„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 01, 29.09.2020:
Cyber-Sicherheit und Deep Fakes

Moderation: Ute Lange, Michael Münz
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Münz: Update verfügbar – Ein Podcast des BSI!

Lange: Hallo und herzlich Willkommen bei der ersten Ausgabe von „Update verfügbar“, dem BSI Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Ich bin Michael Münz, und wir melden uns ab jetzt monatlich aus dem BSI in Bonn.

Lange: Und ich finde, bevor wir anfangen, sollten wir mal alle Beteiligten vorstellen.

Münz: Gute Idee. Ich übernehme mal, Ute. Das BSI ist das Bundesamt für Sicherheit in der Informationstechnik und wurde 1991 gegründet, mit Sitz in Bonn. Seine Aufgaben sind in einem Gesetz festgelegt, und kurz gesagt, soll es den sicheren Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft ermöglichen und vorantreiben. Gerade jetzt – auch zuletzt wegen Corona und dem ganzen Digitalisierungsschub, den wir erlebt haben – ist das eine wichtige Aufgabe, wenn es darum geht, Digitalisierung auf allen Ebenen in Deutschland sicher zu gestalten.

Lange: Und die konkreten Aufgaben sind unter anderem, die Netze des Bundes zu schützen, also Angriffe auf unsere Regierungsrechner oder -systeme zu erkennen und auch abzuwehren. Die Wirtschaft, die du schon erwähnt hast, über das Thema IT und Internet-Sicherheit zu informieren und vor allen Dingen für den sicheren Umgang damit zu sensibilisieren. Und wir als Bürgerinnen und Bürger sind auch angesprochen: Das ist der digitale Verbraucherschutz. Das BSI versorgt uns regelmäßig mit Informationen und Tipps über Sicherheit im digitalen Alltag.

Münz: Und genau da sollen wir mit unserem Podcast monatlich ansetzen und aufzeigen, wie man sich in der digitalen und zunehmend vernetzten Welt sicher bewegt. Also nicht Angst machen, sondern eher Tipps geben! Genauso wie man beim Radfahren einen Helm aufsetzt oder beim Autofahren den Gurt anlegt, wollen wir dazu beitragen, dass man sich beim Bewegen in der digitalen Welt mit ein paar Schutzmaßnahmen sicher abdeckt.

Lange: Und wir? Das sind? Ute Lange, ich bin Journalistin, Moderatorin und Trainerin und, gemeinsam mit Michael, Gründerin der Social Bar Bonn. Das ist eine Veranstaltungsreihe, die wir schon seit mehr als zehn Jahren machen. Wir beschäftigen uns mit den Potenzialen von digitalen Medien für gesellschaftliche Entwicklung.

Münz: Ich bin Michael Münz, bin Journalist, Blogger und Buchautor und habe mit Ute die Social Bar vor zehn Jahren ins Leben gerufen. Wir bewegen uns also schon lange in der digitalen Welt und sind da auch schon der einen oder anderen Herausforderung begegnet: der tägliche Versuch, uns mit Spam auf dubiose Webseiten zu lenken, oder mein Blog, der auch schon ein paar Mal gehackt worden ist, oder eben Erpressungsversuche, dass behauptet wurde, ich sei mit meiner Webcam unvorteilhaft gefilmt worden. Das haben wir alles schon erlebt.

Lange: Und zu Beginn des Jahres haben wir einen Vortrag vom BSI bei uns in der Social Bar gehabt. Das war speziell zu dem Informationsangebot für Bürger und Bürgerinnen. Es hat klick gemacht, weil uns plötzlich klar wurde, dass es nicht nur ein technisches Thema ist, wie ich mich absichere, sondern auch eine Frage ist, wie wir uns als Gesellschaft gut vor den Gefahren schützen, die es im Internet geben kann. Und dabei soll der Podcast jetzt helfen: Sie und auch uns beide zu informieren, im digitalen Alltag zu schützen und für die gesamtgesellschaftlichen Auswirkungen ein bisschen mehr zu sensibilisieren. Also ab jetzt monatlich und gemäß unserem Anspruch auf den Plattformen Spotify, Deezer und iTunes! Bitte abonnieren Sie gerne, liken Sie, wie man neudeutsch sagt, und geben Sie uns Rückmeldung, wenn Sie mögen.

Münz: Nach der Einleitung würde ich sagen, steigen wir mal ins Thema ein. Da ist eine Schätzfrage immer ganz cool. Ich habe etwas gefunden, wo ich mal schauen wollte, ob du da eine Einordnung hinkriegst, wie verbreitet bestimmte Sachen sind. Und die Frage, die ich jetzt an dich habe, ist: Wie viele Privatanwender und Privatanwenderinnen sind im vergangenen Jahr von Cyberkriminalität betroffen gewesen, also Menschen zwischen 14 und 69 Jahren? Wie viel Prozent waren das? Was glaubst du? Wie viele von denen sind betroffen gewesen?

Lange: Also, da muss ich erst einmal überlegen, wie viele Menschen das in Deutschland überhaupt sein können. Wenn man jetzt die unter 14-Jährigen herausrechnet und die, die am anderen Ende der Skala sind, schätze ich mal, dass das so um die 60 Millionen Menschen sind und davon fünf Prozent?

Münz: Kalt!

Lange: Zehn Prozent?

