„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 08, 31.05.2021:
Update verfügbar! Der Name ist Programm

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

Lange: Michael, was ist das denn für ein Geräusch?

Münz: Was?

Lange: Hallo? Was ist da los?

Münz: Ich höre dich nicht so gut, Ute. Was sagst du?

Lange: Kein Wunder! Was ist das für ein Geräusch? Mach mal leise!

Münz: Ja, gleich. Mache ich sofort. Warte mal kurz! Ich habe es gleich.

Lange: Hallo? Wir wollen einen Podcast aufnehmen. Das geht so nicht!

Münz: Ja, ist gut! Stopp! Alles klar! Warte! So, jetzt müsste das Geräusch weg sein, richtig?

Lange: Und was war das bitte?

Münz: Das war mein Staubsaugerroboter, von dem ich das letzte Mal erzählt habe.

Lange: Du hast dir einen gekauft?

Münz: Ich habe mir einen gekauft und ich finde den mega.

Lange: Mit WLAN-Schnickschnack und rotem Teppich von der Arbeit und allem Drum und Dran?

Münz: Genau nicht, weil mich diese ganze WLAN-Geschichte nach unserer letzten Folge so beschäftigt hat, dass ich mich dafür entschieden habe, einen Staubsaugerroboter zu kaufen, der nicht im WLAN ist, sondern einfach nur eine Zeitsteuerung hat. Das heißt, der macht sauber, wenn ich nicht da bin, aber nicht, weil ich ihm das von unterwegs sage, sondern weil ich ihm die Zeit mitgegeben habe, wann er gefälligst seine Arbeit verrichten soll. Wenn ich dann wiederkomme, ist hier sauber. Super gut! Echt!

Lange: Aber euer Timing war heute jetzt nicht so gut, weil wir ja eine Podcastfolge aufnehmen sollen.

Münz: Ja, gut. Ich würde mal sagen, dass das jetzt noch die anfängliche Begeisterung über das Gerät ist. Es ist schön, wenn jemand die Arbeit macht, die eigentlich bei mir liegt. Beim nächsten Mal – ich verspreche es – lasse ich es bleiben.

Lange: Okay, gut! Können wir jetzt anfangen?

Münz: Wir können jetzt anfangen. Der Staubsaugerroboter ist zurück in seiner Ecke, lädt und lässt uns jetzt in Ruhe.

Lange: Gut, dann tun wir das doch!

Lange: Hallo und herzlich willkommen zu „Update verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Ich bin Michael Münz. Wir melden uns auch in diesem Monat wieder nicht aus dem Bundesamt für Sicherheit in der Informationstechnik, sondern corona-bedingt noch einmal aus unseren Home-Offices.

Lange: Wir haben ein paar Themen mitgebracht, über die wir heute sprechen möchten. Das erste Thema kommt von dir, Michael. Du hast während der letzten Folge ein „Update verfügbar“-Signal bekommen, das dich ein bisschen irritiert hat. Erzähl doch mal!

Münz: Ja, das stimmt. Wir haben in der letzten Folge nicht nur über meinen Roboter gesprochen, sondern über Datenabsaugen und wie das alles passieren kann, dass man persönliche Daten vielleicht an falschen Stellen ins Netz angibt. Während wir die Folge aufgenommen haben, bekam ich von einem Musikerportal, wo ich angemeldet bin, die Nachricht, dass meine Daten wahrscheinlich im Netz aufgetaucht seien. Die Seite heißt Reverb und ist eine Seite, auf der man Musikinstrumente verkaufen kann. Ich kaufe dort manchmal Plugins und Programme zum Musikmachen. Von dieser Seite hat ein IT-Experte eine Datenbank im Netz gefunden, die die Namen, Adressen, Telefonnummern, E-Mail-Adressen und auch die PayPal-Adressen von allen 5,6 Millionen Nutzern enthielt. Meine sind dabei. Das ist auch für mich ärgerlich, aber es sind zum Beispiel auch die Daten von bekannten Musikern dabei, aus Bands wie Black Sabbath oder Smashing Pumpkins oder Nine Inch Nails. Die gute Nachricht ist, dass in diesem Datensatz keine Bezahlinformationen enthalten sind. Aber ich habe trotzdem erst einmal mein Passwort geändert. Auch wenn die Daten jetzt wieder aus dem Netz sind, ist es trotzdem so, dass man mit dem, was verfügbar war, ganz gute Phishing-Aktionen starten kann. Wenn man so viele Informationen hat, kann man sich schnell als jemand anderes ausgeben und Geschäfte anbahnen, die nicht gut gemeint sind.

Lange: Wir hatten beim letzten Mal über diesen Facebook-Datenklau gesprochen. Da lag das eigentliche Problem schon Jahre zurück, aber die Daten sind erst jetzt aufgetaucht. Du bist

auch einer von den 533 Millionen Nutzern, die betroffen sind, wie du erzählt hast. Das heißt, wenn die Daten einmal draußen sind, weiß man auch nicht genau, wer die abgefischt hat.

Münz: Ja, genau.

Lange: Und bist du gleich zwei Mal betroffen. Das ist auch nicht so schön.

Münz: Mal gucken, wann ich den Hattrick reiße.

