„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 42, 30.04.2024

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

Ute Lange: Ihr seid bei Update verfügbar gelandet, dem Podcast für Sicherheit im digitalen Alltag, und ich bin Ute Lange..

Michael Münz: Mein Name ist Michael Münz, und in dieser Folge verraten wir euch, wie ihr eure Daten und Geräte künftig noch besser vor Schadsoftware schützen könnt. Die Erkenntnis oder die Eingebung zu dieser Folge haben wir eigentlich der Deutschen Bahn zu verdanken.

Ute Lange: Das musst du jetzt mal erläutern, das verstehe ich nicht. Wie sollen es die Hörer und Hörerinnen verstehen? Hast du ein Erlebnis gehabt oder beim Bahnfahren aus dem Fenster geschaut, und eine Eingebung hat dich übermannt?

Michael Münz: Ich stand kürzlich am Hauptbahnhof vor dem großen Display, und es war kaputt. Also ich konnte nicht sehen, wann und wo mein Zug fährt, und das hat mich an einen Vorfall vor ein paar Jahren erinnert. Da war Schadsoftware schuld. Es gab einen Virus, WannaCry, der in kürzester Zeit in ganz vielen Ländern unzählige Systeme lahmgelegt hat, und die Bahn war damals auch betroffen, sodass ihre Displays damals nicht funktionierten und die Fahrgastinformationen nicht anzeigten. Seitdem denke ich immer, wenn ich so kaputte Displays sehe: „Da steckt doch mehr dahinter, darüber will ich mehr erfahren.“ Deswegen sprechen wir jetzt über Schadsoftware.

Ute Lange: Finde ich eine gute Idee, vor allen Dingen, weil ja Menschen da draußen, die uns jetzt zuhören, auch schon andere Sachen erlebt haben: Laufwerke, die auf- und zugehen, ohne dass man irgendwas gemacht hat. Daten, die vor den eigenen Augen verschwinden. Oder komische E-Mails, die einen erreichen und wo man nicht so genau weiß, wie hängt das alles zusammen mit dem, was ich jetzt hier gerade mache? Ich finde das ein gutes Thema, ich freue ich mich darauf!

Michael Münz: Wir haben uns eine Expertin vom BSI eingeladen, die, dafür sind wir sehr dankbar, heute auf ihr Mittagessen verzichtet hat und stattdessen mit uns ihre Tipps und Hinweise teilt, wie wir unsere Geräte und Daten künftig besser vor Schadsoftware schützen können. Wir freuen uns sehr, dass sie da ist, Letitia Kernschmidt.

Letitia Kernschmidt: Hallo, schön, dass ich da sein darf.

Ute Lange: Wir freuen uns, dass du dir die Zeit nimmst, und hoffen, dass wir dich nicht allzu hungrig werden lassen. Wir sind hungrig nach Informationen. Sag doch mal kurz, was du im BSI machst, und wie häufig du in deinem beruflichen Alltag mit Schadprogrammen zu tun hast.

Letitia Kernschmidt: Ja, im BSI bin ich im Referat für die Vorfallsbearbeitung und die Verbindungsstelle zum Nationalen Cyber-Abwehrzentrum. Wir haben also bei uns tatsächlich die Vorfallsbearbeitung, wenn etwas passiert ist, zum Beispiel ein Befall mit Schadsoftware bei wichtigen Institutionen, und tatsächlich gehört das bei uns zum Berufsalltag. Schadsoftware ist allgegenwärtig in meinem Job.

Michael Münz: Dann dürfte es dir leichtfallen, mir erst mal auf die Sprünge zu helfen, was es mit diesen ganzen Begriffen auf sich hat: „Schadsoftware, Virus, Trojaner, Wurm - also bei mir geht da schon viel durcheinander. Ich vermute mal, Schadsoftware ist der Oberbegriff, und darunter gibt es dann mehrere Varianten?

Letitia Kernschmidt: Genau, als Synonym verwenden wir erstmal die Begriffe Schadsoftware, Schadprogramme und Malware. Das ist erstmal der ganze Oberbegriff für alles, jede Art von Software, die irgendetwas tut, was man nicht will, sage ich jetzt mal laienhaft gesprochen. Du hast auch schon WannaCry angesprochen, das ist tatsächlich ein super Beispiel, weil man daran ganz viele verschiedene Dinge erklären kann. WannaCry war in erster Linie eine Ransomware. Das bedeutet, eine Schadsoftware, die auf dem Gerät, das betroffen ist, alle Dateien verschlüsselt und dann in der Regel von den Betroffenen ein Lösegeld fordert. Das ist auch nach wie vor immer noch eine der größten Gefahren im Internet, oder, ich sage mal, eine Art von Schadsoftware, die momentan überall kursiert. Also WannaCry ist aus dem Jahr 2017, aber es ist immer noch tagesaktuell, wenn man über Ransomware spricht.

