„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 24, 30.09.2022:

„Ich habe nichts zu verbergen“ – dem Mythos auf der Spur

Moderation: Ute Lange, Michael Münz
Gast: Michael Meier, Rheinische Friedrich-Wilhelms-Universität Bonn
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

***Münz**:* Ich bin Michael Münz. In dieser Folge geht es um den oft gesagten und gehörten Satz „Ich habe ja nichts zu verbergen“. Wir schauen uns an, wie viel an diesem Satz wirklich dran ist und wie viel wir wissentlich oder unwissentlich im Netz von uns preisgeben.

Lange: Michael und ich haben dafür gegenseitig unsere Spuren im Netz verfolgt und gelesen, was wir preisgeben und posten, vor allem, was wir vielleicht nicht möchten, dass ihr über uns wisst. Was könnte man im schlimmsten Fall mit diesen Daten anfangen? Um das gründlich zu machen, haben wir einen Experten eingeladen, der sich hauptberuflich mit solchen Schnüffeleien im Netz beschäftigt. Dazu gleich mehr, aber zuerst ein kleiner Rückblick auf die aktuellen Maschen, mit denen wir und ihr um unsere Daten gebracht werden.

***Münz**:* Ich muss noch schnell mein Telefon stummschalten, weil das in letzter Zeit ständig klingelt. Ich kriege regelmäßig Anrufe von Mobilnummern, die nicht in meinem Kontaktbuch sind. Eigentlich gehe ich bei solchen Anrufen nicht mehr ran, weil ich aus 24 erschienenen Folgen des Podcasts verstanden habe, dass ich nicht immer alles annehmen muss, was kommt. Weil es aber so viel waren, bin ich doch rangegangen, und bei allen Anrufen war es so, dass die Gegenseite innerhalb von einer Sekunde aufgelegt hat. Ich war neugierig und habe recherchiert, was das vielleicht für eine Masche ist. Es sind offenbar Lock-Anrufe. Die rufen mich nur an und legen dann auf, damit ich zurückrufe und in einer Kostenspirale lande, oft bei einer Tonbandansage, die mich möglichst lange in der Warteschlange halten soll. Also ich blockiere jetzt alle Nummern, die kommen und gehe nicht mehr bei anderen Telefonnummern ran. Ich weiß, dass meine Telefonnummer bei mehreren Datenleaks in der Vergangenheit mit dabei war, und wir hatten auch Beispiele von Smishing gehabt. Das hat mich auch betroffen. Jetzt weiß ich, dass ich einfach nicht rangehe, wenn jemand mobil anruft. Wenn es wichtig ist, melden sie sich schon.

Lange: Ich hatte auch solche Anrufe, allerdings ist es bei mir mehr auf dem Festnetz vorgekommen. Ich konnte meine Neugier, wer da dran ist, zum Glück ganz gut ignorieren

und somit auch die meisten Anrufe. Dafür sind bei mir vermehrt Phishing E-Mails eingegangen, meistens mit dem üblichen „Wenn du nicht A machst, zum Beispiel Login für ein Konto überprüfst, passiert B“. In einer E-Mail wurde mir beispielsweise angedroht, dass meine Webseite abgeschaltet wird, wenn ich nicht alle meine Daten eingebe. Selbst wenn diese E-Mails echt aussehen, was sie häufig nicht tun, lösche ich sie sofort. Das habe ich auch in 24 Folgen des Podcasts gelernt. Es gibt aber eine neue Masche, die einen anderen Faden aufnimmt. Es wird einem in der Betreffzeile versprochen „Jetzt Energiepauschale sichern“ oder „Bereit für Ihren Energiebonus“. Das ist ein sehr heißes Thema für viele Menschen. Wir wissen durch die Berichterstattung, dass die steigenden Kosten viele sehr belasten, und ich fürchte, dass der eine oder andere deswegen darauf reinfällt, weil ihm oder ihr versprochen wird, dass das Geld bald kommt. Ganz wichtig zu wissen ist, dass die Energiepauschale entweder vom Arbeitgeber ausgezahlt oder bei der Einkommenssteuererklärung im nächsten Jahr verrechnet wird. Das heißt, dass irgendeine Bank oder eine Institution dir niemals das Geld überweisen wird. Deswegen muss man bei solchen Betreffzeilen nicht drauf gehen. Das BSI rät auch ab, auf Links zu gehen, die persönliche Daten oder Ähnliches wollen. Das ist einfach ein neuer Spin dieser fiesen Masche. Wir verlinken euch die Infos vom BSI dazu in den Shownotes.

