„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 26, 30.11.2022:

Smart Toys – wenn der Teddy gefährlich wird

Moderation: Ute Lange, Michael Münz
Gast: Martin Gobbin, Stiftung Warentest
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

***Münz**:* Mein Name ist Michael Münz. In dieser Folge geht es um Sicherheit in deutschen Kinderzimmern. Wir sprechen über Smart Toys. Smart Toys sind Spielzeuge, die Daten sammeln, sich vernetzen und Daten hin und her senden. Wenn ihr überlegt, Smart Toys zu Weihnachten zu verschenken, ist diese Folge und Tipps unseres heutigen Gastes was für euch. Wir sprechen unter anderem auch über Spielzeuge, die bei Erwachsenen zum Einsatz kommen. Bleibt dran, um über Datensicherheit in deutschen Schlafzimmern zu erfahren, aber spult nicht vor!

Lange: Sonst würdet ihr weitere Nachrichten und Tipps von uns verpassen. Wir haben einen kleinen Rückblick auf die vergangenen Wochen vorbereitet. Es sind verschiedene Berichte und Studien erschienen, die sich mit Sicherheit in unserem digitalen Alltag beschäftigt haben. Ich finde, dass deren Überschriften wie die zwei Seiten einer Medaille klingen.

***Münz**:* Das ist mir auch aufgefallen. Die eine Seite ist: immer mehr Menschen bewegen sich wie selbstverständlich im Internet. Die Onlinestudie von ARD und ZDF hat herausgefunden, dass 95 Prozent der deutschsprachigen Bevölkerung ab 14 Jahren das Internet nutzt, 80 Prozent davon täglich. Wir sind alle rund um die Uhr online unterwegs. Damit kommen wir zur anderen Seite der Medaille: das Internet ist kein Ponyhof.

Lange: Leider überhaupt nicht. Das BSI hat zwei aktuelle Studien veröffentlicht und deren Überschriften lauten „Die Gefährdungslage im Cyber-Raum ist so hoch wie nie“ und „Weiter leichtes Spiel für Cyber-Kriminelle“. Im ersten Bericht, dem BSI-Lagebericht, werden Schwachstellen in Soft- und Hardware-Produkten thematisiert. Demnach wurden im Jahr 2021 mehr als 20.000 Schwachstellen in Softwareprodukten registriert. Das entspricht einem Zuwachs von zehn Prozent gegenüber dem Vorjahr. Das ich eine ganze Menge.

***Münz**:* Warum sollten wir das wissen? Warum sollte das uns zu denken geben?

Lange: Wir haben öfter darüber gesprochen, dass jede Schwachstelle in Soft- und Hardware-Produkten ein potenzielles Einfallstor für Angreifer und Angreiferinnen ist und die

Informationssicherheit in Verwaltung, Wirtschaft und Gesellschaft gefährdet. Beispielsweise durch Ransomware-Angriffe auf Unternehmen, Universitäten, Behörden, Krankenhäuser und andere lebenswichtige Einrichtungen, die sich zum Ziel setzen, Lösegeld zu erpressen. Diese Angriffe gelten als aktuell größte Bedrohung im Cyberbereich.

***Münz**:* Das Digitalbarometer des BSI macht unter anderem deutlich, wie oft wir Opfer von Cyberangriffen werden. Jede beziehungsweise jeder Vierte ist demnach bereits einmal Opfer von Cyberkriminalität geworden. Ich gehöre auch dazu. Wir erinnern uns, dass Michael Meier vor zwei Folgen darauf hingewiesen hat, dass Daten von mir im Netz zu finden sind. Ich bin zum Glück noch nicht finanziell zu Schaden gekommen, wie leider viele andere. Den größten finanziellen Schaden verursachten laut der Studie Betrugsmaschen, wodurch Betroffene durchschnittlich 674 Euro verloren haben.

Lange: Bei diesen Studien musste ich an die Anfänge des Internets denken. Früher waren diejenige, die online waren, die Minderheit. Um uns zu verlocken, wurde eine Werbung mit Boris Becker gedreht. Ich weiß nicht, ob du dich an die erinnerst. Er saß vor einem Rechner, hat sich per Modem eingewählt und am Ende gefragt „Bin ich jetzt drin?“. Als er die Bestätigung bekommen hat, hat er sich gefreut. Es war sehr einfach. Heute ist es offensichtlich für die Cyberkriminellen genauso einfach, bei uns reinzukommen. Wir sind alle im Netz, was viel mehr Angriffsmöglichkeiten bietet. Das ist für mich die Klammer zwischen diesen Studien.

