„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 16, 29.12.2021:

Das Tor zur Welt – Router einfach absichern

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

Lange: Hallo und herzlich Willkommen zu einer neuen Folge von „Update verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Ich bin Michael Münz und wir hoffen, dass ihr die Feiertage gut überstanden habt. Ute, was hast du in den vergangenen Tagen so gemacht?

Lange: Eigentlich nichts Aufregendes. Es war richtig ruhig. Ich habe mit der Familie ein bisschen zu viel gegessen, wie das wahrscheinlich viele da draußen auch gemacht haben. Ich habe ein bisschen pausiert, die Füße hochgelegt, mich an meinen Geschenken erfreut. Ich bin ein bisschen draußen gewesen und ansonsten bin ich faul gewesen. Kann man das hier so sagen? Ja, oder?

Münz: Kann man. Zwischen den Jahren kann man das auf jeden Fall. Ich glaube, das ist total okay.

Lange: Und du? Wie war es bei dir?

Münz: Ja, im Prinzip ähnlich. Feiertage habe ich mit der Familie verbracht und dann habe ich ein bisschen die Füße hochgelegt und auch ein paar neue Geräte ausprobiert, die ich über Weihnachten neu bekommen habe. Unter anderem habe ich mein Telefon eingerichtet, damit es auch sicher ist. Wir predigen jetzt seit 15 Monaten bestimmte Sicherheitsvorkehrungen. Da wollte ich auch mal dafür sorgen, dass mein Handy dem entspricht, was wir erzählen. Ich habe solche Einstellungen wie Touch ID, oder die Zwei-Faktor-Authentifizierung eingerichtet, damit ich beim Bezahlen beim Aldi oder beim Onlinebanking ein gutes Gefühl habe. Ansonsten habe ich zwischendurch ein paar Sachen im Fernsehen geguckt oder gestreamt und so etwas. Du auch?

Lange: Streaming ist ein kleiner wunder Punkt, das funktionierte bei mir nicht richtig.

Münz: Oh, da wollte ich aber keinen wunden Punkt treffen.

Lange: Ja, ich hatte gedacht, dass ich mich auch mal hinsetze und schau mir die eine oder andere Serie anschaue, von der ich gehört habe, weil ich mal Zeit habe. Das hat nicht geklappt und dann war ich ein bisschen genervt. Mein Neffe, der ja meine private IT-Abteilung ist, sollte seine Weihnachtsfeiertage nicht mit meinem Internet-Problem

zubringen. Ich habe stattdessen einfach die Bücher gelesen, die ich geschenkt bekommen habe. Ich habe so eine Minibibliothek gekriegt und das ist ja auch immer ganz schön.

***Münz**:* Mini-Bibliothek ist ein gutes Stichwort, denn: So besinnlich und ruhig wie wir es die vergangenen Tage hatten, hatten es, glaube ich, viele IT-Admins nicht. Die waren vermutlich beschäftigt mit der Bibliothek Log4J, dieser Schwachstelle, die seit Anfang Dezember diskutiert und immer wieder auch in den Medien auftaucht, bis hin zur Tagesschau. Die beneide ich jetzt wirklich nicht um ihre Arbeit.

Lange: Nein, das war ja schon vor den Feiertagen. Meldungen wie „das Internet brennt" und viele weitere Headlines hat man da gehört. Dabei ist es eigentlich, wenn ich das richtig verstanden habe, nur so ein kleiner Softwareschnipsel, der aber sehr verbreitet ist und in vielen IT-Abteilungen für so eine Programm-Bibliothek genutzt wird. Damit werden Aktivitäten protokolliert und das ist offensichtlich weltweit ein sehr beliebtes kleines Schnipselchen, das sehr verbreitet ist und dadurch große Probleme verursacht. Es ist technisch wohl sehr einfach, diese Lücke auszunutzen. Das wird auch im großen Stil versucht. Ich möchte jetzt – und auch dann, wenn so etwas passiert – nicht mit einer IT-Abteilung tauschen. Das ist eine heiße Sache.