***Münz**:* Gut zu wissen, dass meine Energiepauschale nicht dadurch bei mir ankommt, dass ich irgendwelche Daten von mir im Netz preisgebe. Das ist ein guter Hinweis, danke dir! Bevor wir das Thema Datensicherheit vertiefen, wollte ich kurz auf meinen Reisepass zu sprechen kommen, den ich jüngst für eine Dienstreise brauchte. Es war alles kurzfristig, und daraufhin bin ich mehrmals bei der Stadt Bonn im Stadthaus gewesen, um den Reisepass zu beantragen und dann wieder abzuholen. Das hat auch alles super funktioniert. Vielen Dank an alle, die das ermöglicht haben, damit ich rechtzeitig in den Flieger steigen konnte. Bei solchen Situationen und Gelegenheiten denke ich aber immer wieder daran, ob es wirklich sein muss. Geht so etwas nicht online? Muss ich wirklich zwei, drei Mal ins Stadthaus rennen, um alles in die Wege zu leiten? Ich habe mich dann mit E-Government-Diensten beschäftigt und damit, was man gerade online beantragen kann. Ich bin auch auf eine Studie gekommen, die besagt hat, dass die Hälfte aller Deutschen bei solchen E-Government-Diensten zurückhaltend ist, weil sie Sorge vor der Datensicherheit haben. Das hat mich sehr erstaunt. Danach habe ich schnell geguckt, wie viele Menschen in Deutschland soziale Netzwerke oder Messenger-Dienste nutzen. Das sind nämlich 88 Prozent. Das heißt, viele geben ihre Daten an Privatunternehmen ab, haben aber gleichzeitig Sorge, ihre Daten an viel datensparsamere Dienste des Staates abzugeben. Da habe ich mich gefragt, wie das sein kann. Ute, wie siehst du das? Übertreibe ich jetzt ein bisschen?

Lange: Ich glaube, das ist die Widersprüchlichkeit, die wir beide vermutlich auch in uns haben. Du hast recht, diese E-Government-Dienste sind in der Regel sehr sicher, weil da viel Gehirnschmalz reinfließt und weil es vorher überlegt wird, wie die Daten, die Bürgerinnen und Bürger geben, gut abgesichert werden können. Es gibt vor allem für Daten, die an den Start gehen, klare Richtlinien und Vorschriften, beispielweise was von einem gefordert werden darf, wenn man bestimmte Dienste in Anspruch nehmen will. Im privatwirtschaftlichen Bereich (du hast einige der Plattformen schon genannt) gibt es zwar

auch Regeln und Gesetze, aber die sind viel schwieriger zu überprüfen und einzuhalten. Ich finde, das ist ein guter Übergang zu unserer Spurensuche im Netz, weil wir wahrscheinlich genauso wie viele Menschen diesen Zwiespalt in uns haben. Bei den einen sind wir in Sorge, bei den anderen machen wir es aus unterschiedlichen Gründen gerne und sehr schnell. Willst du wissen, was ich über dich herausgefunden habe?

Münz: Das will ich natürlich. Ich bin nur ein bisschen zurückhaltend, weil ich weiß, dass Millionen Menschen jetzt zuhören. Ich hoffe auf deine Diskretion und darauf, dass vielleicht nicht alle deine Fundstücke hier in der Aufnahme landen.

