„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 02, 30.10.2020:

MIRT – Die BSI-Eingreiftruppe erklärt

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

Münz: Update verfügbar – Ein Podcast des BSI.

Lange: Hallo und herzlich willkommen zu der zweiten Ausgabe von „Update verfügbar“, dem BSI Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Und ich bin Michael Münz. Wir melden uns auch in diesem Monat wieder aus dem Bundesamt für Sicherheit in der Informationstechnik in Bonn. Mit unserem Podcast wollen wir aufzeigen, wie man sich in der digitalen und zunehmend vernetzten Welt sicher bewegt.

Lange: Genauso wie man beim Radfahren einen Helm aufsetzt oder beim Autofahren einen Gurt anlegt, kann man auch das Leben in der digitalen Welt einfach absichern. Und wie das geht, erklären wir jeden Monat an praktischen Beispielen.

Münz: Wie beim letzten Mal schon versprochen, haben wir heute einen Gesprächsgast, der uns wirklich spannende Geschichten erzählen will, aber auch ein paar hilfreiche Tipps geben wird. Vorher wollen wir nochmal zurückschauen auf das, was seit der letzten Folge passiert ist. Ute, wie sieht es aus mit deinem Update seit Folge 01?

Lange: Also erst einmal vielen, vielen Dank für die vielen Rückmeldungen, die wir bekommen haben – entweder das BSI direkt oder Michael und ich. Das hat uns total gefreut, dass die erste Folge offensichtlich gut angekommen ist.

Münz: Und war bei den Zuschriften eine dabei, die du besonders hervorheben magst?

Lange: Ach, da war so dies und das. Aber was ich besonders spannend fand, ist, dass in meinem Bekanntenkreis Menschen jetzt offensichtlich ein bisschen aufmerksamer auf das Thema gucken und ich in den Tagen nach der Veröffentlichung die eine oder andere Geschichte erhalten habe, was sich so im Internet alles tut, und wie man sich dagegen schützen kann.

Münz: Dann haben wir ja schon viel erreicht.

Lange: Auf jeden Fall, aber eine fand ich besonders lustig. Du bist ja auch Kaffeetrinker. Stell dir vor, morgens kommst du in die Küche und anstatt, dass das schöne Getränk da durchläuft, siehst du ein Schild: „Ich funktioniere heute nicht, sondern ich möchte erst einmal X-Summe Bitcoins“.

Münz: Da funktioniere ich auch nicht, da möchte ich direkt wieder ins Bett.

Lange: Genau. Also für einen Kaffeejunkie ist das wahrscheinlich die Horrorvorstellung. Aber es ist gar nicht so abwegig. Die Geschichte, die mir geschickt wurde, war ein Bericht über ein Experiment. Da hat sich ein IT-Experte ein Fabrikat gekauft und hat geguckt: „Wie komme ich da rein?“. Und hat dann natürlich mit seinen Kenntnissen relativ schnell Zugang gehabt. Aber was auch ganz spannend war in dem Bericht, war, dass es auch die Nachlässigkeit der Hersteller sein kann, die das nicht richtig absichern. Und so eine Geschichte „Kaffeemaschine erpresst dich am Morgen“ – das ist eine Schlagzeile, die hat mich natürlich sofort angesprochen.

Münz: Verstehe ich. Angesprochen würde ich bei mir nicht sagen, abgeschreckt eher. Aber alles klar: Dann nehme ich weiter die Espressokanne für die Herdplatte. Ich glaube, da kann so viel nicht schief gehen. Nochmal zurück zu den Rückmeldungen: Da haben wir auch noch die Kommentare durchgelesen, die bei Google und YouTube aufgetaucht sind, und auch bei Twitter und Facebook. Das nehmen wir alles gerne auf. Auch Kritik an unserer ersten Folge haben wir uns angeschaut und werden die gerne aufnehmen, um „Update verfügbar“ weiterzuentwickeln.

Lange: Was ist dir denn so an Themen noch untergekommen?

Münz: Naja, ich habe mich gleich ein paar Tage später ertappt gefühlt, weil da kam so eine E-Mail rein. Ich habe ohne nachzudenken auf den erstbesten Link geklickt, der mich angesprochen hat.

Lange: Wie lange hast du letztes Mal darüber gesprochen, dass man genau das nicht machen soll?

