„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 40, 29.02.2024:

Moderation: Ute Lange, Michael Münz
Gast: Stefan Becker (BSI)
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 mit dieser Folge, das verspreche ich euch schon mal jetzt, machen wir euch zu Vorreitern, ach Quatsch, ich sage gleich zu Pionieren im digitalen Alltag.

Ute Lange: Jetzt denkt ihr vielleicht, das ist viel zu hoch gegriffen? Mitnichten. Wir haben in der letzten Folge schon angedeutet, dass wir nichts weniger als das Ende des Passwort-Dschungels einläuten werden – nie wieder kryptische Zeichenfolgen ausdenken und sie nur Millisekunden später auch wieder vergessen. Bleibt also unbedingt dran, um künftig noch sicherer und gleichzeitig viel komfortabler durchs Internet zu ziehen.

Michael Münz: Ich habe es schon mal ausprobiert, und ich kann sagen, es war viel leichter als gedacht. Gut, ich nutze auch einen Passwortmanager. Der hat mir ein bisschen geholfen, aber am Ende war die Anmeldung über einen Passkey genauso komfortabel und leicht wie mit einem althergebrachten Passwort. Also ich sage mal ganz leise: Servus zu eins, zwei, drei, vier, fünf, sechs, sieben, acht. Und: Hallo zu Passkeys! Immer mehr Webseiten bieten diese Form der Anmeldung an. Und darum haben wir gedacht, schauen wir uns das mal genauer an.

Ute Lange: Ja, und wir haben uns auch einen Gast eingeladen, der unsere Fragen – und bestimmt auch eure – weil wir beide hatten schon eine ganze Menge, und das geht euch vielleicht ähnlich – zu diesem Verfahren auch beantworten kann. Er arbeitet im BSI und hat Passkeys vermutlich schon genutzt, als Michael und ich noch diese, ich glaube dreieinhalb Zoll-Disketten waren das, die man so reinschieben musste, als wir die noch genutzt haben zum Speichern. Wir freuen uns auf den Austausch mit dir. Hallo Stefan Becker!

Stefan Becker: Hallo zusammen.

Michael Münz: Hallo, herzlich willkommen auch von mir Stefan! Bevor wir jetzt in den schon eingeläuteten Fragenkatalog einsteigen und dich mit all den Sachen löchern, die wir zum Thema Passkeys wissen wollen, vielleicht noch ganz kurz von dir die Einordnung, was machst du genau im BSI?

Stefan Becker: Ich bin der Referatsleiter Cybersicherheit für die Wirtschaft und Allianz für Cybersicherheit. Das heißt, ich kümmere mich darum, dass die deutsche Wirtschaft noch cybersicherer wird, und habe ein tolles Private Public Partnership, mit dem wir das machen können.

Ute Lange: Wir haben Passkeys in den vergangenen Wochen öfter mal wahrgenommen. Also bestimmte Anwendungen haben gesagt: Jetzt mit Passkey anmelden, und ehrlich gesagt bin ich da immer sehr skeptisch, weil ich nicht weiß, was mich da im Hintergrund erwartet. Wo kommen die her, und warum sehen wir das im Moment so oft, Stefan? Du hast sicherlich selber schon viel mehr Erfahrungen als wir, hilf uns weiter!

Stefan Becker: Ich glaube, wir haben alle erkannt, Menschen können eigentlich keine Passwörter. Wir können das nicht gut. Das ist ein uraltes Verfahren. In der Antike haben vielleicht schon Menschen im Dunkel am Stadttor geklopft und wollten rein, und dann wurde so ein Passwort abgefragt. Und heutzutage haben wir ja Computer, und das könnten wir doch moderner und digitaler und bequemer machen und sicherer vor allen Dingen. Und so sind Passwörter entstanden. Aber ihr habt vorhin gesagt, ich mach das schon seit zehn Jahren. Ja, seit ungefähr zehn Jahren ist die IT- Welt dabei, diesen Standard zu schaffen. Und sie haben auch diese zehn Jahre irgendwie gebraucht, bis es so richtig schön und rund und ganz einfach geworden ist. Also, diese Standards entwickeln sich seit zehn Jahren, und es gibt Teile davon schon ein paar Jahre. Aber jetzt ist es so weit, dass nicht nur die Standards da sind, sondern alle Browser können das, und die großen Anbieter haben es alle implementiert. Das heißt, wir können so etwas verallgemeinert sagen. Wenn wir Passkeys machen wollen, dann geht es jetzt, ich sag mal, vereinfacht, fast überall. Also, es klappt wohl in den allermeisten Fällen.

