„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 49, 04.12.2024

Moderation: Ute Lange, Michael Münz
Gast: Stefanie Lösing, Kriminalhauptkommissarin beim Landeskriminalamt Nordrhein-Westfalen

---

Ute Lange: Hallo, ihr da draußen. Schön, dass ihr wieder einschaltet. Wir hoffen, euch und euren Daten ist seit unserer letzten Folge nichts passiert. Hier und heute erhaltet ihr auf jeden Fall weitere wertvolle Tipps, wie ihr euren digitalen Alltag absichern könnt.

Michael Münz: In eurem analogen Alltag schließt ihr ja sicher die Haustür ab, wenn ihr ausgeht, oder ihr macht euer Fahrrad fest, wenn ihr es parkt, oder verriegelt das Auto, wenn ihr aussteigt. Aber was tut ihr eigentlich, um eure Online-Identität sicher zu machen, dass die euch nicht geklaut wird?

Ute Lange: Digitaler Identitätsdiebstahl ist leider gar nicht selten. Statistiken sagen, dass mehr als jeder zehnte Erwachsene in Deutschland bereits Opfer von diesem Diebstahl im Netz geworden ist. Die Folgen können schwerwiegend sein, von finanziellen Schäden über Rufschädigung bis zu strafrechtlichen Konsequenzen.

Michael Münz: Wir lassen uns heute erklären, warum Kriminelle so sehr an unseren Online-Identitäten interessiert sind, und natürlich auch, was wir tun können, damit sie uns trotzdem nicht entwendet wird.

Ute Lange: Dazu haben wir heute eine Gesprächspartnerin für euch und uns, die sich ganz dem Thema Prävention von Cybercrime verschrieben hat. Mit ihren Tipps sind wir definitiv besser geschützt als vorher und gut im Internet unterwegs. Herzlich willkommen, Stefanie Lösing, Kriminalhauptkommissarin beim Landeskriminalamt Nordrhein-Westfalen in Düsseldorf.

Stefanie Lösing: Einen schönen guten Tag oder ein Hallo aus Düsseldorf. Ich freue mich, dass ihr mich eingeladen habt und dass ich heute nochmal mit ein paar hoffentlich wertvollen Tipps und Informationen unterstützen kann, dass wir alle besser geschützt sind im Internet.

Michael Münz: Da gehen wir ganz fest von aus, Stefanie. Schön, dass du da bist. Bevor wir in das Thema einsteigen, erzähle uns doch bitte erst, was genau deine Aufgabe beim Landeskriminalamt ist.

Stefanie Lösing: Meine Aufgabe beim Landeskriminalamt ist die Prävention von Cybercrime im weiteren Sinne. Das bedeutet, alle Straftaten, die auf analoge Weise auch mit dem sogenannten Tatmittel Internet begangen werden, fallen auf der Präventionsebene in mein Ressort.

Michael Münz: Warst du schon immer online und im Internet unterwegs oder wie wird man das, was du jetzt bist?

Stefanie Lösing: Ich habe mich irgendwann für die Stelle beworben. Ich bin tatsächlich schon seit über 30 Jahren bei der Polizei, wie ich kürzlich mit Erstaunen festgestellt habe.

Michael Münz: Das war der Moment, als der Blumenstrauß kam?

Stefanie Lösing: Genau, so ungefähr war das. Ich habe viele Jahre in vielen Bereichen bei der Kriminalpolizei gearbeitet, zum Beispiel auch im Bereich von Schwerstkriminalität. Ich habe dann aber irgendwann auch das Bedürfnis gehabt, vielleicht einmal zu versuchen, vor die Tat zu kommen und nicht immer nur hinterherzulaufen oder zu versuchen, die Täter zu ermitteln. Dann habe ich auf Behördenebene vier Jahre im Bereich Kriminalprävention, Prävention von Cybercrime, gearbeitet. Jetzt arbeite ich seit zwei Jahren auf übergeordneter Ebene im Landeskriminalamt Nordrhein-Westfalen im Bereich von Prävention von Cybercrime.

Ute Lange: Fangen wir doch einmal vorne an. Wir haben uns heute vorgenommen, über Identitätsdiebstahl zu sprechen. Was versteht ihr darunter?

Stefanie Lösing: Wenn man Identitätsdiebstahl als Begrifflichkeit im Internet in eine Suchmaschine eingibt, wird vielfach bei Identitätsdiebstahl das Entwenden mit dem gleichzeitigen Missbrauch der Daten in einen Topf geworfen. Schlussendlich ist der Identitätsdiebstahl erst einmal die Wegnahme und das Aneignen von Daten, die zu einer digitalen Identität gehören. Der Missbrauch dagegen muss nicht immer sofort stattfinden, weswegen ich das trenne. Ich sage, wir haben hier den Diebstahl und der Missbrauch der Daten kann dann auch erst viel später erfolgen. So wird der Diebstahl manchmal vielleicht auch erst viel später bemerkt.

Michael Münz: Wo fängt das denn an? Du hast es gerade schon gesagt, es geht um persönliche Daten. Das Erste, was ich mit Identität verbinde, ist der Name. Aber welche Daten darüber hinaus sind für Cyberkriminelle denn interessant?

