„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 41, 28.03.2024

Moderation: Ute Lange, Michael Münz
Gast: Miriam Ruhenstroth, mobilsicher.de
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

Michael Münz: Und mein Name ist Michael Münz und in der heutigen Folge gibt es Tipps für das Gerät, das überall mit euch hingeht und mehr von euch weiß als sonst jemand in der Welt, nämlich euer Mobiltelefon.

Ute Lange: Hand aufs Herz, wann habt ihr das Betriebssystem eures mobilen Gerätes zuletzt aktualisiert? Ich frag doch gleich mal dich, Michael. Wann?

Michael Münz: Ich weiß, das klingt jetzt so, als hätte das mit der Aufnahme zu tun gehabt. Ich habe tatsächlich gestern mein Betriebssystem aktualisiert, weil mein Handy gesagt hat, es gibt etwas Neues. Ich habe gesehen, da sind neue Emojis drin. Die muss ich natürlich haben. Ich habe aber auch in der Beschreibung gesehen, dass da sicherheitsrelevante Updates mit drin sind, und da kann ich als Moderator von „Update verfügbar“ natürlich nicht „nein“ sagen, wenn ich sowas bekomme.

Ute Lange: Sehr vorbildlich. Denn genau um diese Updates geht es in dieser Folge. Es ist nämlich immer noch nicht selbstverständlich, dass jedes Mobilgerät, das da draußen in der Welt unterwegs ist, regelmäßig auf den neuesten Sicherheitsstandard gebracht wird. Warum das ein Problem ist oder für euch und für uns eins werden könnte und was sich bald ändern wird, darüber sprechen wir heute mit unserem Gast.

Michael Münz: Wenn ihr „Update verfügbar“, regelmäßig folgt, habt ihr vor etwa zwei Jahren vermutlich auch schon mal die Sicherheitseinstellung in eurem Handy genauer geprüft und Sicherheitseinstellungen verschärft, denn da haben wir das erste Mal mit unserem heutigen Gast gesprochen. Vielen Dank, dass du noch einmal da bist und uns von eurer Arbeit erzählst, die ihr beim gemeinnützigen Institut für Technik und Journalismus macht und uns Sicherheitstipps gebt, die wir sonst vielleicht nicht bekommen hätten.

Miriam Ruhenstroth: Ja, na klar gerne. Also erstens vielen Dank für die erneute Einladung. Ich freue mich natürlich auch sehr, noch mal hier zu sein. Mein Name ist Miriam Ruhenstroth, und ich leite das Projekt mobilsicher.de. Das ist eine Informationsplattform für Nutzer und Nutzerinnen wie du und ich, auf der wir alles besprechen rund um Sicherheit und Datenschutz und inzwischen auch längere Haltbarkeit für Smartphones und in dieser Rolle bin ich heute hier.

Ute Lange: Das freut uns sehr. Für uns beide ist es ja quasi undenkbar, dass Geräte im Einsatz sind, deren Betriebssysteme nicht mehr upgedatet werden. Nicht umsonst heißt der Podcast eben „Update verfügbar“, und wir haben das Mantra, dass man da immer drauf achten soll. Kannst du uns mal erklären, von wieviel Geräten wir eigentlich sprechen? Also um was geht es da, wenn wir über Mobiltelefone sprechen und deren Betriebssysteme?

Miriam Ruhenstroth: Also wie viele Geräte jetzt im Gebrauch sind, das weiß ich gar nicht genau. Meine letzte Statistik, die ich im Kopf habe, ist, dass jeder Deutsche inzwischen eines hat, und was aber die interessantere Zahl vielleicht ist, ist, dass neben den Geräten, die wir so benutzen, auch noch um die 200 Millionen Geräte in Deutschland in den Schubladen herumliegen und nicht genutzt werden oder vielleicht nach einem Jahr wieder rausgekramt werden. Und diese Geräte sind für unser heutiges Gespräch vielleicht auch ganz interessant. Wenn es dann um die Frage geht, sind die eigentlich noch sicher? Kann man die noch benutzen? Kriegen die noch Updates?

Michael Münz: Ja, man kennt ja den Fall von: „Ach, bei meinem Neffen, ist das Handy kaputtgegangen, hat nicht noch mal jemanden ein Handy über?“ Dann mache ich die Schublade auf und sage: „Hier Junge, ich tue dir mal was Gutes, du kriegst mein altes Handy.“ Solche Geräte.

Miriam Ruhenstroth: Ja, solche Geräte.