Michael Münz: Ich frage mich, ja, wir haben ja jetzt ein Verfahren gelernt seit der Antike, wie du vorhin schon gesagt hast, dass wir sagen: Hallo, ich bin´s, und das ist die Parole, die Losung, das Passwort. Und das habe ich jetzt, seitdem ich das Internet nutze, seit Mitte der 90er Jahre gelernt: So geht das. Alle Dienste basieren darauf, und klar, wir regen uns jedes Jahr auf darüber, dass das Passwort, dass die Menschen da nicht kreativ genug sind und auch nicht sicher genug sind. Aber eigentlich läuft es ja. Wieso, sagst du, sind wir als Menschen nicht für Passwörter gemacht?

Stefan Becker: Wir haben ja ganz viele Anwendungen, ganz viele Accounts. Wir haben Mails, wir kaufen irgendwo ein, wir machen unsere Bankgeschäfte online. Das heißt, es gibt einerseits ganz viele unterschiedliche Anbieter, wo wir uns anmelden müssen. Auf der anderen Seite kann das mit dem Passwort auch nur einigermaßen sicher sein, wenn es eben auch gut gemacht ist, und natürlich nicht überall dasselbe Passwort, und das können Menschen sich nicht gut merken. Auch noch die Verbindung dazu: Der Anspruch ist, es sollte auch schon lang sein und komplex, und das klappt einfach nicht. Und ich glaube, wenn wir mal ehrlich zu uns sind, das wissen wir alle: Wie oft ist es uns schon passiert, dass wir ein Passwort vergessen haben? Und da möchten wir doch mal von weg. Es soll doch mal einfach sein, am besten ganz ohne Passwort, Passwordless.

Ute Lange: Michael hat jetzt einen kleinen Vorsprung. Er hat vorhin gesagt, er hat das schon mal probiert. Ich war da ein bisschen zurückhaltender, weil ich Sorge hatte, dass ich mir irgendwas zerschieße und da nachher an nichts mehr rankomme. Aber wir haben ja jetzt dich als Experten hier. Wo liegt denn der Unterschied zwischen dem, was wir kennen – was

Herausforderungen hat, wie wir alle wissen – und dem, was jetzt kommt, nämlich die Passkeys?

Stefan Becker: Die Idee bei Passkeys ist: Wir lassen das mit dem Benutzernamen, das ist ja übrigens ganz oft die E Mail Adresse, und einem Passwort. Wir lassen das einfach mal weg. Wir machen das gar nicht, sondern wir setzen Kryptografie ein, und zwar ein Schlüsselpaar. Und das, was sich jetzt so kompliziert anhört mit dem öffentlichen Schlüssel und privaten Schlüssel, davon bekommen wir eigentlich nichts mit. Aber es werden solche digitalen Schlüssel anstelle von Passwort und Benutzernamen eingesetzt. Wir sehen die nicht, wir fassen die nicht an, wir haben irgendwie damit zu tun. Aber das passiert alles komplett im Hintergrund, und das ist schon ganz tolle Kryptografie, die da im Hintergrund abläuft, also mathematische, komplexe Verfahren, die dafür sorgen, dass ich zum einen von meinem Anbieter, von dem Dienst auch sicher erkannt werde und zum anderen sicher identifiziert werde und das Ganze auch noch verschlüsselt. Das kann keiner klauen. Also, wir haben da einfach ein ganz anderes Sicherheitsniveau, weil man diese Dinge nicht stehlen kann. Da kann sich auch keiner dazwischensetzen. Also ja, er könnte sich physisch dazwischensetzen, aber er kann nichts damit anfangen, kann keinen Unfug treiben. Er kann sich nicht als wir ausgeben, er kann sich nicht als derjenige ausgeben, zu dem wir gerade wollen, wenn wir online einkaufen wollen oder so etwas. Das geht alles nicht mehr. Und das ist der große Sicherheitsgewinn, und es ist komfortabel.

Michael Münz: Ich habe auch erstmal gedacht, das klingt super, und recherchiere mal ein bisschen, wie das funktioniert, und habe auch gleich die Segel gestrichen. Also wir wissen alle spätestens bei Gesundheitsfragen besser nicht im Internet recherchieren, weil man dann hinterher noch viel, viel mehr Fragen hat als vorher. Deswegen habe ich die Recherche dann gleich wieder vergessen und gedacht, ich melde mich mal an und versuch das mal. Und tatsächlich ging das verhältnismäßig komfortabel. Ich nutze einen Passwortmanager, der hat irgendwie die Kommunikation mit dem E-Mail-Anbieter übernommen, mit dem ich das gemacht habe. Und der Verfahrensprozess lief genauso. Und am Ende habe ich gedacht: Hey, es gibt so viele technische Geräte, die ich nutze, wo ich nicht weiß, wie sie funktionieren, ich mache das bei Passkeys jetzt auch so. Aber damit wir zumindest so ein bisschen so einen Anhaltspunkt davon haben, wer kommuniziert mit wem? Wo liegt dieser Schlüssel oder wo liegen diese Schlüssel? Es gibt offenbar mehrere. Wie viel Hintergrundwissen muss man haben? Kannst du uns das vielleicht noch mal ganz einfach erklären, wer da mit wem kommuniziert und wo diese Schlüssel eigentlich liegen?

