„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 47, 11.09.2024

Moderation: Ute Lange, Michael Münz
Gäste: Karin Wilhelm, BSI-Referatsleiterin und Joachim Schneider, Geschäftsführer der Polizeilichen Kriminalprävention der Länder und des Bundes
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ute Lange: Wir begrüßen euch heute von der Internationalen Funkausstellung in Berlin, kurz auch IFA. Dies ist die Messe für Unterhaltungselektronik und Haushaltsgeräte. Sie feiert in diesem Jahr ihr hundertjähriges Jubiläum, und zwar unter dem Motto: "Innovation für alle".

Michael Münz: Wir haben uns das Thema digitale Sicherheit im Smarthome herausgepickt und zwei Gäste zu uns an den BSI-Stand eingeladen, die unter anderem Tipps zu Anwendungen im Smarthome geben.

Ute Lange: Zum einen haben wir hier den Geschäftsführer des Programms Polizeiliche Kriminalprävention der Länder und des Bundes. Ihr habt auch eine schöne Abkürzung, ProPK, Joachim Schneider. Sehr schön, dass du da bist.

Joachim Schneider: Herzlichen Dank für die Einladung.

Michael Münz: Ein herzliches "Welcome back" geht an Karin Wilhelm, die Leiterin des BSI-Referats Verbrauchersensibilisierung und Informationsvermittlung. Schön, dass du wieder da bist, Karin.

Karin Wilhelm: Hallo. Schön, wieder da zu sein.

Ute Lange: Fangen wir doch gleich mit dir an, Karin. Das BSI bringt zusammen mit der ProPK, also der Organisation von Joachim, einmal im Jahr den Cybersicherheitsmonitor heraus. Das ist eine Studie, die auf einer Onlinebefragung von Internetnutzenden in Deutschland basiert. Wir nehmen in unserem Podcast häufiger auf eure Ergebnisse Bezug. Das weißt du. In diesem Jahr habt ihr den Fokus Smarthome und die Ergebnisse sagen, dass 75 Prozent der Menschen ein Smarthome -Gerät haben. Das sind doch viele. Das sind drei Viertel der Menschen in Deutschland. Bedeuten denn mehr smarte Geräte aus Sicht des BSI auch ein höheres Risiko für Nutzerinnen und Nutzer?

Karin Wilhelm: Ganz genau. Du sprichst den wichtigsten Punkt an. Genau darum haben wir im Cybersicherheitsmonitor einmal dieses Fokusthema gemacht. Wie ist dieses smarte Zuhause? Wir hören, es gibt viele Geräte, und ich glaube, viele da draußen wissen gar nicht, was ein smartes Gerät ist. Wir können hier wundervoll über die IFA laufen und wir sehen Gerät um Gerät bis zur Karaoke-Maschine da drüben. Das sind alles smarte Geräte. Wir haben in der Umfrage gesehen, dass die Menschen da weniger Schutzmaßnahmen nutzen und merken, da ist ein Einfallstor. Genau darum wollen wir heute darüber sprechen.

Ute Lange: Das Einfallstor ist bei smarten Geräten immer die Verbindung zum Netz da draußen. Mein Gerät ist smart, wenn es mit dem Internet kommunizieren kann.

Karin Wilhelm: Ganz genau. Ab da ist es internetfähig. Es gibt immer Daten, die ich von A nach B schicke, sei es bei einer smarten Glühbirne, die sagt: Aus oder an. Ich bin da oder ich bin nicht da. Das sind Informationen, die ich verrate.

Michael Münz: Joachim, wir haben jetzt gehört, es gibt immer mehr Smarthome-Geräte zu Hause, bei unseren Hörerinnen und Hörern dann wahrscheinlich auch. Wie schaut ihr denn als Polizei auf diese Entwicklung und macht euch das an der einen oder anderen Stelle vielleicht auch Sorgen?