Lange: Ich kann dich ein bisschen beruhigen. Es war gar nicht so wahnsinnig viel. Wir kennen uns viele Jahre als Kollegen und Freunde, und es war nicht sehr viel davon, was ich noch nicht wusste. Die Frage, die ich mir gestellt habe bei dem, was ich gefunden habe, ist, was andere vielleicht damit machen könnten. Ich weiß, du legst Musik auf. Dadurch, dass du darüber postest, weiß ich auch, wo du überall aufgelegt hast, und zwar in Bonn, Berlin, Wien etc. Ich weiß auch, welche Sets du auflegst, weil du mir die immer zur Verfügung stellst. Ich weiß, wo du gerne frühstücken gehst, wo du joggen gehst, in welchen Städten du dich gerade aufhältst, weil du das markierst. Ich weiß, wo dein Lieblingsplattenladen ist und mit wem du dich da austauschst und triffst. Und im Rückblick habe ich ein paar kleine Haarkatastrophen gefunden. Du erinnerst dich an diese eine Frisur, die ein bisschen wie Woody Woodpecker aussieht und nicht eine Karnevalsfrisur war, sondern dein echter Haarschnitt. Auch das findet man noch. Ansonsten war ich fast ein bisschen enttäuscht. Mir, die dich schon ein bisschen besser kennt, ist nichts aufgefallen, was mich überrascht hätte. Die Frage wäre, was machen Menschen, die dich nicht kennen, aus diesen ganzen Informationen? Was für ein Bild von Michael Münz zaubern sie sich zusammen? War das diskret genug?

Münz*:* Das war super! Ich werde meine sozialen Profile von hinten anfangend aufräumen, angefangen bei diesen Frisurfotos. Diese ganzen anderen Punkte werde ich mir auch genauer anschauen. Man kann daraus wahrscheinlich vernünftige Bewegungsprofile erstellen und sich ausrechnen, wo ich gerade bin oder nicht bin. Jetzt könnte ich als Retourkutsche das auf den Tisch legen, was ich von dir gefunden habe.

Lange: Mit derselben Diskretion. Wie du sagst, da hören Millionen Menschen zu.

Münz: Auf jeden Fall. Das Ergebnis ist mehr oder weniger dasselbe. Ich kann dich beruhigen, muss aber unsere Hörerinnen und Hörer enttäuschen. Das Frisurfoto von 2011, über das wir noch mal ernsthaft sprechen müssen, habe ich nicht gefunden. Das können wir in den Shownotes auch nicht verlinken. Wer dich aber im Karnevalskostüm sehen will, wird das schon finden. Ich weiß, dass du Mitglied bei der Karnevalsgesellschaft UN Funken bist, und man sieht dich in dieser Rolle in sozialen Netzwerken. Was man noch als Außenstehender und nicht als mit dir befreundete Person findet, sind deine ehrenamtliche Aktivitäten, beispielsweise dass du die Socialbar Bonn organisierst. Man sieht unter anderem, wann und wo es ist und dass du dabei bist. Alles soweit Update Verfügbar-konform. Es gibt allerdings ein Thema, über das ich doch mit dir sprechen wollte, nämlich deine Reisen. Das sind die

Orte, über die du gesprochen hast. Deine Reisen dokumentierst du nicht nachher im Sinne „Guckt mal, wo ich war“, sondern oft auch „Guckt mal, wo ich gerade bin“. Das ist ein Punkt, den wir bei den Folgen, in denen wir über Urlaub sprechen, immer wieder hervorheben. Wenn ihr postet, dass ihr gerade acht Flugstunden von Zuhause weg seid, ist es für andere Menschen vielleicht eine Einladung, vorbeizufahren und die Wohnung auszuräumen. In diesem Sommer hatten wir das Thema noch. Das ist ein Punkt, wo ich als Update Verfügbar-Moderator dir, Ute, sage, dass es nicht das ist, was wir selbst predigen.

Lange: Ja, ich sage doch, Widerspruch. Zwiespältig.

Münz: Genau das. Aber alles andere ist wirklich okay. Zumindest das, was wir finden konnten. Vielleicht gibt es doch noch mehr.

Lange: Dafür haben wir jemanden eingeladen. Ich bin auch ein bisschen erleichtert, dass es langweilig oder wenig aufregend, aber deswegen auch vielleicht wenig schädlich ist. Den Aspekt mit den Markierungen nehme ich mir zu Herzen. Wir haben jetzt noch einen Michael hier. Michael Meier, Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Uni Bonn und Leiter der Abteilung „Cyber Security“ beim Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie. Ganz herzlich willkommen, Michael. Schön, dass du da bist. Magst du dich noch mal vorstellen und erklären, was sich hinter diesem langen Titel verbirgt, wo du arbeitest und zu was du arbeitest?