***Münz**:* Ich kann mich sehr gut an die Werbung erinnern. Ich kann mir auch gut vorstellen, dass es für Hackerinnen und Hacker immer noch leicht ist, sich Zugang zu unseren Daten zu verschaffen. Weißt du, was mich beim BSI-Bericht besonders betroffen gemacht hat?

Lange: Was?

***Münz**:* Dass wir immer noch offenbar nicht genug tun, um uns vor Cyberangriffen zu schützen. So nutzt beispielsweise nur knapp ein Drittel von Befragten die Möglichkeit, Updates automatisch zu installieren. Ich gehe allerdings davon aus, dass die Quote bei Hörerinnen und Hörern von dem Podcast, der Update Verfügbar heißt, viel höher ist. Bitte!

Lange: Bitte! Das Thema Updates wurde in unserem Podcast bereits so häufig angesprochen, dass ich sicher bin, dass die Quote bei unseren Hörerinnen und Hörern höher ist. Um meine These zu überprüfen, könnt ihr uns schreiben, welche Tipps ihr für euren digitalen Alltag beherzigt habt, was für euch besonders wichtig war und was ihr an diejenige weitergibt, die den Podcast nicht hören, aber von eurem neuen Wissen profitieren können. Heute kommen weitere Tipps dazu!

***Münz**:* Wir haben Martin Gobbin von der Stiftung Warentest zu Gast. Mit ihm sprechen wir über Smart Toys, die Spielzeuge, die Daten sammeln und sich womöglich zum Austausch von Daten vernetzen. Smart Toys gibt es in Kinderzimmern, aber nicht nur dort. Hallo Martin! Schön, dass du da bist.

Gobbin: Hallo! Ich freue mich, hier zu sein!

Lange: Herzlich willkommen! Danke, dass du dir Zeit für uns nimmst. Magst du dich kurz vorstellen? Was machst du bei der Stiftung Warentest und wie bist du dorthin gekommen?

Gobbin: Ich bin Technikredakteur und beschäftige mich mit allen möglichen technischen Themen, Geräten und speziell mit der Sicherheit. Das heißt, mit Datensicherheit sowie mit Datenschutz vor Trackern und Angriffen.

Münz: Wie für jeden Gast haben wir für dich eine Entweder-Oder-Frage. Ich bin sehr gespannt, wie es bei dir ausgeht. Worauf würdest du lieber verzichten? Ein Jahr Internet oder ein Jahr Kino?

Gobbin: Das ist sehr schwierig, weil ich großer Kinofan bin und beruflich Filmkritiken schreibe. Allerdings liefert das Internet Filme nach Hause. Deswegen würde ich eindeutig lieber auf Kino verzichten, weil ich die Filme auch zuhause streamen kann.

Münz: Sehr pragmatischer Ansatz.

Lange: Hoffentlich streamst du mit allen notwendigen Sicherheitseinrichtungen. Lass uns auf das heutige Thema kommen. Was genau ist unter dem Begriff intelligentes Spielzeug zu verstehen?

Gobbin: Intelligent oder smart steht immer für vernetzt beziehungsweise internetfähig. Das heißt, dass das internetfähige Spielzeug mit dem Web verbunden werden kann, damit es zum Beispiel Fragen von Kindern flexibel beantwortet. Es gibt auch Spielzeug, das sprechen kann, aber nicht internetfähig ist. Bei einem solchen Spielzeug sind bestimmte Sätze vorinstalliert. Mehr kann das Toy allerdings nicht im Vergleich zu einem internetfähigen Toy, das Weltwissen wie aus dem Browser oder Wikipedia aus dem Internet ziehen kann. Es gilt wegen seiner Flexibilität als smart beziehungsweise schlau.

Münz: Wir haben im Podcast immer wieder gehört, dass ein Gerät, sobald es sich Daten aus dem Internet ziehen kann, diese Daten dort wieder hinschicken kann. Dabei ist es nicht immer klar, welche Daten hin und her wandern. Gilt dieses Risiko nicht nur für Kaffeemaschinen, Staubsauger oder andere Haushaltsgeräte, sondern auch für Spielzeug? Ist das etwas, auf das man achten sollte?