Lange: Da wir Facebook noch einmal erwähnt haben, wird dich interessieren, dass es in Irland eine Organisation gibt, die die Firma mit einer Sammelklage auf Schadensersatz verklagen möchte. Denn es ist genau das Problem: Was ist mit den Daten passiert, die vor Jahren geleakt wurden? Ich habe gelesen, dass die Datenschutzgrundverordnung, die nicht immer so beliebt ist, das auch her gibt.

Münz: So eine Klage ist auf Grundlage der Datenschutzgrundverordnung möglich?

Lange: Genau! Aber es wird wahrscheinlich Jahre dauern, weil es ein langer Prozess werden kann. Andererseits haben jetzt ganz viele, die sich daran beteiligen, und auch die Organisation die Hoffnung, dass die Firmen durch solche Klagen ein bisschen sensibler mit unseren Daten umgehen. Denn wenn es tatsächlich zu einer Verurteilung käme, würde es die Firma auch Geld kosten. Das ist wahrscheinlich nicht so erwünscht.

Münz: Verstehe! Ich werde mir das auf jeden Fall einmal anschauen und beobachten. Vielleicht ergibt sich auch für eine der kommenden Folgen daraus noch eine Erkenntnis, wie solche Klagen behandelt werden und was damit passiert. Das wäre vielleicht ganz spannend. Obwohl ich bei Reverb und bei Facebook dabei war, war ich nicht beim Datenleck von Gorillas dabei. Das ist dieser Fahrradlieferdienst, den es jetzt in mehreren Städten gibt. In Berlin sehe ich die auch manchmal. Die sind schwarzgekleidet, hinten steht Gorillas drauf. Die liefern Lebensmittel aus, wenn man die online bestellt. Von mehr als 200.000 Kunden von Gorillas waren Adresse und Name im Netz abrufbar. Das ist schwierig. Denn wenn solche Daten auftauchen, kann es sein, dass jemand anderes in meinem Namen etwas bestellt und ich dann Sachen bezahlen muss, die ich gar nicht haben wollte.

Lange: Und vielleicht auch teurere Sachen als einen Salat für abends!

Münz: Zum Beispiel! Das kann gut sein! So etwas ist echt nicht ungefährlich und bietet vor allem Kriminellen gute Möglichkeiten, mit den Daten Schindluder zu treiben.

Lange: Das ist eigentlich auch ganz spannend. Wir haben das letzte Mal über Datenlecks gesprochen und irgendwie scannt mein Hirn offensichtlich die Nachrichten jetzt ausgerechnet nach so etwas. Ich habe noch etwas anderes gelesen. Es geht nicht immer nur um Dienstleister oder große Firmen, die wir jetzt schon erwähnt haben, sondern es hat auch eine Partei erwischt. Es gibt eine Wahlkampf-App von der CDU, mit der sie die Aktivitäten ihrer Wahlkämpfer und Wahlkämpferinnen dokumentieren können: Wo war jemand? Mit wem hat er gesprochen? Waren die positiv gestimmt? Sind die für ein weiteres Gespräch

bereit? Möchten die vielleicht Infomaterial? Eine IT-Expertin, eine Softwareentwicklerin, hat sich diese App einmal angeschaut und festgestellt, dass sie zu all diesen Informationen Zugang hatte.

Münz: Ach?

Lange: Sie hat keine böse Absicht gehabt. Sie hat das nur berufsmäßig gecheckt, ob das alles sicher ist. Sie hat das dann dem BSI und dem Datenschutzbeauftragten in Berlin gemeldet. Die Partei hat diese App jetzt erst einmal vom Netz genommen. Aber das zeigt, wie brisant dieses Thema ist: Wenn wir unsere Daten nicht schützen, wenn die Hersteller von solchen Apps oder anderen Programmen das nicht schützen, können Daten schnell in der Welt sein – gerade solche sensiblen Daten, wie deine politische Einstellung oder wie du zu bestimmten Themen stehst. Das ist sehr persönlich. Ich würde nicht wollen, dass das von jedem eingesehen werden kann.

Münz: Der Fall ist auch insofern bemerkenswert, weil es nichts ist, was ich selbst eingegeben habe, sondern was eine dritte Person über mich eingetragen hat. Wenn ein Wahlkämpfer jetzt bei mir klingeln würde und ich mit dieser Person diskutiert hätte, dann würde er Michael Münz, die Adresse und vielleicht noch was über meine politischen Ansichten in die App schreiben. Das heißt, nicht nur ich muss mit dem, was ich mit meinen Daten mache – wo ich sie hinterlasse, vorsichtig sein, sondern ich muss mich auch darauf verlassen können, dass andere mit meinen Daten gut umgehen. Sonst tritt das auf, was du auch gesagt hast. Dann tauchen meine Daten auch ohne mein Zutun im Netz auf. Das ist natürlich echt nicht gut und richtig. Daher ist der Fall auch bemerkenswert. Jetzt vielleicht nochmal eine Überleitung zu einem Fall, den ich noch kurz zum Abschluss erklären oder erzählen wollte: Wenn wir über solche Sachen reden, dann geht es oft um Kriminelle oder was die damit tun wollen. Aber es gibt auch Fälle, wo es gar nicht darum geht, Daten für solche Zwecke zu nutzen, sondern manchmal suchen Leute auch Daten oder Datenlecks, einfach weil sie es können und wollen. Es gab vor zwei Jahren mal ein großes Datenleck. Das hieß das Orbit Datenleck, weil jemand, der sich Orbit nannte, Anfang Januar 2019…

Lange: War das mit den Politikern und Promis, die dann plötzlich ihre Daten im Netz gefunden haben? Das war so eine Adventskalender-Aktion. Da wurde jeden Tag etwas Neues veröffentlicht.

