„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 36 08.11.2023:
Gesichtserkennung, Fingerabdruck und Co. – Die Welt der Biometrie erklärt

Moderation: Ute Lange, Michael Münz
Gast: Martin Gobbin
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: Mein Name ist Michael Münz, und wir freuen uns, dass ihr wieder mit dabei seid, nachdem wir uns schon in der vergangenen Folge beim Thema Fitnessapps näher mit dem menschlichen Körper befasst haben.

Ute Lange: Falls ihr euch jetzt fragt, um was es da geht, und ihr eine Smartwatch habt, dann hört unbedingt in die letzte Folge rein.

Michael Münz: Denn auch dieses Mal geht es um körperliche Themen, sag ich mal. Wir schauen auf Ohren, Augen und Hände, also all die Dinge, die wir als biometrische Daten zusammenfassen, also eindeutige körperliche Merkmale wie Fingerabdrücke, Gesichtsform, Netzhaut der Augen oder Stimme.

Ute Lange: Ja, diese Daten werden im digitalen Alltag immer häufiger genutzt. Face-ID oder auch Fingerabdruck nutzen wir laut einer Studie, die ich gefunden habe, täglich bis zu 60 bis 80 mal so oft schauen wir im Schnitt aufs Handy, und die Studie ist älter. Ich fürchte es ist sogar vielleicht 100 bis 120 mittlerweile, und ich bin schuldig im Sinne der Anklage. Ich glaube, ich greife relativ häufig zu diesem Smartphone.

Michael Münz: Und entsperrst es dann mit mit dem Fingerabdruck.

Ute Lange: Face-ID.

Michael Münz: Ah, okay, alles klar. Ja, ich habe eine andere Situation, wo ich Gesichtserkennung ganz praktisch finde. Ich war letztens auf dem Flughafen unterwegs, und weil ich in einem nicht EU Land gereist bin, muss ich durch so eine Passkontrolle durch und hab mich dann für die biometrische Passkontrolle entschieden, die automatisch passiert, und musste mich dann nicht an die lange Schlange anstellen und fand es total angenehm, weil es einfach meine Wartezeit extrem verkürzt hat.

Ute Lange: Die Wartezeit, Verkürzung finde ich auch sehr angenehm in so einer Situation. Was ich meistens nicht so toll finde, sind diese Aufnahmen, die sie von dir machen. Da sieht man ja aus wie für eine Verbrecher Kartei.

Michae Münz: Nee, ich finde, man sieht aus, als würde man durch so ein Jäger Fernrohr anvisiert werden, ich will das überhaupt gar nicht weiß, was mit einem passiert.

Ute Lange: Ja, Nachteil ist noch ein Stichwort, weil ich bin manchmal in Nachtflügen, das heißt, ich komme relativ früh dann an Flughäfen an, und dann finde ich dieses Licht, das da einem entgegen scheint, nicht so schön. Aber wir schweifen ab. Wir wollten ja über biometrische Daten und deren Sicherheit sprechen, weil es gibt viele Situationen, in denen wir das mittlerweile nutzen zum Einloggen, und irgendwie habe ich den Eindruck, der Trend geht so ein bisschen weg vom Passport.

Michael Münz: Genau den Eindruck habe ich auch, und da wollen wir natürlich wissen, warum biometrische Daten sicherer sein können als bisherige Authentifizierungsmethoden, und natürlich auch, worüber sprechen wir Ute?

Ute Lange: Na ja, wir sprechen darüber, wie wir das einsetzen und es sicher einsetzt, wenn wir es einsetzen, und ich würde auch gerne wissen, wann hat das angefangen? Warum macht man das überhaupt? Und deswegen sind wir total gespannt, was unser Gast zu sagen hat. Wir haben nämlich heute hier im Studio. Ralph Breithaupt, schön, dass du dabei bist!

Ralph Breithaupt: Vielen Dank für die Einladung.

Michael Münz: Hallo, herzlich willkommen auch von mir, Ralph! Du arbeitest im BSI in Abteilung Cyber Sicherheit, in der Digitalisierung und für elektronische Identitäten, und speziell zu jetzt wird es noch interessanter. Bewertungsverfahren für Technologien in der Digitalisierung. Was machst du den ganzen Tag?

Ralph Breithaupt: Ja, ich kann das vielleicht ganz kurz umreißen. Seit 2008 bin ich schon im BSI und komme eigentlich aus einem ganz anderen Bereich. Als Physiker der Grundlagenforschung für autonome Robotik und intelligente Sensor Analyse bin ich zum gekommen, bin dann gleich in das Referat, in dem ich heute arbeite, hineingekommen, und dieses Referat hat im Wesentlichen die Aufgabe, aufkommende Sicherheitstechnologien mit ausreichendem Potenzial zu identifizieren und auf ihre Zuverlässigkeit und auch ihre Schwachstellen hin zu untersuchen. Wenn wir Schwachstellen finden, was eigentlich immer der Fall ist, ist es auch Teil unserer Aufgabe, zusammen mit Herstellern oder Forschungsinstituten oder im Notfall auch alleine angemessene Gegenmaßnahmen zu finden, um die Systeme sicherer zu machen. In dem Zuge habe ich schon mit ganz unterschiedlichen Technologien zu tun gehabt, zum Beispiel interaktive Smartcards, sichere Speichertechnologien oder auch Sicherheit im Automotivbereich. Mein Schwerpunkt aber war von Anfang an der Bereich Biometrie. Zu Beginn lag da der Fokus auf der Fälschungssicherheit biometrischer Systeme, insbesondere Fingerabdruck Systeme.

Aufgrund ihrer Komplexität sehen wir es aber mittlerweile als notwendig an, Biometrie stets ganzheitlich zu betrachten, also die Performanz. Damit ist die Zuverlässigkeit bei der Unterscheidung von Personen gemeint, die Schwachstellen Analyse, insbesondere die Resistenz gegen Fälschung. Das ist ein ganz dickes Thema in der Biometrie und aber auch noch als dritten Zweig die Usability. Das ist so ein Gebiet, was bislang nur recht oberflächlich behandelt wurde, aber tatsächlich ganz große Auswirkungen auf die beiden anderen Zweige hat. Da bei der Biometrie ja immer Menschen mit irgendeiner Maschine interagieren müssen, und je besser sie das tun, desto besser funktioniert auf die Maschine. Um das angemessen tun zu können, leite ich seit 2018 das Team zum Aufbau und Betrieb des Biometrie evaluation Zentrum, kurz zusammen mit der Hochschule rein auf ihrem Campus in aus. Da bin ich auch. Gerade hier haben wir eine Umgebung geschaffen, um biometrische Systeme sehr professionell und effizient zu prüfen und gegebenenfalls neue beziehungsweise verbesserte Sicherheitstechnologien zehn.

