„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 14, 29.10.2021:

Zugriff verweigert! - Erpressung mit Ransomware

Moderation: Ute Lange, Michael Münz
Gast: Alexander Härtel, BSI
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: Mein Name ist Michael Münz. In der heutigen Folge widmen wir uns einem Thema, dass das Bundesamt für Sicherheit in der Informationstechnik in seinem diesjährigen Lagebericht besonders hervorgehoben hat. Dieser Lagebericht ist so etwas wie die jährliche Zusammenfassung über die Bedrohungen im Cyberraum und der Bericht für 2021 ist jetzt in diesen Tagen erschienen. Darin schätzt das BSI die aktuelle Situation als angespannt bis kritisch ein und sagt, dass in Teilbereichen sogar schon Alarmstufe Rot herrsche. Viele Cyberkriminelle seien professioneller geworden und als größte Bedrohung zurzeit werden in diesem Lagebericht Ransomware-Angriffe genannt. Für uns ist das ein Anlass, diesem Thema auf den Grund zu gehen. Wir haben uns dafür einen Experten eingeladen, Alexander Härtel. Von ihm lassen wir uns erklären, was Ransomware eigentlich ist, warum sie so gefährlich ist und natürlich auch, wie wir uns davor schützen können.

Lange: Eine weitere Frage ist: Wo sind wir betroffen als Verbraucher und Verbraucherinnen? Weil die Angriffe häufig nicht mehr nur unmittelbar Einzelpersonen gelten, sondern vermehrt Institutionen und Firmen. Es gibt ein paar aktuelle Beispiele aus den letzten Wochen. Da sind zum Beispiel Schwerin und Witten Opfer geworden und es waren Bürgerämter geschlossen. Einige Zeit lang gab es auch gar keinen Kontakt per Telefon. Die Verwaltungen waren lahmgelegt. Das hieß, man konnte beispielsweise keine Personalausweise, Pässe oder Führerscheine beantragen. Man konnte sich nicht an- oder ummelden, wenn man umgezogen ist. Wir hatten in einer Folge vor Kurzem über den Landkreis Anhalt-Bitterfeld gesprochen. Dort konnten vor einigen Monaten Sozialleistungen nicht ausgezahlt werden, weil die ganzen Systeme blockiert und verschlüsselt und nicht mehr zugänglich waren. Oft dauern die Wiederherstellungen monatelang. Die Technische Universität in Berlin zum Beispiel ist im Frühjahr Opfer eines Angriffs geworden. Vieles ist wiederhergestellt. Aber zum Wintersemester haben vor allem Studierende, die gerade erst anfangen, einige Herausforderungen, weil ihre Studienbescheinigungen sehr spät oder noch gar nicht ausgestellt sind. Ohne die kann man zum Beispiel keine vergünstigten BVG-Tickets kaufen oder beim Vermieter/ Vermieterin nachweisen, dass man Studentin oder Student ist.

Das heißt, wir sind, auch wenn wir nicht direkt Opfer dieser Angriffe sind, mitleidend und unser Alltag kann sich dadurch dramatisch anders gestalten als wir es gewöhnt sind und auch brauchen. Das macht das Thema für uns aus Verbraucherschutzsicht sehr interessant und daher freuen wir uns besonders, Alex, dass du dir heute Zeit genommen hast. Herzlich willkommen!

Münz: Schön, dass du da bist. Wir freuen uns und vielleicht magst du dich erst einmal kurz vorstellen, damit wir dich besser kennenlernen.