Münz: Genau die Nummer! Nur in diesem Fall hat der es gemacht, weil er es machen konnte. Der hat die Daten zusammengesucht – vielleicht aus Apps wie aus dieser Wahlkampf-App oder vielleicht auch aus anderen Quellen zusammengesucht, wo Dinge im Netz standen, die da nicht hätten stehen sollen. Er wollte einfach nur zeigen, dass er es kann – wahrscheinlich auch, um sich in der Szene ein bisschen Aufmerksamkeit zu verschaffen.

Lange: So eine Art Mutprobe? Hier bin ich. Ich bin super.

Münz: Ja, genau! Die Motive für solche Datenklaus sind ganz vielfältig und führen auch dazu, dass ganz viel passieren kann. Das sollte man nicht außer Acht lassen, wenn man Daten irgendwo eingibt oder auch eingeben lässt.

Lange: Was sagen uns jetzt denn all diese Beispiele? Wie gehen wir am besten damit um?

Münz: Immer gucken, wo man seine Daten hingibt! Es ist nicht nur wichtig, wo ich sie selbst eintippe, sondern auch wem ich sie sage. Ansonsten gilt: starke Passwörter für jeden Dienst und auch gern mal wechseln, damit auch der Zugang zu meinen eigenen Daten schwierig ist.

Lange: Weißt du, was mir noch einfällt? Ein Passwort für ein Programm! Nicht einmal ein super Passwort ausdenken und dann auf alles darüberlegen! Denn wenn das Passwort kompromittiert ist, hast du wieder ein Problem. Dann ist die Tür weit offen. Dann kann jeder – in Anführungszeichen – in deine Wohnung spazieren.

Münz: Das stimmt, das auf jeden Fall! Starke und verschiedene Passwörter für jeden Dienst, den man hat! Skepsis bei E-Mails – Stichwort Phishing, was wir hier schon öfter erwähnt haben! Die Informationen, die darinstehen, müssen nicht zwangsläufig von der Person sein, von der die E-Mail vorgibt zu sein. So authentisch die auch klingen mag! Genau genommen ist das nichts Neues. Das ist auch der Grund, warum der Podcast so heißt, wie er heißt, nämlich „Update verfügbar“. Es geht darum, dass man Updates von Apps oder Software einspielt, damit darin womöglich enthaltene Sicherheitslücken geschlossen werden.

Lange: Genau zu dem Thema sind von unseren Hörern und Hörerinnen Vorschläge gekommen. Wir hatten eingeladen, uns zu sagen, worüber wir in der nächsten Folge sprechen sollen. Ein Wunsch war tatsächlich Updates und wie man damit umgeht und worauf man achten sollte. Den erfüllen wir jetzt heute. Erst einmal Danke an diejenigen, die uns diese Rückmeldung gegeben haben. Wir haben diese gern aufgenommen. Ich dachte, wir fangen noch einmal ganz von vorne an: Warum gibt es eigentlich Updates? Ich bin auch schuldig im Sinne der Anklage, denn ich bin auch manchmal genervt, wenn etwas aufpoppt und ich gerade keine Zeit dafür habe. Ich bin dann ein bisschen irritiert, weil ich nicht weiß, ob das jetzt wichtig ist oder nicht und ob ich das jetzt sofort machen muss. Eine wichtige Botschaft ist, dass es die Updates nicht gibt, um uns zu ärgern – auch wenn sie mitten in der Aufnahme eines Podcasts auf dem Rechner erscheinen. Die sind mittlerweile viel, viel wichtiger als Firewalls oder Virenschutzprogramme. Das allein reicht nämlich nicht. Man muss gucken, dass die Programme immer aktuell sind. Es gibt verschiedene Gründe, warum die manchmal nicht aktuell sind. Sicherheitslücken haben wir schon besprochen: dass jemand tatsächlich Zutritt zu deinem Wohnzimmer bekommt – sprich zu deinen ganzen Daten und deinen Geräten. Aber es gibt auch immer mal Fehler, wenn die Software programmiert wird. Das ist menschlich. Wir machen auch Fehler, wie du heute Morgen mit deinem Sauger. Das war die falsche Zeit, um so etwas auszuprobieren.

Münz: Ich bin auch nur ein Mensch.

Lange: Genau, und Programmierer und Programmierinnen auch! Manchmal sind es aber gar keine Fehler, sondern wir Anwender und Anwenderinnen sind manchmal sehr kreativ und nutzen Programme anders, als es ursprünglich gedacht war. Dann wird nachgebessert. Manchmal werden Anwendungen auch komfortabler für uns gemacht. Es gibt Updates, wenn zum Beispiel Rückmeldungen kommen, dass das nicht funktioniert oder weniger nutzerfreundlich ist. Es gibt zwei Varianten bei den Sicherheitslücken. Die eine ist schon bekannt, weil ganz viele Leute schon betroffen sind. Wir haben sehr viele Fälle bereits erwähnt. Dann finden die Hersteller in der Regel ziemlich schnell eine Lösung und man sollte unbedingt sofort updaten. Dann gibt es noch eine Variante, über die ich bisher gar nicht nachgedacht habe. Wenn zum Beispiel die Softwareentwicklerin das BSI oder andere Behörden über die Wahlkampf-App informiert und die dann wiederrum die Hersteller oder die programmierenden Firmen von diesen Anwendungen informieren, dann wird ein Hinweis gegeben, dass es jetzt ein Update gibt, um mögliche Sicherheitslücken zu schließen. Das ist dann auch wieder das Einfallstor für Leute, die vielleicht nicht nur gute Absichten haben. Für mich klingt das ein bisschen wie ein Hase und Igel Spiel zwischen Hackern und Herstellern.