Stefanie Lösing: Ich würde einmal sagen, dass durchaus alle Daten, die ein Krimineller bekommen kann, interessant sind. Aber wenn man sich erst einmal auf der digitalen Ebene, das anschaut, sind das sicherlich Kontodaten, mein Benutzername und vor allen Dingen die Zugangsdaten, also mein Schlüssel zur digitalen Wohnung. Aber es kann immer noch ganz viele weitere Daten geben, die Schnittmengen zum Analogen haben, also sowohl das Geburtsdatum, die Anschrift, vielleicht auch Kreditkartendaten, Kontodaten als auch im weitesten Sinne eben auch Zugangsdaten. Das kann auch ein Profilbild von mir sein. Also alle Daten, die mit mir als Person zusammenhängen oder in Verbindung zu bringen sind, sei es jetzt verstärkt im analogen oder im digitalen Bereich, sind interessant für Täterinnen oder Täter.

Ute Lange: Du hast eben schon den Unterschied gemacht zwischen der Aneignung der Daten, da gibt es sicherlich auch viele unterschiedliche Wege, und dem nächsten Schritt, damit irgendetwas zu machen, was nicht gesetzeskonform und für den Eigentümer der Daten auch unangenehm ist. Wie gehen Täter denn vor? Was sind verschiedene Wege, diesen Zweisprung auf Seiten der Kriminellen dann auch lukrativ zu machen?

Stefanie Lösing: Erst einmal zum Erlangen der Daten, da gibt es natürlich ganz viele, verschiedene Formen. Ich beschränke mich jetzt zunächst einmal auf die, die aktuell immer sehr, sehr stark im Fokus ist, und das zu Recht. Übermorgen haben wir den Black Friday. Da wird sicherlich auch noch einmal eine Rolle spielen, was ich unter der Überschrift Online-Betrug zusammenfasse. Online-Betrug kann auf ganz viele verschiedene Arten und Weisen stattfinden. Eine der sicherlich gängigsten und häufigsten angewendeten Varianten ist das sogenannte Phishing, was sicherlich ein "alter Hut" ist. Aber Phishing, beziehungsweise die Täterinnen und Täter, passen sich ja auch immer den aktuellen Gegebenheiten an. Daher haben wir inzwischen ganz viele verschiedene Varianten und Unterformen, die einfach zu der aktuellen gesellschaftlichen Entwicklung gehören. Inzwischen spricht man auch von einer Unterform des Phishings, dem sogenannten Quishing, also mit Q. Was haben wir alle mittlerweile verstärkt in unserer Umgebung? QR-Codes. Wenn ich einen QR-Code abscanne, komme ich auf eine Internetseite. Da haben wir jetzt auch schon Vorgehensweisen von Täterinnen und Tätern gehabt, dass ein QR-Code dafür genutzt wurde.

Michael Münz: Phishing in all seinen technischen Ausprägungen, angefangen von einer E-Mail mit einem Link, oder Smishing, also eine SMS, wo irgendetwas drinsteht, oder eben Quishing, alle haben eigentlich dasselbe Ziel. Dieses Ziel ist, dass ich auf etwas klicke und auf eine Seite komme, wo ich dann meine Daten eingebe. Das ist eigentlich das, was man in diesem Phishing erst einmal möchte, richtig?

Stefanie Lösing: Ganz genau das ist es, ja. Deswegen ist tatsächlich in diesen Zeiten, wo das immer wieder verstärkt auftaucht, wirklich wichtig und der oberste Satz, erst einmal Ruhe zu bewahren, weil die Täter immer gerne auch mit Zeitdruck und mit dem Faktor Stress arbeiten. In der heutigen Zeit will man immer erreichbar sein und bekommt einen Schreck, wenn es heißt: "Ihre SIM-Karte läuft morgen ab", oder: "Ihr Konto wurde gesperrt." In dem Moment, vielleicht aufgrund von Zeitdruck oder auch von innerlichem Stress, reflektiert man gar nicht: "Kann das jetzt eigentlich richtig sein? Ist das wirklich von demjenigen, von dem es vermeintlich herrührt?" Man denkt: "Oh, ich muss sofort handeln." Und deswegen ist Ruhe zu bewahren, erst einmal durchatmen und das noch einmal genau zu prüfen wirklich einer der ersten wichtigen Hinweise, um sich davor zu schützen.

Michael Münz: Du hast gerade auch schon erwähnt, dass es nicht nur technische Anpassungen sind, sondern auch inhaltliche. Wir hatten das im Podcast auch immer wieder einmal, dass es saisonale Anlässe sein können. Jetzt, wie du schon gesagt hast, fängt die Einkaufszeit an. Auf einmal kommen tolle Angebote, wo man sich überlegt: "Ach, das könnte ich vielleicht haben." Oder es gab ja auch bezüglich Energie immer wieder Versuche, Leute dazu zu bewegen, dass man irgendwo draufklickt, weil man günstiges Gas, Strom oder was auch immer bekommt. Also auch da passen sich Kriminelle an. Da ist nicht immer jeder Phishingversuch gleich. Die sehen nicht nur technisch unterschiedlich aus, sondern können auch inhaltlich ganz verschiedene Formen annehmen.