Ute Lange: Kürzlich erst gehabt, Michael. Danke, dass du das mit uns teilst Michael.

Michael Münz: Wir sind ja auch im digitalen Alltag ganz nah dran an den Lebenserfahrungen unserer Hörerinnen und Hörer. Von daher dachte ich, nenne ich das mal als Beispiel.

Miriam Ruhenstroth: Zu den Zahlen zum Betriebssystem gibt es aber auch noch eine ganz interessante Info. Abgesehen davon, wie viele Handys es tatsächlich gibt, haben wir Zahlen dazu, wie groß der Anteil ist von aktuellen oder nicht aktuellen Betriebssystemen, die genutzt werden. Ich habe gerade nochmal nachgeschaut, vor der Aufnahme hier, und es ist besser geworden. Wir beackern das Thema schon seit acht Jahren, und es war schon viel, viel katastrophaler. Je nachdem welche Statistik man guckt, 65 bis 70 Prozent benutzen ein aktuelles Android, also nicht das aktuellste, aber eins, was zumindest noch irgendwelche Updates von Google bekommt. Der Rest benutzt eins, dass keine Updates mehr bekommt.

Ute Lange: Wo wir jetzt die ganze Zeit Updates sagen, können wir noch mal kurz gucken, über welche Art von Updates wir sprechen. Warum sollte ich die denn machen? Für welche Funktionen sind die denn gut? Also warum könnte es denn überhaupt schlimm sein, wenn ich für mein Handy gar keine Updates mehr fürs Betriebssystem bekomme? Damit wir das noch mal einordnen.

Miriam Ruhenstroth: Das waren jetzt einige Fragen, die gar nicht so einfach zu beantworten sind: “Von welchen Updates sprechen wir überhaupt?“. Also, da sitzen wir schon immer an unseren Texten, wenn wir das erklären wollen, weil das gar nicht so einfach ist. Also grundsätzlich sprechen wir vom Betriebssystem, also Android oder IOS und nicht von den einzelnen Apps, da können wir später nochmal dazu kommen. Die müssen auch aktualisiert werden. Aber bei dem Betriebssystem, gerade bei dem Android-Betriebssystem, das in Deutschland häufiger vorkommt als die anderen, gibt es halt verschiedene Arten von Betriebssystem-Updates. Manche kommen von Google und manche kommen vom

Hersteller, und das sind die sogenannten Sicherheitsupdates, und von denen sprechen wir eigentlich. Es geht um das, was im Menü, wenn man in die Einstellung geht, unter Sicherheitsupdates zu sehen ist.

Michael Münz: Dazu noch eine Nachfrage. Das heißt, wir sprechen auch davon, dass ich von einem Hersteller ein Gerät kaufe, und dieser Hersteller versorgt mich mit dann mit Updates?

Miriam Ruhenstroth: Genau, das ist eine ganz wichtige Frage. Von wem kriege ich die Updates überhaupt? Und deswegen habe ich das jetzt so ein bisschen aufgedröselt, weil das ist, genauso wie du es sagst, Michael. Die Sicherheitsupdates, die muss der Hersteller liefern, weil sie auf das einzelne Modell angepasst werden müssen. Jetzt gibt es sozusagen noch eine Ebene drüber, Updates die auch das Android-Betriebssystem betreffen, die aber nicht ganz so tief an die Bauteile gehen. Die kann Google auch liefern, und die kommen oft ein bisschen länger. Aber diese Sicherheitsupdates, die muss der Hersteller liefern, und der kann das entscheiden, ob er das macht oder nicht, und das ist das Problem.

Michael Münz: Und bei IOS ist es so, da ja Betriebssystem und Telefon vom selben Hersteller sind, sprechen wir da nur von einer Institution sozusagen, die die Updates schickt.

Miriam Ruhenstroth: Genau. Genauso ist es.

Ute Lange: Okay, nun wollen ja aber Menschen freie Wahl haben, welche Geräte sie sich kaufen, und sind jetzt vielleicht trotzdem gerade verunsichert. Gilt das denn auch für mein Gerät? Woran erkenne ich, dass das Betriebssystem meines Gerätes nicht mehr upgedatet wird, also dass ich es zwar noch benutzen kann, aber wenn es um diese Sicherheitseinstellung und andere Dinge geht, der Hersteller mir nichts mehr anbietet? Wie erkenne ich das?