Ute Lange: Ja, wenn ich da gleich mal einhaken darf, das finde ich total spannend, auch die Kombination, die du da hast, also sowohl in als auch in der Forschung. Ich würde aber gerne nochmal einen Punkt zurückgehen. Was sind denn aus deiner Sicht, ihr seid ja Expertinnen dafür biometrische Daten, also was fasst man darunter zusammen? Michael hat ja eben schon mal gesagt: Gesicht, Fingerabdruck, ect., aber was gehört für euch alles dazu, was wir vielleicht als gar nicht so einen Blick haben?

Ralph Breithaupt: Also tatsächlich umfasst das Gebiet der Biometrie einer riesengroßen Menge an verschiedenen Merkmalen oder Modalitäten. Dabei muss man sagen, digitale Biometrie umfasst solche biologischen Merkmale, die hoch individuell für einen Menschen sind und technisch erfasst werden können. Sonst macht es ja keinen Sinn. Und da gibt es, wie gesagt, ganz viele verschiedene Modalitäten. Man unterscheidet da zwischen statischen und dynamischen Merkmalen. Zu den statischen Merkmalen also gehören körperliche Merkmale, die sich bei allen Menschen kaum ändern, also klassischerweise Merkmale wie, wie ihr schon gesagt habt, Gesicht, Fingerabdruck oder auch das Wählen, Muster der Hände oder Finger, die DNA oder die Irismuster, aber auch solche interessanten Geschichten wie Ohren beispielsweise, was sogar polizeilich verwendet wird, wenn es Ohren Abdrücke bei Leuten gibt, die an der Tür gehorcht haben. Die kann man tatsächlich benutzen, um solche Leute zu identifizieren. Auf der anderen Seite gibt es die dynamischen Merkmale, da zählt sowas wie die Handschrift dazu beispielsweise. Aber es gibt so nen ganzen Unterbereich der Verhaltens Biometrie, zu der zum Beispiel die Gangart gehört. Also manchmal, wenn man so einen lauten Gang hat wie wir im BSI, hört man immer schon, wer da entlanggeht, der Schrittzahl, der Stärke des Auftritts und andere kleinen Feinheiten, aber auch das Tippen auf der Tastatur und die Bewegung der Computermaus gehören da ganz prominent dazu. Letztere sind zum Beispiel sehr, sehr beliebt in Skandinavien für die Authentifizierung im Online Banking Bereich.

Michael Münz: Wo du jetzt schon online banking, sagst ich, hätten wir jetzt, glaube ich, schon mal drei Anwendungsfälle, die verhältnismäßig weit verbreitet sind, würde ich mal

sagen, also Gesichtserkennung am Zoll oder das Entsperren des Handys? Ähm, zu welchen Gelegenheiten hat sich dann? Haben sich biometrische Daten denn jetzt auch mittlerweile schon durchgesetzt, wo wir sie im digitalen Alltag, wo wir den im digitalen Alltag begegnen?

Ralph Breithaupt: Ja, da unterscheiden wir letzten Endes zwischen zwei Feldern. Das eine ist die Authentifizierung, wenn es also darum geht, einen Menschen so zu prüfen, dass wir sehen können, ob er die Berechtigung hat, um zum Beispiel durch eine Tür durchzugehen, also Zugangs, Authentifizierung oder bestimmte Dienste abzurufen, und auf der anderen Seite haben wir die Identifikation. Bei der Identifikation hat man in der Regel große Datenbanken, die dann benutzt werden, um beispielsweise Bildaufnahmen oder Fingerabdrücke, die man auf, ähm, die man an Tatorten wiederfindet, dagegen zu vergleichen und zu schauen, welche Personen es wirklich ist. Die Identifikation ist da etwas, was wir immer so ein kleines bisschen kritisch sehen, weil man da natürlich auch Menschen überwachen kann, was wir definitiv nicht unterstützen. Wir kümmern uns hauptsächlich um die Authentifizierung, aber es gibt nun mal Fälle, wo das, wo die Identifikation, notwendig ist. Im polizeilichen Bereich beispielsweise ist das so eine wichtige Geschichte. Zum Glück haben wir es hier in Deutschland aber immer mit einem sehr großen Level an Datenschutz zu tun. Die Dsgvo, die Datenschutzgrundverordnung, zwingt alle europäischen Länder dazu, sehr, sehr vorsichtig mit solchen Sachen umzugehen und allgemeine Überwachung auch über die Biometrie nur unter größten Auflagen zu ermöglichen. Die Authentifizierung, wie gesagt, wird in ganz verschiedenen Fällen eingesetzt. Du hast das wesentliche schon genannt, mit dem sich das BSI beschäftigt. Das eine sind Bereiche der Grenzkontrolle, wo es also darum geht, ein Lichtbild aus dem Pass als Referenz zu nehmen und dann ein Livebild dagegenzuhalten, damit zu vergleichen und zu schauen, ob derjenige, der da jetzt durchgehen möchte, auch wirklich zu seinem Pass gehört. Das ist ein ganz, ganz wichtiges Sicherheitsmerkmal, was genutzt wird auf der anderen Seite, neben diesen sogenannten hoheitlichen Anwendungen im polizeilichen und Krenz Kontrollbereich kümmern wir uns aber auch sehr, sehr intensiv um alles, was die Menschen heutzutage so beschäftigt im Alltag. Und da ist das Smartphone. Wann hat es angefangen? 2013, glaube ich, mit Finger-ID ist da einfach ein ganz, ganz wesentlicher Player geworden. Alles landet heutzutage auf dem Handy, von vom Online Payment, E government, Anwendung, Fernsteuerungs, Möglichkeiten, alles Mögliche soll ja im Handy laufen. Wir reden auch schon über Pläne, den Führerschein oder den Personalausweis auf das Handy zu bringen, weil einfach jeder ein Handy hat, und da sind zwei Entwicklungen sehr, sehr wichtig gewesen. Die eine ist, dass die Hersteller die Handys sehr sicher gemacht haben, also die haben die Speicher so abgesichert, dass man die tatsächlich auch im Nachhinein nicht mehr so einfach Foren auslesen kann. Wir haben da so ein trusted Element in diesen Dingern, die auch zertifiziert sicher sind, und das andere allerdings ist dann die Tür, durch die der Mensch durchgehen muss, um sich gegen seinem gegenüber seinem Handy zu authentifizieren, und da haben wir jetzt einige Jahre Erfahrung hinter uns. Jeder hat mal mit Pins versucht, mit Passwörtern oder diesem Insen Muster. Ähm, und ich denke, allesamt sind wir uns einig, dass zwar Pins und Passworte einen beweisbaren Level an Sicherheit haben. Je länger die Pinnen, je länger das Passwort, desto

sicherer ist das. Gegen Blut Force Angriffe ist ganz klar. Aber jetzt kommt wieder der Mensch ins Spiel. Ähm, richtig lange Passworte oder Pins können wir uns einfach nicht merken oder wollen es nicht. Die meisten können es jedenfalls nicht, und dann fängt man an, so ganz leicht erratbare Passworte zu benutzen. Dann gibt es ja jedes Jahr die 100 häufigsten Passwörter.

