„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 38, 22.12.2023:

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

Michael Münz: Update verfügbar. Ein Podcast des BSI.

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

Michael Münz: Mein Name ist Michael Münz, und ich begrüße euch zur letzten in 2023 aufgenommenen Folge. Jahresabschluss. Ute, was löst das bei dir aus?

Ute Lange: Also zunächst mal, dass ich das Gefühl habe, das Jahr ist rasant schnell vergangen, und ich kann es kaum fassen. Daher freue ich mich auch auf ein paar ruhige Tage, bevor das nächste Jahr wahrscheinlich noch mehr Fahrt aufnimmt – ist mal so eine Spekulation. Ich habe mir vorgenommen in dieser Zeit ein bisschen weniger digital, mehr analog unterwegs zu sein, das heißt, raus an die frische Luft, rein in meinen zu hohen Bücherstapel und rauf auf meine Yogamatte. Und bei dir so?

Michael Münz: Bei mir ist tatsächlich auch mehr analog und weniger digital, aber anders als du es gemeint hast. Ich habe mir für zwei Wochen einen analogen Synthesizer ausgeliehen, also der hat kein MIDI, kein WLAN. Also falls jemand was sagt, der greift überhaupt keine Daten ab. Da kann ich mir sicher sein, dass der mir nur Zeit raubt und nicht Daten. Aber das soll der ja auch, und lustigerweise musste ich, um den zu bekommen, doch nochmal meinen Personalausweis aus der Tasche holen und den in so eine App halten, damit die Leute auch wissen, wo sie das Gerät hinbringen sollen. Ausweisapp ging da also nicht, aber ja, ansonsten kann ich aber sicher sein, dass das Gerät datensicher ist.

Ute Lange: Okay, vielleicht habt ihr euch ja auch neue Geräte rund um oder zu Weihnachten gegönnt, ausgeliehen, geschenkt, gekauft. Wie ihr die absichert und warum ihr das unbedingt tun solltet, könnt ihr unter anderem in der Folge zu Smart Toys nachhören. Die haben wir, ich glaube, vor dem letzten Weihnachtsfest mal aufgenommen, und die verlinken wir euch nochmal in den Shownotes. Lohnt sich immer, nochmal reinzuhören. Wer jetzt so einen neuen Stapel Geräte hat, sollte sich erstmal in Sicherheit ein bisschen schlau machen.

Michael Münz: Ja, und wenn ihr jetzt denkt, es wäre doch schön, man könnte bei Geräten einfach davon ausgehen, dass sie so ein Mindestmaß an IT-Sicherheit mitbringen, dann

haben wir jetzt hier die richtige Empfehlung für euch, denn mittlerweile gibt es ein Label, mit dem ihr die IT-Sicherheit von Produkten checken könnt.

Ute Lange: Vielleicht habt ihr es ja auch beim vorweihnachtlichen Shoppen schon auf einer Verpackung im Ladenregal gesehen. Falls nicht, dann werdet ihr es nach dieser Folge jedenfalls nicht mehr übersehen sehen. Denn über dieses Label, das IT- oder IT-Sicherheitskennzeichen werden wir heute sprechen. Wo kommt es her? Was sagt es aus? und worauf kann ich mich dabei verlassen, wenn es auf einem Produkt ist?

Michael Münz: Diese Fragen stellen wir doch am besten jemandem, der den Prozess von Anfang an begleitet hat, und wir freuen uns also auf die Antworten von Paul Trinks vom BSI. Schön, dass du da bist, Paul.

Paul Trinks: Hallo zusammen.

Ute Lange: Ja, herzlich willkommen auch von mir! Paul, bevor wir dich jetzt mit Fragen zu diesem neuen Label löchern, sag uns doch mal ganz kurz, was du im BSI genau machst.

Paul Trinks: Ja sehr gerne! Ich bin jetzt seit gut drei Jahren beim BSI und begleite eigentlich von Anfang an auch das Thema IT-Sicherheitskennzeichen bei uns im Haus mit, weil es eben auch für uns als Behörde ein neues Thema ist, und ja, ich freue mich, heute mit euch gemeinsam darüber zu reden.

Michael Münz: Danke dir. Dann fangen wir doch mal ganz vorne an, als du zum BSI kamst. Gab es da schon die Idee dieses IT-Sicherheitskennzeichens, oder habt ihr die da am Anfang entwickelt? Wie war da die Entstehung?