Miriam Ruhenstroth: Da muss man nachgucken. Man muss tatsächlich aktiv in die Geräteeinstellung gehen und am besten dort ins Suchfeld Update …nee, am besten Android eintippen, und dann findet man, welche Android-Version aktuell installiert ist. In diesem Menüpunkt findet man auch, von wann das letzte Sicherheitsupdate ist. Da steht ein Datum, und auf dieses Datum kommt es an. Es kommt nicht darauf an, wann ich das bekommen habe, sondern von welchem Datum es ist. Wenn dieses Datum ein Jahr alt ist, dann ist sehr wahrscheinlich, dass dieses Gerät keine weiteren Updates mehr bekommen wird. Also, ihr seht schon, es ist auch so ein bisschen Kristallkugel gucken, weil man nie weiß, kommt das nächste noch oder nicht. Das sagen einem die Hersteller auch mal nicht, und man muss so ein bisschen raten.

Michael Münz: Und es hilft offenbar ja nicht, dass ich meinen Nachbarn frage, von wann sein Update ist, weil, wenn er das Handy von einem anderen Hersteller hat, die haben ja wahrscheinlich auch unterschiedliche Policies und updaten auch nicht immer zur gleichen Zeit. Also selbst da kann ich mich nicht mal eben am Stammtisch vergewissern, dass ich sicherheitstechnisch auf dem letzten Stand bin, weil wir alle anderen Stände haben.

Miriam Ruhenstroth: Das stimmt nicht. Diese Daten, dieses Sicherheits-Patch-Datum, das ist schon festgelegt für alle. Also, wenn ich dieses Level, ich sag mal, dass 2023 Sicherheits-Patch von Oktober habe, dann habe ich das. Dann bin ich auf diesem Stand. Es gibt aber Hersteller, die zum Beispiel nur alle Vierteljahre so ein Sicherheits-Patch liefern und dann die ganzen vergangenen Patches da mitreinpacken, also die ganzen vergangenen

Sicherheitslücken dort in einem Update reparieren. Das heißt also, wenn mein letztes Update, ich sag mal, vom Februar 2024 ist, dann weiß ich, ich bin auf einem aktuellen Level. Aber ich weiß halt nie, ob mein Handy alle Vierteljahre ein Update bekommt, jeden Monat – jeden Monat wäre das Beste. Oder nur alle halben Jahre. Das gibt es auch.

Ute Lange: Ich bin jetzt hinreichend verwirrt, aber wir wollen ja zur Klarheit beitragen. Es scheint ein komplexes Thema zu sein. Deswegen sprechen wir mit dir, um das einmal so ein bisschen aufzuklären und unsere Hörer und Hörerinnen und auch uns beide noch ein bisschen sensibler dafür zu machen. Wie behalte ich den Überblick? Also was hast du da für Tipps, wenn ich jetzt ein Gerät habe, das vielleicht nicht automatisch von sich aus sagt: „Hallo Update… Update!“ Was gibt es für Routinen, die man sich aneignen kann, die du empfehlen kannst?

Miriam Ruhenstroth: Ich empfehle bei Betriebssystem-Updates für Smartphones tatsächlich das Auto-Update zu aktualisieren. Man kennt das aus der Computerwelt, dass man immer ein bisschen warten soll mit dem Update, bis alle Fehler beseitigt sind. In sehr einzelnen Fällen gibt es das auch bei Smartphones, dass ein Update zum Beispiel auf eine neue Android-Version kommt, und es gibt Fehler, aber in der Regel passiert das nicht. Es ist auf jeden Fall die bessere Variante automatisch zu aktualisieren, als es zu vergessen. Wenn es ein Auto-Update gibt, sollte man es anschalten. Die meisten Geräte weisen einen darauf hin, dass es ein neues Update gibt, und dann muss man es installieren. Man sollte es auch zeitnah installieren und nicht warten. Wenn das der Hersteller nicht anbietet, was mir jetzt aber nicht bekannt wäre, dass das irgendjemand nicht macht, dann wäre es schon eine gute Routine, einmal im Monat einfach nachzugucken und Updates zu installieren. Ich möchte aber auch dazu sagen, es klingt so ein bisschen wie, alle Klarheiten beseitigt. Es kommt aber nicht auf den Stichtag an. Also da sprechen wir sicher später noch mal drüber, was dann eigentlich passiert, wenn mal ein Update nicht da ist. Ich möchte jetzt niemanden hier aus diesem Podcast gehen lassen, der dann denkt: “Oh, ich weiß nicht, ob mein Gerät sicher ist.“ Das ist es schon. Wir sprechen da von Vorgängen, die sich auch mal vier, fünf Wochen verzögern, und ob das jetzt vier Wochen früher kommt oder vier Wochen später, das ist nicht kriegsentscheidend. Da sollte man sich auch ein bisschen entspannen bei dem Thema.