***Münz**:* Die Gefahr besteht darin, dass diese Programm-Bibliothek ein Einfallstor ist für kriminelle Aktivitäten aller Art. Alles, was wir an Problemen und Fiesheiten in den vergangenen Monaten besprochen haben, ist dadurch möglich. Dazu ist es noch auf eine einfache Art möglich: Kriminelle können ganz einfach Schadsoftware einrichten, Daten klauen und Ransomware reinschmuggeln. Das sind alles Sachen, die dadurch möglich sind. Ich habe auch mitbekommen, dass das nicht mal zwingend Angriffe sein müssen, die jetzt passieren. Es kann auch sein, dass Kriminelle ihre Software jetzt einschleusen, ein bisschen warten, bis sich die Aufregung gelegt hat, und dann aktiv werden. Das deckt sich auch ein bisschen mit der mit der Beobachtung, von der ich kürzlich gelesen hatte, dass solche Hacking-Angriffe gern mal zu Zeiten passieren, in denen IT-Abteilungen vielleicht gerade nicht besetzt sind, zum Beispiel am Wochenende, nachts oder zu Urlaubszeiten. Man kann noch gar nicht genau absehen, welche Folgen dieser Cybervorfall hat, weil noch gar nicht genau klar ist, wann und in welcher Form diese Sicherheitslücke Log4j ausgenutzt wird.

Lange: Bisher wirkt es so, als betrifft dieser Vorfall auch eher IT-Abteilungen oder Menschen, die Server und Rechenzentren betreiben. Aber wir als Verbraucherinnen und Verbraucher sind wieder indirekt betroffen. Das haben wir in anderen Fällen schon beobachten können. Wenn zum Beispiel Dienste nicht zugänglich sind oder meine Daten irgendwo abgefischt wurden und ich selbst kriege das gar nicht mit, weil ich eben nicht direkt betroffen bin, dann habe ich wahrscheinlich nachher auch einen Schaden. Da viele Menschen zwischen den Jahren denken, sie hätten Zeit – und die haben sie vielleicht auch – sich um Sicherheitsangelegenheiten zu kümmern, nennen wir an dieser Stelle nochmal unsere Tipps, die wir immer wiederholen: Führt Updates für eure Systeme durch, von denen ihr wisst, dass sie auf euren Geräten sind. Du hast sie vorhin schon erwähnt: Ihr solltet die Zwei-Faktor-Authentisierung unbedingt einrichten, weil sie doppelten Boden gibt. Wenn

zum Beispiel meine Daten tatsächlich kompromittiert sind, also gestohlen wurden, von anderen genutzt werden, brauche ich, um mich in meine Konten einzuloggen mit der Zwei-Faktor-Authentisierung noch eine zweite Sache, die ich besitze: mein Fingerabdruck, meine Gesichtserkennung, eine SMS, die mir zugeschickt wird, oder ein Code, den ich per E-Mail bekomme. Das heißt, das kann man immer machen, selbst wenn man vielleicht nicht direkt von dieser Bibliothek betroffen ist.

***Münz**:* Eine Bibliothek mit diesen Auswirkungen! Das ist wirklich verrückt, wenn man sich das genauer anguckt. Die Sachen, die du gerade genannt hast, sind auch ganz unabhängig vom aktuellen Fall. Ich fühle mich bei diesen ganzen Cyber-Security-Nachrichten mittlerweile auch so, als würden wir immer von der nächsten Welle sprechen, die wir auch in anderen Kontexten immer wieder hören. Und ja, solche Sicherheitsvorkehrungen sind nie verkehrt, weil es immer aktuelle Fälle gibt. Kannst du dich noch an den Emotet-Fall erinnern? Über den haben wir ganz am Anfang unserer Podcastfolgen im vergangenen Jahr gesprochen. Dieser Virus war ja mittlerweile weg.

Lange: Ja, das erinnere ich auch. Da gab es doch Überschriften, dass dieser Virus vom Markt ist.

***Münz**:* Der ist wieder zurück. Der ist wieder da. Auferstanden aus … Ob es so einen Schrottplatz für Viren gibt? Wenn es das gibt, dann ist er von dort auf jeden Fall wieder herausgekrabbelt und er verbreitet sich wieder. Noch mal zur Erinnerung für alle, die das schon verdrängt haben: Das war ein Virus, der sich über authentisch aussehende Phishing-Mails verschickt hat. Der Virus hat sich Kontakte aus einem infizierten System herausgesucht und dann Mails verschickt mit Anhängen, in denen so etwas stand wie: „Kannst du vielleicht mal darauf gucken?“. Das sah alles richtig authentisch aus. Das machte die Gefahr so groß, dass viele Mails angeklickt wurden und sich diese Schadsoftware dann auf den Rechnern installieren konnte. Emotet ist dann im Prinzip auch eine Hintertür: Wenn die erst einmal auf- und zugemacht werden kann, dann können andere Sachen einfach hinterher geschoben werden, wie eben auch Ransomware oder andere Fiesheiten. Deshalb macht es immer Sinn, wenn man ein paar Minuten hat, sich noch einmal zu überlegen: Ist mein System eigentlich gerade sicher? Kann ich davon ausgehen, dass jetzt gerade niemand meinen Rechner gehackt hat oder meine Daten zieht oder mitliest, was ich gerade mache?