Paul Trinks: Ja, sie war gerade frisch geboren, tatsächlich. Um das IT-Sicherheitskennzeichen zu verstehen, muss man erst mal verstehen, dass es sich beim Verbrauchermarkt, zumindest was das Thema Cybersicherheit angeht, um einen ziemlich unregulierten Markt handelt. Und den hat man sich dann so um die 2019/2020er Jahre mal etwas genauer angeschaut, beispielsweise auch im Rahmen unseres Berichts zum digitalen Verbraucherschutz 2020. Da hatten wir uns mal sechs Produkte relativ wahllos vom Markt genommen und auf Sicherheitslücken getestet. Und wir berichten dann eben in diesem digitalen Verbraucherschutzbericht, dass allein in diesen sechs relativ wahllos gekauften Produkten schon 7.000 Schwachstellen gefunden worden sind, also unterschiedliche Kritikalität. Aber es waren eben tatsächlich 7.000 Stück. Im gleichen zeitlichen Rahmen gab es auch das Digitalbarometer des BSI. Dort hat man Verbraucherinnen und Verbraucher zum Thema Cybercrime befragt, und die haben dann eben angegeben, dass jeder Vierte der Befragten schon mal Opfer von Cybercrime gewesen ist.

Also, das heißt, wir haben gesehen, dass es am Verbrauchermarkt ein Problem mit Cybersicherheit gibt. Das Problem haben auch Verbraucherinnen und Verbraucher selbst erkannt. Die haben wir dann nämlich auch nochmal befragt. Wir haben repräsentative Umfragen gemacht gemeinsam mit dem Bundesministerium des Innern, und dort haben 77,3 Prozent der Befragten damals angegeben, dass sie sich eben beim Kauf von IT-Produkten mehr Informationen zum Thema IT-Sicherheit wünschen. Und genau vor dem Hintergrund haben wir dann eben 2021 entschieden, das IT-Sicherheitskennzeichen einzuführen. Das kam damals aus dem IT-Sicherheitsgesetz 2.0. Der Gesetzgeber hat uns als Behörde damit

beauftragt, dieses IT-Sicherheitskennzeichen einzuführen, um genau dieses Problem zu adressieren, also Transparenz am Verbrauchermarkt zu schaffen und Verbraucherinnen und Verbrauchern Orientierung beim Thema IT-Sicherheit zu geben.

Michael Münz: Du hattest gerade schon ganz am Anfang erwähnt, IoT-, also Internet of Things-Geräte habt ihr da geprüft – also Thermostate, Hauseingangssicherungen, Kameras, solche Dinge. Also, bei uns die Kaffeemaschine kommt immer mal wieder vor oder der Staubsauger.

Ute Lange: ...dein Staubsauger…

Michael Münz: Genau, der Staubsauger. Das sind so die Geräte, die ihr euch damals angeguckt habt, Paul?

Paul Trinks: Genau, also vernetzte Produkte.

Ute Lange: Das heißt, das ist eigentlich für Menschen wie mich, Michael, unsere Hörer und Hörerinnen gedacht, die dadurch eine größere Sicherheit bekommen sollen, wenn sie Produkte kaufen. Wie kommt es denn jetzt auf Geräte drauf? Also, da geht ja nicht einer von euch rum und klebt die überall drauf, und dann ist da ein Siegel drauf oder eben so ein Label.

Michael Münz: Oder macht eine große Shopping-Hall und guckt dann mal.

Ute Lange: Wie ist der Prozess und was steckt dann da drin, wenn das Label drauf ist?

Paul Trinks: Genau! Also, wir erteilen das IT-Sicherheitskennzeichen in sogenannten Produktkategorien. Das heißt, wir als BSI legen Kategorien von Produkten fest, in denen wir das IT-Sicherheitskennzeichen erteilen. Wir haben das Ganze 2021 gestartet für Breitbandrouter und E-Mail- Dienste. Das waren unsere ersten beiden Produkte. Ihr merkt, auch, bei Produkten denkt man jetzt in erster Linie an Sachen, die irgendwie im Regal stehen. Das IT-Sicherheitskennzeichen ist aber tatsächlich auch für digitale Dienste gedacht, also zum Beispiel eben E-Mail-Dienste. Dann haben wir den Anwendungsbereich des Kennzeichens im vergangenen Jahr nochmal ganz massiv erweitert um quasi alle Produkte, die irgendwie IoT und Smart-Home-Home Produkte sind – wir nennen die smarte Verbrauchergeräte. Alles, was in irgendeiner Art und Weise vernetzt ist, kann jetzt auch das IT-Sicherheitskennzeichen bekommen.