Michael Münz: Angenommen, ich stelle fest, bei mir ist jetzt wirklich seit einem Jahr nichts mehr passiert. Ich sehe meine Betriebssystemversion, mein Hersteller hat da seit einem Jahr nichts mehr gemacht. Dann sagst du? Offenbar nicht sofort wegschmeißen, sondern durchatmen. Und was mache ich dann?

Miriam Ruhenstroth: Genau durchatmen. Es gibt dafür kein Standard-Rezept. Ich kann nicht sagen, nach der und der Zeit darf man das und das nicht machen, sondern es kommt darauf an zu verstehen, was eigentlich die Bedrohung ist. Diese Updates sind dazu da, dass sie Sicherheitslücken, also zum Beispiel Fehler im Softwarecode schließen, die entdeckt worden sind, und solche Sicherheitslücken oder Fehler größerer oder kleinerer Art, die werden permanent gefunden, wöchentlich, täglich und es gibt einen Grund, warum es diese, warum es diese kleinen Fixes, diese Updates einmal im Monat und manchmal sogar öfter gibt. Das sind aber keine Fehler, die dein Gerät sofort unsicher machen, sondern das sind Fehler, die möglicherweise zusammen mit anderen Fehlern irgendwann mal dazu führen, dass ein Gerät angreifbar ist. Und angreifbar heißt ja nur, da gibt es eine Möglichkeit, die muss dann auch noch ausgenutzt werden. Wir gucken eben sehr, wie werden solche Sicherheitslücken

tatsächlich für die normalen Nutzer ausgenutzt, und das wird immer dann gemacht, wenn es einfach ist, wenn es billig ist und wenn man damit irgendeine Art von Profit machen kann.

Es gibt noch die andere Kategorie von Angriffen, die teuer sind, wo sozusagen der Angreifer viel Geld bezahlen muss, um das technisch umzusetzen, und der dann ein Interesse hat, weil diese Person irgendwie ein Gegner ist oder gezielt gehackt werden soll. Um diese Kategorie von Angriffen kümmern wir uns nicht, wenn man denkt, man ist da im Fadenkreuz, dann muss man natürlich andere Maßnahmen ergreifen. Aber für die normalen Nutzer sind die Angriffe interessant, die durchgeführt werden können, weil sie einfach sind, und das sind fast immer Angriffe, die so funktionieren, dass die Nutzer sich selbst eine Schadsoftware installieren. Man muss tatsächlich an irgendeinem Punkt selber auf „Installieren“ tippen. Und die Sicherheitslücken werden eigentlich im Vorfeld ausgenutzt, weil sie Möglichkeiten bieten, einen irgendwie auszutricksen. Zum Beispiel erlaubt Android eigentlich nicht, dass ein Browser-Pop-up den ganzen Bildschirm bedeckt. Wenn es da irgendeinen Fehler gibt, dann findet eine Webseite vielleicht doch einen Weg, das zu machen. Dann muss ich aber immer noch darauf reinfallen und irgendwann auf „Installieren“ tippen, um mir diese Schadsoftware dann tatsächlich zu installieren. Und deswegen sagen wir, es kommt sehr darauf an, wie man sein Gerät nutzt, ob man solchen Angriffen überhaupt begegnet oder ob das unwahrscheinlich ist, weil ich sowieso nur telefoniere, meine zehn Apps benutze, die ich kenne, und irgendwie zwei Nachrichtenseiten, die ich kenne, aufrufe. Dann ist es sehr, sehr unwahrscheinlich, dass mir so eine Angriffsmasche überhaupt begegnet, und dann ist es erst mal nicht so schlimm, selbst bei einem Jahr ohne Updates passiert da nichts Schlimmes. Was man tatsächlich nicht mehr machen sollte, ist, Dinge zu nutzen auf dem Telefon, bei denen der Schaden groß ist, wenn wirklich was passiert, also Online-Banking, Zugriff auf die dienstliche Infrastruktur, also da, da ist das Risiko einfach zu groß. Aber wenn ich da meinen privaten Facebook Account benutze und meine Navigationsapp und meine Fotos mache, dann kann man schon einschätzen und sagen: „Okay, das Risiko ist jetzt nicht so groß, wenn ich mich vernünftig verhalte.“ Deswegen machen wir viel Aufklärung dazu. Wie sehen solche Angriffe überhaupt aus? Woher kommen die? Wo begegne ich denen?