Münz: Daran habe ich auch gerade gedacht.

Lange: Es gibt eine Lücke. Entweder ist sie schon bekannt und wird ausgenutzt oder es gibt eine, die noch nicht bekannt ist. Aber in dem Moment, in dem sie bekannt wird, fangen die Kriminellen an zu überlegen, wie sie diese ausnutzen können. Das heißt, gerade bei Sicherheitsupdates ist es sehr empfehlenswert sie sofort zu machen, damit wir nicht dazwischen geraten.

Münz: Das ist Hase und Igel zwischen Hacker und Programmierer und wir Nutzer und Nutzerinnen sind auch noch mit dabei. Das heißt, wenn ich mir die Lösung, die die Hersteller schnell anbieten, nicht installiere und das Rennen mitlaufe, dann stehe ich trotzdem dumm da, obwohl es ein Update gibt.

Lange: Ja.

Münz: Das klingt tatsächlich nach einem nicht endenden Wettlauf.

Lange: Das wird auch immer schneller und deswegen gibt es auch immer öfter Updates. Ehrlich gesagt, bin ich für mich aufmerksamer geworden, seitdem wir diesen Podcast hier machen. Ich habe das Bild, dass ich meine Wohnung auch verschließe, wenn ich sie verlasse. Das ist eine Art Routine, da ich nicht möchte, dass meine Wohnung sperrangelweit aufsteht und sich jeder bedienen kann. So ähnlich ist es auch bei meinen Daten. Im Zweifelsfall gefährde ich nicht nur mich, sondern auch andere, zum Beispiel durch Phishing-Aktionen, die dann gestartet werden, oder durch meinen Backofen, der Teil eines Botnetzes werden könnte – wie beim letzten Mal besprochen. Die Vorstellung verfolgt mich! Danke für das Bild!

Münz: Du hattest vorhin einen Punkt erwähnt, den ich noch einmal aufgreifen wollte. Updates wollen gar nicht nerven. Aber es gibt durchaus Situationen, in denen automatische

Updates auch in einem doofen Moment kommen. Ich weiß noch: Ich habe mal vor Jahren in einem Club aufgelegt. Es war zwei oder drei Uhr morgens und irgendwann fing der Ton des Rechners, mit dem ich Musik gemacht habe, ein bisschen zu haken und zu poltern an. Nach einer Viertelstunde kam auf einmal das Fenster, auf dem stand, dass das Windows Update jetzt fertig sei.

Lange: Ein super Moment dafür!

Münz: Auf jeden Fall! Ich könnte mir vorstellen, dass man manchmal bei automatischen Updates ein bisschen überrumpelt ist, wenn sie einen zu einem ungünstigen Zeitpunkt erreichen. Hattest du nicht auch mal so etwas in der Art?

Lange: Ja, aber ich will gar nicht darüber reden. Ich habe nicht realisiert, dass es ein Betriebssystem-Update ist. Ich habe es angeklickt, weil ich jetzt sehr wachsam bin. Dann hat das 50 Minuten gedauert. Der Kurs, den ich an dem Tag online geben sollte, kam immer näher und näher und mein Rechner war noch nicht betriebsbereit. Auch deswegen finde ich den Vorschlag von unseren Hörern und Hörerinnen, sich damit noch einmal zu beschäftigen, spannend. Auch nochmal zu gucken, wie man damit umgehen kann! Im Fall von Windows gibt es jetzt den Patchday. Am zweiten Dienstag jeden Monats versorgt Microsoft sein Betriebssystem und weitere Programme, die darunter laufen, mit Updates. Das sind dann nicht nur Fehler, die behoben werden oder Anwendungen, die verbessert werden, sondern vor allen Dingen geht es oft um Sicherheitslücken. Das heißt, darauf kann man sich auch einstellen. Man hat es im Hinterkopf: zweiter Dienstag jeden Monat. Anhand unserer Beispiele sollte man vielleicht nicht dann unbedingt Aktualisierungen durchführen, wenn man gerade Musik auflegt wie du vor Beginn eines Trainings steht wie ich. Das war minderschlau, um es einmal offen zu sagen. Aber es gibt Regelmäßigkeiten. Das haben auch andere Hersteller von anderen Betriebssystemen. Dann gibt es die Koppelung von Computer und mobil bei manchen Betriebssystemen. Wobei es die mobile Anwendung für Smartphones bei Windows seit letztem Jahr wohl nicht mehr gibt. Es gibt keinen Support mehr. Man muss sich überlegen, ob das noch eine gute Wahl für ein Gerät ist, wenn man überhaupt nicht mehr updaten kann, weil es dann vielleicht noch weiter ausgenutzt wird.