Stefanie Lösing: Das ist richtig. Ich sage immer ganz gerne: "Alter Hut in neuem Gewand." Wenn man Phishing hört, denkt man: "Ach ja, kennst du." Aber genau deswegen, weil die sich immer anpassen, ist das auch ein Stück weit ein zeitloses Ding, gerade auch mit dem Smishing. Ich bekomme eine vermeintliche SMS in Zusammenhang mit einer Paketzustellung. Jetzt stehen wir kurz vor Weihnachten oder wir haben den Black Friday und

wir machen tatsächlich alle seit der Coronapandemie verstärkt Online-Shopping. Das heißt, wir bekommen auch Pakete. Wenn man da in einem falschen Moment einfach ungeprüft in so einer Smishing-SMS auf den Link klickt, weil man eben das Paket vielleicht dringend erwartet oder eben nicht so sensibel ist, dann hat man ganz schnell einmal irgendwo seine Daten eingegeben. Der Täter hat vielleicht Glück und er bekommt Geld und zusätzlich, als Zugewinn, noch Daten, die er dann verkaufen oder auch im Zweifelsfall später einmal für andere Dinge benutzen kann. Das ist ein sehr wichtiges Thema und ich finde es echt gut, dass wir heute noch einmal eine Sendung dazu machen. Ich glaube, Identitätsdiebstahl ist ein sehr aktuelles Thema, da wir alle immer mehr digital unterwegs sind.

Ute Lange: Nun bin ich vielleicht unachtsam gewesen und bin auf so etwas hereingefallen. Ich bin darauf getappt, habe den Link geklickt, merke das und dann passiert eine Weile gar nichts. Wie würde ich denn merken, dass meine Identität in so einem Prozess tatsächlich gestohlen wurde? Ich erinnere mich vielleicht gar nicht daran. Auf was kann ich achten oder was sind Warnzeichen, dass so ein einfacher Klick vielleicht doch noch mehr bewirkt haben könnte, als einfach nur unachtsam gewesen zu sein?

Stefanie Lösing: Ich denke, es ist wichtig, dass man regelmäßig seine Geldbewegungen auf dem Konto checkt, also dass man im Blick hat, ob es vielleicht merkwürdige Abbuchungen gibt. Hat da vielleicht auf einmal eine Fluggesellschaft Geld abgebucht, was gar nicht sein kann? Natürlich wären merkwürdige Nachrichten, merkwürdige SMS, merkwürdige E-Mails oder auch Anrufe so Dinge, auf die man dann achten und hellhörig werden sollte, wenn da irgendetwas nicht stimmt. Was man auf jeden Fall auch in Erwägung ziehen kann, sind die sogenannten Identity-Leak-Checker von unterschiedlichen Anbietern. Das kann man googeln. Da würde ich dann auf jeden Fall ein Angebot nehmen, das von einem offiziellen Anbieter ist. Da kann man E-Mail-Adressen überprüfen, ob die zum Beispiel einmal in einem sogenannten Datenleck aufgetaucht sind. Das wäre noch eine Sache, die man machen könnte.

Michael Münz: Damit sprichst du schon eine andere Variante an, wie Cyberkriminelle an meine Daten kommen könnten, also nicht, indem ich sie aktiv eingebe, weil ich auf irgendwas geklickt habe, was ich nicht hätte machen sollen, sondern weil sie die Daten auf anderen Wegen bekommen haben, zum Beispiel über einen Daten-Leak.

Stefanie Lösing: So ist es. Das ist auch noch eine Variante. Ich hatte jetzt gesagt, ich beschränke mich auf den Online-Betrug, aber natürlich gibt es unterschiedliche Varianten, wie meine digitale Identität oder Daten von mir abhandenkommen können. Dazu zählt selbstverständlich auch ein Datenleck irgendeines Anbieters. Aus dem Grund wäre es wichtig, dass man immer kritisch ist und sich überlegt, ob man seine Daten jetzt wirklich da eingibt. Natürlich freue ich mich immer, wenn irgendeine Internetseite auch ein gutes Angebot hat, aber man muss sich wirklich hinterfragen. Muss ich da jetzt wirklich meine ganzen Daten eingeben? Ist das so wichtig? Wie sicher sind meine Daten bei dem- oder derjenigen, wo ich die jetzt gerade hinterlege? Gut, ein Datenleck kann natürlich auch bei großen Plattformen auftauchen, aber da sollte man auch immer noch einmal ein bisschen vorsichtig sein. Der Begriff Datensparsamkeit, auch wenn es manchmal schwerfällt, der ist in diesen Zeiten sicherlich durchaus angebracht.

Ute Lange: Wir sagen hier gerne, wenn es zu schön ist, um wahr zu sein, dann ist es das meistens auch nicht. Wenn mir ein Preisausschreiben irgendetwas verspricht, ich dafür aber

jedes Datenset, das von mir vorhanden ist, auf einer Seite eingeben soll, dann ist vielleicht auch eher Vorsicht geboten.

Stefanie Lösing: Ja, das würde ich definitiv auch sagen.