Gobbin: Ja. Jedes Gerät, das im Internet ist, kann gehackt werden. Die Frage ist, wie schwierig es ist und welche Daten ausgetauscht werden. Smart Toys sind dazu da, um mit dem Kind zu sprechen beziehungsweise dazu, dass das Kind mit dem Toy sprechen kann. Das heißt, es gehen Sprachaufzeichnungen rüber. Oft kann man sich ein Account anlegen, das Informationen wie Klarname des Kindes, sein Geburtsdatum und eventuell sein Foto enthält. Es wird außerdem die IP-Adresse gespeichert, die oft den ungefähren Standort verrät. Diese Informationen werden mitgeteilt und liegen beim Anbieter, was nicht unbedingt ein Problem ist, solange der Anbieter sie nicht missbraucht. Diese Informationen liegen teilweise auch bei den Eltern, die alles abhören können, was das Kind zu dem Toy gesagt hat. Es stellt sich dabei die Frage, ob das Kind nicht auch gegenüber den Eltern ein Recht auf Privatsphäre hat. Das allergrößte Problem sind aber Hackerinnen und Hacker. Wenn die beim Anbieter

gespeicherten Daten schlecht gesichert sind, können sie abgegriffen werden. Das heißt, dass Angreifende Sprachaufzeichnungen, Fotos, Namen sowie Adressen der Eltern und des Kindes stehlen können.

***Münz**:* Das klingt in der Theorie recht bedrohlich. Hast du vielleicht ein paar Beispiele, die deutlicher machen können, welche Auswirkungen eine schlecht gehütete Datensammlung haben kann oder Beispiele davon, wenn es nicht klar ist, was mit den Daten passiert.

Gobbin: Im Smart Toy-Bereich gab es bereits verschiedene Hacks. Als die smarte Barbie, die sogenannte Hello Barbie von dem Spielzeughersteller Mattel auf den Markt kam, haben diverse Sicherheitsforscherinnen und -forscher sofort gezeigt, wie man die Sprachaufzeichnung entwenden kann. Es kann sehr problematisch sein, weil das Kind die Barbie mag und dem Toy intime Sachen anvertraut. Bei den Anbietern VTech und CloudPets wurden über zehn Millionen Konten von Eltern und Kindern gestohlen, die unter anderem Informationen über reale physische Adressen, Namen der Kinder, Geburtstagsdaten sowie Fotos enthielten. Alle diese Daten waren sehr leicht zu rauben, weil die völlig ungesichert im Internet auf dem Amazonserver lagen und nicht mit einem Passwort geschützt waren. Neben den Hacks gibt es noch andere Gefahren. Wir hatten vor ein paar Jahren Smart Toys im Test, eins von denen war ein Roboter, mit dem man sowohl das Kind abhören als auch direkt mit dem Kind sprechen konnte. Es hat wie eine Freisprechanlage funktioniert. Man konnte auch Text in der App eingeben, sodass der Roboter den in seiner Stimme vorliest. Wenn ich der Hacker oder die Hackerin bin und direkt mit dem Kind spreche, könnte es sein, dass das Kind Angst hat oder die Eltern das hören. Es wäre für mich als Angreifer oder Angreiferin gefährlich. Viel bequemer ist es, Text in die App einzugeben, sodass der Roboter den Text mit seiner Stimme vorliest, dem das Kind vertraut. Das ist sehr gefährlich, weil ich entweder das Kind zu mir einladen, es bedrohen oder ausfragen könnte. Für dieses Ausforschen und Kommunizieren mit dem Kind war keinerlei Hack nötig, da der Roboter mit Bluetooth verbunden werden konnte. Ich brauchte weder eine PIN eingeben noch den physischen Zugriff auf das Toy haben. Ich musste nur in der Nähe sein und ein bluetoothfähiges Handy haben. Das heißt, ich brauchte weder Spezialhardware noch Hacker-Skills. Jeder und jede, der oder die ein bluetoothfähiges Handy hat und in der Nähe des Toys ist, kann sich damit verbinden und das Kind damit abhören, ihm drohen oder es einladen.

Lange: Martin, wir haben öfter darüber gesprochen, dass es zwei bis drei Aspekte bei Datensicherheit gibt. Ich höre jetzt raus, dass viele von diesen Spielzeugen nicht die nötigen Sicherheitsmaßstäbe oder -möglichkeiten hatten. Es besteht für mich aber als Elternteil oder als Kind die Möglichkeit, selbst etwas zu machen, wenn ich mir ein Spielzeug zulege. Können wir das voneinander ausdifferenzieren? Worauf sollte ich als jemand, der ein Spielzeug zu Weihnachten verschenken möchte, bei der Datensicherheit achten?