Lange: Aber um noch mal auf diese Art von Phishing zurückzukommen: Wir haben schon oft den Tipp gegeben, dass man, wenn man sich nicht sicher ist, die Mail gar nicht erst anklicken soll oder alternativ die Absender-Mail-Adresse prüfen soll. In diesem Fall muss man noch einen anderen Tipp geben, denn: Wenn das tatsächlich Kontaktadressen sind – wenn ich beispielsweise eine Mail bekommen würde, die angeblich von deiner E-Mail-Adresse kommt, dann könnte ich trotzdem versucht sein, darauf zu klicken. Das heißt, wenn eine Mail ankommt, bei der ich denke, dass die gar nicht von dir sein kann, frage ich dich lieber noch mal. Denn: Das scheint ja jetzt noch eine tückischere Variante von Phishing zu sein, die sich wieder verbreitet.

***Münz**:* Auf jeden Fall! Wir schicken uns ja ständig Post hin und her mit Word-Dateien und so weiter: Wenn da wirklich etwas kommt, was gerade nicht in unseren aktuellen Produktionsablauf passt, dann auf jeden Fall nachfragen. Es ist eine kleine Paranoia, die ich an mir festgestellt habe, dass ich da skeptisch werde.

Lange: Das nennt man Vorsicht. In diesem Fall ist es gesunde Vorsicht.

***Münz**:* Okay, danke – das beruhigt mich. Dann ist es ja nicht so schlimm um mich bestellt und mein Glaube an die Menschheit kann vielleicht noch ein bisschen bestehen bleiben.

Lange: Auf jeden Fall. Hier ist wirklich in vielerlei Hinsicht Vorsicht geboten. In den letzten Wochen ist mir eine Nachricht aufgefallen, in der in der Überschrift stand, dass Millionen Router Sicherheitsmängel aufweisen. Das ist aufgefallen, weil Computerexpertinnen und -experten sich WLAN-Router genauer angeschaut haben.

***Münz**:* Das sind diese Dinger, die wir alle zu Hause stehen haben.

Lange: Genau, wir alle. Ohne sie kommst du nicht ins Netz und auch die meisten Dinge, über die wir sprechen, kannst du ohne Router gar nicht machen. In einem Test ist nun herausgekommen, dass es Sicherheitslücken gibt, die von geringfügig bis schwer gehen. Getestet wurden mehrere Hersteller. Ich habe da gedacht, dass wir mal über dieses Teil reden, denn es ist ein bisschen das Tor zu dem, über das wir hier reden. Wenn du das nicht hast, geht es nicht. Ich muss gestehen, dass ich selbst nicht wusste, was man damit alles macht. Das steht in der Ecke und tut halt sein Ding. Was hältst du davon, dass wir das heute näher beleuchten? Ich glaube, dass viele damit so umgehen wie ich.

***Münz**:* Finde ich gut. Als ich die Meldung gesehen habe, hat mich das auch an das erinnert, was Katharina in der letzten Folge erzählt von der Haustür hat, die wir ja auch nicht sperrangelweit offen stehen lassen. Der Router ist für mich so etwas wie die Tür zum Internet. Der stellt die Verbindung her und alle Daten, die hinein oder herausgehen, gehen eben durch diese Tür. Von daher finde ich es total schlüssig, dass wir uns bei all den Sicherheitstipps, die wir hier geben, auch so ein Teil mal genauer angucken, das jeder von uns Zuhause hat. Das ist vielleicht gar nicht so verkehrt. Dann können wir mal schauen, was man mit einem Router alles machen kann, um ihn abzusichern.

Lange: Vielleicht haben ja auch andere Leute zu Weihnachten neue Geräte geschenkt bekommen oder sich selbst geschenkt und wollen jetzt loslegen, wenn sie es noch nicht getan haben. Das könnte hilfreich sein.

***Münz**:* Ja, vielleicht hören die uns gerade auf dem neuen Handy zu, das die Daten über den Router gezogen hat. Dann gucken wir doch mal, wie der Weg der Daten ist und was man damit alles anstellen kann: Was steckt im Router? Was können wir heute nicht mehr sehen und nicht mehr hören? Das war früher anders, da war e das sogenannte Modem. Das ist dieses …

Lange: … „Piep-piep-piep-piep-piep-piep-piep-Gerät mit dem lauten Geräusch.