Ute Lange: Wenn wir jetzt aber einmal auf die andere Seite schauen, was ist denn so attraktiv für Kriminelle am Identitätsdiebstahl? Ich habe jetzt eine Serie von E-Mails bekommen, dass angeblich meine Webseite, die ich habe, gesperrt wird, wenn ich nicht eine Zahlung veranlasse. Die Summen variierten zwischen 10 Euro und 2,30 Euro, mit denen sie am Ende zufrieden gewesen wären, wenn ich denn gezahlt hätte. Aber das sind keine großen Beträge. Also damit können Kriminelle doch auch keinen großen Umsatz machen. Was ist daran so attraktiv?

Stefanie Lösing: Ich würde sagen, das Motiv ist erst einmal, grundsätzlich den Fuß in die Tür zu bekommen, weil es am Anfang auch realistisch klingen soll. Das haben wir bei anderen Modi Operandi auch, dass, um eben den Auftakt zu geben oder, wie gesagt, den Fuß in die Tür zu bekommen, zuerst mit kleinen Beträgen gearbeitet wird, um erst einmal anzufüttern. Danach läuft das dann weiter. Warum sind die Daten attraktiv? Ich mache immer gerne Vergleiche zur analogen Welt. Es gibt viele Leute, die sagen: "Was habe ich schon? Was können die bei mir schon holen? Ich habe doch nichts zu verbergen." Das sind klassische Sätze. Aber denken Sie einfach einmal an den Kennzeichendiebstahl. Kriminelle stehlen Autokennzeichen, weil sie dann dieses Kennzeichen an ihr Fahrzeug machen und damit im schlimmsten Fall eine Geldautomatensprengung irgendwo durchführen. Erst einmal sind es dann Ihre Daten, die da im Fokus stehen. Wenn ich das jetzt auf das Internet münze, klingelt es im schlimmsten Fall bei Ihnen morgens und die Kollegen stehen da mit einem Durchsuchungsbeschluss, weil leider Gottes der Tatverdacht aufgrund der Daten, mit denen die Straftat begangen wurde, erst einmal auf Sie zurückfällt. Das wäre wirklich eines der Worst-Case-Szenarien, die passieren. Es ist sehr vielfältig, was sie mit den Daten machen können. Die werden sicherlich auch im Internet gehandelt und man kann, je nach Daten, natürlich auch unmittelbar auf Konten zugreifen.

Michael Münz: Ich glaube, wir sollten es an dieser Stelle vielleicht noch einmal klarmachen. Es gibt eigentlich keine Daten, die zu trivial sind, als dass man sie nicht doch für irgendetwas gebrauchen könnte, also auch Namen von Katzen, Geburtsdaten, Vorlieben, die man in sozialen Netzwerken einmal angegeben hat für Bücher, Musik und vieles andere. Es ist völlig egal. Alles, was an Daten vorhanden ist, kann auch gegen mich verwendet werden.

Stefanie Lösing: Das ist definitiv so. Gerade in diesen Zeiten auch im Zusammenhang mit möglichen Deep-Fake-Methoden, also dass ich Inhalte fälsche. Alles, was ich über jemanden weiß, kann ich auch benutzen. Man sollte sich gut überlegen, also „think before you click“, bevor man irgendetwas hochlädt. Früher haben wir immer im Zusammenhang mit Schulen gesagt: "Mache doch einmal den Omatest, bevor du etwas hochlädt," gerade natürlich Bilder und Videos. Frage dich: "Könnte ich es meiner Oma zeigen?" Das ist jetzt ein bisschen trivial, aber man sollte sich wirklich immer hinterfragen.

Ute Lange: Wir haben ein Beispiel von jemandem zugeschickt bekommen, dem so ein Identitätsdiebstahl offenbar widerfahren ist. Wir hatten in der vergangenen Folge auch Hörerinnen und Hörer gefragt, ob ihnen etwas passiert ist, was sie uns zuschicken wollten. Daraufhin hat Janine aus Hamburg uns diesen Vorfall erzählt:

Janine: Ich hatte früher einen Mail-Account bei Yahoo. Ich glaube, es war in 2016, als es anfing, dass Leute aus meiner Kontaktliste ominöse Mails bekamen, die angeblich von mir verschickt worden waren. Darin sollten sie dann auf einen Link klicken und wer weiß, wo dieser Link hingeführt hat. Ich habe diese Mails nicht verschickt. Ich habe keinen Zugriff auf diese Mails, habe mehrmals mein Passwort geändert und inzwischen auch meinen Account gelöscht. Aber noch bis letztes Jahr haben mir Leute geschrieben, dass sie wieder eine dieser Mails bekommen haben, und ich kann nichts dagegen tun.

Michael Münz: Da wäre jetzt die Frage an dich, Stefanie, ist das ein Phänomen, das dir bei deiner Arbeit immer wieder einmal unterkommt?

Stefanie Lösing: Bei meiner aktuellen Arbeit ist das sicherlich nicht der Fall, weil ich nicht mehr an der Front arbeite. So drücke ich es einfach einmal aus. Ich bin nicht mehr mit Ermittlungsverfahren betraut, aber durchaus im Gespräch mit auswertenden Dienststellen. Natürlich höre ich regelmäßig, auch im Austausch mit anderen Kolleginnen und Kollegen, dass solche Fälle vorkommen oder jemand sich an die Polizei wendet, weil er festgestellt hat, dass etwas nicht stimmt. Mit seinem Namen oder unter seinem Account wurden irgendwelche Dinge gemacht, wie ich es eben beschrieben habe. Das kommt vor.

