„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 17, 31.01.2022:

Schwachstelle in Log4j – eine Bilanz

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

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

***Münz**:* Ich bin Michael Münz. Weil es die erste Folge von „Update verfügbar“ im Jahr 2022 ist, wünschen wir euch ein Frohes neues Jahr. Wir hoffen, ihr hattet einen guten Start, und wir freuen uns auf weitere Folgen von “Update verfügbar” in den kommenden Monaten. Anfang des Jahres ist immer eine Zeit, in der man sich Vorsätze macht. Wie ist das bei dir? Hast du welche gemacht und womöglich schon gebrochen?

Lange: Mein Vorsatz war, sich keine Vorsätze vorzunehmen. Dann hatte ich doch welche, also habe ich den Vorsatz schon gebrochen. Ich wollte mir weniger vornehmen und ein bisschen weniger tun, um mehr Zeit für Pausen und Ruhe zu haben. Das fand ich ziemlich anstrengend, aber das geht vermutlich vielen da draußen so. Sind wir jetzt schon im dritten Jahr der Pandemie? Ich finde das ein bisschen anstrengend, und der Vorsatz ist, nicht so viel zu machen. Und den Vorsatz, sich nicht so viel vorzunehmen, habe ich schon gebrochen.

***Münz**:* Okay, das ist ein kleines Paradoxon, oder? Sich vorzunehmen, wenig zu machen. Aber gut, bei mir ist es so, dass ich mir überlegt habe, ich würde gerne, nachdem ich Ende des Jahres ein bisschen faul war, wieder ein bisschen mehr Sport machen. Und der IT-Vorsatz, den ich habe, ist, bei meinen Backups ein bisschen ordentlicher zu werden. Ich hatte eine Phase, in der ich relativ konstant Sachen auf anderen Festplatten abgespeichert habe. Das ist dann aber im letzten Quartal 2021 liegengeblieben. Da würde ich gerne noch mal rangehen und alles absichern, was mir wichtig ist, damit ich alles noch parat habe, wenn im Zweifelsfall was passieren sollte. Das sind bei mir die Punkte, die ich mir vorgenommen habe für 2022. Wir können dann darüber berichten, wie ordentlich ich gewesen bin.

Lange: Ich frage dich spätestens im letzten Quartal dieses Jahres, ob der Vorsatz noch Bestand hat. Alles gerät meistens ein bisschen durcheinander, wenn es hektisch wird. Ich hätte auch einen kleinen IT-Vorsatz jetzt, wo du das erwähnt hast. Ich habe aus den Gesprächen im Freundes- und Familienkreis gemerkt, dass das Wissen, dass wir hier durch den Podcast erwerben, anderen nützlich sein kann. Da noch nicht alle unseren Podcast hören, was sie hoffentlich demnächst beginnen, möchte ich mein Wissen ein bisschen mehr

teilen, weil ich denke, das kann vielen helfen. Und wir haben offensichtlich auch Leute im Freundeskreis, die, wenn sie den Podcast hören, daraus Schlussfolgerungen ziehen. Wir hatten bei dir auf dem Facebook-Account auch eine Reaktion auf die letzte Folge, in der wir über IT-Sicherheit bei Routern gesprochen haben.

***Münz**:* Ja, genau. Eine Freundin von uns hatte sich gemeldet und uns auf Facebook berichtet, dass sie aufgrund unserer Folge ihr Netzwerk neu aufgebaut und extra ein Gastnetzwerk eingerichtet hat. Ich bin nächste Woche da und bin gespannt, was mir präsentiert wird. Ich glaube, sie hat sogar geschrieben, sie hatte sich einen QR-Code eingerichtet. Den müsse ich scannen können und bin dann in ihrem Gastnetzwerk. Fand ich auf jeden Fall sehr witzig, weil sie eigentlich keine IT-Expertin ist, und die hat sich eher von uns den Anstoß geben lassen, ihr Netzwerk zu prüfen und zu ergänzen.