Münz: Wärmer, aber immer noch kalt!

Lange: Nun sag schon!

Münz: 25 Prozent der Privatanwenderinnen und Privatanwender haben schon mal schlechte Erfahrungen gemacht, also sind von Cyberkriminalität betroffen gewesen.

Lange: Das sind 15 Millionen Menschen in Deutschland.

Münz: Das ist richtig viel, aber die Bandbreite ist auch echt weit. Das geht von Betrug beim Online-Shopping über den Versuch, das Konto zu hacken, also Fremdzugriff auf Online-Konten, aber auch Cybermobbing fällt darunter! Und dann sind es auch viele Angriffe, die über E-Mail stattfinden, also Ausspionieren von Daten, der Versuch, Schadsoftware zu verbreiten oder auch Phishing zu betreiben. Dazu kommt noch, dass von den 25 Prozent, die wir jetzt haben, ein Drittel auch einen wirtschaftlichen Schaden hatte, Geld verloren hat.

Lange: Das ist doch ein bisschen so wie bei mir im Sommer. Da ist mir ganz analog die Handtasche geklaut worden, und das Geld, das ich in der Tasche hatte. Das war ärgerlich – zugegeben, es war auch ausnahmsweise mal ein bisschen mehr als üblich. Aber was viel ärgerlicher war, war das ganze Gerenne hinterher, also Kreditkarten, Kontodaten, Personalausweis, Führerschein. Es war wochenlang und grässlich. Das ist ja wahrscheinlich, wenn dir online sowas passiert, nicht anders.

Münz: Das Gerenne, was du gerade beschrieben hast, hast du dann auch. Du musst deine Passwörter ändern und auf Verdacht auch sehen, dass du die an anderen Stellen, wo du erst einmal wahrscheinlich nicht betroffen warst, auch änderst, damit Leute nicht versuchen, mit dem einen Passwort andere Konten anzugreifen. Es ist schon viel Arbeit und zeigt auch, dass jeder eigentlich Opfer von so einer Masche werden kann. Nur das Anklicken eines Anhangs oder eines Links kann schon ausreichen, um ein Opfer zu werden an der Stelle. Dann werden deine Daten ausspioniert oder dein Rechner wird als Versender von E-Mails missbraucht oder du wirst Teil eines Netzwerks, das dann Webseiten angreift.

Lange: Das zeigt aber im Umkehrschluss auch wieder: Wenn ich selbst gut damit umgehe oder souverän bin mit meiner Sicherheit, dann kann ich andere schützen, weil ich dann eben nicht Verbreiterin werde von den Dingen, die du gerade erwähnt hast.

Münz: Auch in diesem Fall ist der Schutz relativ einfach, also was den E-Mail-Angriff angeht. Spam zum Beispiel: diese unerwünschten Nachrichten, die massenhaft erst mal ungezählt per E-Mail verschickt werden. Davor kann man sich eigentlich selbst relativ gut schützen und so dann auch verhindern, dass du Schadsoftware oder andere Sachen verbreitest.

Lange: Woher wissen denn die Absender dieser Spams meine E-Mail-Adresse?

Münz: Ja, das kann viele Ursachen haben. Ich weiß, dass viele denken: Von mir haben sie die nicht! Aber in Wirklichkeit haben sie die von dir. Es gibt dann irgendeinen Anreiz, wo du denkst „Oh, super, ein iPad gewinnen!“. Dann tippe ich mal meine E-Mail-Adresse ein. Oder Newsletter-Abo oder solche Geschichten! Solche Daten können dann auch schon mal beim Falschen landen, also nicht bei dem, von dem man denkt, dass er es ist. Das ist eine Variante, dass man wirklich selbst die Person ist, die die Daten von einer Hand in die andere

überreicht. Dann gibt es sogenannte Crawler, also Programme, die das Internet durchforsten.

Lange: Das heißt krabbeln, oder?

Münz: Das heißt krabbeln, genau. Die gucken sich alles an, was nach E-Mail-Adresse aussieht, und sammeln, kopieren und speichern es ab. Das ist ein relativ bekanntes Phänomen. Das führt auch dazu, dass auf Webseiten bei einer E-Mail-Adresse, z.B. „info@-“ oder „mail@bsi.de“, das @-Zeichen nicht mehr als dieser Klammeraffe dargestellt wird, sondern ausgeschrieben wird: Klammer auf, „at“, Klammer zu. Das soll verhindern, dass der Bot – dieses Programm, das das Internet durchforstet und durchkrabbelt – das als E-Mail-Adresse erkennt und abspeichert. Was auch schon mal auftritt, ist, dass man so eine E-Mail-Adresse nur noch als Grafik speichert. Auch dann weiß das Programm nicht, dass es sich um eine E-Mail-Adresse handelt. Und dann dritte Variante, die an dieser Stelle auch relevant ist: der Datenklau, also dass Datenbanken gehackt werden und E-Mail-Adressen und auch Passwörter herausgezogen werden. Das ist relativ häufig und immer mal wieder kriegt man als Nutzer so eine E-Mail: „Ja, da ist etwas passiert. Und bitte ändern Sie Ihr Passwort“. Das kommt schon mal vor. Und es gibt so gewaltige Datenklaus, wo Daten aus verschiedenen Hacker-Angriffen zusammengetragen werden. Im vergangenen Jahr zum Beispiel gab es einen, da steckten in 600 Gigabyte Daten 2,2 Milliarden E-Mail-Adressen drin. Die sind zwar vielleicht auch nicht mehr ganz frisch, aber für einen Hacker oder Angreifer ist es natürlich ganz leicht, die erst einmal automatisiert anzuschreiben und zu schauen, was passiert.

