alle

Informationen, die vor Ort sind, auch vor Ort gesichtet und im Hinblick darauf ausgewertet, dass man das System dann wieder aufbauen kann.

Lange: Während du mit deinem Bulli unterwegs bist Robert, was machst du denn Katharina? Was sind Dinge, die dann in deinem Arbeitsgebiet anstehen?

Sook Hee Koch*:* Vorab will ich über drei Punkte sprechen: Ransomware hört sich immer sehr kompliziert an. Da kommt als Erstes immer die Frage auf: Wieso lässt du deine Balkontür auf? Oder wieso schließt du deine Wohnungseingangstür nicht richtig ab und lässt dein Portemonnaie offen auf deinem Flurzimmerschrank liegen, wo es jeder sehen kann? Wieso gibst du deine PIN von der EC-Kartenzahlung ein und schützt dich nicht bei der Eingabe? Oder wieso lässt du deine Kontonummer oder Kontodaten irgendwo herumliegen? Man sollte dem Täter nicht die geringfügigsten Hindernisse geben, die er überwinden muss. An dieser Stelle müssen wir die Bürgerinnen und Bürger sensibilisieren. Das sind einfache Verhaltensweisen, mit denen man schnell noch den einen oder anderen Angriff abwehren könnte. Zweitens: Das Thema Ransomware scheint immer sehr weit weg zu sein, weil es häufig Unternehmen betrifft. Eben hast du erzählt, dass es im Einzelnen auch Bürgerinnen und Bürger betrifft – so wie wir es auch bei MediaMarkt Saturn gemerkt haben. Das betrifft letztendlich auch die Konsumentinnen und Konsumenten. Wir haben auch in Amerika einen Fall gesehen, der im Bereich Fleischproduktion stattgefunden hat. Was ist irgendwann, wenn wir kein Fleisch oder kein Toilettenpapier mehr einkaufen können – gerade in der Pandemie? Das, was jetzt so weit weg erscheint, ist dann doch eigentlich sehr nah für uns. Das dritte Thema ist Cyber-Sicherheit. Das hört sich immer pompös an. Cyber-Sicherheit kann man nur zusammen gewährleisten. Sprich, man muss das gesamtstaatlich angehen. Wenn jeder in seiner eigenen Suppe herumrührt, dann kommt man im Gesamten nicht weiter. Ich sage immer: Wir müssen den Blick über den Tellerrand hinaus stärken, zusammenführen und komplementär an einem Ziel arbeiten. Dann können wir wirklich das Grundproblem angehen. Hier kommen wir jetzt zu meiner Aufgabe. Ich sitze im nationalen Cyber-Abwehrzentrum. Das ist eine Kommunikations- und Kooperationsplattform mit den wichtigsten Behörden im Bereich der Cyber-Sicherheit. Wir haben hier den Bundesnachrichtendienst für Cyber-Bedrohungen aus dem Ausland. Der ist natürlich für Firmen und Unternehmen wichtig, die gerade im Ausland sind. Wir haben das Bundesamt für Verfassungsschutz. Das ist natürlich für Unternehmen hier in Deutschland sehr wichtig, weil die einen starken Wirtschaftsschutz haben und wir dahingehend beraten. Dann haben wir aber auch noch die Polizei, die im Bereich der Strafverfolgung auch irgendwann mal einen Täter dingfest machen muss. Es ist gut, dass wir dem Opfer helfen und auch hier die IT-Systeme wieder aufbauen. Wenn wir aber den Täter nicht irgendwann mal dingfest machen, dann kann er weiter agieren. Natürlich ist das im Bereich der internationalen Strafverfolgung sehr schwierig, aber irgendwann muss man auch mal anfangen. Man kann nicht immer sofort aufgeben. Und hier haben wir das Bundeskriminalamt und die Bundespolizei. Zudem haben wir weitere Behörden mit der Bundeswehr, sprich das Kommando Cyber- und Informationsraum, sowie das Bundesamt für Bevölkerungs- und Katastrophenschutz. Als letztes, innerhalb der Bundeswehr, gibt es den militärischen Abschirmdienst. Und was soll ich machen? Ich habe natürlich den Vorteil, dass ich den Blick aus der Perspektive der