Gleichzeitig ist die Frage: Wie kommt jetzt die Ransomware irgendwo drauf? Du hast gerade schon den Begriff Virus genannt. Das ist tatsächlich die häufigste Variante. Das bedeutet zum Beispiel: über einen E-Mail-Anhang, oder man klickt auf einen Link, der auf eine maliziöse Webseite führt, wo das runtergeladen wird. Es gibt verschiedenste Wege.

Aber es gibt auch sowas wie einen Wurm. Das hat man vielleicht auch schon mal gehört. Das war bei WannaCry eine Besonderheit, dass er sich wurmartige ausbreiten konnte, damals über das SMB-Protokoll, über eine Schwachstelle, und das heißt, dass die Nutzer und Nutzerinnen da gar nicht aktiv was tun mussten. Sondern das ist eben das Besondere an einer wurmartigen Schadsoftware, dass die sich selber in Netzwerken ausbreiten kann, und das macht sie natürlich nochmal um einiges gefährlicher.

Ute Lange: Das sind jetzt schon verschiedene Kategorien von Schadprogrammen oder Schadsoftware. Vielleicht gehen wir dann mal in die Einzelnen rein. Was beabsichtigen sie oder verursachen sie? Das hat bestimmte Hintergründe, warum es verschiedene Zugänge gibt, um dann am Ende uns Schaden zuzufügen.

Letitia Kernschmidt: Genau, also eins haben wir schon angesprochen: Ransomware ist momentan immer noch das schlimmste Übel. Es gibt aber zum Beispiel auch Schadsoftware, die darauf aus ist, Daten auszuspionieren, zum Beispiel sogenannte Keylogger, die alles mitprotokollieren, was man eintippt. Damit können zum Beispiel Zugangsdaten abgegriffen werden, auch alle anderen möglichen persönlichen Daten. Also einfach Datenraub ist dann

das Ziel. Es gibt aber auch Schadsoftware, die bestimmte Werbung ausspielt, dann immer, wenn man seinen PC hochfährt, ploppt überall Werbung auf. Auch das ist eine Variante.

Ihr hattet schon mal über Smart-Home-Geräte gesprochen und über Botnetze da drin, dass man das Gerät in irgendeiner Weise fernsteuern möchte, um dann damit andere Sachen auszuschalten, beispielsweise über sogenannte DDoS-Attacken. Man könnte auch Krypto-Malware draufhaben, oder Bitcoin-Mining über kompromittierte Geräte betreiben. Es gibt verschiedenste Szenarien, wofür das ausgenutzt werden kann.

Michael Münz: Und wenn ich dich gerade richtig verstanden habe, kriege ich das manchmal mit, also dann sehe ich entweder Werbung oder meine Daten sind verschlüsselt, aber es gibt auch Anwendungen, die ich gar nicht mitbekomme. Keylogger ist so ein bisschen der Höhepunkt meiner Paranoia, muss ich sagen. Aber es kann noch sein, dass mein Gerät Teil eines Botnetzes ist, ohne dass ich das mitbekomme, oder dass da Bitcoins geschürft werden, ohne dass ich das richtig mitkriege?

Letitia Kernschmidt: Genau. Ransomware oder Werbung. Werbung ploppt auf, die ist sichtbar, mit dem Rechner geht nichts mehr. Schadsoftware, die im Hintergrund läuft, kann durchaus erst mal eine Weile unbemerkt laufen, gerade wenn das vielleicht auch Smart-Home-Geräte betrifft, die jetzt nicht alle unbedingt Displays haben oder etwas anzeigen, wo das auffallen würde. Bei Krypto-Malware würde es auffallen, wenn das Gerät plötzlich immer sehr heiß ist und immer auf Volllast läuft, dann könnte einem auffallen, dass irgendwas mit diesem Gerät nicht stimmt. Aber ja, es kann auch gut versteckt laufen.