Lange: Was kann passieren? Spam hast du schon erwähnt. Was bedroht mich im Zweifelsfall noch, wenn meine E-Mail-Adresse auf diesem Weg an Leute gerät, wo sie eigentlich nicht hin sollte?

Münz: Es sind auch drei Varianten, die dann auftreten können. Eine Variante ist der klassische Spam: Dann kriegst du halt Post, dass du ein Produkt oder eine Dienstleistung erwerben sollst – von der Potenzpille über jetzt aktuell Schutzmasken; oder im Sommer hab ich viel Ventilatoren-Werbung gesehen. Das ist eine Variante, da versucht man, dich damit irgendwie zu belästigen und auf eine Webseite zu holen. Dann gibt es auch manchmal Anhänge oder Links, die dazu führen, dass du dir ein Programm installierst, was auf deinem Rechner dann die Daten ausspioniert oder, wie gesagt, dich Teil eines Netzwerks werden lässt. Und dann gibt es dieses Phishing, das ich auch schon ein paar Mal erwähnt habe. Dieser Köder, den man auswirft, ist der Versuch, Nutzerinnen dazu zu bewegen, Zugangsdaten preiszugeben.

Lange: Das ist ein bisschen wie der Trickbetrug an der Haustür früher. Es gibt immer eine analoge Variante, die wir schon kennen, wo wir uns aber schützen, weil wir gelernt haben, uns zu schützen. Also, ich mache meine Tür jetzt nicht mehr einfach so ohne weiteres auf. Wenn ich eine Gegensprechanlage habe, dann benutze ich die. Wenn ich einen Türspion habe, gucke ich. Manche Leute haben ja auch Ketten vor der Haustür, bevor sie aufmachen. Und im Zweifelsfall, wenn da jemand in einer seriös aussehenden Uniform vor mir steht,

dann frage ich nach einem Dienstausweis, um sicherzugehen, dass ich nicht Opfer werde von irgendeinem Betrug.

Münz: Genauso könnte man eigentlich auch an E-Mails herangehen. Das ist ein ganz gutes Bild. Da gibt es unterschiedliche Wege, sich zu vergewissern, ob das, was ich da bekommen habe, authentisch ist. Wobei: Am besten kommen die E-Mails erst gar nicht bei dir an. Es gibt ja auch Provider, die dafür sorgen, dass E-Mails schon viel früher abgefischt werden und gar nicht erst bei dir ankommen. Ein aktuelles Virenschutzprogramm ist etwas, was helfen kann, oder eine aktuelle Firewall. Dann hast du da schon einmal viel aussortiert. Und für das, was dann noch bei dir ankommt, ist Skepsis – tatsächlich wie auch eine Tür – manchmal der beste Weg: Kenne ich den Absender? Wie ist es sprachlich, also macht es auf mich den Eindruck, als hätte das ein Muttersprachler verfasst? Das Deutsche ist natürlich auch mit dem Umlaut für international agierende Hacker eine Herausforderung, weil die Umlaute eben nicht dargestellt werden. Bei meinem Namen Michael Münz ist das sehr hilfreich, wenn ich schon sehe, dass der falsch geschrieben ist. Das ist für mich ein Hinweis, dass es vielleicht jemand ist, der weiter entfernt von mir ist und jetzt nicht im direkten Kontakt sonst mit mir steht. Und wie ist es mit Firmenlogo oder Kontaktdaten? Sehen die echt aus? Und wenn ich im Zweifel bin, dann lösche ich das Ding einfach. Im Zweifelsfall, wenn es eine ernste Geschichte ist, dann kommt es nochmal wieder oder auf einem anderen Weg bei mir an. Ich lösche es, ich klicke nichts an und beantworte auch nichts und gebe keinen Hinweis darauf, dass ich als Empfänger wirklich aktiv bin und unter dieser E-Mail-Adresse irgendetwas mache.

Lange: Aber ich kann mich doch im Zweifelsfall auch abmelden. Beim Newsletter ist ja zum Beispiel immer unten immer noch so ein Ding „Wenn Sie das nicht mehr bekommen möchten, dann melden Sie sich hier ab.“ Dann ist doch gut, oder?

Münz: Das ist ja das Fiese. Dieser Abmeldelink ist oft der Köder, der dazu führt, dass die Leute am anderen Ende sehen: „Oh, da ist jemand aktiv und hat diese Post bekommen. An den schicken wir jetzt weiterhin Post“. Das ist echt ein fieser Trick, um Leute dazu zu bewegen, dann doch noch irgendetwas anzuklicken, wenn schon die fünf Links darüber nicht funktioniert haben. Dann bist du erst recht in der Falle. Und es gibt da noch den Punkt der Anhänge, den ich jetzt an dieser Stelle nochmal betone, weil sogar unverdächtig aussehende Dateien, also Word- und Bilddateien, die man halt relativ häufig bekommt, sogar schon Gefährdungen enthalten können. Auch von anderen Dateiformen wie PDFs oder ZIP-Dateien, die ja auch schon mal per Mail ankommen, geht eine Gefahr aus. Das sind echt Sachen, auf die man auf keinen Fall klicken kann, weil man sich nicht sicher sein kann, was damit eigentlich passiert.

