„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 06, 30.03.2021:
Sichere Passwörter und erfolgreiche Comebacks

Moderation: Ute Lange, Michael Münz
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Lange: Es hat geklappt. Ich bin wieder drin. Michael? Michael, bist du da?

Münz: Endlich! Ja, ich bin da. Wir haben es geschafft. Sind Karin und Max noch da?

Lange: Nein, die scheinen ausgeflogen zu sein.

Münz: Puh, dann scheint ja alles noch einmal gut gegangen zu sein.

Lange: Naja, schon, aber ich habe dir von Anfang an gesagt, dass wir bei den Sicherheitsvorkehrungen sorgfältiger sein müssen. Aber du meintest ja, Fahrradhelm sei ein sicheres Passwort.

Münz: Ja, ja! Reib es noch einmal rein! Ich weiß, aber ich war einfach zu bequem, mich mit Passwort-Managern, Safes oder Zwei-Faktor-Authentisierung zu befassen.

Lange: Aber das passiert uns nicht noch einmal, dass wir hier andere in den Podcast reinlassen!

Münz: Auf keinen Fall! Lass uns die Folge nutzen, um das ganze Thema mit Passwortschutz und so zu bearbeiten und hier alles sicher zu machen.

Lange: Okay, das machen wir heute. Aber erst einmal etwas, auf das ich mich schon so lange freue: Hallo und herzlich willkommen zur neuen Ausgabe von

„Update verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Ich bin Michael Münz und wir melden uns auch in diesem Monat wieder nicht aus dem Bundesamt für Sicherheit in der Informationstechnik in Bonn, sondern wegen der Pandemie noch einmal aus dem Home-Office.

Lange: Auch wenn wir heute noch nicht wieder in unserem vertrauten Studio sind, fühlt sich das doch schon ein bisschen wie nach Hause kommen an.

Münz: Finde ich auch! Lass uns noch ein bisschen aufräumen hier und dann steigen wir ins Thema an.

Lange: Du glaubst nicht, was ich hier noch von Karin und Max gefunden habe! Da liegt ein Ausdruck mit dem Titel „Die häufigsten Passwörter“.

Münz: Die beiden dachten wohl, dass sie es damit in unsere Accounts schaffen. Ich vermute mal, „Fahrradhelm“ und „Münz80“ stehen nicht darauf.

Lange: Nein, es ist total originell, ehrlich gesagt: „1 2 3 4 5 6“. Es wird noch besser: „1 2 3 4 5 6 7 8“. Und das absolut sicherste Passwort der Welt: „1 2 3 4 5 6 7 8 9“.

Münz: Okay! Da waren wir ja doch ein bisschen einfallsreicher.

Lange: Aber geholfen hat es auch nicht wirklich, oder?

Münz: Ja! Bleibt also die Frage, was denn hilft, damit ich meine Passwörter nicht verliere und sie mir nicht geklaut werden. Ich meine, ich bin ja auf mehreren hundert Webseiten angemeldet: soziale Netzwerke, E-Mail, Banking, Shopping. Wie soll ich mir die ganzen Passwörter merken?

Lange: Das ist eine gute Frage! Die habe ich mir auch eine Weile gestellt. Vor allen Dingen kann es auch richtig teuer werden, wenn du so ein Passwort nicht mehr weißt oder verlierst.

Münz: Du meinst, weil jemand mit meinen Daten dann zum Beispiel Geld von meinem Konto stiehlt?

Lange: Ja, das ist eine Möglichkeit. Aber ich habe letztens etwas gelesen: Es geht offensichtlich noch ganz anders. Da hat ein deutscher Programmierer das Passwort für die Festplatte vergessen, auf der er seine Bitcoins gespeichert hat.

Münz: Das heißt, der kommt nicht an sein Geld heran? So wie ich, wenn ich am Geldautomaten meine PIN vergessen habe?

Lange: Im Grunde genommen ist es so etwas ähnliches. Allerdings geht es bei diesem erwähnten Programmierer um eine andere Summe als bei dir, vermute ich zumindest.

Münz: Wieso? Von welchem Betrag sprechen wir denn?

Lange: Also laut der Meldung hat er auf dieser Festplatte 7.002 Bitcoins.

Münz: Das macht in realer Währung?

Lange: Nur 220 Millionen US-Dollar!

Münz: 220 Millionen US-Dollar? Das Geld ist da und er kommt nicht daran?