Joachim Schneider: Es stimmt uns auf jeden Fall nachdenklich. Das sind zum einen die Ergebnisse unserer gemeinsamen Befragung des Cybersicherheitsmonitors, die uns wertvolle Hinweise liefern. Ich komme nochmal darauf zurück. Es ist generell so, dass die Kriminalität in Deutschland immer digitaler wird. Wir haben im Cybercrime-Bereich Zuwächse in den letzten zehn Jahren von über zwei Dritteln. In gleichem Maße sind in der Zeit die Eigentumsdelikte in der analogen Kriminalität über ein Drittel zurückgegangen. Das zeigt schon ein Stück weit, wo die Reise hingeht, auch für uns und mit Blick auf Smarthome – auch wenn ich im Moment keine akuten Warnmeldungen habe. Deswegen machen wir aber auch Prävention. Dazu soll es nämlich gar nicht kommen. Wir beobachten mit Sorge, wenn 75 Prozent der Bürgerinnen und Bürger Smarthome-Geräte haben und dann ein Drittel davon noch nicht einmal etwas davon gehört hat oder eine Information hat, dass von diesen Geräten auch Gefahren und Risiken ausgehen. Da klingeln bei mir als Präventioner alle Alarmglocken. Das ist klar. Das wird viel zu stark vernachlässigt. Die Menschen verkennen ein Stück weit, glaube ich, dass sie in ihren Häusern mit solchen smarten Anwendungen neben ihren normalen Türen, die sie haben, ihren Haustüren und Terrassentüren, weitere Türen haben, nämlich digitale Türen. Die gilt es in gleichem Maße zu sichern, wie sie ihre Haustüre, Keller- und Terrassentür auch sichern.

Michael Münz: Danke dir. Wir schauen einmal in den Cybersicherheitsmonitor und schauen einmal, wie die Menschen auf die Fragen zum Thema Smarthome geantwortet haben. Offenbar sind sich viele Menschen der Risiken, die im Smarthome entstehen können, gar nicht bewusst: Dass beispielsweise ein Saugroboter oder ein Smartspeaker mit Schadsoftware infiziert werden kann, wissen nur 42 Prozent der Befragten, also noch nicht einmal die Hälfte. Nur etwa ein Drittel hat davon gehört, dass Unbefugte sensible Daten abfangen und diese Informationen auch missbrauchen können.

Ute Lange: Wir haben es gehört, viele machen sich über die Sicherheitsaspekte nicht so umfassende Gedanken. Wie schätzt ihr das im BSI für Smarthome-Geräte ein? Wie real ist das Problem, dass die Menschen angegriffen werden, oder, wie Joachim gerade gesagt hat, sie weitere, nämlich digitale Türen in ihr Zuhause aufmachen?

Karin Wilhelm: Die Wahrheit ist, wir haben die digitalen Türen schon auf. Wir haben die Geräte in unser Leben gelassen, ohne sie genau zu kennen. Ich habe hier drei Beispiele. Fangen wir mit etwas ganz Einfachem an. Eine Fernbedienung, die hat jeder zu Hause.

Ute Lange: Nicht nur eine.

Karin Wilhelm: In der Regel nicht nur eine. Das war lange Zeit sehr komplex. Viele können mit ihrer Fernbedienung in die Mediathek gehen und einen Streamingdienst anwählen. Da sage ich: "Vorsicht, das ist Internet". Das heißt, es ist ein internetfähiges Gerät. Was wir in Fernbedienungen manchmal finden, ist ein Mikrofon. Warum ist das da? Vielleicht soll es eine Sprachsteuerung ermöglichen. Mikrofon bedeutet: Inhalte, die ich in meinem Wohnzimmer sage, in meinem Schutzraum, können aufgenommen werden. Da sollte ich mich schlaumachen. Aber es gibt noch andere Beispiele. Der Staubsaugroboter zum Beispiel kartiert meine Wohnung. Das liegt vielleicht in der Cloud. Das sind sehr sensible Daten von mir. Eines finde ich noch superspannend. Eine Glühbirne kann ein smartes Gerät sein, wenn ich sie vielleicht mit dem Handy steuere. Das gibt es tatsächlich nachweislich, dass Glühbirnen mein WLAN-Passwort speichern, und das tun die vielleicht ungesichert. Wenn eine Glühbirne, also ein Gerät, von dem ich manchmal gar nicht wahrnehme, dass es da ist, tatsächlich mein WLAN-Passwort ungesichert speichert, dann kann das theoretisch jeder sehen. Das ist keine schöne Sache. Darum sagen wir immer, Gäste-WLAN ist für smarte Geräte eine gute Idee.

