„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 13, 30.09.2021:

h4ppy b1r7hd4y – 1 Jahr Update verfügbar!

Moderation: Ute Lange, Michael Münz
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. Wir melden uns heute zum ersten Mal seit ganz, ganz langer Zeit wieder aus dem Bundesamt für Sicherheit in der Informationstechnik in Bonn.

Lange: Wir sind noch dabei, uns im Studio wieder einzurichten. Ehrlich gesagt ist es ziemlich aufregend gerade, hätte ich nicht gedacht.

Münz: Das hätte ich auch nicht gedacht. Wir haben jetzt die letzten Monate auch immer mit Rotlicht und so gearbeitet und wussten, dass wir jetzt aufnehmen. Aber jetzt zusammenzustehen in einem Raum, sich anzugucken und zu denken „Okay, das läuft jetzt alles und das rote Licht blinkt.“, das ist schon etwas anderes. Aber es ist schön. Ich freue mich, dass es geklappt hat und dann auch noch zur Geburtstagsfolge, wo hier alles angefangen hat.

Lange: Ein Jahr „Update verfügbar“! Das ist jetzt heute die 13. Folge. Ich freue mich.

Münz: Ich finde es auch super! Wenn ich so zurückdenke an die vergangenen zwölf Monate, da haben wir echt viele Themen gemacht. Gibt es eine Folge, gibt es ein Thema, Ute, das bei dir hängengeblieben ist? Bei welcher Folge denkst du „Die mochte ich am liebsten.“?

Lange: Ich fand alle Folgen spannend und interessant, da es für uns ja auch eine Reise ist, eine ganz neue Welt und ein neues Thema. Eine ist mir besonders in Erinnerung geblieben, allein wegen der Überschrift: die mit der Dirndl-Mafia, Onlineshopping. Diese Dirndl sind mir im Gedächtnis geblieben. Erstens finde ich Dirndl manchmal ganz nett und außerdem war das so ein Bild für all das, was im Onlineshopping schieflaufen kann. Da ging es ja um diese sogenannten Fakeshops, die aussehen wie echte Shops. Sie hauen unsereins, aber auch die Händler und Händlerinnen, übers Ohr, weil sich da jemand daraufsetzt und vorgibt, er würde etwas verkaufen, was es in echt tatsächlich gibt, aber bei dir kommt nichts an. Der Händler ist geschädigt. Dieses Bild „Die Dirndl-Mafia“, das ist wirklich eine Folge, die ich nicht vergessen habe.

Münz: Okay, das verstehe ich gut. Bei mir sind es zwei Folgen, die hängen geblieben sind. Die eine ist das Gespräch, welches wir mit Meike hatten zum Lagezentrum. Wie sie beschrieben hat, wie sie hinter einem Wasserfall sitzen und von da aus das ganze Internet im Blick haben, das fand ich sehr beeindruckend. Das war für das Gespräch total gut. Die andere war jetzt im Sommer mit Florian zum Thema Gaming. Das war super, weil Florian so ein total cooler Typ war, der beide Themen echt gut zusammengebracht hat – Gaming und Sicherheit. Es hat mir richtig gut gefallen und ich glaube, wir hätten noch stundenlang mit ihm sprechen können.

Lange: Ja, das fand ich auch sehr spannend – vor allen Dingen, weil er mehr als Gamer gesprochen hat und nicht als Sicherheitsexperte. Einerseits hat er selbst diese persönliche Erfahrung und ist in dieser Welt so versiert und zu Hause. Andererseits betonte er aber diesen Aspekt „Wie können wir Gamer und Gamerinnen dafür sensibilisieren, dass sie ihre Daten, ihre Konten etc. schützen?“. Denn es wird immer gefährlicher – in Anführungszeichen. Die Angriffe nehmen zu und selbst wir als normalsterbliche Verbraucher und Verbraucherinnen müssen zunehmend wachsamer sein.

Münz: Für die, die gerade zuhören, ist unsere Empfehlung, noch einmal ein bisschen herunterscrollen in den Folgen und die Folgen heraussuchen, über die wir gerade gesprochen haben, weil die uns besonders am Herzen liegen. Ansonsten, wenn ihr anderer Meinung seid, dann schickt uns auch gerne, welche eure Lieblingsfolgen aus den vergangenen zwölf Monaten waren, da sind wir auch sehr gespannt.