Ute Lange: Nun ist Janines Fazit ein bisschen resignativ. Sie sagt, sie kann nichts dagegen tun. Siehst du das auch so?

Stefanie Lösing: Nein, ich würde das jetzt nicht ganz so negativ darstellen wollen. Wo man natürlich am meisten machen kann, ist sicherlich auf der Präventivebene. Das heißt, ich kann ganz viele Dinge machen oder Dinge unternehmen, um erst einmal vorzubeugen, dass mir so etwas nicht passiert. Man muss auch als Polizei immer klar sagen, einen hundertprozentigen Schutz gibt es nicht. Also man kann nie sagen: "Ich bin jetzt vor allem hundert Prozent sicher." Aber, genau wie beim Einbruchdiebstahl auch, man kann es den Tätern so schwer wie möglich machen, vielleicht sogar so schwer, dass es gar nicht mehr attraktiv ist und wirklich nicht passiert. Dazu zählt sicherlich auf der Präventivebene, dass man starke Passwörter verwendet und mindestens eine Zwei-Faktor-Authentifizierung benutzt. Wenn sich jemand zum Beispiel in meinen Mail-Account einloggte, würde ich jetzt auf meinem Handy eine Benachrichtigung bekommen und sehen, dass ich das nicht gewesen bin und dass irgendetwas nicht stimmt. Dann kann ich auch sofort tätig werden und bestimmte Schutzmechanismen in Anspruch nehmen, auch die, die mir von dem Anbieter ermöglicht werden. Ich kann mich dafür interessieren und darum kümmern, anstatt mich darauf zu verlassen, dass es schon gutgehen wird. Das ist auf jeden Fall eine Variante. Habe ich eine E-Mail-Adresse oder vielleicht mehrere? Ich empfehle immer, auf jeden Fall mehrere zu haben und vielleicht sogar eine, die ich eben nicht für jedwede Kommunikation nutze. Wobei es dann gut wäre, die E-Mail-Adressen auch, regelmäßig in einem Identity-Leak-Checker zu überprüfen, gerade die, die vielleicht nicht so häufig benutzt werden. Wenn jetzt tatsächlich das Kind in den Brunnen gefallen ist, kann man eigentlich nur noch versuchen, den Schaden zu begrenzen, also diesen möglichst kleinzuhalten. Dazu gehört sicherlich, der verantwortlichen Internetseite oder dem Anbieter, in dem Fall des E-Mail-Accounts, sofort eine Benachrichtigung zu geben, eine Anzeige zu erstatten und auch das Umfeld zu warnen. Mit der E-Mail-Adresse kann man das Umfeld dann sicherlich nicht warnen, aber gerade dann ist es gut, wenn man noch eine zweite hat. Natürlich sollte man auf jeden Fall auch die Passwörter ändern, wenn man mitbekommt, dass so etwas passiert

ist. Das hat sie hier auch gemacht. Gut, das ist immer eine Einzelfallbetrachtung und sicherlich sind die Daten, die ich hier habe oder die ich jetzt gerade bei dem Einspieler gehört habe, nicht ausreichend. Es gilt vielleicht zu prüfen, was genau man da im Einzelfall hätte anders machen können oder sollen.

Ute Lange: Aber du bist völlig im Team, Vorbeugen ist besser als weinen?

Stefanie Lösing: Gut, weinen oder sich ärgern ist durchaus nachvollziehbar. Aber es gilt dann sicherlich, den Schaden zu begrenzen und vorbeugen ist definitiv in jedem Fall immer gut.

Michael Münz: Wir hatten vorhin auch schon darüber gesprochen, wie sich der Diebstahl von Online-Identitäten beziehungsweise die Instrumente, die genutzt werden, verändert hat. Denke jetzt einmal an den Dauerbrenner SMS, den wir auch immer wieder hier im Podcast besprechen, da Smishing auch nicht weggeht. Was ist denn jetzt an Techniken ganz neu dazugekommen, wo ihr denkt: "Oje, das könnte demnächst tatsächlich eine Welle werden"?

Stefanie Lösing: Ich hoffe nicht, dass es eine Welle wird. Da gibt es auch verschiedene Bereiche und ich könnte sicherlich mehrere benennen, gerade im Betrugssektor. Aber da sind wir auch wieder beim klassischen Phishing. Wenn wir jetzt auf der SIM-Kartenebene oder auf der SMS-Ebene bleiben, gibt es ein Phänomen, was hier vereinzelt auch schon aufgetreten ist. Das ist das sogenannte SIM-Swapping. Es ist mir wichtig, dass wir da noch einmal sensibilisieren und den Zuhörerinnen und Zuhörern sagen: "Schaut einmal, da könnt ihr vielleicht noch ein bisschen mehr darauf achten, um eben vorzubeugen", so wie wir es gerade gesagt haben. Beim sogenannten SIM-Swapping ist es so, dass die Täterinnen oder Täter quasi meine Mobilfunknummer, also meine Handynummer, übernehmen. Das ist dann natürlich ziemlich unangenehm, weil sie mit der Nummer viel machen und anrichten können.