Münz: Ich bin iOS Nutzer, um mal den Bogen von Desktop zu mobil zu schlagen. Sprich, ich habe ein iPhone, mit dem ich arbeite und telefoniere und alles Mögliche mache. Da ist es wirklich so, dass ich ständig darauf hingewiesen werde, dass es Updates gibt: nicht nur von Apple, die ein Update ihres Betriebssystems zur Verfügung stellen und wollen, dass ich es herunterlade, sondern auch die ganzen Apps, die ich habe, werden ständig aktualisiert. Immer blinkt irgendwo eine eins oder eine Zahl, die mir den Hinweis gibt, dass ich gefälligst wieder ein Update für die App installieren müsste. Ich habe das eine Zeit lang automatisch gemacht. Aber dann bin ich zwei, drei Mal auf die Nase gefallen, weil entweder ein Update in so einer Situation kam, in der ich die bestimmte App gerade brauchte, oder ich nach dem Update beim Start der App meine Passwörter neu eingeben musste und ich die gerade nicht parat hatte.

Lange: Ich sage nur, dass Passwortmanager auch auf mobilen Geräten funktionieren. So hast du sie immer dabei.

Münz: Ja, aber ich wollte jetzt gerade sagen, wie ich zum Beispiel vor einem Mietfahrrad stand und zu einem Termin losfahren wollte. Die App wollte aber nach der Neuinstallation das Passwort von mir haben. Ich musste dann zu Fuß laufen und habe meinen Termin gerade so noch erreicht. Deswegen verzichte ich auf automatische Updates. Ich weiß, wir predigen etwas anderes. Dafür gucke ich ein, zwei Mal die Woche diese Liste der Apps durch, die ich aktualisieren muss und mache das dann mit der Hand. Damit komme ich ganz gut klar.

Lange: Das ist doch vielleicht auch ein ganz guter Tipp für unsere Hörer und Hörerinnen. Man sollte sich einen Überblick verschaffen, über das, was man hat. Ich installiere auch mal wild eine neue App, weil sie irgendwie schick aussieht, und dann brauche ich sie nie. Das heißt, ich räume bei mir regelmäßig auf. Wenn ich irgendwie das Gefühl habe, dass der Bildschirm nicht mehr für den ganzen Kram reicht, den ich installiert habe, und ich mich an manche Sachen auch gar nicht erinnern kann, dann nehme ich sie wieder herunter und brauche mich auch nicht um Aktualisierungen zu kümmern. Aber so eine Übersicht ist gut, wo es automatisch passiert-. Meistens wird es nachts installiert. Dadurch ist es sehr nutzerfreundlich, es sei denn, dass man eine Nachteule bei der Arbeit ist. Aber das kann man vielleicht auch noch anpassen. Du hast heute auch wieder ein bisschen länger gearbeitet. Das hast du vorhin erzählt.

Münz: Genau.

Lange: Aber wenn man das manuell macht, kann man sich das vielleicht auch aufschreiben, damit man nicht den Überblick verliert. Ich habe für mich mittlerweile das Motto, dass weniger mehr ist. Manche Sachen sind gerade im Hype und dann probiert man das mal aus. Wenn ich die dann zwei, drei Wochen gar nicht nutze, lasse ich es wieder. Dann nehme ich sie auch wieder herunter, weil mich das auch ein bisschen entlastet. Sonst habe ich so ein bisschen das Gefühl von ‚fear of missing out' – kurz ‚FOMO'. Das sind Drohungen, gegen die man auch mal angehen muss.

Münz: Das stimmt.

Lange: Jetzt haben wir über die beiden Systeme gesprochen, die wir gut kennen. Wir haben vielleicht auch Leute, die uns zuhören, die andere Systeme nutzen.

Münz: Das stimmt.

Lange: Darüber musste ich mich ein bisschen schlauer machen.

Münz: Das hast du bestimmt auch, so, wie ich dich kenne.

Lange: Zum Beispiel wird man bei Android auch informiert, wenn es Updates für das Telefon oder für das Gerät gibt. Es gibt auch regelmäßig diese Sicherheitspatches für verschiedene Smartphones. Aber ich wusste nicht, ist, dass es unterschiedliche Zeitpunkte gibt, wer wann

wie upgedatet wird. Es gibt zunächst die Geräte, die Google selbst herstellt. Dann folgen die Geräte von den Vertragspartnern. Und dann gibt es Geräte von anderen Herstellern, die vielleicht nicht direkt im unmittelbaren Umfeld sind. Da kann es tatsächlich sein, dass jemand, der ein Google Gerät hat, ein Update bekommt, während andere, die andere Geräte haben, das vorherige Update noch gar nicht haben. Das wusste ich gar nicht, denn bei mir passiert das alles relativ automatisch. Manche Hersteller machen das auch nicht monatlich, sondern immer, wenn es gerade dran ist. Das kann in unterschiedlichen Rhythmen sein. Aber ich nehme an, dass Nutzer von diesen Geräten und diesen Betriebssystemen das auch im Blick haben. Und wenn nicht: Ich habe mich auf der Seite vom BSI schlau gemacht. Dort kann man sich das noch einmal angucken. Wenn man zum Beispiel ein Linux Gerät hat, mit dem ich mich auch nicht so auskenne, findet man dort Informationen dazu.