Ute Münz: Du hast ja gerade schon angesprochen, dass es unterschiedliche Geräte sein können, die befallen werden oder die angegriffen werden. Was betrifft es denn alles? Also, wir denken in erster Linie jetzt mal ans Internet, weil ich mir irgendwo über einen Anhang was reinziehe. Aber wir hatten auch mal eine Folge mit den White Hat Hackern (Update verfügbar Folge 21). Die haben zum Beispiel um Menschen in Firmen, wo sie tätig waren, zu testen, USB-Sticks auf Parkplätzen liegen lassen und haben sie damit animiert, sie in ihren Rechner zu stecken. Da war Zeug drauf, dass offensichtlich eher schädlich als nützlich war.

Letitia Kernschmidt: Genau also grundsätzlich könnte man jetzt erst mal sagen, dass Schadsoftware auf jedem Gerät laufen kann, auf dem Software im Allgemeinen läuft, egal ob dieses Gerät jetzt am Internet hängt oder nicht. Die Frage ist natürlich: Wie kommt es drauf? Und die nächste Frage: Wozu? Also ich kann über einen USB-Stick Schadsoftware auf ein Gerät bringen, was nicht am Internet hängt. Die Frage ist dann: Was habe ich davon? Also entweder muss der USB-Stick danach wieder an ein internetfähiges Gerät gehängt werden, sonst habe ich als Angreifer aus der Ferne ja nichts davon und komme nicht an die Daten ran. Oder ich muss physisch mir den hinterher wieder klauen. Deswegen würde ich sagen, das ist jetzt eher das seltenere Szenario, aber nicht unmöglich, dass das passiert. Deswegen grundsätzlich: Erstmal jedes Gerät, was Software kann, kann auch Schadsoftware.

Michael Münz: Jetzt kann ich mich natürlich zurücklehnen und denken, ja, die Daten auf meinem Rechner, die sind ja jetzt auch nicht so spannend. Was soll mir schon passieren? Was sagst du so Leuten, die so eher unbedarft und so ein bisschen entspannt mit ihren Daten umgehen? Wie groß ist denn die Gefahr für jeden Einzelnen von uns?

Letitia Kernschmidt: Also grundsätzlich kann das erst mal jeden und jede treffen. Es gibt Schadsoftware, die auch für die ganz breite Masse ausgelegt ist. Die haben jetzt kein spezifisches Ziel vor Augen, die Angreifer dahinter, die wollen erst mal möglichst viele erreichen und kompromittieren, und man muss immer so ein bisschen überlegen. Was heißt das: Ich habe nichts zu verbergen? Klar, das ist mal schnell dahingesagt, dieser Satz. Aber ich glaube, jeder kennt den emotionalen Wert. Stell dir vor, alle deine Babyfotos sind weg. Klar, die sind in unserer Generation vielleicht noch alle ausgedruckt, aber jetzt sind Fotos alle nur noch digital. Stell dir vor, alle Fotos sind weg. Was das emotional für uns bedeutet. Oder die Hochzeitsbilder, da hängt man dran. Oder in Richtung Online-Banking gedacht. Ich habe vielleicht nichts zu verbergen, aber ich habe vielleicht trotzdem Geld, und ich weiß nicht, wie du das findest, wenn plötzlich jemand deine Konten komplett leerräumt. Vielleicht hast du in dem Sinne nichts zu verbergen, aber durchaus zu verlieren. So könnte man das vielleicht umformulieren.

Michael Münz: Wenn jemand anderes als ich das Konto leerräumt …!

Letitia Kernschmidt: Richtig, richtig!

Michael Münz: Gibt es denn auch gezielte Angriffe? Also sagen wir mal, es gibt die breite Masse und machen sich dann auch Hacker die Mühe, gezielt Leute anzupeilen? Und was wären das dann für Menschen oder auch Menschengruppen, die sich besonders Gedanken machen müssten?

Letitia Kernschmidt: Genau, man kann das echt ganz gut unterteilen. Also, es gibt zum einen diese wirklich massenhaft verschickte Schadsoftware, die man jetzt kennt, die in Spammails drin ist, die in Phishingmails drin ist, in E-Mails mit maliziösen Anhängen. Die gehen an die riesenbreite Masse raus, und die haben auch kein konkretes Ziel. Dann gibt es – ein bisschen abgewandelt davon – Angreifer, die machen das auch erst mal so, und dann gucken sie sich an: Wo bin ich ihnen eigentlich überall gelandet? Wo habe ich es überall geschafft zu kompromittieren? Die picken sich dann ihre Betroffenen raus, beispielsweise, um deren Daten zu verschlüsseln und richtig hohes Lösegeld zu verlangen. Dann gucken sie, ob da ein richtig großes deutsches Unternehmen drin ist. Das schnappen sie sich und lassen die anderen erst mal links liegen.

