„Update Verfügbar – ein Podcast des BSI "

Transkription für Folge 04, 29.01.2021: Hacken im Namen der Gesundheit

Moderation: Karin Wilhelm Maximilian Berndt, BSI

Gast: Dr. Dina Truxius, BSI

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wilhelm: Hallo?!

Berndt: Hallo!

Wilhelm: Ja, ich glaube, wir sind drin. Wir haben uns tatsächlich in den Podcast des BSI gehackt. Einfach durch die Hintertür hereingeschlichen. Das ist der Wahnsinn!

Berndt: Vielleicht fangen wir aber einmal ganz vorne an: Wir sind Max und Karin und wir arbeiten im BSI. Wir sind also Teil des Teams hinter „Update verfügbar". Wir haben Ute und Michael auf die Ersatzbank geschickt für heute.

Wilhelm: Ich gebe zu: Nicht jeder im BSI ist ein Profi-Hacker. Aber um in den Account von Ute zu kommen, musste ich einfach nur raten.

Berndt: Und, was war ihr Passwort?

Wilhelm: Fahrradhelm!

Berndt: Ja, ok, darauf wäre ich, glaube ich, auch gekommen. Sie reden im Podcast ja immer wieder davon.

Wilhelm: Genau, das ist so als würde ich Cyber-Sicherheit als Passwort wählen. Aber die Frage ist: Hast du es bei Michael denn genauso leicht gehabt?

Berndt: Naja, fast. Michael hat sein Passwort mit einer Zahl erweitert, aber sicher war es dadurch auch nicht wirklich! Es hieß Münz80.

Wilhelm: Ach so, das ist dann wahrscheinlich sein Geburtsjahr.

Berndt: Ja, wahrscheinlich. Aber weil das Passwort auch so kurz war, war es innerhalb weniger Minuten erraten.

Wilhelm: Wenn wir die beiden wieder sprechen, müssen wir ihnen unbedingt ein paar Tipps geben.

Berndt: Du meinst so etwas wie, dass sie kein Passwort nutzen sollen, das im Wörterbuch steht oder zufällig ihr Nachname ist?

Wilhelm: Ganz genau, und dass die Länge beim Passwort sehr wohl ganz entscheidend ist. Im Prinzip ist dieses Mal alles gut gegangen, weil nur wir uns hier hereingeschlichen haben. Aber so ein Hack kann auch deutlich böser ausgehen als ein gekaperter Podcast. Heute soll es ja, wie angekündigt, um das Thema Gesundheit gehen. Da sprechen wir auch von wichtigen und wirklich sensiblen Daten. Erst habe ich gedacht, dass wir beide dazu eigentlich wenig zu sagen haben, weil wir uns so selten im Krankenhaus aufhalten – Gott sei Dank. In Pflegeheimen sind wir eigentlich auch nie zu Besuch. Aber dann fiel mir ein: Max, du hast doch diesen Blutzucker-Sensor, den nutzt du doch regelmäßig. Wenn man so ein Gerät manipuliert, dann hat man bestimmt ein richtiges Problem, oder?

Berndt: Das kannst du wohl laut sagen! Also, der Sensor klebt ständig auf meiner Haut und misst mit einer kleinen Nadel, die durch meine Haut sticht, meinen aktuellen Blutzuckerwert. Der Wert wird dann alle paar Minuten an mein Handy geschickt. Ich kann ihn da ablesen oder mein Handy kann auch Alarm schlagen, wenn der Wert eine gewisse Grenze unterschreitet oder überschreitet. Wenn sich jetzt jemand einen Scherz erlauben würde oder jemand möchte aus anderen Gründen das Gerät manipulieren und damit die Werte verändern, dann würde ich eventuell zu viel Insulin spritzen, weil ich glaube, dass mein Blutzuckerwert zu hoch ist. Das könnte wiederum schwere Unterzuckerung oder Ohnmacht zur Folge haben.