Ute Lange: Eins, zwei, drei, vier, fünf, sechs, sieben, acht, neun scheint immer noch das beliebteste zu sein, haben wir schon häufiger hier thematisiert.

Ralph Breithaupt: Die, die für die Karte ist, dann mit im Portmonee auf einem Zettel.

Ute Lange: Bei dir etwa nicht, Ralph? Das ist doch der einfachste Weg, sich die zu merken, sonst sperrt man sich die Karte.

Ralph Breithaupt: Ich sage dazu erst mal nichts, aber ein Zettel habe ich jetzt nicht. Ich hab dann einfache Formel für alle meine Passworte, aber der Punkt ist der, der Punkt ist der. Hier kommt jetzt dieser große Vorteil der Biometrie rein, das heißt, wir haben diese sichere Handy. Wir müssen irgendwie Zugriff haben auf das Handy selbst und auf alle Applikationen auf dem Handy, und da muss man sich jetzt irgendwas vorstellen, mit dem man sich als Nutzer gegenüber dem Handy authentifiziert. Pins und Passwörter, wie schon gesagt, sind nicht die beliebtesten, sind jetzt nicht unsicher, aber man kann sie leicht auch umgehen. Zudem muss man sagen, wenn man mal in Köln auf dem, beim Karneval in der Kneipe sieht, wie Leute bezahlen, ist es da immer so eng, dass die Auto Kartenleser ganz hochgehalten werden müssen. Dann kann man wunderbar in den sammeln. Also, es gibt bei jeder Technologie.

Ute Lange: Und du glaubst, im Kölner Karneval kann sich irgendeiner der anderen Gäste dann die Nummer merken, die er oder sie gerade gesehen hat.

Ralph Breithaupt: Der Punkt ist, hier sieht man ganz deutlich den Vorteil und den Grund warum. Wann war das Mai 2022 die großen Hersteller Microsoft, Google, Apple und Co sich entschlossen haben, mit dem Projekt zu sagen, ja, Pins und Passwörter will keiner mehr. Wir brauchen alternative Authentifizierungsmöglichkeiten im Handy, und da bleibt ja dann nur noch die Biometrie übrig. Keiner will noch extra token oder andere Schlüssel mit sich schleppen. Das heißt, die Biometrie wird am Ende der einzige Schlüssel sein, mit dem wir das Tor zum Handy aufmachen und zu allen Diensten des Smartphones. Und da muss man natürlich dann sich ganz genau die Frage stellen, wie sicher sind denn jetzt wirklich biometrische Systeme, wie zuverlässig sind die? Und tatsächlich fängt es dann an, sehr komplex zu werden, insbesondere auch für so eine Zertifizierungsstelle wie dem BSI.

Michael Münz: Noch einmal, weil ich gerade anfange, mich mit einem Passwort Manager zu befassen und da jetzt alles zu transferieren, damit ich halbwegs sicher digital unterwegs bin und meine Zettelwirtschaft mal aufhört. Lohnt sich der Aufwand noch, Ralph, oder erzählt er mir in sechs Monaten, dass das mit den Passwörtern vorbei ist?

Ralph Breithaupt: Also tatsächlich befasse ich mich ja jetzt seit über 15 Jahren mit Biometrie. Ich mag die Technik sehr gerne, aber sie ist von allen Authentifizierungsmethoden die komplexeste, nicht aus Sicht der Nutzer. Da muss man, da kann man nichts vergessen, da kann man nichts verlieren, man hat seinen Finger dabei, sein Gesicht dabei. Das ist wirklich das wunderschöne an der Sache. Das Dove ist, die gesamte Komplexität kommt so richtig auf Seiten der Entwickler auf der einen Seite. Die haben es wirklich sehr, sehr schwer in diesen wdrei Bereichen: Performanz, Überwindung, Sicherheit und und usability. Das ist wirklich eine Riesenherausforderung. Immer noch, aber auch für uns, für die Leute, die es evaluieren und testen sollen, wird es immer schwieriger, das zu tun, denn man braucht wirklich, um das testen zu können, immer wieder viele, viele Menschen, die, die als Tester zur Verfügung stehen, oder Evaluatoren, die mit sehr viel Erfahrung diese Systeme dann angreifen. Aber um deine Frage zu beantworten, ja, es lohnt sich auf jeden Fall. Also im Augenblick sind wir fest der Meinung, dass man sich noch nicht 100 prozentig nur auf die Biometrie verlassen sollte. Wir plädieren da sehr, gerade bei Anwendungen, um die es auch wirklich um Geld geht, wie online banking, Videoident, Verfahren und ähnliches, für die zwei Faktor Lösung, also immer eine Kombination aus etwas leichter, wie zum Beispiel Biometrie, und etwas sicheren wie einem Passwort oder einer. Das macht im Augenblick den größten Sinn, teilt so ein bisschen die Last auf und erhöht die Sicherheit ganz enorm.

Ute Lange: Mich interessiert das, ist jetzt vielleicht noch mal einen Schritt zurückgesprungen. Aber die Biometrie forscht ja nicht und ist nicht erfunden worden, damit wir ein sicheres Smartphone haben, obwohl wir jetzt davon profitieren, und du bist ja schon ganz lange tätig. Ich denke bei sowas ja auch gerne mal an so ältere Jameson Filme, wo das damals Science Fiction mäßig gezeigt wurde. Also dass, das klingt jetzt vielleicht nicht so schön, aber dass man sich ein Finger von jemanden besorgt hat in so einem Film, um das dann da draufzulegen oder sogar ihres nachempfunden hat, das ist ja eher die kriminelle Seite. Aber es wird ja einen guten Grund gegeben haben, warum man das überhaupt entwickelt hat. Das interessiert mich auch, und nun haben wir schon Experten hier heute vor Mikro, also ohne dass wir jetzt den ganzen Podcast in diese Richtung entwickeln wollen. Aber ganz kurz mal erklärt, wo kommt das eigentlich her, wofür war das anfangs gut?