So, und jetzt war ja deine Frage, wie man das Kennzeichen bekommt. Es ist so, dass das IT-Sicherheitskennzeichen im Kern ein Herstellerversprechen in die IT-Sicherheit des Produktes ist. Das bedeutet, jede dieser Produktkategorien, die wir haben, ist mit ganz konkreten IT-Sicherheitsanforderungen verknüpft, die wir als BSI an solche Produkte stellen. Und in einem ersten Schritt muss dann der Hersteller selbst prüfen, ob sein Produkt eben diesen Anforderungen entspricht. Das kann er selbst tun, das kann er aber beispielsweise auch durch einen externen Dienstleister tun lassen. Und erst wenn der Hersteller oder Anbieter zu der Feststellung kommt, dass sein Produkt eben unseren Sicherheitsanforderungen entspricht, dann kann er bei uns einen Antrag auf Erteilung des IT-Sicherheitskennzeichens stellen. Und was wir dann im BSI machen, ist eine sogenannte Plausibilitätsprüfung. Das heißt, wir schauen, ob die Angaben, die uns der Hersteller zu dem

Produkt macht, die er uns zu seiner Konformitätsprüfung macht, ob die für uns logisch und nachvollziehbar sind. Wir schauen im Übrigen auch, ob der Hersteller oder das Produkt bei uns aktuell mit einer Schwachstelle bekannt ist. Und erst wenn das alles positiv verlaufen ist – diese Plausibilitätsprüfung positiv verlaufen ist – dann erteilen wir in einem ersten Schritt das IT-Sicherheitskennzeichen.

Das ist auch der Punkt, an dem dann viele Leute uns fragen: „Hey, liebes BSI wollt ihr euch wirklich nur auf so ein Herstellerversprechen verlassen?“ Und genau das tun wir aber nicht, weil das IT-Sicherheitskennzeichen einen noch viel spannenderen Schritt hat. Wir haben nämlich einen nachgelagerten Prozess der Marktaufsicht. Das heißt, jedes Produkt, das ein IT-Sicherheitskennzeichen trägt, wird von uns über die gesamte Laufzeit des Kennzeichens beaufsichtigt. Das heißt, die Kolleginnen und Kollegen nehmen beispielsweise Stichproben vom Markt oder werden anlassbezogen tätig und schauen dann, ob im Produkt wirklich das drin ist, was der Hersteller im Rahmen seiner Herstellererklärung auch zugesichert hat.

Ute Lange: Da würde ich gerne mal nachfragen: Weil du gesagt hast, ihr habt Anforderungen an diese Produkte, die sich um dieses Label bewerben, sag ich mal. Welche Anforderungen zum Beispiel gibt es da, und was habe ich da als Verbraucherin davon? Also, auf was kann ich mich dann verlassen, wenn das nachher draufgeklebt wird?

Paul Trinks: Also ganz wichtig ist erstmal, dass es beim IT-Sicherheitskennzeichen immer um Basisanforderungen geht, also um ganz grundlegende IT-Sicherheitsanforderungen, von denen wir als BSI ohnehin der Meinung sind, dass die eigentlich jedes Produkt einhalten sollte. Und da geht es zum Teil um relativ banale Dinge, also beispielsweise bei IoT-Produkten, dass dort keine universellen Standardpasswörter verwendet werden, weil wir wissen, wenn man dann ein Passwort rausgefunden hat, sind logischerweise auch alle anderen Produkte, die dieses Passwort verwenden, von einem Cyberangriff beispielsweise betroffen. Da geht es aber zum Beispiel auch darum, dass Schnittstellen deaktiviert sind, wenn sie nicht in Verwendung sind, einfach um Einfallstore für solche Cyberangriffe zu minimieren.

Wir stellen aber durchaus auch managementbezogene Anforderungen, also zum Beispiel, dass ein Hersteller einen Mindestsupportzeitraum transparent macht, so dass der Verbraucher, die Verbraucherin, schon zum Zeitpunkt der Kaufentscheidung weiß: Hey, das Produkt bekommt so und so lange Updates. Oder, dass der Hersteller einen Meldeprozess für Schwachstellen hat. Das heißt, Verbraucherinnen und Verbraucher, die das IT-Sicherheitskennzeichen irgendwo an einem Produkt finden, können sich einerseits sicher sein, dass der Hersteller das Produkt eben nach unseren Sicherheitsanforderungen gestaltet hat – Stichwort: Security by Design. Sie können sich aber auch darauf verlassen, dass wir als BSI, als staatliche Stelle, dieses Produkt im Blick behalten.