Lange: Da brauche ich ja mehr als einen Helm und einen Anschnallgurt. Das klingt jetzt schon nach ganz schön viel, was ich berücksichtigen muss.

Münz: Ja, aber du hast– wie bei deinem Beispiel an der Tür vorhin – ein mehrstufiges Verfahren, sozusagen, um für Sicherheit zu sorgen. Und das sollte in diesem Fall dann

eigentlich auch gelten, sodass es keine schwerwiegenden Folgen gibt. Den einen Punkt, den ich vorhin erwähnt hatte, dass man ja auch auf den Absender guckt und schaut, wer mich da anschreibt, kann man natürlich auch fälschen. Das ist dann natürlich besonders gemein.

Lange: Ja, es gab ja jetzt in der Pandemie E-Mails, zum Beispiel von der Bank, die sehr echt aussahen. Ich habe so eine bekommen, die sicherstellen wollte, dass die Bank auch während des sogenannten Lockdowns noch gut mit mir in Kontakt bleiben kann. Du wirst auf eine Eingabemaske geführt und sollst deine ganzen Daten noch einmal eingeben. Aber irgendwie sah das komisch aus, und es war noch nicht die Adresse, die sonst von meiner Bank kommt. Also habe ich es nicht gemacht. Jetzt, wo ich dir so lausche, war das offensichtlich die richtige Entscheidung.

Münz: Auf jeden Fall! Und was auch besonders gemein ist: Es gibt immer mal wieder Spam-Mails oder Warnhinweise, die angeblich vom BSI kommen, wo wir ja gerade sind, die aber gar nicht von hier sind. Das sind gefälschte Absender, und eigentlich verbreitet das BSI Warnmeldungen niemals über Massen-E-Mail und informiert stattdessen über aktuelle Gefahren auf der Webseite oder gibt Empfehlungen an die Presse heraus. Das ist natürlich besonders gemein, wenn so eine vertrauenswürdige Quelle dir Post schickt und du dann trotzdem löschen musst. Das habe ich auch mit unseren Ansprechpartnern hier im BSI diskutiert. Sie haben auch diese Empfehlung gegeben. Wenn so eine als massenmedial erkennbare Post ankommt, dann auf nichts klicken, weil das BSI eben anders kommuniziert, und einfach löschen.

Lange: Neben deinem Tipp, den gesunden Menschenverstand einzusetzen, ist das, glaube ich, eine gute Stelle, um auf eine Webseite hinzuweisen. Gerade solche Massen-E-Mails kann man auf der Seite „www.internet-beschwerdestelle.de“ melden. Wenn so eine BSI-Massen-E-Mail bei mir ankäme, könnte ich das dort melden und so eventuell andere davor schützen, dass sie die E-Mail auch noch bekommen. Das Verfahren ist relativ einfach. Auf diese Weise kann jeder dazu beitragen, dass diese Spams individuell und auch im größeren Rahmen nicht so einen Schaden anrichten, wie du ihn teilweise geschildert hast.

Münz: Ja, das ist eine gute Idee. Versender von Spam sind darauf aus, menschliche Eigenschaften wie Hilfsbereitschaft und Vertrauen oder Angst oder Respekt vor Autoritäten auszunutzen, um den Empfänger zu manipulieren und ihn zu irgendetwas zu bewegen. Und beim Thema Manipulieren hast du, glaub ich, ja auch noch eine neue Variante entdeckt, die das Ganze noch schwerwiegender erscheinen lässt.

Lange: Ja, wobei die Masche selbst, um die es jetzt geht, seit Jahren bekannt ist. Es gibt sie aber jetzt mit einem Update mit modernen Mitteln.

Münz: Update verfügbar.

Lange: Auch bei kriminellen Maschen gibt es das. Hast du schon mal vom sogenannten CEO-Fraud oder Präsidenten-Betrug gehört?

Münz: Ich bin weder das eine noch das andere. Von daher bin ich da wahrscheinlich noch nicht die Zielgruppe gewesen. Aber das klingt schon mal nicht gut.