Lange: Genau. Der ist offensichtlich kein Einzelfall. Es gibt wohl mehr Menschen, die damals zu Beginn von Bitcoin investiert haben, sich ein Passwort eingerichtet haben, über die Jahre nichts mehr damit gemacht haben und sich jetzt – wo es offensichtlich richtig abhebt – an die Passwörter nicht erinnern können.

Münz: Bei Bitcoins gibt es ja keine Bank, die einem eine neue Karte samt PIN ausstellt. Oh man, ich würde durchdrehen. Das ist echt ein krasser Fall, der mir aber genauso gut hätte passieren können. Ich weiß noch, ich habe einmal das Passwort für mein Telefon-Backup vergessen. Ich habe da gesessen und Passwort nach Passwort eingegeben. Ich habe es nicht hingekriegt. Ich hätte mir das besser aufschreiben sollen. Oder hast du einen besseren Tipp, damit ich bei Passwörtern nicht den Überblick verliere?

Lange: Also aufschreiben ist genau der Tipp, den wir nicht geben, weil das so ziemlich die unsicherste Variante ist. Aber ich habe eine Lösung für mich gefunden. Ich habe mir einen Passwort-Manager eingerichtet.

Münz: Ja, aber Ute, komm! Mal Hand aufs Herz: Du hast Tage gebraucht, damit das dann irgendwie fertig wurde, oder?

Lange: Wenn es nur Tage gewesen wären! Eher Jahre! Zumindest vom ersten Ansatz, dass ich mich damit beschäftigt habe, bis zur vollständigen Umsetzung kürzlich! Aber seit dem Schreck hier mit dem Podcast-Klau durch Karin und Max habe ich das jetzt alles fertig und jedes neue Passwort, das ich eingebe, geht ganz flott.

Münz: Aber ich meine „flott"? Wenn du „Jahre" sagst, dann passt „flott" ja nicht wirklich dazu. Was hat denn da so lange gedauert?

Lange: Naja, dahinter ist eine kleine Geschichte. Wie gesagt, der erste Ansatz war schon früher. Wie du weißt, ich habe einen persönlichen IT-Berater. Mein Neffe macht so etwas beruflich. Immer wenn es irgendwo in der Familie ein IT-Problem gibt, dann rufen wir ihn an. Ich hatte wieder mal so einen Fall von „irgendetwas mit Computer" und hatte einen Notruf abgesetzt. Dann kommt er sofort und kümmert sich. Das macht er echt super. Während er sich gekümmert und repariert hat, was immer da kaputt war oder nicht funktionierte, hat er gesagt: „Ich brauche das Passwort!" Ich habe ihm dann meine Liste gereicht, die natürlich auch total sicher in der obersten Schublade neben meinem Schreibtisch lag. Alle Tipps befolgt, die man hier so kriegt vom BSI! Da hat er die Hände zusammengeschlagen und hat gesagt: „Nein, das geht gar nicht. Ich bin schon da. Jetzt richten wir dir einen Passwort-Manager ein". Gesagt, getan! Die ersten 20, 30 Passwörter haben wir dann auch zusammen eingerichtet. Ja und dann…

Münz: Und dann? Das habe ich mir nämlich gedacht: Das ist das, was keinen Spaß macht. Ich meine: Dann kam etwas dazwischen, keine Lust, keine Zeit. Oder was war der Grund für die Verschleppung?

Lange: Bequemlichkeit ist tatsächlich ein Faktor. Das will ich gar nicht verschweigen. Meine Liste, die Papierliste, war ja noch da. Bei neuen Konten habe ich mich dann manchmal daran erinnert, dass ich so ein „Passwort-Dingens" eingerichtet habe. Aber die ganze Liste zu übertragen, dazu hatte ich überhaupt keine Zeit, also eigentlich keine Lust. Es war eine Kombination

aus beidem, denke ich mal. Dann ist es aber irgendwie kompliziert geworden, weil erstens hatte ich ein paar von den Passwörtern in dem Passwort-Safe drin und ich hatte immer noch meine Liste. Dann vergisst du mal ein Passwort. Kennst du das? Dann musst du ein neues einrichten. Was mache ich auf der Liste? Durchstreichen und darüber kritzeln! Es wurde also irgendwann relativ unübersichtlich und hat mich selbst genervt. Da wir jetzt seit einer Weile regelmäßig über Datensicherheitsfragen sprechen und recherchieren für den Podcast, hat mein Gewissen sich dann irgendwann gemeldet und hat gesagt: „Jetzt wird es aber Zeit, sei mal vorbildlich. Mach das mal, was du anderen so erklärst!“

Münz: Wie viel Zeit ist dann noch vergangen, bis du endlich fertig wurdest?

