„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 19, 31.03.2022:

Mobil sicher! Smartphones und Apps

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

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

***Münz**:* Und mein Name ist Michael Münz. In dieser Folge dreht sich alles um das Gerät, mit dem die meisten von euch uns gerade hören: das Handy. Wir sprechen mit einem Gast darüber, wie man das Gerät, das wir immer bei uns haben, sicher machen kann. Dazu gleich mehr, aber erst sprechen wir über ein paar Themen, die uns seit dem letzten Update beschäftigt haben.

Lange: Als erstes wollen wir auf unsere in der letzten Folge erwähnte Einladung zurückkommen, dass ihr beim Digitalbarometer der Süddeutschen Zeitung mitmacht. Das ist ein Onlinefragebogen, mit dem wir anhand von Themen wie digitale Kommunikation oder IT-Sicherheit herausfinden können, wie fit wir im Digitalen sind. Wir haben uns gefreut, etliche Rückmeldungen bekommen zu haben, und wir haben den Eindruck, dass ihr, unsere Hörerinnen und Hörer, da relativ fit seid. Von den möglichen 100 Punkten hatten wir Ergebnisse zwischen 55 und 95. Das finden wir Spitze. Wir wollen aber mit dem Podcast weiter daran arbeiten, dass die digitale Kompetenz von uns allen zunimmt. Wir beide, Michael und ich, lernen in jeder Folge dazu und tun das sicherlich auch heute.

***Münz**:* Wir kommen aber auch bei Update Verfügbar nicht drum herum, über den Krieg in der Ukraine zu sprechen, weil der unter anderem digitale Auswirkungen hat. Das BSI warnt zum Beispiel seit dem 15. März vor dem Einsatz von der Virenschutzsoftware des russischen Herstellers Kaspersky. Hintergrund ist die Sorge darüber, dass die Virenschutzsoftware mit ihren grundsätzlich tiefen Eingriffen in ein System missbraucht werden könnte. Im Kontext des Krieges, den Russland gegen die Ukraine führt, könnte der russische IT-Hersteller zum Beispiel selbst offensive Operationen durchführen oder gegen seinen Willen dazu gezwungen werden, Zielsysteme anzugreifen. Es wäre unter anderem möglich, dass Kaspersky selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert wird oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht wird.

Lange: Alle Nutzerinnen und Nutzer dieser Virenschutzsoftware können von solchen Operationen betroffen sein, seien es Unternehmen, Behörden, Betreiber kritischer Infrastruktur oder auch wir, Verbraucher und Verbraucherinnen. Deswegen empfiehlt das BSI, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch andere Produkte zu ersetzen. Auf der Seite vom BSI gibt es eine ganze Menge Informationen dazu, die wir euch auch in die Shownotes packen. Da findet ihr Tipps für das weitere Vorgehen, um euch in dieser Situation besser abzusichern.

Münz: Ich habe in den vergangenen Wochen versucht, zu verstehen, welche Aussichten der Cyber-Krieg beziehungsweise digitale Kriegsführung hat. Zu dem Thema kann ich unseren Geschwister-Podcast CYBERSNACS empfehlen. Da hat Dirk Häger, Abteilungsleiter des Bereichs Operative Sicherheit beim BSI, nachvollziehbar erklärt, welche unterschiedlichen Ebenen dieser Krieg auf digitale Verhältnisse hat, wie man sich schützen kann und worauf man achten muss. Den Podcast kann ich nur empfehlen, wir setzen den Link in die Shownotes.

Lange: Ich kann mich mit einer weiteren Empfehlung anschließen. Ich habe mir den Podcast von Übermedien angehört, als Linus Neumann vom Chaos Computer Club zu Gast war, und fand den sehr interessant. Es gibt darum, was der Begriff Cyberwar bedeutet, welche Attacken es seit der russischen Invasion in die Ukraine gab und ob deutsche Unternehmen, vor allem Medienhäuser, Journalistinnen und Journalisten davon betroffen sind. Ich kann den Podcast nur empfehlen. Das ist noch ein Tipp für die Shownotes von uns.

Münz: Die Frage, die sich für uns, Verbraucherinnen und Verbraucher, stellt, ist, was ich selbst in der Situation, in der wir gerade sind, tun könnte? Diese Frage hat ein Bekannter aus diesem Podcast auf seine eigene Art beantwortet.