Michael Münz: Durch das SIM-Swapping, auf Deutsch SIM-Tauschen, übernehmen Betrüger die Kontrolle über die Mobilfunknummer einer Person. Dafür bestellen sie zum Beispiel eine E-SIM, also eine digitale SIM-Karte, nachdem sie sich auf anderen Wegen Zugang zu den persönlichen Daten und zum Account verschafft haben. Dann sperren Sie den Besitzer von seiner eigenen Rufnummer aus. Da so das Mobilfunk- und Mail-Konto schlimmstenfalls erfolgreich übernommen werden können, ist den Betrügern Tür und Tor für weitere Missbräuche geöffnet.

Michael Münz: Würde das auch so eine Zwei-Faktor-Authentifizierung aushebeln? Ich frage nur, um das Ganze ein bisschen einzuordnen.

Stefanie Lösing: Ja, genauso ist es. Damit können sie viel machen, wenn alles schiefläuft. Ich stelle oft die Frage, wie viele Passwörter jemand benutzt. Wenn man ein Passwort für alles hat, dann sage ich immer: "Ja, das ist wie ein Generalschlüssel. Wenn der Täter das eine Passwort hat, dann kommt er überall rein." Jetzt habe ich eine Zwei-Faktor-Authentifizierung und der zweite Faktor, also der Schlüssel, den mir jetzt der Anbieter schickt, kommt als SMS auf meine Handynummer, die der Täter oder Täterin übernommen hat. Ebenso wissen diese, dass ich da und da auch noch ein Konto habe. Dann würde ich als Täter oder Täterin natürlich flugs versuchen, mich auch in die entsprechenden Konten einzuloggen. Da ich die Handynummer habe und der Schlüssel auf die SIM-Karte kommt, bekomme ich den zweiten Schlüssel auch und kann noch in weitere Konten eindringen.

Wenn die Nummer einmal übernommen ist, würde das den zweiten Faktor tatsächlich aushebeln.

Ute Lange: Das klingt jetzt unschön. Wenn mir das passiert, was kann ich denn dann noch machen? Unter Umständen komme ich nicht mehr an meine Anwendungen heran, weil jemand anders die Kontrolle über die Telefonnummer übernommen hat und damit eben auch Zugänge bekommt.

Stefanie Lösing: Genauso ist es. Wir haben eben schon über Auffälligkeiten gesprochen. Wenn man selbst zum Beispiel auf einmal kein Netz mehr hat oder man, was wir eben gesagt haben, merkwürdige Anrufe oder merkwürdige SMS bekommt, ist das eventuell ein Anzeichen dafür, dass jemand anders meine Handynummer übernommen hat. Dann ist es auf jeden Fall extrem wichtig, so schnell wie möglich den Vorfall beim betroffenen Dienst oder bei dem betroffenen Anbieter zu melden, also dem Telefonanbieter. Da sind wir auch wieder im Bereich Prävention. Habe ich mich vorher vielleicht einmal bei meinem Telefonanbieter oder bei meinem SIM-Kartenanbieter damit auseinandergesetzt, welche Zugangsmöglichkeiten es da gibt? Habe ich dann noch andere Zugangsmöglichkeiten? Weiterhin sollte man auf jeden Fall auch Anzeige erstatten und die Zugangsdaten sowie natürlich auch weitere Zugangsdaten ändern.

Ute Lange: Ich danke schon einmal bis hierhin, Stefanie. Da war schon viel dabei. Ich würde das jetzt noch einmal ganz kurz auch für mich selbst zusammenfassen. Ich glaube, der Punkt, der bei mir hängengeblieben ist, und dazu würde ich gerne noch einmal ein Beispiel bringen und mit dir abgleichen, ist einfach die generelle Skepsis bei allem, was uns erreicht, also bei allen Nachrichten oder auch Freundschaftsanfragen. Ich wollte jetzt auf diesen Fall kurz noch zu sprechen kommen, dass ich auch bei Freundschaftsanfragen in sozialen Netzwerken nicht einmal mehr sicher sein kann, dass das die eigentliche Person ist. Die kann auch gedoppelt sein. Also ich schaue mir das Foto von der Ute und ihre Vorlieben, die sie angegeben hat, an. Ich sehe dann genauso aus und schreibe noch dazu: "Ich habe meinen alten Account aufgegeben. Bitte nimm meine Freundschaft jetzt mit diesem Account an." Auch in solchen Fällen sollte man auf jeden Fall skeptisch bleiben, weil es immer sein kann, dass jemand anderes dahintersteckt.

Stefanie Lösing: Ja, da bin ich ganz deiner Ansicht. Tatsächlich sollte man jetzt in diesen Zeiten und auch in denen, die wir noch vor uns haben, vorsichtig sein. Das ist ähnlich wie bei dem Überqueren einer Straße. Ich achte darauf, ob die Ampel rot oder grün ist. Heutzutage muss man bewusst immer kritisch sein. Ich hinterfrage, ich lasse mich nicht unter Druck setzen. Nachfragen schützt einfach. Nachfragen bei den von mir abgespeicherten Daten, dass ich, wenn ich etwas bekomme, auch von einem Anbieter, dann händisch selbst Kontakt mit ihm aufnehme und das tatsächlich nicht über mir zugespielte Inhalte mache. Man sollte immer kritisch sein und tatsächlich auch versuchen, ruhig zu bleiben.