Strafverfolgungsbehörden habe, weil wir auch viel mit der Justiz zusammengearbeitet haben, damals. Ich kenne die Polizei sehr gut, aber ich habe jetzt auch die Sicht des BSI. So erkenne ich die Stärken jeder einzelnen Behörde, aber auch die Zuständigkeiten jeder einzelne Behörde, und kann dann sagen: Wir haben hier Schnittmengen, lasst uns doch mal an einen Tisch kommen. Ein Beispiel ist der Fall der Uniklinik Düsseldorf. Da hatten wir damals einen Server-Angriff, an dem vielen Sicherheitsakteure beteiligt waren, zusammen mit dem Opfer und dem Dienstleister. Es heißt dann, miteinander zu arbeiten statt gegeneinander. Hier konnten wir viele Prozesse verschlanken, aber auch Zeit ersparen, indem wir gesagt haben: Jetzt schalten wir uns alle zusammen und gehen auch gemeinsam ans Ziel. So konnten wir dem Betroffenen Unterstützung anbieten.

Münz: Jetzt hast du mir eine ganze Reihe an Behörden aufgezählt, die an solchen Fällen mitwirken und da auch Auge mit darauf werfen. Das passiert aber nicht, wenn es nur darum geht, dass Leute ihre Kaffeemaschinen nicht zur Reparatur zurückgeben können. Was macht das Ganze so ernst in diesen Ransomware-Fällen? Was ist das?

Sook Hee Koch: Das ist die Grundversorgung für die deutsche Gesellschaft. Wenn wir an einer kleinen Stellschraube etwas verstellen, dann kann es sein, dass beispielsweise der Strom ausfällt, oder dass es an einer Lieferkette hapert. Es kann sein, dass wir zum Beispiel dann irgendwann keine Autos mehr bestellen können, oder dass es im Bereich der Milchversorgung Probleme gibt. Da muss Deutschland als demokratischer Staat seine Gesellschaft schützen. Wir haben hier wichtige Unternehmen genannt, die in diesem kritischen Sektor, die werden auch kritische Infrastrukturen genannt, diesen Schutz leisten müssen. Das gilt auch zum Beispiel für ein Unternehmen wie die Deutsche Bahn im öffentlichen Nahverkehr. Stell dir jetzt einfach mal vor, die ganzen Anzeigen funktionieren nicht! Was wir damit für ein Chaos auslösen! Das sind Kleinigkeiten, die doch eine sehr große Wirkung haben. Wir wissen alle, dass Deutschland wirtschaftlich sehr stark ist, viele Kompetenzen hat, und natürlich auch seine Stärken hat. Wer Stärken hat, da kann der eine oder andere auch neidisch werden. Der möchte dann auch gerne was abgraben. Das gilt es zu verhindern – sprich, es präventiv anzugehen und diejenigen außerdem für die einzelnen Gefahren zu sensibilisieren. Dafür haben wir verschiedene Behörden – diejenigen, die für das Ausland zuständig sind, und diejenigen, die innerhalb Deutschlands zuständig sind. Wir haben ja das Trennungsgebot: Nachrichtendienst und Polizei und Grundgesetz. Wenn es irgendwo eine gemeinsame Schnittmenge gibt, kommuniziert man auf der gesetzlichen Grundlage und mit einem gemeinsamen Ziel: Cyber-Sicherheit für Deutschland.