***Münz**:* Ja, ich habe mein erstes Modem damals bei einem Gewinnspiel einer Krankenkasse gewonnen. Das war 1997, auch um diese Jahreszeit, zu Jahresbeginn. Das war so eine kleine weiße Kiste, die ich in die Telefondose stecken musste und auf der anderen Seite mit meinem PC Tower – bis zur Hüfte ging das Ding damals noch – verbinden musste. Dann musste ich noch ein Programm starten, in dem Telefonnummern hinterlegt waren. Ich konnte zuhören, wie das Modem diese Telefonnummern gewählt hat. Dann hat auf der anderen Seite auch ein Modem abgenommen. Die beiden haben gesprochen und dann kam dieses charakteristische Geräusch, das du vorhin nachgemacht hast. Wenn die beiden mit ihrer Unterhaltung fertig waren, war ich im Internet mit einem Gerät für den Zeitraum, in dem diese Verbindung stand. Das Internet war ja nicht für 24 Stunden permanent verfügbar. Das gab es damals gar nicht. Ich hatte ein Gerät, das mit dem Internet für einen bestimmten Zeitraum verbunden war. Das hat eine Telefonleitung besetzt. Das war es. „Ich bin im Internet drin." So hat Boris Becker das früher immer in dieser Werbung gesagt. Dieses Ding, dieses Modem, hört und sieht man heute gar nicht mehr. Das ist im Router integriert und arbeitet versteckt. Aber das Prinzip ist dasselbe: Es stellt die Verbindung zum Internet her, aber heute nicht mehr nur für ein Gerät, sondern für ein Netzwerk.

Lange: Wir wollen heute nicht mehr jedes Mal, wenn wir ins Internet wollen, dieses Kabel in die Buchse stecken. Ich erinnere mich auch. Das sind Geschichten aus unserer Jugend, an die sich viele überhaupt nicht erinnern. Das heißt, jetzt gibt es diesen Router, in dem alles drinsteckt, denn wir haben ja auch alle mehr als ein Gerät, das wir mit dem Internet verbinden. Wir wollen, dass unser Fernseher läuft. Wir haben vielleicht einen internetfähigen Staubsauger, du nicht – darüber haben wir gesprochen. Du willst verhindern, dass deine Daten abgesaugt werden. Aber es gibt Spielzeuge, es gibt Kaffeemaschinen, es gibt Handys, es gibt Rechner oder die Steuerung von Rollladen. Diese Geräte sind alle mit dem Internet verbunden. Wir haben schon einmal über Smart Home gesprochen. Das heißt, das ist jetzt alles mit diesem kleinen Gerät verbunden, so groß sind die gar nicht. Ich habe mir meinen noch mal angeguckt. Es funktioniert heute auch kabellos. Man hat auch nicht mehr diese Buchsen in der Wohnung, die nur für dieses spezielle Kabel da waren. Ich glaube, die gibt es nur noch in älteren Wohnungen. Das wird heute gar nicht mehr eingebaut. Das heißt, Router sind wirklich das Kernstück für so ein Heimnetz heutzutage. Eigentlich schon faszinierend, was sich da entwickelt hat.

***Münz**:* Ja, und dafür, dass es so wichtig ist und alles zentral über dieses Gerät läuft, wird es eher ein bisschen vernachlässigt. Wir packen es aus, stecken es ein und freuen uns, wenn die Lampe leuchtet. Wir drehen uns weg und das war es mit dem Gerät. Das ist ja. Es gibt so viele Mythen zum Thema Router. Ein Mythos zum Thema Router ist, dass man ihn hinstellt und das war es. Ich muss sagen, dass das eben nicht so ist. Denn schon vor dem Hinstellen muss man sich schon überlegen, wo man das Ding hinstellt. Das erklärt sich, wenn wir zurückgehen zu dem Bild mit der Tür und dem Hausschlüssel: Den Schlüssel hänge ich ja auch nicht neben die Tür und sage zu allen: „Kommt rein, hier hängt der Schlüssel".Ich habe den stattdessen an einem Ort, den außer mir niemand erreichen kann. Das ist bei dem Router genauso. Ich habe den an einer Stelle stehen, die dafür sorgt, dass die Netzabdeckung innerhalb meiner Wohnung gut ist, aber gleichzeitig nicht so öffentlich ist, dass jemand, der

hineinguckt, sehen kann: „Ach guck mal, der Michael hat einen Router vom Hersteller XYZ, da schau ich doch mal, was man damit alles machen kann“., Der steht an einem Ort, den von draußen keiner sehen kann.