Münz: Okay, in Ordnung! Das habe ich kapiert. Aber dass die Updates bei Android unterschiedlich getaktet sind, finde ich interessant. Denn bei iOS kommt es tatsächlich mehr oder weniger zeitgleich, wenn Apple ein neues Update verteilt. Wie ist es denn dann? Mein Eindruck ist, dass ich Geräte wie Windows oder IOS länger habe. Ich habe das Gefühl, dass das auch nichts macht, wenn ich die länger habe. Dann kommen in den meisten Fällen weiterhin regelmäßig Updates. Wie ist das denn bei Android? Wenn ich mir mal so ein Gerät kaufe, kann ich mir dann auch sicher sein, dass die Sicherheitsupdates in der Zeit kommen, in der ich das Handy besitze?

Lange: Nein, es scheint noch ein bisschen anders zu sein. Der Updatezyklus ist meistens nach drei Jahren vorbei.

Münz: Okay.

Lange: Dann bist du ein bisschen auf dich selbst gestellt. Das ist dann echt nur etwas für Experten. Ich habe das mir von meiner persönlichen IT-Abteilung, von meinem Neffen, auch noch einmal erklären lassen. Es gibt Möglichkeiten an dem Handy ein bisschen herumzuarbeiten und es praktisch für die Zukunft fit zu machen. Aber das sollte man nur tun, wenn man sich super damit auskennt, denn dabei kannst du es auch kaputt machen.

Münz: Okay.

Lange: Dann ist die Frage: Wenn ich mir ein Gerät kaufe, bei dem ich zwei, drei Jahre später keine Updates mehr bekomme, wäre das auf den ersten Blick vielleicht eine günstige Anschaffung, aber auf den zweiten Blick vielleicht doch teurer. Wenn du ständig neue Geräte kaufst, ist das nicht unbedingt so nachhaltig.

Münz: Wo du gerade günstige Anschaffung sagst: Es gab doch einmal vor ein paar Jahren diesen Fall, wo man in einem Elektrosupermarkt günstige Android Handys kaufen konnte. Hinterher kam heraus, dass die gar nicht mehr aktualisiert wurden. Du hast darauf ein Betriebssystem gehabt, was nicht mehr aktualisiert werden konnte.

Lange: Zum Zeitpunkt, wo du es gekauft hast, war es im Grunde genommen schon out?

Münz: Ja, so war das. Es konnte nicht mehr aktualisiert werden. Das BSI hatte dann einen Testkauf gemacht und konnte tatsächlich Handys kaufen, die nicht mehr upgedatet werden. Die Verbraucherzentrale NRW wollte vor Gericht erstreiten, ob Verkäufer in Supermärkten oder Elektromärkten darauf hinweisen müssen, dass man ein Gerät kauft, das nicht mehr aktualisiert werden kann. Das hat ein bisschen gedauert. Das Oberlandesgericht in Köln hat dann entschieden, dass der Markt das nicht kennzeichnen muss. Meine Empfehlung beim Kauf eines solches Gerätes wäre, auf den Preis zu achten. Der Grund, warum ein Gerät so günstig ist, könnte vielleicht auch daran liegen, dass es schon längst jenseits aller Sicherheitsüberlegungen ist. Dann investiere ich vielleicht lieber etwas mehr Geld und habe ein Gerät, was über einen längeren Zeitraum sicher ist und aktualisiert wird.

Lange: Okay. Das hast du ganz schön beschrieben – als guten Hinweis für die Zuhörer und Zuhörerinnen da draußen. Ich weiß aber, dass du beim Auflegen einen dermaßen antiquierten Computer benutzt. Wie erklärst du das jetzt?

Münz: Gesunder Menschenverstand, würde ich jetzt gerne sagen! Aber darüber kann man wahrscheinlich streiten. Nach meiner Erfahrung, dass mein Windows Rechner nachts ein Update fahren wollte, habe ich gedacht, dass ich umsteige. Ich lege jetzt mit einem Mac auf. Bei dem ist auch die Tonqualität besser. Nachdem ich vor nahezu fünf Jahren diesen Mac eingerichtet habe, habe ich den nie wieder ins Netz gelassen. Denn: Never change a running system! In meinem Falle läuft der tadellos und macht problemlos Musik. Ich will nichts ändern. Ich will nicht, dass irgendein Update irgendwelche Toneinstellungen verändert. Deswegen ist das Gerät im Zustand von 2016. Ich trage im Prinzip eine kleine Zeitkapsel mit mir herum, die super gut funktioniert, aber gar nicht weiß, dass wir schon 2021 haben. Das ist eigentlich auch ein ganz schönes Gefühl. Da bin ich mir auch sicher, dass das keine Gefährdung für Daten oder fürs Musikmachen oder für weitere Anwendungen ist. Das ist der Hintergrund, dass ich das Schätzchen noch weiter mit mir herumtrage.

Lange: Okay! Dann ist es eine sehr überlegte Entscheidung. Das kann auch für jeden, der sich lange überlegt, wie er das macht, okay sein. Ähnlich wie du entschieden hast, dass dein Staubsaugerroboter nicht ins WLAN kommt, damit er nicht noch Daten absaugt, während er bei dir den Fußboden saubermacht. Das ist total okay.