Härtel: Ja, sehr gern. Ich bin der Alexander Härtel. Ich bin eingesetzt im BSI in dem Referat, das sich mit der längerfristigen Beobachtung der IT-Sicherheitslage beschäftigt. Dort bin ich in den Teilteam Threat Intelligence. Das ist kein klar umrissener Begriff. Meine Haupttätigkeit ist fokussiert auf den operativen als auch auf den strategischen Teil. Das Operative muss man sich so vorstellen, dass ich versuche, die Cyberkriminellen in Gruppen einzuteilen und auf längere Zeit zu beobachten: Wie gehen die Angreifer vor? Welche Malware setzen sie ein? In welcher Reihenfolge infizieren sie Geräte oder rollen ihre Malware aus? Auf der anderen Seite gibt es die strategische Komponente, dass man versucht, Trends zu erfassen: Wo gehen die Cyberkriminellen zukünftig hin? Was ist die nächste Bedrohung, auf die wir uns vorbereiten sollten, vor der wir warnen sollten? Das Ganze bereiten wir dann für die verschiedenen Adressaten auf – für die Kollegen, die vor Ort beim Betroffenen sind, bis hin zum Bundestag, wenn man uns Fragen stellt, aber auch natürlich für Verbraucherinnen und Verbraucher wie hier.

Münz: Damit wir noch ein bisschen mehr über dich erfahren, erst mal eine Entweder-Oder-Frage: Lieber lebenslang unsichere Passwörter oder lebenslang schlechten Kaffee?

Härtel: Ganz klar den schlechten Kaffee, den kann man noch durch Tee ersetzen. Aber auf schlechte Passwörter ein Leben lang zu setzen, das ist eine ganz schlechte Idee.

Münz: Das heißt, du nutzt einen Passwortmanager, um dich zu sortieren?

Härtel: Auf jeden Fall, sowohl privat als auch beruflich!

Münz: Okay, und jetzt noch mal kurz deinen Weg ins BSI. Hast du dir gedacht, „Beobachtung von Cyberkriminalität, das ist genau das, was ich immer wollte.“, oder war der Weg vielleicht etwas weniger gradlinig?

Härtel: In dem Bereich der Informatik war er gradlinig. Danach wurde es ein bisschen schwerer, bis ich beim Cybercrime angekommen bin. Das Ganze hat mit einem dualen Studium angefangen – angewandte Informatik über drei Jahre. Alle drei Monate bin ich gewechselt zwischen der Arbeit und dem Studium. Dort habe ich in den letzten beiden Semestern meinen Dozenten für IT-Sicherheit kennengelernt, der auch ein Kollege hier im BSI ist. Darüber ist die Verbindung zum BSI entstanden. Mir war relativ früh klar, dass ich in der Privatwirtschaft nicht arbeiten möchte. Daher kam mir die Gelegenheit sehr gelegen. Über seinen Kurs ist mir dann klar geworden, in welche Richtung ich gehen möchte. Ich habe mich daraufhin beim BSI beworben und im Nationalen Cyber-Abwehrzentrum angefangen,

eine Kooperationsplattform mit allen sicherheitsrelevanten Bundesbehörden Deutschlands. Dort war ich in der Geschäftsstelle für anderthalb Jahre. Das kann man sich so vorstellen, dass wirklich jeder IT-sicherheitsrelevante Vorfall der Bundesrepublik in irgendeiner Form über den eigenen Schreibtisch geht. Man sitzt am Puls der Zeit, wenn man so sagen möchte. Vor anderthalb Jahren habe ich mich entschieden, doch in die längerfristige Beobachtung zu gehen und habe mich dann in den Cybercrime-Bereich reingekniet.

Lange: Okay, dann lass uns doch in das Thema von heute, Ransomware, einsteigen. Kannst du uns erklären, was das ist und was Ransomware macht?