Ralph Breithaupt: Ich versuche mal ganz kurz, also, wie schon sagte, kann man Biometrie für unterschiedliche Anwendungsfälle einsetzen. Authentifizierung ist eine Sache, also wenn James oder mit einer geklauten Hand durch eine Tür geht, durch die nicht gehen, dann ist das eine Sache. Die Identifikation in der Kriminalistik ist die andere Geschichte. Die Geschichte der Biometrie ist tatsächlich schon recht lang, aber letzten Endes muss man sagen, die Biometrie nutzt da ja ein Prinzip, das für uns Menschen ganz natürlich ist. Wir erkennen uns untereinander über das Gesicht, über die Stimme, manchmal auch über Bewegungsmuster oder ähnliche Eigenheiten, und dieses Prinzip wurde jetzt einfach in die Technik übertragen. Das BSI beschäftigt sich da schon jetzt seit Ende der 90er-Jahre, mit dem Mit, mit dem Fach der Biometrie. Damals fing das ganze an, dass politische Entscheidung getroffen wurde, Gesicht und Fingerabdruck in den elektronischen Reisepass

und den Personalausweis zu überführen und das dann später zum Beispiel bei der Polizei, aber auch bei den Grenzkontrollen elektronisch auszulesen und zu nutzen. Und da wurde natürlich die Frage gestellt, wie sicher ist das denn? Jetzt können wir uns darauf verlassen, ist jetzt lange her, 25 Jahre, und es hat sich viel getan in der Zeit. Die Geschichte der Biometrie ist allerdings viel älter, wenn man noch ein kleines Bisschen zurückgeht. Ende des 19 Jahrhunderts hat der Indische Herrscher Fingerabdrücke benutzt, um mehrfach Auszahlung von Pensionen in Indien zu unterbinden. Das heißt, Leute kamen dahin, haben ihr Geld bekommen und damit man wirklich feststellen konnte, dass das nicht immer dreimal derselbe war. Was vorher vorgekommen ist, hat man sich den Fingerabdruck angeguckt. Kurze Zeit später also. Es hat dann sehr schnell die Runde gedreht, hat dann Serve Francisco wissenschaftlich bewiesen, dass sie sich bei Fingerabdrücken um ganz hoch individuelle Merkmale handelt. Selbst Zwillinge haben nicht dieselben Fingerabdrücke, dieselben Grundmuster, aber nicht dieselben Minuten. Und einige Jahre darauf wurden dann Fingerabdrücke ganz schnell über England dann in der Kriminalistik eingesetzt, 1903 dann zum ersten Mal in Deutschland, in Dresden. Fingerabdrücke als Quellennachweis finden sich aber schon in China, im 17 Jahrhundert, aber noch viel später, in Ägypten, hat man alte Ton Siegel gefunden, wo Leute in Fingerabdruck reingedrückt haben, um als Erkennungsmerkmal genutzt zu werden. Also die Idee ist schon sehr alt.

Michael Münz: Von der also auf die Liste der Begriffe, die ich dann heimlich nach so einer Podcastaufnahme google, nehme ich jetzt Minuten mal mit auf und gucke das nochmal nach, was das genau ist.

Ralph Breithaupt: Da kann ich ganz kurz erklären, es geht ganz schnell, es kann jeder an seinen Fingern ziehen. Die Finger haben sogenannte Papillarlinien, also Linien, Muster. Das haben auch Affen beispielsweise noch viel schöner als wir, und an den Füßen noch viel stärker ist einfach eine biologische Hilfe, um besser greifen zu können, um nicht so leicht abzurutschen, besser als glatte Haut. Und diese Linien musste haben eine Grundform in so schleifen Wirbel und was machen? Und Bögen, die man da unterscheidet, und jede Linie endet auch mal oder verzweigt sich. Und diese Punkte, wo sie enden oder sich verzweigen, die nennt man Minuten, und die sind bei jedem Menschen tatsächlich hochindividuell. Und wenn man einfach die Punkte einzeichnen, kriegt man so einen Punkt und musste das tatsächlich sehr schön benutzt werden kann, um Menschen voneinander zu unterscheiden.

Michael Münz: Ich überlege gerade, ob du in deiner Freizeit auch Wahrsager bist, halten sich sehr gut mit den Händen und so wenigen Linien und so weiter auskennst, also ob das vielleicht noch?

Ralph Breithaupt: Ja, das war mein Job, ist er immer noch.

Ute Lange: Und wenn ihr da draußen wüsstet, wie wir jetzt alle hier auf unsere Finger gucken im Studio, dann würdet ihr euch amüsieren. Aber zurück zum Thema. Spannend. Wie lange es das schon gibt, ist es also nicht erfunden worden, um Sicherheit in Smartphones

irgendwie zu erhöhen? Aber wir nutzen sie sehr viel. Das heißt, du hast einige der Vorteile ja schon genannt, die wir als Verbraucher und Verbraucherinnen haben, dass sich diese Technologie so entwickelt hat und eben jetzt auch von Herstellern genau für dieses Gerät, das uns im Alltag begleitet und irgendwie so unser Leben auch organisiert und regelt. Was sind denn vielleicht ein paar Nachteile, wenn ich das jetzt nutze? Also, ich mache das sehr, habe ich ja anfangs auch schon bekannt. Ich habe bei vielen anderen Wendungen also nicht nur ein Passwort Manager und mein Wort für die zweite Stufe, aber ich finde das eigentlich sehr praktisch. Bin ich damit gut beraten, mich so darauf zu verlassen, oder gibt es da ein paar Sicherheitsaspekte, wo du sagst, ja, bei der einen oder anderen Sache sollte man noch mal überlegen, ob es nicht doch noch so eine klassische Lösung gibt.

Ralph Breithaupt: Ja.

Ute Lange: Ja, genau!

