„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 30, 28.04.2023:
Worst-Case-Szenarien – Und wie ihr sie vermeiden könnt

Moderation: Ute Lange, Michael Münz
Gast: Anders Kölligan
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: Und mein Name ist Michael Münz, und auch von mir ein herzliches Willkommen zu dieser Premiere. Ja, genau, ihr habt richtig gehört, wir haben uns für diese Folge was überlegt. Bleibt also dran, aber nicht in den Shownotes gucken, weil sonst ist es ja keine Überraschung mehr.

Ute Lange: Ja das kann ich nur verstärken. Zunächst mal ganz herzlichen Dank für eure Einsendungen. Da waren viele spannende Fragen dabei zum digitalen Alltag und der großen Sicherheit, die wir da haben sollten, und wir möchten die natürlich gerne aufnehmen. Deswegen haben wir uns heute einen Experten eingeladen, der einige davon beantworten kann. Andere folgen dann in anderen Ausgaben des Podcasts. Wir wechseln dazu heute mal unsere Perspektive und sprechen über die Frage, was kann denn schlimmstenfalls passieren, so frei nach dem Motto “What could possibly go wrong?”. Aber wir werden natürlich auch darüber sprechen, wie wir uns, ihr euch und natürlich auch dieser Podcast diese Worst-Case-Szenarien verhindern kann. Michael, was wäre denn für dich eines dieser schlimmsten Fälle?

Michael Münz: Mein Worst-Case-Szenario ist ein Keylogger, also eine Software, die meine Anschläge auf der Tastatur, am Rechner oder von mir aus auch am Telefon mitschreibt und dadurch Zugriff erlangt auf Passwörter, Bankdaten, e-Mail Texte, die ich zum Beispiel schreibe. Also die Vorstellung, dass da was auf meinem Computer ist, was dann alles mitprotokolliert und dann an jemand anders weiterreicht, finde ich ganz schön beängstigend. Ich gucke deswegen auch immer bei Software, wenn ich die installiere, oder bei Apps auch immer, dass die sicher sind. Also ich mache ja nebenbei zum Beispiel noch Musik, und da gehört es auch irgendwie dazu, dass man sich Erweiterungen runterlädt, die dann jemand ins Netz gestellt hat. Aber da gucke ich auch tatsächlich immer, dass es aus einem sicheren Shop oder aus einer sicheren

Quelle kommt, damit ich mir da nichts einfange, was dann meine Sorgen irgendwie, naja bestätigt. Genau das ist mein Worst-Case-Szenario. Welches ist es bei dir Ute?

Ute Lange: Also, bei mir ist es tatsächlich der Gedanke, dass mir ein Social Media Account gehackt wird, weil ich immer mal wieder und gar nicht so selten von Freunden und Bekannten Nachrichten bekomme, wo es dann heißt: "Um Gottes Willen, mein Konto ist gehackt, gehe nicht auf den Link oder lösch diese Nachricht am besten", und ich dann immer sofort denke, oh Gott, habe ich da etwa schon was gemacht? Weil manchmal ist der zeitliche Abstand nicht mehr so nachzuvollziehen zwischen Nachricht, und eventuell habe ich eine Nachricht bekommen, in der so etwas war, und die Sorge ist, dann passiert bei mir jetzt auch was. Also bin ich dann schon in irgendeinem Strudel mit drin, und die andere Sorge ist dann: Oh Gott, wenn mein Konto gehackt wird. Also was muss ich denn da am anderen Ende machen, und wie kann ich mich davor schützen? Also, das sind so zwei Aspekte. Dieses Account-Hacking, das ich immer mal wieder reingespült kriege, als Sorge dadurch, dass es anderen passiert.

Michael Münz: Ja, das kann ich total gut verstehen, kenne ich auch dieses "oh nein ich bin gehackt worden. bitte mach nicht dies und jenes", und ja, wie das kommt, was man dagegen tun kann und was sich daraus alles ergeben kann. Diese Fragen stellen wir heute jetzt in dieser Folge dem Experten, und dann kann ich das Premierengeheimnis ja auch gleich mal lüften, denn wir haben heute jemanden dabei, der schon einmal dabei war.

Ute Lange: Ja, und zwar war er im Sommer 2021 hier bei uns im Podcast. Damals haben wir mit ihm über die Absicherung der bevorstehenden Bundestagswahl gesprochen. Heute geht es um die Absicherung unseres digitalen Alltags. Ganz herzlich willkommen zurück, Anders Kölligan!

Anders Kölligan*:* Ja, hallo zusammen, ich freue mich natürlich wieder hier zu sein, und es ist natürlich jetzt eine besondere Ehre, dann zum ersten Mal der wieder auftretende Gast zu sein. Ja, vielen Dank!

Michael Münz: Ja, wir dachten, bei der Bundestagswahl ist ja alles so weit rund gelaufen. Dann können wir dich da dann doch noch mal dazu einladen und dein Wirken honorieren, an dieser Stelle mit einer zweiten Einladung. Schön, dass du dir wieder die Zeit nimmst für unsere Hörerinnen und Hörer und auch für uns. Und naja also so, wo wir uns wiedersehen, wie ist dir seitdem ergangen? Bei dir alles sicher geblieben? Seitdem?

Anders Kölligan: Ja, wie du schon gesagt hast, ich meine, die Bundestagswahl ist ja zumindest aus der Cyber-Sicherheitsperspektive einwandfrei gelaufen, und da möchte ich natürlich jetzt auch noch mal sagen, ich mache ja nur einen ganz kleinen Teil von dem, was die Bundestagswahlabsicherung angeht, und meine Kolleginnen

und Kollegen auch von den anderen Behörden haben da natürlich den größeren Anteil dran, und deswegen, das ist ein gemeinsames Bestreben, was dann aber auch am Ende ja gut funktioniert hat. Aber es funktioniert alles aktuell ganz, ganz gut.

Ute Lange: Ja, das für alle die, die beim letzten mal noch nicht mehr über dich erfahren haben. Vielleicht magst du nochmal ganz gerade kurz sagen, wo du im BSI tätig bist und was da alles in dieser Arbeit hineinfällt bei dir.