Münz: Genau! Diese Updateüberlegung sollte man letztendlich auch bei jedem Gerät vornehmen, das man kaufen will. Das gilt für Staubsauger genauso wie für Jalousien oder Heizungsthermostate oder auch Türöffner. Ich wollte nur noch einmal erwähnen, dass man sich die Gedanken macht. Wenn man sich eine Anschaffung vornimmt, kann man sich auch beim BSI nochmal ein paar Informationen holen, worauf man achten soll. Es gibt eine Broschüre zum Internet der Dinge – Haushaltsgeräte, die ans Netz angeschlossen sind. Die Publikation ist jetzt auf der Webseite. Die kann man auch herunterladen. Den Link packen wir in die Shownotes. Da können unsere Hörer und Hörerinnen das noch einmal nachlesen. Vielleicht gibt es noch Fragen? Dann kann man die uns auch gern senden. Darauf greifen wir gern zurück.

Lange: Bevor wir unsere ganzen Daten, und wie man uns erreichen kann, angeben, wollte ich noch kurz aus persönlichem Anlass auf eine Anregung von unseren Hörern und Hörerinnen eingehen. Jemand fragte, ob wir nicht mal über Messenger-Dienste und Datensicherheit sprechen könnten.

Münz: Okay.

Lange: Und kaum ausgesprochen bei uns angekommen, fing bei mir im Freundes- und Familienkreis das Bäumchen Wechsel Dich Spiel mit den Messenger-Diensten an. Es gab die große Diskussion über WhatsApp und Datenschutz. Ich glaube, Mitte Mai war der Stichtag. Ich bekomme noch heute nahezu täglich Hinweise, dass die Personen jetzt da und da sind und da nicht mehr sein möchten. Das wird für mich gerade ein bisschen unübersichtlich. Ich habe mittlerweile sieben Messenger-Dienste auf meinem Phone. Ich weiß nicht mehr genau, mit wem ich wo rede. Und manchmal schicke ich noch aus alter Gewohnheit in dem alten Chat Nachrichten. Aber so langsam sortiert es sich. Ich weiß gar nicht mehr – entweder habe ich es beim BSI oder woanders gelesen, aber den Tipp fand ich total hilfreich, gerade wenn man in Gruppen unterwegs ist: Ich habe die Gruppe von meiner Yogaausbildung. Ich habe die Gruppe von meinen besten Freunden. Ich habe die Familiengruppe. Es kommen noch ganz viele andere Gruppen dazu. Mit einigen von denen habe ich mich jetzt kurz ausgetauscht. Wenn es jemanden in der Gruppe gibt, der sagt, dass er hier nicht mehr sein will und frägt, wo wir denn hingehen können, dass wir uns dann gemeinsam verständigen, wohin wir wechseln. So bin ich mit allen der Gruppe auf diesem anderen Messenger-Dienst – mittlerweile gibt es ja eine ganze Reihe von Möglichkeiten – und muss immer zwischen der Gruppe und Individuum hin und her wechseln. Das macht es nämlich für mich unübersichtlich. Ich weiß nicht, wie es bei dir ist. Hast du jetzt auch schon so ein kleines Sortiment? Bei mir ist das wie ein Blumenstrauß an Messenger-Diensten, den ich jetzt zur Verfügung habe.

Münz: Ja, habe ich auch. Tatsächlich ist es eine Eigenart von Menschen, dass sie bestimmte Kommunikationskanäle bevorzugen. Es war schon vor dieser WhatsApp Diskussion der Fall, dass ich einen Bekannten hatte, der lieber SMS mochte. Mit einem anderen habe ich über Threema geschrieben. Aber ein Großteil der Kommunikation läuft über WhatsApp und ein bisschen den Facebook Messenger. Und ich habe bei WhatsApp tatsächlich auch ein paar Hinweise von Leuten bekommen, die sich abgemeldet und gesagt haben, dass sie nur noch über einen anderen Dienst erreichbar seien. Es ist so ein bisschen wie bei einer Party. Die Party bei dem einen Anbieter ist nur mittelmäßig gut, aber da sind wenigstens alle Leute. Wenn man zu der anderen Party geht, fühlt man sich dort vielleicht wohl, aber man steht dort allein herum und fragt sich, wo denn alle geblieben sind.

Lange: Dann ist es mit dem Wohlfühlen auch bald vorbei.

Münz: Ja, genau. Insofern finde ich deinen Hinweis zum Umziehen über Gruppen eigentlich eine ganz gute Idee. Denn das hilft, dass ganze Herdenbewegungen oder Völkerwanderungen losgetreten werden. Das ist eigentlich auch eine ganz gute Entwicklung,

dass man nicht mit jedem Kontakt einzeln darüber diskutieren muss. Finde ich gut! Das werde ich mir auch mal überlegen.

Lange: Ich weiß nicht, wie es dir geht. Aber seit ich diesen Podcast mache, gelte ich als Datensicherheitsexpertin. Ich finde das ein bisschen übertrieben, denn ich bin hier auch nur in einer großen Lernkurve. Ich habe mir noch einmal angeguckt, worauf man achten kann oder sollte, wenn man sich für eine Messenger App entscheidet. Vertrauenswürdigkeit des Anbieters. Wie vertraue ich dem Anbieter? Das kann individuell unterschiedlich sein. Was man aber auch berücksichtigen sollte, wenn man Wert auf seine Privatsphäre legt, ist, dass es in unterschiedlichen Ländern unterschiedliche Gesetze zum Schutz dieser Privatsphäre gibt. Da sollte man sich ein bisschen schlau machen und für sich ein Gefühl entwickeln, ob das okay für mich ist oder nicht. Es gibt da unterschiedliche Ansichten. Wichtig ist aber auch noch einmal zu berücksichtigen, dass ich meist weitreichende Rechte vergebe, wenn ich mich irgendwo anmelde – zum Beispiel ein Zugriff auf meine ganze Kontaktliste. Wollen denn die Menschen in meiner Kontaktliste, dass ich das so weitergebe? Das ist eine Frage, die mich auch mittlerweile mehr beschäftigt. Sollten die Nachrichten verschlüsselt sein? Nicht, dass dann die ganze Welt mitliest! Das wollen wir sowieso schon nicht, wenn wir uns privat unterhalten wollen – dass zum Beispiel die ganze U-Bahn mithört. Kann ich Kontakte blockieren oder tue ich das auch, wenn sie mir komisch vorkommen?