Meier: Das mache ich sehr gerne. Ich bin Universitätsprofessor, gebe Vorlesungen und forsche zusammen mit meinem Team. Was die Forschung und darüber hinaus Beratungsdienstleistungen angeht, bin ich auch beim Fraunhofer FKIE tätig. Das heißt, wir helfen den anderen, Risiken in den Griff zu bekommen, die aus IT resultieren. Die Erfahrungen und Kenntnisse, die wir dort sammeln, geben wir in Weiterbildungen wieder, zum Beispiel an der Uni in dem Studiengang Cyber Security, den ich leite.

Münz: Bevor wir weiter darüber sprechen, was du forscht und was du vielleicht auch über uns geforscht hast, gibt es noch eine Entweder-oder-Frage, die wir jedem Gast stellen. Mal schauen, wie du dich entscheidest. Wenn du das Twitter-Passwort des Bundeskanzlers oder eines anderen Regierungsmitglieds findest, gibst du es gleich zurück oder hast du erstmal eine Woche Spaß?

Meier: Ich habe eine Woche Spaß, wobei Spaß relativ ist. Wir werden gleich darauf noch zu sprechen kommen, aber ich denke, ich würde damit Dinge tun, die wir auch mit anderen Passwörtern tun.

Münz: Das heißt, es ist nicht so unüblich, dass ihr bei eurer Arbeit auf Passwörter von anderen stoßt.

Meier: Genau. Das ist tatsächlich das Ziel unserer Arbeit, wobei wir diese Passwörter weniger missbräuchlich nutzen wollen, sondern vielmehr herausfinden wollen, ob die noch aktuell genutzt werden. Zum Beispiel das Twitter-Passwort des Bundeskanzlers. Wenn es drei Jahre alt ist und inzwischen nicht mehr genutzt wird, gibt es da kein großes Problem. Oft kommt

leider das Phänomen vor, dass Nutzerinnen und Nutzer ihre Passwörter bei vielen verschiedenen Diensten nutzen. Es stellt sich die Frage, ob es vielleicht nicht nur der Twitter-Account, sondern auch andere Zugänge des Bundeskanzlers gibt, die man mit diesem Passwort öffnen kann. Für mich als Sicherheitsforscher wäre es interessant, wie die Bedrohung aussieht, die von diesem Passwort ausgeht.

Münz: Wo findet ihr so ein Passwort? In welchen Ecken des Netzes seid ihr unterwegs, um solche Sachen zu finden?

Meier: Man muss sich überlegen, dass im Prinzip auch Kriminelle, die gezielt Jagd auf solche Passwörter durch Phishing, Schadsoftware, Eindringen bei verschiedenen Onlinediensten und Datenbanken machen, mit speziellen Techniken im Internet kommunizieren. Manchmal wird in dem Kontext der Begriff Darknet gebraucht. In diese Kommunikation kann man sich einklinken. Man kann beobachten, was für Kommunikation dort stattfindet, ob jemand über irgendwelche neuen Errungenschaften prahlt und welche Datenbestände in dem Zusammenhang ausgetauscht werden. Genau die besorgen wir uns und analysieren diese. Es geht dabei nicht nur um das klassische Internet, sondern auch um bestimmte Foren oder Messenger-Chats, anhand von denen man analysieren kann, was es in diesen Kreisen Neues gibt.

Lange: Das heißt, ihr macht das, was wir gemacht haben, aber auf einer tieferen Ebene. Im Gegensatz zu den Kriminellen versucht ihr aber dabei, Erkenntnisse darüber zu gewinnen, wie wir uns besser schützen können. Wir haben beide nicht wahnsinnig aufregende Dinge über uns gefunden, die man aber trotzdem nutzen könnte. Michael hat die Markierungen der Orte genannt, die vielleicht zu unterbleiben haben. Was hast du gefunden? Ich gehe davon aus, dass du auch ein bisschen geguckt hast, bevor du dich auf das Gespräch mit uns eingelassen hast. Wir sind sehr neugierig.

Meier: Ich habe geschaut. Wir schauen auch systematisch, zu welchen Personen sich problematische Zugangsdaten in unseren Sammlungen finden, um Betroffene warnen zu können. Ute und Michael, ich habe geschaut, ob ich etwas zu euren E-Mail-Adressen in unseren Datenbeständen finde. Zu Ute habe ich nichts gefunden. Zu Michael schon. Zu irgendeiner Zeit sind sowohl Klartext-Passwörter als auch Passwörter in einer verschlüsselten Form abhandengekommen. Bevor das ausgestrahlt wird, sollte man prüfen, ob die immer noch im Dienst sind. Zum Beispiel mit dem Leak Checker von der Uni Bonn, den meine Arbeitsgruppe betreibt. Wenn das alte Passwörter sind, sind die Bedrohungen hier nicht mehr präsent und es besteht kein Problem. Sollten die aber irgendwo noch genutzt werden, dann gibt es ein Problem.