Wilhelm: Das wäre dann aber ganz schön krass. Ich glaube, generell kann man sagen: Wenn digitale Gesundheitsgeräte manipuliert werden, kann das schnell gefährlich ausgehen. Darum gibt es solche Menschen, wie unseren heutigen Gast Dr. Dina Truxius, die sich um die Sicherheit solcher Produkte kümmern. Hallo, Dina!

Truxius: Hallo!

Berndt: Dina haben wir heute in unser Home-Office geschaltet, denn sie arbeitet im BSI im Bereich Cyber-Sicherheit im Gesundheits- und Finanzwesen. Sie spricht heute mit uns über die Sicherheit von vernetzten Medizinprodukten.

Wilhelm: Der eine oder andere wird sich jetzt fragen: Vernetzte Medizinprodukte?! Was ist das eigentlich ganz genau? Dina, da kannst du uns bestimmt ein paar Beispiele nennen, oder?

Truxius: Ja, Karen, das ist eine spannende Frage, was vernetzte Medizinprodukte sind. Ich verstehe darunter Produkte, wie beispielsweise eine Insulinpumpe, die mit einer App kommunizieren kann, aber vielleicht auch eine Pillendose, die meiner App meldet, ob ich meine Medikamente regelmäßig genommen habe. Aber natürlich auch Patientenmonitore, zum Beispiel in Krankenhäusern, die sowohl untereinander kommunizieren als auch mit einer Zentralstation. Oder denken wir mal weiter an Intensivstationen, wo man nicht nur solche Monitore zur Überwachung von Patienten nutzt, sondern vielleicht auch Infusionspumpen, die entsprechende Medikamente den Patienten zuführen. Klassischerweise sind mehrere um das Bett herumgruppiert, bei denen die Daten zu einer zentralen Station, einer Überwachungsstation, geleitet werden, wo dann im Prinzip die Überwachung stattfindet.

Wilhelm: Das sind ja echt viele Geräte, die du hier aufzählst. Du bist für die Sicherheit dieser Geräte zuständig? Oder wie darf ich mir deinen Alltag im BSI vorstellen?

Truxius: Ja, das ist so tatsächlich richtig, aber hier müssen wir ganz klar unterscheiden: Ich bin für die IT-Sicherheit von diesen Produkten zuständig und nicht für die Patientensicherheit dieser Produkte. Das heißt, wir kümmern uns darum, ob die Kommunikation zum Beispiel zwischen dem Produkt und einer App oder den Produkten untereinander sicher ist, ob also die Kommunikationsschnittstellen sicher sind. Werden die Daten sicher übertragen? Sind sie entsprechend geschützt oder muss man zusätzliche Schutzmaßnahmen einbauen? Genau deswegen mache ich relativ viel Projektarbeit. Bei zwei meiner Projekte, einmal das Projekt „eCare – Digitalisierung in der Pflege“ und auch das Projekt „ManiMed – Manipulation von Medizinprodukten“, haben wir uns ein paar Medizinprodukte – im Fall von eCare auch IoT-Produkte – sicherheitstechnisch angeschaut, um den IT-Sicherheitszustand dieser Produkte erst einmal einschätzen und bewerten zu können. Sprich, wir haben diese Produkte, platt gesagt, gehackt, haben das aber im Vorfeld mit den Herstellern natürlich abgesprochen.

Berndt: Wenn ich aber von Gesundheit und Technik höre, dann denke ich zuallererst einmal an Corona. Wir nehmen jetzt auch aus unserem Home-Office auf. Hast du denn die Corona-Warn-App selbst auf dem Handy installiert? Und was hältst du von der App?