Joachim Schneider: Vielleicht darf ich da anknüpfen. Aus polizeilicher und kriminologischer Sicht sind es natürlich genau diese persönlichen Daten, die es auch zu schützen gilt. Das sind Bewegungsmuster und Anwesenheitsinformationen. Das mögen zum einen Gewohnheiten sein, die man aus Marketingsicht in irgendeiner Form lohnend auswerten könnte. Aber das wäre natürlich auch für perfide Kriminelle eine willkommene Einladung, hier zu generieren, wann die Leute wo sind und wer im Haus ist, wenn es ihnen gelingt, diese persönlichen Daten, diese Zugänge, diese digitalen Türen zu nutzen – sprich die Zugänge zu hacken, wenn sie nicht geschützt sind, wie du gerade gesagt hast.

Michael Münz: Wir haben viel über die Risiken gesprochen, aber vielleicht bringen diese neuen technologischen Entwicklungen auch Chancen mit. Meistens ist die Technologie gar nicht schlecht, sondern die Leute, die sie bedienen oder falsch nutzen oder richtig nutzen, aus Sicht der Cyberkriminellen natürlich. Wie ist es denn perspektivisch? Kann uns Smarthome vielleicht auch schützen? Du hast gerade schon von den digitalen Türen gesprochen. Kann Smarthome auch Türen schließen, dass ich mir, wenn ich abwesend bin, keine Gedanken machen muss?

Joachim Schneider: Uns als Polizei kommt immer die Rolle des Mahners zu. Wir laufen immer ein Stück Gefahr, dass es bei Themen wie künstlicher Intelligenz oder jetzt auch im Smarthome-Bereich in die Richtung geht, dass es dämonisiert wird. Das möchten wir gar nicht. Das möchte ich klipp und klar sagen. Solche Geräte haben auch viele, viele Vorteile für Menschen mit Einschränkungen zum Beispiel. Wir möchten das nicht dämonisieren, sondern ganz im Gegenteil. Wir wollen auf Risiken hinweisen. Wenn man den Kontext Smarthome-Geräte und Einbruchschutz herstellt, muss ich klar sagen: Für sich allein kann Smarthome keinen wirksamen Einbruchschutz gewährleisten. Wir haben im Jahr ungefähr knapp 80.000 Wohnungseinbrüche in Deutschland und darüber hinaus nochmal 90.000 Einbrüche in Keller, Dach oder Waschküchen. Wenn gute Sicherungstechnik in Form einer mechanischen Sicherung verbaut ist, dann bleiben ungefähr knapp die Hälfte der Einbrüche im Versuchsstadium hängen. Das spricht klar eine deutliche Sprache. Wenn ich sage mechanische Sicherung, dann meint das natürlich eine entsprechende Bauweise von Türen und Fenstern, entsprechende Verriegelungen, sichere Schlösser oder Verglasung, die das Einsteigen verhindern. Das sind die Zeichen der Zeit. Dennoch kann Smarthome eine gute Ergänzung sein. Wir alle geben den Tipp: Wenn Sie im Urlaub oder abwesend sind, lassen

Sie bitte nicht den Eindruck erwecken, das Haus ist derzeit unbewohnt. Smarthome ist natürlich genial. Rollladen hoch oder herunter, wenn der elektrifiziert ist. Die Lichtsteuerung ist machbar. Man kann auch so ein Stück weit mit Smarthome sehr gut und sehr leicht Anwesenheit simulieren in Zeiten von Abwesenheit, was natürlich dann potenzielle Einbrecherinnen und Einbrecher abhalten wird. Man sollte sich vielleicht überlegen, was man denn braucht. Ob ich aus der Ferne meine Haustür auf- und zumachen können muss, das halte ich für ein hohes Risiko und würde sehr stark abwägen, ob ich diese Anwendung tatsächlich in mein Haus einbaue. Man sollte am Anfang wirklich prüfen, ob es das wirklich braucht.

Ute Lange: Das leitet sehr schön dazu über, was wir hier auf der IFA auch gemacht haben. Wir haben uns nämlich mit Besuchern und Besucherinnen unterhalten und haben gefragt, wie sie sich das digitale Zuhause in der Zukunft vorstellen, und wir hören jetzt einmal einige der Antworten.

Umfrage:

Person 1: Wir lassen uns durch KI zu viel aus der Hand nehmen durch genau diese Smarthome-Technik.

Person 2: Wenn sich die ganzen Hausarbeiten von selbst erledigen würden. Das wäre ein Traum.