Münz: Das erklärt diese vielen Anrufe, die ich in den vergangenen Wochen bekommen habe. Daten von mir werden offensichtlich getauscht oder sind offen zugänglich. Danke für den Tipp und für diese Warnung. Das schaue ich mir auf jeden Fall an und habe noch ein paar Tage Zeit, um mich abzusichern, bevor das alles in die Öffentlichkeit geht. Danke, das ist sehr wichtig.

Lange: Du sagst, irgendwelche Daten von Michael sind ungeschützt und wurden eventuell geleakt, also sind draußen in der Welt. Wenn das mir passiert, kann ich die wieder zurückholen? Du hast gerade die Vermeidungsstrategie genannt, und zwar sichere Passwörter einrichten, sie häufiger wechseln, ein Auge draufhaben. Wo sind aber die Möglichkeiten, wen es schon da draußen ist?

Meier: Das ist das Problem, das man immer hat, wenn Geheimnisse offenbart werden oder, wie man in der Fachsprache sagen würde, die Vertraulichkeit verloren gegangen ist. Das ist nicht so einfach zu reparieren. Eigentlich gar nicht. Man könnte höchstens das Individuum, das diese vertraulichen Informationen zur Kenntnis gewonnen hat, aus dem Weg räumen. Das kennt man vielleicht von James Bond: „Wenn ich dir das sage, dann muss ich dich töten". Aber das ist natürlich nicht realistisch. Das ist genau die Herausforderung, wenn Geheimnisse abhandenkommen. Man kann versuchen, diese abgeflossene Information wieder in den Griff zu bekommen, allerdings mit sehr diffizilen Techniken. Man kann versuchen, das zu verrauschen. Zum Beispiel, wenn Information von dem Router abgeflossen ist, kann ich versuchen, viele andere gefälschte Informationen zu streuen, sodass es für denjenigen, der die Information von dem Router nutzen möchte, nicht klar ist, welche dieser Informationen richtig sind. Das wäre eine Technik, die aber eher der Strohhalm ist, nach dem man greift. Man hat an vielen Stellen nur wenig Möglichkeiten. Wenn es um Geheimnisse geht, die wir als Zugang zu Diensten oder Ähnliches nutzen, wäre der Rat, die einfach durch neue Zugangskennwörter auszutauschen. Das Problem mit dem abgeschlossenen Geheimnis ist, dass sich jemand illegitim Zugang zu einem Dienst verschafft und unter der Identität agiert, um das in den Griff zu kriegen.

Münz: Wir haben jetzt darüber gesprochen, dass Informationen geleakt sind, und dass Kriminelle die bekommen. Gibt es Menschen, Kriminelle, die sich die Mühe machen, unterschiedliche Daten zu einem Paket zusammenzutragen und daraus Schindluder zu treiben, beispielweise Fake-IDs zu erstellen? Macht jemand sich die Mühe, um das, was an verschiedenen Stellen im Netz ist, zusammenzutragen?

Meier: Definitiv. Das ist auch sehr lobenswert. Ich will es an einem Beispiel klar machen. Wir haben schon über die Energiepauschale gehört, weil es ein aktuelles Thema ist, das viele betrifft, und manchmal genutzt wird, um Leute auszutricksen und zur Preisgabe von personenbezogenen Daten zu bewegen. Michael, ich habe von Ute über dich gelernt, dass du Platten auflegst. Vielleicht buche ich dich für eine Veranstaltung oder mache dir ein Angebot zu der neuesten Platte von XY zu einem besonderen Preis und versuche, dich in den Kontext zu bringen, wo du eine gewisse Vertrauenswürdigkeit mit dir trägst und auf den Link klickst. Genau für so etwas werden diese Informationen genutzt beziehungsweise können genutzt werden, um einen Kontext herzustellen, in dem man ein Opfer zu Dingen bewegen kann, die er besser nicht tut.

