„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 45, 31.07.2024

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

Ute Lange: Hallo und herzlich willkommen. Es ist Sommer. Endlich, muss man fast sagen, und Urlaubszeit. In dieser Folge erfahrt ihr, wie ihr eure Daten und Geräte urlaubssicher macht.

Michael Münz: Mittlerweile haben in allen Bundesländern die Sommerferien begonnen. Die Wahrscheinlichkeit, dass ihr diese Folge also irgendwo von unterwegs hört, ist relativ hoch.

Ute Lange: Seid ihr am Meer, am Pool oder in den Bergen? Wir sind neugierig. Schickt uns gerne eure Lieblingsfotos, wo ihr die Folge gerade hört. Das geht an die E-Mail Adresse: podcast@bsi.bund.de.

Michael Münz: Falls ihr noch zu Hause seid, umso besser. Dann könnt ihr mit den Tipps dieser Folge eure Daten reisesicher machen, bevor es losgeht. Über einen dieser Tipps, liebe Ute, müssen wir beide ein ernstes Wörtchen reden, weil den befolgst du wiederholt nicht. Ich habe erst letztens wieder Sachen von dir gesehen, wo ich gedacht hätte, wir wären darüber hinweg. Das wäre ich mal der Expertin, die wir heute dabeihaben, petzen, und die hat hoffentlich auch ein ernstes Wort für dich, damit solche Sachen nicht nochmal passieren.

Ute Lange: Ich bin mir jetzt gerade gar keiner Schuld bewusst und bin sehr neugierig, was du da entdeckt hast oder vermeintlich entdeckt hast. Damit sie auch tatsächlich etwas dazu sagen kann, holen wir unsere Expertin gleich mal herein. Sie ist wiederholt hier, und wir freuen uns sehr. Liebe Karin Wilhelm vom BSI, schön, dass du wieder dabei bist.

Karin Wilhelm: Hallo, ich freue mich auch sehr, auch wenn ich heute besonders aufgeregt bin, weil ich zum ersten Mal zum Interview hier bin.

Michael Münz: Das stimmt, deine Stimme haben wir hier schon mal gehört, aber nicht als Interviewgast, sondern als Moderatorin. Zu Coronazeiten hast du schon zwei Folgen von Update verfügbar moderiert, und dann dachten wir, tauschen wir einmal die Seite und schauen, wie du dich auf der anderen Seite machst.

Karin Wilhelm: Ich fand euren Job schon damals sehr schwer. Das war eine Notlösung, die wir gefunden hatten. Ich fand es damals schon sehr schwer, was ihr da macht und wie ihr uns immer tolle Podcasts zaubert. Von daher bin ich jetzt zuversichtlich, in guten Händen zu sein mit euch.

Ute Lange: Was machst du jetzt im BSI? Damals hast du noch etwas anderes gemacht. Was ist aktuell deine Aufgabe?

Karin Wilhelm: Ich bin im BSI zuständig für Verbrauchersensibilisierung und Informationsvermittlung. Wir stellen uns Fragen wie, was können die Menschen gut gebrauchen, um ihr Wissen zu steigern, rund um die Cybersicherheit? Wir hören in das Haus hinein. Da haben wir sehr viele Expertinnen und Experten, die unfassbar kluge Sachen sagen. Wir versuchen, die so einfach wie möglich nach draußen zu bringen und überlegen uns Formate wie den Podcast, aber auch was kann man auf eine Website schreiben? Gibt es einen Flyer, der da nützlich sein kann? Darüber machen wir uns Gedanken und versuchen, die Welt ein bisschen besser zu machen, sodass sich Verbraucherinnen und Verbraucher sicher und selbstbestimmt in der digitalen Welt bewegen können.

Ute Lange: Du hast eben schon gesagt, du bist etwas aufgeregt, weil du heute Fragen beantworten und nicht stellen sollst. Fangen wir gleich damit an. Warst du schon in Urlaub, oder fährst du noch? Wenn ja, wohin geht es dieses Jahr?

Karin Wilhelm: Ich bin total urlaubsreif und freue mich, dass mein Urlaub noch ansteht. Der geht mit der Familie ans Meer. Ich freue mich schon total, dass bald ein bisschen frischer Wind durch meine Haare wehen wird, und dass ich ein bisschen mehr nach draußen gehe und weniger an digitalen Geräten hänge. Da habe ich jetzt Lust drauf.