Ute Lange: Dann würde ich jetzt einmal die Gegenfrage stellen. Michael hat sich jetzt meines Kontos bemächtigt. Da müssen wir darüber sprechen, das kommt gar nicht infrage. Ich stelle fest, dass da jemand so tut, als sei er ich und stellt Anfragen oder schreibt vielleicht auch Dinge, die gar nichts mit mir zu tun haben, die ich auch nicht für mich in der Welt haben will, weil ich nicht dazu stehe. Was kann ich dann tun, wenn mir so etwas passiert?

Stefanie Lösing: Definitiv Kontakt mit dem Anbieter aufnehmen, sagen, dass da etwas nicht stimmt und das Konto gesperrt werden muss. Es gibt heutzutage unterschiedliche Meldefunktionen bei den Anbietern. Dann sollte man nach Möglichkeit auf jeden Fall dieses Kennwort und auch vielleicht weitere Kennwörter ändern, die in Rede stehen könnten. Auf jeden Fall würde ich auch immer sagen, Anzeige erstatten ist definitiv ebenfalls wichtig, auch für weitere Dinge, die dann später passieren. Dann kann man auf jeden Fall sagen, dass man Anzeige erstattet hat.

Ute Lange: Es ist wie mit dem gestohlenen Auto. Wenn ich nach der Geldautomatensprengung sage, das Auto ist mir geklaut worden, ist das nicht so gut, wie es vorher schon gesagt zu haben.

Stefanie Lösing: Das würde ich auch so sehen. Es ist aber definitiv auch der Fall, dass Sie mit Ihrer Anzeige auch uns als Polizei unterstützen, weil jede Anzeige wieder unterschiedliche, andere Hinweise auf den Sachverhalt hat. Kriminalpolizeiliche Arbeit ist manchmal einfach auch wie ein Puzzle, wo mir vielleicht ein Puzzleteil fehlt. Das bekomme ich möglicherweise durch die vierte, fünfte oder sechste Anzeige, die ich zu einem Fall bekomme. Das sind also zwei verschiedene Sachen.

Ute Lange: Das heißt, es muss mir auch nicht peinlich sein, wenn mir so etwas passiert und ich dann bei euch erscheine, sondern, im Gegenteil, ihr könnt mit der Information auch noch etwas anfangen? Ich fände es schon peinlich, wenn mir das passierte, ganz ehrlich. Viele von uns, und davon bin ich auch nicht frei, denken: "Das kann mir gar nicht passieren. Ich mache schon alles, was der Podcast immer sagt." Die ganze Liste habe ich jetzt für unsere Hörer und Hörerinnen erklärt, dass ich das hoffentlich alles intus habe und schön sicher bin, aber wer weiß?

Stefanie Lösing: Ja, liebe Ute, ich danke dir, dass du dieses sehr wichtige Thema ansprichst. Das ist auch uns als Polizei und ebenso als Kriminalprävention ein wichtiges Thema. Das nennt man nämlich Victim-Blaming oder Täter-Opfer-Umkehr. Deswegen habe ich in meiner beruflichen Zeit auch vermieden zu sagen, darauf hereinfallen, weil ich finde, dass das schon ein bisschen impliziert, dass der andere unvorsichtig war. Ich persönlich würde sagen, Online-Betrug kann jedem passieren. Es kann in jedwede Lebenssituation einfach gerade völlig hineinpassen und dann drücke ich einmal auf den Knopf, auf den ich vielleicht in einem anderen Fall nicht gedrückt hätte. Täter-Opfer-Umkehr heißt dann, wer sind denn eigentlich die bösen Buben? Die bösen Buben sind doch die, die uns angegriffen haben, und nicht die, denen es passiert ist. Das sollten diejenigen, denen es passiert ist, sich wirklich vor Augen führen. Es kann jedem passieren und die Bösen sitzen auf der anderen Seite. Deswegen sollte einem das niemals peinlich sein. Danke schön dafür.

Ute Lange: Dann habe ich doch gleich noch eine Nachfrage. Wenn das jedem passieren kann. Stefanie, ist dir auch schon einmal etwas passiert?

Stefanie Lösing: Ja, tatsächlich hatte ich auch schon eine entsprechende Erfahrung. Ich führe das jetzt nicht näher aus, sondern sage nur als Beispiel zu dieser Situation, ich habe drei Dinge gleichzeitig gemacht und es passte. Es passte inhaltlich komplett, sodass ich nur gedacht habe: "Ich muss jetzt schnell handeln." Ich war komplett im Flow. Ich kenne auch noch andere Kollegen. Es war mir hinterher, wenn ich es jetzt wirklich einmal ganz trivial sagen kann, extrem peinlich, gerade weil ich vom Fach bin. Ich hatte aber schon vorher

diese Botschaft immer herausgebracht, nicht erst, seitdem mir das passiert ist. Aber es hilft manchmal. Ich habe hinterher gedacht: "Sehr gut, jetzt kannst du den Leuten noch besser erklären, warum es wirklich jedem passieren kann."