Lange: Beim Stichwort IT-Experte oder IT-Expertin fällt mir ein: Ich habe mich darüber gefreut was ich auf LinkedIn am Ende des Jahres gesehen habe: Hier hat ein IT-Experte seine Top 5 Podcasts aus dem Jahr 2021 veröffentlicht, und „Update verfügbar" war unter dieser Top 5. Das hat mich sehr gefreut, weil auch Menschen, die offensichtlich schon mehr über das Thema wissen, gerne bei uns reinhören.

***Münz**:* Vielen Dank auch für die vielen Rückmeldungen der vergangenen Monate. Das hat uns sehr gefreut. Taggt uns auch gerne in eurem Post zum Podcast oder schreibt uns über die Kontaktadressen. Wie ihr uns erreichen könnt, erzählen wir am Ende jeder Folge.

Lange: Was gab es noch, seit wir das letzte Mal hier vor dem Mikro gesprochen haben? Die Schlagzeilen des ersten Monats 2022 mit IT-Bezug: was ist dir aufgefallen, Michael?

***Münz**:* Zum einen ist mir alles aufgefallen, was mit Log4j zu tun hat. Das ist die Schwachstelle, über die wir in der letzten Folge berichtet hatten. Da gibt es ein paar neue Entwicklungen. Darüber sprechen wir aber gleich ausführlich. Deswegen gehe ich besser auf ein anderes Thema ein, um nicht zu viel vorwegzunehmen, und zwar „Smishing". Da habe ich aufgehorcht, weil das auch ein Thema ist, dass wir im vergangenen Jahr besprochen haben. Das sind diese SMS, in denen ein Link drin war. Häufig waren das Paketdienste, die angeblich irgendwas liefern würden, dann musste man auf den Link klicken…

Lange: …oder Gewinnspiele, die dir versprechen, dass du um Millionen reicher wirst, wenn du da draufklickst.

***Münz**:* Ich habe trotzdem nicht draufgeklickt. Aber nichtsdestotrotz ist die Gefahr weiterhin da, dass diese Links per SMS verschickt werden. Deswegen heißt es „Smishing" und nicht „Phishing" - wegen SMS. Es gibt Zahlen, die mich aufhorchen lassen. Ich glaube, bis zu 100 Millionen SMS sind unfreiwillig von infizierten Geräten verschickt worden. Das war eine Zahl, die mich sehr beeindruckt hat und auch ein bisschen nachdenklich gemacht hat, dass diese Masche noch immer so stark im Umlauf ist.

Lange: Apropos alte Masche. Ich habe auch etwas gelesen über eine Masche, die ich selbst schon ein paarmal am Telefon erlebt habe und von der ich dachte, dass es sie gar nicht mehr

gibt, aber offensichtlich bleibt sie populär, und zwar die sogenannte Microsoft Masche. Dabei ruft dich angeblich jemand von Microsoft an und behauptet, sie hätten ein Problem festgestellt, und sie würden dir jetzt am Telefon helfen wollen. Sie führen dich dann durch bestimmte Schritte und am Ende wollen sie nur Zugang zu deinem Rechner. Ich habe das tatsächlich ein paar Mal erlebt. Beim ersten Mal war ich etwas unsicher und habe das Gespräch eine Weile geführt, bis es mir sehr seltsam vorkam. Die letzten Male, wenn ich solche Anrufe bekam, auch von ganz unterschiedlichen Telefonnummern, habe ich immer sofort aufgelegt und das Gespräch gar nicht erst begonnen.

***Münz**:* Solche Anrufe hatte ich auch immer wieder. Aber mittlerweile gehe ich an Nummern, die ich nicht kenne, nicht ran, erst recht, wenn sie aus dem Ausland sind. Ich hatte oft Anrufe aus England oder Österreich. Ich hatte schon erzählt, dass da wahrscheinlich auch solche Anrufe dahinterstecken.

Lange: Kann gut sein, ja.

***Münz**:* Als wir uns das letzte Mal gesehen haben, haben wir auch über den Angriff auf das Internationale Rote Kreuz gesprochen. Das hast du gesehen.