Michael Münz: Es geht aber nicht nur um das, was man im Urlaub macht, sondern auch, wie man seinen Urlaub vorbereitet. Ich zum Beispiel mache erst mal die Standards, also Updates laden und Back-ups machen. Dann lade ich alle wichtigen Dokumente wie Tickets oder Visum und Reservierungen auf das Handy und in die Cloud, damit ich die immer dabeihabe, weil ich nicht mehr ausdrucke. Was ich auch mache, ich stöpsel meinen Router aus, bevor ich fahre, damit hier alles offline ist und sich niemand mit meinem Netz verbinden kann. Stehen diese Sachen auch bei dir auf der Liste, und würdest du dann sagen: "Michael, fahr ruhig in den Urlaub. Alles gut gemacht."

Karin Wilhelm: Das hört sich schon sehr gut an. Ich glaube, unser Verhalten ist sehr ähnlich. Ich würde für mein Verhalten noch hinzufügen, ich bin eine Hörspieltante und lade mir immer meine Hörspiele herunter, damit ich die nicht später irgendwo herunterladen muss, sondern direkt auf meinem Handy habe.

Zusatzinfo: Deaktiviert beim Smartphone den Aufbau von Datenverbindungen im Ausland, wenn ihr keinen entsprechenden Tarif habt. Smartphones und darauf installierte Apps können im Hintergrund Daten versenden und empfangen, und das kann im Ausland richtig teuer werden.

Karin Wilhelm: Aber es gibt vielleicht noch Tipps. Wenn man so ein etwas anderes Verhalten hat, wie mein Schwiegerpapa beispielsweise. Der hat alle seine Accounts auf dem PC, und wenn er unterwegs ist, funktioniert das nicht mehr wie zu Hause. Da kann man sich erste Gedanken machen, weil man beispielsweise einen Passwort-Manager zu Hause hat, der auf dem mobilen Gerät nicht geht, oder man hat eine Liste, die man in der Schublade einschließt. Die sollte man nicht unbedingt mitnehmen, aber vielleicht braucht man unterwegs doch einen Zugang. Dann sollte man sich die Fragen stellen: Wie erinnere ich mich daran, oder wie erinnert sich mein Gerät daran, dass ich mitnehme? Das wäre auch noch eine wichtige Frage.

Ute Lange: Wie ist es überhaupt mit Geräten? Soll man die alle mit in den Urlaub schleppen? Es kann auch einer zugreifen und einem ein Gerät abhandenkommen? Wie hältst du es damit?

Karin Wilhelm: Genau, es kann immer sein, dass ein Gerät abhandenkommt, und da ist es immer sinnvoll, dass niemand sofort auf mein Gerät zugreifen kann. Einen Geräteschutz kann ich genauso auf dem Smartphone haben wie auf dem Tablet. Die Frage ist, ob ich alle Geräte brauche oder ob ich nicht, wie ich mir das vorgenommen habe, lieber Lust habe, durch die Natur zu streifen. Da ist jeder anders. Wer Geräte mitnehmen möchte, sollte sich Gedanken machen, ob er da einen Geräteschutz einrichtet. Die meisten haben eine Gesichtserkennung oder eine PIN hinterlegt. Das ist der erste Schritt zur Sicherheit, aber es kann trotzdem abhandenkommen, also muss man vorsichtig sein.

Michael Münz: Früher musste man oft klären, wer die Blumen gießt in der Abwesenheit oder das Haustier füttern oder solche Geschichten. Mittlerweile haben viele Leute ein Smarthome, wo viele Sachen automatisiert funktionieren. Wie ist es damit? Kann ich die Maschinen weiterlaufen lassen, auch wenn ich weg bin, oder gibt es da auch noch etwas woran ich denken sollte, bevor ich die Haustür hinter mir zuziehe und abschließe?

Karin Wilhelm: Das ist eine Frage der Abwägung. Es gibt Smarthome-Technik, die beispielsweise den Eindruck erwecken kann, hier wohnt noch jemand. Beispielsweise kann ich die Rollladensteuerung so programmieren, dass sie abends hochgeht, und es geht ein Licht an. Das gibt mir ein Gefühl von Sicherheit. Jedes Gerät, was sich vielleicht in meiner Wohnung noch bewegt oder bestimmte Aktionen ausführt, sei es der Staubsaugroboter, der noch mal durchwischt, kann etwas anstellen. Vielleicht hat er etwas umgeworfen. Es liegt Wasser auf dem Boden, und das Parkett oder der neue Boden ist dahin. Jedes Gerät, das noch in irgendeiner Form durch die Wohnung fährt, kann auch von außen durch Cyberkriminelle missbraucht werden. Das besteht weiterhin, deshalb ist mein Ratschlag, immer so viel wie möglich ausstellen. Alles, was aber eine sinnvolle Verwendung hat, wie beispielsweise die Rollladensteuerung, da würde ich es genauso machen. Da muss man nur schauen, ob das gut abgesichert ist.