Lange: Ne, ist es auch nicht. Die Masche gilt als Klassiker in der Internetkriminalität. Hier sind aber weniger Privatpersonen wie du oder ich gemeint, sondern meistens Mitarbeiter in Firmen, die in der Buchhaltung oder im Rechnungswesen arbeiten, also die Finanztransaktionen für ihre Firmen unternehmen dürfen. Die bekommen dann vermeintlich vom Chef oder der Chefin, also dem CEO, dem Chief Executive Officer – deswegen heißt diese Masche so – eine E-Mail, in der Sie angewiesen werden, eine Summe X – meistens größer, jetzt geht es hier nicht um Kleingeld – auf ein Geschäftskonto im Ausland, also ein fremdes Konto, zu überweisen. Meistens oder häufig folgt dann entweder eine zweite E-Mail oder ein Anruf, aber nicht vom Chef oder der Chefin, sondern von einer Person, die angeblich in dieser Transaktion beteiligt ist, um dem Ganzen noch mehr Glaubwürdigkeit zu verleihen. Die Opfer werden auch oft unter Druck gesetzt, also zum Beispiel Freitagnachmittag, 16 Uhr: „Das Geld muss dann und dann da sein, sonst droht eine Vertragsstrafe, weil der Partner im Ausland das Geld unbedingt haben will“. Sie werden zur Vertraulichkeit angeregt, so nach dem Motto „Das ist ein ganz heißes Projekt, nur Sie und ich wissen davon“. Darauf fallen offensichtlich ziemlich viele rein, sonst wäre das nicht so bekannt. Und immer wieder gibt es neue Tricks und Tipps. Die Täter gehen ziemlich geschickt vor. Sie verschaffen sich vorher Informationen über die Firma, zum Beispiel auf der Webseite: Wer ist der Geschäftsführer, die Geschäftsführerin? Haben die vielleicht irgendwelche Investitionen im Ausland in einer Pressemitteilung bekannt gegeben? Dann wissen sie schon eine ganze Menge. Gibt es E-Mail-Erreichbarkeiten? Gibt es Mitarbeiter, die in Social Media vielleicht ein bisschen etwas über die Firma erzählt haben? Es ist gar nicht so schwierig, diese Informationen zu finden, wie man denkt. Die Schäden sind allerdings beträchtlich. Ich habe einige Fälle gelesen, wo bis zu 40 oder 50 Millionen Euro transferiert wurden, und das Geld ist dann größtenteils futsch. Es kommt nicht wieder. Die US-Bundespolizei, das FBI, geht weltweit von Schäden in Milliardenhöhe aus. In Deutschland gibt es Staatsanwaltschaften in der ganzen Republik, die in mehr als 200 Fällen schon ermitteln. Nicht alle Fälle werden bekannt, weil die Firmen auch nicht alles bekannt geben, weil sie einen Imageschaden fürchten und vielleicht auch Sorge haben nach dem Motto „Wie kann man so blöd sein? Wie kann man auf so etwas reinfallen?“. So etwas gibt man vielleicht nicht so gerne zu, dass man da etwas vertrauensselig war.

Münz: OK, verstehe. Das ist schon eine neue Form des Manipulierens und der Beeinträchtigung. Wo man aber auch im Zweifelsfall, wenn es eine Person ist, die man nicht kennt, am Telefon sagen kann: „Komisch, ich lass es mal lieber bleiben“. Aber da hört die Geschichte wahrscheinlich gar nicht auf.

Lange: Der neue Ansatz baut auf dem alten auf. Aber die neue Variante, die seit einiger Zeit beobachtet wird, kommt noch viel realistischer daher, weil moderne Technologie genutzt wird. Die Täter machen sich künstliche Intelligenz zunutze. Sie nutzen selbstlernende Software, die Audiodateien, die man sich besorgt hat auf irgendeinem Wege, als Basis

nimmt, um die Sprechweise, den Tonfall und die Tonlage des Chefs oder der Chefin nachzuahmen. Das klingt alles so realistisch. Auch die Reihenfolge wird gerne umgekehrt: Erst kommt der Anruf und später eine E-Mail. Das heißt, da ist Vertrauen und Kontakt hergestellt. Und wenn du überlegst: Du hast ja vielleicht auch schon mal Anrufe bekommen von Leuten, die im Auto sitzen oder gerade mit der Bahn unterwegs sind. Da ist die Audioqualität manchmal nicht so gut. Wenn man dann das Gefühl hat, dass es die Person ist, dann glaubt man das vielleicht schnell. Das kommt jetzt schon immer häufiger vor. Da gibt es etliche Fälle, wo es auch um große Summen ging. Die Art von Angriff mit künstlicher Intelligenz nennt man Deep Fake, weil da zwei Dinge zusammenkommen: Deep Learning, maschinelles Lernen, und Fake, also die Fälschung. Das heißt, ich werde übers Ohr gehauen, weil das so klingt, als wäre das eine Person, die ich schon kenne. Selbst Fachleute können das manchmal gar nicht richtig unterscheiden, ob es echt ist oder nicht, weil es so gut gemacht ist.

Münz: Da frage ich mich aber genauso, wie du vorhin bei den Mails gefragt hast: Woher kommen die Audio-Inhalte, mit denen gefälschten Nachrichten zusammengebaut werden? Klar, so ein CEO hält mal einen Vortrag oder einen TED Talk oder gibt auf einer Konferenz oder in der Presse ein Interview. Dann kann man die Audiodateien oder Videodateien entsprechend abgreifen, umbauen, und schon hat man Inhalte, die ursprünglich so nie gesagt worden sind.

Lange: Ja, und es gibt ja im Moment eine Mode für Podcasts. Wir machen ja jetzt auch einen. Der ist auch öffentlich verfügbar. Ich glaube, Audiodateien zu finden, ist wahrscheinlich heute überhaupt nicht mehr so schwer.

Münz: Das heißt, ich muss alle Leute, die mich kennen, mal vorwarnen, dass vielleicht etwas Komisches ankommen könnte.