Ute Lange: Danke für das Teilen und die Offenheit. Das beruhigt mich jetzt ein bisschen. Wenn es mir passiert, rufe ich dich an und dann fühle ich mich nicht mehr so schlecht.

Stefanie Lösing: Das ist sehr gut. Es reicht schon, dass man sich aufgrund der ganzen Umstände schlecht fühlt. Da muss man sich nicht auch noch schlecht fühlen, weil man aus Versehen einmal falsch geklickt hat. Man muss auch wirklich sagen, dass die Täter so raffiniert vorgehen, dass es manchmal sehr frech und fies ist. Wenn man da nicht voll bei der Sache ist, kann es schiefgehen. Deswegen ist dieser Grundsatz, Ruhe zu bewahren, wichtig. Ob ich jetzt gerade einmal drei tiefe Atemzüge mache, vor die Tür gehe oder, für Raucherinnen und Raucher, eine Zigarette rauche, es braucht irgendeine Systematik, die mich wieder herunterholt. Wenn ich dann hinterher wieder draufschaue, sage ich: "Kann das eigentlich wirklich sein? Das ist schon merkwürdig." Ja, es wäre auf jeden Fall wichtig, sich im entsprechenden Moment daran zu erinnern.

Michael Münz: Das machen wir beide, Ute und ich, auf jeden Fall. Spätestens jetzt haben wir das verinnerlicht.

Stefanie Lösing: Das ist schön. Ich hoffe, die anderen, die zuhören, auch.

Michael Münz: Wir haben auf jeden Fall wieder einiges mitgenommen. Danke dir dafür, auch für das Teilen und für das Anerkennen, dass es jedem und jeder passieren kann. Ich denke, das ist eine wichtige Botschaft. Essenziell ist, dass man daraus lernt und sensibler beziehungsweise aufmerksamer ist. Wir haben eine Standardliste, was wir immer an Tipps herausgeben. Dein Ruhe-Bewahren wird jetzt auf diese Liste kommen. Was nimmst du mit, Michael?

Stefanie Lösing: Das freut mich.

Michael Münz: Ich nehme mit Skepsis, Ruhe bewahren und nicht unter Druck setzen lassen, vor allen Dingen auch noch einmal das Thema Passwort und Datensicherheit mit. Fünf Euro für einen Sneaker, also Newsletter abonnieren für fünf Euro und dann bekommt man die nächsten Schuhe günstiger, da sollte man sich wirklich überlegen, was passiert denn mit den Daten, die ich da eingebe? Ich glaube, da werde ich jetzt eher zurückhaltender sein, wenn ich künftig solche Angebote bekomme.

Ute Lange: Ich werde dich daran erinnern, wenn es das nächste Mal welche gibt.

Stefanie Lösing: Das fällt manchmal schwer.

Michael Münz: Stefanie sagt auch schon, es fällt manchmal schwer, sich da zurückzuhalten. Aber ich glaube, ich werde mit meinen Daten noch vorsichtiger sein.

Ute Lange: Ganz herzlichen Dank, Stefanie, dass du dir die Zeit genommen hast. Es hat viel Spaß gemacht und wir hoffen, dass ihr da draußen auch neue Erkenntnisse mitgenommen habt. Wenn ihr weitere wollt, dann folgt uns doch auf eurer Podcast-Plattform. Da gibt es viel

aus der Vergangenheit zu hören, aber auch neue Folgen in der Zukunft. Michael, was machen wir das nächste Mal?

Michael Münz: In der nächsten Folge greifen wir noch einmal das Thema Künstliche Intelligenz auf. Noch einmal, weil wir schon im Sommer 2023 eine Folge hatten, in der wir uns mit dem Thema befasst haben. Seitdem ist mit ständig neuen Entwicklungen ungeheuer viel passiert auf dem Gebiet. Da wollen wir noch einmal innehalten und schauen, wo wir bei dem Thema eigentlich gerade stehen. Außerdem habe ich gehört, dass es in der nächsten Ausgabe auch etwas zu feiern gibt. Lasst euch überraschen.

Ute Lange: Wie immer gilt, schickt uns eure Fragen zum Thema, damit wir sie dann auch beantworten können. Schreibt uns über die BSI-Kanäle auf Facebook, Instagram, Mastodon oder YouTube oder schickt uns eine E-Mail an die Adresse podcast@BSI.Rundfunk.de. Wir freuen uns immer, von euch zu hören.

Michael Münz: Wir freuen uns auch, von Stefanie vielleicht in der nahen Zukunft wieder einmal etwas zu hören. Vielen Dank, dass du da warst.

Stefanie Lösing: Ich danke auch. Es hat mir sehr viel Spaß gemacht. Danke schön.

Michael Münz: Euch und natürlich auch dir, Stefanie, wünschen wir eine schöne Adventszeit und sichere Einkäufe jetzt erst einmal. Bis bald. #00:37:00-5#

Stefanie Lösing: Tschüss.