Ute Lange: Mir fällt gerade etwas ein. Ich habe im Bekanntenkreis Menschen, die offensichtlich schon viel Smarthome steuern und die, bevor sie am Flughafen einchecken, nochmal kurz checken, ob ihr Smarthome sicher ist. Ist das eine gute Idee?

Karin Wilhelm: Ich sehe das etwas kritisch, weil man sich Folgendes vorstellen muss: Ich bin am Flughafen, und wie habe ich meine Verbindung nach zu Hause? Stecke ich beispielsweise im öffentlichen WLAN? Dann nenne ich das sensible Daten, weil Informationen über mein zu Hause gerade in diesem öffentlichen WLAN geteilt werden und möglicherweise über eine Anwendung, die nicht verschlüsselt ist. Was bedeutet das? Theoretisch könnte jemand die abgreifen. Da wäre ich immer vorsichtig. Wenn ich sicher bin, in einem WLAN zu sein, das mir vertraut ist, weil es beispielsweise von einem Familienangehörigen ist, oder wenn ich sicher bin, dass es sich hier um eine verschlüsselte Anwendung handelt, kann ich natürlich schauen, was zu Hause los ist. Ich würde das aber nicht überall tun und schon gar nicht an öffentlichen Plätzen mit öffentlichem WLAN, wo ich nicht weiß, wie sicher das ist und wie gut das eingerichtet worden ist.

Zusatzinfo: Wenn ihr wichtige Dokumente wie Reisepässe, Ausweise, Flugtickets, Buchungsunterlagen oder Impfpässe einscannt und diese auf einem USB-Stick oder in der

Cloud speichert, dann solltet ihr diese unbedingt verschlüsseln oder mit einem Passwort schützen.

Michael Münz: Das betrifft nicht nur Flughäfen, sondern wir kommen jetzt an den Moment, wo man die Zimmertür aufmacht, von der Bude, der Suite oder wo auch immer man seinen Urlaub verbringt und denkt: Angekommen. Ich muss erst mal allen Leuten zeigen, wie cool der Whirlpool oder die Natur hier ist. Was auch immer man sich gebucht hat. Dann stellt sich dieselbe Frage, oder? Ich kann nicht einfach, das Nächstbeste nehmen, was da herumliegt, selbst wenn es vom Hotel ist, ohne zu wissen, was da los ist.

Karin Wilhelm: Das kommt darauf an. Ich bin immer für Lösungen. Ich habe das Bedürfnis, meiner Oma aus dem Urlaub so ein Foto zu schicken. Da sind wir bei den Messenger-Diensten, und viele von denen sind Ende-zu-Ende verschlüsselt. Das ist gut und es war nicht immer so. Vielleicht hat der eine oder die andere diese Debatte mitbekommen und sich gefragt: "Wofür brauche ich das?" Für genau solche Momente, dass ich, wenn ich meinem Messenger vertrauen kann, ins Hotel komme und sage: "Oma, das ist ein ganz toller Pool hier, uns geht es gut. Vielen Dank." Das ist das eine. Ihr habt schon herausgehört, dass ich öffentlichem WLAN grundsätzlich sehr skeptisch gegenüber bin. Warum ist das so? Ich vergleiche das immer mit einer öffentlichen Toilette. Das Bild hinkt ein wenig. Aber es ist so, bei einer öffentlichen Toilette gehe ich hin, und es gibt wenige, die richtig angenehm sind. Da duftet es, die Seife ist toll. Da fühle ich mich richtig wohl, und weiß, hier bin ich safe. Wie viele davon sind aber auch schmutzig, wo ich mich unwohl fühle? Genauso ist es auch mit dem WLAN. Nur, weil mein Hotel einen sehr guten Eindruck macht und vielleicht die Menschen alle sehr nett sind, heißt das nicht, dass dieses WLAN sehr akkurat eingerichtet ist und dass sich jemand um Sicherheit Gedanken gemacht hat. Ganz im Gegenteil, das ist oftmals gar kein Kriterium, und da weiß ich nicht, was ich bekomme. Es besteht immer die Gefahr, dass Daten abgegriffen werden. Im einfachsten Fall sehen die Menschen, dass ich gerade auf der Seite war und mich da umgeschaut habe, wo man die nächste Tour machen kann. Im schlimmsten Fall aber kriegen sie vielleicht andere Daten von mir, die ich nicht teilen möchte, und das würde ich immer versuchen zu vermeiden.