Stefan Becker: Ich habe ja schon gesagt: Man sieht das gar nicht so, man bekommt das gar nicht so mit. Was wir ja aber im alten Verfahren mitbekommen, ist, dass wir unsere E-Mail-Adresse eingetippt haben, dass wir uns ein Passwort ausgedacht haben, dass wir das meistens auch noch mal bestätigen mussten, damit wir auch sicher sein können, dass es auch von uns richtig geschrieben werden kann. Das lassen wir jetzt weg. Und was dort passiert, ist, dass ich, wenn ich zu meinem Dienstanbieter gehe, egal ob das jetzt ein E-Mail-Dienst ist, ob ich online einkaufen will oder was auch immer wir im Internet tun, und ich sage jetzt, ich möchte gerne Passkeys machen, dann wird tatsächlich dieses Schlüsselpaar, von dem wir reden, das wird jetzt erzeugt. Dazu werden kryptografische Verfahren genommen, und diese Verfahren ergeben jetzt zwei Schlüssel. Davon kriegen wir nichts mit. Das passiert im Hintergrund. Den öffentlichen Schlüssel, den behält jetzt der Diensteanbieter. Und ich bekomme also meinen privaten Schlüssel, und der wird jetzt – ich sage zunächst mal irgendwo abgelegt bei mir – wir können vielleicht gleich noch mal darüber sprechen, wie wir

den verwalten und was wir davon sehen und merken. Und wenn wir jetzt das nächste Mal wiederkommen, also, das heißt, ich möchte online einkaufen, ich möchte mich bei meinem Mail-Dienstleister oder bei Social Media oder wo auch immer identifizieren, und wir wollen ja jetzt sicher sein, dass wir das auch sind: Was dann im Hintergrund passiert, ist, dass der Dienstanbieter, der sendet jetzt diesen öffentlichen Schlüssel, also wir sagen auch, der sendet eine Challenge, also sagen wir mal, eine Matheaufgabe, aber eine total schwierige, lange, hässliche Matheaufgabe.

Michael Münz: Das sind doch alle Matheaufgaben! Entschuldigung!

Stefan Becker: Und was jetzt passiert, ist: Diese Matheaufgabe, diese Challenge, kommt zu uns. Und mit unserem privaten Schlüssel, ohne dass wir das selber jetzt machen müssen, den rauskramen müssen und in die Hand nehmen müssen, wird diese Challenge, ich sag jetzt mal, signiert, gelöst. Und an dem Ergebnis, an dem richtigen Ergebnis dieser Aufgabe, kann der Dienstanbieter erkennen: Okay, das ist Stefan Becker und deswegen, da bin ich mir jetzt sicher, deswegen kannst du jetzt mailen, kannst du jetzt einkaufen, Geld überweisen, was auch immer. Das ist der Effekt, und das kann gerne auch noch jemand Böses irgendwo im Internet belauschen. Er kann nichts damit anfangen!

Michael Münz: Bei Matheaufgaben und der eine löst und der andere fragt, denke ich gleich: Dann gehe ich in der Zeit schon mal einen Kaffee machen, weil für mich Matheaufgaben lösen einfach auch eine bestimmte Zeitspanne bedeutet. Ich vermute bei Passkeys ist es aber nicht so.

Stefan Becker: Das ist das Gute: Wir haben ja schnelle Computer heutzutage. Auch ein Mobiltelefon macht das in Sekundenbruchteilen. Das geht schneller als ein Passwort eintippen, ganz bestimmt!