Gobbin: Ich fange mit dem ersten Teil der Frage an, und zwar was ich als Elternteil machen kann, wenn ich überlege, meinem Kind ein Smart Toy zu schenken. Zunächst sollte man googeln. Es ist schon bekannt, dass es zu diesem und jenem Toy, das man für das Kind ausgesucht habe, bereits Sicherheitsvorfälle bekannt sind. Also zuerst einfach recherchieren,

was bereits vorgefallen ist. Außerdem gibt es ein paar Merkmale, auf die man achten kann. Einige Toys haben zum Beispiel keine ständige Internetverbindung. Die holen sich ab und zu ein Software-Update aber sind nicht ständig mit dem Internet verbunden. Das ist ein Vorteil, weil die Datenverarbeitung dann lokal stattfindet. Das heißt, es wird nicht alles, was das Kind zum Toy sagt, sofort ins Internet übertragen. Noch kann man schauen, ob das Toy ein Mikrofon und eine Kamera hat. Wenn beides fehlt, ist es ein Vorteil, weil das Kind nicht aufgezeichnet werden kann, weder was es sagt, noch wie es aussieht oder was es tut. Wenn Mikrofon und Kamera vorhanden sind, kann man sich anschauen, wie sie aktiviert werden, und zwar ob sie daueraktiv sind oder ob man die manuell aktivieren muss. Das wäre ein Vorteil, weil man dann zumindest nicht unbemerkt beobachtet werden kann. Wenn ich ein Smart Toy kaufe, bietet es sich an, dass ich es selbst austeste und weiß, wie es funktioniert, bevor ich das dem Kind schenke. Wichtig wäre es, das Toy nach der Nutzung auszuschalten. Sonst ist es möglicherweise im Standby-Betrieb und kann immer noch Daten sammeln. Sehr wichtig sind starke Passwörter. Ihr habt dies in eurem Podcast bereits öfter thematisiert. Normalerweise habe ich ein Nutzeraccount bei dem Anbieter, das ich einrichte. Wenn ich ein schwaches Passwort verwende, sind die Daten sehr leicht zu stehlen. Aus diesem Grund sollte man das nicht unterschätzen und ein starkes Passwort verwenden. Stark heißt möglichst lang und komplex. Es soll kein existierendes Wort sein. Für verschiedene Dienste muss man ein eigenes Passwort verwenden, das heißt nicht dasselbe, das bereits für den E-Mail-Account oder Amazon verwendet wird. Wenn so ein Passwort gestohlen werden sollte, wären viele Accounts betroffen. Deswegen braucht jedes Account ein eigenes starkes Passwort.

***Münz**:* Viele der Punkte, die du genannt hast, wiederholen wir immer wieder in unseren Folgen, beispielsweise Themen wie Passwort und Updates. Es hat mich betroffen gemacht, dass ich mich als Verbraucher oder Verbraucherin nicht darauf verlassen kann, dass ein Toy, das ich bekomme, zumindest einen standardisierten Sicherheitsaspekt hat. Ich muss mir das Gerät, das ich gekauft habe oder verschenken will, sowie seine Einstellungen noch einmal genauer anschauen. Es gibt also offensichtlich keine Regulierung beziehungsweise Gesetzgebung, die bestimmte Gefährdungen von vornherein ausschließt.

Gobbin: Da kommen mehrere Probleme zusammen. Diese Toys werden oft von Firmen produziert, die vielleicht sehr gut darin sind, einen Roboter oder einen Teddy zu bauen, aber bisher in ihrem ganzen Firmenleben mit IT-Sicherheit nichts zu tun hatten. Das ist ein Problem. Es kommt hinzu, dass sie Marktdruck haben und ihre Waren schnell auf den Markt ohne ausführliche IT-Sicherheitsüberprüfung wie zum Beispiel einen kostspieligen Penetrationstest bringen wollen. Die Ware soll günstig verfügbar sein. Was Regulierung betrifft, gelten natürlich bestimmte Gesetze, unter anderem die Datenschutzgrundverordnung und andere Datenschutzgesetze. Das Problem dabei ist, dass es sich um die Zuständigkeiten gerangelt wird. Wer ist für Smart Toys zuständig? Ist es die Bundesnetzagentur, die vor ein paar Jahren Puppe Cayla verboten hat? Ist es das BSI? Sind es die Landesdatenschutzbehörden? Wer ist dafür zuständig? Außerdem besteht folgendes Problem: es gelten zwar Datenschutzgesetze, aber es gibt meines Wissens keine technischen Mindestanforderungen, die sehr sinnvoll wären. Ich hatte erklärt, dass das Hauptproblem