Lange: Wobei es Fälle geben soll, in denen Menschen das Gerät tatsächlich gut sichtbar auf Fensterbänken vor großen Gartenfenstern stehen haben und vielleicht auch gern so platzieren, dass man das voreingestellte Passwort sieht. Es ist ein zweiter Mythos, dass man das Ding installiert, einsteckt und gut ist. Und die Voreinrichtungen und Voreinstellungen lieber nicht verändert.

Münz*:* Never change a running system.

Lange: Genau das ist der Fehler. Das ist ein ganz wichtiger Punkt. Du hast so ein Gerät, das voreingestellt ist. Du kannst das auch gern so lassen, aber das ist dann total unsicher. Das Router-Passwort sollte man als allererstes ändern, bevor man alle anderen Dinge macht. Man sollte nicht das Passwort behalten, das auf dem Aufkleber auf dem Router klebt. Ich habe bei mir geguckt: Da ist tatsächlich dieses alte Passwort drauf. Wenn ich das jetzt umdrehe und ins Fenster stelle, kann das jeder sehen. Es ist aber, Gott sei Dank, geändert worden. Aber das ist ja nur eines der Passwörter.

Münz*:* Das wollte ich gerade sagen. Das ist das Router-Passwort und nicht das WLAN-Passwort. Da muss man differenzieren. Es gibt das WLAN-Passwort. Damit verbinde ich mein Gerät mit dem Router. Der sorgt dann dafür, dass das Internet für dieses Gerät funktioniert. Es gibt es auch noch das Router-Passwort, mit dem ich diese Einstellung, die du gerade beschrieben hast, an dem Router vornehmen kann. Damit kann ich auch etwas machen: Ich kann Browser öffnen und dann aus der Gebrauchsanleitung einen Link ablesen, über den ich die Oberfläche dieses Routers aufrufen kann. Da kann ich mich einloggen und dann stehen mir alle möglichen Funktionen zur Verfügung, die ich einstellen kann. Unter anderem, was du jetzt gerade schon richtig erwähnt hast, kann ich die Passwörter ändern, die dort hinterlegt sind.

Lange: Das klingt jetzt viel komplizierter als es ist. Ich habe mir das tatsächlich noch mal angeguckt und das ist eigentlich ganz komfortabel. Es lohnt sich, einmal ein bisschen Zeit zu investieren, um das Gerät abzusichern und nicht im Nachhinein das Nachsehen zu haben. Das heißt also, man darf die Einstellung an einem neu gekauften Router ändern. Man soll es sogar, weil man sie auf sich verändern soll und bei Passwörtern nicht das Passwort behalten soll, das auf dem Aufkleber steht. Man soll es auch nicht irgendwo an den Rechner hängen oder an die Haustür. Das ist so ein bisschen wie mit einem Haustürschlüssel. Und es gilt: immer wieder updaten, updaten, updaten. Ein zweiter Mythos oder ein dritter – wir sind ja schon bei drei, ist: Wenn der Router einmal eingerichtet ist, muss man damit nichts mehr machen. Nein, das Gegenteil ist der Fall: Das sollte man schon!

Münz*:* Auch für Router gilt: Updates installieren und immer aktualisieren, um Sicherheitslücken zu schließen. Denn – das haben wir ja zu Beginn schon angesprochen: Es treten immer wieder neue Fälle von Cyberkriminalität auf. Irgendeine Sicherheitslücke ist

leider immer da. Es gibt immer etwas Neues, auf das man achten muss: „Bin ich für die aktuellen Schwierigkeiten gewappnet?“, „Kennt mein Router die?“, „Hat der Hersteller Updates zur Verfügung gestellt, die dafür sorgen, dass aktuell bekannte Sicherheitslücken geschlossen werden?“. Da sollte man auf jeden Fall immer dranbleiben und sehen, dass der Router aktuell ist und weiß, was er machen soll.

Lange: Wenn ich das nicht mache und so eine Sicherheitslücke bekannt ist – es gibt ja auch noch andere als die, die wir eingangs erwähnt haben, dann öffne ich tatsächlich wieder meine Haustür und dann sind vielleicht die Urlaubsfotos futsch. Die hat sich jemand herunter gesaugt. Meine ganze Kommunikation, zum Beispiel meine E-Mails, kann mitgelesen werden. Eines meiner Geräte und auch mein Router können ein Teil von einem Botnetz werden. Die werden für kriminelle Geschäfte missbraucht. Ich werde dann plötzlich Teil einer kriminellen Aktivität, obwohl ich eigentlich überhaupt nicht die Absicht dazu habe. Das heißt: Aufpassen und immer wieder: Updates, Updates, Updates! Manchmal komme ich mir vor wie eine Platte mit einem Sprung, aber man kann es nicht oft genug sagen.