Lange: Ja. Wir haben öfter über erbeutete Daten gesprochen. Dieses Mal hat es eine Organisation getroffen, die besonders sensible Daten speichert, weil es um Menschen geht, die auf der Flucht sind oder sich in anderen Lebenskontexten befinden, die nicht so einfach sind. Die müssen sich darauf verlassen können, dass ihre Daten nicht irgendwo im Netz landen. Das Rote Kreuz hat jetzt die Verursachenden dieses Lecks über die Presse angesprochen und darum gebeten, diese Daten nicht zu veröffentlichen, weil es besonders sensible Daten sind. Selbst solche Organisationen sind offensichtlich nicht vor Angriffen gefeit.

***Münz**:* Zum Glück gibt es auch Nachrichten, die einem das Gefühl geben, man ist diesen Angriffen nicht schutzlos ausgeliefert. Ich hatte etwas über einen Ermittlungserfolg gelesen bei dem Ermittlerinnen und Ermittler aus zehn Ländern Server stilllegen konnten, über die Cyberkriminelle in einem VPN Netzwerk kommuniziert haben. VPN – wir erinnern uns und kennen das vielleicht auch aus dem Home-Office, das ist dieser – wir nennen es Tunnel – in dem man von vorne und von hinten die Kommunikation starten kann und auf den sonst niemand Zugriff hat. Das nutzen Cyberkriminelle auch, um ihre Anonymität zu gewährleisten. Da ist jetzt was stillgelegt worden und das hat mich ein bisschen beruhigt, weil ich dachte, man kriegt diese Menschen doch irgendwie gefasst und muss ihnen nicht nur, wie in diesem „Hase und Igel Spiel“, hinterherlaufen. Das war etwas, was mich ein bisschen beruhigt hat.

Lange: In dieselbe Kategorie fällt das, was ich gesehen habe. Es ist noch gar nicht so lange her, dass der russische Inlandsgeheimdienst eine ganze Menge Personen aus der Cybercrime Gang „REvil“, über die wir auch berichtet haben, verhaftet und das Geld konfisziert hat. Das ist auch eine gute Nachricht, dass selbst in einer Region, in der relativ viele Verursachende

ihrer Tätigkeit nachgehen können, auch eingegriffen wird. Ich finde das ist ein schöner Aspekt in dem „Gute Nachrichten- Blog“. Hoffentlich sind es gute Nachrichten.

Damit kommen wir zum Thema des Tages. Du hattest Log4j erwähnt. Darüber haben wir in der letzten Folge berichtet. Damals gab es Schlagzeilen wie „Das Internet brennt“. Wir wollen jetzt, einen Monat später, darüber sprechen, was sich seitdem getan hat. Dafür haben wir Christoph Lobmeyer aus dem BSI eingeladen, der sehr nah dran war. Herzlich willkommen, Christoph. Schön, dass du dir heute Zeit für uns nimmst.

Lobmeyer: Hallo ihr beiden.

Lange: Was machst du im BSI und wie bist du da hingekommen? Stell dich kurz vor.

Lobmeyer: Ich bin Christoph, Incident Händler im BSI. Das bedeutet, dass ich Betroffene bei IT-Sicherheitsvorfällen unterstütze. Sowohl technisch mit meinen Kolleginnen und Kollegen als auch bei der Organisation des Wiederanlaufs. Ich habe nach dem Abitur Informatik studiert und bin seit 2015 in verschiedenen Jobs im IT-Sicherheitsbereich tätig, sowohl im Bereich der Vorfallsbearbeitung als auch im Bereich vom Aufbau von Security Operations Centern und CERT. Ich habe das in der Bundesverwaltung gemacht, habe aber auch für eine Unternehmensberatung gearbeitet.

Münz*:* Kannst du bitte die Abkürzung „CERT“ einmal auflösen?

Lobmeyer: Ein CERT ist ein Computer Emergency Response Team. Das ist eine Bezeichnung für Computer-Notfall-Teams. Das ist auch der Bereich, in dem ich jetzt im BSI arbeite. Das ist die Gruppe von Leuten im IT-Sicherheitsbereich, die sich um Vorfälle kümmert, um die zu beheben.