Münz: Oder Anfragen stellen zur Kommunikation? Anfragen von Leuten, die du nicht kennst!

Lange: Genau! Du wirst irgendeiner Gruppe hinzugefügt und kennst niemanden in der Gruppe. Wie kommen die auf dich? Nicht so beliebt, aber manchmal auch hilfreich ist es, die Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen anzugucken und nicht einfach nur drauf zu klicken und zu sagen, dass ich alles akzeptiere. Denn ich weiß dann gar nicht, was ich alles akzeptiert habe und was im Zweifelsfall mit meinen Daten passiert.

Münz: Nur dass ich jetzt nicht den falschen Eindruck bekomme: Wie oft machst du das? Wie konkret guckst du dort hinein?

Lange: Nein, das sagen wir jetzt nicht öffentlich!

Münz: Okay!

Lange: Aber ich bin aufmerksamer geworden.

Münz: Ich wollte doch nur mein Gewissen beruhigen.

Lange: Wir wollen dafür sensibilisieren. Und ich merke, dass ich in den letzten Monaten dafür sensibler geworden bin. Und wenn wir das bei anderen auch vermitteln können, dann sind wir am Ende alle ein bisschen besser geschützt. Das ist das Hase und Igel Spiel. Vor allem ist das ein Domino Spiel. Wenn ich auf meine Daten nicht achte, dann gefährde ich vielleicht auch die Daten von anderen. Aber das sind nur ein paar Tipps für Messenger-Dienste. Es gibt noch mehr auf der Webseite des BSI. Und ich habe die Überlegung präsentiert, wie man damit umgeht, dass es so große Angebote gibt. Es sollte die auch die

Frage beantwortet werden, wo ich das Gefühl habe, guten Gewissens meine Gespräche verschlüsselt, sicher und in einem Umfeld führen kann, mit dem ich gut leben kann. Das ist auch eine wichtige Frage.

Münz: Ja, das ist doch ein schönes Schlusswort.

Lange: Es gibt nicht ‚one size fits all'.

Münz: Ja, genauso wie wir alle Individuen sind, um das Leben des Brian zu zitieren. Genau, das ist ein schönes Schlusswort für diese Folge. Dann können wir mal gucken, was wir für die nächste Folge vorbereitet haben.

Lange: Was machen wir beim nächsten Mal?

Münz: Wir haben einen Kollegen aus dem Lagezentrum des BSI zu Gast, der uns über seine Arbeit erzählt. Ich bin schon sehr gespannt auf die eine oder andere spannende Anekdote, die ich mir im Hintergrund ein bisschen geheimdienst-mäßig vorstelle.

Lange: Ich bin gespannt, ob sich diese Vorstellung erfüllt.

Münz: Apropos Hintergrund: Ich wollte das nur noch einmal verifiziert wissen. Die Geräusche im Hintergrund sind nicht in meinem Kopf? Die sind vor deiner Haustür?

Lange: Die sind gerade vor meiner Haustür. Das ist natürlich im Home-Office eine der Herausforderungen, wenn man vorm Mikro steht.

Münz: Gut, dass wenigstens mein Staubsauer aus ist.

Lange: Ich konnte die Baustelle bei der Stadt leider nicht abbestellen.

Münz: Oder einfach zurück in die Ecke schicken, so wie ich meinen Staubsauger am Anfang der Folge!

Lange: Nein, das war hier nicht möglich. Damit leben wir jetzt gerade. Aber wir sind sowieso schon am Ende.

Münz: Ja.

Lange: Wir weisen nochmals darauf hin, dass Sie uns auf Spotify, Deezer, Google und iTunes hören können. Abonnieren Sie uns. Mögen Sie uns. Schicken Sie uns Rückmeldungen. Wir freuen uns sehr über Ihre Tipps und Erfahrungen für den digitalen Alltag, aber auch über Hinweise, mit welchen Themen wir uns beschäftigen sollen.

Münz: Du hast jetzt die Kanäle genannt, aber man kann uns auch über Facebook, Instagram, Twitter, YouTube und die E-Mail-Adresse bsi@bsi.bund.de kontaktieren. Es gibt genügend Wege uns zu erreichen. Wir greifen Ihre Hinweise oder Fragen super gerne auf. Das hilft uns dabei, auch selbst noch einmal zu gucken, was es mit dem einen oder anderen Thema auf sich hat und wie ich mich selbst im digitalen Alltag schützen kann.

Lange: Und weil es hier jetzt sehr laut wird, sage ich schon mal Tschüss und bis zum nächsten Mal! Bleiben Sie gesund und uns gewogen! 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/

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