Person 3: Was ich da noch spannend finde, sind die Smart-Health-Systeme mit Überwachung der Körperfunktionen und wie ich sicherstelle, dass ich gesund bleibe.

Person 4: Wenn die zu intelligent werden, hätte ich doch ein bisschen Angst davor.

Person 5: Bei den Komponenten, die man kauft, weiß man gar nicht, was drinsteckt, wo die Daten abfließen und ob da möglicherweise auch irgendwelche Schadsoftware ihr Unwesen treibt.

Person 6: Sicherheitsaspekte? Ich würde hoffen, dass man dann darauf achtet, dass keine Daten dazu gespeichert werden, wann ich nach Hause komme oder wann bei mir der Fernseher und die Musik angehen.

Michael Münz: Wir haben gerade zum Schluss gehört, Karin, dass einige Leute den Eindruck haben, sie verlieren ein bisschen den Überblick. Ich hole mir ein Gerät herein, muss mir die Bedienungsanleitung anschauen und es in mein Netz integrieren. Dann hole ich mir das nächste. Irgendwann habe ich vielleicht auch keine Lust mehr, jedes Mal das Passwort zu ändern oder mir anzuschauen, ob ich wirklich alle Sicherheitseinstellungen in dem achten Menü auf Seite zwei habe. Wie ist es für euch als BSI, wenn ihr dann merkt, die Leute haben ein bisschen den Überblick verloren oder drohen, ihn zu verlieren? Was empfehlt ihr denn den Nutzerinnen und Nutzern, die vor dieser Aufgabe stehen, neue Smarthome-Geräte in einen bislang geschützten Bereich zu integrieren?

Karin Wilhelm: Das ist eine riesig schwere Aufgabe. Das kann ich gut nachvollziehen. Wenn wir über die IFA gehen, gibt es so viele Geräte hier. Das ist Wahnsinn. Dann bekommt man richtig Lust. Eins könnte auch in mein Leben passen und ich nehme das mit nach Hause. Das soll ich jetzt da irgendwie einfügen. Das funktioniert nicht. Ich weiß gar nicht, ob

ich dafür ein eigenes Netz brauche. Ich komme an meine Grenzen. Ich will nur, dass es läuft. Dafür habe ich totales Verständnis. Was können wir als BSI leisten? Erstmal eine erste Orientierung. Das sieht man hier auch sehr schön am Stand. Wir haben ein Kennzeichen, nämlich das IT-Sicherheitskennzeichen. Das werden die Hörerinnen und Hörer eurer Podcast-Reihe natürlich auch kennen. Aber das ist schon einmal etwas. Wenn das auf Produkten draufsteht, dann heißt das, den Sicherheitsanforderungen des BSI hat der Hersteller hier Genüge getan. Die bleiben auch in Kontakt mit uns und das ist schon einmal prima. Das reicht aber leider insofern nicht, als es auch darum ging, alles zu vernetzen. Es ging auch darum, alles in mein Sicherheitskonzept zu integrieren. Ich finde, da fängt es an. Das ist eine Frage der Haltung. Es ist eine Frage davon, zu fragen, ob ich wirklich alles brauche. Du hast gesagt es, Joachim. Brauche ich wirklich alles? Das ist tatsächlich die erste Frage. Brauche ich alles? Brauche ich jede Funktion? Brauche ich Mikrofone in meiner Fernbedienung? Das sind Fragen, die sich Verbraucherinnen und Verbraucher stellen und auch selbst entscheiden müssen und vielleicht kommen sie zu einem "Ja". Das darf man als Antwort haben, aber das muss ich immer mitdenken, und da kommt die Schwierigkeit auf. Das ist sicher.

Michael Münz: Der Podcast ist auch ein Angebot an Nutzerinnen und Nutzer, sich nochmal ein bisschen weiter mit dem Thema Cybersicherheit und auch der Absicherung des Hauses Gedanken zu machen. Welche Angebote habt ihr denn noch, die über den Podcast hinausgehen? Gibt es etwas auf eurer Webseite?