Michael Münz: Ich habe zwei traumatische Erlebnisse, also eins mehr, eins weniger, die mich davon abhalten, jede Toilette aufzusuchen, um in deinem Bild zu bleiben. Es gab eine Stieg Larsson-Verfilmung mit Lisbeth Salander, dieser Hackerin, wo jemand in einer Hotellobby saß und geguckt hat, welche Daten im ungesicherten Hotelnetz gerade geteilt werden, und konnte die protokollieren. Da habe ich noch gedacht, das ist Film. Dann war ich auf einem Barcamp, wo am Ende des Tages jemand aufstand und sagte: "Wer hat hier eigentlich die E-Mail-Adresse, kontakt@michaelmuenz?" Ich sagte: "Hier, ich!" Da hatte die Person den Tag über aus dem ungesicherten Veranstaltungs-WLAN alle Daten mitgeschrieben und mir im Klartext mein E-Mail Passwort gezeigt von damals. Und da habe ich gedacht: "Junge, sei lieber vorsichtig, putz immer schön die Brille ab und so weiter." Also sei einfach vorsichtig bei den Daten, die du teilst und über welches Netzwerk du sie teilst. Karin, wenn ich da bin, woran sehe ich denn, dass das Netzwerk safe ist?

Karin Wilhelm: Da kriege ich sofort Gänsehaut. Das ist doch ein echter Moment, wenn jemand sagt: "Ich habe dich virtuell gesehen." Das ist das Problem. Man kriegt es nicht mit, wenn man gesehen wird. Woran sehe ich das? Man überliest das, aber in den Einstellungen, wenn man sich mit einem WLAN verbindet, steht das da auch manchmal. Da steht dick: ungesichertes Netzwerk. Es steht nicht dick, sondern ist eher dünn geschrieben, meine ich.

Dann überliest man das, aber es ist ein wertvoller Hinweis. Man muss sich das so vorstellen: In der Regel sind Hotel-WLANs nicht wirklich Passwort-geschützt. Es gibt oft ein Passwort für alle. Was bedeutet das? Da kommen viele herein. Worauf muss ich noch achten? Wenn sich Kriminelle überlegen, welchen Angriff sie fahren können, gibt es manchmal die Möglichkeit, dass sie sagen: "Ich mache einen Hotel- oder Airbnb-Namen, der so ähnlich klingt. Vielleicht lockt sich jemand bei mir ein. Da brauche ich überhaupt nichts machen." Wir müssen uns Cyberkriminelle als etwas faul vorstellen. Die sitzen nicht unbedingt mit einem Hoodie am Pool und denken: Planscht ihr nur im Pool, ich greife eure Daten ab. So habe ich mir das lange Zeit vorgestellt, aber es ist so, dass sie wenig Aufwand haben wollen. Sich die Mühe zu machen, sich ins Hotelfoyer zu setzen und alle Daten des Hotels abzugreifen, ist für sie eher müßig. Es besteht auch das Risiko, dass sie da ergriffen werden. Wer ist der Mensch, der da die ganze Zeit auf den PC schaut?

Michael Münz: Im Hoodie.

Ute Lange: Am Pool. Pool heißt meistens warm und ein Hoodie ist warm, das passt nicht wirklich.

Karin Wilhelm: Genau, wir merken schon, das Bild kann nicht funktionieren. Darum sind es oft eher automatisierte Dinge, die uns erwischen, beispielsweise ein Hotspot, der gefälscht ist, ein Fake-Hotspot. Bei dem ich aber denke, der ist vom Hotel. Da sollte man sicher sein. Oft bekommt man ein Zettelchen gereicht, aber manchmal auch gar nichts. Ich kenne es selbst, dass man dann guckt, was gibt es hier? Das scheint mir plausibel. Plausibel reicht da nicht unbedingt. Das ist zum Beispiel eine Möglichkeit. Ich würde immer empfehlen, im öffentlichen WLAN wachsam zu sein. Weniger ist hier mehr. Wir sind im Urlaub. Ich hoffe, viele von den Zuhörerinnen und Zuhörern müssen da keine Bankgeschäfte machen. Die sind vielleicht alle schon erledigt. Wir müssen nicht sensible Daten von A nach B bringen, und wenn es doch passiert, dann müssen wir uns etwas einfallen lassen.