Lange: Du meinst den Teenager, der seit einer Weile die Flugbewegungen von Elon Musk trackt und die auf seinem Twitter-Account öffentlich bekannt macht? Diese Fähigkeiten hat der junge Mann jetzt genutzt, um Flugbewegungen von russischen Superreichen, die wir gemeinhin als Oligarchen bezeichnen, zu überwachen und auf Twitter zu veröffentlichen. Man kann jetzt sehen, welche Luxusmaschinen oder Helikopter von wo nach wo unterwegs sind. Ob die Personen drin sind, ist natürlich unbekannt, aber er scheint damit auf Interesse getroffen zu sein. Der Account hat eine ganze Menge neuer Follower gewonnen, seitdem er sich damit beschäftigt.

Münz: Auf jeden Fall eine Art und Weise. Weil ich nicht coden oder programmieren kann, habe ich mir überlegt, was ich in dieser Situation tun kann, um dazu beizutragen, dass die Informationsflut, die täglich auf uns einstürzt, ein bisschen sortierter ist. Ich bin nach den ersten Tagen dazu übergegangen, Inhalte noch genauer zu prüfen und unter anderem beim Teilen genau zu überlegen, ob ich das wirklich tun muss. Es kommen recht viele Informationen auf uns nieder, und ich möchte nicht Gefahr laufen, falsche Informationen zu teilen, weil es von allen Seiten Fakes gibt. Dafür gibt es zahlreiche Beispiele. Für mich ist die Lehre aus den vergangenen Wochen, dass ich noch genauer gucke, was ich teile, was echt ist und wie ich schnell überprüfen kann, ob nicht alte Bilder genutzt werden. Da bin ich sehr

vorsichtig geworden. Es gibt aber auch andere Methoden, um aktiv Leute zu unterstützen, die gerade in schwierigen Situationen sind. Ich habe zum Beispiel letzte Woche Tickets für den Zoo in Kiew gekauft. Es gibt da einen Zoo, in dem offenbar noch Tiere leben und die natürlich weiterhin gepflegt werden müssen. Viele der Beschäftigten sind geflüchtet oder setzen sich im Krieg ein. Man kann die Tiere und den Zoo unterstützen, indem man Tickets kauft, die online gekauft und bezahlt werden können. Es gibt eine englische Seite, da habe ich ein paar Tickets gekauft. Ich fahre natürlich nicht hin, aber ich weiß, dass das Eintrittsgeld gut ankommt. Ansonsten kaufe ich jetzt viel Musik digital ein, deren Erlöse bei Initiativen landen, die entweder Menschen in der Ukraine unterstützen oder Menschen, die sich auf die Flucht gemacht haben.

Lange: Ich bin sicher, dass es viele andere Initiativen gibt, die ihr unterstützen mögt oder schon unterstützt habt. Ich glaube, da sind wir alle im Moment sehr interessiert und aufmerksam.

Ich bin bei der Recherche zur heutigen Folge noch auf ein ganz anderes Thema gestoßen, was, was die Sicherheit von Handys, also der Geräte betrifft, die wir alle gerne dabeihaben. Dabei bin ich auf einen Artikel gestoßen, in dem berichtet wurde, dass Ermittlungskräfte in den USA die durch Fitnesstracker, Handys, PCs, Smartwatches etc. erhobene Daten sammeln und die gut für ihre Ermittlungen nutzen können, sowohl, um Beschuldigte zu überführen, als auch um Menschen, die in Verdacht geraten sind, zu entlasten. Mit diesen Daten sind teilweise die Tagesverläufe der beteiligten Personen nachzuvollziehen. Ich habe selbst ein paar Mal gedacht, was über mich bekannt ist, was ich nicht möchte, dass andere Menschen wissen. Deswegen freue ich mich, dass wir Miriam Ruhenstroth von mobilsicher.de heute bei uns haben, die uns mehr dazu sagen könnte. Herzlich willkommen!

Ruhenstroth: Hallo und danke, dass ich hier sein kann.

Münz*:* Wir freuen uns auch. Wir dachten, bevor wir dich mit unserem Fragenkatalog löchern, bitten wir dich, dich kurz vorzustellen. Was machst du bei mobilsicher.de und was ist das für eine Initiative?

Ruhenstroth: Ich freue mich sehr heute bei euch zu sein, und vielen Dank für die Einladung. Ich bin Projektleiterin bei mobilsicher.de, einem Projekt, das es schon seit sechs Jahren gibt. Ich habe auch eine von den beiden Trägerorganisationen, das Institut für Technik und Journalismus, mitgegründet, und wir machen noch einige andere Projekte. Heute geht es um mobilsicher.de, eine Plattform, die eigentlich als rein journalistisches Projekt angefangen hat. Ich habe auch journalistischen Hintergrund und habe mich dann erst in den technischen Teil eingefuchst. Das war learning by doing und ich hätte zunächst auch nicht gedacht, dass ich mich über sechs Jahre lang mit Smartphones beschäftigen würde. Sie sind allerdings dermaßen vielfältig und wichtig in unserem Alltag, dass immer was Neues dazukommt. Mit mobilsicher.de wollen wir euch, Leuten, die keine IT-Nerds sind, viele Dinge, die es dazu zu wissen gibt, einfach erklären und nahebringen.