***Münz**:* Das stimmt, aber es ist auch sehr wichtig. Damit kommen wir zu noch einem Mythos, der wahrscheinlich viele Menschen in einer falschen Ruhe hinterlässt, nämlich dem Gedanken: „Warum sollte sich jemand in mein Netzwerk hacken? Es hat doch niemand Interesse daran, meine Urlaubsfotos löschen. Das ist doch alles gar nicht relevant für andere.“ Aber, du hast es gerade schon erzählt, es geht oft gar nicht darum, dass jemand herausfinden will, was ich in meinem Heimnetzwerk mache. Eines der Szenarien, in dem mein Netzwerk interessant ist, ist diese Botnetz-Geschichte. Das bedeutet, dass Geräte in meinem Netzwerk fremdgesteuert und für kriminelle Aktivitäten eingesetzt werden. Zum Beispiel können von deinem Account Phishing-Mails versendet werden. Das sind diese sogenannten DDoS-Attacken. Hier werden ganz viele Rechner in einem Netzwerk zusammengeschlossen. Daraufhin rufen diese Webseiten auf, die dann unter dieser Last der Aufrufe zusammenbrechen. Das passiert auch großen Anbietern wie zum Beispiel Yahoo oder Ebay oder Amazon. Die werden immer wieder mal Ziel von solchen Attacken. Dahinter stecken sogenannte Botnetze von Rechnern, die gekapert wurden, weil die in ungesicherten Netzwerken standen. Dieses hier ist nur eines der möglichen Szenarien.

Lange: Um da kurz einzuhaken: Robert, der BSI Experte, der bei uns in der letzten Folge zu Gast war, hatte ja auch erklärt, wie verbreitet das ist. Wir hatten, glaube ich, über gekaperte Kaffeemaschinen oder Backöfen gesprochen. Das klang erst so ein bisschen seltsam, aber wenn das internetfähige Geräte sind, können die tatsächlich in so ein Netzwerk reinkommen und damit „die Kraft“ dieser Netzwerke verstärken. Ich selbst merke das ja gar nicht. Ich kann beteiligt sein, weil mein Gerät beteiligt ist, weil ich mein Gerät nicht geschützt habe. Das heißt, ich werde Teil von einer Bedrohung für andere. Dieser Aspekt beschäftigt mich immer mehr. Auch die Fraga danach, wie es verhindert werden kann, dass ein bei mir so harmlos herumstehender Router oder auch die Kaffeemaschine im Zweifelsfall dazu beitragen, dass irgendwo eine Internetseite kollabiert, weil dort massenhaft Nachrichten eingeschickt werden und das ganze System daraufhin einknickt.

***Münz**:* Was ich auch noch richtig perfide finde, ist diese Arbeitsaufteilung, die es offensichtlich unter Cyberkriminellen gibt. Jeder spezialisiert sich auf das, was er gut kann. Wenn sich jemand Zugang zu meinem Heimnetzwerk verschafft hat, gibt es Börsen, in denen Cyberkriminelle mein Netzwerk dann anbieten. Dafür kriegen die Geld. Dann kommt der nächste und treibt Unwesen in meinem Netzwerk. Das ist etwas, was ich auf gar keinen Fall will.

Lange: Ja, das ist ziemlich viel kriminelle Energie und auch viel eindeutig nicht freundlicher Wille, der dahintersteckt. Das bringt mich zu einem anderen Thema: Oft hat man Freunde und Freundinnen zu Besuch oder Familie und denen unterstelle ich jetzt keine kriminelle Energie. Ich habe aber auch gelernt, dass es nicht so gut ist, wenn ich die in das Netzwerk lasse, wo meine sensiblen Daten abgelegt sind, auch wenn ich ihnen vertraue. Dieses Netzwerk braucht einen gewissen Schutz und deshalb habe ich mir ein Heimnetz eingerichtet. Das war auch gar nicht so schwierig. Ich habe auch den Vorteil, dass ich jemanden habe, der mich dabei unterstützt. Der hat mir gezeigt, wie das geht. Ich glaube, du warst auch schon mal in diesem Netzwerk, als du hier warst. Das ist jetzt ein anderes WLAN als das, was ich selbst nutze. Das finde ich ziemlich beruhigend, denn das gibt mir das Gefühl „Okay, da kann keiner mehr was einschleusen“. Ich gebe auch keine Daten her, zum Beispiel auf dein Handy, von dem ich jetzt weiß, dass es sehr geschützt ist. Aber es könnte ja auch ein Handy einer anderen Person sein, bei der ich nicht so sicher bin, dass sie ihr Handy schützt. Das finde ich eigentlich ganz gut. Das war wirklich eine Sache von zwei Minuten. Jetzt kann ich das immer anbieten und ich muss nicht das Originalpasswort hergeben. Ich habe auch schon erlebt bei Freunden und Freundinnen, dass ich nach einem WLAN-Passwort frage und ich dann zu der Box geschickt wurde, in der der Router lag als er gekauft wurde. In der lag ein Zettel mit dem Originalpasswort. Das musste ich dann nutzen. Ich glaube, da werde ich beim nächsten Mal sofort sagen: „Komm, lass uns mal gucken, ob wir das ändern können“. Denn jetzt, wo ich mich damit noch mal beschäftigt habe, ist mir aufgefallen, wie viele Menschen das noch machen. Das ist der Hammer! Diese Zettel liegen auch teilweise vorn auf der Schlüsselablage oder irgendwo auf dem Schreibtisch oder sie hängen an einer Pinnwand. Das ist nicht so eine super Idee.