Karin Wilhelm: Natürlich. Ich lade jeden immer gerne ein, einmal zu uns auf die Webseite zu kommen. Wir haben einen ausgebauten Bereich zum Thema Smarthome. Wir haben auch Broschüren zum Internet der Dinge, wer es lieber in Print mag. Ich habe vielleicht noch einen konkreten Tipp und habe auch nochmal Zahlen mitgebracht. Bei den Kaufentscheidungen ist den Menschen IT-Sicherheit sehr wichtig. Da haben wir eine Zahl von über 76 Prozent. Das ist schon mächtig viel. Aber im Cybersicherheitsmonitor haben wir Unterkategorien abgefragt. Ist ihnen das Preis-Leistungs-Verhältnis wichtig? Ist ihnen vielleicht eine Update-Verpflichtung wichtig? Da sehen wir klar, dass die Menschen sagen, Hauptsache, es läuft und Hauptsache, der Preis und die Leistung stimmt. Das kann ich nachvollziehen. Aber ich mache Werbung dafür, sich gerade beim Kauf über solche Dinge Gedanken zu machen und sich Fragen zu stellen, damit man später seine Ruhe hat. Sonst kauft man sich Dinge, es ist vielleicht zu komplex und man baut die unsicher ein. Dann laufen die sehr, sehr lange Zeit mit und sind sehr betreuungsintensiv. Darum würde ich sagen, wenn man sich auf unseren Seiten informiert, sollte man gerne einmal diesen Fokus auf den Kauf setzen und sich da schon die richtigen Fragen stellen, damit man später Ruhe hat.

Ute Lange: Vielen Dank dafür. Das leitet über zu dir, Joachim, und zwar zu der Frage, was passiert, wenn das Kind denn nun einmal in den Brunnen gefallen sein sollte. Wer uns folgt, hat hoffentlich genügend Vorkehrungsmaßnahmen getroffen. Aber nun stelle ich fest, dass eines meiner Smarthome-Geräte von Unbefugten gehackt wurde. Da hat sich jemand mit meinen Daten auf den Weg gemacht und andere Sachen getrieben. Lohnt sich das denn, wenn ich euch das melde, und bei der Polizei Anzeige erstatte? Das ist nochmal ein weiterer Schritt, den ich machen muss, und unter Umständen ist mir das auch peinlich, wenn ich zugeben muss, dass ich die guten Tipps von Karin und ihren Teams gar nicht erst berücksichtigt habe.

Joachim Schneider: Was du jetzt schilderst, ist leider auch Realität. Deswegen bin ich mehr als dankbar, dass wir neben den PKS, den Zahlen der polizeilichen Kriminalitätsstatistik, gemeinsam mit dem BSI in unserem Cybersicherheitsmonitor die Möglichkeit haben, auch in das Dunkelfeld zu schauen, also was die Leute wirklich erlebt haben. Wenn ich dort schon sehe, jeder Vierte ist in den letzten zwölf Monaten Opfer einer Cyberattacke, eines Cybereingriffs oder einer Straftat geworden, dann macht das den Umfang schon deutlich. Ich appelliere an die Leute: Meldet das an uns, nehmt uns mit! Zum einen sind wir natürlich bemüht, hier schon im Vorfeld mit Präventionsmaßnahmen aktiv zu werden. Aber wir sind natürlich auch dankbar dafür, wenn wir diese perfiden Kriminellen erwischen. Das muss man auch einmal klar sagen. Das ist schon ein Ziel. Aber mit jeder Anzeige, mit jedem Modus Operandi, der uns gewahr wird, oder vielleicht auch mit neuen Entwicklungswellen, macht man auch ein bisschen Opferschutz. Das ist Kriminalprävention. Das heißt, wenn wir merken, da kommt ein neues Phänomen nach oben, dann haben wir natürlich die Möglichkeit, sehr schnell potenzielle Opfer zu warnen und damit natürlich die Opferwerdung zu verhindern. Das ist Kriminalprävention at its best.

Michael Münz: Das heißt, auch wenn es nur um 50 Euro geht oder andere Themen. Alles, was wir euch als Polizei mitteilen, hilft euch dann auch, die Prävention auszubauen?

Joachim Schneider: Genau. Zum einen sind das Straftatbestände. Wir reden hier nicht über Falschparken oder einen abgelaufenen Parkschein. Wir reden da tatsächlich schon über Straftatbestände, wenn es in diesen Intimbereich geht. Vorhin hatten wir es: Der Wohnungseinbruch ist ein Verbrechenstatbestand – nicht unter einem Jahr Gefängnis.