Lange: Ich würde gerne an der Stelle auch noch einmal zu Robert zurückkommen, weil ich vorhin bei dem Bulli so ein Bild im Kopf gehabt habe, dass ihr relativ krimimäßig in das Auto springt, vielleicht sogar mit Blaulicht, und dann da vorfahrt. Ich werde jetzt wahrscheinlich enttäuscht, weil du mir erklärst: „Das ist ganz anders und geht viel ruhiger ab“. Bitte erzähl uns doch mal, wie das so ist, wenn ihr tatsächlich herausfahrt! Können wir das vielleicht auch beobachten? Merken wir, wenn ihr irgendwo seid oder seid ihr immer sehr clandestine unterwegs?

Formanek: „Clandestine“ ist vielleicht der falsche Begriff. Gleichwohl ist es schon so, dass wir in der Regel versuchen keine große Aufmerksamkeit zu erreichen. Das ist oft auch im Sinne des Unternehmens. MediaMarkt hat beispielsweisedurch die mediale Begleitung ohnehin schon sehr viel Aufmerksamkeit bekommen. Wer jetzt aber aus dem BSI vor Ort ist, welche Vorfallsbearbeiter oder welche Polizeibeamten vor Ort sind, darüber spricht man nicht. Das ist in der Regel auch nicht im Sinne des Betroffenen. In der Regel will man seine Arbeit erledigen und die soll ja vor allem dann ruhig sein. Eines der wesentlichen Elemente, die das Involvieren des BSI in solche Sachverhalte mit sich bringt, ist die Ruhe, die das BSI da verbreiten kann. Wenn man von so einer Schadsoftware betroffen ist, dann ist das in der Regel erstmal eine absolute Katastrophe für die jeweils Betroffenen. Wir können den Vorteil anbieten, dass wir, nachdem wir wissen, welche Tätergruppierung vor Ort oder eingedrungen ist, sehr analytisch vorgehen und versuchen bestmöglich zu unterstützen – im schwersten Fall sogar mit einem eigenen Krisenmanagement. Wir waren mal bei einer Landesverwaltung, genauer gesagt bei einer Kommunalverwaltung mit vor Ort, bei der wir auch das Krisenmanagement mit unterstützt haben. Auch das ist Aufgabe des BSI. Wir sind nicht immer direkt vor Ort und fahren dort mit Blaulicht und Martinshorn vor, sondern wir analysieren die Situation; zum Beispiel in Bonn, aus dem BSI heraus, und mit der notwendigen Ruhe. Wir sind, ich sag mal, in dem Nachteil, dass wir mit solchen Vorfällen drei bis fünf Mal in der Woche in einem größeren Maßstab zu tun haben. Die einzelnen Betroffenen sollten das hoffentlich nur einmal in ihrem Leben erleben, vielleicht auch ein zweites Mal, aber das reicht dann für die Betroffenen auch. Wir gehen abends ins Bett und die Betroffenen müssen ihr System wieder aufbauen. Das ist ja noch nicht damit getan, dass man von neun bis fünf Uhr arbeitet und dann geht man nach Hause. Insofern mag das ein bisschen enttäuschend sein, aber wir haben tatsächlich kein Blaulicht.

Münz: Du sprachst vorhin von der Katastrophe für die Betroffenen. Die kommt ja aber nicht allein. Diese Lösegelderpressungen sind häufig zum Beispiel durch die Veröffentlichung von bereits gestohlenen Daten begleitet. Außerdem gibt es noch diese DDoS-Attacken, die du uns vielleicht doch noch einmal erklären müsstest: Was verbirgt sich denn dahinter? Diese Attacken tauchen ja auch oft in diesem Kontext auf.