Truxius: Ja, tatsächlich habe ich die Corona-Warn-App auch auf meinem Handy installiert. Ich war vielleicht nicht vom ersten Tag an dabei, sondern habe sie erst, glaube ich, zehn Tage nach dem Erscheinungsdatum im Juni installiert; vielleicht auch auf Druck von Freunden und Bekannten, die mich gefragt haben, warum ich als BSI-Mitarbeiterin genau diese App noch nicht installiert habe, wenn sie denn so sicher ist. Ich finde die App tatsächlich sehr gut. Sie ist sehr datensparsam. Im Gegensatz zu anderen Ländern haben wir, finde ich, eine sehr gute Datenschutz-Policy dahinter. Es ist eine Open Source Entwicklung gewesen. Das heißt, jeder konnte sich an der Entwicklung beteiligen. Der Code ist öffentlich zugänglich. Im Prinzip konnte jeder dazu beitragen und sich genauer anschauen, was da so gemacht wird. Tatsächlich hatte ich bisher schon mehrfach die Anzeige von Risikobegegnungen, aber glücklicherweise immer mit niedrigem Risiko. Ich hatte hauptsächlich

vielleicht eine oder maximal zwei. Das höchste waren tatsächlich einmal drei Risikobegegnungen, die mir angezeigt wurden. So konnte ich letztendlich am eigenen Leib oder mit der eigenen App erfahren, dass unsere App tatsächlich funktioniert.

Wilhelm: Ja, ich bin auch ein großer Fan der Corona-Warn-App und freue mich jeden Tag, wenn mein Status da grün ist. Bis jetzt habe ich da immer Glück gehabt. Aber in diesen Tagen fällt es mir wie vielen anderen sehr schwer, die ganze Zeit Zuhause zu bleiben. Man arbeitet von Zuhause, kommt nicht vor die Tür, sieht keine Menschen. Und, was ich auch ganz schlimm finde: Man bewegt sich so wenig. Darum habe ich mir jetzt einen Schrittzähler besorgt. Der erinnert mich stündlich, dass ich mich mal bewegen soll. Wenn ich abends sehe, dass ich mich wirklich nur in mein Home-Office gerollt habe am Tag, dann gehe ich noch eine Runde spazieren. Der hat auch meine Pulsdaten und beim Joggen sagt er mir, welche Strecke ich wie lange gelaufen bin. Das finde ich alles sehr praktisch, aber da stellt sich mir schon die Frage, ob das denn alles so sicher ist. Da würde ich gerne deine Meinung als Expertin hören. Was hältst du denn von so einer App?

Truxius: Naja, ich muss zugeben, dass ich mich inzwischen auch selbst tracke beziehungsweise meine Fitness. Vielleicht auch aus den von dir genannten Gründen, dass man sich viel im Home-Office befindet und sich weniger bewegt als sonst. Ich denke, generell sollte einem hier klar sein, dass man gewisse Daten preisgibt, um solche Analysen über diese App zu realisieren. Sprich: „Steh mal bitte auf, du hast dich zu wenig bewegt“ oder ähnliches. Das ist immer eine Preisgabe von personenbezogenen Daten und das sollte man sich klar machen. Nichtsdestotrotz ist vielleicht auch der Mehrwert darin zu sehen, dass man eben daran erinnert wird, dass man aufsteht. Eine Möglichkeit, so wie ich das auch handhabe, ist, dass man solche Apps, denen man erst einmal nicht über den Weg traut – ich muss auch zugeben, dass ich mich zum ersten Mal tracke mit der App und einem Wearable, zum Beispiel auf einem anderen Smartphone installiert und nicht auf dem, was man für andere Zwecke nutzt. Aber das ist natürlich ein Luxusproblem.

Wilhelm: Vielleicht kann ich an der Stelle noch eine Frage stellen. Du hast auch das Wort Wearable gerade genutzt: Wofür steht das eigentlich?

Truxius: Also, ich verstehe unter einem Wearable ein Produkt, ein Gerät, was man tragen kann – von „to wear“, auf Deutsch tragen. Das wäre jetzt in dem Fall meines Fitnesstrackers ein kleines Armband, was mit der App kommuniziert und im Prinzip meine Schritte, meine Aktivitäten und auch meine Nicht-Aktivitäten aufzeichnet und an die App weiterleitet.