Ute Lange: Ich war kürzlich auf einem Yoga Retreat in Spanien. Da fahre ich einmal im Jahr hin. Da hat man viel Zeit am Pool. Niemand von uns hat da im Hoodie gesessen, aber wir haben durchaus am Pool online gesurft. Dann gab es Gedanken wie: Das sieht nett aus, wollen wir nicht auf das Konzert gehen? Was einem plötzlich in seiner Freizeit in den Sinn kommt. Ich bin schon immer ein bisschen die Mahnerin. Bin ich die Spielverderberin, oder sollten die dann doch auf jemanden wie mich hören, dass lieber nicht zu machen in der Situation?

Karin Wilhelm: Beim öffentlichen WLAN würde ich immer erst mal empfehlen, seid skeptisch. Ihr wisst nicht, wer da vielleicht mitlesen kann und wie sicher es ist. Es ist aber vollkommen klar, dass ihr euch digital bewegen wollt. Was haben wir also für Möglichkeiten? Erstens, wir könnten Dinge vermeiden. Vermeidet sensible Daten und Shoppingtouren. Ihr könnt natürlich sagen, dass ihr auf Webseiten surft oder ähnliches, weil ihr sagt: "Ich gehe das Risiko ein, dass jemand sieht, dass ich gerade die Nachrichten lese." Die zweite Möglichkeit sind verschlüsselte Dienste. Verschlüsselte Dienste bedeutet, dass nur ich das auf meinem Gerät sehen kann. Dann wird es verschlüsselt, und dann geht es zu der Person, der ich etwas schicken möchte. Das ist im Wesentlichen wichtig für Messenger, aber es gibt auch beispielsweise Angebote für Online-Banking, die verschlüsselt sind. Checkt das vorab und schaut genau, ob es Ende-zu-Ende verschlüsselt ist. Dann könnt ihr das Risiko eingehen. Die dritte Möglichkeit wäre ein VPN-Zugang. Ich empfehle euch, ladet das nicht im Urlaub runter. Macht euch den Stress nicht dort. Da wollt ihr nur genießen und entspannen. Man

muss sich schon ein bisschen einlesen und sich überlegen, welcher passt gut zu mir. Dazu gibt unsere BSI-Website auch ein paar Hinweise, worauf man da achten kann. Wie funktioniert ein VPN? Ein VPN kann man sich wie einen Tunnel vorstellen. Ich kommuniziere sensible Daten an eine andere Person, und das kann keiner abgreifen, weil die durch einen schmalen Tunnel gehen. Von rechts und links ist es geschützt. Das sind Dinge, die ihr euch überlegen könnt, dann habt ihr einen entspannten Urlaub.

Michael Münz: Ich bin froh, Ute, dass du diesen Urlaub ansprichst, denn ich hätte es auch getan. Karin, ich muss dir etwas erzählen, was die skeptische Pool-Surferin, die angebliche Mahnerin, tatsächlich macht, wenn sie im Urlaub ist. Alle aus Utes Adressbuch wissen, dass Ute in Echtzeit in Spanien ist, weil sie Fotos und Videos aus dieser Zeit in ihren WhatsApp-Status postet. Wir müssen gar nicht darüber reden, dass man hier etwas kauft oder Sonstiges. Wir haben vor zwei Jahren in diesem Podcast mit Michael Meier von der Universität Bonn darüber gesprochen, dass man besser keine Echtzeitinformationen über Abwesenheit postet, weil sonst jeder weiß, dass die Wohnung leer ist. Da kann der Staubsauger-Roboter noch zehnmal hin und her fahren, und jeder denkt, ich höre etwas, die Ute ist bestimmt zu Hause, weil sie das nicht ist, denn ihre Fotos landen im Whatsapp-Status. Ich war wirklich, ich will nicht sagen, entsetzt, aber ich habe gedacht: Ute, das hatten wir schon einmal. Karin, jetzt bist du da, weil auf mich und den Michael Meier hört sie offensichtlich nicht. Sag du etwas dazu?