Lange: Weißt du, was mir jetzt noch einfällt? Es gab noch eine, die ich ganz spannend fand. Und zwar die Sonderfolge, die wir mit Anders gemacht haben zur Bundestagswahl und Datensicherheit im Hintergrund. Das fand ich insofern ganz bemerkenswert, weil wir nicht sehen, was da im Hintergrund alles läuft, was dazu dient, dass so eine Wahl dann auch digital sehr sicher wird, obwohl sie ja, wie wir wissen, sehr analog ist. Wir waren ja nun kürzlich alle im Wahllokal und haben unser Kreuzchen auf Papier gemacht. Aber Monate im Voraus wurde sehr sensibilisiert, auch gerade bei den Kandidaten und Kandidatinnen, bei den Parteien, bei sozialen Netzwerken. Und welche Freude er an seiner Arbeit hat! Das war die zweite Folge, bei der ich das Gefühl hatte, dass er das echt total gern macht. Das sprang so rüber im Gespräch, obwohl wir das Gespräch auch noch digital geführt haben und uns nicht angucken konnten. Das war echt sehr beeindruckend. Das ist mir auch im Gedächtnis geblieben.

Münz: Und die Lehren aus einem Jahr Podcast zum digitalen Alltag, was würdest du dazu sagen?

Lange: Ich bin dann wieder beim Fahrradhelm, also wie ich beim Fahrradfahren den Helm aufziehe – ich habe übrigens mittlerweile einen, wie du weißt – und wie ich beim Autofahren den Gurt anlege; oder auch die Wohnung, die ich abschließe, um mich abzusichern. Im analogen Leben habe ich doch mehr darüber erfahren und mache es auch mehr, dass ich mich in der digitalen Welt besser absichere und nicht ganz so sorglos mit den Dingen umgehe. Das ist eine Lehre.

Münz: Ich habe für mich festgestellt, dass ich zum einen mittlerweile sensibilisiert bin für Sicherheitsfragen. Ich bin viel unterwegs. Wenn ich dann im ICE sitze und denke „Muss ich jetzt wirklich über das Netz im Zug meine Kontodaten abfragen?“, bin ich jetzt vorsichtiger geworden. Über meinen Staubsauger-Roboter hatten wir auch gesprochen, bei dem ich mich ausdrücklich gegen einen entschieden habe, der über das Internet gesteuert werden kann. Gleichzeitig habe ich so eine Gelassenheit bekommen. Ich habe zum Geburtstag noch einmal Spam-E-Mails bekommen, wo versucht wurde, mich zu erpressen und worüber wir in der ersten Folge schon gesprochen hatten. „Ich habe dich mit der Videokamera deines Laptops gefilmt“, die lösche ich jetzt einfach. Ich denke, den Trick habe ich verstanden. Damit kommt man mir jetzt nicht mehr. Von daher habe ich jetzt, glaube ich, mehr Einblick in das, was machbar ist und wie ich mich dagegen schützen kann. Das heißt nicht, weil ich die nächste Frage schon antizipieren kann, dass ich alles mache, was tatsächlich geboten ist. Aber ich komm da schon ganz gut heran.

Lange: Ich stelle die Frage heute nicht, weil ich die jedes Mal stelle. Aber was du zu den Phishing-E-Mails gesagt hast, das stimmt auch bei mir. Ich klicke viele Sachen gar nicht mehr an, wo ich wahrscheinlich vor einem halben, dreiviertel oder einem Jahr gedacht hätte „Oh Gott, meine Bank schreibt mir, ich muss meine Sicherheitsvorkehrungen updaten“. Dann gucke ich auf die E-Mail und sehe, dass das nichts mit meiner Bank zu tun hat. Dann lösche ich das auch total beruhigt. Dann kommt das vielleicht zweimal am Tag wieder oder eine Woche später. Aber dann weiß ich, dass sie gerade wieder versuchen, irgendetwas bei mir abzufischen. Von daher ist es auch etwas, was man, glaube ich, mit ein bisschen Aufmerksamkeit relativ schnell erkennen kann. Und noch eine Sache, die ich gelernt habe, ist Datensparsamkeit. Das ist ja das Mantra des BSI. Aber das kann ich auch verstehen, so wenig wie möglich angeben und immer nur dann, wenn es wirklich nötig ist. Da bin ich ein bisschen zurückhaltender geworden.

Münz: Das klingt gut und deckt sich auch mit mir. Was du sagtest mit Phishingversuchen oder diese SMS-Wellen, die es ja auch gab mit „Dein Paket wird nicht rechtzeitig geliefert.“. Da habe ich auch verstanden und gucke lieber noch einmal genau hin. Wer ist der Absender? Wurden Umlaute verwendet? Wie ist die Formulierung? Ich habe auch wirklich viel mitgenommen aus dem vergangenen Jahr, muss ich ehrlich sagen.