Münz*:* Bevor wir auf das eigentliche Thema kommen, würden wir dir gerne eine Entweder-Oder-Frage stellen, die dich hoffentlich überrascht und zu einer spontanen Reaktion führen wird, sodass wir noch mehr über dich erfahren werden.

Lobmeyer: Ich bin gespannt.

Münz*:* Die Frage an dich lautet: Lieber lebenslang unsichere Passwörter oder lebenslang schlechten Kaffee?

Lobmeyer: Lieber lebenslang schlechten Kaffee. Ich trinke keinen.

Münz*:* Gäbe es ein anderes Getränk, das wir dir wegnehmen dürften, wenn du dafür schlechte Passwörter haben dürftest?

Lobmeyer: Ich möchte keine schlechten Passwörter haben – das tut mir leid. Aber ich glaube, ohne Mate könnte ich nicht lange überleben.

Münz*:* Alles klar.

Lange: Okay, dann sollten wir unsere Frage in Zukunft wohl noch etwas anpassen.

***Münz**:* Dann Fragen wir in Zukunft nach Kaffee, Mate, oder Tee. Wir kommen jetzt zu Log4j. In der letzten Folge hatten wir gemutmaßt, dass IT-Administratorinnen und -Administratoren hektische Feiertage gehabt haben wegen Log4j, dieser Schwachstelle, die bekannt geworden ist und viele Systeme und Anwendungen betroffen hat. Wie waren deine Feiertage und was war Log4j in der Situation für uns alle für eine Bedrohung?

Lobmeyer: Meine Feiertage waren relativ entspannt. Die Tage und Wochen vorher waren allerdings turbulent. Ihr habt das sicherlich mitbekommen. Wir haben als BSI eine Warnmeldung rausgegeben. Ich glaube, am 11. Dezember haben wir die Warnstufe auf Rot hochgeschaltet. Rote Warnmeldung heißt, dass die IT-Bedrohungslage extrem kritisch ist und dass wir damit rechnen, dass IT-Sicherheitsteams oder IT-Betriebsteams außerhalb ihrer normalen Arbeitszeit arbeiten müssen, um das Problem zu lösen. Diese Schwachstelle war deshalb so kritisch, weil Log4j als Komponente einer Software in vielen unterschiedlichen Programmen eingebaut ist. Sowohl in Programmen, die auf Privatrechnern sind, als auch in Programmen, die im Internet verfügbar sind, bspw. Webseiten und IT-Dienste, die dort angeboten werden. Das ist an der Stelle das Entscheidende. Dadurch, dass diese Bibliothek in so vielen verschiedenen Komponenten eingebaut ist, und wir zum Teil gar nicht genau wussten, in welchen überhaupt, sind wir davon ausgegangen, dass diese Schwachstelle schnell und kurzfristig von Cyberkriminellen ausgenutzt wird. Die benutzen diese Schwachstelle, um Zugriff auf fremde Systeme zu bekommen.

***Münz**:* Mittlerweile ist die Sicherheitsstufe zurück auf Gelb gesetzt worden. Ist das ein Zeichen für Beruhigung? Können wir uns jetzt alle entspannen? Sind eure schlimmsten Erwartungen und Befürchtungen nicht eingetroffen?

Lobmeyer: Wer bis jetzt nicht gepatched hat, hat wahrscheinlich ein großes Problem. Das ist die Aussage, die dahintersteckt. In dieser Akutphase Ende Dezember wollten wir dadurch, dass wir diesen Druck aufgebaut haben, sicherstellen, dass die Firmen und Organisationen ihre IT-Netzwerke kurzfristig absichern. Das ist der Grund, weshalb wir die Warnmeldung auf „Rot“ geschaltet haben. Wir wollten sagen: „Ihr müsst jetzt außerhalb eurer regulären Arbeitszeit arbeiten.“ Es ist jetzt Mitte Januar und es gibt natürlich immer noch Systeme, die verwundbar sind. Die Schwachstellen in solchen Systemen sind wahrscheinlich schon ausgenutzt worden, deshalb ist die Warnmeldung runtergestuft. Jetzt liegt der Fokus darauf, zu schauen, ob sie in der Akutphase ausgenutzt wurden bzw. dass die Updates für IT-Programme bei Firmen kurzfristig installiert werden.