einiger Toys die ungesicherte Bluetooth-Verbindung war. Beim Erstverbinden war weder eine PIN noch physischer Zugriff nötig. Dieses einfache Mittel würde bei solchen Fällen reichen. Es müssten also gesetzliche Mindestanforderung geschaffen werden. Wenn man solche Bluetooth-Toys baut, sollte man zumindest voraussetzen, dass eine PIN bei der Ersteinrichtung nötig ist.

Lange: Wenn ich über meine elektrischen und teilweise mit dem Netz verbundenen Geräte zuhause nachdenke, gibt es bei manchen doch Regeln. Ich glaube, man kann keine Kaffeemaschine oder keinen Fön auf den Markt bringen, die nicht nach bestimmten Standards sicher sind. Wie sieht das bei intelligenten Spielzeugen aus? Gibt es entweder bei HerstellerInnen und Hersteller oder bei denjenigen, die für Regulierung zuständig sind, die Erkenntnis, dass es darauf kritischer geachtet werden soll? Was hat sich getan, seitdem ihr eure Tests gemacht habt und Schwachstellen entdeckt habt?

Gobbin: Ich weiß leider nicht, wie es bei den Anbietern aussieht. Dazu müsste man mit denen sprechen. Ich glaube, dass es im politischen Sinne immer noch zu wenig Bewusstsein gibt. Du hast erwähnt, es gibt sehr viel Regulierung, wenn man beispielsweise irgendein Gerät auf den Markt bringt, wobei elektrische Sicherheit geprüft wird. Wenn ein neues Shampoo oder eine Zahnpasta auf den Markt kommt, gibt es auch alle möglichen Testverfahren. Das Internet ist allerdings im politischen Sinne oft noch Neuland und wird zu wenig beachtet. Deswegen wird etwas eher schnell verboten, wie beispielsweise Puppe Cayla, aber es wird sich aus meiner Sicht noch zu wenig darum gekümmert, die Mindestanforderungen zu schaffen. Es wäre eine relativ leichte Option, die Geräte zumindest etwas sicherer zu machen, indem man als Standard setzt, dass die Bluetooth-Verbindung geschützt sein muss.

Münz*:* Wir haben bereits angekündigt, dass das, was für Kinderspielzeuge gilt, auf Spielzeuge für Erwachsene in Schlafzimmern übertragbar ist. Immer mehr Sextoys haben Netzanbindung. Kann man das, was wir über Kinderspielzeuge gesagt haben, auf das übertragen, was Erwachsene sich untereinander schenken? Gibt es da auch die Gefahr?

Gobbin: Da gibt es genau die gleichen Gefahren. Der Unterschied liegt nur daran, dass es um andere Daten geht. Es gab schon die schlimmsten Fälle. Es gab in letzter Zeit ein Keuschheitsgürtel für Männer, der das ganze Geschlechtsteil umschließt, wobei der Partner steuern kann, wann es wieder befreit werden darf. Das Problem an dem Keuschheitsgürtel lag daran, dass es keine physische Möglichkeit gab, das Schloss zu entsperren, sondern es war nur per App möglich. Das hätte man als Ransomware missbrauchen können. Man könnte jemanden erpressen, indem man sagen würde ‚ich lasse dich nicht raus, wenn du nicht so und so viel Bitcoin bezahlst'. Es gab ein Vibrator mit einer eingebauten Kamera. Wozu eine Kamera bei einem Vibrator gut sein soll, ist eine andere Frage, aber es war möglich, die aufgezeichneten Videos abzugreifen. Es gab ein anderes Toy, das während der Nutzung unbemerkt Tonaufnahmen gemacht hat. Man kann sich vorstellen, wie die Tondateien sich anhören. Es können im Extremfall auch physische Schäden entstehen. Bei einem Vibrator oder ähnlichem Gerät kann der Motor ordentlich hochgedreht werden. Wenn ein Fremder