Lange: Ja, aber du kannst dich natürlich auch schützen. Da gilt das alte Sprichwort: Vertrauen ist gut, Kontrolle ist besser. Wenn einem ein Vorgang dubios vorkommt oder ungewöhnlich, dann kann man das ja sorgfältig prüfen, bevor man aktiv wird. Man kann zum Beispiel die E-Mail-Adresse checken: Ist es dieselbe, die der Chef, die Chefin sonst auch nutzt, oder ist da plötzlich eine andere Endung? Ist die Ansprache dieselbe, die ich sonst von dieser Person kriege? Wenn ich mir nicht sicher bin, dann kann ich ja auch einfach mal zurückrufen unter der mir bekannten Telefonnummer, damit ich einfach sicher gehen kann: Ist das wirklich von der Person? Das hat zum Beispiel ein Mitarbeiter bei der Schokoladenfirma Ritter Sport gemacht. Der hat so eine Anweisung bekommen und wunderte sich über einige Dinge, darunter die E-Mail-Adresse. Aber was ihn besonders stutzig gemacht hat, ist, dass der Chef ihn in dieser E-Mail gesiezt hat. Die waren im realen Leben schon seit Jahren per Du. Dann hat er einfach zum Telefon gegriffen und hat zu seinem Chef gesagt: „Du, ist das wirklich von dir? Er hat gesagt „Nee!“. Sie waren sich dann sicher, dass es ein versuchter Betrug ist. Sie haben sofort die Staatsanwaltschaft und Polizei eingeschaltet und haben dann – das liest sich echt wie ein Krimi – in einem mehrstufigen Verfahren Fallen ausgelegt für die Täter. Es hat dann ein paar Tage gedauert, aber die sind

tatsächlich hineingetappt und sind zu mehreren Jahren Haft verurteilt worden. Und die Firma hat halt nicht Geld irgendwohin transferiert, wo sie es nie wiederbekommen hätte.

Münz: Was mich an der Stelle noch interessieren würde: Waren die Täter Personen, die in der Nähe waren und sich das gesondert angeguckt hatten oder wo saßen die am Ende?

Lange: Am Ende ist einer der Täter in Israel verhaftet worden. Das ist online eigentlich ziemlich egal, wo du sitzt. Das haben wir jetzt in den letzten Monaten auch gelernt. Die Informationen sind im Internet verfügbar. Wenn du weißt, was du brauchst für so einen Betrug, dann recherchiert du das. Von wo du das macht, ist egal.

Münz: Bei Deep Fakes habe ich eigentlich bislang immer an Videos gedacht. Ich weiß noch, wie wir vor fünf Jahren alle bei Böhmermann und dem Varoufakis Finger darüber beratschlagt haben, ob der jetzt gar nichts gemacht und uns nur reingelegt hat oder ob es eine aufwendige Produktion war oder ob Varoufakis den Mittelfinger wirklich bei diesem Vortrag gezeigt hat. Aber das geht jetzt ja offensichtlich auch noch in eine ganz andere Richtung.

Lange: Ja, das Erste, worüber berichtet wurde, waren Videos. Die tauchten Ende 2010, glaube ich, das erste Mal in den USA auf, auch mit dem Begriff Deep Fakes, weil es um diese mit künstlicher Intelligenz bearbeiteten Videos ging. Da hatten Nutzer auf einer bekannten Plattform Filme hochgeladen, in denen Gesichter von prominenten Schauspielern etc. auf die Körper von Pornodarsteller und -darstellerinnen montiert oder reingerechnet waren; nicht montiert, es ist ja tatsächlich eine Rechenleistung, die da erbracht wird. Das wirkte zwar, wenn wir das heute angucken, noch etwas plump nach dem Motto „Warum hat das jemand geglaubt?“. Aber es war etwas Neues. Für die Betroffenen war das natürlich ein beträchtlicher Schaden für Reputation, aber auch emotional – wie peinlich das ist. Du kriegst es auch so schnell nicht wieder aus der Welt. Die Technik hat sich aber mittlerweile so rasant entwickelt, dass es Videos gibt, denen es eben nicht mehr anzumerken ist. Selbst Fachleute sind sich nicht sicher trotz all ihrer Methoden, die sie entwickelt haben. Das wird ja parallel entwickelt: Die, die Deep Fakes machen, nutzen die Technologie. Dann gibt es eine ganze Menge Menschen, die versuchen, genau das zu verhindern. Die entwickeln Sicherheitsstufen. Das ist wie ein kleines Wettrennen, Hasel und Igel bei Deep Fakes. Aber das ist selbst für Experten und Expertinnen heute häufig nicht mehr zu erkennen: Ist es das oder ist es das nicht?

Münz: Manchmal wird es ja aufgelöst. Ich erinnere mich noch an dieses Video von Barack Obama, wo er sich über seinen Nachfolger im Amt lustig macht. Da war hinterher im Abspann zu sehen, dass das eine Fälschung war.

Lange: Ja, du hast es dir bis zum Ende angeschaut, aber viele machen das nicht. Die sehen dann nur das Erste und erfreuen sich daran, dass er dieses Schimpfwort für seinen Nachfolger nutzt und klicken dann weiter. Das war eigentlich ein Deep Fake, das vor Deep Fakes warnen sollte. Das Video ist es von einem US-amerikanischen Regisseur, der fast so

sprechen kann wie Obama. Der hat die Tonlage, hat die Gestik und die Mimik und, wie du sagst: Am Ende blendet er dann sein Gesicht neben das von Barack Obama ein. Man sieht, dass sie parallel sprechen und man versteht, wie das wahrscheinlich hergestellt wurde. Aber in der schnelllebigen Zeit gucken sich viele das ja gar nicht bis zu Ende an und glauben dann, was da gezeigt wurde.