***Münz**:* Wir sind sehr gespannt. Ich zähle mich selbst zur Zielgruppe, weil ich mein Handy genauso wie den Hausschlüssel immer dabeihabe. Das reicht mir, um durch den Alltag zu kommen. Jetzt würden wir dir gerne unsere Entweder-Oder-Frage stellen, mit der wir unsere Gespräche immer einleiten. Ute und ich dachten, wir würden gerne wissen, ob du lieber jemandem dein Handy oder dein Tagebuch geben würdest.

Ruhenstroth: Lieber mein Handy, denn es hat eine Bildschirmsperre.

***Münz**:* Hat dein Tagebuch hat kein Schloss, das dafür sorgt, dass keiner reingucken kann?

Ruhenstroth: Mein nicht vorhandenes Tagebuch hätte so was vielleicht, aber meine Bildschirmsperre hat sechs Ziffern, und die sind deutlich schwerer zu knacken als ein kleines Schloss, das sogar ich wahrscheinlich mit meinen begrenzten Lockpicking-Fähigkeiten aufkriegen würde.

***Münz**:* Gut zu wissen. Wir sind schon halb im Thema drin, was Sicherheit angeht. Wir haben im Podcast viel über Sicherheit am PC, im Smart Home und im Auto gesprochen. Wo unterscheidet sich die Sicherheit beim Handy von den anderen Dingen, die wir im Podcast besprochen haben?

Ruhenstroth: Das Wichtige beim Handy ist, dass man immer mitdenken muss, dass man dieses Ding mit sich rumträgt. Wer hat auf dieses Gerät Zugriff? Das ist eine andere Situation als bei einem Desktop-PC oder bei einem Smart Home, die immer an einem bestimmten Ort bleiben. Dieser Mobilitätsaspekt ist wichtig. Außerdem gibt es technisch einige Besonderheiten, die zum Teil aber auch für mehr Sicherheit sorgen. Mobilgeräte haben andere Betriebssysteme und da gelten ein paar andere Regeln.

Lange: Kannst du ein bisschen über diese Umgebung sprechen, die das von den anderen Geräten unterscheidet? Warum sollte man so aufmerksam sein und das Smartphone im Blick haben?

Ruhenstroth: Weil das Smartphone im Alltag permanent bei uns ist. Man muss sich überlegen, vor wem man sich schützen will, wenn wir über Sicherheit sprechen. Beim Mobilgerät ist es die Gruppe von Menschen, die um einen herum sind, also meine Kolleginnen und Kollegen, meine Familie, mein neugieriges Geschwisterkind oder Leute im Restaurant. Wenn ich schnell auf die Toilette gehe, kann man das Gerät stehlen. Der Themenkomplex Verlust und Diebstahl spielt eine größere Rolle. Das sind Dinge, die mit meinem elektronischen Auto eher nicht passieren.

***Münz**:* Verstehe ich dich richtig, dass es mehrere Ebenen gibt, die wir beim Thema Sicherheit beachten müssen? Erstens das Technische: Apps, Dateneinstellungen etc., zweitens Leute in meiner Umgebung, die Zugriff auf mein Handy haben. Sie können beispielweise Nachrichten sehen, die auf meinem Sperrbildschirm erscheinen. Drittens ist Verlust und Diebstahl. Das sind die drei Ebenen, die man sich im Hinterkopf behalten sollte, wenn man darüber nachdenkt, das Handy oder die Nutzung des Handys sicherer zu machen.

Ruhenstroth: Auf jeden Fall. Also eine große Rolle spielen die Apps, die ich benutze und vor allen Dingen, woher ich sie kriege.

Münz*:* Kannst du da vielleicht ein paar Hinweise geben, die wir, wenn wir das nächste Mal eine App im Store runterladen, bedenken sollten?