Lange: Aber ich kann mich nicht zurückhalten. Ich muss die Frage jetzt doch noch einmal stellen. Und zwar stelle ich sie dir als eine Entweder-Oder-Frage. Was würdest du eher machen oder was wäre dir lieber? Einen Passwortsafe einzurichten oder alle deine Zwei-Faktor-Authentisierungen noch einmal neu zu machen?

Münz: Ich versuche gerade den Arbeitsaufwand abzuschätzen. Es ist nicht so, dass meine Passwörter nicht organisiert sind. Sonst würde ich im digitalen Alltag überhaupt nicht mehr klar kommen.

Lange: Aber auf Zetteln?

Münz: Ja, gut. Noch einmal zurück zur Frage, die du gestellt hast. Vernünftig wäre zu antworten: Passwort-Manager. Aber ich glaube, ich würde eher im Prozess der Zwei-Faktor-Authentisierung, den ich jetzt begonnen habe, weitermachen und mir die Einrichtung eines Passwort-Manager aufheben, wenn ich mal Zeit habe. Ich muss lachen, weil ich noch nicht genau weiß, wann das sein könnte. Aber ja, ich bin jetzt ein bisschen geschult durch die ganzen Politikerantworten von gestern, die ich nach der Wahl gesehen habe. Ich würde mal sagen „sowohl als auch", ein ganz klares „Jein". Dann drehe ich den Spieß um und frage dich: Würdest du lieber auf ein Jahr Internet oder ein Jahr Yogamatte verzichten?

Lange: Das ist ja keine Frage. Dann würde ich auf Internet verzichten. Du weißt, wie sehr ich Yoga liebe. Das ist eine knifflige Frage.

Münz: Denken wir mal darüber nach, was alles wegfällt.

Lange: Auch mein Online-Yoga fällt dann weg. Das ist eine fiese Frage.

Münz: Das hatte ich gehofft.

Lange: Lass mich darüber nachdenken, vielleicht habe ich bis zum Ende der Folge eine Antwort. Aber das ist eigentlich die Wahl zwischen Pest und Cholera. Ohne Internet ist man aufgeschmissen heutzutage.

Münz: Ja, finde ich auch.

Lange: Können wir das vertagen? Da habe ich jetzt keine Antwort darauf. Das ist echt nicht nett.

Münz: Das war der Sinn und Zweck dieser Übung. Ich erinnere dich noch einmal am Ende der Folge. Ich schreibe es mir gerade auf.

Lange: Wo wir jetzt zurückgeblickt haben, lass uns doch einmal nach vorne blicken. Wir haben jeden Monat eine Folge. Was würdest du denn gerne als Thema machen, was wir bisher noch nicht hatten?

Münz: Ich würde gerne etwas machen zum Thema „Keylogger", so heißen die, glaube ich. Das sind Anwendungen, die dir auf den Rechner gespielt werden und alles mitkriegen, was du machst. Ich wüsste gerne, was da geht, wie das auf meinen Rechner kommt, was solche Anwendungen mitschneiden können und was dann daraus passieren kann. Das, muss ich ehrlich sagen, finde ich auch eine ganz, ganz fiese Vorstellung, dass auf meinem Rechner etwas ist, was mitschreibt und sieht, was ich tue; und dass alle meine Passwörter, Webseiten und so weiter bei jemandem Dritten landen. Das finde ich echt fies. Da würde ich gerne wissen, wie ich mich davor schützen kann. Das ist die Spitze meiner Paranoia an der Stelle.

Lange: Gut, das finde ich ein spannendes Thema. Sollten wir tatsächlich in Erwägung ziehen.

Münz: Und du? Was würdest du gerne hier behandeln?

Lange: Wir haben oft über Hacker gesprochen. Ich würde so jemanden gerne einmal live vor dem Mikro haben und erfahren: Wie kommt man dazu? Wie lernt man das? Gibt es dafür eine Akademie? Ein Studium? Was ist der Reiz daran? Sind alle nur Bösewichte? Wir haben oft über diese ganzen Ransomware-Attacken, über das Blockieren von Systemen und andere Sachen gesprochen. Da möchte ich gerne jemanden vis à vis stehen haben und mit ihm oder ihr darüber sprechen. Das fände ich spannend.