Ute Lange: Okay, das klingt schon mal ganz gut. Für mich ist noch die Frage, du hattest es gerade schon so angedeutet, Stefan: Gesetzt den Fall, ich mache das jetzt zu Hause vor meinem Computer, und ich finde das mit den Schlüsseln ganz hilfreich. Aber wenn dieser Schlüssel jetzt nur auf meinem Computer zu Hause ist und ich beim nächsten Mal ein anderes Gerät nutze, also bei meiner Schwester zu Besuch bin, und wir wollen uns was angucken und da rein, oder ich habe mein Mobiltelefon dabei. Wo ist denn jetzt da Komfort? Oder kriege ich das alles auf allen Geräten? Weil beim Passwortmanager, der ist synchronisiert, den habe ich mir eingerichtet. Das finde ich superpraktisch. Also selbst die Szene, die Michael letztens hatte, vor einem Leih-Bike zu stehen und das Passwort nicht zu wissen, ist mit einem Passwortmanager überhaupt nicht mehr gegeben. Das heißt, ich gucke, und dann sehe ich, dass das Bike jetzt zu haben ist oder welche Situationen im Alltag eben auch ein Passwort erfordern. Wie ist das denn mit diesen Schlüsseln, auch wenn sie keine analogen Schlüssel sind? Aber das Bild gefällt mir, das kann ich jetzt für mich mir auch vorstellen.

Stefan Becker: Ja, ihr seid natürlich schon eurer Cybersicherheitszeit voraus. Wenn ihr einen Passwortmanager verwendet, der damit umgehen kann, dann merkt man, glaube ich, gar nichts davon. Aber die Menschen, die Passkeys sich ausgedacht haben und implementiert haben, haben auch an den Fall gedacht, dass jemand keinen Passwortmanager hat. Und die Funktion dazu, die du gerade beschrieben hast, damit das trotzdem geht und auch einfach geht. Die sind da alle mit dabei. Es gibt immer die Möglichkeit, diesen Schlüssel über meine ganzen Endgeräte, die ich habe, also Computer,

Desktop-Computer, Laptop, Mobiltelefon, Tablet, überall entsprechend zu synchronisieren. Das heißt, die sind da überall, ohne, dass ich das groß merke. Oder ich kann das auch so machen, das hängt ein bisschen mit dem Dienstanbieter zusammen, dass ich das zum Beispiel alles mit meinem Mobiltelefon auslösen kann. Das heißt, man kann es sogar so machen: Ich sitze am Computer und will jetzt online einkaufen, und auf meinem Handy ploppt dieser Schlüssel auf, und ich bestätige das nur noch, zum Beispiel mit Gesichtsscan, Fingerabdruck oder auch mit dem Freischaltcode des Handys, so wie wir das Handy auch entsperren. Also so kann sich das darstellen. Es geht in jedem Fall. Das Verfahren Passkeys hat genau an diese ganzen Dinge gedacht, damit die Schlüssel, ohne dass ich da jetzt hinterherlaufen muss und mich um die kümmern muss, dass die dort überall von der Funktion her zur Verfügung stehen. Mit einem Passwortmanager ist das ganz besonders einfach.

Ute Lange: Na ja, ich meine, wir machen ja schon eine Weile diesen Podcast und lernen auch was dabei. Von daher sind wir da auch vielleicht einen Schritt voraus. Aber wir haben ja sehr viele Hörer und Hörerinnen, die schon länger bei uns dabei sind, die wahrscheinlich genauso versiert sind wie wir mittlerweile. Deswegen machen wir das hier zusammen. Das heißt, das haben wir jetzt verstanden. Das wird ja aber auch als ein sicheres Verfahren angeboten im Moment, also viel sicherer als das, was wir bisher kennen mit E-Mail-Adresse, Passwort und so. Worin liegt denn der Vorteil, oder was macht das so viel sicherer? Du hast eben schon mal gesagt, wenn da einer im Internet lauschen würde, dann könnte er vielleicht was hören oder mitkriegen, aber er könnte damit nichts anfangen. Wir hatten schon mal den Fall in einer Folge, dass jemand über uns recherchiert hat und zum Beispiel gesehen hat, dass Michaels E-Mail-Adresse irgendwie in einem Leak aufgetaucht ist. Das konnte er bestätigen und musste damals ein paar Sachen selbst machen. Vor sowas haben wir ja alle ein bisschen Angst, weil das auch zunimmt. Wie ist das mit Passkeys? Sind wir dann davor geschützt?