Ralph Breithaupt: Also, die Biometrie macht die ganze Thematik ein bisschen komplizierter, und das kommt daher. Wenn man es mit normalen Pins oder Passwort und zu tun hat, dann kann es ja mal sein, dass das Passwort oder die Pin auch mal in falsche Hände gerät. Wenn man das weiß, man hat den Zettel verloren zum Beispiel, dann kann man zu seiner Dienststelle gehen und sagen, bitte, gebt mir ein neues Passwort, bitte gebt mir eine neue Pin. Das ist jetzt mit dem Gesicht ein bisschen schwieriger, das heißt sogenannte Revocation oder Erneuerung von von diesem Passwort biometrischer Eigenschaft. Das ist schon ein bisschen schwierig. Bei Finger haben wir zum Glück in der Regel zehn davon. Da könnten wir zur Not auf den anderen Finger gehen, aber auch bei bei der Hand beispielsweise wird es dann auch schon wieder sehr eng. Das heißt, wir haben bei der Betrie einfach den Fall, dass wir anders denken müssen. Beim Pin oder Passwort reden wir von einem Geheimnis, man kann bei einem Gesicht aber wirklich nicht mehr von einem Geheimnis sprechen. So, und das bedeutet, dass unsere Anwendungen, die wir mit Biometrie schützen, mit anderen Regeln spielen müssen. Die müssen von vornherein darüber nachdenken. Wie kann ich das System vor Missbrauch schützen? Das ganz grundlegende Regel ist immer, immer, wenn man eine Annahme hat, bei einer Sicherheitstechnik, die man nicht prüft, hat man Sicherheitsproblem. Bei der Biometrie ist es die Annahme, dass da ein Mensch steht, der seine biometrischen Merkmale einem Sensor zeigt. Das sind auch wirklich seine, und anhand der Merkmale kann man ihn jetzt authentifizieren oder eben nicht. Das Problem ist, wenn man das nicht überprüft, ob das auch wirklich so passiert, dann kann es sein, dass ein Mensch, der andere Merkmale, die ihnen Sensor hält, zum Beispiel gefälschte Finger oder eine eine Gesichtsmaske oder einfach nur ein Foto von einem von dem Menschen, der eigentlich authentisiert ist, mit einem Display, also mit dem Handy, einfach die Kammer halten. All das ist auf einmal möglich. Da reden wir halt von Artefakten oder Fälschungen nach ISO, von Präsentation, Attac, also nach Angriffen auf die Präsentationsphase in der Biometrie, und das ist ein generelles Problem, mit dem wir uns in der Biometrie natürlich rumschlagen müssen. Normalerweise ist Biometrie immer dann besonders toll, wenn man es in Superweist, also in überwachten Situationen, anwenden kann. Wenn ein Mensch steht, der genau sieht, was da

passiert, und wenn er genau hinguckt, ist es dann mit den Fälschungen auch oft sehr, sehr schwierig in allen sogenannten Angst superweist, also nicht überwachten Situationen, und da gehört das Handy hier nur mal dazu, haben wir das Problem, dass wir sagen können, selbst wenn die Zuverlässigkeit der Biometrie hoch genug ist, also die Erkennungsraten, die sind wirklich mittlerweile gerade in der Gesichtserkennung unglaublich hoch geworden, sehr zuverlässig geworden, ist, wirklich toll. Was da gemacht wird, gemacht wurde, haben wir immer noch das Problem, dass wir uns gegen Fälschung wehren müssen. Das heißt, gerade die Flexibilität, die bei der Erfindung der biometrischen Algorithmen erreicht worden ist, da kann man mittlerweile zehn Jahre älter sein oder mal die, mal die sein oder mal sonnengebräunter Haut haben oder ähnliches, sogar eine Brille aufsetzen. Das macht alles heute überhaupt nichts mehr. Auch Kopfdrehungen, die früher schwierig waren, sind heute kein Problem mehr. Aber gerade diese Flexibilität sorgt dafür, dass ich fast alles in den Sensor zeigen kann, was auch nur ansatzweise die richtigen Merkmale aufweist. Das heißt, da ist Tür und Tor geöffnet für den Einsatz von Fälschung. Da kann man mal sehen, wie sich die Gebiete so gegenseitig bedingen, und das heißt, wir haben jetzt schon seit vielen Jahren die Aufgabe auch mit den Herstellungen und mit Forschungsinstituten angegangen. Also nicht nur wir natürlich da Methoden zu finden, wie wir Fälschung erkennen können. Da gibt es solche Methoden, wie ein Sensor, der Haut erkennt beispielsweise und Haut von anderen Materialen unterscheiden können, weil wir davon ausgehen, dass die meisten Gesichter schon aus Haut bestehen oder die Finger. Da haben wir Pulserkennungen beispielsweise. Da haben wir Ähm, drei d Erfassungssysteme, die schauen, ob das, was da in den Sensor gehalten wird, wenigstens so grundlegend die Form eines menschlichen Gesichtes hat, und ähnliche Sachen. Also, es gibt Fingerabdrucksensoren auf dem Markt, die haben bis zu 40 sogenannte Pd, also Präsentationen, die taktischen Fälschungs, Erkennungs Kanäle, die dann irgendwie das miteinander so verrechnen müssen, dass sie hoffentlich wirklich echte Finger von allen möglichen Fälschungen unterscheiden können. Und hier haben wir das Problem für die Hersteller, aber auch für uns als Tester, die das dann ja irgendwann zertifizieren und feststellen müssen, dass es keine vollständige Liste an fälschungs Materialien gibt. Man kann da von vom Baumarkt, also von silikonen Latex und was der, was Klebstoffe bis hin in die Küche gehen, verschiedenste wie ein Apfel hat oder sonst irgendwas benutzen, Zwiebel hat, habe ich mal benutzt. Das war auch sehr hübsch.

Michael Münz: Und das hat funktioniert?

Ralph Breithaupt: Ähm, das kommt halt immer auf das System an.

Ute Lange: Wir wollen jetzt aber keine Anleitung für Fälschungen geben.

Ralph Breithaupt: Heute nur sagen, wie umfassend das ist, und jetzt, welche Nachteile, war die Frage. Dann bringe ich vielleicht mal auf den Punkt, jetzt, wo die Biometrie in den letzten 20 Jahren, gerade in den letzten zehn Jahren, unglaubliche Fortschritte gemacht hat, gerade in der Gesichtserkennung, haben wir es mit Systemen zu tun, die tatsächlich Anforderungen erfüllen können, nominell zumindest, die man für Hochsicherheitsbereiche benötigt,

beispielsweise wir haben, da kann man mal nachgucken, das hat Anforderungen, normal, substanziell und hoch, und es ist immer der Wunsch, jetzt die Biometrie auch in die höchsten Sicherheitsbereiche einführen zu können und benutzen zu können. Jetzt haben wir ein doppeltes Problem, da man Biometrie eigentlich immer nur mit dem mit dem echten System in einer realistischen Umgebung mit möglichst vielen echten Personen testen kann. Man kann da nicht ihre Tochter benutzen oder irgendeine alte Datenbank von einem anderen Sensor. Das geht nicht. Man braucht wirklich das System, so wie es dann eingesetzt werden soll, muss das mit echten Menschen testen. Haben wir da einfach ein Zahlenproblem nach der, wenn ich jetzt mal eine Zahl in den Raum schmeiße, ist die Anforderung einer falsch Akzeptanzrate, also einen Fehler bei der Erkennung in der Biometrie von eins zu 330000 notwendig, um sie für die höchste Sicherheitsstufe zulassen zu können. Das wäre dann nach Adam Riese und Statistik müsste ich da 1 Million Leute durch ein System jagen, um festzustellen, ob diese Zahl auch wirklich erreicht wird. Es gibt da nur noch ein paar, ich sag mal, nicht ganz mathematische Tricks, wie man das reduziert. Aber letztlich kommt man da immer noch nur auf ein paar Tausende, die man auf jeden Fall dadurch jagen muss, um festzustellen, ob diese Leistungsklasse erreicht wird. Bei den Fälschungs Angriffen, also bei der Testung der Fälschung Erkennung, hat man ein ähnlich großes Problem. Es gibt unheimlich viele Möglichkeiten und nämlich viele Materialien, mit denen man ein solches System angreifen kann, und da ist es eine große Herausforderung, so viel zu testen, dass man wirklich sagen kann, ja, jetzt habe ich tatsächlich die Stufe erreicht, und da sind wir gerade. Wir sind gerade dabei, dass die Hersteller sagen, ich habe die Leistungsfähigkeit, ich kann das, und der Rest der Welt, also gerade die, die Zertifizierungsstellen in der ganzen Welt, haben gerade das Problem, einen Weg zu finden, das auch wirklich nachzuweisen, um dann die Zulassung zu gewinnen. Das wollen wir, da sind wir am Arbeiten dran, aber es ist tatsächlich gerade sehr, sehr schwierig.