Härtel: Man hat es wahrscheinlich immer wieder mal gehört, dass das irgendetwas mit Verschlüsselung zu tun hat. In der Regel ist es in Software-Programmen, was wir als Malware bezeichnen, weil es eine böse Absicht verfolgt. Es soll mit Verschlüsselungsalgorithmen Dateien verschlüsseln, so dass man nicht mehr selbst darauf zugreifen kann. Man muss sie erst entschlüsseln, bevor man sie wieder nutzbar machen kann. Das war bis vor einigen Jahren eher so ein Massenphänomen. Es wurde zum Beispiel per E-Mail verteilt oder auf Webseiten als getrackte Software getarnt und es richtete sich mehr gegen den einzelnen Verbraucher und an die Verbraucherin. Aber die letzten anderthalb bis zwei Jahre hat sich das mehr Richtung Unternehmen entwickelt. Das heißt, die Angreifer fokussieren nicht mehr unbedingt die Einzelperson, sondern die ganze Organisation. Das nennen wir auch Big Game Hunting im Fachjargon, das heißt auf Deutsch Großwildjagd. Es geht also darum, die richtig großen Lösegelder abzufangen. Und wir haben das jetzt auch. Wer die Nachrichten verfolgt, hat gesehen, dass mehrere Millionenbeträge teilweise als Lösegeld von einzelnen Opfern verlangt werden. Das heißt, die Angreifer machen tatsächlich richtig Kasse.

Münz: Das Prinzip ist es, Alex, auf einen Rechner oder in ein System zu gelangen und die Daten zu verschlüsseln und dann zu sagen „Ihr bekommt den Schlüssel, um an eure Daten ranzukommen, erst, wenn ihr uns ein Lösegeld bezahlt habt.“ – bei Privatpersonen oder Unternehmen - da muss man differenzieren. Das ist die Idee hinter diesen Ransomware-Angriffen, richtig?

Härtel: Genau das ist die Idee. Man hält quasi die Daten einer Person als Geisel, wenn man so will.

Münz: Oder eines Unternehmens.

Härtel: Oder eines Unternehmens. Bei dem Trend hin zum Big Game Hunting wurde das noch verschärft die letzten anderthalb Jahre. Das haben wir auch im Lagebericht deutlich betont. Es bleibt nicht bei der Erpressung der Daten, die man quasi als Geisel genommen hat, sondern dass man diese Daten auch vorher gestohlen hat und jetzt damit droht, diese zu veröffentlichen – auch als Daten-Leak bezeichnet.

Lange: Darf ich da noch einmal einhaken? Das heißt, wenn so ein Angreifer oder eine Angreiferin es geschafft hat, in dein System reinzukommen, dann klauen sie, während sie noch dabei sind dich zu erpressen, auch schon Daten und bedrohen dich damit dann

nochmal, um den Druck zu erhöhen; damit du tatsächlich bezahlst, damit sich deine Angst verstärkt. Habe ich das richtig verstanden?

Härtel: Die Reihenfolge ist etwas anders. Man muss sich das so vorstellen: Der Angreifer kommt ins Netzwerk, auf den Rechner, und guckt sich dann meistens in der Regel noch um. Er versucht sich, wenn es ein Unternehmen ist, im Organisations-Network auszubreiten. Bevor die Ransomware verteilt, ausgerollt wird – wenn man jetzt bei Software-Sprache bleibt – stiehlt er die einzelnen Daten und zieht sie ab. Dann lässt er die Verschlüsselung laufen. Dabei wird eine Erpresser-Nachricht platziert auf dem System, die einen darauf hinweist, wie man zum Angreifer Kontakt aufnehmen kann. Dabei wird meistens schon in der Erpresser-Nachricht oder spätestens, wenn man in die Verhandlung einsteigt, die Drohung offenbart, dass mit Daten-Leaks gedroht wird. Die Drohung lässt sich quasi in zwei Teile aufteilen. Man könnte einmal nur für die Datenerpressung Geld verlangen und auch für die Daten-Leaks, einzelne Angreifer machen das auch. Aber die meisten kombinieren das dann, um den Druck beim Betroffenen zu maximieren, damit man wirklich zu der Handlung kommt: „Ich muss jetzt Lösegeld zahlen, um den Schaden zu verringern".

Münz: Am Anfang hatte Ute schon ein paar Beispiele genannt, wo Ransomware genutzt worden ist, um Institutionen oder auch Unternehmen unter Druck zu setzen. Welche Beispiele kannst du nennen, bei denen du sagst, dass das die klassischen Fälle von Ransomware sind, von denen man vielleicht auch schon mal gehört hat durch die Presse oder so.