Stefan Becker: Ja, das ist das Gute daran. Wir haben, wie gesagt, ein ganz anderes Sicherheitsniveau. Ihr habt völlig Recht, es gibt einen Passwort-Checker der Uni Bonn, da liegen etwas über 30 Milliarden Benutzeraccounts und Passwortkombinationen vor. Bei irgendwo 8 Milliarden Menschen auf der Welt sehen wir schon: Das ist eine irre Menge. Da sind die Passwort-Leaks, die bekannt geworden sind im Internet. Und die haben die gesammelt. Da kann man das überprüfen. Das zeigt nur, das ist ein Riesenproblem. Das will ich damit sagen. Und wenn wir jetzt dieses Verfahren Passkeys nutzen, dann sind wir eben weg davon. Es wird kein Benutzername, kein Passwort mehr übermittelt, sondern diese beiden Schlüssel, von denen ich gerade gesprochen habe, die interagieren jetzt. Das Gute daran ist. Wenn jemand professionell kriminell versucht, zum Beispiel Benutzeraccounts zu bekommen durch Phishing, indem er vielleicht irgendwo einbricht bei einem Dienstanbieter, Mail-Anbieter, was auch immer, und die dort alle klaut und die dann auch da knackt, dann hat er die halt. Aber mit diesen Schlüsseln kann er nichts anfangen. Das heißt, in dem öffentlichen Schlüssel von dem Diensteanbieter, da ist auch die Identität des Diensteanbieters mit drin. Das heißt, wenn den jemand anders nimmt, dann funktioniert das nicht. Wenn jemand anders meinen Schlüssel nimmt, dann wird es eben auch schwierig. Er müsste wissen, von welchem Dienstanbieter das kommt. Denn das sieht man denen auch nicht an. Das heißt aus krimineller Sicht, egal welchen Aufwand der treibt, das skaliert nicht. Jetzt wissen wir ja, es ist in der Cybersicherheit immer so ein Igel-Hase-Rennen. Also, die Kriminellen denken sich was aus, und die Leute, die Cybersicherheit machen, versuchen wieder, etwas dagegen zu finden. Das ist so ein bisschen wie ein Wettrennen. Bei diesem

Wettrennen hier mit Passkesys, da gehen wir jetzt echt mal einen Schritt weiter. Wenn man das richtig implementiert hat, dann gibt es keine Idee, wie man das wirklich massenweise irgendwie hinbekommen könnte als Krimineller, um das zu unterlaufen. Da sind wir, ich bin ein bisschen vorsichtig, ich weiß ja nicht, welche Innovationskraft auf der anderen Seite noch ist, aber aktuell geht das einfach nicht. Und ich bin auch recht zuversichtlich, dass das noch eine ganze Weile so bleiben wird. Also massenhaft geht es nicht. Ich könnte mir jetzt natürlich vorstellen, wenn Kriminelle mit ganz viel Energie und ganz viel Aufwand und im Einzelfall und durch Menschen versuchen, jetzt mit ganz viel Social Engineering dort etwas zu machen, dass es dem ein oder anderen vielleicht mal gelingen würde. Aber das werden immer totale Einzelfälle bleiben, und sie sind auf Täterseite irrsinnig aufwendig zu machen. Das ist der Vorteil.

Michael Münz: Und wenn ich jetzt mein Handy liegen lasse? Also angenommen auf meinem Handy lägen meine Schlüssel und jemand kriegt mein Handy in die Hand. Wie sieht es denn dann damit aus? Dann hat er doch alle.

Stefan Becker: Ja, aber der müsste ja auch erst mal dein Handy, das Zugangshindernis, was du dort hast, dein Code, dein Gesicht, dein Fingerabdruck, das muss er ja auch erstmal alles überwinden. Also, da ist ja schon auch der Schutz. Das ist auch die Idee, dass man diesen zweiten Faktor eben hat auf dem Mobiltelefon. Und du weißt ja wahrscheinlich, dass, wenn du festgestellt hast, dass du dein Mobiltelefon verloren hast, du kannst es ja auch fernlöschen und all diese Dinge. Da kommen jetzt die klassischen Sicherheitsmaßnahmen an diesen Stellen hervor. Aber derjenige, der das ausnutzen will, müsste dein Handy schon im entsperrten Zustand stehlen, sonst kommt er da auch wieder nicht weiter. Denn diese Passkeys werden insbesondere auf den mobilen Endgeräten in einem ganz geschützten Speicherbereich abgelegt, verschlüsselt abgelegt. Und jemand, der dein Handy im gesperrten Zustand in die Finger bekommt, kommt da erst mal nicht dran.

Michael Münz: Ich kriege ja mindestens einmal am Tag einen Gruß vom Prinzen aus Nigeria.

Ute Lange: Immer noch? Der ist aber hartnäckig.

Michael Münz: Ja, wahrscheinlich wird einmal täglich die Datenbank der Uni Bonn abgefragt mit den Passwörtern und den Mailadressen, und ich kriege auf jeden Fall täglich Post von diesem Prinzen, der gerne hätte, dass ich auf eine Webseite gehe und da noch mal meine Kontaktdaten bestätige. So will der das ja von mir. Und dann gehe ich auf eine Seite, die so aussieht wie ein E-Mail- Dienst oder ein Online- Shop oder ich weiß nicht was, und soll dann da was eingeben. Helfen, auch Passkeys da, dass solche Fallen nicht mehr funktionieren.