Münz: Ja, ich weiß, ich fühlte mich auch ertappt. Aber in diesem Fall fühlte ich mich auch sicher, weil das war der Newsletter des BSI, also der authentische, offizielle, richtige Newsletter des BSI, wo ich dachte, da kann mir nichts passieren. Und außerdem haben die mit Social Engineering genau mein Thema herausgefischt, was ich gerade hatte, nämlich die Top Ten der Phishing-Fallen. Und da konnte ich mich nicht zurückhalten. Für dich wäre aber auch etwas dabei gewesen. Das Thema aus der letzten Folge mit den Deep Fakes war auch drin. Das wird noch einmal anschaulich erklärt. Und weil wir beim letzten Mal ja auch über Datenlecks und den Diebstahl von E-Mail-Adressen gesprochen haben, war da noch eine zweite Geschichte drin, die ich mitnehmen wollte oder hier nochmal kurz ansprechen möchte. In dem Newsletter ging es um einen Hacker, der in San Francisco zu 88 Monaten Haft für 117 Millionen Anmeldedaten von Plattformen wie LinkedIn und Dropbox verurteilt wurde. Er hatte die Daten geklaut. Die Geschichte ist fast eine Staatsaffäre geworden, weil

es um so unterschiedliche Länder ging, die sich beteiligt fühlten. Da kann man sehen, wie eigentlich ein Datendiebstahl auf einmal solche Dimensionen bekommen kann, die man sich vorher eigentlich nicht ausdenken konnte.

Lange: Das passt ganz gut. Wir hatten ja letztes Mal schon angekündigt, dass wir dieses Mal einen Gast dabei haben – jemand, der hier im BSI arbeitet. Der hat also auch mit Datenklau, Erpressung und anderen Sachen zu tun. Und ich bin schon sehr gespannt darauf, was er von seiner Arbeit erzählen kann.

Lange: Ja, das ist doch eine gute Überleitung zu unserem heutigen Gast. Der hat nämlich eine ganze Menge spannende Geschichten mitgebracht. Wen haben wir da?

Münz: Ja, hier bei uns ist Michael Dwucet. Schön, dass Sie da sind und uns aus Ihrer Arbeit erzählen wollen.

Dwucet: Ja, Hallo!

Lange: Sie leiten hier im BSI ein Referat, das sich mit Sicherheitsvorfällen beschäftigt und auch zugleich die Verbindungsstelle zum Nationalen Cyber-Abwehrzentrum ist. Darüber wollen wir natürlich mehr erfahren, deswegen haben wir Sie eingeladen. Herzlich willkommen!

Dwucet: Ja, Dankeschön.

Münz: Und natürlich wollen wir noch aus Ihren Erlebnissen und Erfahrungen wertvolle Tipps ableiten, die im digitalen Alltag Sicherheit geben können.

Lange: Herr Dwucet, Sie sind unter anderem für das Mobile Incident Response Team verantwortlich. Das steht für mobile Eingreif-Truppe für Zwischenfälle, also Sicherheitsvorfälle. Was bedeutet das konkret? Was machen Sie da? Und vor allen Dingen: Für wen machen Sie das?

Dwucet: Das Mobile Incident Response Team, oder auch kurz MIRT, ist ein Team im BSI, was die entsprechende Ausrüstung hat und auch das entsprechende Personal, um bei einem Cyber-Sicherheitsvorfall einem Dritten kompetent helfen zu können. Ich fange erst einmal kurz an zu erzählen, wer diese „Dritte“ sind, denen wir helfen können. Anhand dessen erkläre ich, was wir mit dem Team machen. Also, unsere Zielgruppen, wem wir helfen können, die sind in einem Gesetz definiert, dem sogenannten BSI-Gesetz. Da steht einmal drin, dass wir natürlich für die Bundesverwaltung verantwortlich sind, also den Bundesbehörden helfen können, aber auch den Kritischen Infrastrukturen in Deutschland oder kurz KRITIS, also typische kritische Infrastrukturen wie Krankenhäuser, Energieversorger oder auch andere. Es gibt noch einen weiteren Punkt, wo wir auch helfen dürfen. Das sind die sogenannten herausgehobenen Vorfälle, wo ein Wiederanlauf der Systeme in einem öffentlichen Interesse steht. Ich mache mal ein kurzes Beispiel: Wir haben gerade COVID-19. Vielleicht gibt es einen kleinen Zulieferer für einen zukünftigen Impfstoff, der die kleinen Glasröhrchen oder was auch immer zuliefert. Der ist kein KRITIS und auch