Härtel: Klassisch sind natürlich die Fälle mit den höchsten Lösegeldern oder die, wo tatsächlich die Betroffenheit deutlich spürbar ist. Diese kommen in die Medien. Im deutschen Bereich werden sich einige wahrscheinlich noch an den Vorfall beim Uniklinikum Düsseldorf, dem UKD, erinnern letztes Jahr; wobei der Fall schon wieder aus den klassischen Fällen herausfällt, da die Angreifer wahrscheinlich nicht die Absicht hatten, das Uniklinikum zu verschlüsseln, sondern die damit in Zusammenhang stehende Universität. Dort ist also eine Verwechslung entstanden. Wenn wir in den letzten Wochen schauen: Anhalt-Bitterfeld war der erste Fall, wo auch ein Katastrophenfall ausgerufen wurde, um schnell reagieren zu können. Oder auch Witten jetzt die letzten Tage, wo auch eine Stadtverwaltung getroffen wurde. Wenn wir in den internationalen Raum gehen, war in den Medien dieses Jahr Colonial Pipeline im Osten der USA als einer der größten Pipeline Betreiber betroffen. In der Folge konnte dann auch zum Beispiel Benzin nicht ausgeliefert werden und die komplette Ostküste hat mehrere Wochen den Atem angehalten. Oder es gab auch den Vorfall vor einigen Monaten mit Kaseya, wo weltweit tausende Unternehmen durch einen einzelnen Angreifer getroffen wurden.

Lange: Du hast ja vorhin schon beschrieben, dass du zwei Aufgabengebiete hast, also operativ und strategisch; nicht nur du, sondern mit deinen Kollegen und Kolleginnen in dem Referat. Welche Rolle spielt denn das BSI in so einem Ransomware-Fall? Habt ihr aktuell Kontakt zu Witten oder Schwerin gehabt zum Beispiel? Ich weiß von einem Gespräch mit deinem Kollegen Dwucet in einer Folge über Düsseldorf. Da war das BSI damals mit einer

mobilen Eingreiftruppe wohl auch da. Aber welche Rolle spielt ihr generell bei dem Thema Ransomware und vor allen Dingen auch bei öffentlichen Einrichtungen – bei systemstützenden Infrastrukturen, für die ihr zuständig seid?

Härtel: Wenn wir es zunächst allgemein betrachten, dann ist das Motto des BSI „Hilfe zur Selbsthilfe“. Das heißt, wir stellen Empfehlungen und auch Schritt-für-Schritt-Anleitungen zur Verfügung, wie man auf einen Angriff reagieren sollte. Das stellen wir jedem Betroffenen, der sich an uns wendet, zur Verfügung. Und dann kommt es darauf an, welche Position der Betroffene einnimmt. Ist es zum Beispiel eine kritische Infrastruktur oder die Bundesverwaltung? Dann greifen wir auch vor Ort ein, wenn der Betroffene das wünscht; mit der mobilen Eingreiftruppe, wie du es genannt hast, unserem Mobile Response Team. Wenn es ein herausragender Vorfall ist und unsere Anwesenheit gewünscht ist, dann unterstützen wir auch vor Ort. Das sind zum Beispiel Incident Handling Personen vor Ort im Krisenstab, die unterstützen oder über einen längeren Zeitraum über remote beraten. Man wird auch von Strafverfolgern hinzugezogen und gibt Beratung für den Wiederaufbau aber auch zum Vorgehen der Angreifer.

Lange: Wir haben jetzt gehört, was alles möglich ist. Wie sieht es denn mit präventiven Empfehlungen aus, die das BSI ausspricht, wo ich mich weiter informieren kann, sowohl als Unternehmen als auch als Verbraucher, um diesem Trend entgegenzuwirken, von dem wir ja schon gesprochen haben?