Berndt: Jetzt ist es ja das eine, wenn ein Hacker sieht, dass Karin am Tag nur 500 Schritte gegangen ist. Aber wie sieht das aus, wenn ich im Krankenhaus bin und ich bin an Geräte angeschlossen, die vielleicht manipuliert wurden oder ich bekomme ein Implantat? Kann ich mir da sicher sein, dass die Geräte eben nicht manipuliert sind? Was kann da schlimmstenfalls passieren?

Truxius: Also, wenn ich mir unsere Projektergebnisse – gerade aus dem Projekt ManiMed – anschaue, wo wir uns ausschließlich auf Medizinprodukte fokussiert haben, die eben auch im Krankenhaus eingesetzt werden, wie zum Beispiel Patientenmonitore, Implantate mit Zubehör, Infusionspumpen oder Beatmungsgeräte, kann ich schon mal Entwarnung geben. Was wir gesehen haben, ist, dass diese Produkte sehr robust sind – die Medizinprodukte an sich. Sprich, die Pumpen pumpen, die Beatmer beatmen, die Monitore monitoren und die Schrittmacher machen Schritt, um das mal einfach zu sagen. Was wir gesehen haben, ist, dass die Vernetzung, also die Kommunikation mit anderen Produkten oder die Kommunikation untereinander von Produkten, häufig nicht unbedingt unseren sicherheitstechnischen Anforderungen aus IT-Sicht genügt hat. Deswegen würde ich da erst einmal Entwarnung geben; auch dadurch, dass Krankenhäuser besonders abgesichert sind und solche Produkte auch in abgesicherten Umgebungen betrieben werden sollen. Nichtsdestotrotz, wenn man unsere Ergebnisse sieht, dass wir IT-Sicherheitslücken im Prinzip bei allen Produkten gefunden haben – in unterschiedlichem Schweregrad natürlich, sollte man hier nicht aufhören. Man sollte die IT-Sicherheit absolut im Blick behalten, um eben keine offenen Scheunentore zu ermöglichen und Hackern dann praktisch das Eindringen in ein Krankenhaus zu erlauben.

Dazu wäre auch noch zu sagen, dass ich der Meinung bin, dass es für solche Angriffe häufig etwas mehr braucht. Ich müsste mir schon einen Arztkittel oder einen Blaumann anziehen, um in das Krankenhaus zu kommen, um mich beispielweise dort in das Netzwerk einzuschleusen und um solche Geräte überhaupt manipulieren zu können. Das ist von außen häufig relativ schwierig, würde ich sagen – zumindest das, was wir gesehen haben.

Berndt: Das klingt erst einmal beruhigend. Jetzt haben wir über die Seite der Hacker gesprochen, die eventuell versucht in ein Krankenhaus einzudringen oder in die Infrastruktur. Ich habe aber zuletzt auch häufiger von Menschen gehört, die in ihre eigenen Geräte eindringen, zum Beispiel Diabetiker, die versuchen ihre Insulinpumpe zu hacken, um da irgendwelche Zusatzfunktionen herauszuholen. Warum macht man so etwas genau und was hältst du davon?

Truxius: Ja, Max, das sind spannende Fragen. Ich würde dir gern erst die erste beantworten, warum Patienten so etwas machen. Warum hacken Patienten zum Beispiel ihre Insulinpumpen? Na klar, um eine bessere Versorgung für sich zu haben und um mit dem Produkt tatsächlich besser leben zu können. Gerade im Bereich der Insulinpumpen stellt man sich häufig – wenn man nicht Diabetiker ist – vor, dass so eine Insulinpumpe eigentlich die Funktion der Bauchspeicheldrüse übernimmt. Das ist aber tatsächlich nicht so, sondern eine Insulinpumpe pumpt per se erst einmal nur Insulin. Es gibt aber Bestrebungen, weswegen dann Patienten solche Pumpen sicherheitstechnisch oder it-mäßig verändern – ich will jetzt gar nicht sagen hacken, um eben eine möglichst natürliche Funktion dieser Pumpe nachzuahmen. Solche Pumpen kann man als sogenanntes Closed-Loop-System benutzen. Das ist aber so weder vom Hersteller noch von der Zulassung her vorgesehen. Das ist also in dem Sinne verboten. Es obliegt aber natürlich dem Patienten selbst. Wenn man etwas machen kann, dann kann man es zumindest auch einmal ausprobieren. Das tun auch einige, weil es tatsächlich einen positiven Effekt hat. Das heißt, diese Pumpen sind zum Beispiel mit einem Mess-Sensor verbunden, der kontinuierlich den Blutzuckerspiegel misst und eine Rückmeldung an die Pumpe gibt. Die