Münz: Das finde ich auch gut. So einen Halunken? Wir haben tatsächlich über die Motivation von Hacken gesprochen - Erpressung oder diese Script Kids, die einfach mal gucken und probieren, was sie können. Vielleicht gibt es tatsächlich Leute, die für einen guten Zweck hacken. Das wäre natürlich auch interessant.

Lange: Schauen wir einmal! Wir hatten auch unsere Hörer und Hörerinnen, also euch da draußen, gefragt und haben ein paar Vorschläge bekommen, die wir ganz spannend finden. Wir wissen noch nicht, in welcher Reihenfolge und wie wir das hier berücksichtigen können, aber wir werden es auf jeden Fall aufnehmen. Da war zum Beispiel etwas zum Thema Ransomware dabei. Das ist ein großes Thema, welches wir immer mal wieder hier angesprochen haben. Bildung, also Datensicherheitsbildung, Informatik etc. fand ich auch ganz spannend. Was hast du auf der Liste?

Münz: Ich habe noch das Thema Datenlöschung. Wie löscht man Daten, so dass sie ganz weg sind? Du willst dein Handy oder deinen Laptop an jemand anderes verkaufen und dann willst du aber sicher sein, dass dann niemand deinen Passwort-Manager knackt zum Beispiel. Das wäre schwierig.

Lange: Dafür müsste man einen haben. Running Gag, lassen wir das.

Münz: Danke! Das Thema QR-Codes war auch noch mit dabei, das hat jemand eingesandt. Das fand ich auch spannend, weil ich mein Handy ja mittlerweile überall gegenhalte. Gelernt durch Testzentren, Veranstaltungseinloggen und so weiter. Den QR-Code scannen und dann ist gut! Das Thema Sicherheit bei QR-Codes hat jemand eingereicht. Fand ich auch spannend. Da müssen wir mal schauen, wie wir das aufgreifen können. Vielen Dank auf jeden Fall für die Einsendung. Das fanden wir gut und greifen wir bestimmt in irgendeiner Form demnächst auf. Jetzt kommt noch der Überblick zu den Themen, die noch geblieben sind, bevor wir ins Schwerpunktthema kommen.

Lange: Wir haben noch ein paar Themen, zum einen mit Blick auf die Folge von Anders, das Special zur Bundestagswahl. Da ist die Frage: Haben diese ganzen Bemühungen im Hintergrund tatsächlich dazu geführt, dass das alles sicher abgelaufen ist? Ich persönlich habe jetzt nichts gelesen, was für große Beunruhigung gesorgt hat. Wie ist das bei dir?

Münz: Ich war auch gespannt. Es gab tatsächlich ein paar Szenarien, wo man dachte, die zuvor gesammelten Daten würden vielleicht am Wahltag für Desinformation oder irgendwelche großen Kampagnen genutzt werden. Die eine oder andere Meldung zu „Warum ist die Wahlurne nicht richtig abgeschlossen?“ oder „Dieser oder jene Kandidat hat irgendetwas Dummes gemacht.“ gab es, aber ich habe jetzt nichts gesehen, wo ich gedacht

hätte, dass es eine ganze Wahl umschmeißen könnte. Es war, glaube ich, in erster Linie ruhig. Das muss man, genauso wie das Wahlergebnis, in den kommenden Tagen und Wochen noch einmal analysieren. Auf den ersten Blick habe ich auch gedacht, dass da nichtswar, was zu größerer Sorge hätte Anlass geben können.

Lange: Das war auch mein Eindruck. Es gab Angriffe, über die wir immer mal wieder gelesen haben – einzelne Abgeordnete mit Phishing-E-Mails. Aber die waren offensichtlich auch schon sehr, sehr sensibel und gut gebrieft. Da ist nichts passiert, was das Ergebnis insgesamt in Frage stellen müsste.

Münz: Was witzig ist, ist ein ganz anderes Thema. Was ein witziger Zufall ist, dass, wo wir jetzt hier zusammenstehen, das neue Digitalbarometer in dieser Woche erscheint. Ich weiß noch bei der ersten Folge von „Update verfügbar“ war das Digitalbarometer auch die Grundlage unserer Arbeit. Da ist es natürlich spannend zu gucken, wie sich die Zahlen verändert haben. So wie es aussieht, hat sich bei der Schätzfrage, die ich dir in der ersten Folge gestellt habe, nicht viel getan. Die Frage war damals „Wie viele Privatanwender sind von Cyberkriminalität betroffen?“. Es waren 25 Prozent im Digitalbarometer 2020, also jeder Vierte. Die Zahl hat mir ein Vögelchen zu gezwitschert. Die Zahl ist offensichtlich gleich geblieben. Was neu ist oder auffällig ist, dass in der Altersgruppe der 19- bis 29-Jährigen, also derjenigen, die so gerade geschäftsfähig werden...