Härtel: Wir haben für Unternehmen zum Beispiel einen Bericht über Ransomware, wo sowohl präventive als auch reaktive Maßnahmen aufgelistet sind. Aber wir haben auch den umfangreichen Grundschutzkatalog, der auch grundsätzliche IT-Sicherheitsempfehlungen ausspricht. Wir beobachten im Unternehmensumfeld immer wieder, wenn wir zu einem Vorfall gerufen werden, dass es schon immer mal wieder an den Grundlagen hapert. Wenn man sich die schon zur Brust nehmen würde, wie beispielsweise das Netzwerk zu segmentieren, also quasi die Verteidigung in der Tiefe, hätte es ein Angreifer schwerer, nachdem er erfolgreich angedrungen ist. Es ist außerdem wichtig, sich darüber Gedanken zu machen, wie man Ernstfall reagiert: Hat man Backups, die man wieder einspielen kann? Sind diese vom Netzwerk getrennt? Und natürlich gibt es solche grundsätzlichen Maßnahmen wie Patch-Management oder das Sensibilisieren der eigenen Mitarbeiter und Mitarbeiterinnen. Eine der häufigsten Angriffsvarianten ist immer noch über die E-Mail, auf die der Empfänger klickt oder irgendetwas ausführt. Auf der anderen Seite gibt es natürlich den einzelnen Verbraucher oder Verbraucherin: Auch wenn die Angriffe mehr in Richtung Unternehmen gehen, werden immer noch Einzelpersonen direkt zum Ziel von Ransomware. Die wirklich wichtigste Empfehlung, die man als Privatperson umsetzen sollte, ist, Updates getrennt vom Computer aufzubewahren und zwar so, dass man damit wieder von Null starten kann. Also ein Rechner neu aufsetzen, das geht als Privatperson. Da kann man sich auch Hilfe holen. Die Daten sollte man sicher haben.

Münz: Du sagst gerade, dass man Update auf getrennten Rechnern oder getrennten Festplatten haben sollte, aber du meintest Backups auf getrennten Rechnern oder

Festplatten. Und Updates auf der Stelle zu machen, ist das, was wir in jeder Folge mittlerweile predigen. Das heißt, im Prinzip sind die Empfehlungen, die du an Unternehmen hast oder an die IT-Administratoren von Unternehmen oder Institutionen gar nicht so anders als die an die Verbraucherinnen und Verbraucher. Am Ende bleibt für mich immer noch die Erkenntnis, dass der Faktor Mensch eine große Rolle spielt, ob man betroffen ist oder nicht. Ich als Person kann am besten noch mal genau überlegen, ob die E-Mail, die bei mir ankommt, wirklich authentisch ist, und ob ich auf das, was da dranhängt ist, oder auf den Link klicken soll.

Lange: Es war auch eine Nachricht aus dem IT-Bericht, dass der Faktor Mensch eine große Rolle spielt; und zwar, wenn wir das nicht tun. Wir versuchen immer aus den Folgen herauszuholen, was wir machen können. Was betrifft uns eben auch in unserem Alltag? Ich habe jetzt mitgenommen, dass es sich, wie Michael schon gesagt hat, gar nicht so wahnsinnig unterscheidet bei Unternehmen und mir als Privatperson. Ich habe natürlich nicht die IT-Infrastruktur hier zu Hause, die jemand in einem großen Unternehmen hat. Aber es ist wichtig, diese Sorgfalt, diese Vorsicht, diese Skepsis, die wir ja im analogen Leben, wie wir auch häufiger sagen, gegenüber bestimmten Dingen haben, eben auch für das Internet, für digitale Angebote zu entwickeln. Was machst du denn so privat, um deine Infrastruktur zu Hause abzusichern? Also beruflich bist du in einer Behörde, die das alltäglich macht. Aber was hast du für Tipps aus deinem Alltag, die heute unseren Hörerinnen helfen können, sich gegen Ransomware-Attacken zu schützen?