keine Behörde. Aber wenn der jetzt ausfällt, könnte das Auswirkungen haben auf die Impfstoff-Produktion. Und dann wäre natürlich auch ein Wiederanlauf seiner Systeme in einem besonderen öffentlichen Interesse. Und was machen wir jetzt bei diesen Unternehmen oder auch Behörden? Da gibt es eigentlich zwei Punkte: Wenn wir vor Ort kommen und einem helfen, gibt es einmal die Richtung, dass wir versuchen aufzuklären, was passiert ist. Wie kam es zu dem Angriff? Wie kam der Angreifer rein? Was hat er gemacht? Und das zweite ist dann, dass wir versuchen zu helfen, dass die Systeme wieder anlaufen können, also die Wiederherstellung, und was man dabei alles beachten muss. Und teilweise muss man auch abwägen zwischen: „Will ich jetzt genauer herausfinden, was derjenige gemacht hat, der Angreifer im Netzwerk? Was hat er genau gestohlen? Oder steht im Fokus eher „Die Systeme sind so wichtig, die müssen schnell wieder anlaufen!“ und auf dieses ganze Aufklären können wir ein bisschen verzichten. Da fahren wir in der Regel auch vor Ort hin und bringen ganz viel Technik mit. Wir haben eine entsprechende Ausrüstung dabei zum Kopieren der Festplatten, Mobile Server, aber auch sowas wie, gutes Beispiel, Ventilatoren. Wenn wir mal vor Ort fahren, es ist gerade Sommer und wir kriegen nur einen kleinen Raum mit unserer ganzen Technik, dann wird es sehr heiß. Das ist auch so eine Lessons-learned aus früheren Vorfällen, dass wir so etwas auch selbst mitbringen.

Münz: Ich hätte jetzt gedacht, die wären zur Beruhigung der betroffenen Personen, dass die sich unter einen Ventilator stellen können.

Dwucet: Nein, das ist auch immer so der erste Satz vor Ort, den wir sagen müssen: „Keep calm and keep going.“, also ruhig bleiben. Panik hilft auch keinem mehr. Und jetzt mal langsam an den Vorfall herangehen, mal überhaupt einen Überblick verschaffen, ist meistens doch sehr hilfreich.

Lange: Darf ich noch einmal einen Schritt zurückgehen? Bevor Sie da sind: Wie können denn die Behörden oder die Gruppen, für die Sie verantwortlich sind, wie Sie eben geschildert haben, überhaupt mit Ihnen in Kontakt treten? Und, wie erfahren Sie als BSI oder als Team von solchen Vorfällen? Haben die alle Ihre Telefonnummer parat oder einen direkten Draht zu Ihnen?

Dwucet: Also für die, für die wir auch eine Verantwortung haben, die sind natürlich alle bei uns registriert. Die kennen wir. Da gibt es ein Meldeverfahren: Die haben unsere Telefonnummer, oder besser gesagt die Telefonnummer des Nationalen IT-Lagezentrums, das die zentrale Ansprechstelle ist. Dort melden die sich und das Lagezentrum übergibt dann den Vorfall an uns. Das sind so die, die uns kennen. Und bei den anderen ist es meistens so, dass wir noch vor ihnen von dem Vorfall wissen; also dass wir das Problem durch einen Dritten mitgeteilt bekommen haben. Dann treten in der Regel wir auf die jeweiligen Unternehmen zu.

Münz: Viele Ihrer Fälle sind ja vertraulich, gehe ich mal von aus, gerade wenn Regierungsspitzen betroffen sind. Aber vielleicht gibt es trotzdem ein aktuelles Beispiel, aus

dem Sie uns ein bisschen erzählen können, damit wir eine Idee davon bekommen, wo Sie ansetzen, was das für Fälle sind, für die Sie gerufen werden, und wie Sie dann dort vorgehen**.**

Dwucet: Genau. Sie haben es ja angesprochen bei den Einsätzen, wo es vielleicht um APT-Vorfälle geht…

Lange: Bitte! Jetzt muss ich die Abkürzung erklärt haben.

Dwucet: APT, nennt sich Advanced Persistent Threats. Das sind gezielte Angriffe auf Unternehmen oder auch Behörden, wo in der Regel von einem staatlichen Hintergrund ausgegangen wird, also staatliche Spionage und andere Angriffe. Darüber kann ich nicht so öffentlich reden. Was wir im letzten Jahr eigentlich am meisten hatten, sind Vorfälle aus dem Bereich des Cybercrime, wo es vor allem auch um Ransomware-Angriffe geht, also Erpressung und die Verschlüsselung der Systeme. Einer der prominentesten Fälle, den wir dieses Jahr hatten, war der Fall beim Universitätsklinikum Düsseldorf. Der war ja im Sommer in der Presse und wir sind auch vor Ort gewesen, um sie zu unterstützen. Dort wurden die Systeme der Klinik verschlüsselt, weshalb sich das Klinikum ja zeitweise sogar von der Notaufnahme neuer Patienten abmelden musste. In so einem Fall steht natürlich ganz klar der Wiederanlauf der Systeme im Vordergrund. Was wir aber auch relativ häufig erleben: Wenn es um Ransomware geht, um Verschlüsselung, dann ist das Kind erst einmal in den Brunnen gefallen. Die Systeme sind verschlüsselt und jetzt kann ich erst einmal nichts tun, weil Entschlüsseln kann ich in der Regel nicht ohne den Entschlüsselungs-Key. Ich muss also aus den Backups die Daten wiederherstellen.