***Münz**:* Nicht wirklich, aber das Aufteilen des Netzes ist eine super Idee. Du hast ein Netz nur für dich, über das die Sachen gehen, die für dich wichtig sind: deine Kommunikation, deine Bankgeschäfte und andere Bereiche, in die du deine Gäste, deine Freunde und Bekannte, ansonsten nämlich hineinlässt. Diese Aufteilung macht auch Sinn, wenn man sie für alle internetfähigen Geräte einrichtet. Du hast dann einen Bereich, über den der Fernseher seine Streaming-Daten zieht oder über den die Kaffeemaschine ferngesteuert werden kann. So kannst du einfach sicherstellen, dass die Daten, die dir wichtig sind und die du auf keinen Fall anderen Leuten zugänglich machen willst, nicht erreicht werden können. So kann weder jemand in das Netz reinkommen, noch können Geräte mithören, welche Passwörter du benutzt. Diese Aufteilung des Netzwerks ist total cool und auch beruhigend. Und du hast völlig recht: Wenn man erst mal auf der Router-Oberfläche ist und sich im Browser anguckt, wo die einzelnen Einstellungen sind, dann ist es gar nicht so ein großer Aufwand. Du musst

hinterher vielleicht noch mal ein paar Passwörter an deinen Geräten ändern, weil der Fernseher dann versucht mit dem alten Schlüssel reinzukommen, aber das war es.

Lange: Was man auch noch machen kann, was aber die betroffene Zielgruppe oftmals nicht so toll findet, ist: Du kannst ja auch den Zugang zum Internet steuern. Wenn zum Beispiel Kinder oder junge Menschen in deinem Haushalt leben, und du das Gefühl hast, dass sie zu viel Zeit im Internet verbringen, kannst du den Zugang einstellen. Das ist nicht immer beliebt, wie ich aus meiner Familie weiß. Die Jungs fanden das gar nicht cool. Die wären, glaube ich, lieber woanders hingezogen, wo es diese Einschränkung nicht gegeben hätte. Das kann man auch über diesen Router einstellen. Oder auch vielleicht für sich selbst: Es sind nicht nur junge Menschen, die vielleicht zu viel Zeit im Netz verbringen oder zu häufig an ihre Gaming Box gehen. Man kann sich da auch selbst Zeiten einrichten. Das kann noch ein hilfreicher Aspekt sein. Wie gesagt, der kann vielleicht zu innerfamiliären Diskussionen führen, aber die kann man dann ja führen.

Münz*:* Mich haben tatsächlich schon Jugendliche gefragt, nachdem sie gehört hatten, dass bei mir zu Hause das Internet 24 Stunden zugänglich ist, ob sie nicht bei mir einziehen und ihre Elternhäuser verlassen könnten. Aber das konnten wir klären und so weit ist es dann nicht gekommen. Noch ein letzter Punkt, den ich mir angewöhnt habe: Ich bin viel unterwegs und habe mir in den vergangenen Monaten ein paar Routinen angewöhnt, wie zum Beispiel, dass ich immer meine Haustür abschließe. Dann hatte ich mal während meiner Abwesenheit einen Wasserschaden. Jetzt drehe ich in der Küche das Wasser ab, gieße schnell die Blumen und als letztes, bevor ich gehe, ziehe ich noch den Stecker vom Router, sodass er während meiner Abwesenheit gar nicht an ist. Das fühlt sich eigentlich ganz gut an. Einfach zu wissen: Wenn ich nicht da bin, kommt auch kein anderer an das Ding heran und kann sich hier bei mir im Netzwerk einnisten. Das ist zwar sehr rustikal würde ich mal sagen, aber mein Gefühl dabei ist irgendwie ganz schön.