Lange: „Flügge“ geworden sind, um bei dem Vögelchen zu bleiben.

Münz: Genau! Da ist der Wert, dass jeder Dritte betroffen ist von Cyberkriminalität. Also in dieser Altersgruppe, 19 bis 29 Jahre, sind mehr Leute von Cyberkriminalität betroffen.

Lange: Da wäre es interessant, den Hintergrund zu erfahren. Ich spekuliere jetzt einmal. Die sind wahrscheinlich, im Vergleich zu anderen Altersgruppen, noch viel digitaler unterwegs; und mit einer größeren Selbstverständlichkeit als vielleicht die Menschen am anderen Ende der Skala, die wir normalerweise Senioren und Seniorinnen nennen. Aber das ist jetzt eine Spekulation. Das kann man nachlesen, denn das Digitalbarometer ist veröffentlicht und auf den Seiten des BSI zu finden. Wer mehr darüber wissen möchte, wir verlinken das in den Shownotes.

Münz: Das würde ich auch vorschlagen. Ich schaue auf jeden Fall mal rein, weil da wirklich viel Interessantes in den letzten Jahren dabei war. Mal gucken, wie sich die Zahlen verändert haben.

Lange: Und wer überhaupt Lust auf mehr Cyber-Sicherheit hat, der kann sich auf den Seiten des BSI auch das Programm von dem ECSM angucken. Das ist der „European Cyber Security Month“. Das ist eine Sensibilisierungskampagne der Europäischen Union und findet jedes Jahr im Herbst statt. Ich habe mal geguckt. Da gibt es ein Wahnsinns-Programm, bundesweit, zu unterschiedlichen Themen. Für den Alltagsgebrauch, für Firmen, für Unternehmen, für Hochschulen etc. Wer jetzt Lust hat, ist herzlich eingeladen. Auch das verlinken wir in den Shownotes, um sich und sein Umfeld noch ein bisschen datensicherer zu machen.

Münz: Prima! Dann kommen wir zu dem Thema, was wir jetzt ein bisschen ausführlicher besprechen wollten. Wir haben uns angeguckt, auf welchem Gerät, ihr, liebe Hörerinnen und Hörer, uns am meisten. Und die Antwort ist: Mobiltelefon.

Lange: Sehr naheliegend, weil man es überall mitnehmen kann. Ich fühle mich gerade nackig, muss ich ehrlich sagen. Wenn wir hier ins Studio ins BSI kommen, dann müssen wir unsere Geräte abgeben, weil hier alles abgesichert ist. Und jetzt kann ich bestimmte Dinge gerade nicht tun.

Münz: Aber es ging mir genauso, weil zum einen hatte ich mir die fiese Frage, auf die wir noch zu sprechen kommen, aufs Handy geschickt, damit du die im Vorfeld gar nicht erst siehst. Ich wollte dann ein bisschen hier scrollen, während du nicht guckst. Aber das geht jetzt nicht. Ich musste sie mir tatsächlich merken, was auch eine Herausforderung ist. Zum anderen war das Licht aus dem Studio so schön, dass ich dachte „Oh, das muss ich erst einmal fotografieren, um es auf meinem Instagram-Account zu posten". Hosentaschen leer, ich habe kein Handy. Es sind tatsächlich immer solche Schreckmomente, wo ich denke, ich habe wirklich etwas Wichtiges vergessen. Ich habe alles auf dem Telefon außer meinen Hausschlüssel. Ohne Handy funktioniert es bei mir nicht. Ich könnte nur mit Handy durch die Gegend fahren und hätte alles dabei, außer meinen Hausschlüssel.

Lange: Wo du Schreckmoment sagst: Du erinnerst dich, dass letztes Jahr im Sommer mir meine Tasche geklaut worden ist. Das war weniger schön und der Schreckmoment war: Wo ist mein Handy? Es war Gott sei Dank in dem Moment, wo es passiert ist, auf meinem Tisch vor mir. Ich wäre total aufgeschmissen gewesen, weil nur da meine ganzen Infos sind. Ich merke mir fast nichts mehr. Früher konnte ich jede Telefonnummer auswendig. Jetzt ist die da gespeichert. Lass uns deswegen mal gucken, was wir berücksichtigen müssen, wenn wir ein Smartphone mit uns herumtragen, was ja auch ein Gerät ist, was Eintrittspunkte bietet für Datenklau und andere Sachen. Womit fangen wir an? Was müssen wir als Allererstes machen, wenn wir das richtig sicher machen wollen?