Lange: Das war gar nicht so viel, weil ich mich selbst ein bisschen überlistet habe. Ich hatte diesen Elan Anfang des Jahres und wollte das jetzt alles machen. Ich habe aber gedacht: „Naja, damit ich nicht gleich am ersten Tag scheitere, verlege ich diese Aufgabe auf drei Tage“. Am Ende war es gar nicht so viel, wie ich befürchtet hatte. Es ging sogar relativ schnell.

Münz: Okay, und schnell ist dann wie schnell?

Lange: Ich habe an drei Tagen jeweils so eine halbe Stunde, vielleicht mal 40 Minuten, meine Liste abgearbeitet, alles eingetragen. Ich konnte dann meine Liste zerreißen, schreddern – weg. Es ist jetzt alles im Passwort-Manager. Was ich super finde, seit ich den habe: Ich kann sowohl auf meinem Rechner Zuhause als auch auf meinem Mobiltelefon jedes Passwort sofort finden und ich kann mich bei den meisten Diensten dann auch sofort mit einem Klick anmelden. Das ist schön synchronisiert. Wenn ich etwas Neues eingebe, dann ist das immer auf beiden Geräten gleich dabei. Das einzige, was ich mir jetzt noch merken muss, ist das Masterkennwort für diesen Passwort-Safe. Wenn das weg ist, glaube ich, habe ich dann doch ein ernsteres Problem.

Münz: Das ist dann wie bei dem Bitcoin-Typen, der an die Daten nicht mehr herankommt?

Lange: Genau, oder ich nicht mehr an meine Passwörter herankomme und wieder von vorne anfange.

Münz: Und wie würdest du das verhindern?

Lange: Ich habe mir beim BSI etwas angeguckt. Die haben ganz gute Tipps. Darauf wäre ich selbst nicht gekommen. Ich verrate es auch nicht, weil ich muss mir ja mein Passwort selbst merken. Aber da gibt es schöne Hinweise für Eselsbrücken, die man sich bauen kann. Ich habe mir eine gebaut und mir etwas ausgesucht, was sehr sicher ist. Das werde ich garantiert nie wieder vergessen.

Münz: Gut, der Aufwand klingt schon beachtlich. Jahre, Tage, Selbstüberlistung und Eselsbrücken! Aber ich denke, es lohnt sich wirklich, meine Passwörter auch mal zu sortieren. Nicht, dass ich große Vermögen auf Festplatten verschlüsseln würde, aber es gibt ja nun wirklich genügend andere Beispiele dafür, was mit erratenen oder auch mit gestohlenen Passwörtern passieren kann.

Lange: Du meinst, noch mehr als hier, als die uns den Podcast gekapert haben?

Münz: Das passiert nicht noch einmal! Aber konkret denke ich eher an so etwas wie Identitätsdiebstahl, wenn jemand deine Identität nutzt oder – um es korrekter auszudrücken – missbraucht, um sich Vorteile zu verschaffen: um in Onlineshops einzukaufen unter deinem Namen oder Mobilfunkverträge abzuschließen oder auf Online-Dating-Plattformen teure Abos abzuschließen, für die du dann die Rechnung erhältst. Betrüger und Betrügerinnen nutzen die gestohlenen Daten auch, um Bankkonten zu eröffnen oder an Kreditkarten heranzukommen, illegale Geschäfte zu eröffnen oder einen Reisepass zu beantragen. Das ist vielleicht auf den ersten Blick alles ein bisschen weit hergeholt, aber Schätzungen zufolge ist jeder vierte Internetnutzer oder jede Internetnutzerin in Deutschland schon einmal Opfer von Identitätsmissbrauch geworden. Neben dem ganzen Ärger, den man hat, finde ich den finanziellen Schaden besonders krass, der da entsteht. Der ist beträchtlich. Studien sagen, dass in den letzten sechs Jahren

durch diese Art von Cyberkriminalität weltweit – Achtung, große Zahl – 112 Milliarden US-Dollar gestohlen worden sind. Das macht pro Minute – du kannst dir vorstellen, wie lange ich daran jetzt gerechnet habe – 35.600 US-Dollar.

Lange: Pro Minute?

Münz: Pro Minute!