Münz: Ich kann dir sagen, das ist auf jeden Fall vielversprechender als die E-Mails zum Thema „14 Kilo in 4 Wochen abnehmen", die ich gerade kriege. Bei einer John Prine Platte im

guten Zustand müsste ich mich zurückhalten. Ich verstehe aber jetzt das Prinzip. Danke für die Einordnung.

Lange: Wir sind viel online unterwegs. Wir haben uns jetzt Social Media-Profile und Postings angeguckt, aber wir haben auch Informationsverhalten. Wir wollen etwas recherchieren, zum Beispiel zum Thema Energiepauschale. Ich möchte wissen, wie das funktioniert, und gehe ins Internet. Was hinterlasse ich dabei für Spuren, die vielleicht unvermeidbar sind? Wo kann ich durch mein Verhalten Dinge lassen, die zum Beispiel zu einem umfassenderen Profil von mir führen?

Meier: Im Prinzip gibt es verschiedene Vorgehensweisen. Man muss verschiedene Arten von Datensammlungen unterscheiden. Wenn man zum Beispiel im Onlineshop einkauft, wollen die uns nur Gutes. Die versuchen, unser Einkaufserlebnis zu optimieren und die besten, interessantesten Angebote direkt als erstes zu platzieren. Dazu müssen Sie uns kennenlernen. Genau dieses Kennenlernen heißt, dass sie immer wieder erkennen, dass es Michael Meier oder Ute ist, der oder die einkauft. Dafür muss man zunächst irgendein Merkmal erfassen, sodass ich denjenigen, der gerade in meinem Onlineshop ist, wiedererkenne. Dann kann ich sein Verhalten im Shop über die Zeit erfassen und analysieren und ihn davon ausgehend mit entsprechenden Angeboten versehen. Zum Beispiel, weil ich gesehen habe, dass der sich für Fahrradkleidung interessiert, was bedeutet, dass er mit einem Fahrrad fährt. Vielleicht will er auch ein neues Fahrrad kaufen. Die Werbeindustrie versucht, die Einkaufsabläufe zu optimieren. Man kann immer argumentieren, dass es im Interesse des Kunden ist. Vielleicht ist es so, aber es ist in erster Linie im Interesse des Verkäufers, weil er seinen wirtschaftlichen Erfolg damit steigern will. Unter Umständen ist es mir als Einkäufer nicht recht, dass der Laden mich so gut kennt und durchleuchtet. Ich habe Möglichkeiten, mich dagegen zu wehren, dass der Laden mich immer wieder erkennt. Zum einen kann ich die sogenannten Cookies, die man an vielen Stellen akzeptieren muss, ablehnen. Wenn man noch ein bisschen weiter gehen will, wobei man dafür fast technischer Experte sein muss, kann man sich anonymisiert im Internet bewegen. Dann ist es für so gut wie niemanden möglich zu erkennen, wer man ist und dass man, wenn man wiederkehrt, schon da war. Normale Verbraucherinnen und Verbraucher können einfach die Cookies ablehnen, wenn man Sorge hat, dass der Verkäufer, bei dem man regelmäßig ist, zu viel über einen lernt.

Münz: Wir haben viel über uns als Personen gesprochen und darüber, wie wir mit den Daten, die wir preisgeben oder die uns abgeknöpft werden, in ungewollte Situationen geraten. Hat dieses Datensammeln oder die Möglichkeiten, die sich daraus ergeben, nicht auch eine Dimension, die über das Individuum hinausgeht? Macht es was Gesellschaftliches? Ändert das was, wenn wir mehr oder weniger vorsichtig sind mit den Daten, die wir preisgeben?

Meier: Es tut das. Das ist auch das Hauptproblem. Natürlich kann ich mich als Einzelner beschweren, wenn jemand meine Daten stiehlt und meine Dienste auf meine Kosten nutzt. Das ist schon ein Problem, aber es geht noch weiter. Vielleicht nutzt er diese Dienste, um damit gegenüber anderen aufzutreten. Zum Beispiel meldet sich jemand bei meinem Twitter-Konto an und gibt Nachrichten unter meinem Namen preis oder er meldet sich bei