Ruhenstroth: Was man beim Thema Apps oder sichere Ads auf dem Handy beachten sollte, ist, dass all die Schadsoftware, Tricks oder anderes, was mir mit Software auf dem Handy passieren kann, immer nur dann funktioniert, wenn ich selbst mitmache. Da ist immer ein Schritt, bei dem man selbst auf Installieren klicken muss. Diesen Schritt nennt man im Jargon Social Engineering. Ich werde auf nicht technische Art zu irgendwas gebracht, was ich eigentlich nicht tun sollte. Ich werde manipuliert oder betrogen. Das ist wichtig, denn das ist der Schritt, bei dem man sich am besten und am effizientesten schützen kann, wenn man diese Tricks durchschaut. Auf dem Handy funktioniert das, was wir aus der Computerzeit kennen, nicht – und zwar dass sich irgendetwas von selbst installiert, wodurch irgendetwas passiert und sich fortpflanzt. Zum Beispiel Viren, die sich von selbst kopieren und auf andere Geräte verbreiten. Das funktioniert beim Handy nicht.

Lange: Wir fassen das Thema App jetzt zusammen: Ich bin durchaus in der Lage, das zu verhindern, weil ich vermeiden kann, dass etwas installiert wird, weil ich da draufdrücken muss. Kannst du ein Beispiel dafür nennen? Wenn ich zum Beispiel irgendwo sehe, dass alle von der neuesten App sprechen, die man unbedingt haben muss. Dann bin dadurch versucht, gehe in meinen App Store und finde die App. Was sind die Schritte, bei denen ich wachsam sein sollte, damit bestimmte Dinge nicht passieren? Was ist mit den ganzen Berechtigungsanfragen, die Apps immer haben? Wenn man diese App haben möchte, ist man manchmal flott und unaufmerksam. Was sind eure Tipps? Wie gehe ich damit um, wenn ich in der Versuchung bin, das zu machen, was alle machen?

Ruhenstroth: Wenn das alle machen, ist es ein ganz gutes Zeichen. So funktioniert es aber meistens nicht. Es funktioniert so, dass man beispielsweise eine WhatsApp Nachricht von jemandem, den man kennt bekommt. Da steht: Hey, ich habe dieses Video gefunden. Bist du das? Man will natürlich unbedingt wissen, ob man in irgendeinem Video ist. Man klickt auf den Link auf dem Smartphone und dann öffnet sich eine Seite. Die sieht so aus, als würde man auf ein Video klicken können. Man klickt darauf, und es kommt eine Nachricht, dass man etwas herunterladen und installieren soll. Man kennt vom Computer, dass es komische Formate gibt, deswegen installiert man das Ding. Das Handy fragt, ob man die App wirklich installieren will. Klar, ich will unbedingt wissen, was das ist. Plötzlich gibt es da kein Video. Ich habe aber bereits etwas installiert. Das ist das Schadprogramm. So funktionieren die Tricks, mit denen ich dazu gebracht werde, irgendwas, was keine bekannte große App ist, auf meinem Handy zu installieren. Meistens sind die Apps auch nicht im Google Play Store. Bei Android kommen die allermeisten Apps aus dem Play Store. Google prüft ein bisschen, welche Apps da zur Verfügung stehen, wodurch es nicht einfach ist, ein Schadprogramm einzuschleusen. Sobald ich etwas außerhalb von meinem Play Store installiere, was bei Android auch funktioniert, gibt es keine Überprüfung davon, was das ist. Das heißt, da sollte

man extra vorsichtig sein. Es gibt im Grunde nur zwei oder drei Quellen, die wir empfehlen, wo eine App außerhalb vom Play Store installieren werden kann. Man sollte nur dann etwas außerhalb vom Play Store installieren, wenn man sich sicher ist und man es kennt und weiß, warum das nicht im Play Store ist. Im Play Store gibt es allerdings auch Tricks. Das war während der Corona-Pandemie gut zu beobachten: Obwohl Google es schnell unterbunden hat, kamen im Play Store am Anfang der Pandemie, Pandemie-Apps, die im Titel irgendwas mit Covid zu tun hatten, beispielsweise Covid-Tracker. Die Angst und der Hype um diese Pandemie wurden ausgenutzt, damit Leute irgendwas installieren, ohne nachzudenken, und das nicht genau überprüfen. Mainstream Apps, das heißt Apps, die jeder hat, über die jeder spricht und über die es Hintergrundinformation gibt, sind meistens nicht die schädlichen.

***Münz**:* Wir haben in der Vergangenheit die Erfahrung gemacht, dass es saisonale Betrugsversuche gibt. Zum Beispiel, Dirndlverkauf während des Oktoberfests oder bei der Playstation 5 während des Weihnachtsgeschäfts. Solche Entwicklung kann man auch bei Apps sehen. Die greifen aktuelle Sorgen oder Trends auf und versuchen, auf ein Handy zu kommen.