Pumpe tätigt dann automatische Insulinabgaben, wenn sie benötigt werden. Sprich, nicht nur vor dem Essen, wie das ein klassischer Diabetiker mit seinem Pen macht, sondern es ist sozusagen eine automatisierte Insulinzufuhr – ähnlich wie die Bauchspeicheldrüse das tun würde, wenn sie noch funktionieren würde. Nichtsdestotrotz muss man hier natürlich aufpassen. Das Loopen hilft sicherlich und bei vielen Patienten senkt es beispielweise den Langzeitzuckerwert, der für viele wichtig ist, deutlich. Die Patienten erfahren dadurch eine bedeutend angenehmere Therapie und müssen sich vielleicht auch weniger Sorgen machen. Solche Ideen existieren auch für Kinder und Alte. Dennoch muss man sagen, dass man nicht nur durch einen Angriff, wie wir ihn zeigen konnten, sondern auch durch Loopen – wenn man das nicht richtig macht – zum Beispiel zu viel Insulin abgeben könnte und dies auch tödlich für Patienten enden könnte.

Berndt: Du sprichst jetzt von einem Angriff, wie ihr ihn hättet durchführen können. Worum ging es da? Was hättet ihr tun können?

Truxius: Wir haben uns im Projekt eine Insulinpumpe angeschaut, die mit einer App kommuniziert und die auch praktisch mit einer App gesteuert werden kann. Diese Pumpe könnte prinzipiell – wenn auch nicht vorgesehen – für ein Closed-Loop-System genutzt werden. Was wir gefunden haben, ist, dass die Kommunikation zwischen der Pumpe und der App nicht so sicher war. So, dass wir mit relativ einfachem technischem Equipment – Hobbyfunker-Equipment – diese Kommunikation zwischen Pumpe und der App sozusagen absaugen hätten können. Wir hätten dann entsprechend die Kommunikation manipulieren können, sodass wir praktisch die Pumpe hätten übernehmen können. Wir hätten der Pumpe diktieren können, dass entsprechend Insulinabgaben getätigt werden, die der Patient dann auch nicht mehr hätte unterdrücken können. Das heißt, dass einzige, was der Patient hätte tun können, wäre, sich die Nadel und praktisch das Schlauchsystem vom Bauch zu reißen, um das zu verhindern.

Berndt: Und dann habt ihr sicherlich den Hersteller kontaktiert? Wie haben die darauf reagiert, dass man ihr Gerät so leicht manipulieren konnte?

Truxius: Ja, auch diesem Hersteller, so wie allen anderen in diesem Projekt, war klar, dass wir sie bzw. ihre Produkte „hacken“. Es kann natürlich vorkommen, dass wir Schwachstellen finden, die auch einen Einfluss auf die Patientensicherheit haben können, so wie in diesem Fall. Der Hersteller hat sehr schnell reagiert. Er hat ein Update bereitgestellt, was genau diese Schwachstellen behebt, sodass dieser Angriff eben nicht mehr möglich ist. Dieses Update wurde dann auch ins Feld gebracht. Das heißt, die Pumpen, die dieses Update bekommen haben, kann man in dieser Form nicht mehr manipulieren. Ich denke, der Hersteller war auch sehr dankbar für diese Information. Glücklicherweise konnte man dadurch, dass man die Pumpe in den Flugmodus praktisch gestellt hatte, die Kommunikation zwischen Pumpe und App unterbinden. So war auch dieser Angriff sofort nicht mehr möglich und dann durch das entsprechende Update komplett behoben.