Lange: Du hast gesagt, dass es im Wesentlichen Menschen in Firmen betraf, die die IT-Server bedienen bzw. programmieren oder warten. Habt ihr Beispiele, bei denen wir als normale Verbraucherinnen und Verbraucher das auch mitbekommen haben? Gab es Seiten, die abgeschaltet werden mussten oder Dienste, die nicht genutzt werden konnten in der Zeit?

Lobmeyer: Ich kann selbstverständlich jetzt nicht über Vorfälle sprechen, die wir bearbeitet haben. Wir sprechen nicht über Vorfälle von anderen Leuten, vor allem dann nicht, wenn wir sie unterstützt haben. Ich kann sagen, dass diese Schwachstelle am Anfang im

Zusammenhang mit dem Computerspiel Minecraft aufgefallen und öffentlich bekannt geworden ist. Das ist das Spiel, in dem man Klötzchen durch die Gegend schieben muss und sich so eine Welt bauen kann etc. Das war eines der ersten Systeme, die als betroffen galten. Dahinter steckt natürlich eine große Community, wodurch die Aufregung in den entsprechenden Foren und Internetseiten groß ist. Microsoft hat das gepatched, das bedeutet, das Unternehmen hat die Schwachstelle geschlossen. Es gab aber noch andere Dienste. Ich habe nach öffentlichen Berichten geschaut und da steht zum Beispiel, dass auch iCloud verwundbar war, obwohl Apple das fix gepatched hat.

***Münz**:* Wenn du sagst, dass Microsoft das gepatched hat, heißt das, dass ich als Verbraucher nix machen muss, weil die Verantwortung woanders liegt und ich davon nicht betroffen bin? Oder muss ich auch irgendwas machen?

Lobmeyer: An dem Minecraft-Beispiel kann man es gut beschreiben. Microsoft hat die Empfehlung ausgesprochen, alle Fenster von Minecraft zu schließen und das Programm, mit dem man startet, neu zu starten. Dann zieht er sich automatisch die Updates, in dem Fall die vom Microsoft Server. So ist es bei allen Programmen. Wenn ich nicht selbst Softwareentwicklerin oder -Entwickler bin, bin ich darauf angewiesen, dass die Hersteller der Programme Updates rausbringen.

Lange: Noch mal der Tipp für Verbraucherinnen oder Verbraucher. Wenn ich mir nicht sicher bin, ob das, was ich benutze, davon betroffen war oder noch ist: Programm schließen, alles herunterfahren und danach Updates ziehen. Updates, Updates, Updates – das ist unser Mantra hier.

Lobmeyer: Da würde ich auf jeden Fall zustimmen.

***Münz**:* Jetzt hast du gesagt, dass diese Schwachstelle in vielen Anwendungen mit drin ist. Ist das etwas, was häufig vorkommt? Ist es oft so, dass Codeschnipsel in anderen Anwendungen verwendet werden? Heißt das, dass so etwas wie Log4j künftig auch an anderen Stellen passieren kann?