Formanek: Wenn die Daten veröffentlicht sind, dann ist es immer klug zu wissen, dass diese Daten veröffentlicht sind. Wenn personenbezogene Daten veröffentlicht werden, dann muss der Dateneigentümer, beispielsweise MediaMarkt oder eines der anderen Unternehmen, die ich genannt hatte, die betroffenen Personen und mindestens die Aufsichtsbehörden informieren. Dann entscheiden die Datenschutzaufsichtsbehörden gemeinsam mit den Betroffenen, welche Art von Bedrohungsszenario da entsteht. Hier haben wir auch wieder diesen Blick in die Zukunft: Je nachdem welche Daten das Unternehmen verlassen haben, kann man einschätzen, wie gefährdet die Personen sind, die hinter diesen Daten stehen. Im schlechtesten Fall wird beispielsweise ein Personalausweis, ein Reisepass, eine Kreditkarteninformation und vieles mehr veröffentlicht und dementsprechend muss man natürlich die Betroffenen informieren. Wenn diese Daten veröffentlicht werden, ist Zeit ein wichtiger Faktor. Das heißt, wenn man als Bürgerin oder als Bürger von so einem Vorfall liest, sollte man sich selbst überprüfen und sich die Frage stellen: „Habe ich mit diesem

Unternehmen in letzter Zeit zu tun gehabt?“. Wenn ja: In welcher Form? Um im weiteren Schritt auch nachsehen zu können, ob man auch betroffen ist. Wenn ich beispielsweise einen Reisepass habe kopieren lassen, dann ist es klug, wenn man überprüft, ob die die Daten veröffentlicht worden sind.

Münz: Das heißt, als ich in der Zeitung zum Fall MediaMarkt gelesen habe, hätte ich mir auch denken können: „Ich ändere vielleicht noch einmal mein Passwort, weil ich schon online paar Mal Sachen eingekauft habe?“.

Formanek: Das Online-System von MediaMarkt war tatsächlich nicht betroffen, das sind andere Systeme. Insofern war die öffentliche Berichterstattung schon sehr zutreffend. Aber das sind natürlich genau die Dinge, auf die man als Bürgerin und als Bürger durchaus auch achten sollte. Ich würde trotzdem mein Passwort ändern, weil ich da auch ein Stück weit paranoid bin, aber deswegen bin ich vielleicht auch im BSI. Aber das sind genau die Dinge, auf die man achten sollte.

Lange: Katharina, du hattest vorhin schon so schöne Analogien: Ich lasse nicht meine Balkontür auf im analogen Leben und ich lege vielleicht auch meinen Schlüssel nicht sichtbar im Flur ab, weil ich nicht möchte, dass jemand weiß, dass er da ist und sich dann damit vielleicht Zugang zu etwas verschafft. Aus deinen unterschiedlichen Erfahrungen: Was kann ich denn online alles machen, damit ich niemanden hereinlasse in Systeme und damit sich keiner bei mir umschauen und vielleicht Schindluder betreiben kann; vor allen Dingen, wenn es um Dinge geht, die jetzt auch bald anstehen? Ich gehe mal davon aus, dass alle anfangen, Weihnachtseinkäufe zu machen und andere Dinge. Wie kann ich mich absichern und was sollte ich generell berücksichtigen? Was gibst du uns für Tipps?

Sook Hee Koch: Das BSI hat für die Bürgerinnen und Bürger extra gute Ratschläge im präventiven Bereich, die erklären, wie ich mich diesbezüglich schützen kann. Zum Beispiel mit einer Zwei-Faktor-Authentisierung. Aber auch einem sicheren Passwort. Das Passwort sollte nicht unbedingt „12345“ lauten. Schön wäre es, ein paar Zeichen zwischen den Zahlen zu haben, die kann man ja ruhig nutzen. Wenn etwas passiert ist, sag ich nur: Melden Sie diesen Vorfall! Wenn wir nicht irgendwann über das Problem sprechen, weil es nicht sichtbar ist, dann können wir das Problem nicht angehen. Wir haben das Problem, dass es ein hohes Dunkelfeld in diesem Bereich gibt. Was nicht sichtbar ist, das wissen wir in Deutschland, darüber sprechen wir nicht und dann haben wir auch kein Problem. Das stimmt aber nicht, das ist nicht die Realität. Von daher kann ich Ihnen nur sagen: Stellen Sie bitte eine Strafanzeige. Wir brauchen Zahlen und Fakten, um in der Politik mit der Bitte nach vorne gehen zu können. Wenn alle mal ein bisschen über den Tellerrand schauen, dann hoffe ich doch, dass wir auch zukünftig, weiter gute Ziele erreichen können. Folgen Sie den Präventionstipps des BSI und der Polizei.