Karin Wilhelm: Ich finde es toll, dass ihr gut aufeinander aufpasst, weil die digitale Welt ist immer herausfordernd, und das sind Dinge, die passieren einem. Das ist so verführerisch. Ich kann es mir vorstellen, Ute, dass du deinen Freundinnen und Freunden zeigen wolltest, hier ist es geil. Aber so ein Status ist vielleicht nicht der richtige Weg gewesen. Tatsächlich sendest du damit ein Signal. Gott sei Dank, wurde deine Wohnung nicht leer geräumt. Vielleicht machst du beim nächsten Mal einen Gruppenchat auf, über den du berichtest, eine geschlossene Gruppe, oder du schickst eine Mail oder verschickst sie einzeln. Ansonsten verstehe ich dein Bedürfnis, aber du hast sehr viele Daten in die Welt herausgesandt. Wenn dich jemand da beobachtet, hätte der dir das böse auslegen können. Ist aber nicht passiert, oder?

Ute Lange: Zu meiner Ehrenrettung möchte ich sagen, dass wir damals mit Michael Meier über Social Media gesprochen haben und ich es seitdem nicht mehr mache, weil ich sehr wohl auf ihn gehört habe. Ich nehme euren Hinweis aber dankend an und werde mir für meine nächste Auszeit, die bald auch ansteht, etwas anderes überlegen. Oder ich habe ja auch gelernt, dass man in Messenger-Diensten einstellen kann, wer den Status sehen darf. Das ist ein bisschen mühselig, aber ich könnte die Leute aussortieren aus meinem Adressbuch, von denen ich nicht möchte, dass sie das wissen. Dann habe ich fast eine Chatgruppe. Wieder etwas gelernt, danke.

Karin Wilhelm: Das klingt nach einer sehr guten Lösung.

Michael Münz: Nächster Urlaub ist gut. Man kommt nach dem Urlaub nach Hause. Nehmen wir an, die schönste Zeit des Jahres ist vorbei, ich komme nach Hause und habe nachträglich meine Fotos geteilt und Fotoalben gemacht, die ich nur mit bestimmten Leuten teile. Dann habe ich das gemacht, was du sagst, Karin, ich war abstinent und habe nicht viel in meine Mails geguckt. Dann mache ich mein E-Mail-Postfach auf, und da sind hunderte von Mails. Newsletter, die man bestellt hat, irgendwelche Nachfragen und so weiter. Hat man dann nicht den Wunsch, seinen Posteingang schnell aufzuräumen? Vielleicht wird man

nachlässig und klickt schneller mal auf Sachen, auf die man sonst nicht geklickt hätte? Was ist deine Erfahrung? Wie ist es, wenn du deinen Posteingang aufmachst nach dem Urlaub?

Karin Wilhelm: Das ist tatsächlich eine kleine Falle. Alles, was wir unter Zeitdruck machen, und das ist oft, wenn man viele E-Mails hat. Man denkt, komm, schnell weg. Dann neigt man dazu, auch die eine oder andere Phishing-E-mail nicht zu erkennen. Deswegen ist es ratsam, das einmal zu scannen. Bei Dringlichkeit muss man immer aufpassen. Daran erkennt man Phishing-E-maisl am ehesten. Die sind gut. Phishing-E-mails sind ein betrügerischer Angriff in irgendeiner Form. Beispielsweise könnte das eine vermeintliche meiner Bank sein oder meines Urlaubsanbieters, und auf einmal denke ich: Das muss ich schnell erledigen, sonst kriege ich Ärger. Wenn man dieses Gefühl hat, ist es ratsam, noch einmal zu gucken. Das sind die Dinge, die man noch mal kurz liegen lässt und sich überlegt, ist es wirklich plausibel? Wenn man Zweifel hat, einfach zum Telefonhörer greifen und anrufen. Das will man in dem Moment nicht machen, denn man will nur schnell diese Mails abarbeiten. Es lohnt sich aber, weil es eine Flut an Phishing-E-mails gibt und wir in Stresssituationen am anfälligsten sind und selbst die besten darauf hereinfallen.