Münz: Gerade heute habe ich noch ein neues Video gesehen, in dem der aktueller US-Präsident Donald Trump vorkommt. Das ist es eine ähnliche Strategie. Aber ich habe auch erst gedacht: Wie haben Sie das Ding gemacht?

Lange: Ja, dieses Video ist ehrlich gesagt von Anfang an als Deep Fake bezeichnet worden. Das ist von einem russischen Sender, der Werbung für seine Berichterstattung über die bevorstehende US-Wahl macht. Es wird gleich eingeblendet, dass es Deep Fake ist. Das ist technisch extrem gut gemacht. Das lässt einen dann über andere Dinge nachdenken. Aber es sind auch Dinge drin, die sind so unglaubwürdig: Die Perücke, die sie der Person, die angeblich der amerikanische Präsident ist, aufgesetzt haben, ist wirklich so daneben. Selbst wenn du erst mittendrin in das Video einschaltest und das eingeblendete Anfangsstatement, dass es ein Deep Fakes ist, und die Einblendung am Ende nicht gesehen hast, kommst du gar nicht auf die Idee, dass es realistisch ist. Aber es ist insofern realistisch, als dass sie – wir haben eben über Audio-Dateien gesprochen – Zitate aufgenommen haben, die er tatsächlich gesagt hat in unterschiedlichen Kontexten. Diese haben sie dann in diesem Film verwendet, um daraus eine Geschichte zu drehen. Es ist tatsächlich eine Herausforderung zu unterscheiden: Was ist echt und was ist nicht es nicht?

Münz: In dem Fall ist es aufgelöst. Das ist ganz gut und wird wahrscheinlich auch keine politische Krise auslösen. Aber in anderen Fällen ist es doch so gekommen, dass da nicht nur Einzelne, sondern eine ganze Nation betroffen war.

Lange: Ja, aber auch anders, als man denkt. Da geht es um einen Fall in einem afrikanischen Staat vor etwa zwei Jahren. Da tauchte ein Video in sozialen Medien auf, das den Präsidenten bei einer Rede zeigte. Die Geschichte dahinter ist, dass dieser Präsident monatelang vorher im Ausland war, weil er schwer erkrankt war. Viele wussten gar nicht, ob er noch lebt, weil er lange nicht öffentlich sichtbar gewesen ist. Manche hatten ihn auch schon für tot erklärt. Dazu kam, dass es kurz vor einer Wahl war in dem Land und die Situation politisch eh ein bisschen unruhig und aufgeheizt war. Als dieses Video erschien, hat der politische Gegner gesagt: „Das ist ein Deep Fake, das stimmt nicht, der ist tot. Das kann er nicht sein“. Das wiederum hat so viel Misstrauen erzeugt, dass das Militär eine Woche später einen Putsch versucht hat. Der ist gescheitert. Der Präsident ist mittlerweile genesen. Er ist auch weiterhin im Amt. Aber allein der Verdacht, dass es ein Deep Fake sein könnte, reichte aus. Bis heute ist der Verdacht nicht bewiesen. Das ist das Interessante an dem Fall. Selbst Fachleute sind sich nicht sicher, ob es ein echtes Video ist oder ob es gefälscht wurde. Aber die Konsequenzen waren so gravierend, dass es tatsächlich fast zu einem Umsturz gekommen wäre.

Münz: Da muss ich doch noch mal drüber nachdenken. Offensichtlich kann es durchaus sein, dass in einem bestimmten gesellschaftlichen Klima, das vielleicht durch Zerrissenheit und Misstrauen geprägt ist, solche Anlässe wie ein Deep Fake Video zu Umbrüchen führen können. Da können wir vielleicht auch in einer der folgenden Folgen nochmal drüber nachdenken, wie solche Geschichten erst einmal den Einzelnen erreichen und was sie dann für Folgen für eine Gesellschaft haben können. Da bleibt aber dann umso mehr die Frage: Was kann ich denn dazu beitragen, dass es nicht noch schlimmer wird?

Lange: Ja, das ist auch wieder so eine Binsenweisheit. Um sich und andere zu schützen, reicht der gesunde Menschenverstand. Wenn etwas unwahrscheinlich daherkommt oder mir sehr, sehr seltsam erscheint, dann ist es das häufig auch. Und wenn mir zum Beispiel etwas komisch vorkommt, dann ist meine erste Regel für mich: Ich gucke nochmal nach anderen Quellen. Gibt es irgendetwas, was das widerlegt, was ich da gerade sehe? Oder gibt es mehr Informationen dazu, mehr Hintergrund? Kann ich mich schlau machen? Und wenn ich dann immer noch nicht sicher bin, dann teile ich einfach nicht. Ich möchte das nicht verbreiten und vielleicht dazu beitragen, dass es schlimmer wird. Oft verbreitet sich eine Falschmeldung, weil viele es unbedacht verteilen und die Korrektur dann eben nicht mehr teilen. In Indien ist das nicht nur einmal, sondern mehrfach passiert. Da sind Falschmeldungen über so einen Messenger-Dienst geteilt worden, und zwar zigtausendfach. Und das hat in bestimmten Regionen die Menschen so aufgebracht, dass andere dabei gelyncht wurden, weil die Korrektur eben nicht mehr geteilt wurde. Das ist natürlich die gruseligste Variante von unbedachtem Teilen, die man sich vorstellen kann. Das heißt, im Zweifelsfall lieber nicht teilen und eben nicht dazu beitragen, dass sich etwas verbreitet, was nachher zu einer schlimmeren Situation führen kann.