Ruhenstroth: Es gibt so ein paar ganz einfache Regeln, die auf gesundem Menschenverstand basieren. Es ist Scam, wenn eine App mir etwas verspricht, was eigentlich nicht möglich ist. Beispielsweise eine App, die mir verspricht, dass ich kostenlosen Zugang zu allen Filmen habe, die sonst etwas kosten, eine App, die mir verspricht, dass mein Handy viermal so schnell läuft wie sonst oder eine App, die mir verspricht, dass ich das Passwort vom WhatsApp-Account meiner Freundin rausfinde. Das ist nicht realistisch. Bei Apps, die etwas Erstaunliches versprechen, muss man sofort misstrauisch werden. Es gibt noch ein paar Hinweise wie zum Beispiel komische Grammatik, seltsame Fehler, geringe Anzahl der Nutzerinnen und Nutzer etc., das sind alles Zeichen. Im Grunde ist das Betrugselement aber das Versprechen von irgendetwas, was es nicht gibt. Da muss man sofort aufmerksam werden.

Lange: Wir haben schon häufiger gelernt und auch gesagt, dass, wenn es zu schön ist, um wahr zu sein, es das wahrscheinlich auch nicht ist. Was kann man, außer, dass man selbst wachsam ist, noch tun? Wir haben vor allem am Anfang dieser Folge über Virenschutzsoftware bei PCs gesprochen. Gibt es zusätzliche Sicherheitssoftware für Smartphones, die Schwachstellen oder Sicherheitslücken in Apps erkennt? Braucht man das beim Mobiltelefon?

Ruhenstroth: Es gibt Dinge, die man tun kann. Antivirensoftware auf dem Smartphone wäre aber nicht das Erste, was ich dabei empfehle. Das hat verschiedene technische Hintergründe. Für Apple-Geräte gibt es keine Antivirussoftware, nur für Android. Android-Geräte sind so konzipiert, dass jedes Programm, das darauf läuft, nur in seinem kleinen Bereich läuft und es nicht sehen kann, was die anderen Programme tun. Das ist, was ein Programm auf dem Desktop tut. Das analysiert, was andere laufende Anwendungen während der Laufzeit tun. Das kann eine Antivirussoftware auf dem Smartphone nicht. Sie kann zwar die Datei analysieren und eine Markierung erkennen, die früher als Schadprogramm identifiziert

wurde, aber es ist im Grunde leicht zu unterlaufen. Diese Programme sind erst dann sinnvoll, wenn man viele verschiedene Apps aus verschiedenen Quellen außerhalb des Play Stores installiert, Otto-Normalverbraucherinnen und Verbraucher brauchen sowas nicht. Es gibt aber ein paar andere Einstellungen, über die wir gleich reden können.

***Münz**:* Ich würde gerne auf die anderen Aspekte des Themas Sicherheit kommen, über die wir schon kurz gesprochen haben. Wie kann ich mich verhalten, damit ich verhindern kann, damit meine Umgebung, mein Umfeld, oder andere nicht ungewollt Informationen über mich und mein Leben über mein Smartphone erhalten? Wie bei dem Beispiel mit dem Sperrbildschirm: da tauchen Informationen auf, die andere sehen können aber nicht sehen sollten. Gibt es Einstellungen, die du vielleicht bei deinem Handy eingestellt hast, damit sowas nicht passiert?

Ruhenstroth: Das Wichtigste, um das Smartphone vor dem direkten Umfeld zu schützen, ist der Sperrbildschirm. Wir sind hier erbarmungslos und raten von Entsperrungen die wie ein Muster aussehen, oder dem Entsperren mit dem Fingerabdruck, nur damit es schneller geht, ab. Es hilft nur eine mindestens sechsstelligen PIN, die man niemandem verraten darf. Auch nicht dem Partner, auch nicht meinem Kind und nicht dem liebsten Kollegen, der schnell etwas nachschauen soll. In diesem Fall muss man sie danach ändern und die Bildschirmsperre so einstellen, dass sie sofort wieder zugeht, nicht erst nach fünf Minuten. Sonst ist der Griff zum Smartphone von irgendjemandem, der gerade da ist, während man weg ist, einfach und schnell zu bewerkstelligen. Was das Muster angeht, kann der Kollege über die Schulter gucken und sich das merken, vor allem wenn diese Linie dazu erscheint. Auf unserer Seite haben wir ein Beispiel, wie ein wirksames Muster aussieht. Ein Fingerabdruck hilft zwar gegen die Kolleginnen und Kollegen, aber wenn es um konflikthafte Beziehungen geht, ist es auch nicht mehr ausreichend. Es ist schon passiert, dass der Fingerabdruck im Schlaf, im betrunkenen Zustand oder mit Gewalt genommen wurde. Außerdem gibt es noch die Einstellung, dass die Nachrichten, die ich bekomme, nicht über der Bildschirmsperre erscheinen. Das sollte man auch machen. Man muss sich die Mühe machen, erst zu entsperren, sonst kann jeder sehen, von wem ich gerade Nachrichten kriege. Das ist eine niederschwellige Übergriffigkeit, die sehr oft passiert. Das, was bei WhatsApp und anderen Messengern passiert, ist gerade privat und zum Teil auch heikel. Ich kenne mindestens zwei Beziehungen, die daran zerbrochen sind, dass der Partner beziehungsweise die Partnerin gesehen hat, von wem eine WhatsApp-Nachricht gekommen ist. Da muss man aufpassen.