Anders Kölligan: Ja, also ist jetzt natürlich auch ein bisschen Wiederholung, aber was sich geändert hat, ich bin jetzt in einem anderen Referat, von der Nummer her, OC 16, heißt es jetzt, und wir sind zuständig für die Sicherheit in Internet, Infrastrukturen und Diensten. Und tatsächlich, jetzt im Rahmen der Bundestagswahl waren das dann halt vor allem dieser Diensteaspekt und jetzt auch wieder dieser Diensteaspekt, warum ich jetzt hier bin. Vor allem fallen darunter halt alle möglichen Dienste, die im Netz angeboten werden, auf Webseiten, aber auch dann insbesondere die sozialen Netzwerke, und deswegen gerade so Themen wie Accountsicherheit, die ja jetzt hier im Worst-Case-Szenario sozusagen der Fokus sind. Das ist mit einer meiner Aufgabenschwerpunkte.

Ute Lange: Und vielleicht kannst du noch kurz die Abkürzung auflösen, OC , für alle, nicht Insider und Insiderinnen. Wofür steht das bei euch?

Anders Kölligan: Also, OC ist operationale Cyber-Sicherheit. Das heißt, im Prinzip sind wir dafür zuständig, dass der Betrieb auch sinnvoll läuft. Also, es gibt natürlich dann noch andere Abteilungen im BSI, unter anderem, was jetzt hier vielleicht für die Hörerinnen und Hörer interessant sein könnte, halt dann den Verbraucherschutz als Abteilung im BSI oder als Referat im BSI.

Michael Münz: Prima, also wir freuen, dass du dabei bist. Wir haben in den vergangenen Wochen Fragen der Hörerinnen und Hörer eingesammelt, ein bisschen sortiert und gehen die dann jetzt mal mit dir durch und schauen mal, was eigentlich alles schief gehen kann. Bist du bereit?

Anders Kölligan: Ja!

Michael Münz: Okay! Dann wäre die erste Frage, die ich an dich hätte: “Was ist eigentlich so schlimm an meinem Passwort? Eins, zwei, drei, vier, fünf, sechs, das nehmen doch alle!”

Anders Kölligan: Ja, weiß ich nicht, ob das alle nehmen. Ich hoffe, dass das heutzutage nicht mehr so stark verbreitet ist. Ich würde jetzt nicht sagen, dass es ein schlimmes Passwort an sich ist, aber man muss sich natürlich Gedanken darüber machen, wo man dieses Passwort einsetzt. Das hat natürlich verschiedene Aspekte. Also erst mal ist es auch ein recht kurzes Passwort. Ich glaube, mittlerweile sollte eigentlich fast jede und jeder mitbekommen haben, dass das kein sicheres Passwort

auf jeden Fall ist. Also es ist natürlich irgendwie ganz nützlich, wenn man mal schnell irgendwo ein Passwort braucht, und einem nicht wichtig ist, dass das dann auch sinnvoll abgesichert ist. Aber Problem Nummer eins ist natürlich, Zahlenfolgen oder Buchstabenfolgen an sich sind leicht zu erraten. Die meisten Account-Hacks werden automatisch durchgeführt und nicht etwa, das halt eine Person wirklich wie im Film vor dem Computer sitzt und 1000 Passwörter versucht einzugeben. Das würde natürlich viel zu lange dauern, sondern das wird natürlich automatisiert, und es gibt natürlich Datenbanken dafür, die können sich dann halt Hackerinnen und Hacker auch zum Beispiel im Darknet einkaufen. Die sind dann zum Beispiel aus Datenleaks, und da werden natürlich hoch frequentierte Passwörter, die werden sozusagen als erstes dann normalerweise in den Algorithmen versucht. Die Userdaten werden halt einfach ausprobiert, mit verschiedenen Passwörtern, und eins von den Passwörtern, was sicherlich als allererstes abgefragt werden, ist sowas wie eins, zwei, drei, vier, fünf, sechs oder QWERTZ und so weiter, also kurze Folgen, die auf der Tastatur einzugeben sind. Kurz danach kommen dann natürlich solche Passwortkombinationen, wie wenn man Namen und Geburtsdatum hat, oder von den Kindern und solche personenbezogenen Daten, die sind ja oft auch im Internet, zum Beispiel in den sozialen Medien, zu finden, und versierte Hackerinnen und Hacker könnten da natürlich Passwortkombinationen finden, die dann auch schnell mal zum Erfolg führen können, und deswegen macht es schon Sinn, sich Gedanken darüber zu machen, welche Passwörter man verwendet.

Michael Münz: Und der Erfolg der Hacker ist ja dann unser Worst-Case-Szenario. Also angenommen, jemand würde jetzt von meinem Mail Account das Passwort erraten und wäre dann in meinem Mail Account drinnen. Was sind denn dann so die Szenarien, die dann auch aus der BSI Sicht diejenigen sind, wo ihr sagt, das ist schon mal ganz schlecht, weil?

Anders Kölligan: Also tatsächlich ist das wirklich der Worst-Case, also im Normalfall ist das der Worst-Case also tatsächlich, wenn man einen e-Mail Account verwendet, nur einen einzigen und auf den alle Konten, zum Beispiel registriert hat, und dann hat tatsächlich jemand freien Zugang zu diesem Account. Das ermöglicht im Prinzip dann ja auch den Zugang zu allen anderen Accounts, die mit diesem e-Mail Account verknüpft sind. Und das ist dann zum Beispiel, man kennt das ja selbst, man hat mal das Passwort auf einer bestimmten Plattform vergessen. Da gibt es halt diese Passwort zurücksetzen Links und dieser ganze recovery Prozess, der funktioniert zum großen Teil über e-Mail. Das muss nicht zwangsläufig so sein, das ist auch mit Sicherheit sinnvoll, sich zu überlegen, ob das so sein sollte bei der entsprechenden Plattform. Aber im Normalfall läuft das über e-Mail, und über eben diesen Zugang kann dann halt auch die Person, die da den Zugang hat, sich Zugang zu allen möglichen anderen Accounts verschaffen und dann, was ihr jetzt auch zum Beispiel schon angesprochen hat, was dann auch noch fatal sein kann, ist, diese Person kann sich dann als ich selbst, als Inhaber dieses e-Mails accounts ausgeben und anderen