Stefan Becker: Ja, diese Seite, wo du deine E-Mail-Adresse und dein Passwort eingibst, die gibt es ja nicht mehr. Das heißt, wenn das der Dienstleister ist, den du schon auf Passkeys umgestellt hast, dann gibt es diese Seite nicht mehr. Und wenn dir dann einer sagt, gibt das hier mal ein, dann würdest du wahrscheinlich merken: Moment, ich habe ja schon Passkeys. Das ist das eine. Das andere ist, das sind jetzt so ein bisschen die Details. Aber der Anbieter, wenn der Passkeys wirklich richtig implementiert, würde er auch die Möglichkeit, sich noch mit Benutzernamen und Passwort anzumelden, eliminieren. Das heißt, das geht gar nicht mehr. Also, wenn dann noch jemand kommen würde, und würde dich dann selbst unter diesen Umständen immer noch erfolgreich dazu bringen, wer weiß, was er für tolle Ideen hat, dass du da etwas eingibst, dann ist das funktionslos. Dann kann er damit ja auch

nichts anfangen, denn selbst, wenn er sie gewinnen sollte, also wenn er dich überwindet, dann geht's beim Anbieter wieder nicht weiter, weil der hat das ja schon abgeschaltet. Also, da ist die Tür richtig zu.

Ute Lange: Das ist ja ein häufiger Fall, den du gerade beschrieben hast, Michael, diese sogenannten Phishing E-Mails und die gefälschten Webseiten, auf die man dann kommt. Ich habe jetzt vor kurzem etwas bekommen, über das wir auch schon öfter gesprochen haben, aber ich war noch nie Empfängerin. Ich habe so eine SMS gekriegt, wo jemand schrieb: Hallo Papa, ich habe mein Telefon verloren, das ist meine neue Nummer. Kannst du mal so ein Messenger Dienst benutzen? Erstens kann ich kein Papa sein, rein biologisch. Ich bin eine Frau, und zweitens habe ich keine Kinder. Also das war irgendwie so doppelt doof von denen, beziehungsweise es war einfach wahrscheinlich so zufällig verschickt, also irgendwo Handynummer rausbekommen und einfach mal testen, hallo, ist da jemand am anderen Ende? Was ist denn mit diesen Tricks jetzt, wenn ich Pass benutzt habe, für was immer, welchen Anbieter? Bin ich davor dann auch geschützt? Das ist ja eine Falle, in die doch noch viele tappen. Die ist zwar ziemlich perfide, es werden ja auch so Nachrichten gefaked, Leute seien im Krankenhaus und man müsste irgendwie 20.000 Euro bezahlen. Also alles über dieses Smishing, also SMS-Phishing. Ist das dann auch, ich sag mal, Teil der Geschichte mit Passkeys?

Stefan Becker: Dazu müsste man sich jetzt ganz genau angucken, was kommt danach, wenn du auf diese SMS antwortest? Aber: Passkeys beschränkt sich natürlich in der Funktion auf die Identifizierung, Authentifizierung beim Beginn einer digitalen Handlung. Also, ich will Mails machen, ich will einkaufen gehen, ich will vielleicht auch Geld überweisen. Das ist die Stelle, wo Passkeys wirkt. Wenn jetzt jemand mit klassischem Social Engineering unter Umgehung all dieser – ich sag jetzt mal, Zugangskontrollen – sich eine Möglichkeit ausdenkt, dich zu einer Geldüberweisung zu bringen oder etwas ähnlichem, dagegen, hilft es dann nicht.

Ute Lange: Das haben wir schon oft beschrieben, dass man sich da auch noch mal ein paar analoge Sicherheitsschritte angewöhnen sollte, dass man nicht alles glaubt, was einem da so entgegengeworfen oder gesimst wird. Michael, du hattest aber gerade noch eine Regung, du wolltest noch eine Frage stellen.

Michael Münz: Das stimmt, und die leite ich mal so ein. Es gibt in diesem Podcast, in jeder Folge, den Moment, wo jemand sagt: Wenn es zu schön ist, um wahr zu sein, dann ist es meist auch gar nicht wahr so. Und jetzt höre ich dich über Passkeys reden und denke die ganze Zeit, das klingt eigentlich alles ganz schön. Aber ist es auch zu schön, um wahr zu sein? Oder andersrum gefragt: Du hast uns beide echt begeistert für das Thema. Hast du uns denn was verschwiegen?

Ute Lange: Gibt es etwas, was dich stört, beziehungsweise noch eine Hürde, die in Zukunft vielleicht doch noch genommen werden muss?