Lange: Das sind schöne Stichworte: Messenger-Dienste und Sicherheit oder Verschlüsselung. Welche Tipps gibt es dafür? Beziehungsweise was bedeutet die Verschlüsselung bei Messenger-Apps und welchen Nutzen hat es? Welche zusätzliche Sicherheit bietet sie mir?

Ruhenstroth: Wenn wir über das Thema verschlüsselte Messenger sprechen, haben wir ganz andere Risiken im Blick, gerade wenn es um Ende-zu-Ende-Verschlüsselung geht. Es geht nicht mehr darum, dass irgendein Partner oder Partnerin meine Chats sieht, sondern darum,

ob jemand den Messenger-Dienst, den ich benutze, und dessen Server irgendwie kompromittieren und dort meine Nachrichten abfangen könnte. Da sprechen wir von sogenannten State-Sponsored-Angriffen, also staatliche Sicherheitsbehörden, Geheimdienste oder auch die Mafia und finanzkräftige Kriminelle. Sowas kann immer passieren. Da gibt es die berühmte Ende-zu-Ende-Verschlüsselung, die so funktioniert, dass es auf meinem Absendergerät verschlüsselt wird, verschlüsselt auf den Server des Dienstes gesendet wird und von dort auch verschlüsselt auf das Endgerät. Erst auf dem Endgerät wird es entschlüsselt. Das heißt, es ist ganz egal, was Kriminelle auf dem Server des Dienstes finden, weil sie das nicht lesen können. Das ist wichtig, vor allem auf einer größeren gesellschaftlichen Ebene, damit es klar ist, dass auch sehr mächtige Institutionen sich nicht massenhaft Zugriff auf die Kommunikation verschaffen können. Es ist State of the Art, es gibt keinen Grund, das nicht zu machen. Deswegen ärgern wir uns ein bisschen über Produkte, die das nicht machen. Sogar WhatsApp ist Ende-zu-Ende verschlüsselt. Es gibt keinen Grund, ein nicht Ende-zu-Ende verschlüsseltes Produkt zu verwenden.

***Münz**:* Welche Berufsgruppen beziehungsweise Menschengruppen können davon betroffen sein, wenn von staatlicher Seite oder von Organisationen versucht wird, auf das Handy zu kommen? Wir leben in einer Zeit, in der Menschen sich organisieren, vor allem Aktivisten und Aktivistinnen, Journalisten und Journalistinnen. Vielleicht sind das die Gruppen, die du im Blick hast und die du für solche groß angelegten Überwachungsversuche als gefährdet siehst?

Ruhenstroth: Die sind natürlich individuell gefährdet. Menschenrechtsaktivisten und -aktivistinnen, Journalisten und Journalistinnen müssen damit rechnen, dass Dienste direkt angegriffen werden, um auf ihre Kommunikation zuzugreifen. Ich würde jetzt nicht sagen, dass jeder Mensch, der nicht zu dieser Personengruppe gehört, sich zurücklehnt und denkt, dass er Ende-zu-Ende-Verschlüsselung nicht braucht, weil es auch um Massenüberwachung und vor allem anlasslose Massenüberwachung geht, die uns alle betrifft. Wer damit rechnen muss, dass es jemanden gibt, der richtig viel Geld auf den Tisch legt, um einen direkt und gezielt anzugreifen, muss mit ganz anderen Dingen rechnen als alle anderen. Da reichen unsere Tipps nicht mehr aus. Es gibt leider Angriffsvektoren, bei denen es reicht, eine SMS zu bekommen, und dadurch kann das Gerät kompromittiert werden. Das sind Schadprogramme im Kaliber von Pegasus und NSO, die richtig teuer sind und die Sicherheitslücken ausnutzen, die noch niemand kennt. Solche Sicherheitslücken werden für mehrere Millionen Euro gehandelt. Da hat man wirklich wenig Chancen, sich dagegen zu schützen. Das heißt, Leute aus dieser Personengruppe müssen damit rechnen, dass Ihr Gerät nicht sicher ist.