Münz: Also womit fangen wir an? Bei mir ist es die Touch-ID. Ich habe bei meinem Handy eingerichtet, dass mein Daumenabdruck bzw. die Abdrücke von mehreren Fingern dafür sorgen, dass das Handy entsperrt wird. Der Grund ist, dass ich es meistens mit rechts mache. Wenn ich aber auf dem Fahrrad schnell etwas nachgucken muss, dann nehme ich es mit der linken Hand raus. Deswegen habe ich den linken Daumen genommen, um das Handy zu entsperren. Aber ich trage einen Helm. Es ist nicht so, dass ich komplett unvorsichtig bin.

Lange: Das geht jetzt in eine andere Sicherheitsfrage, ob du auf deinem Fahrrad auf dein Handy gucken solltest. Das habt ihr alle nicht gehört. Kein Beispiel, dem wir folgen sollten. Aber Touch-ID oder Gesichtserkennung, das habe ich mich im letzten Jahr häufiger gefragt, denn ich habe die Gesichtserkennung nicht drin. Meine Schwester hat es zum Beispiel. Wenn sie dann die Maske auf hat, funktioniert das natürlich nicht. Auf jeden Fall sollte man das Smartphone so absichern, dass man eine Sperre im Handy hat über PIN oder über biometrische Daten, damit niemand außer einem selbst das Handy öffnen kann.

Münz: Das Touch-ID habe ich zum Teil auch für einzelne Apps noch einmal eingerichtet. Weil ich einfach sicher sein will, dass niemand zum Beispiel beim Onlinebanking meine Zahlen gucken kann, oder bestimmte Chat-Verläufe wirklich nur für mich sichtbar sind. Wo es geht, mache ich das einfach.

Lange: Also doppelte Sicherheit?

Münz: So gut wie, genau.

Lange: Der Name des Podcasts ist Programm: Updates, Updates, Updates. Wenn eins verfügbar ist, auch bei den Apps auf dem Smartphone auf jeden Fall machen.

Münz: Ja, das habe ich auch gelernt. Ich gucke da wirklich. Wir hatten, glaube ich, schon einmal darüber gesprochen, dass ich so jemand bin, der gerne kontrolliert, wann die Updates kommen. So ist es auch weiterhin. Ich gucke wirklich regelmäßig nach, ob es irgendetwas Neues gibt – nicht nur auf dem Handy, sondern auch bei anderen Geräten, wie dem Laptop. So kann ich sicher sein, dass alle Sicherheitslücken, die gerade bekannt sind, auch bei mir schnell geschlossen werden. Das gilt auch fürs Handy. Ich bin in einem Betriebssystem gefangen mit meinem Mobiltelefon und weiß, dass die Apps, die ich da herunterladen kann, auch aus einer Quelle kommen; dass sich schon jemand darum gekümmert hat, dass das schon alles seine Richtigkeit hat. Aber es gibt auch Betriebssysteme, wo man sich von anderen Quellen Apps herunterladen kann. Da würde ich sagen: besser nicht.

Lange: Vertrauenswürdige Quellen sind, glaube ich, das Stichwort, egal welches Betriebssystem du hast. Es gibt noch den Moment, wo man vielleicht von seinem Smartphone Dinge auf ein anderes Gerät übertragen will und einen Stick oder etwas ähnliches braucht. Man sollte natürlich sicher sein und wissen, was man dafür nutzt, und dass man auch den Rechner kennt, auf den man das bringt; nicht irgendwo bei irgendjemandem. Es ist ja sowieso keine gute Idee, dass ich Leute Sticks in meinen Rechner hineinstecken lasse, wenn ich nicht sicher bin, ob die nicht irgendetwas darauf haben, was ich nicht installiert haben will und umgekehrt.

Münz: Ich war einmal bei einer Konferenz. Ein Flugzeugbauer erzählte, dass er immer wieder Leute trifft, die sagen „Ach, ich habe gerade einen USB-Stick, kann ich den bei dir kurz dranstecken?“. Er sagte, dass er niemanden irgendetwas in seinen Rechner stecken lässt. Das gilt auch fürs Telefon. Nichts an einen Rechner stecken, den man nicht kennt! Da kann man sich vielleicht doch noch etwas einfangen.