Lobmeyer: Einfach gesagt – ja. Software wird meistens nicht so entwickelt, dass es einen Entwickler gibt oder eine Entwicklerin, der oder die in dem entsprechenden Keller oder in dem entsprechenden Großraumbüro sitzt und dann quasi mit einem leeren Blatt oder einem leeren Fenster, wo die Software reingeschrieben wird, anfängt. Es ist vielmehr eine Mischung aus dem Zusammenfügen bestehender Komponenten und zu denen eigene Komponenten dazu entwickelt werden. Ein Beispiel mit Log4j: Log4j ist eine Bibliothek, vereinfacht gesagt, ein Softwareschnipsel, der dazu benutzt wird, um beispielsweise Fehlerfälle zu protokollieren. So können die Leute, die dieses Programm betreiben, zum Beispiel im Rahmen von Internetanwendungen, bei Fehlern oder Störungen prüfen, was passiert ist und ob es an irgendeiner Stelle vielleicht ein technisches Problem gibt. Man kann sich vorstellen, dass es dieses Verfahren nicht nur bei einer Anwendung gibt, sondern bei ganz vielen unterschiedlichen Anwendungen, praktisch bei fast jeder Anwendung. Deshalb ist irgendjemand irgendwann mal hingegangen und hat gesagt: „Na prima, das ist offensichtlich,

was gebraucht wird. Ich schreibe jetzt eine Bibliothek drum herum.“ Andere Firmen, andere Organisationen und andere Projekte haben diese Bibliothek dann eingebunden, wenn sie den Bedarf hatten, etwas zu protokollieren. Deshalb ist diese Bibliothek an so vielen unterschiedlichen Anwendungen verbaut.

***Münz**:* Diese Herangehensweise kommt also häufiger vor, dass man sich kurze Schnipsel sucht, die schon vorliegen, und die in die eigenen Anwendungen einbaut.

Lobmeyer: Richtig, das kommt häufiger vor. Das ist, wie Software prinzipiell entwickelt wird. Man erfindet das Rad nicht immer neu, sondern man kauft sich vielleicht den Reifen bei irgendeinem Zulieferer. Bei Log4j wird der Reifen nicht beim Zulieferer gekauft, sondern da gibt es eine Beschreibung, wie man einen Reifen baut, und die ist öffentlich verfügbar.

Lange: Jetzt war Log4j offensichtlich sehr verbreitet und deswegen habt ihr Druck aufgebaut mit eurer Warnung. So habt ihr allen klar machen wollen, dass man schnell was tun muss. Ich habe das zum ersten Mal so wahrgenommen, dass es eine Warnstufe Rot gab. Aber vielleicht auch nur, weil ich aufmerksamer geworden bin. Wie häufig kommt das vor? War das jetzt eine Ausnahmesituation, die sich durch die starke Verbreitung ergeben hat? Oder habe ich einfach die anderen Roten Warnungen nicht wahrgenommen?

Lobmeyer: Die Roten Warnmeldung geben wir tatsächlich sehr selten raus. Ich glaube, insgesamt ist es eine Handvoll. Allerdings war das Jahr 2021 an der Stelle eine Besonderheit. Da gab es nämlich zwei Warnungen dieser Warnstufe Rot. Die erste war Anfang des Jahres 2021 und es ging um Exchange. Das ist ein E-Mail-Service, der von Microsoft entwickelt und zur Verfügung gestellt wird. Da hatten wir schon eine Warnmeldung Rot rausgegeben und dann Ende letzten Jahres mit Log4j aus gleichen Gründen, nämlich weil die Schwachstelle sehr leicht aus dem Internet ausnutzbar war und weil die entsprechende Software, die dieses Problem hat, sehr weit verbreitet war.

***Münz**:* Für uns als Verbraucherinnen und Verbraucher stellt sich irgendwann die Frage: ist das irgendwann mal vorbei? Ist Log4j irgendwann behoben? Die Lehre ist, Updates zu ziehen und dafür zu sorgen, dass die Computersysteme immer auf dem aktuellen Stand sind. Das nehme ich mit. Ist das irgendwann mal vorbei? Oder kann es sein, dass wir in sechs Monaten noch mal über Log4j sprechen, weil es neue Entwicklungen gibt?