Michael Münz: Jetzt, wenn ich mir ein neues Mobiltelefon kaufe, dann ist da ja kein Zertifikat drauf geklebt, dass mir sagt, hier werden die höchsten Sicherheitsstandards eingehalten und durchgeführt. Woher weiß ich denn, dass das Gerät tatsächlich auch so sicher ist, wie es sein sollte, damit niemand anders, mit Zwiebel, Haut und meinem fertigen Fingerabdruck darauf abgezogen, dann mein Handy entsperrt?

Ralph Breithaupt: Also, beim Smartphone haben wir es tatsächlich zwar mit dem größten biometrischen Markt zu tun. Wenn dann an einem Wochenende 100 Millionen Geräte verkauft, dann kann man da mit den etlichen Bereichen wirklich nicht gegen Anstinken. Aber da hat es bislang andere Regeln gegeben, muss ich ganz klar sagen. Im hoheitlichen Bereich war die Sicherheit immer an erster Stelle. Da musste man wirklich verhindern, dass die falschen Leute über die Grenze kommen. Deshalb war das immer ein ganz, ganz großer Punkt, der auch sehr zentral bei den Systemen bedacht wurde. Bei den Smartphones lief das so ein bisschen anders. Die Smartphone Hersteller haben von Anfang an eher auf Konvinienz, auf die Bequemlichkeit der Nutzer einen Schwerpunkt gelegt. Deshalb waren die ersten biometrischen Sensoren zum Fingerabdruck, Sensoren, die wir hatten. Ähm ja, also nicht

nicht auf Sicherheit entwickelt worden, sondern da ging es darum, dass es schnell gehen muss und dass man möglichst wenig falsch Rückweisung raten hatte. Das hat man sehr schnell gemerkt. Ähm, und wir haben dann sehr viel mit den Herstellern diskutieren müssen über Jahre, dass wir gesagt haben, bitte, bitte, nehmt dann auch die Falscherkennung, die Fälschungs Erkennung mit in euer Portfolio auf. Nehmt das bitte ernst! Und am Anfang haben die gesagt, ihr hört mal zu, unsere Lifecycle Lifecycle unserer Produkte ist 18 Monate. Ähm, da können wir eigentlich jetzt keine große Kommune Criteria Zertifizierung, die ein Jahr dauern kann und richtig viel Geld kostet, durchziehen. Das würde nichts bringen, und außerdem, so, eine Zertifizierung ist nur so lange gültig, wie die Hardware und Software unverändert bleibt. Also bei jedem Abdate müsste man das eigentlich erneuern. Das waren so ein bisschen versteinerte: Ähm.

Michael Münz: Äh, ja!

Ralph Breithaupt: Herangehensweisen bei Zertifizierung als BSI haben wir anders als die internationale Zertifizierung auch nationale Sachen, wie technische Richtlinien zum Beispiel, wo wir da ein bisschen flexibler sein können, und das tun wir auch gerade. Da haben wir so eine technische Richtlinie entwickelt, die 31, 66 speziell für Biometrie in mobilen Endgeräten. Da versuchen wir, das mal ganz neu anzupacken. Die ist auch veröffentlicht, kann man sich mal angucken, und da wird man auch merken, wir versuchen wirklich unser Bestes. Aber es ist auch wirklich schwierig, dieses System einzufangen. Die gute Nachricht ist, die Hersteller sind mittlerweile auf die andere Seite gewechselt. Die haben Fälschung, Erkennung als wichtiges Thema identifiziert und akzeptiert. Also Apple, Google und Co haben das einfach jetzt als notwendige Forderung für ihre Hersteller eingebracht. Appel mit face de ist da ja auch eine ganz bekanntes Verfahren. Aber auch alle anderen haben mittlerweile mindestens einen Fingerabdruck oder Gesichtserkennung mit drin. Und vor kurzem mussten wir einen Schnelltest machen. Für die Gesundheitsakte und das E Rezept mussten wir ganz schnell die Frage beantworten, wie sicher sind denn jetzt die aktuellen Smartphones für den Einsatz, für diese Government Anwendung? Da hatten wir nur ganz wenig Zeit, haben uns ganz schnell die wichtigsten Smartphones Deutschlands besorgt und haben die uns genau angeguckt.

Michael Münz: Hm!

Ralph Breithaupt: 5000.

Michael Münz: Ende zusammengebracht. Die haben ihre Finger darauf.

Ralph Breithaupt: Ja, wir haben tatsächlich erst mal nur die Fälschungs Erkennung überprüft, ob das zumindest sicher ist, und da mussten wir feststellen, die, die Welt ist noch nicht ganz perfekt, aber die Hersteller sind dabei. Gerade bei der Gesichtserkennung ist viel passiert. Es war vorher völlig ungeschützt, also da hätte man irgendein Foto oder sonst irgendwas da vorhalten können, und das war's. Dann gab es die ersten Blinzeln, Erkennungs, Fälschungs Finder. Da musste man halt die Augen ausschneiden, seine eigenen durchstecken und blinzeln oder stift hinten hoch und runter halten. Dann war das mit der blinzler Kennung

auch durch. Also diese Entwicklung hat es beim Smart von dann alles schon gegeben. Mittlerweile werden vor allen Dingen Ki Verfahren eingesetzt, massiv, um Fälschungen zu erkennen, und das ist gar nicht mal so schlecht. Also, es gibt da noch Schwachstellen. Natürlich. Aber der, der erste wichtige Schritt ist gegangen, und ich bin da sehr, sehr froh, dass die Hersteller sich dazu bereit erklärt haben. Beim Fingerabdruck ist noch viel zu tun, finde ich. Da kann man noch mehr erreichen, da ist noch Luft nach oben.