Ute Lange: Das kann ich nur bestätigen. Es ist manchmal in einem fast schon beunruhigenden Zusammenhang mit Dingen, die im Leben passieren. Ich hatte vor einer Weile mit einem Paketdienst ein bisschen Kontakt und Ärger. Kurz darauf kriegte ich von vermeintlich anderen Paketdiensten ständig Nachrichten, mein Paket wäre jetzt abzuholen. Da war ich super aufmerksam, weil ich dachte, irgendwie ist es komisch und habe die alle gelöscht. In einem unbedachten Moment hätte ich vielleicht auch daraufgeklickt, weil ich hatte ja die Situation, dass mir ein Paket abhandengekommen ist. Du sagtest gerade Urlaubsanbieter oder Plattformen. Gibt es auch Vorfälle, über die du berichten kannst, wo wir besonders aufmerksam sein sollten? Michael hat gerade schon gesagt, nach dem Urlaub ist für viele Menschen vor dem Urlaub. Manche haben lange Planungszeiten. Dann ist man vielleicht auch noch entspannt. Worauf sollte ich achten, wenn ich schon den Ausblick auf das nächste Jahr werfe?

Karin Wilhelm: Das ist ein sehr wichtiges Thema, weil ich glaube, das ist noch mit das größte Einfallstor. So gibt es beispielsweise viele Vorfälle im Bereich dieser Portale. Stellen wir es uns so vor: Ich habe meine Koffer schon gepackt und klappe meinen Laptop auf. Auf einmal steht da: Hier ist etwas mit der Buchung schiefgegangen. Sie müssen dringend Geld bezahlen. Das ist alles nicht gut gegangen, sonst brauchen sie morgen gar nicht anreisen. Was wird jeder denken? Ach du meine Güte, ich muss sofort aktiv werden, sonst kann ich morgen nicht anreisen. Das ist mein eigentliches Bedürfnis. Wenn man dann überweist, ist das Geld weg. Was ist da passiert? Es war doch über mein Buchungsportal, eigentlich ist doch alles prima. Leider nicht. Es gibt solche Angriffsfälle, da sind viele Mittel beteiligt. Ich habe mir die erklären lassen. Es ist so, dass beispielsweise an verschiedene Hotels Mails mit Schad-Software geschickt werde. Es braucht nur ein Mitarbeiter oder eine Mitarbeiterin, den falschen Link zu klicken, und auf einmal hat man ein Schadprogramm in diesem Hotelsystem eingeschleust, das Daten abgreift. Was für Daten greifen die ab? Zum Beispiel den Zugang zum Buchungsportal. Was machen die damit? Die verkaufen das zum Beispiel im Darknet. Dann kommt jemand anderes. Der erste ist ein Angreifer, der gut abgreifen kann und dann kommt ein anderer Angreifer oder eine Angreiferin, fairerweise, die sich sagt: "Ich könnte diese Daten gut gebrauchen, weil ich kann gut angreifen. Der andere konnte abgreifen, ich kann angreifen." Und dann nutzen die diese Zugangsdaten zum Portal, um auch da an die Informationen zu kommen. Die wissen, die Wilhelm will ans Meer. Da ist ihre

Location. Dann können die ziemlich genau mit suggerieren, das ist dein Urlaubsziel. Da musst du nachzahlen. Auf einmal ist es sehr plausibel, denn es ist mein Urlaubsanbieter, alle Rahmendaten stimmen, und ich kriege einfach nur Stress. Da bin ich am ehesten geneigt zu sagen, zahlen, weil sonst weinen hier alle und ich obendrauf, denn ich kriege meinen Urlaub nicht. Das ist sehr erfolgreich, und da muss man am meisten drauf achten. Was macht man da? Am besten das Hotel anrufen. Es kommt wieder das Anrufen. Wir müssen uns bestätigen lassen, dass das alles seine Richtigkeit hat. Niemals schnell überweisen ist die Devise, sondern immer erst mal überlegen, prüfen und nachfragen.

Michael Münz: Ich bin noch einmal kurz ein Klugscheißer an dieser Stelle. Ich rufe nicht die Nummer an, die in dieser Mail steht, richtig? Sondern ich suche die aus dem Telefonbuch heraus, oder was auch immer.

Karin Wilhelm: Ja, das ist die beste Ergänzung. Das ist alles mitgedacht, und das müssen wir uns auch so vorstellen. Ich habe selbst oft gedacht, warum wollen die mich selbst angreifen? Der Klassiker: was gibt es bei mir zu holen? Das ist alles automatisiert. Die machen ihre Testläufe, und dann merken sie: Wir können gleich die falsche Telefonnummer hereinstellen. Sie schicken viele Mails raus. Es ist nicht nur das eine Hotel, das ich vielleicht besuche, sondern es sind viele, denn es ist gerade Sommerzeit. Da kann man sich auch ein kleines Servicecenter aufbauen, ein Fake Servicecenter und Anrufe entgegennehmen. Guter Hinweis.