Michael Münz: Das heißt, der Faktor Mensch spielt auch in diesem Falle einfach noch eine große Rolle.

Miriam Ruhenstroth: Sogar noch eine viel größere Rolle, als wir es aus der Computerwelt kennen, und das will ich auch immer wieder betonen, weil für Computer hat man mehr Nutzerrechte, die sind ganz anders konstruiert und ermöglichen damit viel mehr Möglichkeiten, aber auch viel mehr Angriffe. Also zum Beispiel dieses: „Ich rufe eine Webseite auf, und irgendwas installiert sich da plötzlich“, das gibt es auf Smartphones praktisch nicht. Wenn jemand einen Weg findet, das zu machen, dann verkauft er den für ein paar Millionen an die NSO Group, weil, das sind sehr, sehr teure, wertvolle Angriffe, die begegnen einem nicht einfach so.

Michael Münz: Die NSO Group sind Leute, die wir kennen müssten?

Miriam Ruhenstroth: Genau das sind Firmen, die professionelle „Spyware“ herstellen und an Staaten verkaufen, die diese natürlich nur zu legitimen Zwecken der Verbrechensbekämpfung einsetzen. Da werden richtig hohe Preise bezahlt.

Michael Münz: Okay, dann verstehe ich jetzt den Kontext, in dem du das jetzt gerade erwähnt hast, und wie viel Energie man da offensichtlich reinstecken muss, um so eine technische Veränderung herzuleiten.

Ute Lange: Aber vielleicht noch mal, um Klarheit zu schaffen. Wenn es Angriffe gibt, von denen du erzählt hast, die einfach zu machen sind und auf die Menschen hereinfallen, dann gibt es ja auch immer Warnungen. Also nicht nur vom BSI, wo der Podcast herkommt. Da gibt es noch andere Stellen, die sagen, jetzt läuft gerade eine Masche, passt auf! Dann weißt du ja, dass du gefährdet sein könntest. Wenn du nicht das aktuellste Sicherheits-Update hast, nachdem du nach dieser Folge geguckt hast, weißt du dann auch, wann du aufmerksamer sein solltest. Das war schon mal sehr hilfreich. Für mich hat sich das jetzt ein bisschen auseinanderdividiert. Nun gibt es verschiedene Hersteller, die auch unterschiedlich kostspielig in der Anschaffung sind, spielt das eine Rolle bei den Sicherheits-Updates? Wenn ich mehr Geld ausgebe, habe ich da eine höhere Sicherheit, dass mein Hersteller mich häufiger bedient?

Miriam Ruhenstroth: Da bin ich ganz vorsichtig, denn es ist nicht automatisch so. Gerade Samsung hat lange Zeit sehr hochpreisige Telefone verkauft und war gar nicht gut mit der Update-Policy. Das hat sich jetzt geändert, muss ich dazu sagen. Es gibt immer wieder sehr verkaufsstarke Mittelklassetelefone, die dann doch auch sehr, sehr lange geupdated werden. Insofern möchte ich gar nicht sagen, kauft euch ein Highend-Telefon und dann seid ihr automatisch auf der sicheren Seite. Aber ich sage mal so, tendenziell ist es natürlich schon so, dass die großen Hersteller ihre teuren Geräte auch mehr vermarkten und dann eher länger updaten als die Günstigen.

Michael Münz: Ich kann ja schon mal spoilern, dass es einen Silberstreif am Horizont gibt, was diese ganze Update-Policy und auch Verbraucher- und Verbraucherinnen-Interessen angeht. Ich wollte aber, bevor wir da einsteigen, noch einmal kurz nachfragen. Angenommen, ich kaufe mir jetzt ein Handy und stelle beim Einschalten fest: Moment mal, das Betriebssystem ist jetzt ein oder zwei Jahre alt, und ich bin mir nicht ganz sicher, ob das jemals nochmal aktualisiert wird. Kann ich das Ding dann wieder zum Händler zurückbringen? Und dann so wie John Cleese einen toten Papageien auf den Tisch klopfen und sagen: „Das Ding ist tot, das nehmen Sie mal bitte schön wieder zurück!“ Oder heißt es, Pech gehabt?