Michael Münz: Karin und Joachim, vielen Dank, dass ihr da wart. Da waren sehr, sehr viele Punkte dabei, die ihr uns und unseren Hörerinnen und Hörern hier von der IFA mitgegeben habt. Ich nehme auf jeden Fall mit, dass Geräte für Smarthome immer auch eine Tür sind und im Zweifelsfall Türen öffnen. Da sollten wir am besten selbst steuern, wann das der Fall ist und wann das nicht der Fall ist. Das Zusammenspiel von tatsächlich baulichen Maßnahmen, also Fenster, Türen, Schlösser und so weiter, und digitalen Maßnahmen können zusammen einen Schutz ergeben.

Ute Lange: Das nehme ich auch mit. Ich habe aber noch zwischen den Zeilen ein paar andere Sachen gehört, und das führt zu unserer Platte mit dem Sprung, die wir manchmal auflegen. Was für digitale Geräte generell gilt, scheint auch für Smarthome-Geräte zu gelten. Das heißt, ein gutes Passwort einstellen und Updates ziehen. Ich sehe dich nicken, Karin. Was hast du vielleicht noch für praktische Tipps im Schnelldurchlauf kurz vor Schluss?

Karin Wilhelm: Zwei-Faktor-Authentisierung gibt es oder auch die Dinge einmal offline nehmen. Das sind viele Möglichkeiten, die man nutzen sollte und über die man sich erstmal im Klaren sein muss. Was habe ich für Möglichkeiten? Ich sage immer: Updates, Updates, Updates – auch da müssen Sicherheitslücken unbedingt geschlossen werden.

Ute Lange: Wenn ihr da draußen jetzt Lust habt auf mehr Tipps, gibt es die alle schwarz auf weiß in dem schon genannten Cybersicherheitsmonitor und natürlich auf den BSI-Seiten. Wir verlinken euch einiges davon in den Shownotes. Es gibt Broschüren und Tipps für den Alltag. Schaut da rein, es lohnt sich.

Michael Münz: Bevor wir Karin und Joachim von unserem Talk hier entlassen, würde ich gerne von euch beiden noch einmal etwas wissen. Du hast es vorhin einmal erwähnt. Ich

stehe dann auf der IFA und da ist ein Gerät, das ich mitnehmen möchte. Hast du hier auf der IFA eines gesehen, wo du als Nächstes hinläufst, um einmal zu schauen, ob du das nach Hause transportieren kannst?

Karin Wilhelm: Ich wollte schon mit der Frage konfrontiert, was ich von der Karaoke-Maschine halte. Die werde ich mir nochmal genauer anschauen.

Michael Münz: Joachim, ist bei dir irgendwas dabei?

Joachim Schneider: Nein. Der Überblick ist Wahnsinn. Die Innovation ist hier enorm, aber ich habe persönlich für mich noch nichts gefunden, für das ich unbedingt einen Bedarf habe.

Michael Münz: Danke dir. Trotzdem noch viel Spaß beim Herumschauen. Euch auch vielen Dank fürs Zuhören. Wenn euch diese Folge gefallen hat, dann folgt uns gerne auf eurer Podcast-Plattform, denn dann verpasst ihr nicht die nächste Ausgabe von "Update verfügbar". Zu Gast ist die Leiterin einer Hackerschool und auch einer ihrer Schülerinnen. In meinem Gedankenbild haben wir das nächste Mal einen Jedi-Ritter und einen Padawan dabei. Mit beiden sprechen wir über die Rolle von IT-Kompetenzen in der digitalen Gesellschaft und wie frühzeitige Bildung dazu beitragen kann, die Cybersicherheit zu verbessern. Wir sind auf jeden Fall schon einmal sehr gespannt.

Karin Wilhelm: Frag bitte nach, ob die einen Hoodie trägt.

Michael Münz: Auf jeden Fall. Das machen wir.

Ute Lange: Wenn ihr da draußen Fragen habt, die wir mit den beiden in der nächsten Folge klären sollten, oder ihr Feedback geben möchtet zu dieser oder auch anderen Folgen, dann schreibt uns doch über die BSI-Kanäle. Die gibt es auf Facebook, Instagram, X, ehemals Twitter, Mastodon und YouTube. Es gibt auch traditionell eine E-Mail-Adresse. Die lautet: podcast@bsi.de. Wir freuen uns immer, von euch zu hören.

Michael Münz: Wir freuen uns auf die nächste Folge mit euch und für euch. Passt bis dahin gut auf eure Daten auf. Bis dann. Tschüss.