Lobmeyer: In einer idealen Welt wäre es genau wie du sagst, Michael. Wir würden einfach alle Updates installieren, dann wäre alles gut und wir beschäftigen uns mit dem nächsten Problem. Leider haben wir die Erfahrung gemacht, dass das genauso nicht passiert. Klar, es gibt viele Organisationen, die die Sicherheitslücken schließen und es gibt Firmen, die Updates rausbringen, aber es gibt auch eine ganze Menge von Organisationen, die keine Updates installieren, obwohl Updates verfügbar sind. Und das ist natürlich ein Problem, weil die Systeme natürlich noch verwundbar sind und weiter ausgenutzt werden können. Das ist Teil 1 des Problems. Teil 2 des Problems ist, dass wir und andere Sicherheitsforschende in dieser Akutphase davon ausgehen, dass diese Schwachstelle von Cyberkriminellen ausgenutzt wurde. Die haben damit aber noch nicht unbedingt was gemacht. Das, was wir

jetzt befürchten, ist, dass diese Zugriffe, die auf fremde IT-Systeme geschaffen wurden, irgendwann in der Zukunft ausgenutzt werden, um weitere Maßnahmen vorzunehmen. Zum Beispiel um Verschlüsselungstrojaner zu installieren und vielleicht auch Daten abzuziehen. Deshalb reiht sich das ein in die Reihe von Cyberkriminellen, die Schwachstellen im IT-System ausnutzen, und natürlich Schwachstellen, die stark bekannt werden und sie auch bei den Cyberkriminellen bekannt werden, die diese dann auf Halde legen. Irgendwann gibt es einen Stapel von Zugangsdaten und irgendwann arbeiten sie diesen Stapel durch und installieren beispielsweise Verschlüsselungstrojaner. Das heißt – long Story short – wir werden damit wahrscheinlich noch länger zu tun haben.

Lange: Wir kommen noch mal zum Anfang unseres Gesprächs zurück. Michael, wer jetzt noch keine guten Vorsätze für dieses Jahr hat, gibt es hier ein paar Anregungen für die IT-Sicherheit? Denn Vorsicht ist bekanntlich besser als Nachsicht. Es ist möglich, dass ich damit rechnen muss, falls meine Schwachstelle ausgenutzt wurde, dass es mich ein halbes Jahr später auf irgendeine Art und Weise, vielleicht auch unvorbereitet und unvermittelt trifft. Ich habe gepatched, ich habe die Sicherheitslücke geschlossen, aber die Kriminellen haben vorher schon entweder was dagelassen oder was mitgenommen, nämlich meine Daten. Das heißt, wer noch keine guten Vorsätze hat, guckt euch die Kacheln auf Social Media vom BSI genau an – besonders die, bei denen es um diese Vorsätze ging. Das sind Maßnahmen, die nicht so lange dauern. Aus der eigenen Erfahrung weiß ich, dass das meistens recht schnell geht, wenn man sich erst einmal überwunden hat, Und es lohnt sich tatsächlich, Vorsicht walten zu lassen, korrekt, Christoph?

Lobmeyer: Ja, das, was du gerade gesagt hast, ist wichtig. Das Schließen der Schwachstelle ist das eine, aber es kann auch sein, dass, bevor man die Schwachstelle geschlossen hat, sich bereits jemand eingenistet hat. Das heißt, es reicht nicht aus, die Schwachstelle einfach zu schließen, sondern man muss auch nachschauen, ob sich in der Zwischenzeit (seit dem Bekanntwerden der Schwachstelle bis zum Zeitpunkt des Patchens) da jemand schon eingenistet hat.

Lange: Oder was mitgenommen hat. Manchmal sind es Datenpakete, die woanders landen.

Lobmeyer: Genau. Das kommt im späteren Schritt. Jetzt in der Akutphase haben einige Leute die Schwachstelle bei sich im Netzwerk geschlossen und haben nicht nachgeguckt, ob noch ein Zugang von den Angreifern schon angelegt wurde. Die haben jetzt natürlich ein Problem.

Münz*:* Vielen Dank, Christoph, für die Einordnung und vor allem für die vielen Hinweise, die wir uns im Alltag immer wieder vor Augen halten und beherzigen sollten. Vielen Dank. Das war wirklich sehr aufschlussreich.

Lobmeyer: Ich danke euch auch.

Lange: Du sagtest gerade „viele Tipps“, Michael. Was ist bei dir hängengeblieben, was wir noch mal bündeln sollten?