Härtel: Privat sollte man natürlich Updates automatisch einspielen, aber auch die eigenen Daten getrennt auf eine Festplatte als Backup zu sichern – auch das automatisch, falls mal der Rechner so abstürzt. Das ist dann nützlich. Ebenfalls ist ein wesentlicher Punkt, mit den eigenen Daten bewusst umzugehen; zu wissen, wo welche Daten liegen, wo meine persönlichen Daten überall hinterlegt sind. Wie ich ja eingangs erwähnt hatte, werden Ransomware-Angriffe, wenn es um Unternehmen geht, meistens von Daten-Leaks begleitet. Da kann man auch sekundär Betroffener werden, dass die eigenen Daten abfließen. Von daher muss man aus einem bewusst sein, welche Passwörter man da hinterlegt hatte. Ist es wirklich ein einzigartiges Passwort? So sollte es sein. Die Passwörter speichere ich selbst über einen Passwortmanager. Darüber kann man sich Passwörter auch generieren lassen. Dann musss man dann kein Gehirnschmalz hineinstecken. Das sind so die grundsätzlichen Sachen. Wenn man sich einmal diese halbe Stunde bis Stunde genommen hat, sich darüber Gedanken zu machen, wo man eigentlich überall vertreten ist im Internet, dann muss man das nicht noch einmal machen, sondern nur, wenn man einen neuen Dienst nimmt. Dann muss man sich die Minute nehmen und das Passwort in den Passwortmanager eintragen. Dann ist gut. Dieser initiale Schritt ist wichtig, den sollte man auf jeden Fall machen.

Münz: Ich habe noch zwei Sachen, die ich gern von dir wissen würde. Die eine ist über die Leute, die die Ransomware verteilen. Was sind das für Leute? Sie sind im weitesten Sinne Kriminelle. Aber sind es Programmierer? Oder gibt es schon so eine Dienstleistungsstruktur? Wenn ich eine Idee habe, kann ich mir Leute zusammenstellen oder Dienstleistungen bestellen, die mir dabei helfen Ransomware zu verteilen. Sind das Script Kids, die einfach

Langeweile haben und nur schauen wollen, wie gut sie schon sind? Wer steckt denn hinter Ransomware-Angriffen heutzutage?

Härtel: Dienstleistung trifft es tatsächlich sehr gut. So, wie wir es beobachten oder auch wie das Bundeskriminalamt in seinem Jahresbericht dargestellt hat, muss man sich Cybercrime als einen eigenen Wirtschaftszweig vorstellen. Das heißt, dass es für jeden Teil eines Angriffs dort eine Dienstleistung gibt – jemanden, der nur diesen Teilschritt anbietet. Wenn es zum Beispiel um den initialen Angriff geht, gibt es diese sogenannten Access Broker oder Access Services. Das sind Angreifer, die haben sich nur darauf spezialisiert, auf einen Rechner zu kommen, in ein Netzwerk einzudringen und den Zugang dann weiterzuverkaufen. Ein Beispiel: Nehmen wir mal an, dass das BSI mich total frustriert und ich aus dem Behördenleben aussteige. Privatwirtschaft mag ich auch nicht. Dann wäre der logische Schritt, dass ich Cyberkrimineller werde. Die Fähigkeiten habe ich ja aus meinem beruflichen Vorfeld. Ich hätte alle Dienstleistungen da. Ich muss mir die Sachen nur zusammen beziehen und könnte sofort starten mit einem Cyberangriff. Und das ist tatsächlich auch die Realität. Die Cyberkriminellen sind teilweise auch frustrierte Leute, die in ihrem IT-Umfeld nicht die Anerkennung oder die Bezahlung bekommen haben. Die sagen dann, dass sie in dem Feld immerhin mehr Geld kriegen, als wenn sie eine 40-Stunden-Woche bei einem Unternehmen verbringen. Das ist tatsächlich die Realität. Dadurch kommt auch Expertise in den Cybercrime-Bereich rein. Da sind dann auch begabte Programmierer, die uns Verteidigern das Leben schwer machen.