Personen, die zum Beispiel in meiner Kontaktliste sind, e-Mails schreiben, die dann halt auch so aussehen, als würden sie von mir kommen. Da gibt es natürlich dann zum Beispiel die Möglichkeit, einfach auf e-Mails zu Antworten, die schon dagewesen sind. Das sieht dann sehr legitim aus und ist schwer zu erkennen für den gutversierten Nutzer. Das kann auch alles zum Teil automatisiert werden, das einfach auf e-Mails geantwortet werden, das Informationen aus den e-Mails herausgelesen werden und die dann halt eben für die weitere Verbreitung zum Beispiel von Schadsoftware genutzt werden kann und auch um wieder den Bogen zu machen, ist das auch einer der Wege, wie dann zum Beispiel ein Keylogger auf deinen Computer heruntergeladen werden kann, zum Beispiel durch einen Link zu einer Schadsoftware, oder das die Schadsoftware in Form von zum Beispiel versteckt in einem regulären Office Dokument schon mit heruntergeladen wird. Und dadurch, dass halt eben dieser E-Mail-Account der Zugang zu so vielen Möglichkeiten ist, kann das halt zum richtigen Schneeballeffekt führen, der nicht nur mich betrifft, sondern auch viele andere. Von daher ist das mit Sicherheit einer der schlimmsten Worst-Cases, die man sich so vorstellen kann.

Ute Lange: Okay, wir wollen ja auch darüber sprechen, wie wir das verhindern können. Aber eine Frage beschäftigt mich dann doch noch, wenn wir über Passwörter sprechen, wenn man mehr als einen Account hat, was wir in der Regel heute ja alle haben, weil ganz viele Dinge digitalisiert sind. Das ist ja auch eine Erleichterung im Alltag. Was für mich aber überhaupt keine Erleichterung ist, ist, dass ich mir für jedes Konto dann irgendwas neues einfallen lassen muss, und du hast bestimmt auch noch ein Hinweis, wie denn so ein Passwort aussehen soll, wenn es nicht eins, zwei, drei, vier, fünf, sechs ist. Was ist denn, wenn ich jetzt sage, es ist für mich leichter, ich erfinde mal ein Passwort, das auch all den Sicherheitskriterien, die heute empfohlen werden, entspricht, und nutze das dann einfach für alles, was ich habe, also meine Bankkonten, meine Social Media Accounts, meine Online Shops, was immer ich online mache, damit ich mir nicht so viele verschiedene Sachen merken muss, weil mein Gehirn hat ja vielleicht auch eine Erinnerungskapazität, und die ist mittlerweile manchmal ein bisschen überfordert mit den ganzen Passwörtern.

Anders Kölligan: Ja, richtig, also Ute, du hast natürlich Recht, also es muss auch praktikabel sein der Umgang mit Passwörtern, und das ist natürlich der Spagat, den man haben muss. Also muss natürlich möglichst komplexe, möglichst lange Passwörter haben. Das sind so die Maximen, die man haben muss, um ein sicheres Passwort zu generieren, und das macht natürlich, wenn man dann für jede Plattform ein eigenes Passwort hat, das macht es dann natürlich zunehmend schwierig. Zu dem Zweck kann ich auf jeden Fall empfehlen, dass man Passwort-Manager verwenden sollte. Also das sind Programme, wo man dann im Prinzip durch ein Master-Kennwort, was man dann hoffentlich auch nirgendwo anders verwendet, eben Zugriff auf die ganzen anderen Passwörter hat. Die haben dann zum Teil auch Plug-Ins, dass man die automatisch eingeben kann oder eingeben lassen kann. Das

funktioniert also auf jeden Fall schon mal sehr gut. Da ist dann auch meistens tatsächlich eingebaut, dass man sich Passwörter generieren lassen kann, die dann auch wirklich zufällig sind. Die kann man sich natürlich selbst dann gar nicht mehr merken. Aber diese Passwörter sind halt sehr schwer für einen Hacker zu entschlüsseln, und das Problem, was du ja jetzt schon angesprochen hast, ein Passwort für alle, ist halt genau das, was ich eben auch schon gesagt habe, wenn dieses Passwort dann einmal rauskommt, wie auch immer, also das kann zum Beispiel in einem Datenleak drinnen sein oder auf irgendeine Art und Weise sonst an die Öffentlichkeit geraten sein. Das kann ja auch passieren, dass man das selbst jemandem gibt, und dann hat man es selbst nicht mehr unter Kontrolle, wo dieses Passwort hingeht. Das ist ein großes Problem auch was wir versuchen natürlich zu verhindern, ist, dass Passwörter dann zum Teil bei weniger namenhaften Betreibern im Klartext gespeichert werden. Das heißt, da gibt es irgendwo eine Datenbank, wo dieses Passwort dann im Klartext vorliegt, und wenn dann jemand Zugriff auf die Server dieses Betreibers hat, dann kann er im Prinzip auch alle diese Passwörter einlesen und die gesamten Userdaten. Das sollte eigentlich nicht so sein. Eigentlich sollten Passwörter gehasht gespeichert werden. Das heißt eigentlich, dass die in einer Form gespeichert werden, wie dass sie nicht mehr zu entschlüsseln sind. Aber der Betreiber selbst kann da trotzdem noch prüfen, ob ich das richtige Passwort eingegeben habe oder nicht. Darauf kann man sich aber nicht zwangsläufig verlassen, und deswegen sollte man erst mal davon ausgehen, dass diese ganzen Passwörter dann sichtbar sein könnten, und daher ist es auf jeden Fall sinnvoll, für jede Plattform ein eigenes Passwort zu wählen, weil sonst hat man halt direkt alles verloren. Wenn man jetzt so ein schwieriges Passwort oder ein komplexes Passwort generieren möchte, was sich immer ganz gut empfiehlt, ist, in irgendeiner Weise Sätze mit Abkürzungen zum Beispiel zu verwenden, Sonderzeichen einzubauen und dann halt zu versuchen, sich Eselsbrücken irgendwie einzubauen, sollte dann halt ein relativ langes Passwort ergeben. Wenn man dann noch unterstützt wird von den Passwort-Managern, glaube ich, ist das ganz gut zu managen, und jetzt so wirklich kritische Anwendungen wie Online Banking, der Michel angesprochen hatte, sollte man sowieso möglichst in einem sicheren Umfeld machen, also jetzt möglichst nicht aus einem öffentlichen Netzwerk heraus die Daten kommunizieren. In einem regulärem Fall also, wenn man jetzt in einem Kaffee sitzt und nutzt W-Lan, das ist meistens unverschlüsselt, das heißt, man muss sich darauf verlassen, dass die Passwörter auf einer anderen Ebene verschlüsselt werden. Das sollte im Normalfall der Fall sein. Aber gerade was sowas angeht, ist natürlich Vorsicht besser als Nachsicht, und ein kompromittiertes Passwort ist deutlich mehr Arbeit, als wenn man sich vorher die Mühe macht und ein sicheres Passwort für jede Plattform erstellt.