Da sind meistens Kriminelle dahinter mit einem finanziellen Interesse. Dann gibt es aber auch Angriffe, die wirklich ganz gezielt ausgeführt werden. Die haben dann einen nachrichtendienstlichen Hintergrund, meistens von fremden Mächten, die suchen sich schon wirklich sehr gezielt ein Opfer raus. Also, natürlich ist es dann ein Betroffener mit irgendeinem hohen Wert für die. Also sei es jetzt, um Wirtschaftsspionage zu betreiben, sei es auf staatlicher Ebene, um Staatsgeheimnisse zu erbeuten, in die Richtung gedacht. Und die gehen dann wirklich ganz gezielt vor, um zu versuchen, diesen einen Betroffenen zu infizieren. Das sind dann aber in der Regel eben nicht du und ich, sondern das sind dann offizielle Persönlichkeiten.

Michael Münz: In seinem jüngsten Lagebericht geht das BSI von rund einer Viertelmillion neuer Schadprogrammvarianten aus, und das an jedem Tag.

Ute Lange: Reden wir über Menschen wie Du und ich. Das andere sind vielleicht auch andere Behörden, die sich dann noch intensiver damit beschäftigen. Ich habe jetzt so eine

Antiviren-Software. Wir hatten vorhin schon das Wort Virus. Dann bin ich doch eigentlich safe, oder? Oder muss ich trotzdem ständig aufmerksam sein, dass mir nichts passiert?

Letitia Kernschmidt: Ja, also, ich hoffe, du bist immer aufmerksam, denn es ist gut, wenn man eine Antivirensoftware draufhat. Wichtig ist auch, dass die wirklich up to date ist. Wenn man so eine Freeware-Testversion nutzt, da wird nicht immer alles aktuell eingespielt. Und das andere ist auch, dass sie eine trügerische Sicherheit geben, so wie du gerade gesagt hast. Ich habe das doch jetzt, jetzt muss ich nicht mehr aufpassen. Jetzt kann ich mein Hirn abgeben und alles machen, die rettet mich schon. Das wäre schlecht. Also es ist so, die Antivirensoftware kann dich nur vor dem schützen, was die Antivirensoftware auch kennt, und es kommen jeden Tag neue Varianten dazu. Es kommen auch ständig neue Arten und Formen von Schadsoftware dazu, und wenn da jetzt etwas dazukommt, was die Antivirensoftware oder die Firma, die hinter der Antiviren-Software sitzt, auch noch nicht kennt, dann ist das natürlich da auch nicht drin. Wenn die nicht up to date ist, dann hat die das auch nicht drin, und dann wird die das auch nicht erkennen, und insofern sollte man sich nicht darauf verlassen. Es ist eine Komponente, aber sicher nicht vollständig.

Michael Münz: Und wenn ich dann merke, ich bin betroffen, wie gehe ich dann vor? Nehmen wir eines der schlimmeren Beispiele, da steht dann: „Hallo Michael, wir haben deine Daten verschlüsselt, gibt uns Geld, und dann kriegst du sie zurück.“ Was mache ich denn dann?

Letitia Kernschmidt: Genau, das kann passieren, denn absolute Sicherheit gibt es nicht, das Kind ist in den Brunnen gefallen. Jetzt predigen wir Schritt eins: Ruhe bewahren. Ich hoffe, du hast alle unsere BSI-Tipps, die es so gibt, befolgt und kannst jetzt im Zweifelsfall einfach deine externe Festplatte mit einer Datensicherung, die nicht alt ist, herausziehen. Damit könntest du dein ganzes System wieder retten. Und natürlich, weil du ja vorbildlich bist, würdest du das Ganze auch noch zur Anzeige bringen, damit die Kollegen und Kolleginnen der Strafverfolgungsbehörden dem auch nachgehen können. Du willst schnell deine Daten und deine Systeme wieder haben. Ich empfehle ein Offline-Back-up, Offline-Back-up, Offline-Back-up, das ist die wichtigste Möglichkeit, denn dann könntest du im Zweifelsfall dein Gerät plattmachen, neu aufspielen, und alles ist wieder gut.

Michael Münz: Okay, ich habe da mal noch eine Nachfrage.

Ute Lange: Du fragst für einen Freund?