Münz: Wenn ich jetzt tatsächlich betroffen bin – ob jetzt als Unternehmen und Institutionen oder auch als Privatperson: Bezahle ich dann und wann kriege ich meine Daten wieder?

Härtel: Wahrscheinlich nicht! Die Empfehlung des BSI ist es, grundsätzlich kein Lösegeld zu zahlen, weil man nie sicher sein kann, ob man tatsächlich die Daten wieder bekommt. Wenn es um einen Angriff geht, wo auch mit Daten-Leaks gedroht wird, weiß man nicht, ob die Daten nicht vielleicht doch später noch veröffentlicht oder unter der Hand weiterverkauft werden an andere Cyberkriminelle. Als Betroffener kann man das nicht verhindern. Man ist quasi auf das Vertrauen von jemandem angewiesen, der bereit war, einem alles zu verschlüsseln und die Unternehmensgrundlage zu entziehen oder auch die Daten, die einem am Herzen liegen, zu verschlüsseln und für immer unbrauchbar zu machen. Da stellt sich die Frage, ob man demjenigen tatsächlich das Vertrauen entgegenbringen kann und sollte.

Lange: Vorsorge ist besser als das Nachsehen zu haben - sowohl als Unternehmen, Institution oder auch als Privatperson. Ich rekapituliere noch einmal die wichtigsten Tipps. Man kann die offensichtlich nicht oft genug sagen: Updates, sichere Passwörter, nicht mit dem Internet verbundene Backups und vor allen Dingen eine gesunde Portion Skepsis und Vorsicht, wenn man digital unterwegs ist und sich seinen digitalen Alltag möglichst sicher gestalten möchte. Das habe ich jedenfalls mitgenommen. Michael, hast du noch etwas gehört, was wir unseren Hörerinnen am Ende noch mal zusammenfassend präsentieren sollten?

Münz: Nicht bezahlen! Das ist ja tatsächlich so ein Punkt, an dem man wahrscheinlich kommt, wenn man beispielsweise feststellt, dass die Familienfotos der vergangenen zwei Jahrzehnte weg sind oder meine ganzen Passwörter oder was auch immer. Nicht zu bezahlen, nehme ich auch noch als wichtigen Hinweis mit. Alex, gibt es von dir noch irgendetwas, was wir beide jetzt nicht erwähnt haben?

Härtel: Nein, ich würde sagen, das ist gut auf den Punkt gebracht.

Lange: So, dann verabschieden wir dich zu deinem schlechten Kaffee, für den du dich entschieden hast, weil du sichere Passwörter vorziehst. Das ist natürlich aus deiner Sicht und vor allen Dingen aus Sicht des BS wahrscheinlich die bessere Wahl. Und du sagst ja, dass man auf Tee umsteigen kann. Wir haben beim nächsten Mal hier vor unserem Mikro zwei Menschen, die sich genau mit dem auskennen, was man braucht, um erfolgreich Systeme zu hacken. Wir haben nämlich zwei Hacker hier. Ich persönlich bin sehr gespannt, was die aus ihrem Alltag berichten und was wir an Präventionstipps von denen noch mitnehmen können. Wir bedanken uns ganz herzlich, Alex, dass du dir die Zeit genommen hast.

Härtel: Immer gerne.

Münz: Ja, vielen Dank! Super, danke schön!

Lange: Wir hoffen, dass ihr uns alle weiter verfolgt und „Update Verfügbar“ auf euren Plattformen abonniert, damit ihr keine Folge verpasst.

Münz: Und wie immer gilt: Wir freuen uns über Hinweise, Ideen, Anregungen und auch Kritik. Ihr könnt uns kontaktieren über die BSI-Kanäle auf Facebook, Instagram, Twitter oder YouTube oder auch eine E-Mail schicken an bsi@bsi.bund.de. Wir freuen uns auf Post und bis dahin weiterhin alles Gute und bis zur nächsten Folge!

Härtel: Tschüss!

Lange: Ja, bis bald. 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