Miriam Ruhenstroth: Nein, es ist nicht so „Pech gehabt“. Wenn ich es bekomme und merke, dass es keine Updates mehr gibt, dann kann ich es sowieso zurückschicken. Also das Widerrufsrecht ist da, und dann fällt diese Update-Geschichte auch unter die Gewährleistungsfrist. Und zwar gibt es für digitale Geräte seit 2022 eine Gesetzesänderung, die eine erweiterte Gewährleistungsfrist vorsieht für digitale Geräte. Sie betrifft, dass der normale sichere Betrieb, den ich erwarte, beim Kauf gewährleistet sein muss, und zwar so lange, wie ich das erwarten kann.

Wenn ich, zum Beispiel, vor zwei Jahren ein Handy gekauft habe, und die normalen Fristen sind abgelaufen, und es bekommt keine Updates mehr, dann würde das unter die erweiterte Gewährleistungsfrist fallen. Der Händler müsste laut Gesetz dafür sorgen, dass ich das weiter sicher benutzen kann. Das kann er natürlich nicht. Also schlagen die Verbraucherzentralen vor, tatsächlich auf eine Preisminderung zu pochen. Das ist nicht weit verbreitet, das Wissen, um diese gesetzlichen Änderungen, und es ist auch noch nicht vor Gericht durchgefochten worden. Wie das dann tatsächlich läuft, wenn sich ein Händler dann

weigert, das zu machen. Wie das dann tatsächlich in den Details entschieden wird. Aber ich empfehle jedem, der denkt, das kann jetzt nicht wahr sein, das kann man doch nicht erwarten, dass dieses Handy jetzt keine Updates mehr bekommt, sich in dem Fall erst mal an den Händler zu wenden. Dummerweise ist der Händler zuständig und nicht der Hersteller, der ja eigentlich der Einzige ist, der für die Updates sorgen kann. Das ist natürlich eine kleine Fehlkonstruktion in diesem Gesetz.

Ute Lange: Wollte ich gerade anmerken, denn das ist ja vielleicht für den Händler oder das Geschäft, wo ich das gekauft hat, dann auch gar nicht so einfach, das durchzusetzen gegenüber dem Hersteller. Aber da kommt ja vielleicht dein Spoiler rein, der Silberstreifen am Horizont, den du schon angekündigt hast, Michael. Was hast du denn da in der Hinterhand, beziehungsweise was möchtest du unbedingt loswerden?

Michael Münz: Ich habe mitgekriegt, dass die EU ab 2025 Hersteller dazu verpflichtet, ihre Update-Garantie auf fünf Jahre auszuweiten. Noch so ein Nebenaspekt des Ganzen ist, dass spätestens vier Monate nach Erscheinen das Update für alle Smartphones bereitstehen muss. Und na ja, also gerade nach dem, was wir alles von dir gehört haben, Miriam, frage ich mich, ob das dann tatsächlich der Sicherheitsstandard ist, auf den wir Verbraucherinnen und Verbraucher jetzt gewartet haben und der uns eine Sorge abnimmt.

Miriam Ruhenstroth: Absolut, das ist ein absoluter „Game Changer“, würde ich sagen. Das ist sehr gut und diese Pflicht gilt ja nicht ab Markteintritt, sondern wenn dieses Gerät über drei Jahre hergestellt wird, dann ab letztem Marktverkauf. Das ist wirklich sehr, sehr gut, wenn wir vergleichen, was so zu Zeiten von Android 5 und 6 los war. Da konnte man zum Teil mit einem jährlichen oder gar keinem Update rechnen. Ich wollte auch zum vorherigen Punkt nochmal sagen, zu dieser erweiterten Widerrufsfrist. Wir sprechen jetzt von fünf Jahren Updates. Gleichzeitig ist es so, dass man aktuell Geräte kaufen kann, die schon jetzt, veraltet sind. Also, man kann die als neue Geräte kaufen. Da denke ich schon, es ist vielleicht auch nicht schlecht, die Händler ein bisschen in die Pflicht zu nehmen, weil sowas sollte man einfach nicht verkaufen. Das ist dann auch nicht mehr ein Hersteller-Problem, sondern das ist einfach nicht okay so.

Michael Münz: Wenn ich im Laden stehe und ein Handy kaufen will, der Preis und das Display sind gut, soll ich in diese Überlegung miteinbeziehen, wie es mit den Updates aussieht? Von wann sind die und kriegt das überhaupt noch mal wieder Updates? Empfiehlst du das?