Michael Münz: Ja, also na ja. Ich habe auch Cloud-Systeme. Ich habe Abos oder bezahle monatlich bei verschiedenen Anbietern, dass ich dort Sachen parke. Wie sicher sind denn die Cloud-Systeme? Also meine Fotos werden zum Beispiel bei dem einen Anbieter hochgeladen, und andere Daten lade ich hier hoch. Also, da habe ich das Portfolio schon ein bisschen gestreut. Aber angenommen, mein Rechner wäre verschlüsselt, könnte ich denn dann von einem anderen Gerät immer noch auf die Daten in der Cloud zugreifen?

Letitia Kernschmidt: Also grundsätzlich, wenn die Angreifer es nicht geschafft haben, Zugriff auf deine Cloud zu bekommen, dann ja. Wenn aber alle Zugangsdaten für die Cloud auf deinem Rechner hinterlegt waren und die Angreifenden sie erbeuten konnten, dann können die natürlich auch auf dahinter hängende Systeme zugreifen. Dann ist es auch egal, ob das dann ein Cloud-Account war oder ob das eine externe Festplatte ist, wo du immer dein Back-up machen wolltest, die aber immer noch am Gerät hängt. Also, das ist immer die Frage.

Haben die eine Möglichkeit, da drauf zu kommen? Wenn ja, dann ist wahrscheinlich dort auch alles weg, entweder gelöscht, leergeräumt, verschlüsselt. Oder sie hatten nicht die Zugangsdaten. Dass sie von extern noch auf deine Cloud gekommen sind, anders als auf diesem Weg, da sind deine Daten schon eher sicherer. Aber gerade, wenn man das jetzt mit einem automatischen Upload hat, und alle Zugangsdaten sind hinterlegt, dann kommen die natürlich auf den Weg drauf.

Ute Lange: Also okay, das ist wieder dieser gesunde Menschenverstand: „Vorsicht ist besser als Nachsicht." Nicht das Gehirn abschalten, sondern regelmäßig Updaten und vielleicht auch nicht auf jede Mail, die man so bekommt, eingehen und antworten, weil es könnte ja irgendwas hinten dranhängen, was einem Dinge auf den Rechner zieht oder in das System zieht, die man nicht so gerne da haben möchte. Das finde ich schon mal eine wichtige Info, nicht nur für uns, sondern auch für die, die uns jetzt zuhören. Aber du hattest ja auch erwähnt, das war unter dem Stichwort Botnetze, dass es Sachen gibt, wo ich gar nicht so genau mitbekomme, dass ich beteiligt bin, weil das auf eine andere Art und Weise auf meinen Rechner gelangt, beziehungsweise, wenn es dort ist, anders verwendet wird. Wie kann ich denn da, „Vorsicht ist besser als Nachsicht" praktizieren?

Letitia Kernschmidt: Genau also, da kann man jetzt auch wieder ein bisschen unterscheiden. Ich nehme noch mal Michaels Beispiel vom Anfang mit WannaCry. WannaCry hat sich über die EternalBlue-Schwachstelle verbreitet, und diese Schwachstelle war auch schon bekannt, und es gab auch Updates und Patches von Microsoft dafür. Das Problem ist nur, die Leute haben diese Patches nicht eingespielt, und deswegen waren die Systeme nach wie vor verwundbar, und deswegen konnte sich das WannaCry wahnsinnig weit verbreiten.

Und das ist eigentlich auch genau der Punkt. Wenn die Schwachstellen bekannt sind und es dafür auch Patches und Lösungsmöglichkeiten gibt, dann ist wirklich die Devise immer: updaten, updaten, updaten. Aber ich habe ja auch gesagt, es gibt nicht die absolute Sicherheit. Es könnte jetzt auch eine Zero-Day-Schwachstelle sein, das heißt, die ist nur dem Angreifer bekannt und dem Rest der Welt nicht. Dann helfen natürlich nur die ganzen Präventions- und Detektionsmaßnahmen, die ich eingerichtet habe, denn dann könnte es immer passieren, dass die ausgenutzt wird, selbst wenn mein System eigentlich auf dem aktuellsten Stand ist. Und dann ist es wichtig, dass man weiß, wie detektiere ich das, was jetzt kompromittiert ist, und was mache ich, wenn ich es entdecke?