Ute Lange: Also, das mit der guten Nachricht hat mich jetzt doch beruhigt. Allerdings sprechen wir ja hier öfter mal auch über die kriminelle Seite dieser IT Sicherheit, das ist ja in jeder Folge sprechen wir über Hecken und andere Angriffe. Mich würde jetzt nochmal interessieren, wie kommen denn die Menschen, die daraus ein Geschäft machen, an meine biometrischen Daten? Also ich lass ja mein Handy auch nicht so oft alleine. Oder wie gibt es da auch mit biometrischen Daten? Wir sprechen ja auch oft über andere Daten. Also, wir hatten mal eine Folge, wo jemand über uns so ein bisschen recherchiert hat und gefunden hat, dass zum Beispiel mich als e Mail Adresse mal in irgendeinem Datenleck oder andere Sachen drin war.

Michael Münz: Nein.

Ute Lange Ja, du hast ja dann auch bitte schön was gemacht. Deswegen ist das ja jetzt auch ganz sicher wieder für dich. Aber was ist mit biometrischen Daten? Wie kommt die Dunkelheit der IT Sicherheit da dran, und wie kann ich das verhindern?

Ralph Breithaupt: Ja, das ist tatsächlich auch ein ganz interessantes Thema, und da zeigt sich, dass man Biometrie ganz unterschiedlich einsetzen kann, im Einfach, und da muss man auch ganz anders denken. Das ist ein wunderschönes Beispiel. Du hast dein Smartphone genannt. Wenn ich mein Smartphone einfach nur erstmal entsperren möchte, ähm, dann ist das eine Sache zwischen einem Menschen und dem Smartphone, und das Schlimmste, was passieren kann, ist, dass ich, dass ein falscher, ein nicht autorisierter Mensch diese Smartphone öffnen kann. Was er dazu benutzen kann, ist, wie gesagt, entweder ein Bild von deinem Gesicht, das kann er aus Facebook geklaut haben, oder einfach direkt abfotografiert haben und dann dem Sensor zeigen oder einen Fingerabdruck. Und bei den heutigen Smartphones, die alle gleich aussehen, schön glatt sind, hinterlässt ein Zeigefinger und Daumen eigentlich überall. Da hätte ich also wirklich überhaupt kein Problem, das. Ich glaube, so zwei, drei Minuten wunderschön abzunehmen und digital ein bisschen nachzuarbeiten und dann daraus eine Fälschung zu machen. Ähm, also, an die Daten kommen geht bei der Biometrie prinzipiell relativ leicht. Bei vielen Modalitäten, bei der Hand Wähne und Finger Wähne, ist es ein bisschen schwieriger. Das kann man nicht so einfach von der Ferne sehen. Ähm, und so muss man tatsächlich bei jeder Mobilität neu drüber nachdenken. Welche Risikofaktoren sind dort zu beachten? Wie leicht ist, die Biometrie zu stehlen in dem Sinne, und wie leicht ist ja auch nachzumachen, das muss man sich tatsächlich immer wieder neu überlegen. Auf einer anderen Seite haben wir das Problem, dass Biometrie auch zentral benutzt wird, also in Datenbanken. Es gab da einige

Dienstleister, zum Beispiel auch Banken, die Biometrie aufgenommen haben und dann zentral gespeichert haben in großen Datenbanken und dann diese Daten benutzt haben, damit man sich online authentifizieren konnte, zum Beispiel über die Kamera. Dann wurde halt das der Vergleich, nicht auf dem Gerät zu Hause gemacht, sondern zentral in irgendeinem Rechenzentrum. Und hier kam es in den letzten Jahren tatsächlich immer wieder zu Daten. Klaus, und ein großer Datenklau hat, glaube ich, mal 80 Millionen Datensätze, Fingerabdrücke, Gesicht und ähnliches gestohlen. Und dann haben wir das Problem, das wir vorhin angesprochen haben, wir können uns jetzt nicht mal eben neues Gesicht zaubern oder neuen Zeigefinger basteln. Ähm, da ist dann die Frage, wie machen wir das ist? Ist dann die Biometrie verbrannt oder nicht? Um das zu verhindern, gab es natürlich die verschiedensten Ideen. Wenn man Datenbanken hat, die man klauen kann, kann man massenhaft angreifen, und der Schaden ist gleich gleichermaßen viel, viel größer, als wenn ich nur ein System eingreife. Ähm, um das dann zu vermeiden, hat man darüber nachgedacht, die templates, also die Daten, die man abspeichert, diese Referenzdaten, gegen die dann verglichen wird, so zu verändern, dass man sie nicht missbrauchen kann, also dass man daraus zum Beispiel nicht die biometrischen Merkmale zurück auslesen kann. Das nennt man dann template Protection Maßnahmen, und da gibt es die verschiedensten Ideen, die auch vielversprechend sind, aber noch nicht ganz den Level erreicht haben, die wir gerne hätten. Eine schöne Kombination ist es also, wenn das unbedingt sein muss, dass dass man zentral biometrische Daten speichert, und dann kann man tatsächlich eine ganz simple Idee anwenden, dass man sagt, dieses Template, also diese Referenz, die ich habe, die teile ich auf, zum Beispiel 70, 30 speichere 70 Prozent beim zentral am Server ab, und 30 Prozent behält der User. Und welche 30 Prozent da sind, das wird dann immer zufällig bestimmt. Wenn ich das so mache, kann ich weder mit dem mit der einen, mit dem einen Teil, noch mit dem anderen Teil irgendwas anfangen. Erst bei dem Vergleich bei dem Prozess, der dann ansteht, die man dann sicher machen kann über Kryptografie, bringe ich die beiden Sachen wieder zusammen, kann dann einen Vergleich durchführen. Ähm, und kann die den biometrischen Prozess beenden. Und selbst wenn dann diese 70 Prozent mal geklaut werden, ist nicht die ganze Biometrie verbrannt. Und das sind so einfache Beispiele, wie man damit umgehen kann. Ähm, ja, und ansonsten muss man sich, wie gesagt, immer wieder überlegen, dass man neben der Biometrie auch noch andere Faktoren parallel benutzt, damit das nicht so stark einreißen kann. Das ist.