Münz: Wenn ich jetzt über das nachdenke, was wir besprochen haben, wie wir von der Potenzpille zum Putsch gekommen sind, ist das schon ein ganz schöner Ritt und vielleicht auch eher verunsichernd als das, was wir eigentlich wollen. Aber das ist ja auch kein „Gehen Sie auf jeden Fall offline“-Podcast, sondern ein „Gehen Sie sicher online“-Podcast. Vielleicht an dieser Stelle auch noch einmal der Hinweis, dass all das nicht passieren muss, wenn man sich schützt im digitalen Alltag genauso wie im analogen mit Fahrradhelm und Anschnallgurt. Es heißt, auch im digitalen Alltag Menschenverstand walten zu lassen und ein paar Schutzmaßnahmen einzuziehen, damit man weder persönlich noch in anderem Rahmen für Schaden anfällig wird.

Lange: Also ich persönlich verspreche mir noch ein bisschen mehr Hinweise für dieses unfallfreie Unterwegs-Sein im digitalen Alltag vom European Cyber Security Month. Das ist der europäische Cyber-Sicherheits-Monat. Für „Cyber“ habe ich immer noch keine gute deutsche Übersetzung gefunden. Vielleicht finden wir die noch. Jedenfalls ist der ECSM eine jährliche Kampagne der Europäischen Union, wo es darum geht, Bürger, Unternehmen, Behörden etc. für Sicherheit im digitalen Alltag zu sensibilisieren, mit Tipps und Tricks auszustatten. Da kann jeder teilnehmen.

Münz: Das ist ja so ein bisschen das, was wir hier auch machen wollen. Aber dann geballt in einem Monat und mit unterschiedlichen Themen vermutlich.

Lange: Das BSI ist Koordinator, man findet auch auf der Webseite das Programm. Man kann also suchen nach Angeboten für Jugendliche, für Senioren, für Behörden, für Medien, für Firmen. Da gibt es alles Mögliche. Gleichzeitig gibt es Behörden, die Angebote machen. Es gibt Firmen, die Angebote machen. Es gibt Hochschulen, die Angebote machen. Man kann sich zum Beispiel informieren in Online-Seminaren: Wie kann ich mich bei Phishing schützen? Wie kann ich meinen digitalen Nachlass regeln, bevor es zu spät ist? Es gibt eine ganze Vielfalt. Ich glaube, da ist für jeden, der sich dafür interessiert, was dabei. Da kann man sich einfach Anregungen holen in dem Kalender, der jetzt öffentlich ist.

Münz: Dann weiß ich ja schon, was ich jetzt im Oktober mache. Und dann würde ich vorschlagen, wir sehen uns dann Ende Oktober wieder für ein Update und gucken, was wir gelernt haben. Eine Sache haben wir aber schon vorbereitet.

Lange: Ja, da freue ich mich besonders drauf. Und zwar haben wir einen Kollegen aus dem BSI, der dem sogenannten Mobile Incident Response Team arbeitet. Die Abkürzung lautet MIRT und steht für mobile Eingreiftruppe bei solchen Vorfällen. Das ist eine Art Feuerwehr für digitale Sicherheit, die ausrückt, wenn es irgendwo brennt! Der Experte steht uns Rede und Antwort. Ich glaube, die erste Frage, die ich stellen werde, ist, ob die auch an so einer Stange wie der Feuerwehr runterrutschen, wenn der Alarm losgeht.

Münz: Das klingt super, das würde ich auch gerne wissen. Und vielleicht hören dann ja auch ein paar junge Menschen zu und denken: „Oh ja, das ist der Berufswunsch. Das will ich später auch mal machen“. Prima, klingt super. Und dann noch der Hinweis, vielleicht an dieser Stelle, dass ein paar Sachen, die wir angesprochen haben, zum Nachlesen und Weiterlesen auch in den Shownotes stehen zu diesem Podcast-

Lange: Ja, und natürlich auch der Hinweis: Wo können Sie den hören? Bei Spotify, Deezer und iTunes. Also bitte abonnieren, liken, Rückmeldungen schicken. Wir freuen uns auch über Ihre Tipps und Erfahrungen für den und aus dem digitalen Alltag. Sie können das BSI auf Facebook, Twitter und YouTube erreichen. Wenn Sie eine E-Mail schicken wollen, dann lautet diese mail@bsi-fuer-buerger.de. Und nicht nur bei deinem Nachnamen, sondern bei allen Umlauten im Internet machen wir ein „u“ und ein „e“ daraus. Wir freuen uns auf jeden Fall auf Post.

Münz: Auf jeden Fall! Dann sehen und hören wir uns in einem Monat wieder! Bis dahin Tschüss aus dem BSI.

Lange: Tschüss, bis bald!

Besuchen Sie uns auch auf:

https://www.bsi-fuer-buerger.de
https://www.facebook.com/bsi.fuer.buerger
https://www.twitter.com/BSI_Presse

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