Michael Münz: Und würde eine Zwei-Faktor-Authentisierung denn dafür sorgen, dass der Worst-Case niemals eintritt, kann ich mich dann zurücklehnen?

Anders Kölligan: Ja, also ich meine, ich möchte jetzt hier keine Panik schüren, aber so 100-prozentig kann ich das nicht bestätigen, aber eine Multifaktorauthentifizierung, also Zwei-Faktor-Authentifizierung macht das ganze so viel sicherer, also so viel deutlich sicherer, dass es sich auf jeden Fall lohnt, die immer einzurichten. Also klar, zweiter Faktor, aber natürlich gibt es da auch Möglichkeiten, dass das zum Problem führen kann, also typischerweise, man verliert in irgendeiner Weise sein Smartphone, was oft als zweiter Faktor genutzt werden kann, oder auch einfach nur die SIM-Karte kommt abhanden oder ähnliches, und dann ist schnell mal dieser zweite Faktor weg. Und wenn dann die Person, die versucht einen zu hacken, dann möglicherweise auch noch an das eigene Passwort kommt, dann kann das natürlich auch schon dazu führen. Aber das ist natürlich deutlich seltener als einfach nur, dass ein einfaches Passwort gehackt wird. Also deswegen ich denke das ist schon unwahrscheinlich, aber auch da muss man es halt nicht unbedingt darauf anlegen.

Ute Lange: Kannst du denn nochmal ganz kurz erklären, was ihr unter zwei Faktor versteht? Also normalerweise habe ich eine E-Mail, die ich eingeben muss, und der zweite Faktor ist dann was, oder kann es sein?

Anders Kölligan: Ja, also, der reguläre Fall ist natürlich, du hast halt irgendwie einen Accountnamen, musst ein Passwort eingeben, dann zählt dieses Passwort dann sozusagen als der erste Faktor, und dann als zweiten Faktor hat man üblicherweise, oder das ist, glaube ich, aktuell wahrscheinlich noch das weiteste verbreitete weitere Verfahren ist, dass man dann halt sich eine SMS zusenden lässt und diese SMS enthält halt einen einmaligen Code der jetzt nur für dieses eine Log-In gültig ist, dass man dann zusätzlich noch eintippt, das ist, ich glaube, das kennen wahrscheinlich alle Zuhörerinnen und Zuhörer zur Genüge. Das macht man halt sehr häufig. Wie gesagt, also, es ist schon deutlich sicherer als nur das Passwort. Da gibt es aber auch noch sicherere Varianten. Also, typischerweise gibt es da halt dann Hardware-Token, also extra dedizierte Geräte, die dann zum Beispiel diese Codes generieren, zum Beispiel oder auch andere Verfahren nutzen. Man kann sich die auch als App runterladen, dann auf sein Smartphone, dass man halt eben nicht auf diesen SMS Transfer angewiesen ist, sondern dass man das lokal auf seinem Smartphone einrichten kann, und das ist auf jeden Fall sehr zu empfehlen. Da gibt es natürlich auch verschiedene Anbieter, die bieten alle ähnliche Produkte an, würde ich sagen. Da bietet sich aber auch natürlich dann an, um nochmal auf diese sicheren Apps zuzugreifen, dass man da halt die typischen bekannten Hersteller von diesen Apps, halt auf die zurückgreift und jetzt nicht irgendein unbekanntes Produkt verwendet, außer man informiert sich vorher ordentlich.

Michael Münz: Jetzt haben wir ja ein bisschen darüber gesprochen, was passieren kann, wenn sich jemand bei mir in meinen Mail Account reinhackt. Utes große Sorge

ist ja, dass sie sich jemand bei ihr in die Social Media Accounts reinhackt. Worauf kann sie sich denn dann einstellen, wenn das passiert ist?

Anders Kölligan: Du meinst jetzt auf die Gefahren?

Michael Münz: Hm ja.

Anders Kölligan: Was ich nicht empfehlen würde, was es auch in den sozialen Medien gibt, ist halt zum Beispiel, da gibt es ja auch dieses Single-Sign-On Prinzip, also dass man sich zum Beispiel dann bei einem Social Media Anbieter eingeloggt hat und sich dann auf einer anderen Webseite einloggen möchte, und der bietet einem dann direkt an, das über den zu machen. Das hat zum einen mal datenschutzrechtliche Bedenken im Hintergrund, aber auch dann ist es natürlich auch so, wenn man dann halt Zugriff auf den Social Media Account hat, dann kommt man auch möglicherweise schon bei einem Shop rein, und dann kann der Hacker im eigenen Namen irgendwie sich Produkte zusenden lassen oder sowas. Abgesehen davon ist es natürlich auch äußerst unangenehm, dass der Hacker oder die Hackerin dann in den privaten Angelegenheiten von einem deutlich rumschnüffeln kann. Also alle privaten Informationen stehen dann ja offen, die können natürlich auch runtergeladen werden. Diese Funktionen gibt es sowieso, und alle diese privaten Informationen könnten dann auch zum Beispiel wieder genutzt werden, um andere zu kompromittieren. Wenn ich dann zum Beispiel sehen kann, hatte ich eben schon mal mit den Passwörtern angesprochen, wann die Kinder zum Beispiel geboren sind, das sind eher so typische Kandidaten, um daraus ein Passwort zu generieren, dann ist auch schnell das Passwort erraten, wenn man denn so etwas als Passwort verwendet hat, und zum anderen ist es dann auch schon wieder in die Richtung, ich weiß nicht, ob wir eben den Fachbegriff genannt haben, das Phishing, also, das heißt, ich gebe mich als eine andere Person aus und versuche diese Person dann halt eben von meiner Agenda zu überzeugen. Also, typischerweise könnte ich dann zum Beispiel, wenn ich jetzt mich als Ute eingeloggt habe und kann dann halt den Michael eine Nachricht schreiben. Dann könnte ich ja sagen, hier, ich habe diesen tollen Shop gefunden, guck dir den doch mal an, hier gibt es dieses und jenes tolle Angebot, und der arme Michael klickt dann auch auf den Link, weil er denkt, ach ja, die Ute die kenne ich ja, die ist vertrauenswürdig und klickt dann blauäugig auf diesen Link. Und vielleicht hat er noch Glück, dass er dann halt wirklich tatsächlich nur auf einen Fakeshop zum Beispiel umgeleitet wird, wo er erstmal überhaupt dann gezwungen wird, sozusagen seine Kreditkartendaten einzugeben oder ähnliches, und vielleicht kommt er dann noch auf die Idee: Moment mal, vielleicht stimmt das gar nicht so, aber eventuell ist das dann halt auch ein Download Link, wo ganz subtil dann automatisch irgendwie eine Software installiert werden kann. Das kann durchaus passieren und das ist auch wieder so eine Gefahr für das ganze Umfeld. Und ja, wie gesagt, also, es ist natürlich auch super unangenehm, alleine jemanden zu haben, der sich selbst in einem Account befinden kann, und auch im nahen Namen überhaupt