Münz: Das ist total sinnvoll, dass so zu sagen. Es gibt tatsächlich viel Material auf den Webseiten des BSI, wo wir uns auch immer wieder bedienen und uns schlauer machen. Ich wollte aber noch einmal, weil ich das in der Frage angekündigt habe und weil ich glaube die Antwort gar nicht mitgekriegt zu haben, zu den DDoS-Attacken zurückkommen. Robert,

vielleicht kannst du noch ein, zwei Sätze dazu sagen, damit das jetzt nicht so allein im Podcast stehen bleibt.

Formanek: Gern! DDoS-Angriffe ist ja Distributed Denial of Service, oftmals sind es nur DoS-Angriffe, also Denial of Service. Das bedeutet, dass ein Dienst, der im Internet steht, erst einmal nicht verfügbar ist. Was heißt das im Einzelnen? Bei einem Onlineshop sehen wir beispielsweise ganz unterschiedliche Vorgehensweisen, aber ich beschreibe es der Einfachheit halber an dem klassischen Vorgehen. Es werden sehr viele Anfrage an einen Server geschickt. Der Webserver ist zunächst ein binäres System. Das heißt, er antwortet oder antwortet nicht. Er antwortet natürlich allen, die Anfragen stellen. Wenn zu viele Anfragen gleichzeitig kommen und der Server nicht adäquat oder angemessen skaliert ist, antwortet er eben der hunderttausendsten Anfrage nicht. Wir sehen oft, dass bestimmte Täter beispielsweise sogenannte Botnets missbrauchen. Ein Botnet ist ein Netz, wo ein Stück Software auf den jeweiligen Computer, in der Regel von Privatpersonen, aber auch von Unternehmen, geschickt wird. Dieser Bot macht dann nichts anderes als genau diese eine Anfrage oder diese vielen Anfragen an den Server zu stellen. Bei den Betreibern des Webservers tritt dann das Problem auf, dass sie sich dagegen wirklich nur sehr schwer wehren können. Das heißt, sie können sich dagegen nur mit einem sehr professionellen Umfeld wehren, weil diese Anfragen von überall herkommen. Das ist das Botnet oder der Denial of Service als kurze Erklärung.

Münz: Wird so etwas auch schon als Erpressung genutzt? Du hast ja gerade schon gesagt, dass man sich dagegen nur schwer schützen kann.

Formanek: So etwas wird tatsächlich auch als Erpressung genutzt. Wir hatten in diesem Sommer ein paar Mal den Versuch, Systeme tatsächlich mit einem DDoS-Angriff überziehen lassen zu können. Da wurde angekündigt, dass ich jetzt ab morgen oder in vier Tagen einen DDoS-Angriff erleide, wenn ich nicht eine bestimmte Summe, in der Regel in Bitcoins, begleiche. Zum Testen und zum Teasern wird dann schon mal ein kleines bisschen „ge-DDoSt“. Die Unternehmen erleiden dann tatsächlich einen DDoS-Angriff, der dann auch in einer Kapazität vorhanden ist, die schon nachdenklich stimmt. Manchmal ist es so, dass diese Tätergruppierungen noch einmal kommen und dann tatsächlich einen großen DDoS-Angriff gegen das Unternehmen richten. Das ist eine ganz klassische Erpressung, denn für Unternehmen, wie beispielsweise MediaMarkt, ist der Onlineshop vermutlich ganz besonders wichtig. Es gibt aber auch Unternehmen, die ausschließlich auf den Webverkauf abzielen und für die wäre das natürlich eine Katastrophe.