Lange: In jeder Minute der letzten sechs Jahre? Das ist ganz schön viel. Das ist beängstigend, ehrlich gesagt. Wie kommen die Kriminellen denn an so persönliche Daten? Ich meine, ein Bankkonto oder einen Reisepass kann man ja nicht einfach mit einem Passwort von sozialen Medien oder so beantragen. Da musst du ja noch mehr Daten angeben.

Münz: Das stimmt. Wenn sie sich zum Beispiel in Accounts reinhacken in sozialen Medien oder bei Online-Firmen, ist da vielleicht doch mal deine Adresse hinterlegt – als Lieferadresse oder so. So kommen sie an den Zugang zu deinen Daten, die sie dann für ihre Zwecke missbrauchen und oft ohne, dass du es merkst und bis es zu spät ist. Was auch noch passiert: Neben Hacks wird mit Spam oder Phishing-E-Mails versucht, dir die Daten zu entlocken. Dann wird in einer fingierten E-Mail von irgendeinem Anbieter oder einer Bank nach deiner Anschrift, nach deiner Telefonnummer oder manchmal auch nach Zugangsdaten gefragt. Die Daten werden dann von denen, die sie abfragen, nicht nur dafür genutzt, sondern die landen über Verkauf im Internet auch bei anderen Leuten. Und Es gibt dann mehrere Täter, die versuchen, damit im Internet oder auch analog Schaden anzurichten.

Lange: Ja, das Thema Spam und Phishing hatten wir schon einmal. Da habe ich mir auch die Tipps, die du damals gegeben hast, gemerkt. Da bin ich ein bisschen aufmerksamer geworden.

Münz: Das will ich jetzt aber einmal wissen. Dann zähl mal auf! Wie war das damals?

Lange: Du hast gesagt, ich soll E-Mails von Menschen, die ich nicht kenne, am besten ungelesen löschen. Wenn es wichtig ist, käme die E-Mail auch wieder. Dann könnte man beim zweiten Mal überlegen, ob man nicht doch hineinguckt. Das hast du gesagt. Ich soll keine Anhänge öffnen, die ich nicht kenne – auch komische Dateiformate oder Sachen, die mir ein bisschen „fishy" vorkommen. „Fishy" heißt ja auf Englisch „verdächtig". Wenn das so aussieht, dann ist es das vermutlich auch. Ich habe mich in den letzten Wochen und Monaten tatsächlich auch ein bisschen öfter ertappt, dass ich zurückhaltender bin. Das waren super Tipps. Aber bei Identitätsmissbrauch scheint es ja noch um andere Sachen zu gehen. Was muss ich denn noch machen, damit mir das nicht passiert?

Münz: Generell gilt für deine Daten: am besten unter Verschluss halten. Das hast du mit deinem Passwort-Manager zum Beispiel schon ganz gut gemacht. Wenn du von einer Person oder von einer Webseite oder per E-Mail aufgefordert wirst, persönliche Informationen zu teilen, dann immer erst einmal prüfen, ob die Anfrage echt ist. Beispielsweise würde eine Bank niemals per E-Mail um die Bestätigung deiner Bankdaten oder nach deiner PIN fragen. Darauf muss man sich gar nicht einlassen.

Lange: Da sind wir wieder ein bisschen beim gesunden Menschenverstand, den wir schon ein paar Mal hier angesprochen haben: Dass ich Dinge, die ich in der analogen Welt nicht machen würde – einfach an eine Freundin Zugangsdaten weitergeben, auch online nicht machen soll. Das habe ich verstanden. Ich weiß aber, dass es noch eine Möglichkeit gibt, seine Daten sicherer zu machen als sie vielleicht jetzt bei dir sind.

Münz: Damit spielst du bestimmt auf die Zwei-Faktor-Authentisierung an, die ich auch bislang aus Bequemlichkeit bei vielen Dienstleistern noch nicht eingerichtet habe.

Lange: Über mich lästern, weil ich mit meinem Passwort-Manager so viel Zeit vertrödelt habe, zugegebenermaßen, aber selbst auch nicht alles machen, was einem empfohlen wird. Die Beispiele, die wir eben hatten, sollten dich jetzt eigentlich motivieren, doch näher in das Thema einzusteigen.

Münz: Ja, das stimmt. Aber weißt du?! Ich stehe davor und weiß nicht genau, wie es weiter geht und was ich machen soll und wen ich fragen könnte. Und dann fällt mir ein: Ich frag doch einmal dich. Du scheinst dich damit auszukennen. Also, Ute, was hat es denn damit auf sich und was sollte ich tun?

Lange: Du willst doch jetzt nur, dass ich über diesen Begriff noch einmal stolpere.