Nachrichten zu schreiben oder Sachen zu löschen oder ähnliches, und wenn man dann halt zum Beispiel auch verknüpft ist mit seiner eigenen Firma, mit seiner eigenen Organisation und dann in deren Namen irgendwelche Posts absetzt, das kann natürlich auch sehr gefährlich sein, auch für die berufliche Zukunft sozusagen. Also da gibt es multiple Möglichkeiten, wie das zu einem echten schlimmen Worst-Case werden kann.

Ute Lange: Also, ich bin total überzeugt, dass ich das absolut nicht haben will. Anders brauchst du gar nicht weiter ausmalen, das klingt gruselig. Wie kann ich das denn verhindern? Also wenn wir jetzt speziell über Social Media Accounts sprechen und wenn ich zum Beispiel das Single-Sign-On, wie du das genannt hast, also mit einem Passwort auf mehrere Plattformen des selben Anbieters, das habe ich jetzt schon mitgenommen. Auf gar keinen Fall. Jedes Konto hat ein eigenes Passwort, und das manage ich mit dem Passwort-Manager, wenn ich dir jetzt richtig zugehört habe.

Anders Kölligan: Ja das passt so!

Ute Lange: Passt so. Aber was kann ich denn sonst noch tun, wenn ich mich jetzt auf den Plattformen vielleicht sowieso schon befinde, wenn ich nach der Sendung jetzt dafür sorgen will, dass das alles sicherer wird bei mir? Was kann ich dann tun, und was können auch die, die uns jetzt zuhören, tun?

Anders Kölligan: Ja, also, ich wollte jetzt natürlich keine Angst machen vor diesen Plattformen. Ja, diese Plattformen, die kann man schon durchaus nutzen. Also es ist sicherlich grundsätzlich kein Sicherheitsbedenken, aber es lohnt sich auf jeden Fall. Was mich halt angesprochen hatte, ja, Zwei-Faktor- Authentifizierung. Alle großen Platformen bieten mindestens eine sichere, Zwei-Faktor-Authentifizierung an und bieten noch mehr Möglichkeiten. Ich denke, es ist ganz klar, es lohnt sich, mal zehn Minuten auf die Einstellung zu gehen. Die sind in den Apps verfügbar, die sind in der in der Weboberfläche verfügbar. Da gibt es halt dann meistens so ein Zahnrad, da klickt man drauf, da gibt's Sicherheitseinstellungen, da einfach mal wirklich durchzugucken, wenn man was nicht versteht, dann ist auch kein Problem. Kann man googeln, findet man sehr gute Informationen, unter anderen natürlich vom BSI, aber auch zum Beispiel von den Verbraucherzentralen und im Zweifelsfall gibt es mit Sicherheit jemanden, den man fragen kann: “was bedeutet denn das?”. Das hat eigentlich immer jemand im Umfeld und da einfach mal wirklich mit Vernunft diese Einstellung durchzugehen. Ich denke, das dauert zwischen fünf und zehn Minuten, wenn man das noch nie gemacht hat und wenn man es schon mal gemacht hat, also wenn man den ganzen Drill schon kennt aus einer anderen Plattform, dann wahrscheinlich deutlich weniger. Und diese zehn Minuten, die sind wirklich sinnvoll investierte Zeit, und da kann man halt auch eben diese Zwei-Faktor-Authentifizierung anmachen, und das lohnt sich auf jeden Fall. Da muss man auch keine Angst haben, dass man sich dann jedes mal einloggen muss mit der Zwei-

Faktor-Authentifizierung. Die Betreiber haben dann nämlich auch sinnvolle Möglichkeiten zu erkennen, ob man sich zum Beispiel auf dem Gerät schon mal eingeloggt hat und ob das dann als sicher anerkannt wird oder nicht. Und ich glaube, dadurch kriegt man eigentlich einen ganz guten Kompromiss aus Sicherheit und "ease of use" sage ich mal, also Nutzerfreundlichkeit. Das kriegt man dann schon mal ganz gut hin. Dann würde ich aber grundsätzlich auch sagen, man sollte auch so ein bisschen die Maxime der Datensparsamkeit grundsätzlich befolgen. Ja, also, man sollte auch auf den sozialen Netzwerken gucken, auch mal in die Privatsphäreneinstellungen möglichweise gehen und nochmal gucken, was ist denn da überhaupt für andere einsehbar, weil, wie gesagt also, diese Informationen können im Zweifelsfall auch für Accountkompromittierung genutzt werden. Aber vieles andere, und vielleicht sind da auch wirklich Informationen, die man gar nicht möchte, dass die in der Öffentlichkeit sind, und da gibt es dann meistens verschiedene Einstellungen, dass es zum Beispiel nur Freunde und Bekannte sehen können oder dass es eben ganz sichtbar ist oder auch nur ausgewählte Gruppen. Diese verschiedenen Möglichkeiten gibt es, und ich denke, es lohnt sich, diese Informationen einmal durchzugehen und dann wirklich mal mit Vernunft ranzugehen. Muss ich das wirklich teilen oder eben nicht? Und dann halt möglichst nur das angeben, was man auch wirklich tatsächlich teilen möchte, und nicht mehr?