Stefan Becker: Ja, also, natürlich muss jetzt mein Anbieter das Verfahren auch anbieten. Ja, also, die Großen tun das alle, aber es wird sich vielleicht auch noch jemand finden lassen, der es noch nicht anbietet. Das ist natürlich schade. Aber da gebe ich vielleicht auch gerne den Tipp, sich vielleicht an den Anbieter anzuwenden und zu sagen: Hey, es gibt doch pass, ich möchte das gerne machen. Vielleicht hilft das ja auch. Und so ein kleines bisschen haben wir nicht gesehen, dass es sich - wie soll ich sagen - wie gehen wir denn mit diesen

privaten Schlüsseln um? Das haben wir bisher so ein bisschen zurückgestellt. Ihr habt es ganz kurz angedeutet. Die große Frage ist ja: Was ist jetzt, wenn ich das Ding verliere? Also, Michael, du hast schon so ein bisschen das Szenario Handy-Klau gesagt. Was ist, wenn ich meine Passkeys jetzt auf diesem Endgerät habe, und fällt mir jetzt ins Meer oder ist weg? Der Hund beißt drauf, ich weiß es nicht. Also im echten Leben haben wir ja alle wahrscheinlich für das, was uns wichtig ist und für das wir einen richtigen normalen analogen Schlüssel wie unseren Hausschlüssel haben, haben wir ja meistens noch einen zweiten Schlüssel. So ist es auch in dieser Welt. Also gibt eigentlich idealerweise natürlich einen zweiten Schlüssel. Und das ist die große Frage, wo ist denn der? Ja, und da kann ich jetzt gestalten, und das ist das, was wir so ein bisschen elegant ausgeblendet haben, bisher. Und das ist so: Wenn ich jetzt bei einem der Großen bin, einem Betriebssystemanbieter oder Mobiltelefonanbieter, die sorgen dafür, wenn ich das will, dass sie verschlüsselt sozusagen meinen Zweitschlüssel, meinen Sicherheitsschlüssel ablegen. Und wenn mir mein Handy gestohlen wird oder es geht kaputt, und ich richte mir ein neues ein, dann kommt auch der Schlüssel wieder dazu. Ja, also, da ist eine Möglichkeit. Ich kann aber auch mir zum Beispiel diese Schlüssel auf eine spezielle Hardware – da gibt es USB-Token, die extra dafür gemacht sind. Die sehen aus wie ein USB-Stick, sind aber kein USB-Stick. Die sind sozusagen so ein Schlüsseltresor, sag ich mal. Da könnte man die auch aufbewahren. Man kann so etwas auch nutzen, wenn man ganz viel Sicherheit haben will, dass diese Schlüssel grundsätzlich nur auf diesen Token sind. Dann muss man den aber immer dabeihaben. Ich will uns sagen, mit der Verwahrung dieses Zweitschlüssels, meines des Back-up-Schlüssels - da gibt es noch eine Reihe von Möglichkeiten und Unterschieden. Das macht das auch alles ein bisschen komplexer. Aber das ist so der Bereich, da sollte man sich ein bisschen Gedanken machen: Wie mache ich das denn, damit mir im Falle eines Falles, wenn es mal ganz schlimm kommt, dass ich nicht da abgeschnitten bin von allem? Da gehört noch ein bisschen Gehirnschmalz, Aufwand oder ein bisschen Kümmern dazu. Das ist aber nicht schwer und wird einem auch von den vielen großen Dienstanbietern gerne abgenommen.

Ute Lange: Ja, aber das ist jetzt nicht so schwer für unsere Hörer und Hörerinnen, weil wir ja auch bei allen anderen digitalen Daten immer empfehlen, dass es noch eine Offline-Back-up-Version geben soll, die nicht mit dem Internet verbunden ist. Also, das ist auch so ein bisschen eine Platte hier mit einem Sprung, die wir immer mal wieder auflegen. Von daher gehen wir mal davon aus, dass die Leute, die hier regelmäßig zuhören, das sowieso schon beherzigen, und jetzt auch bei Passkeys sollte das nicht die größte Hürde sein, sondern das machen wir ja schon automatisch. Also gehe ich jetzt mal davon aus. Michael guckt jetzt ein bisschen an die Decke, aber er hat ja jetzt mittlerweile auch ein Passwortmanager. Das heißt, das ist so eine Übung, die finde ich jetzt nicht so schwierig. Und ich muss gestehen, das Gespräch mit dir hat mich jetzt für das Thema ein bisschen mehr interessiert. Als wir entschieden haben, diese Folge zu machen, habe ich gedacht: Oh Gott, das wird so technisch. Ich weiß gar nicht, ob das so leicht vermittelbar ist, aber mit den Schlüsseln und dass da keiner mehr drankommt, dass ich ein bisschen abgesichert bin, das klingt für mich jetzt recht überzeugend und vor allen Dingen eben auch komfortabel. Wir haben ja alle immer so ein bisschen Angst davor, dass das mit dem Digitalen so kompliziert wird, wenn wir so viele verschiedene Dinge machen müssen. Ich werde mir wahrscheinlich bei meinen Anbietern das nächste Mal, wenn die mich fragen, möchten, sie sich mit Passkey anmelden, tatsächlich das machen.