meinem E-Mail-Konto an und schreibt E-Mails in meinem Namen. Das heißt, er nutzt die Reputation meiner Person gegenüber anderen, indem er meine Identität nutzt. Die anderen haben dabei so gut wie keine Chance, festzustellen, dass es nicht Michael Meier ist, der am anderen Ende kommuniziert, sondern irgendjemand, dem es gelungen ist, die dienstspezifische Identität von Twitter oder von E-Mail zu übernehmen und damit zu kommunizieren. Wenn das um sich greift, haben wir eine Situation, in der wir nichts und niemandem mehr vertrauen können, da jegliche Kommunikation gefälscht sein kann. Das bringt eine unsichere Situation und man muss sich fragen, ob wirtschaften, handeln, Austausch und Kommunikation überhaupt noch funktionieren können, wenn man sich nie sicher sein kann, dass auf der anderen Seite nicht jemand ganz anderes gerade aktiv ist und sich nur einer bekannten Identität ausgibt.

Münz: Das heißt, dass wir am Anfang mit der Frage über den Twitter-Account des Bundeskanzlers richtig gelegen haben. Wenn man in der Politik oder in der Gesellschaft niemandem glauben kann, weil es immer sein kann, dass jemand anders die Strippen zieht, hat es Auswirkungen auf unser Zusammenleben als Gesellschaft.

Meier: Genau. So ist es.

Münz: Wir haben auch geguckt, was wir über dich finden können, und es gibt keine großen Enthüllungen. Da kann ich dich beruhigen. Dies bringt uns zu der Frage, was du machst, damit Typen wie Ute und ich nichts von dir finden, was nicht gefunden werden soll.

Lange: Ich könnte zum Beispiel bei dir, Michael Meier, nicht über Frisuren, Karneval oder Urlaub sprechen. Wir hatten gehofft, dass wir ein bisschen mehr außer deiner Berufstätigkeitsidentität finden, aber du machst etwas anders als wir. Uns interessiert natürlich, was das ist.

Meier: Ich glaube, dass der Hauptunterschied daran liegt, dass ich viele Onlinedienste nicht nutze, nicht weil ich etwas gegen die habe, sondern es ist einfach nicht in meinem Interesse. Wenn ich auf Reisen gehe, berichte ich nicht darüber. Das ist einfach nicht mein Hobby. Ich nutze schon ein paar soziale Netzwerke, insbesondere um Kontakte zu Menschen aufrechtzuerhalten, die ich aus der Vergangenheit kenne oder mit denen ich weiterhin Kontakt haben möchte, aber auch da bin ich nicht der intensive Berichterstatter über das, was mir heute passiert ist. Es geht um Kontaktpflege, Kontaktaufnahme, kurzen und sehr spezifischen Austausch. Ich glaube, das ist der Hauptunterschied und der Grund, warum man zu meinem Privatleben wenig online findet, nämlich weil ich es nicht dokumentiere.

Lange: Das ist eine bewusste Entscheidung, sich zurückzuhalten und es für berufliche Zwecke zu nutzen.

Meier: Es ist zum einen eine bewusste Entscheidung und zum anderen liegt es nicht in meinem Interesse, das zu tun. Es ist nicht so, dass ich es bewusst nicht tue, aus Sorge, dass etwas passieren könnte, sondern mir fehlt einfach das Interesse, solche Dinge zu beschreiben und zu dokumentieren. Ich habe einfach andere Hobbies als diese.

Münz: Über die wir nie was erfahren werden.

Lange: Welche denn? Würdest du ein Hobby hier erwähnen wollen oder geht das zu weit?

Meier: Ich bin zum Beispiel zuletzt wieder dem Sport aufgesessen und versuche es, mich ein bisschen im realen Leben zu bewegen, draußen auf der Straße oder im Wald. Das wäre ein Beispiel von einer Aktivität. Als ich noch jünger war, fand ich es sehr erlebnisreich, sich zu moderner elektronischer Musik zu bewegen. Den Karneval habe ich vor Kurzem entdeckt, indem ich einmal mitgemacht habe. Glücklicherweise kam direkt darauf Corona, sodass meine Neugier, mehr zu erfahren und zu erleben, ein bisschen ausgebremst wurde. Das wird sich aber in näherer Zukunft vielleicht ändern.

Lange: Spannende Gemeinsamkeiten. Michael, Michael und Ute.