Michael Münz: Beim Thema Datensparsamkeit fallen mir die ganzen Gewinnspiele ein, für die ich mich dann immer wieder mal anmelde. Das ist doch ungefährlich, oder?

Anders Kölligan: Ja, also, das ist halt auch wieder so ein bisschen das Problem. Zum Teil werden diese Gewinnspiele ja auch von Drittanbietern sozusagen im Auftrag von XY irgendwie engagiert, und da ist dann halt auch wieder die Frage, ja, dann verteilt man seine Informationen über zig Millionen Server im Internet, so viele vielleicht nicht, aber über viele Server. Man weiß, man hat auch selbst nicht mehr den Überblick, wo liegen denn jetzt tatsächlich die Daten vor? Welche Daten werden auch im Hintergrund möglicherweise dann geteilt? Also wenn ein Gewinnspiel dann über eine Social Media Plattform läuft, dann wird ja zumindest wahrscheinlich dann der Name transferiert, möglicherweise die Telefonnummer. Vielleicht muss ich das auch angeben, dann bei der Umfrage, und all diese Informationen, die sind potenzielle Sicherheitslücken, die auch ausgenutzt werden können und die gerade typischerweise in solchen Datenleaks dann halt auch die Herkunft der Daten sind, und da muss man sich halt im klaren darüber sein, und die Gewinnspiele lohnen sich ja am Ende auch für die Anbieter tatsächlich nur dadurch, dass eben diese Daten, diese Daten sind ja auch wertvoll auch für legitime Zwecke, also zum Beispiel für das Anbringen von personifizierter Werbung. Also was ja ein relativ vernünftiger Grund ist, das ist ja kein Hacking Vorfall oder ähnliches, und diese legitimen Zwecke, das macht ja auch Sinn. Aber man muss sich halt im klaren sein, ich bezahle mit diesen Daten für die Möglichkeit, an diesem Gewinnspiel zum Beispiel teilzunehmen.

Ute Lange: Ich würde da gerne, weil du gerade das Wort Hacking nochmal gesagt hast, vielleicht für alle Fälle, die wir jetzt besprochen haben, die Frage stellen, wenn ich gehackt werden sollte und darüber Kenntnis erlange, egal auf welchem Weg, was sind die ersten drei Sachen, die ich aus deiner Sicht am schnellsten sofort tun sollte?

Anders Kölligan: Ja, also ich würde erst mal sagen, also ich sag mal, die nullte Sache ist, überhaupt solche Meldungen ernst zu nehmen. Also ich denke, wenn ich halt aus dem Beispiel eben, also wenn der Michael sagt, hier, du hast mir so einen komischen Link geschickt, Ute, ich bin mir nicht sicher, ob das richtig ist, guck doch bitte mal, ob da irgendwie in deinen sozialen Netzwerken alles in Ordnung ist. Hast du mir das wirklich geschickt? Halt einfach diese Rückfrage auch zu machen, wenn man komische Links von irgendwelchen Leuten kriegt, möglichst über eine andere Plattform, zum Beispiel durch ein Telefonat sicherstellen, hast du mir das wirklich geschickt? Hey Ute hast du mir tatsächlich jetzt diesen Link geschickt oder eben nicht? Und das kann dann halt auch wirklich ein Hinweis sein auf so eine Kompromittierung und die sollte man auf jeden Fall ernst nehmen. Und ich denke, Schritt eins ist, zu versuchen, das, ob man selbst noch Zugriff auf den Account hat, und dann halt das Passwort ändern. Das ist auf jeden Fall das allerwichtigste. Meistens ist es ja, wenn es jetzt nicht gerade unbedingt der e-Mail Account ist, hat man ja noch Zugang zum Account, weil die Änderung eines Passwortes ist üblicherweise nicht ohne weitere Bestätigung möglich. Das heißt, der Hacker hat wahrscheinlich nur die aktuellen Zugangsdaten und kann nur über diese darauf zugreifen, und dann ist halt wirklich Schritt eins: Passwort ändern. Wenn man das Passwort geändert hat, dann wird man scheinlich schon feststellen, es kommen keine weiteren Nachrichten mehr, dann hat man zumindest erstmal schon mal die Gefahr gebannt und kann dann natürlich gucken, welche Probleme sind dann überhaupt aufgetreten, welchen Schaden habe ich möglicherweise verursacht? Dann kann man auf jeden Fall dann eben die anderen informieren, also zum Beispiel die Kontakte informieren, dass der Account gehackt war, und versuchen halt, den Schaden möglichst rückgängig zu machen, wenn das dann noch möglich ist. Aber im Zweifelsfall, das kann ja auch tatsächlich sein, dass man keinen Zugriff mehr zum Account hat, und in dem Fall sollte man auf jeden Fall versuchen, als erstes die Plattformbetreiber zu informieren. Die haben alle für solche Fälle Hotlines oder auch e-Mail Adressen, wo einem schnell geholfen wird, und das erste, was die natürlich dann machen, ist, den Account sperren, und das ist halt im Prinzip effektiv ja genau das gleiche. Ich möchte erst mal verhindern, dass weiter der Zugriff auf diesen Account besteht, und das ist halt, wie gesagt, das allerwichtigste, und deswegen also, um noch mal die drei Sachen zusammenzufassen, ja erstmal versuchen, das Passwort zu ändern. Wenn das nicht geht, dann würde ich mich beim Betreiber melden, dass die den Account sperren können, und dann halt wirklich zu gucken, was ist denn möglicherweise passiert, und eventuell daraus dann auch noch weitere Konsequenzen zu ziehen. Also, wenn man dann wieder Zugriff auf seinen Account

hat, Zwei-Faktor-Authentifizieurng anmachen, die Sicherheitseinstellungen überprüfen und so weiter. Das ist dann auf jeden Fall natürlich das wichtigste. Jetzt sind wahrscheinlich vier bis fünf Punkte, je nachdem, wie man gezählt hat. Aber ich denke, das wichtigste ist, erstmal zu verhindern, dass weiter Accountzugriff besteht für die Person, die man raus haben will aus einem Account.