Münz: Das ist dann also nicht so wie bei der Feuerwehr, die, sobald das Telefon klingelt, rausfahren müssen, um sofort akut irgendetwas zu beenden. Sondern, wie Sie schon gesagt haben: Es hat schon gebrannt und jetzt geht es darum, die Ursache und auch sozusagen die Wiederaufnahme des Betriebs sicherzustellen?

Dwucet: Genau, es ist meistens nicht so wie bei der Feuerwehr. Meistens ist es auch relativ unspektakulär, wie wir anfangen. Also meistens, wenn sich Betriebe bei uns melden oder wir uns bei ihnen melden, telefonieren wir erst einmal oder machen eine Videokonferenz und machen eine kleine Beratung: Was ist passiert? Was kann man jetzt tun? Was sind die ersten Schritte? Wie können wir unterstützen? Um dann, wenn es sich herausstellt, dass es sinnvoll ist, auch vor Ort zu gehen, unsere Sachen zu packen und im BSI die entsprechenden Experten zusammenzusuchen. Wir nehmen auch meistens so ein Mix aus Leuten mit. Also man braucht vor Ort die unterschiedlichsten Rollen. Was wir zum Beispiel haben, ist der Incident-Manager, der ein bisschen mehr in Richtung Management arbeiten muss: die Geschäftsführer und die Sicherheitsverantwortlichen betreuen und den ganzen Vorfall koordinieren. Es gibt darüber hinaus die vielen technischen Experten, die Forensiker und die Malware-Analysten.

Münz: Entschuldigung, was für Analysten?

Dwucet: Schadsoftware-Analysten, die wirklich so eine Schadsoftware bis auf das letzte Byte auseinandernehmen können. Was wir im BSI auch haben, sind Experten aus den ganzen anderen Bereichen und Abteilungen: Experten für Industriesteuerungen, Handys und ganz viele andere Bereiche, auf die wir natürlich auch zurückgreifen können, wenn es denn für den Vorfall notwendig sein sollte.

Lange: Und jetzt muss ich meine Frage vom letzten Mal stellen. Haben Sie so eine Rutsche, einen Notfallpack, oder wie muss ich mir das vorstellen? Sie haben ja schon von Geräten gesprochen, die Sie mitnehmen.

Dwucet: Nein, so eine Rutsche haben wir nicht oder so eine Einsatzstange. Wir fahren meistens auch gar nicht so schnell raus. In der Regel führt man die ersten Gespräche hier aus dem BSI und fährt dann entweder am gleichen Tag, also nachmittags raus, oder am nächsten Vormittag, weil das Kind ja schon in den Brunnen gefallen ist. Gut, bei Ransomware-Fällen ist es ein bisschen eiliger als bei, ich sag mal, Spionage-Vorfällen. Bei denen ist es meistens so, dass der Angreifer schon seit Wochen im Netz ist. Und ob ich innerhalb von einer Stunde, von zwei oder einem Tag reagiere, macht auch keinen großen Unterschied mehr.

Lange: Das heißt, die haben sich dann schon bedient mit dem, was sie suchen, wenn sie in das System eingedrungen sind?

Dwucet: Genau, das kann man ja nicht mehr rückgängig machen, wenn schon Daten abgeflossen und gestohlen sind. Die kann ich nicht einfach so zurückholen. Aber ich kann versuchen, aufzuklären: Was hat der Angreifer gesucht? Was hat er sich mitgenommen? Am Anfang ist meistens nicht klar, was alles passiert ist. Und ich kann auch versuchen, herauszufinden, wie der Angreifer vorgegangen ist. Vielleicht so als Analogie, die ganz gut ist, auch wieder mit COVID-19: Was versucht wird, ist ja immer einen „Patienten Null“ zu finden. Genau das versuchen wir auch, den „Patient Zero“ herauszufinden. Das Gerät, das meistens am auffälligsten ist, wo man die Infektion bemerkt, ist meistens nicht das Gerät, wo der Angreifer reinkam, weil er da nur eine kleine Hintertür gehabt hat. Von der hat er sich weiter vorgearbeitet, bis es irgendwann mal irgendwo im Netzwerk aufgefallen ist. Wir haben meistens das eine System, das wir uns anschauen, analysieren, und wir gucken, was da passiert ist: Wie kam ein Angreifer daraufhin meistens in ein weiteres System im Netzwerk? Und so gehen wir immer weiter, bis wir irgendwann wirklich diesen „Patient Zero“ finden und sagen können: Genau auf dieses System kam der Angreifer in dieses Netzwerk herein. Dann können wir herausfinden, wie er es überhaupt geschafft hat, in dieses System einzudringen von außen.

Lange: Gibt es da so besonders populäre Methoden oder Vorgehensweisen, die Sie erleben?