Münz: Ich wollte kurz für unsere Hörerinnen und Hörer das zusammenfassen, was sie anerkennen müssen, und welche Ratschläge für den digitalen Alltag übrigbleiben. Cookies nehme ich mit. Du hast gesagt, dass es eine Möglichkeit wäre, dafür zu sorgen, dass man nicht immer wiedererkannt wird, wenn man durch eine digitale Tür läuft. Ich habe verstanden, dass Passwörter bei der Frage nach Sicherheit im digitalen Alltag ein Riesenthema sind. Ich nehme mit, dass man in eurem Leak Checker reinschaut, um zu gucken, ob man überhaupt betroffen ist. Was ich auch noch mitnehme, ist die Skepsis bei Anfragen, die vertraut wirken, und zwar dass man im Zweifel doch nicht draufklicken soll. Gibt es noch etwas, was du unseren Hörerinnen und Hörern an dieser Stelle mitgeben willst und was ich unterschlagen habe?

Meier: Ich will bei den Passwörtern ein bisschen konkretisieren. Es ist wichtig, dass man für jeden Dienst ein anderes Passwort benutzt. Bei circa 100 Diensten, die wir heutzutage nutzen, ist es schwierig, sich die alle im Kopf zu merken. Deswegen sollten wir geeignete Hilfsmittel nutzen. Geeignet wäre zum Beispiel ein Stück Papier, das niemals online geht, obwohl es ein bisschen unhandlich ist. Man kann auch den Passwort-Manager nutzen, den einem dabei hilft, sich die Vielzahl verschiedener Passwörter für die einzelnen Dienste zu merken. Das ist ein sehr nützliches Werkzeug, wenn man den richtig benutzt. Ganz grundsätzlich bei allem, was im Digitalen stattfindet, bin ich der Meinung, dass wir ein bisschen intensiver kontrollieren müssen, als wir es im realen Leben tun, weil es dort leichter gefälscht, ausgetauscht und manipuliert werden kann. Wir müssen stärkere Kontrollmechanismen nutzen, zum Beispiel indem wir nachschauen, dass unser Passwort eventuell doch irgendwo abhandengekommen ist. Unter Umständen kann man selbst gar nichts für, sondern die andere Seite hat es verbummelt. Deswegen brauchen wir Kontrolldienste, bei denen man als Verbraucherin oder Verbraucher selbst überprüfen kann, ob solche Daten abhandengekommen sind.

Lange: Zwei schöne Themen aufgenommen, die wir hier öfter besprechen. Michael und der Passwort-Manager sind ein wiederkehrendes Thema, ich will nicht näher darauf eingehen. Das andere ist die Analogie zum Analogenleben. Wir haben schon Gäste hier gehabt, die gesagt haben, dass sie auch nicht ihre Haustür sperrangelweit offenlassen, wenn sie das Haus

verlassen. Wir haben uns im Analogenleben bestimmte Sicherheitsmechanismen angewöhnt, und das hast du schön übernommen, ohne dass du das Gleichnis kennst, dass wir genauso eine Sorgfalt im digitalen Alltag uns aneignen sollten. Wir danken dir ganz herzlich für deinen Besuch, für deine Infos und die Hinweise, die du unseren Hörerinnen und Hörern mitgegeben hast. Wir freuen uns, dass du da warst. Ganz herzlichen Dank!

Münz: Vielen Dank. Das war wieder eine in vielerlei Hinsicht erkenntnisreiche Folge. Ich hoffe, das war es auch für euch, diejenigen, die uns zugehört haben. Auf die nächste Folge freuen wir uns schon sehr, weil wir eure Themen aufgreifen wollen. Schickt uns eure Themenvorschläge, wenn ihr denkt, dass Ute und ich uns darüber austauschen sollten, um euch die wichtigsten Informationen dazu zu geben. Schreibt uns, kontaktiert uns über die BSI-Kanäle auf Facebook, Instagram, Twitter sowie YouTube.

Lange: Unsere E-Mail-Adresse ist bsi@bsi.bund.de. Wir freuen uns auf Post! Bis wir uns wieder hören, liked und folgt Update Verfügbar auf euren Podcast Plattformen. So verpasst ihr keine Folge oder könnt auch frühere Folgen noch einmal hören, wenn sie euch gefallen haben. Wir freuen uns auf das Wiederhören. Bis bald. 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