Ute Lange: Genau das wäre jetzt die nächste Frage. Also wie kann ich denn, wenn ich komische Dinge auf meinem Rechner beobachte, reagieren? Du hattest schon gesagt, vielleicht wird er sehr heiß, nicht alle haben heute noch CD-ROM-Laufwerke, aber wenn da eins immer rein und raus kommt oder ich plötzlich E-Mails bekomme? Das ist mir tatsächlich letzte Woche passiert. Der Absender ist mir bekannt, es ist eine Freundin von mir, aber da war so kryptisches Zeug drin, und als Moderatorin dieses Podcast habe ich natürlich erst mal gelöscht, und es war auch nachher, als ich bei ihr nachgefragt habe, nicht von ihr. Aber was gibt es da für Vorgehensweisen, die hilfreich sind?

Letitia Kernschmidt: Gerade wenn es jetzt auf deinem eigenen Laptop ist und passiert. Also in deinem Fall müsste ja deine Freundin ran. Aber gehen wir mal von dir selbst aus. Du merkst bei dir seltsames Verhalten, dann kannst du als Privatperson erst mal gucken, ist meine Antiviren-Software auf dem aktuellen Stand? Hat die schon alle aktuellen Updates gezogen, dann kann man erst mal einen Komplett-Scan seines Systems machen. Das hilft

auch oftmals schon, und man stellt etwas fest. Dann wird es natürlich, sage ich mal, ein bisschen schwieriger, auch vielleicht, wenn man sich nicht auskennt. Aber man kann sich natürlich auch angucken, welche Programme laufen eigentlich gerade? Die kann man sich ja aufrufen, und wenn man da beispielsweise Programme sieht, die sehr seltsam aussehen, die man auch nicht kennt, wo man auch die Namen nicht zuordnen kann, dann kann man vielleicht davon schon einmal weiter ausgehen. Ich sag mal so, wenn man nicht herausfindet, was hier der Fall sein könnte, hat man hoffentlich gute Back-ups gemacht. Man kann sein Windows-System, wenn man einen Windows-Rechner hat, einfach immer platt machen und neu aufsetzen und noch mal bereinigt die Daten aufspielen und gucken, wie sich das Ganze dann verhält. Also das ist immer die Nothammer-Lösung, wenn man sonst nicht weiterkommt. Aber oftmals ist das auch die sauberste Lösung.

Michael Münz: Dann gehörst du bestimmt zu der Fraktion, die so denkt: „No Back-up, no mercy“, also alles, was man nicht gebackupt hat, ist halt auch nicht wichtig.

Letitia Kernschmidt: Ja, das ist ein krasser Spruch, aber ich würde ihn tatsächlich auch unterstützen. Was man vielleicht machen kann, man sucht sich eine Wochenroutine. Was machst du so einmal die Woche? Einkaufen gehen oder etwas anderes? Man sagt sich: „Gut, wenn ich jetzt samstags immer meinen Wocheneinkauf mache, dann stecke ich meine Festplatte an und lasse die Sicherung laufen, während ich beim Einkaufen bin. Wenn ich zurück bin, ziehe ich sie wieder ab und habe eine Datensicherung gemacht.“ Dann habe ich zumindest, sage ich mal, ein wochenaltes Back-up. Das ist in der Regel jetzt nicht so schlimm, wenn man Daten von vor drei Tagen verliert, als wenn man jetzt wirklich alles verliert, dann hat man das einfach mal in seine Routine miteingebaut. Das wäre zum Beispiel mal eine Idee, die man sich überlegen könnte, und man sollte das vielleicht auch zumindest einmal getestet haben, ob das Back-up auch funktioniert.

Ute Lange: Den Tipp finde ich jetzt noch viel wichtiger als den ersten, weil ich mich darauf verlasse, und da ist etwas schief gegangen, dann bin ich ja wirklich…ich sage es jetzt nicht, aber ihr wisst, was ich meine. Bist du denn selbst schon mal betroffen gewesen, Letitia?

Michael Münz: Das würde ich auch gerne wissen, jetzt nach den ganzen klugen Ratschlägen.

Letitia Kernschmidt: Nee, tatsächlich könnte ich mich nicht daran erinnern, jemals mit Schadsoftware wirklich ein Problem gehabt zu haben.

Ute Lange: Also, du hast jedenfalls noch nie etwas gemerkt. Das ist doch schon mal eine gute Nachricht.

Letitia Kernschmidt: Das heißt nicht, dass es nicht der Fall ist.