***Münz**:* Kommen wir zu dem Fall, der uns allen passieren kann. Ich verliere mein Handy. Miriam, was kann ich machen, damit, wenn es tatsächlich passiert, der Verlust mich nicht so schwer trifft?

Ruhenstroth: Das ist der Klassiker. Wichtig ist: Vorsorge ist besser als Nachsorge. Das heißt, alles, was ich dagegen machen kann, muss ich machen, bevor mein Handy verloren geht. Wichtigstes Thema dabei ist, dass es Ortungsdienste von den großen Betriebssystemen

Anbietern Apple und Google gibt. Nutzt die! Die sind gut. Es gibt Leute, die Angst haben, dass Google immer weiß, wo sie sind. Das ist aber nicht so ein Problem, und der Mehrwert ist wirklich riesig. Wenn ihr die nutzt, merkt euch, dass ihr die Zugangsdaten zu eurem Google-Konto braucht. Hinterlegt die irgendwo, das ist wichtig. Wenn das Handy weg ist, und ihr kommt über den Computer nicht mehr in euer Google-Konto, bringen euch die Ortungsdienste auch nichts. Das sind die beiden wichtigsten Dinge. Echt praktisch, wenn man das Gerät im Bus liegen gelassen hat, diese Dienste sind empfehlenswert. Die muss man vorher aktivieren, obwohl sie inzwischen auch fast standardmäßig aktiviert sind. Zweites wichtiges Thema dabei ist wieder die Bildschirmsperre. Ihr wollt nicht, dass derjenige, der das Ding im Bus findet, gleich die Nacktfotos anschaut. Dagegen schützt eine gute Bildschirmsperre. Dann ist das Risiko, dass jemand Zugang auf alles hat, gering. Wenn das Gerät wirklich weg ist, müsst ihr sämtliche Dienste, mit denen das Ding verknüpft ist, sperren, und das Passwort sowie die Zugangsdaten ändern. Einmal alles durchgehen. Das ist zwar viel Arbeit, aber das müsst ihr machen.

***Münz**:* Sind das auch die Punkte, die für den Fall gelten, wenn das Handy gestohlen wird?

Ruhenstroth: Ja. Wenn es geklaut wird, ist der zeitliche Ablauf natürlich ein bisschen anders. Wenn es klar ist, dass es ein Diebstahl war, sollte man lieber sofort sowohl die SIM-Karte als auch alle Karten, die damit verbunden sind, sperren. Auch hier ist die Bildschirmsperre das Wichtigste. Ein unversperrtes Handy gestohlen zu kriegen ist richtig doof. Es ist wissenswert, dass neuere Smartphones relativ gut dagegen geschützt sind, dass zum Beispiel der Dieb oder die Diebin das Handy zurücksetzen und als neu verkaufen kann. Das funktioniert nicht mehr so gut auf neueren Geräten. Die Daten sind auch gut verschlüsselt. Zur Sicherheit sollte man aber, wenn es wirklich gestohlen ist, bei allen Diensten, die damit verknüpft sind, wie E-Mail, Amazon-Konto usw. das Passwort ändern und daran denken, ein Backup zu machen.

***Münz**:* Backup ist auf jeden Fall ein Thema bei uns.

Ruhenstroth: Ja, Backup ist ein Thema und ist auch ein ärgerliches Thema. Es ist auch so, dass das Handy kaputt gehen kann.

Lange: Du hast schon viele Aspekte angesprochen. Gibt es noch etwas, was dir besonders auf dem Herzen liegt, wo du sagst, das muss jetzt noch raus?

Ruhenstroth: Ja. Ein wichtiges Thema, das wir noch nicht angesprochen haben, das aber sehr viele Leute betrifft, sind die aktuellen Kostenfallen, die Abofallen. Ich habe, auf irgendwas geklickt und habe jetzt ein Abo an der Backe oder ich habe auf nichts geklickt und habe trotzdem irgendwelche Kosten auf meiner Mobilfunkrechnung. Diese klassischen Kosten, die entweder von meinem Google-Konto abgebucht werden oder noch schlimmer von der Mobilfunkrechnung. Das ist eine ganze Betrugsindustrie. Es gibt tausende verschiedene Tricks, die ich jetzt nicht alle einzeln erklären will, weil es eine ganz einfache Sache gibt, mit der man das unterbinden kann, und zwar die Drittanbietersperre. Ihr könnt bei eurem Mobilfunkanbieter sagen, dass ihr nicht möchtet, dass Dinge über die Mobilfunkrechnung bezahlt werden können. Dann funktionieren diese ganzen Sachen nicht mehr. Das muss man

sich allerdings selbst und proaktiv drum kümmmern, weil das keine Standardeinstellung ist. So kann niemand mehr über eure Telefonrechnungen etwas kaufen.