Wilhelm: Da sind doch aber schon gute Neuigkeiten dabei. Erst einmal sind viele Produkte recht sicher und zweitens testet ihr das auch regelmäßig. Im Zweifel wird das natürlich auch umgesetzt. Wie wichtig ist denn IT-Sicherheit für viele Hersteller? Was sind denn da deine Erfahrungen?

Truxius: Das ist eine sehr gute Frage, die du mir hier stellst. Ich bin häufig nicht unbedingt so zufrieden mit dem Umgang hinsichtlich der IT-Sicherheit. In dem Fall mit der Insulinpumpe war ja tatsächlich die Patientensicherheit gefährdet. Da müssen Hersteller umgehend reagieren. Es gibt keinen Weg daran vorbei. Was die IT-Sicherheit betrifft, ist es oft leider nicht ganz so einfach und es kann natürlich ein bisschen dauern, weil IT-Sicherheit keine Priorität hat in dem Sinne, sondern nur dann, wenn sie eben die Patientensicherheit gefährdet. Hier würde ich mir wünschen, dass Hersteller auch entsprechende IT-Sicherheitshygiene betreiben, dass sie darauf achten, dass sie entsprechende Prozesse implementieren – und zwar von Anfang an. IT-Sicherheit ist nichts, was man nachher obendrauf baut. Es ist etwas, was man von vornherein bedenken sollte. Man sollte darauf achten, dass die Reaktionen entsprechend schnell sind entsprechend der Kritikalität der Schwachstellen, wenn man etwas findet.

Berndt: Kritikalität? Kannst du das einmal kurz erklären? Was bedeutet das bei Medizinprodukten?

Truxius: Unter Kritikalität verstehe ich das Folgende: Es ist erst einmal kein Problem, sage ich mal so ganz salopp, wenn Schwachstellen entdeckt werden. Es geht darum, dass Schwachstellen erst einmal ausgenutzt werden, damit dieser Effekt eintritt. Dann geht es praktisch um die Ausnutzbarkeit und um die Wahrscheinlichkeit der Ausnutzung dieser Schwachstellen. Und um das besser einschätzen zu können, vergeben wir sozusagen Noten von sehr wahrscheinlich bis nicht wahrscheinlich, also kritisch bis niedrig. Wir bewerten, wie wahrscheinlich es ist, dass eine Schwachstelle ausgenutzt wird, was für einen Effekt sie nachher hat und wie schlimm das letztendlich ist. Das verstehe ich unter Kritikalität. Es gibt Schwachstellen, die liegen zum Beispiel in nachgeschalteten Systemen. Die hätten keinen direkten Einfluss auf die Patienten, so wie viele, die wir auch im Projekt gefunden haben. Aber natürlich haben die Schwachstellen, die ich vorhin für die Insulinpumpe beschrieben habe, eine hohe Kritikalität, weil ihre Ausnutzung vielleicht technisch nicht ganz so kompliziert ist und weil sie einen Einfluss auf die Patientensicherheit haben.

Berndt: Ach so! Danke!

Wilhelm: Dann hoffen wir, dass die Hersteller auch die Cyber-Sicherheit bald sehr wichtig nehmen, auch dank eurer Arbeit. Aber vielleicht stellt sich jetzt der ein oder andere Zuhörer, die eine oder andere Zuhörerin, die Frage: Was kann ich denn jetzt tun? Wie kann ich mich schützen, um nicht irgendwie in Gefahr zu kommen? Worauf muss ich achten? Welche Fragen muss ich stellen? Was muss ich nachschauen? Hast du da ein paar Tipps und Empfehlungen für den Alltag?