Dwucet: Wir sehen meistens zwei Methoden, die relativ häufig genutzt werden. Das eine ist, dass einfach Schwachstellen auf nicht gepatchten Systemen genutzt werden.

Münz: Also nicht aktualisierte Systeme?

Dwucet: Genau, also Systeme, für die es schon Aktualisierungen gibt. Die wurden quasi nicht eingespielt und der Angreifer konnte genau dann diese Schwachstelle nutzen, um sich auf das System zu kopieren und diese Hinterstelle oder diese Hintertür auszunutzen. Und ein prominentes Beispiel, was wir dieses Jahr gesehen haben: Es gibt oder es gab eine Schwachstelle in dem Software-Produkt Citrix. Das ist ein Produkt, was viele Unternehmen einsetzen, damit ihre Mitarbeiter remote arbeiten können.

Münz: Aus dem Home-Office Kontext kennt man das, oder?

Dwucet: Genau, das ist im Home-Office Kontext auch sehr verbreitet. Da gab es im Dezember eine Schwachstelle, die auch relativ zeitnah vom Hersteller gepatcht wurde. Unser Computer Emergency Response Team des Bundes, das CERT-Bund, alarmiert heute im Oktober noch eine Vielzahl an Providern, dass sie immer noch Systeme in ihrem Netz von Kunden haben, die nicht aktualisiert sind. Und das ist gerade bei dieser Schwachstelle, sag ich mal, wirklich besonders schlimm, weil wir wissen, dass genau diese Schwachstelle von diesen ganzen Ransomware-Gruppen ausgenutzt wird, um sich Hintertüren auf Systemen zu verschaffen.

Lange: Das ist also fast wie eine Einladung.

Dwucet: Genau, und vor allem kann man über entsprechende Tools, Scanner, auch diese Systeme einfach im Internet finden. Das tun die Angreifer auch. Man lädt die Angreifer förmlich ein, eine Hintertür aufzutun. Und irgendwann, wenn die Angreifer mal so weit sind, dass sie sich auch bewusst sind, dass sie das Unternehmen überhaupt kompromittiert haben. Die haben ja so viele Unternehmen kompromittiert zeitweise, dass sie gar nicht wissen, wo sie anfangen sollen mit Weitermachen, mit Verschlüsselung. Bis sie irgendwann an der Reihe sind, das kann schon Monate später sein nach der ursprünglichen Infektion.

Münz: Das heißt, diejenigen, die diese ganzen Einfallstore finden und über den Weg sich ins System arbeiten, die haben eine Liste von erfolgreichen, also aus ihrer Sicht erfolgreich gefundenen Einfallstoren. Sie arbeiten die dann nach und nach ab. Sie gehen dann rein, also auch manuell, tippen sich da ein. Sie sitzen vor einem Schirm und sorgen dafür, dass sie sich dann irgendwelche Administratorenrechte zum Beispiel besorgen.

Dwucet: Genau. Die gucken, gerade wenn diese Schwachstellen frisch herauskommen, ob man die relativ einfach ausnutzen kann. Sie machen es dann und haben meistens am Anfang so viel Erfolg, dass sie gar nicht alles auf einmal schaffen. Sie arbeiten dann ihre Liste durch. Oder, was auch passiert ist teilweise, dass sie diese Listen verkaufen an andere Kriminelle, um schon mal so Geld zu machen, und die anderen können es dann ausnutzen. So kommen die Angreifer auf das System, schauen sich um und gucken: Wie kriegen sie mehr Rechte? Wie kommen sie von diesem einen System auf andere Systeme im Netzwerk? Dann versuchen sie irgendwann, durchs Netzwerk durch auf den sogenannten Domain Controller zu kommen, wo alles verwaltet wird, wo der Administrator auf dem System alle Rechte hat. Wenn sie das geschafft haben und auch diese Rechte haben, dann dürfen sie alles das im

Netzwerk machen, was auch der Administrator darf. Dann ziehen sie Daten ab in der Regel oder kopieren sie sich weg und verschlüsseln alle Systeme und auch alle Backups auf einmal.

Lange: Und das ist das, was in dem Universitätsklinikum in Düsseldorf auch passiert ist. Da war alles verschlüsselt.

Dwucet: Genau. Die hatten diesen Ransomware-Angriff. Sie hatten Systeme, die verschlüsselt waren. Dann ist natürlich die einzige Möglichkeit, die einem bleibt, Backups wiederherstellen, die es da auch gab. Aber gerade so ein Wiederherstellungsprozess dauert einfach, bis so etwas wieder angelaufen ist. Das ist nicht einfach wie Zuhause: „Mal kurz kopieren!“. Man hat große Datenbanken und andere Systeme. Die müssen alle wieder richtig wieder anlaufen. Das ist schon ein größerer Aufwand, den man betreiben muss, selbst wenn man Backups hat, die auch funktionieren.