***Münz**:* Das haben wir in einer der früheren Folgen gehabt. Ich habe nachgeguckt, ob ich eine Drittanbietersperre schon eingerichtet hatte. Das hatte ich. Das, was für diesen und viele der anderen Tipps gilt, ist die Tatsache, dass man es nur einmal macht und dann nie wieder. Dann ist man an der einen oder anderen Stelle abgesichert. Es ist nicht so, dass man bei jeder Nutzung des Handys 15 Gedankenprozesse durchlaufen muss und sich Sorgen machen, ob man alles richtig gemacht hat. Viele der Sachen, die du erwähnt hast, sind eine einmalige Einstellung, möglichst zu Beginn der Einrichtung des Handys. Dann hat man ein paar Sorgen weniger, was Datensicherheit im digitalen Alltag angeht.

Ruhenstroth: Das ist auf jeden Fall so!

Lange: Lasst uns ganz kurz zusammenfassen, was man bei der Ersteinstellung berücksichtigen sollte. Was ist bei dir hängengeblieben, Michael?

***Münz**:* Bei mir ist das Thema Backup hängengeblieben. Das ist ein Thema, mit dem ich mich immer wieder beschäftige. Sperrbildschirm ist bei mir hängengeblieben. Das war ein Punkt, über den ich noch nicht nachgedacht habe, zum Beispiel dass PIN die sicherste Methode ist. Ich habe noch gemerkt, dass ich wissen soll, wo mein Handy ist und dass ich dafür sorgen soll, dass ich das lokalisieren kann. Jetzt würde ich gerne hören, was bei dir noch hängengeblieben ist, Ute.

Lange: Bei mir ist das hängengeblieben, was wir schon häufiger als Thema hatten, und zwar dass der gesunde Menschenverstand sehr hilft. Wenn etwas zu schön klingt, um wahr zu sein, ist es das vermutlich auch nicht. Noch, dass ich beim Handy genauso wie bei E-Mails nicht bei irgendeiner Nachricht „Du bist in einem Video“ draufklicke und dann etwas installiere, weil meine Neugier mich überrennt, sondern dass meine Skepsis wach bleibt, meine Wachsamkeit hoch ist und dass ich bei Dingen, die gerade gehypt werden, ein bisschen vorsichtiger sein sollte, weil unter Umständen eine ganz banale Betrugsmasche dahintersteckt und man auf mein Geld aus ist. Wir packen in die Shownotes, was Miriam an Angeboten gemacht hat, wie man sein Handy absichert. Bei Mobilsicher findet ihr eine ganze Menge Tipps und Tricks, über die Miriam heute gesprochen hat. Ich fand es sehr informativ. Vielen Dank, dass du dabei warst, Miriam. Schön, dass du dir die Zeit genommen hast.

Ruhenstroth: Danke auch. Hat mir Spaß gemacht.

***Münz**:* Für uns bleibt noch der Blick auf die nächste Folge, wo wir uns mit dem Thema Digitalisierung in der Schule beschäftigen werden. Da haben wir auch einen Gast, mit dem wir darüber sprechen können, welche Veränderungen die Digitalisierung in der Schule mit sich bringt und wie man da sicher im Alltag sein kann.

Lange: Bis es soweit ist, folgt Update Verfügbar auf euren Podcast Plattformen. So verpasst ihr keine Folge und könnt in vorherige Folgen hineinhören.

***Münz**:* Wie immer gilt: kontaktiert uns gerne über die BSI-Kanäle auf Facebook, Instagram, Twitter und YouTube. Wir gucken immer rein und schauen, was ihr uns als Rückmeldung zu den Folgen sagt. Das könnt ihr auch per E-Mail tun: bsi@bsi.bund.de. Da kommt auch die Rückmeldung an, die uns dorthin schickt.

Lange: Wir freuen uns auf eure Post und Nachrichten, egal auf welchem Kanal. Bis wir uns wieder hören alles Gute und wir freuen uns! 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/
https://social.bund.de/@bsi

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