Lange: Ich würde gern Katharina noch etwas fragen, beziehungsweise Bezug nehmen auf die Kulisse, vor der sie steht. Ihr da draußen seht sie nicht, aber wir sehen sie. Dann komme ich gern noch einmal zu Robert zurück, der vielleicht auch noch ein paar Tipps hat, wie Weihnachten auch beim Einkaufen sicher sein kann. Katharina, Robert hat vorhin schon von einem Bulli gesprochen. Du stehst heute für diese Aufnahme auch von einem Bulli. Auch wenn unsere Hörer und Hörerinnen den nicht sehen: Was hast du denn für einen Bulli?

Sook Hee Koch: Das ist nicht mein Bulli, das ist der Bulli meiner alten Cyber-Kollegen des Landeskriminalamts Nordrhein-Westfalen. Die haben jetzt aktuell einen neuen Cybercrime-Bulli, mit dem sie an die Einsatzorte fahren. Er ist gut ausgerüstet – wirklich sehr modern, mit guten technischen Mitteln. Die werde ich natürlich jetzt im Einzelnen nicht beschreiben.

Lange: Schade!

Sook Hee Koch: Da es sich hier um polizeiliche Instrumente handelt, müsste man eine offizielle Anfrage beim LKA in NRW stellen.

Lange: Da wir dich ja jetzt kennen, werden Michael und ich das machen. Vielleicht ist das für uns unser Weihnachtswunsch. Danke dir, dass du das noch einmal erläutert hast. Der Anblick ist einfach so schön, ich musste den teilen.

Sook Hee Koch: Aber wir müssen dazu sagen, dass das nur ein Hintergrundfoto war.

Lange: Ja, das hätten wir jetzt nicht verraten müssen. Es war so beeindruckend. Danke dir und wir kommen auf das Angebot zurück, dass man da eine offizielle Anfrage stellen kann. Wir beide sind ja sehr, sehr wissbegierig. Robert, unsere Hörer und Hörerinnen sind vielleicht auch wissbegierig: Katharina hat schon einige Tipps für das sichere Navigieren im digitalen Alltag, gerade mit Blick auf Weihnachtseinkäufe und andere Dinge, genannt. Hast du denn noch welche aus deiner Erfahrung und vielleicht auch ein paar Tipps wie du es praktizierst so kurz vor Weihnachten?

Formanek: Ganz klassisch und ganz tatsächlich: Ich nutze die Kampagne #einfachaBSIchern, die das BSI gestartet hat, weil mir da immer wieder gezeigt wird, was ich denn eigentlich tun kann und auf welche sehr einfache Art und Weise ich mich eigentlich schützen kann. Diese Kampagne umschreibt einfach wesentliche Merkmale, die mir helfen zu erkennen, ob ich es mit einem vermeintlich seriösen Unternehmen zu tun habe, indem ich eben nicht jedem geringen Preis hinterherjage. Das kann trotzdem durchaus sinnvoll sein, je nach Geldbeutel ist es auch notwendig. Trotzdem sollte man sicherstellen, dass man seine Ware auch bekommt und diese Kampagne beschreibt zum Beispiel auch, welche Art von Zahlungsmethoden mir angezeigt werden sollten. Mit sehr einfachen Mitteln wird darauf hingewiesen, dass ein vorhandenes Impressum wichtig ist, weil ich dann im Zweifel auch einen Ansprechpartner oder eine Ansprechpartnerin habe, beispielsweise bei einer Reklamation. Durch die Technik werde ich ja auch unterstützt. Im Browser kann ich zum Beispiel feststellen: Ist dieses System denn eigentlich auf sichere Kommunikation abgestellt? Und dergleichen mehr ist möglich. Die Kampagne #einfachaBSIchern kann ich allen Zuhörerinnen und Zuhörern durchaus empfehlen an dieser Stelle.

Münz: Ein Punkt, den wir schon einmal angesprochen hatten, ist das Thema eigener Account. Bei vielen Shops muss ich Accounts einrichten. Die wollen ja auch eine E-Mail-Adresse haben, zu der sie dann zum Beispiel die Rechnung hinschicken können, wenn das System das gerade hergibt. Gibt es bei der Account-Sicherheit noch irgendetwas zu beachten? Passwörter hatten wir schon, aber gibt es darüber hinaus noch irgendetwas, was du immer machst, wenn du dich irgendwo anmeldest?