Miriam Ruhenstroth: Unbedingt. Selbst bei seriösen und etablierten Technik-Händlern kann man ein Samsung Galaxy 9 kaufen, also das bekommt auf gar keinen Fall mehr Updates und da steht halt einfach das Betriebssystem dabei. Da steht aber nicht, dass es keine Updates mehr gibt. Also man wird da auch nicht darauf hingewiesen. Das habe ich gerade noch einmal recherchiert. Man kann sogar Telefone kaufen, wir haben es gerade ausprobiert für einen Bericht, den wir vorhaben. Man kann sogar Windows-Telefone kaufen, die also nicht nur keine Updates mehr bekommen, sondern das ganze Betriebssystem samt Backend-Funktionen wurde eingestellt. Da funktioniert gar nichts mehr, da geht nicht mal mehr ein App Store. Und die kann ich als Neugerät im Internet kaufen, und da dürften schon die Händler mal in die Pflicht genommen werden.

Ute Lange: Das heißt aber im Umkehrschluss für alle, die uns jetzt zuhören, dass, wenn ich mir überlege, mir ein neues Gerät zu kaufen, dass diese Frage: „Gibt es noch Updates?“, auf

jeden Fall gestellt werden sollte. Wenn es keine Updates mehr gibt, dann kann ich mich vielleicht für ein anderes Gerät entscheiden. Wenn es mir nicht mitgeteilt wird, so wie du jetzt gerade beschrieben hast, dann sollte ich auf jeden Fall fragen. Nicht dass ich hinterher feststelle, dass es ein alter Knochen ist, der zwar schick aussieht, aber keine Updates mehr kriegt.

Miriam Ruhenstroth: Ich kann mir vor allen Dingen vorstellen, jetzt mit der neuen Update-Pflicht, dass es so einen Resterampen-Verkauf geben wird von den alten Geräten, die keine Updates mehr anbieten. Mir war das nicht so klar, dass sozusagen ein Gerät, das ich neu im Laden kaufe, vielleicht schon ein Jahr alt ist. Bei einem Kleidungsstück spielt das ja auch keine Rolle, aber bei einem Handy, gerade wenn jetzt diese Update-Pflichten kommen, spielt es eine ganz große Rolle. Ich gehe ins Geschäft, das Gerät ist schon vor drei Jahren auf den Markt gekommen. Die Update-Pflicht gilt nicht. Deswegen schmeißen die das billig raus, und ich denke mir, ich mache einen Schnapp, aber in Wirklichkeit kaufe ich ein Gerät, was veraltet ist.

Michael Münz: Ja, dann hat es jetzt 25 Minuten gedauert, bis ich sagen kann, wenn also etwas zu schön ist, um wahr zu sein, und ich ein Handy sehe, was irgendwie schick, aber günstig ist, dann ist es wahrscheinlich auch einfach zu schön, um wahr zu sein.

Miriam Ruhenstroth: Könnte auf jeden Fall gut sein, dass es dann an diesem alten Betriebssystem liegt. Einfach mal nachfragen.

Michael Münz: Danke.

Ute Lange: Ja, ich finde, das war sehr aufschlussreich. Mir fällt jetzt gerade keine weitere Frage mehr ein, weil ich jetzt noch verarbeite, aber ich nehme auf jeden Fall mit, dass diese Frage, wenn ich ein neues Gerät kaufe: „Gibt es dafür noch Updates“? ganz oben auf meiner Liste stehen sollte. Vielleicht sogar noch vor der Farbe, vor dem Display und anderen schicken Features, die die Geräte heute so haben. Was nimmst du denn mit Michael?

Michael Münz: Ich muss sagen, dass es mir gut gefallen hat, wie du Miriam, den Faktor Mensch noch mal reingebracht hast. Also, dass es natürlich wichtig ist, dass unsere Geräte auch technisch auf dem neuesten Stand sind und wir uns da einfach keine Gedanken machen müssen, dass wir da Gefahr laufen, irgendwelche Probleme zu haben. Also es war gut, glaube ich, dass wir an dieser Stelle auch noch mal gesagt haben, dass wenn wir nicht zustimmen, dann können auch bestimmte Sachen gar nicht passieren, und das ist so dieser Faktor Mensch, den wir auch immer mal wieder als Thema haben. Es hilft, auch bei meinem Telefon nicht immer gleich zuzustimmen, weil ich denke, nee, 34 Seiten Betriebsbedingungen oder Geschäftsbedingungen lese ich mir nicht durch. Da muss ich noch stärker reflektieren, was ich da in meinem Handy zulasse, und was nicht. Also von daher, vielen Dank Miriam. Das war echt wichtig.