Michael Münz: Okay, ich würde gerne noch einen Punkt ansprechen, der immer so ein bisschen mitgeschwungen ist, die ganze Zeit auch gerade beim Thema Zwei-Faktor-Authentifizierung oder Zwei-Faktor-Authentisierung. Da müssen wir uns auch noch mal irgendwann mal einigen, welche Verwendung wir da eigentlich nutzen wollen. Aber da kommt ein Code aufs Handy, und du hattest vorhin irgendwann mal erwähnt, das Handy ist dann, man hat vielleicht mal das Handy auch verloren, und dann ist es weg, und ich stelle dann vor, jemand anderes hat es in der Hand. Was also, wenn jemand dieses Gerät von mir in die Finger bekommen würde, welches sind denn die Szenarien, die dir aus deiner BSI und Experten Sicht dann am meisten sorgen machen würden?

Anders Kölligan: Typischerweise. Ein größeres Problem wäre ja natürlich, man braucht ja eigentlich, normalerweise muss man ja zumindest noch einen PIN oder halt so eine Mustererkennung noch haben, um auf das Smartphone dann Zugriff zu haben. Deswegen, da ist halt auch wieder typischerweise der Appell, also gerade diese Muster, die sind typischerweise eher unsicher. Das kann ganz leicht mal jemand übersehen, wie das funktioniert, wie das Muster aussieht, auch die PIN. Man kann kaum umher, selbst wenn man es nur aus dem Augenwinkel sieht. Eine vierstellige PIN kann man sich ohne weiteres, weil gerade so merken. Und wenn man da noch zusätzlich dass Smartphone hat, hat man im Prinzip das gesamte digitale Leben der betreffenden Person in seinen Händen. Das ist natürlich das größte Problem. Ältere Smartphones, das ist bei den typischerweise. Ich hoffe, dass ich jetzt hier nicht Unsinn erzähle, aber ich glaube, mittlerweile ist es standard, dass Smartphones verschlüsselt sind. Das heißt, typischerweise sollte jemand von außen, wenn er eben diesen Zugang nicht mehr hat ohne die Ausnutzung weiterer Schwachstellen sollte er nicht mehr auf die Daten auf dem Smartphone zugreifen können. Ich hoffe, dass das auch weiter so ist, aber das kann bei älteren Geräten eben noch nicht der Fall sein, dass die verschlüsselt sind. Bei den Geräten gibt es dann auf jeden Fall in den Einstellungen die Möglichkeit, die zu verschlüsseln, außer die sind extrem alt, das glaube ich aber nicht, dass die noch häufig vorkommen. Also, da könnte man auch nochmal den Appell liefern. Guckt noch mal in die Sicherheitseinstellung der Smartphones, überprüft nochmal, dass ihr möglichst, wenn ihr solche PINs verwendet, also mindestens sechs bis acht Zeichen eintippt. Aber sicherer sind auf jeden Fall die anderen Möglichkeiten, auf das Handy zu entsperren, also zum Beispiel der Fingerabdruck oder die Gesichtererkennung. Die ist auch aktuell sehr sicher. Das bieten eigentlich alle aktuelleren Smartphones an, und das würde ich auf jeden Fall empfehlen, das als sichere Methode zu haben, das Smartphone zu entsperren. Ja, und

sonst als Worst-Case. Ich meine typischerweise, wenn man das Smartphone entriegeln kann. Man hat Zugriff auf alle e-Mails, typischerweise, man hat möglicherweise auch noch Zugriff auf die Authentifizierungsapp. Wenn die dann da drauf sind, auf die SMS, auf jeden Fall. Die Authentifizierungsapp sind typischerweise noch mal mit einer PIN oder so gesichert. Kann natürlich sein, dass es dann auch die gleiche ist wie vom Smartphone. Kann man auch in den Einstellungen dann überprüfen, ob man die vielleicht nochmal separat haben möchte? Dann hat man noch eine Ebene an Sicherheit darüber. Aber alleine der Zugriff auf die e-Mails und auf die SMS, wie vorher schon angesprochen, ermöglicht einem Halt wirklich den Zugang zu so vielen Accounts, und das ist natürlich beliebig gefährlich. Und gerade auch die Social Media Apps, die werden ja nicht nochmal entsperrt, also die kann man dann ja auch einfach aufrufen. Wenn man Zugang zum Handy hat, dann kann man halt, wie gesagt, allen möglichen Schabernack treiben und kann halt Links posten, kann im eigenen Namen sprechen. Es gibt beliebig viele Möglichkeiten, das dann halt zu nutzen, und deshalb, wie gesagt, auch da Sicherheitseinstellungen überprüfen und möglichst sichere Passwörter verwenden oder beziehungsweise jetzt in dem Fall.

Ute Lunge: Hm anders, wir haben ja gesagt anfangs, dass wir heute mal die Perspektive wechseln und die Worst-Cases so ein bisschen besprechen. Aber natürlich, um folgendes zu erreichen: das wir alle nach dieser Folge noch mal checken, ob wir deine Tipps auch beherzigen. Sicherlich werden wir noch einige Sachen in den Shownotes verlinken. Das BSI hat da eine ganze Menge Informationen, und du hast ja auch die Verbraucherzentralen erwähnt, was für mich jetzt ganz klar geworden ist: Vorsicht ist besser als Nachsicht. Das ist ja so eine sehr plakative Aussage, aber du hast ja schon beschrieben, bestimmte Einstellung nochmal überprüfen, nochmal gucken, ist weniger Zeit, als wenn tatsächlich was passiert ist, weil das kann ja den ganzen Rattenschwanz, oder du hast auch Schneeballsystem gesagt, nach sich ziehen, was sicherlich viel, viel mehr Zeit in Anspruch nimmt. Du hast uns heute ganz, ganz viel Zeit geschenkt. Aber eine Frage möchte ich doch noch ganz kurz stellen, bevor wir zum Abschluss kommen. Unser Name, der Podcast Name ist ja Programm Update Verfügbar. Was kann mir denn schon passieren, wenn ich das mal nicht mache? Michael ist ja so ein Kandidat. Vielleicht magst du da gerade reinspringen, Michael, dass du dir dreimal überlegst, ob du ein Update sofort installierst. Weil was war letztens? Du wolltest dir ein Fahrrad leihen, und dann wusstest du dein Passwort nicht mehr oder so.