Münz: Das würde ich nie wollen.

Lange: Ich versuche es einmal. Die Zwei-Faktor Authentisierung, die manchmal auch Zwei-Faktor-Authentifizierung genannt wird, bezeichnet einen Vorgang, mit dem ich mich mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten, also Faktoren, in einem Dienst identifiziere. Das ist jetzt die offizielle Beschreibung dieses Vorgangs. Man kann es auch ein bisschen einfacher ausdrücken, weil ich sehe gerade, dass bei dir so Stirnrunzeln entstehen. Um mich anzumelden, brauche ich etwas, was ich weiß. Das ist das eine, zum Beispiel meine E-Mail-Adresse oder eine PIN. Ich brauche dann noch etwas Zweites, etwas, das ich besitze, zum Beispiel eine Smartcard oder mein Mobiltelefon. Manchmal ist der zweite Schritt auch ein biometrisches Merkmal wie mein Fingerabdruck oder die Gesichtserkennung, die im Moment manchmal darunter leidet, dass man ja Masken anhat. Aber das wäre ein zweiter Weg, wie ich mich identifiziere, wenn ich mich irgendwo anmelde.

Münz: Okay, „wissen“ und „besitzen“ kann ich mir merken. Das klingt gut. Das ist dann also dasselbe wie beim Onlinebanking: am Rechner einloggen und dann die TAN aber aufs Handy kriegen und bestätigen müssen.

Lange: Genau! Da gibt es unterschiedliche Vorgehensweisen, aber du meldest dich zunächst wie gewohnt bei deinem Dienst an, egal, welcher das ist. Der schickt dir dann auf unterschiedlichen Wegen noch einen Code – eine weitere Information, zum Beispiel aufs Handy. Das kann eine SMS sein. Mittlerweile haben viele Banken auch eine extra App. In der kriegst du dann einen Code, den du nochmal eintippst, oder du bestätigst das mit deinem Fingerabdruck.

Aber es gibt immer einen zweiten Schritt, bevor der Zugang dann praktisch gewährt wird.

Münz: Handy oder App habe ich meistens am Start. Im Grunde klingt es auch gar nicht so aufwendig, wie du es beschrieben hast – wie diese andere Geschichte mit dem Passwort-Manager. Tatsächlich kommt mir das Prinzip auch bekannt vor aus dem Home-Office. Wenn ich da in das Datennetz meines Arbeitgebers will, muss ich auch auf dem Handy parallel etwas bestätigen.

Lange: Das ist auch gut so, weil IT-Sicherheit im Home-Office im letzten Jahr eine viel größere Bedeutung bekommen hat. Früher haben nicht so viele Menschen im Home-Office gearbeitet oder nicht so regelmäßig. Und wenn, dann war das vorher alles besprochen und organisiert. Wir erinnern uns: Vor einem guten Jahr mussten viele von uns – mehr oder weniger, von jetzt auf gleich – ab nach Hause. Das hat viele Firmen ganz schön an ihre Grenzen gebracht. Die mussten improvisieren, mussten erst einmal gucken, wie sie das alles organisieren. Dabei ist IT-Sicherheit an manchen Stellen etwas vernachlässigt worden, weil es andere Fragen gab. Das hatte allerdings für einige Unternehmen relativ schnell unangenehme Konsequenzen, weil die Cyberkriminellen sich sehr rasch auf die Situation eingestellt haben. Die haben nicht lange gefackelt und gewartet, sondern haben sich Mittel und Wege ausgesucht. Ich habe ein paar Berichte damals gelesen und jetzt nochmal nachrecherchiert, dass zu Beginn der Pandemie vermehrt Angriffe aufgetreten sind auf Firmennetze, die tatsächlich den Eintritt über die Rechner der Mitarbeiterinnen und Mitarbeitern, die zu Hause gearbeitet haben, gefunden haben. Das war möglich, weil es noch nicht so richtig gut gelaufen ist, weil es vielleicht noch nicht diese Zwei-Faktor-Authentisierung gab, weil es noch nicht sichere Verbindungen zwischen den Firmen und dem Home-Office gab. Viele haben jetzt nachgebessert. Da gibt es mittlerweile ein großes Bewusstsein auf allen Seiten. Was aber auf jeden Fall immer noch eine Aufgabe von uns oder dir ist – du arbeitest ja auch teilweise im Home-Office für deinen Arbeitgeber, wenn wir zu Hause oder auch unterwegs arbeiten, dass wir dabei nicht die Firmen-IT oder deren Daten, was ja

teilweise auch unsere Daten sind, gefährden. Das heißt, auch dafür ist genau diese Zwei-Wege-Identifizierung, der Zugang, den man eben mit einer zweiten Hürde versieht, unbedingt empfehlenswert.