Miriam Ruhenstroth: Ja, gerne. Ich möchte zu dem Thema Updates auch noch eine Sache sagen. Wenn ich im Laden stehe und gerade jetzt, bevor diese Pflicht in Kraft tritt, ein Gerät kaufe und frage: „Wie lange kriegt das denn noch Updates?“, dann kann es gut sein, dass der Händler das gar nicht weiß, weil es der Hersteller gar nicht sagt. Aber es gibt einige Geräte, für die haben die Hersteller eine Zusage gemacht, und es ist ein bisschen unübersichtlich, das herauszufummeln, für welche es eine Zusage gibt und für welche nicht. Und für einige sind diese Zusagen jetzt auch schon ziemlich lang. Gerade hatten wir

Samsung erwähnt. Bei Pixel ist es auch so. Da kann ich euch, jetzt kommt der kleine Werbeblock, auch nochmal den Handy-Check ans Herz legen. Das ist eine kleine Webanwendung, die wir kürzlich veröffentlicht und in der wir das tatsächlich zusammengetragen haben. Das heißt, man kann dort ein Modell eingeben, und dann, wenn wir wissen, dass es dafür eine Update-Zusage gibt, dann steht es dort auch. Damit ist man fünf Jahre „safe“.

Michael Münz: Ja, gut, dass du es erwähnst. Weil als du vorhin von der Kristallkugel sprachst, dachte ich, ach Moment, es gibt doch eine, nämlich handycheck.de, wo ich jetzt die Tage nochmal hineingeguckt hatte. Ja, super, dann können wir auch da unseren Nutzerinnen und Nutzern noch etwas Konkretes an die Hand geben, wo sie sich dann auch darauf verlassen können. Guter Hinweis, danke dir!

Miriam Ruhenstroth: Ja, den kann ich sehr ans Herz legen.

Ute Lange: Danke euch und allen im Hintergrund, die diese, ich sage mal, Raussuch-Arbeit gemacht haben. Du hast gerade schon erwähnt, es ist vielleicht nicht ganz so übersichtlich für uns Verbraucher und Verbraucherinnen, und schön, dass wir jetzt noch so einen praktischen Tipp zum Ende mitgeben können. Ich habe schon beim letzten Mal, Miriam, als wir mit dir gesprochen, das eine oder andere zu meinem Handy gelernt. Es war wieder sehr, sehr aufschlussreich. Wer die letzte Folge mit ihr nicht gehört hat, das ist, glaube ich, zum Teil immer noch aktuell, was du uns damals mitgegeben hast, der kann gerne, wenn er „Update verfügbar“, schon auf seine Plattformen verfolgt, reinhören.

Michael Münz: Folge 19

Ute Lange: Folge 19, das ist der praktische Tipp, nochmal reinzuhören. Wie geht es denn euch jetzt so? Nach den Tipps geht ihr jetzt gleich mal euer Betriebssystem checken, ob das noch aktuell ist? Wenn ihr das tut, dann hören wir gerne darüber. Schreibt uns, gerne über die BSI-Kanäle auf Facebook, Instagram, X ehemals Twitter, Mastodon sowie YouTube. Ich überlasse dir wieder die E-Mail-Adresse, Michael.

Michael Münz: Gerne, also, ihr könnt uns eure Erfahrungen dann auch an die Mailadresse schicken: podcast@bsi-bund.de. Wir hören tatsächlich gerne von euren Erfahrungen, wie ihr euch im digitalen Alltag zurechtruckelt und was euch so anlässlich unserer Folgen dann so alles widerfährt. Also schreibt uns gerne.

Ute Lange: An der Stelle schon mal „Danke“. Es gab nach unserem letzten Aufruf, dass wir eure Themen gerne mit aufnehmen wollen, auch schon Rückmeldungen, die wir gerade sichten. Aber wir laden euch wieder ein, uns für die nächsten Folgen Ideen mitzugeben, Fragen, die ihr schon immer mal beantwortet haben wolltet, Vorfälle, die euch passiert sind, wo ihr gerne Tipps haben möchtet, wie ihr sie beim nächsten Mal verhindern könnt, und bis das passiert, wünschen wir euch eine gute Zeit.

Michael Münz: Ja, danke Miriam, auch an dich!

Miriam Ruhenstroth: Ja, vielen Dank. Das hat mir Spaß gemacht. Tschüss!