Münz: Jetzt haben wir über Patches gesprochen, also Updates, die nicht gemacht worden sind. Es gibt aber wahrscheinlich noch andere Einfallstore, die Hacker nutzen?

Dwucet: Genau. Das Zweite, was auch relativ häufig geschieht, ist sogenanntes Phishing, also das die Angreifer viele, teilweise Millionen, E-Mails versenden an alle möglichen Leute, also wirklich breit gefächert, mit Schadsoftware im Anhang. Das können irgendwelche Word-Dokumente oder andere Dokumente sein, die Sie aufmachen, die da von Ihnen irgendwelche Rechte haben wollen und wo drinsteht „Bitte aktivieren Sie Macros, sodass Sie die Inhalte sehen“. In dem Moment, wo Sie das tun, wird genau diese Schadsoftware ausgeführt und installiert die Hintertür auf Ihrem Rechner.

Münz: Das heißt, dass leider auch der Einzelne sozusagen eine Sicherheitslücke sein kann, wenn er in bestimmten Situationen falsch reagiert.

Dwucet: Genau. Wenn es dem Einzelnen passiert - es kann ja uns allen mal passieren, dass er mal kurz einen schwachen Moment hat oder einfach nicht drüber nachdenkt und dann so eine E-Mail anklickt. Dann ist es passiert. Ich muss dann gucken, wenn es passiert ist, dass ich entsprechend auch reagiere und handle. Es kann jedem passieren und da sollte ich auch offen sein, gerade wenn ich im Unternehmen bin. Ich habe eben erzählt, dass es teilweise danach noch Wochen dauern kann, bis wirklich das ganze Unternehmen angegriffen oder verschlüsselt wird. Und jetzt kann man noch ohne großen Aufwand diese Infektionskette stoppen. Wenn ich jetzt den IT-Support anrufe und sage: „Ich habe diese eine komische E-Mail angeklickt, diesen komischen Anhang. Es ist irgendetwas passiert, aber schau doch mal vorbei“. Dann ist das Schlimmste, was passieren kann, dass der Rechner neu installiert wird und sich neues Passwort gesetzt werden muss. Das war es dann aber auch. Dieses Ausmaß ist natürlich deutlich geringer, als wenn die ganze Firma verschlüsselt ist.

Lange: Das heißt also, ich kann selbst auch dafür sorgen, dass sich das nicht weiterverbreitet, wenn ich meine Nachlässigkeit oder Gutgläubigkeit in dem Moment dieser Datei gegenüber

sofort mitteile und sage: „Hier, den sollten wir isolieren, meinen Rechner, ich hatte da etwas Seltsames drauf“.

Dwucet: Genau. Das ist auch das, was wir auf jeden Fall empfehlen. Da geben wir auch als BSI den Firmen was an die Hand. Wir haben die sogenannte IT-Notfallkarte, die man sich beim BSI herunterladen kann. Das ist so eine verbreitete Karte, wo die Firmen ihre Ansprechpartner vom IT-Support bei IT-Notfällen eintragen können: die Telefonnummer, die E-Mail-Adresse. Auch das Vorgehen ist auf der Karte beschrieben. Man sich das ein bisschen so vorstellen wie eine typische „Hilfe, es brennt!“-Karte, die wir aus jedem Bürogebäude kennen. Die Karte ist für die Mitarbeiter: Wenn mal etwas Komisches passiert ist, soll der Mitarbeiter wissen, was er jetzt überhaupt tun kann, und muss sich nicht überlegen, ob es dem IT-Support oder dem Vorgesetzten genannt werden muss. Damit dann nicht folgt: „Oh nein, dann sage ich es lieber doch keinem“. Das ist dann nämlich die schlechteste Lösung

Münz: Ich sehe ja auch nicht sofort, dass etwas passiert ist. Sie haben das ja beschrieben: Das dauert im Zweifelsfall ein bisschen, bis sich die Auswirkungen von so einer angeklickten Datei dann irgendwie zeigen.

Dwucet: Dann lieber mal melden, weil Sie sind bestimmt nicht der Erste im Unternehmen, der mal so eine E-Mail angeklickt hat. Das passiert allen.

Lange: Wenn ich das jetzt übertrage auf mich als Privatanwenderin: Über Updates, die man regelmäßig machen soll, haben wir in der letzten Ausgabe schon gesprochen. Über Phishing und nicht auf Links klicken, die man nicht kennt, haben wir auch schon gesprochen. Mehr so dein Stichwort, Michael. Sie hatten vorhin aber Backups erwähnt. Also in der Firma gehe ich davon aus, dass man regelmäßige Backups hat – außer Sie erklären mir jetzt das Gegenteil aus Ihrer Erfahrung. Aber was mache ich als Privatperson, damit mir das nicht passiert? Was mache ich, wenn ich zum Beispiel plötzlich einen Rechner habe, der komplett verschlüsselt ist?