Michael Münz: Ich würde da mal reinspringen und gestehen, dass ich tatsächlich einmal von Schadsoftware befallen war. Aber nicht ich, sondern ich hatte einen Hoster, wo ich eine Webseite laufen hatte, und da kam irgendwie Schadsoftware drauf, da kamen politische Nachrichten und Botschaften und so an. Ich konnte das dann alles löschen. Aber mir war auch lange nicht klar, ob die von meinem Rechner auf den Server ging und ob die von dem Server vielleicht bei Besuchern dann auch gelandet war. Also da habe ich dann auch echt drei Tage viel recherchiert und rumtelefoniert. Aber offensichtlich war das dann in meiner

Webseiten-Software eine Schwachstelle, die jemand ausgenutzt hat, um da was abzulegen, um dann meinen Kunden fröhliche Botschaften zu schicken, die nicht von mir kamen. Den Fall hatte ich tatsächlich auch schon mal. Das war dann nicht mein Rechner, sondern ein anderer, wo ich dann aber auch kein Update gefahren hatte, und da kam das dann her.

Ute Lange: Und was hast du gelernt?

Letitia Kernschmidt: Das ist ein super Fall, den du da ansprichst.

Michael Münz: Aus deiner Perspektive. Wahrscheinlich aus meiner nicht so, aber ja, ich glaube, ich weiß, worauf du hinauswillst.

Letitia Kernschmidt: Nee, ich wollte sagen, dass es ein super Beispiel ist, weil es tatsächlich ganz, ganz vielen Leuten passiert. Also, es ist ja immer die Angst, oder viele sagen immer mal schnell: „Oh, ich bin gehackt worden“, und dann hat man ganz schnell die großen Namen im Kopf von den ganzen Plattformen, die man so benutzt, sei es zum Shopping oder Social Media. Das ist aber oftmals gar nicht der Fall, denn die haben ja auch viel Budget und viele Leute, die sich darum kümmern, und dass die gehackt werden, ist jetzt gar nicht so oft der Fall. Aber ganz, ganz viele Leute haben ein Ein-Mann oder Ein-Frau Unternehmen, einen kleinen Online-Shop, einen Blog, eine Website, wo sie irgendwas draufhaben. Das haben wirklich ganz, ganz viele Leute, und wenn man sich diese Webseiten mal anschaut, die haben oftmals auch einen Log-in oder brauchen Kundendaten, gerade wenn es ein kleiner Shop ist. Die haben leider oft gar nicht die Kapazitäten, die haben nicht das Wissen, die haben nicht das Budget, und die sind natürlich ein super Einfallstor für Angreifende, um dann beispielsweise Schadsoftware in dem Onlineshop zu hinterlegen und von allen Kunden, die dort einkaufen, einfach die gesamten Daten, am besten Zahlungsdaten, Kreditkartendaten und so weiter abzugreifen. Und dann merkt man das vielleicht als Shop-Betreiber gar nicht so schnell und ist aber dann tatsächlich eine Gefahr auch für andere. Und das ist natürlich dann auch noch mal ein anderes Szenario, was aber auch viele treffen kann.

Ute Lange: Du hattest gerade gesagt, dann betrifft es eben auch viele andere. Ich denke, das ist ja auch noch mal eine gute Botschaft, dass, wenn wir uns schützen, schützen wir andere mit. Also das Beispiel meiner Freundin, wenn ich da jetzt auf den Link gegangen wäre, das sah erst mal vertrauenswürdig aus, und die Ansprache war auch passend. Dann hätte ich mir vielleicht was eingefangen, was ich nicht so schnell wieder losgeworden wäre, und ich habe sie natürlich hinterher auch informiert und hab gesagt, du, dein System scheint irgendwie befallen zu sein, hat sich einen Schnupfen geholt oder was immer da passiert ist, weil du schickst jetzt komisches Zeug rum, und das kann andere ja auch gefährden. Das finde ich noch mal einen guten Hinweis, und du hattest überhaupt eine ganze Menge gute Tipps, die Michael und ich jetzt noch mal im Schnelldurchlauf aufzählen. Also, du hast auf jeden Fall gesagt, offline Back-ups, offline Back-ups, offline Back-ups, das war meine Nummer eins, Michael, was ist bei dir Nummer zwei?

Michael Münz: Update verfügbar. Also Nummer zwei ist Updates fahren. Updates fahren, Updates fahren. Immer dafür sorgen, dass Betriebssoftware, Programme oder, wie in meinem Fall auch auf Servern die Anwendungen, die man fährt, aber natürlich auch die Anti-Virus-Software oder Firewall-Software, die man hat, immer auf den neuesten Stand zu halten. Das gilt nicht nur für meinen Rechner und mein Telefon oder Tablet, sondern eben auch für alle anderen Geräte, die ich im Netz habe, also Jalousien und Staubsauger. Wir

haben lange nicht mehr über meinen Staubsauger gesprochen. Dass ich auch bei diesen Geräten immer darauf achte, dass die immer die neuesten Updates haben. Das nehme ich mit als Nummer zwei.