***Münz**:* Das erste, was bei mir hängengeblieben ist: Ich muss nicht zwingend wissen, wie Software programmiert wird oder was es mit Log4j oder vielleicht anderen Fällen genau im Detail auf sich hat. Wenn dann aber solche Sicherheitslücken bekannt werden, sorge ich dafür, dass meine Betriebssysteme auf dem letzten Stand sind, damit ich Sicherheitsupdates, wenn sie ergänzt wurden, auf meinen Endgeräten installiere. Was bei mir hängengeblieben ist, ist, dass ich auch bei Anwendungen, die ich häufig nutze, immer darauf achte, dass ich die aktuelle Version nutze. Im Zweifelsfall sollte man sie noch mal runterladen und neu installieren. Und – nochmal zum Thema „Backups“: Daten, die mir wirklich wichtig sind, habe ich auf einem anderen Gerät gespeichert, auch physisch. Zum Beispiel auf einer externen Festplatte. Im Zweifelsfall, wenn bei meinem Rechner irgendwas passiert, sind sie sicher und ich kann sie von einem anderen Gerät einspielen.

Lange: Zu den Backups hatten wir, in einer anderen Folge schon einmal den Tipp genannt, dass die Geräte nicht mit dem Internet verbunden sein sollten, sodass die für Neustart, wenn er nötig sein sollte, nicht kompromittiert sind und man sich andere Dinge unbewusst oder unabsichtlich in das eigene System holt.

***Münz**:* Ich habe eine Schublade, in der ein paar alte externe Festplatten immer wieder hin und her klappern. Da ziehe ich mir alles rüber, was wichtig ist.

Lange: Wunderbar. Wir hören und sehen uns bei der nächsten Folge. Bis dahin liked und folgt „Update Verfügbar“ auf eurer Podcast Plattform. So verpasst ihr keine Folge und könnt auch in die älteren noch einmal reinhören. Wir haben schon über Ransomware gesprochen, als wir Kolleginnen und Kollegen von Christoph dabeihatten, die auch aus der Vorfallsbearbeitung berichtet haben. Wir haben schon zu allen möglichen Themen gesprochen. Es lohnt sich immer, die älteren Folgen anzuhören. Für die, die noch mehr zur IT-Sicherheit wissen wollen, gibt es noch einen ganz konkreten Anlass in den nächsten Tagen.

***Münz**:* Da gibt es den IT-Sicherheitskongress des BSI, der am 1. und 2. Februar stattfindet. Es geht zwei Tage lang um Themen der Cybersicherheit und darum, wie wir uns vor all den Gefahren schützen können, auf die wir immer wieder hinweisen. Wenn ich jetzt Gefahren sage, heißt das nicht, dass wir Angst verbreiten wollen, sondern dass wir uns um die Sicherheit im digitalen Alltag sorgen. Wir sind, im besten Fall, der Fahrradhelm, den man aufsetzt, um unbeschadet durch den Datenverkehr zu kommen.

Lange: Wer es nicht schafft oder den IT-Sicherheitskongress verpasst hat, kann sich auf der BSI-Webseite die wichtigsten Informationen ansehen. Der Blick darauf lohnt immer. Die Kanäle in den Sozialen Medien vom BSI auf Facebook, Instagram, Twitter sowie YouTube sind rund um die Uhr erreichbar, falls ihr irgendetwas nachschauen wollt.

***Münz**:* Oder falls ihr uns erreichen wollt. Das sind keine Einbahnstraßen, die die Kolleginnen und Kollegen vom BSI betreiben, sondern ihr könnt uns gern darüber kontaktieren. Wer es lieber klassisch mag, gerne auch über bsi@bsi.bund.de. Wir freuen uns immer, wenn ihr uns

schreibt, wenn wir Hinweise auf Themen bekommen oder ihr uns mitteilt, was wir im Podcast noch verbessern können. Immer gerne her damit.

Lange: Alles Gute, bleibt gesund, zuversichtlich und optimistisch. Bis dann. Tschüss.

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