Ute Lange: Doch nahezu das perfekte Schlusswort für diejenigen da draußen, die sich jetzt nach dieser Folge überlegen, mache ich das oder mache ich das nicht, oder mache ich das bei allen Sachen? Also das nehme ich jetzt nochmal mit, vielen Dank dafür auf. Das ist auf jeden Fall ein Tipp, den ich beherzige. Ich bin ja auch für bequem. Ich hab ich ja schon bekannt, dass ich diese Technologien ganz gerne nutze, weil vieles schneller geht, aber bei mir ist es häufig so, dass es nur einer von zwei Faktoren ist. Ich hab ja durch diesen Podcast auch eine Lernkurve hinter mir und versuche, mich und meine Daten und auch mein Gerät und alles so zu schützen, dass ich gar nicht erst in die Situation komme, dass ich trubel Sting machen muss oder in irgendeinem Lack oder so auftauche. Was nimmst du denn mit Michael,

nachdem Ralph ja also wirklich von ersten Ton abdrücken bis moderne Smartphones die Biometrie nochmal im Schnelldurchlauf für uns erklärt hat?

Michael Münz: Also, ich würde sagen, die neue Facette in meiner mit diesem Podcast stetig wachsender Paranoia ist es, mein Handy jetzt regelmäßig abzuwischen, damit überhaupt niemand die Fingerabdrücke, die ich da drauf hinterlasse, auch nur annähernd ablesen kann. So. Ich glaube also, ich sehe die Welt ja nach jeder Folge immer mit neuen Augen, und das ist jetzt, ich würde mein Handy jetzt mit neuen Augen sehen und regelmäßig fischen.

Ute Lange: Ja, ich sehe dich jetzt also ständig dein handy Screen putzen. Ja!

Michael Münz: Nicht auf die Rückseite.

Ute Lange: Auch alles, ja.

Michael Münz: Die Rückseite natürlich auch, also da können sie drauf verlassen. Neue Bewegung bei mir!

Ute Lange: Ja, okay, aber wie ist es denn für euch da draußen, die jetzt diese Folge hören? Wir hoffen, ihr hattet auch ein paar wichtige Erkenntnisse und Tipps. Was macht ihr denn mit dem gehörten?

Michael Münz: Ja, und das sollt ihr uns bitte sagen, weil uns das natürlich interessiert, was ihr aus dem macht, was wir hier besprechen, und euch vorstellen. Ihr könnt uns das Schreiben über die Kanäle, die es bei YouTube, bei Instagram gibt, bei Facebook also und Tube, oder?

Ute Lange: Die E Mail.

Michael Münz: Die E Mail.

Ute Lange: Ja, es gibt eine e Mail Adresse für den Podcast, und die lautet podcast@bsi.de, und wir freuen uns auf Post.

Michael Münz Und die teilen wir dann auch mit dir. Ralf, vielen dank dafür, dass du da warst und uns diesen geschichtlichen Hintergrund nochmal mitgeliefert hast, von der Antike bis zur moderne. Ganz herzlichen dank! Ich glaube, so eine breite Zeit Spanne hatten wir in der Folge auch noch nie, und ich habe ein bisschen das Gefühl, nach dem, was du so erzählt hast, sprechen wir dich auch irgendwann in naher Zukunft nochmal nochmal zu gucken, wie es sich gerade weiterentwickelt hat, weil ich habe gelernt, dass es ein dynamisches Feld, was du da bearbeitest.

Ralph Breithaupt: Tatsächlich kann ich vielleicht noch hinzufügen, dass jeder etwas dafür tun kann, sein Smartphone beziehungsweise die Biometrie Smartfon besser zu machen. Smartfon. Hersteller denken, dass alle ihre Nutzer besonders auf Bequemlichkeit achten, dass das das allerwichtigste ist. Jetzt muss man aber sagen, so Smarthome benutzen wir für

unterschiedliche Sachen. Man kann 50000 € bei einer Bank in, man kann aber auch einfach nur mal social media account öffnen damit, das heißt, man hat eigentlich Anwendung sehr unterschiedlichen Sicherheitsanforderungen. Was aber die Hersteller noch nicht wirklich umgesetzt haben, ist, das auch auf die Authentifizierungsmethoden umzusetzen. Wir legen einmal wie immer immer gleich unseren Finger auf oder zeigen unser Gesicht ins Handy, und da haben wir jetzt mit den Herstellern darüber gesprochen. Ja, Mensch, wenn es doch um wirklich sichere Sachen geht, Government, Gesundheitsakte, viel Geld, dann fordert doch wenigstens zwei Finger oder Finger und Gesicht, und dann auch übrigens, oder dass man wenigstens mehrfach den Finger auflegt, damit man mehr von dem Finger erfassen kann. Bei all diesen Punkten haben die Hersteller so ein bisschen gezuckt und haben gesagt, ja, das wollen doch unsere Nutzer nicht, das dauert noch zu lange, und das ist viel zu mühsam, und das kann auch schief gehen, und wir sagen da eher, unterschätzt mal bitte die Nutzer nicht! Wenn es dann wirklich um Sicherheit geht, wenn es um was geht, dann sind sie bestimmt auch bereit, noch noch zwei Sekunden mehr zu investieren. Und wenn wir als Nutzer dazu bereit sind, wenn dann erst mal die ersten Hersteller das rausbringen und das dann lieber nutzen als die anderen Sachen, dann zeigen wir den Herstellern, dass es in diese Richtung gehen kann, und es würde die Sicherheit tatsächlich von biometrischen Anwendungen extrem erhöhen. Aber denkt nicht, dass Biometrie generell unsicher ist. Ähm, wir können dieselben Diskussionen für fast alle anderen IT Sicherheit Technologien genauso fühlen.

Ute Lange: Das schöne ist, du kannst ja jetzt mich als Beispiel Anwender nennen. Der würde bestimmt zwei, drei, vier, fünf Finger und auch noch seine Ohren drauflegen, um sicherzustellen, dass ein Mann total sicher ist, weil, wenn er schon bereit ist, dauernd zu wischen, dann macht er das bestimmt auch. Ganz herzlichen Dank für diese Ergänzung, Ralph, noch mehr, um darüber nachzudenken, wie wir sinnvoller und sensibler mit unseren Smartphones und den Anwendungen da drauf umgehen. Wir hören uns wieder, liebe Hörer und Hörerinnen da draußen im nächsten Monat, und wir machen es spannend, weil es ist Weihnachten, da lässt man sich gerne überraschen.

Michael Münz: Genau, und deswegen dürft ihr das Thema in der nächsten Folge selbst auspacken. Wir verraten es hier noch nicht. Ihr müsst jetzt vier Wochen warten.

Ute Lange: Ja, und bis ihr uns wieder hört und wir das neue Thema enthüllen oder auspacken, leigt und folgt ab den verfügbar auf euren Podcast Plattformen, denn so verpasst ihr keine Folge oder hört auch nochmal Ältere rein. Wir freuen uns auf das nächste Mal. Bis dahin, tschüß!

Michael Münz: Tschüss!

Ute Lange: 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