Lange: Dann haben wir noch einen Tipp. Du hast das eben schon kurz erwähnt und ich bin manchmal auch im Zug versucht, Dinge zu tun, für die ich gerade Zeit habe. Das sind öffentliche Netze, bei denen ich nicht sicher sein kann, ob meine Daten nicht irgendwo anders landen. Du hast glaube ich Kontodaten im Zug genannt. Ich bin schuldig im Sinne der Anklage, wenn ich Zeit habe beim Zugfahren, dann mache ich relativ viel Bürokram, weil ich manchmal sonst nicht dazu komme. Das ist nicht die beste Idee, das in öffentlichen Netzen zu machen. Gerade wenn man sensible Daten abruft und verschickt oder etwas organisiert, sollte man hundertprozentig sicher sein, dass es nicht irgendwo anders landet.

Münz: Ich will dir jetzt keine Angst machen, aber ich war tatsächlich mal auf einem Barcamp, wo wir interessanterweise auch noch bei meinem Arbeitgeber in so einem großen Veranstaltungssaal saßen.

Lange: Ich kenne den Saal, ich weiß, welchen du meinst.

Münz: Alle Teilnehmer waren in diesem Netz, in diesem WLAN, was da angeboten worden ist. Mittendrin stand ein junger Mann auf, hielt seinen Laptop hoch und sagte „Ich wollte euch nur sagen, ich habe jetzt hier alle Daten abgefischt, die durch das WLAN gehen". Dann kam der zu mir und zeigte mir im Klartext das Passwort, mit dem ich gerade erst meine E-Mails abgerufen hatte.

Lange: Okay, ein besseres Beispiel, um das zu lernen, gibt es kaum.

Münz: So viel zu „öffentliche Netze". Es ist eine Grauzone, was der junge Mann da gemacht hat.

Lange: Ist das vielleicht der Hacker, den wir hier vor das Mikro bringen könnten? Der weiß offensichtlich, wie das geht. Der kann dann aber auch sagen, wie man das vermeidet.

Münz: Das hoffe ich doch. Das war wirklich ein Moment, wo ich dachte „Okay, im Klartext sogar". Er konnte das wirklich abschreiben. Das ist natürlich echt schwierig. Die Vorstellung, dass wirklich jemand in einem Zug so ein Logging-Programm mitlaufen hat, finde ich wirklich gruselig.

Lange: Genau. Also nur in Netzen unterwegs sein, wo wir sicher sind, dass die Daten nicht irgendwo anders hin verschwinden. Ich finde, dass ein super wichtiger Tipp ist, auch mit meinem Erlebnis letztes Jahr im Sommer, mein Gerät nicht aus den Augen zu lassen. Erstens, damit es nicht ganz entwendet wird. Zweitens, damit nicht jemand, wie in manchen Filmen, es einfach einsteckt, ein Programm installiert, vielleicht etwas abruft, was mir nicht lieb ist, weil es eher privater Natur ist. Also, Blickkontakt mit deinem Smartphone!

Münz: Hatten wir schon über Zwei-Faktor-Authentisierung gesprochen, auch bei Smartphones, beziehungsweise bei Apps?

Lange: Nein, das darfst du aber gerne. Das scheint ja dein favorisiertes System zu sein.

Münz: Auf jeden Fall! Ich habe immer mehr Apps, wo ich für die Zwei-Faktor-Authentisierung, wenn es machbar ist, die Einstellungen entsprechend vornehme. Da kriege ich zusätzlich zum Einloggen auf eine Webseite noch eine SMS geschickt, die ich dann zusätzlich eingeben muss. Das gibt mir zumindest ein gutes Gefühl. Wenn ich schon an der einen oder anderen Stelle nicht ganz so up-to-date bin, was die Sicherheitsvorkehrungen angeht, habe ich zumindest da das Gefühl „Okay, ich logge mich hier ein und erhalte noch eine E-Mail oder eine SMS". Das ist ein ganz hilfreiches System, was dazu beiträgt, dass dadurch mehr Sicherheit ist als ohne.

Lange: Du hast vorhin gesagt „Daten löschen“. Das wäre ein Vorschlag gewesen von einem unserer Hörer. Das ist auch noch ein Tipp, wenn man etwas verkauft oder hergibt, dass man wirklich sicherstellt, dass alles so gelöscht ist, dass niemand mehr darankommt. Sonst hast du vielleicht auch Türen und Tore geöffnet, weil du etwas gespeichert hast, was noch nutzbar ist und man kommt auf deine anderen Daten. Ich find das sind schon mal ganz handfeste Tipps. Gerade für Menschen wie uns, die sich ohne dieses Ding ein bisschen nackig fühlen. Wer mehr wissen will, kann auch beim BSI auf der Webseite noch mal schauen. Verlinken wir in den Shownotes!