Letitia Kernschmidt: Ich hätte auch noch einen dritten, wenn ich den noch ergänzen darf. Weil Michael gerade das Zauberwort hat fallen lassen: Netzwerk. Wenn man ein Netzwerk hat mit mehreren Geräten. Netzwerksegmentierung ist das Zauberwort, was man noch platzieren sollte. Wenn man nämlich wieder an WannaCry zurückdenkt, können wir hier den Bogen noch mal perfekt zum Anfang der Folge schlagen. Wie kann sich ein Wurm ausbreiten? Der kann sich in einem Netzwerk ausbreiten, und wenn das Netzwerk wirklich getrennt ist und eigene Segmente hat, dann kommt er zumindest nicht überall in diesem Netzwerk hin, und so kann man zum Beispiel Geräte, die einem besonders wichtig sind, in verschiedenen Netzwerk-Segmenten haben.

Michael Münz: Oder ein Gast-Netzwerk einrichten, wo die Leute, die so durchmarschieren oder ins Haus kommen, dann unter sich bleiben und meine Geräte nicht befallen.

Letitia Kernschmidt: Genau, das zählt auch dazu.

Michael Münz: Okay, das sind doch drei coole Tipps.

Ute Lange: Wunderbar, und wir danken dir, Letitia und lassen dich jetzt essen gehen und dich deiner täglichen Arbeit wieder widmen. Da waren spannende Aspekte dabei, und wir wünschen dir weiterhin einen schönen Tag.

Letitia Kernschmidt: Schönen Tag, sehr gerne, vielen Dank, das wünsche ich euch auch.

Michael Münz: Dankeschön, und Letitia hatte es ja schon erwähnt. Es gibt vom BSI auch regelmäßige Infos zu Schadsoftware und wie man sich davor schützen kann. Links packen wir mit in die Shownotes und auch natürlich noch mal zu den unterschiedlichen Methoden, die wir jetzt gerade besprochen haben, um eure Daten abzusichern.

Ute Lange: Wenn ihr auch in Zukunft hilfreiche Tipps für euren digitalen Alltag haben möchtet, dann hört doch wieder rein, damit ihr die nächste Folge nicht verpasst. Liket oder folgt Update verfügbar auf euren Podcast Plattformen. Wir hören uns dann wieder in etwa vier Wochen bei der neuen Folge.

Michael Münz: Die neue Folge liegt dann etwa vier Wochen vor den Europawahlen vor und anlässlich dieser und auch vieler anderer Wahlen – wir haben auch noch Landtagswahlen im Herbst, und auch in vielen anderen Ländern wird in diesem Jahr gewählt. Ich glaube, das ist das Superwahljahr global. Angesichts dieser Wahlen wollen wir mal schauen, wie es da eigentlich aussieht beim Thema Desinformation. Wir können uns alle, glaube ich, darauf einigen, dass es Akteure gibt, die versuchen, über Desinformationen Meinungen zu bilden bei Wählerinnen und Wählern und somit versuchen ihre politischen Ziele zu erreichen. Wir sprechen dazu mit einer Expertin, einem Experten, der, die uns erst mal einordnet, was da eigentlich alles passiert, wo die Informationen herkommen, die wir sehen, und auch, wie wir dann erkennen können, ob wir gerade manipuliert werden sollen oder nicht. Also ich finde es ein krasses Thema und bin sehr gespannt auf die Erkenntnisse, die uns da erwarten, und kann euch nur raten, liebe Hörerinnen und Hörer wieder dabei zu sein.

Ute Lange: Und wenn ihr dabei sein möchtet und jetzt schon Fragen habt zu dem Thema, dann lasst uns doch gerne wissen, was ihr zu Desinformation wissen möchtet. Schreibt uns eure Fragen über die BSI-Kanäle auf Facebook, Instagram, X (ehemals Twitter), Mastodon sowie YouTube. Oder schickt uns auch ganz klassisch eine E-Mail, nicht mit Schadsoftware hinten dran, an die Adresse: Podcast@bsi.bund.de, wir freuen uns, von euch zu hören.

Michael Münz: Und wir freuen uns auf die nächste Folge mit euch. Also bis dahin alles Gute, passt auf euch und eure Daten auf, und bis dann in vier Wochen! Tschüss!