Schaden beabsichtigt, kann das wirklich ein Problem sein. Bestimmte Sextoys werden dauerhaft während des Tages getragen, wobei Tragende nicht mit einer Nutzung rechnen. Wenn der Vibrator oder der Butt-Plug in der Sitzung mit dem Chef zu vibrieren beginnt, kann nicht nur physischer Schaden sondern auch Imageschaden entstehen. Es gab zum Beispiel ein Gerät, bei dem die App auf dem Handy alle zwei Minuten nach dem Server gefragt hat. Die URL war offensichtlich pornografisch. Das heißt, wenn ich dieses Toy beziehungsweise mein Handy auf Arbeit habe, sieht mein Admin, dass jemand über das Firmennetz ständig irgendwelche Porno-URLs aufruft. Das kann nicht nur Imageschaden mit sich bringen, sondern auch, falls ich in Iran oder Katar bin, eine Situation, die sehr böse ausgehen kann.

Lange: Also dieselben Probleme wie bei Puppen, Teddys oder anderen Kinderspielzeugen, die wir jetzt besprochen haben. Gelten dabei auch dieselben Vorsichtsmaßnahmen? Wir befinden uns kurz vor der Weihnachtszeit, wenn der eine oder andere Geschenke kauft, egal für welche Altersgruppe. Worauf sollte man generell achten? Einiges hast du schon erwähnt, aber wir könnten es noch einmal zusammenfassen, damit alle sich das auf ihre Einkaufslisten schreiben, wenn es ein ähnliches Geschenk sein soll.

Gobbin: Vor dem Kauf muss recherchiert werden, ob es schon bekannte Sicherheitsrisiken gibt. Wenn es Autoupdates gibt, sollen sie eingestellt werden und es muss bei dem Nutzeraccount starkes Passwort verwenden werden. Ich würde gerne einen vierten Punkt hinzufügen und sagen, dass man eventuell vor dem Kauf überlegen soll. Alle diese schönen Produkte wie Teddys oder Sextoys gibt es auch in dummer Version. Vielleicht ist die dumme Version manchmal die schlauere Wahl, weil alle diese Gefahren damit nicht passieren können.

Münz*:* Das erinnert mich an den Ausspruch einer halbwegs bekannten TV-Persönlichkeit, die gesagt hat „Sei schlau, stell dich dumm“. In diesem Fall würde ich sagen, sei schlau und kauf im Zweifelsfall lieber ein Gerät, das nicht so schlau ist wie das danebenstehende, um Risiken zu entgehen, über die wir gesprochen haben. Vielen Dank, Martin! Es waren sehr viele wertvolle Tipps dabei, vor allem für die Zeit, wenn Leute entweder spontan bei Black Friday Sachen kaufen oder anfangen, Weihnachtsgeschenke zu besorgen.

Lange: Vielleicht überdenken wir grundsätzlich das smarte Spielzeug und schauen, ob es einen ähnlichen Teddy ohne Verbindung gibt. Es wäre auch ein schönes Geschenk, das man auf die Liste nehmen könnte. Wir machen im Dezember eine Pause und freuen uns auf die nächste Folge im neuen Jahr. Wir haben schon ein paar Ideen für Themen. Wir freuen uns aber auch immer über Vorschläge von euch. Schreibt uns.

Münz: Schreibt uns auch gerne, welche neue vernetzte Geräte den Einzug in eure Haushalte gefunden haben. Es würde uns interessieren, wie ihr euch ausstattet und welche unsere Sicherheitstipps ihr beherzigt. Das ist uns besonders wichtig.

Lange: Wie immer gilt: kontaktiert uns gerne über die Kanäle von BSI auf Facebook, Instagram, Twitter sowie YouTube.

Münz: Oder ihr schickt uns eine E-Mail an bsi@bsi.bund.de. Wir freuen uns auf Post von euch!

Lange: Bis wir uns wiederhören, liket und folgt Update Verfügbar auf euren Podcast Plattformen. So verpasst ihr keine Folge. Für die bevorstehende Geschenkeeinkaufszeit gibt es in früheren Folgen mehrere Tipps zum Thema Fakeshops und Online-Bezahlen. Vielleicht mögt ihr da auch noch reinhören.

Münz: Wir wünschen euch alles Gute für die bevorstehende Advents- und Weihnachtszeit und sprechen für euch wieder im Januar 2023.

Lange: Kommt gut ins neue Jahr! Bleibt gesund und alles Gute! Bis bald. 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