Münz: Einen Tipp habe ich aber noch. Und zwar das Thema Backups. Ich glaube, das wird bei Telefonen manchmal vergessen. Zumindest bei dem Telefon, was ich habe, kommt ein Cloud-Speicher mit dazu. Der ist relativ schnell voll und da muss man sich überlegen: Will ich dafür Geld bezahlen? Will ich dafür kein Geld bezahlen? In der Regel, behaupte ich mal, entscheiden sich Kunden und Kundinnen dagegen, dafür Geld auszugeben. Als ich ein neues Handy bekommen habe und es darum ging, von dem alten die Daten herüberzuziehen, habe ich gedacht „Ach komm, kauf dir für zwei Euro im Monat mehr Speicherplatz, schiebe die Daten von dem alten in die Cloud und dann zurück aufs Neue“. Das war ganz gut. Mittlerweile weiß ich es sehr zu schätzen, dass zum Beispiel Fotomaterial oder Videos noch irgendwo anders gelagert sind als auf dem Gerät, welches mir ehrlich gesagt noch drei bis fünf Mal am Tag herunterfällt. Zum Glück nicht vom Fahrrad! Ich habe gerade zum Beispiel eine Reihe von Videointerviews gemacht, die dann wirklich nur auf dem Handy sind. Sobald ich in einem WLAN bin, in einem sicheren WLAN…

Lange: Wichtiger Zusatz!

Münz: …lade ich das Zeug in die Cloud hoch und weiß. Wenn mir das Handy jetzt herunterfällt, dann ist das Material trotzdem da. Das wäre echt doof, wenn mir das verloren geht. Ich glaube, das betrifft auch ganz viele andere Daten, die man auf dem Handy hat. Das ist einfach ein gutes Gefühl, wenn man weiß, die sind nicht nur dort, sondern auch auf einem anderen Gerät oder eben in der Cloud.

Lange: Das stimmt. Das hatten wir für Computer schon einmal mit den regelmäßigen Backups auf eine andere Festplatte oder eben in die Cloud. Dass einem das nicht passieren kann, wenn das Gerät herunterfällt oder etwas anderes passiert.

Münz: Ich glaube jetzt ist noch einmal ein guter Moment, um auf meine fiese Frage von vorhin zu sprechen zu kommen.

Lange: Ich habe immer noch keine Antwort, weil es wirklich wie Pest und Cholera ist. Ich meine, ich könnte Yoga auch ohne Matte machen. Wenn wir uns darauf einigen, dann Internet und Yoga ohne Matte.

Münz: Okay, das Schlupfloch hatte ich dir tatsächlich gelassen. Dann lasse ich das mal durchgehen.

Lange: Okay, ich werde aber noch einmal länger darüber nachdenken. Ich glaube, wir können das Ganze jetzt abschließen. Wie sagt man? It is a wrap? Tipps und Tricks zum Smartphone haben wir einige geteilt. Und sich noch einmal freuen, ein Jahr „Update verfügbar“! Wieder im Studio! Ich fühle mich total wohl, es hat Spaß gemacht.

Münz: Absolut! Ich finde es einen echten Mehrwert. So schön die Folgen auch waren und die Gespräche, die wir mit den Kolleginnen und Kollegen aus dem BSI hatten. Aber zusammenzustehen und ein bisschen zu quatschen bei Leitungswasser und Kaffee ist schon total gut. In jedem Fall!

Lange: Und wenn ihr mehr von „Update verfügbar“ und uns und unserer Freude erfahren möchtet, dann hört uns doch auch beim nächsten Mal wieder zu oder liked und folgt uns auf euren präferierten Podcast-Plattformen. So verpasst ihr keine Folge oder könnt auch noch mal zurückhören, falls ihr noch nicht von Anfang an dabei seid.

Münz: Und wie immer gilt: gerne kontaktieren. Wir haben uns sehr gefreut über die Anregungen zu dieser Folge, zum Geburtstag und die Themenwünsche. Macht das auf jeden Fall weiter! Das war echt toll! Geht am besten über die Kanäle auf Facebook, Instagram, Twitter oder auf YouTube! Oder per E-Mail geht es auch! Das ist die E-Mailadresse: bsi@bsi.bund.de.

Lange: Ganz analog: Grüße! Wir freuen uns auch jedes Mal über eure Post, eure Hinweise, euer Feedback. Und bis wir uns wieder hören, alles Gute!

Münz: Alles Gute! 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