Michael Münz: Auf jeden Fall.

Ute Lange: Du hast es ja schon probiert.

Michael Münz: Ich war ja schon vorher überzeugt, bevor wir diese Aufnahme gestartet haben, und bleibe auf jeden Fall dabei. ihr alle, die ihr uns jetzt gehört habt, ihr wollt ja natürlich auch jetzt nichts anderes machen, als eure Anmeldeverfahren umzustellen auf Passkeys, also hoffen wir jedenfalls. Stefan: Wo finden unsere Hörerinnen und Hörer denn jetzt den Passkey-Knopf?

Stefan Becker: Ja, wo findet man den? Der ist überall woanders, aber da, wo ich meinen Account verwalte, also wo ich noch, wenn ich sie noch hätte, dann meine E-Mail- Adresse ändere, da findet man auch die Möglichkeit, Passkeys einzurichten. Ich denke mal, bei den meisten, es wird noch ein paar geben ohne, dann kann man die vielleicht auch dazu bringen, indem man sie anschreibt: Hey, ich möchte jetzt gerne Passkeys machen, implementiert das doch mal! Da ist die Stelle. Aber wie Ute auch schon sagt, bei ganz vielen wird es jetzt immer wieder, wenn man sich anmeldet, mal angeboten: Willst du jetzt Passkeys machen, und dann kann man da jetzt zuschlagen. Traut euch, macht es einfach! Es tut nicht weh, es ist nicht schwierig, und danach ist man sicher. Und es ist superkomfortabel.

Ute Lange: Da muss ich jetzt gerade eine Werbung von früher denken, die vielleicht einige noch kennen. Das Kind aus dem Zahnarztstuhl: Mami, Mami er hat gar nicht gebohrt, weil regelmäßig Zahncreme genutzt wurde. So ähnlich ist es offensichtlich auch mit Passkeys. Das finde ich schön, kann ich mir leicht merken. Vielen Dank, Stefan, dass du da warst und dir Zeit für uns und unsere Hörer und Hörerinnen heute genommen hast.

Stefan Becker: Sehr gerne, hat mir Spaß gemacht!

Ute Lange: Ja, uns auch.

Michael Münz: Bleibt nur noch die Frage an euch, die ihr uns jetzt zugehört habt. Konnte Stefan euch auch überzeugen? Also wer vorher dann doch erst noch mal ein bisschen mehr wissen möchte, findet das in den Shownotes. Aber ihr könnt den Shownotes-Schritt auch gerne überspringen und es gleich ausprobieren. Also wir raten da auf jeden Fall zu, das so zu machen. Und wenn ihr es dann ausprobiert habt oder es bereits nutzt und ihr eure Erfahrungen mit uns teilen wollt, dann schreibt uns doch gerne über die BSI- Kanäle, die ihr schon kennt: bei Facebook, Instagram, X, also dem, was früher immer Twitter war, Mastodon sowie YouTube oder ihr schickt uns eine Mail an die Adresse.

Ute Lange: Podcast@bsi.bund.de. Wir freuen uns immer auf Post von euch! Und wenn ihr keine Folge mit und von uns verpassen wollt oder nochmal reinhören möchtet in welche, die schon eine Weile zurückliegen, die Themen bleiben ja leider doch immer wieder sehr aktuell. Dann folgt und liked „Update verfügbar“ auf euren Podcast Plattformen, und wir hören uns dann in Person wieder in vier Wochen. Über was sprechen wir dann Michael?

Michael Münz: Wir sprechen dann über das, was euch bewegt. Wir wollen euch jetzt hier noch mal ausdrücklich dazu einladen, uns eure Themenwünsche zuzuschicken, damit wir die aufgreifen können in der nächsten Folge oder in einer der nächsten Folgen. Wir haben immer ein offenes Ohr für euch, das wisst ihr hoffentlich mittlerweile nach 40 Ausgaben. Also schreibt uns gerne, worüber wir uns Gedanken machen sollen, und dann dröseln wir das Thema dann beim nächsten Mal für euch auf.

Ute Lange: Bis dahin: Passt gut auf euch und eure Daten auf und macht es gut! Bis dann Tschüss.

Michael Münz: Tschüss!