Ute Lange: Karin, das war noch ein Supertipp zum Ende unseres Gesprächs, weil für viele Menschen steht der Urlaub noch bevor, und ich kenne eine Menge Leute, die sich sehr kurzfristig entscheiden. Die haben hoffentlich aufmerksam zugehört. Für mich ist da einiges dabei. Vor allen Dingen, dass ich noch einmal meine Live-Berichterstattung aus dem Urlaub, egal auf welchem Kanal, überdenke. Was hast du mitgenommen, Michael? Was ist auf deiner Liste? Du fährst erst in einer Weile in deiner Auszeit.

Michael Münz: Sag es nicht, es dauert noch schrecklich lange. Für mich ist dieses WLAN-Thema das Ding. Ausgelöst durch die Erlebnisse, von denen ich erzählt habe, plus nach dem Gespräch heute, gucke ich noch einmal, ob das Netzwerk, in dem ich bin, wirklich sicher ist. Was mache ich eigentlich, wenn ich mich eingeloggt habe? Manche Sachen müssen nicht sein. Online-Banking oder solche Geschichten lasse ich besser bleiben. Auch dieser Punkt mit den Passwörtern, Karin, den du am Anfang erwähnt hast, dass ich mir überlege, welche Passwörter ich brauche. Ich würde darüber nachdenken, dass, wenn ich sie mitnehme, ich sie auch sicher mitnehme. Ich habe einen Passwort-Manager mittlerweile, aber man muss diese Passwörter auch nicht überall verteilen.

Ute Lange: Kein Post-it vorne in die Handyklappe hinein, wo sie alle drauf sind

Michael Münz: Mit der EC-Karte zusammen, wie früher die Euro-Schecks.

Ute Lange: Das habe ich alles schon gesehen. Es gibt erstaunliche Routinen, die Menschen sich angeeignet haben.

Karin Wilhelm: Ich mache noch einmal Werbung. Niemand sollte versuchen, sich alle Passwörter zu merken. Niemand sollte das versuchen, dafür sind es zu viele. Ich verstehe, dass man skeptisch ist bei Passwort-Managern, aber schaut es euch an. Es lohnt sich und es kann das Leben viel leichter machen. Man muss sich ein bisschen herein wühlen und sich

fragen: Was passt zu mir? Möchte ich meine Passwörter in der Cloud oder auf dem PC? Danach ist das Leben einfacher. Ich kann das nur empfehlen.

Ute Lange: Ich finde es klasse, dass du wieder dabei warst, diesmal auf der anderen Seite des Mikrofons als diejenige, der wir eine Menge Fragen stellen durften. Danke, dass du dir Zeit genommen hast, Karin. Wir wünschen dir und deinen Lieben eine tolle Auszeit am Meer, mit frischem Wind in den Haaren und wenig digitaler Beschäftigung. Hoffentlich bis zu einem nächsten Mal. Danke dir, Karin.

Karin Wilhelm: Vielen lieben Dank. Es war sehr schön bei euch, und ich hätte gar nicht aufgeregt sein müssen.

Michael Münz: So regelmäßig wie der Sommer kommt, wie Ute am Anfang sagte, kommt im August die Gamescom. Für uns auch immer wieder ein Anlass, über Gaming und Sicherheit zu sprechen. Das machen wir in der nächsten Folge auch. Bereitet euch darauf gedanklich vor und schickt uns gerne auch Fragen zu Themen, die ihr rund um das Gaming von uns beantwortet haben wollt. Wir freuen uns. Schickt uns Fotos und Fragen jederzeit an die bekannten Kanäle bei Mastodon, YouTube, Facebook und an die Mailadresse. Sie lautet podcasts@bsi.bund.de. Da alles hinschicken, Fragen, Fotos, Anregungen, Kritik auch. Einfach losschicken.

Ute Lange: Vielen Dank. Wir freuen uns immer, von euch zu hören, und passt gut auf euch auf. Habt einen schönen Sommer, cremt euch gut ein, wenn ihr in der Sonne seid, schützt eure Daten, und bis bald. Tschüss.