Truxius: Ja, vielleicht sollten wir da noch einmal klarstellen: Nicht jeder Bürger bekommt einfach so ein Beatmungsgerät, eine Insulinpumpe oder ein Implantat im Supermarkt oder in einem Medizinprodukte-Shop. Auch Insulinpumpen werden verschrieben und die anderen Produkte, die ich gerade genannt habe, werden spezifisch für Krankenhäuser, also für

Betreiber, verkauft und dort in Betrieb genommen. Nichtsdestotrotz, wie wir das auch im Projekt eCare zeigen konnten, gibt es natürlich Geräte wie Pulsoximeter. Sie sind auch vernetzt und als Medizinprodukt klassifiziert, aber man kann sie so im Onlinehandel kaufen. Bei klassischen Medizinprodukten, die im Krankenhaus betrieben werden und die wir in ManiMed untersucht haben, obliegt die IT-Sicherheit und auch die Sicherheit dem Hersteller. Da kann ich als Patient nicht viel machen, außer kritisch nachzufragen. Das wäre tatsächlich mein Tipp: Seien Sie skeptisch! Schauen Sie sich an, wohin Ihre App redet, was Ihre App macht und welche Berechtigungen sie anfordert. Möchte sie auf Ihre Fotos zugreifen? Möchte sie alle Ihre Kontakte irgendwo anders hin verteilen? Werden Gesundheitsdaten von Ihnen aufgenommen? Werden Sie die ganze Zeit getrackt wie bei unserem Fitnesstracker? Gehen Sie mit gesundem Menschenverstand heran: Möchte ich so etwas? Bringt mir das etwas? Oder verkaufe ich hier letztendlich meine Daten? Natürlich wäre es wünschenswert, wenn insgesamt mehr IT-Sicherheit, gerade auch im Bereich der Wearables oder der IoT-Produkte, stärker von der Bevölkerung gefordert wird, damit Hersteller zukünftig auch mehr Augenmerk drauflegen und mehr in die IT-Sicherheit investieren, um Daten und Menschen auch langfristig zu schützen.

Berndt: Schöne Tipps, die sich auch leicht und ganz einfach im Alltag umsetzen lassen. Insgesamt fand ich das Gespräch sehr beruhigend, dass es Leute wie dich gibt, die sich darum kümmern, dass solche Produkte sicher sind. Deshalb vielen Dank, dass du dir die Zeit genommen hast und hier bei uns im Podcast warst.

Truxius: Ja, vielen Dank, dass ich meine Arbeit, die mich auch wirklich fasziniert, hier vorstellen konnte. Danke!

Berndt: Dann bleibt uns nur noch zu sagen: „Update verfügbar“, gibt es überall da, wo es Podcasts gibt – bei Spotify, Deezer, Google Podcasts oder iTunes zum Beispiel.

Wilhelm: Natürlich freuen wir uns auch auf Ihre Rückmeldung, wenn Sie zum Beispiel sagen, „Ich habe einen Wunsch für ein ganz spezielles Cyber-

Sicherheitsthema“. Geben Sie uns einfach Bescheid. Sie finden uns über Facebook, Twitter, YouTube oder können uns per E-Mail kontaktieren. Alle spannenden Links oder Dinge, auf die wir verwiesen haben, die Sie heute hier im Gespräch gehört haben, die finden Sie auch in den Shownotes. Vielleicht finden wir sogar noch einen interessanten Vortrag von Dina, den wir Ihnen dann auch verlinken werden. Ich glaube, ich habe jetzt hier lang genug gestanden. Max, ich werde jetzt eine Runde laufen gehen. Was machst du jetzt so?

Berndt: Ich werde mal Ute und Michael anrufen, um gemeinsam mit ihnen ein sicheres Passwort für den Podcast-Account zu erstellen.

Wilhelm: Schöne Idee! Uns bleibt an dieser Stelle dann auch nichts mehr zu sagen als: Bis bald zum nächsten „Update Podcast“!

Berndt: Tschüss, bis bald!

Wilhelm: Tschüss!

Besuchen Sie uns auch auf:

https://www.bsi-fuer-buerger.de
https://www.facebook.com/bsi.fuer.buerger
https://www.twitter.com/BSI_Presse
https://www.instagram.com/bsi_bund/

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