Formanek: Zwei Dinge: Ich nutze bei jedem Shop ein eigenes Passwort und ich nutze ein immer möglichst langes Passwort. Was immer das System an Länge zur Verfügung stellt, die nutze ich auch. Das Ganze verwalte ich in einem Passwort-Manager. Und im einfachsten Fall schreibt man es sich auf, dann kann man es einfach abtippen.

Münz: Prima, danke dir. Passwort-Manager ist so ein Begriff, der hier immer wieder auftaucht. Ute, wenn sie noch da ist, würde wahrscheinlich sagen: „Michael, du brauchst den auch!“.

Lange: Ich wollte den gar nicht erwähnen. Ich bin Robert ganz dankbar, dass er das Thema noch einmal angesprochen hat. Wir haben jetzt eine ganze Menge Tipps. Wir haben auch den Hinweis auf die Kampagne. Wir könnten wahrscheinlich noch viel, viel länger mit euch sprechen, aber würden jetzt wahrscheinlich einfach „den Sack zu machen“, wie wir das so schön nennen – die Folge abschließen. Wir danken euch ganz, ganz herzlich. Es war fast wie ein Krimi, euch zuzuhören und zu sehen, was hinter den Kulissen alles läuft, damit wir sicher im digitalen Alltag navigieren können, aber auch was wir tun können, um dazu beizutragen. Dankeschön euch beiden! Hoffentlich haben wir demnächst die Gelegenheit, diesen besagten Bulli zu besichtigen. Das ist gespeichert.

Münz*:* Auf jeden Fall euch beiden schon einmal frohe und sichere Weihnachten!

Formanek*:* Vielen Dank, das wünsche ich euch und den Zuhörerinnen und Zuhörern auch. Dankeschön!

Münz*:* Das war echt viel Input. Darüber muss ich auch noch einmal nachdenken. Es hat super viel Spaß gemacht. Für die nächste Folge haben wir uns vorgenommen, dass mindestens genauso spannend und unterhaltsam zu machen. Was es dann genau wird?! Da müsst ihr euch überraschen lassen, das verraten wir euch an dieser Stelle noch nicht.

Lange: Das ist ja mit Weihnachtsgeschenken auch so: Man soll darüber vorher nicht sprechen. Bis diese Folge kommt, könnt ihr natürlich unseren Podcast „Update verfügbar“ liken und ihm folgen auf euren Podcast-Plattformen. Dann verpasst ihr keine Folge. Vielleicht wollt ihr auch noch einmal in ältere Folgen reingucken. Wir hatten zum Beispiel letztes Jahr vor Weihnachten mal eine, die sich mit Onlineshopping sehr detailliert beschäftigt hat. Also, wer jetzt Appetit darauf gekommen hat…

Münz*:* …reinhören! Die Folge zuvor war auch schon zu Ransomware. In die kann man auch noch einmal reinhören. In der haben wir auch noch ein paar Themen und Tipps zu dieser offensichtlich immer problematischer werdenden Thematik platziert. Und wie immer gilt: Kontaktiert uns gerne über die BSI-Kanäle auf Facebook, auf Instagram, Twitter und YouTube oder schickt uns eine E-Mail an bsi@bsi.bund.de.

Lange: Wir freuen uns immer über Post. Bis wir uns wiedererleben und hören, wünschen wir euch alles Gute! Bleibt weiterhin gesund, passt gut auf euch auf! Bis dann, Tschüss!

Münz*:* Tschüss.

Besuchen Sie uns auch auf:

https://www.bsi.bund.de/
https://www.facebook.com/bsi.fuer.buerger
https://twitter.com/BSI_Bund
https://www.instagram.com/bsi_bund/
https://social.bund.de/@bsi

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185-189, 53133 Bonn