Dwucet: Wenn wir zunächst kurz auf die Firma gucken: Ja, die meisten Firmen sollten Backups haben. Gerade bei den Kritischen Infrastrukturen oder in der Bundesverwaltung gibt es entsprechende Vorschriften, Gesetze, dass es sowas geben muss. Aber Backups haben und die auch wiederherstellen können, sind zwei Paar verschiedene Schuhe. Deswegen gibt es zwar manchmal Backups, aber man kann sie nicht wiederherstellen. Darauf gucken auch die Angreifer und auch gerade im privaten Bereich. Ich sag mal so, das typische Backup, das ein Privatanwender hat, ist seine USB-Festplatte. Die klemmt er sich an den Rechner und spielt alle Daten darauf, die er auch auf dem Rechner hat. Wenn sein Rechner mal kaputt ist, dann hat er sie trotzdem noch auf der USB-Festplatte. Wenn Sie jetzt einen Ransomware-Angriff haben und wenn Ihre USB-Festplatte nicht eingesteckt ist und, zum Beispiel, in Ihrem Schrank liegt, kommt der Angreifer da nicht dran. Wenn Sie aber Ihre Festplatte eh die ganze Zeit an Ihrem Rechner angeschlossen lassen und ein Angreifer ist manuell auf Ihrem Rechner drauf, dann kann er natürlich auch alle Daten auf dieser USB-Festplatte verschlüsseln. In diesem Fall ist es kein Backup in dem Sinne, das Ihnen dann auch

hilft und Ihre Daten sicher verwahrt. Das heißt, Sie müssen auch als Privatperson schauen, dass Sie vielleicht Offline-Backups machen und Ihre USB-Festplatte auch hin und wieder mal abstecken.

Münz: Okay. Und ich meine, wir sind ja alle nur Menschen. Und Sie haben ja vorhin auch schon gesagt, dass man bestimmt nicht der Erste im Unternehmen ist, dem so etwas passiert. Wie ist das hier im BSI? Ist Ihnen so etwas schon mal passiert? Kommt das vor?

Dwucet: Im BSI noch nicht, aber privat schon. Da war ich auch schon beim BSI. Man kennt das ja: Man findet ja so einiges bei Versand-Dienstleistern. Ich habe bei einem bestellt, der mit UPS geliefert hat. Ich kriege eigentlich sonst nie etwas mit UPS. Genau in den Tagen habe ich aber auch eine Phishing-E-Mail bekommen, die sich als UPS-Versandbestätigung getarnt hat. Ich war völlig im Trott Zuhause. Ich habe einfach mal daraufgeklickt und da hat das Gehirn erst wieder eingesetzt, als ich Dokument gesehen habe: „Hier bitte Makros aktivieren!“. An einem normalen Tag hätte ich die E-Mail überhaupt nicht geöffnet, sondern hätte sie sofort als Spam erkannt und gelöscht. Aber das ist an diesem Tag im Trott komplett in die Hose gegangen.

Lange: Wie kann man sich denn vor diesem Trott schützen? Was ist da vielleicht ein Tipp? Wir haben alle so Tage, wo wir vielleicht nicht ganz so aufmerksam sind.

Dwucet: Sich gerade vor diesem Trott zu schützen, ist ganz schwierig und auch nicht immer möglich. Wer sich damit vielleicht ein bisschen vertieft befassen will: Es gibt einen sehr guten Vortrag von Linus Neumann. Der heißt „Hirne hacken“, wo dieses, ich sag mal, unterbewusste Tun, was man so macht, genauer erklärt wird, und wie sich das auch auf unsere Büroarbeit auswirkt. Als Beispiel: Wenn Sie morgens aus dem Haus gehen, Ihre Wohnungstür abschließen, ins Auto gehen, dann können Sie sich im Auto in der Regel nicht erinnern an den Moment, als Sie Ihre Wohnungstür abgeschlossen haben. Das ist einfach unterbewusst passiert. Das ist in Ihrem Gehirn auch nicht gespeichert worden. Aber es ist passiert und genauso gilt das in unserem heutigen Alltag für E-Mails anklicken, Anhänge öffnen. Das passiert so regelmäßig, dass unser Gehirn es irgendwann in so einen unterbewussten Teil verschiebt. Es ist sehr schwierig da herauszukommen, deswegen passiert es. Und da hilft, wie gesagt, transparent zu sein und etwas zu tun, bevor es wirklich schlimmer wird.