Münz: Das leuchtet ein! Wenn es für meine Firma funktioniert und auch gut klappt, dann sollte ich das für meine privaten Accounts auch einrichten. Also da bin ich – ich würde fast sagen – überzeugt.

Lange: Genau! Denn schließlich verlässt du dich beim Radfahren ja auch nicht nur auf deine Fahrkünste, sondern?!

Münz: Ich weiß schon! Auf meinen Fahrradhelm, den ich immer trage! Gut, alles klar, ich bin dabei! Dann werde ich in diesem Jahr den Frühjahrsputz ins Digitale verlegen und meine Passwörter aufräumen beziehungsweise werde ich sie in einen digitalen Safe einräumen.

Lange: Sehr schön, das freut mich! Du willst ja auch nicht, dass wir nach dieser Folge gleich wieder ausgesperrt werden von Karin und Max. Wenn sie es einmal geschafft haben, schaffen sie es vielleicht ein zweites Mal, außer: Wir beugen vor.

Münz: Genau, das werde ich auf jeden Fall. Dann bleibt das hier unser Podcast. Ich würde sagen, wir können auch schon ein bisschen nach vorne in die nächste Folge gucken. Gibt es denn bis dahin noch irgendetwas zu beachten?

Lange: Also für alle, die uns jetzt zuhören und deren Gewissen jetzt ähnlich anschlägt wie meines am Anfang des Jahres und das Gefühl haben, sie sollten sich um ihre Daten ein bisschen bemühen, und die etwas mehr absichern, gibt es eine ganze Menge Tipps, Tricks und Hinweise auf der Webseite des BSI. Ob das diese Zwei-Faktor-Authentifizierung ist – jetzt kann ich sie unfallfrei – oder ob es der Passwort-Safe ist! Wie gestalte ich meine Passwörter? Welche Regeln sollte ich dabei beachten, damit sie auch wirklich nicht von jemand anders erraten werden können? All das findet man auf der Webseite. Da kannst du dich auch orientieren, wenn du deinen Frühjahrsputz machst.

Münz: Auf jeden Fall! Das ist gut zu wissen! ich kann nicht ausschließen, dass ich die eine oder andere Hilfe brauchen werde.

Lange: In die Shownotes packen wir auch ein paar Links für alle, die jetzt Interesse haben und sich ihren Frühjahrsputz auch digital vorstellen können wie du.

Münz: Ja, gut.

Lange: Haben wir sonst noch Infos für unsere Zuhörer und Zuhörerinnen, Michael?

Münz: Die haben wir, nämlich zu der nächsten Folge! Dann nehmen wir uns das Thema Smarthome vor. Unter anderem geht es da noch einmal um die Kaffeemaschine, die mich morgens erpresst. Die begleitet uns schon seit der ersten Folge, glaube ich. Über die würde ich gerne beim nächsten Mal noch einmal reden.

Lange: Okay, das ist ein super Thema. Ich bin sehr gespannt, was wir da Neues lernen. Für Sie alle da draußen, die uns zuhören, noch einmal der Hinweis, dass man uns auf Spotify, Deezer, Google und iTunes hören kann. Bitte abonnieren Sie uns, liken Sie uns! Sagen Sie weiter, dass es diesen Podcast gibt, und senden Sie uns auch gern Rückmeldungen! Wir freuen uns über Ihre Tipps und Erfahrungen für und im digitalen Alltag.

Münz: Kontaktieren kann man uns über die BSI-Kanäle auf Facebook, Twitter sowie YouTube und E-Mail-Adresse mail@bsi-fuer-buerger.de. Wobei bei „für“ und „Bürger“ die Umlaute „u“ und „e“ sind. Wir freuen uns auf Post! Anregungen und Anmerkungen nehmen wir gern auf.

Lange: Ja, gerne auch zu Themen, die Sie beschäftigen, wo Sie vielleicht Fragen haben, wo Sie mehr drüber wissen wollen. Das können wir hier im Podcast aufgreifen! Bis wir uns dann wieder hier hoffentlich im Studio oder vielleicht im Home-Office treffen, eine gute Zeit und bleiben Sie gesund!

Münz: Tschüss aus dem Home-Office und bis bald im BSI!

Besuchen Sie uns auch auf:

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

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