Michael Münz: Genau. Da war die App aktualisiert, und ich musste mich neu einloggen, hatte dann aber auf den Bürgersteig vor dem Fahrradstehen, halt nicht das richtige Passwort dabei und musste dann zu Fuß gehen. So. Deswegen sammel ich gerne so Updates, mache die dann bei mir zu Hause auf einmal. Also wenn ich jetzt beim Telefon bleibe, macht die dann 80 Stück auf einmal, und die Apps, die ich am meisten benutze, gehe ich dann schnell noch einmal durch, um zu gucken, dass,

wenn ich sie dann wirklich brauche, ich dann nicht noch irgendwie großes Passwort rauskramen muss. Wenn ich jemanden per Pay-Pal schnell was überweisen würde oder so, ist es was anderes, wo du jetzt schon denkst, oh mein Gott, und so einer moderiert den Podcast hier?

Anders Kölligan: Nein, also ich meine, man kann sicherlich nicht jede App die ganze Zeit und immer sofort innerhalb von zehn Sekunden irgendwie aktualisieren. Das ist im Normalfall ja auch gar nicht unbedingt notwendig. Aber auch da gibt es natürlich die Einschränkung. Es gibt sogenannte "zero day exploits", also vorher unbekannte Schwachstellen, die ausgenutzt werden, und oft kommt dann halt von den Herstellern sehr schnell auch ein Update, wenn die relativ kritisch sind, also typischerweise dann natürlich auf den Betriebssystemen, also zum Beispiel beim PC, und die sollte man also gerade die Sicherheits-Updates, die sollte man möglichst bald einspielen, das ist schon sehr wichtig. Wenn man jetzt aber kein High-Profile Target, sage ich mal, ist, dann glaube ich, reicht es auch, wenn man das nach ein Paar Tagen mal macht. Aber grundsätzlich kann man natürlich auch einfach automatische Updates einschalten, und das würde ich halt auch empfehlen, und nomalerweise sind dann halt auch die Apps aktuell und in einem vernünftigen Zeitrahmen aktuell. Aber es ist trotzdem also, das muss natürlich jeder selbst entscheiden, wie sicher er sein will. Man muss ja am Ende dann doch immer ein Kompromiss finden aus Sicherheit und eben der Benutzerfreundlichkeit, und die Updates immer sofort einzuspielen und dann zu warten, bis alle das durchgelaufen sind, ist natürlich Benutzer eher unfreundlich. Aber man sollte schon versuchen, gerade die Betriebssysteme sicher zu halten, also upgedatet zu halten. Man muss aber nicht jede App sofort, wenn Update ist, aktualisieren und sonst nicht mehr verwenden. Das funktioniert ja meistens auch noch. Und auch hier muss man halt sagen, die Hersteller sowohl von den Systemen als auch von den Apps, die sind angehalten, dass die Updates häufig genug kommen, aber auch, dass, wenn jetzt ein Update kritisch ist, also wenn das, wenn dieses Update wirklich notwendig ist, um diese App zu benutzen, das ist typischerweise halt zum Beispiel bei der Banking-App notwendig, dass dann auch die alten Versionen der App eben nicht mehr funktionieren. Also, das kann zum Teil halt auch notwendig sein, und das ist natürlich auch eine Sicherheitseinstellung, und dann muss man halt die App aktualisieren, wenn das, wenn dann halt der Zugriff nicht mehr möglich ist, und das ist dann auch vernünftig so.

Ute Lang: Sehr schön, vielen, vielen dank. Ich glaube, wir hätten noch ein paar fragen, aber wir wollen es ja auch überschaubar halten, dass die vielen Tipps auch nachvollziehbar sind. Wie gesagt, ich werde jetzt nach der Aufnahme gleich nochmal bei mir einiges überprüfen in der Hoffnung, dass ich es so eingestellt habe, wie du es schon empfohlen hast. Wir werden, liebe Hörerinnen und Hörer da draußen, in den kommenden Folgen weitere von euren Fragen aufgreifen, so wie wir es heute schon getan haben. Wenn ihr auch eine stellen möchtet, dann schreibt uns doch,

kontaktiert uns gerne über die BSI-Kanäle auf Facebook, Instagram, Twitter sowie YouTube oder Michael, es geht auch per e-Mail.

Michael Münz: Genau über die e Mail Adresse Podcast@BSI.Bund.de. Anders vielen Dank, dass du dabei warst für die vielen Tipps. Ich nehme für mich mit das Ute, wenn ich demnächst von dir für deinen anstehenden Geburtstag irgendwelche Links zugeschickt bekomme, ich auf jeden Fall noch mal frage, ob die auch wirklich authentisch sind. Nicht, dass ich dann irgendwo falsch lande bei irgendeinem Fakeshop oder so. Das hat mich gerade tatsächlich auch nochmal aufgerüttelt. Vielen dank Anders für die vielen Tipps, die heute dabei waren.

Anders Kölligan: Ja, ich danke euch fürs Zuhören und natürlich allen Zuhörerinnen und Zuhörern.

Michael Münz: Und an die gerichtet noch eine bitte. Wir haben noch eine Umfrage laufen, wie euch Update Verfügbar gefällt. Den Link dazu haben wir euch in die Shownotes ausgepackt. Also nutzt das und sagt uns in erster Linie erstmal natürlich, dass ihr uns super findet, aber dann auch gerne, an welchen stellen wir uns noch ändern, verbessern oder mehr in eure Interessen ausrichten sollen. Da sind wir sehr gespannt. Vielen dank fürs Mitmachen schon mal.

Ute Lang: Ja, und wir hören uns dann nächsten Monat wieder bis dahin liket und folgt Update Verfügbar auf euren Podcast Plattformen, denn so verpasst ihr keine von unseren Folgen und könnte auch noch ältere, vielleicht die mit Anders im vorletzten Sommer nochmal nachhören, bis die neue Folge draußen ist. Tschüß!

Michael Münz: Bis das neue Update da ist, wolltest du sagen,

Ute Lang: Genau

Michael Münz: Genau gut, bis dann, tschüß!

Besuchen Sie uns auch auf:

https://www.bsi.bund.de/
https://www.facebook.com/bsi.fuer.buerge r
https://twitter.com/BSI_Bund
https://www.instagram.com/bsi_bund/
https://social.bund.de/@bsi

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