Münz: Dann nehme ich jetzt mal vier Sachen mit aus unserem Gespräch. Das Eine ist, Updates regelmäßig zu prüfen und durchzuführen. Das Zweite ist die Geschichte mit den Backups, dass ich auch dafür sorge, dass die eben nicht permanent Teil meines Systems sind, sondern auch mal offline sind. Dann ist Phishing – so habe ich es verstanden – so ein Punkt, dass ich bei E-Mails immer prüfe, was ich da eigentlich mache. Und das Letzte ist dann der gesunde Menschenverstand, der letztendlich über allem ein bisschen liegt, mit dem man sich aus schwierigen Situationen dann auch schon mal retten kann.

Dwucet: Genau.

Münz: Vielen Dank, dass Sie da waren.

Lange: Spannende Geschichten. Ich könnte jetzt noch eine Menge mehr darüber hören, aber wir haben noch ein paar andere Themen, die wir heute kurz andeuten wollen.

Münz: Und vielleicht noch der Hinweis, dass wir die Sachen, die Herr Dwucet, jetzt in seinen Ausführungen hatte, auch in den Shownotes verlinkt haben, also auch den Neumann-Vortrag und solche Geschichten. Ich hole jetzt mal kurz Luft, weil wir jetzt ein bisschen in der Situation sind wie bei der Folge 01. Man hört die ganzen schwierigen Geschichten und denkt dann: „Puh, Phishing, Datenklau oder so dramatische Notfälle in Krankenhäusern! Da könnte man meinen, das Internet sei voller Gefahren“.

Lange: Ja, aber ich fand es ganz beruhigend, dass es auch eine ganze Menge Tipps gibt. Herr Dwucet hat ja einige mit uns geteilt, wie man sich in dieser digitalen Welt, die zugegebenermaßen relativ komplex ist und auch nicht immer gleich durchschaubar ist, gut schützen kann. Ich komme nochmal zum Bild vom Anfang – Fahrradfahren mit Helm, Autofahren mit Gurt, genauso braucht es Vorsichtsmaßnahmen im digitalen Alltag. Und da waren jetzt ein paar praktische Tipps dabei, finde ich.

Münz: Ja, das stimmt. Und es gibt ja noch viel mehr Tipps für unfallfreies Surfen beim European Cyber Security Month. Den hatten wir ja schon beim letzten Mal erwähnt. Der läuft noch bis Mitte November. Das ist die jährliche Sensibilisierungskampagne der EU zur Computer- und Netzsicherheit. Das gibt es ganz unterschiedliche Institutionen, die Workshops oder Seminare anbieten. Alle Themen und Termine findet man auf der Webseite des BSI, das diesen Monat auch mitkoordiniert.

Lange: Und wenn die Aktion vorbei ist, dann kommt schon fast unsere nächste Ausgabe von „Update verfügbar“**.**

Münz: Ich dachte, du sagst jetzt Weihnachten.

Lange: Nein, aber Advent. Und in der Vorweihnachtszeit gehen viele Menschen online shoppen. Deswegen haben wir uns für das Thema entschieden in der nächsten Ausgabe, weil es da Einiges zu beachten gibt: „Ist der Shop vertrauenswürdig? Wie bezahle ich am besten sicher?“. Und es gibt noch ein paar andere Fragen, auch bezüglich der Versand-E-Mail: „Habe ich wirklich da bestellt, wo mir jetzt gesagt wird, dass ich bestellt habe. Sollte ich daraufklicken oder nicht?“. Das wollen wir alles in der nächsten Folge besprechen.

Münz: Dann bleibt ja nur noch die Frage, ob ich dann Spekulatius und Glühwein mitbringen soll beim nächsten Mal.

Lange: Vielleicht bekommen wir den aber auch hier vom Gastgeber BSI.

Münz: Okay, gut. Erst einmal vielen Dank bis hierin. Die Shownotes sind voll mit Hinweisen und Links zu dem Gehörten aus dieser Ausgabe.

Lange: Ja, und nochmal der Hinweis, wo man uns hören kann. Spotify, Deezer, iTunes und Google. Abonnieren, liken, weitersagen, gerne reinhören, gerne auch Feedback geben. Wir freuen uns. Erreichen kann man uns über die BSI-Kanäle auf Facebook, Twitter und YouTube. Es gibt auch eine E-Mail-Adresse, die ist auch schon genutzt worden nach der letzten Folge. Die lautet mail@bsi-fuer-buerger.de. Wir freuen uns sehr auf Ihre Post.

Münz: Ja, und bis dahin erst einmal Tschüss aus dem BSI. Vielen Dank fürs Zuhören.

Lange: Ja, bis zum nächsten Mal. Tschüss.

Besuchen Sie uns auch auf:

https://www.bsi-fuer-buerger.de
https://www.facebook.com/bsi.fuer.buerger
https://www.twitter.com/BSI_Presse

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