Lange: Das mit dem Stecker ist bei mir nur die Notlösung. Wenn gar nichts anderes funktioniert, zum Beispiel wenn es mit dem Streaming nicht funktioniert, dann mache ich schon mal einen Kaltstart.

Münz*:* Das ist immer beste Lösung. „Haben Sie schon Ihren Rechner an und ausgemacht?“

Lange: „Oder den Router?“ Das ist dann die zweite Frage, wenn du eine IT-Abteilung anrufst.

Münz*:* Bei Druckern auch total beliebt: „Haben Sie schon mal an- und ausgemacht, dass es mal fünf Sekunden aus ist?“. Aber über Drucker müssten wir auch noch einmal reden, diese Dinger. Aber das führt uns jetzt zu weit vom Pfad ab.

Lange: Ich finde, wir haben schon eine ganze Menge an Dingen für uns Revue passieren lassen, zum Beispiel, was so ein Router alles beinhaltet und wie man ihn sicher und gut einrichten kann. Lass uns noch einmal zusammenfassen, so im Schnelldurchlauf, wie das bei manchen Sendungen auch heißt.

***Münz**:* Gut, dann nehme ich mal dir die Platte ab, lege sie auf und sage: Updates, Updates, Updates und individuelle Passwörter. Auf jeden Fall sowohl für den Zugang ins WLAN-Netz als auch für den Zugang zur Router-Konfiguration!

Lange: Okay, ein weiterer wichtiger Punkt: Wo stellt man dieses Gerät hin? Nach Möglichkeit nicht offen sichtbar. Das wäre sonst wie den Hausschlüssel vorne dranhängen, oder? Es gibt tatsächlich Leute, die haben den ja unter einem kleinen Blumentopf und alle in der Nachbarschaft wissen es. Aber das kann eben auch schiefgehen. Und genauso ist es beim Router. Nicht ans Fenster stellen und nicht zeigen, um welches Fabrikat es sich handelt. Und am besten das Passwort nicht nach vorne, sodass man es sehen kann.

***Münz**:* Und dann noch die etwas anspruchsvollere Maßnahmen, wie das Aufteilen des Heimnetzes in Bereiche, sodass sensible Daten nicht an der Kaffeemaschine abgefangen werden können oder dass jemand, der wirklich Zugang zu meinem Netzwerk gefunden hat, gar nicht in den Bereich kommt, der sensibel ist.

Lange: Doch genug zu tun für diese ruhigen Tage zwischen den Jahren, wie man sie nennt. Oder vielleicht auch dann nach dem Silvester Kater oder bevor es in der ersten Januarwoche wieder ein bisschen turbulenter zugeht. Vielleicht ist der eine oder andere Tipp für euch dabei gewesen. Wie gesagt, es lohnt sich auch seinen Router mal näher anzuschauen und weitere Informationen dazu gibt es dann wie immer in den Shownotes.

***Münz**:* Weitere Informationen, auch zu Log4Sell, die Schwachstelle, die bei vielen IT Admins jetzt wahrscheinlich für weniger besinnliche Tage gesorgt hat, gibt es auch auf der der Website des BSI zur Genüge. Da kann man ruhig mal gucken, denn die Themen bleiben uns wahrscheinlich erhalten. Wir melden uns dann wieder im neuen Jahr mit der nächsten Folge. Bis dahin würden wir uns freuen über Likes oder Follows auf den Plattformen, auf denen ihr „Update verfügbar“ hört. So verpasst ihr nämlich keine Folge. Wir freuen uns, wenn ihr uns sagt, dass euch unser Podcast gefällt.

Lange: Wie immer gilt: Kontaktiert uns gerne über die Plattformen des BSI: auf Facebook, Instagram, Twitter sowie YouTube. Und wir nehmen auch gerne E-Mails entgegen. Unter welcher Adresse, Michael?

***Münz**:* Willst du sie nicht sagen? Ich sage sie gern.

Lange: Ich kriege sie nicht stolperfrei heraus.

***Münz**:* Das ist normal. Schickt eine E-Mail an bsi@bsi.bund.de.

Lange: Wir freuen uns auch über jede Art von Post auf diesem Weg! Bis wir uns im nächsten Jahr wieder hören, wünschen wir euch alles Gute, einen guten Start und bleibt gesund. Tschüss, bis bald.

Besuchen Sie uns auch auf:

https://www.bsi.bund.de/
https://www.facebook.com/bsi.fuer.buerger
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