Michael Münz: Jetzt habe ich mich gefragt: Wenn ich Hersteller bin, dann schicke ich einfach dem BSI ein Tipptopp-Gerät. Die gucken sich das eine Gerät an, und die andere Charge stelle ich dann schon mal ins Regal. Und da ist doch super, dass da das Kennzeichen drauf ist. Also, da gibt's kein Schlupfloch dafür, dass da irgendwie bei euch was ankommt, was aber beim Verbraucher nicht ankommt.

Paul Trinks: Genau dafür haben wir eben diesen Prozess der Marktaufsicht. Ich kann das gerne auch nochmal ein bisschen genauer erklären. Es ist tatsächlich so, dass wir das

Kennzeichen nach erfolgreicher Plausibilitätsprüfung erstmal erteilen. Dann später, sobald das Kennzeichen am Produkt ist, können aber unsere Kolleginnen und Kollegen aus der Marktaufsicht losgehen und beispielsweise Testkäufe machen. Also das heißt, sie können irgendein X-beliebiges Produkt vom Markt kaufen, beispielsweise aus dem Ladenregal, aber auch aus einem Onlineshop, und diese Stichprobe kann dann auch wirklich technisch in der Tiefe untersucht werden und geschaut werden: Ist dort wirklich das drin, was der Hersteller im Rahmen seiner Herstellererklärung zugesichert hat? Diese Marktaufsicht kann aber auch anlassbezogen passieren. Also Beispiel: Ein Verbraucher meldet sich bei uns mit einem Hinweis auf eine Sicherheitslücke, oder beispielsweise auch ein Sicherheitsforscher meldet sich bei uns mit dem Hinweis auf eine Sicherheitslücke. Auch dann kann unsere Marktaufsicht tätig werden und genau dieses konkrete Produkt zur Hand nehmen und schauen: Ist dort das drin, was der Hersteller zugesichert hat?

Ute Lange: Wie lange gilt das denn? Also wie lange ist der Prozess eurer Überwachung, ob das noch alles drin ist, was es verspricht?

Paul Trinks: Das Kennzeichen wird grundsätzlich für zwei Jahre erteilt. Über den Zeitraum hinweg behalten wir auch die Produkte im Blick, und danach kann sich die Hersteller natürlich auf eine Verlängerung bewerben. Also er kann dann seine Herstellererklärung erneuern und für weitere zwei Jahre das Kennzeichen bei uns verlängern. Obwohl man eben sagen muss, genau das ist auch der Grund, warum man sich beim IT-Sicherheitskennzeichen eben für einen etwas anderen oder etwas schmaleren Antragsprozess entschieden hat. Das IT-Sicherheitskennzeichen ist ja relativ niedrigschwellig im Zugang, und dann haben wir eben eine starke nachgelagerte Marktaufsicht, und das macht aus zwei Gründen extrem viel Sinn. Einerseits wissen wir, dass sich die IT-Sicherheit von Produkten eigentlich minütlich verändern kann, also Cyberangriffe entwickeln sich fort. Wir wissen, dass Produkte auch über die gesamte Lebenszeit hinweg von Angriffen betroffen sein können, und genau deshalb macht es Sinn, eben nicht nur zu einem Stichtag irgendwas zu prüfen, sondern Produkte über eine gesamte Laufzeit im Blick zu halten. Im Übrigen sehen wir aber auch, dass die Produktlebenszyklen am Verbrauchermarkt extrem kurz sind. Also Produkte werden eingeführt und haben dann eine Lebenszeit am Markt von zwei, maximal drei Jahren. Also, es ist ein sehr schnelllebiger Markt, und genau darauf haben wir reagiert, indem wir eben den Herstellern mit dem Kennzeichen die Möglichkeit geben, die Produkte in einem Idealfall schon nach unseren Anforderungen zu gestalten, dann relativ einfach das IT-Sicherheitskennzeichen zu bekommen, um dann eben direkt mit dem Kennzeichen am Produkt in den Markt zu starten.

Michael Münz: Genau, rein hypothetisch: Das Gerät ist gekennzeichnet, hat eine Dauer von zwei Jahren, und ich sehe es aber am 734.Tag im Laden stehen, und dann ist vielleicht das Label gar nicht mehr gültig. Das Ding steht aber noch im Regal. Wie kann ich denn überprüfen, ob das noch den Standards entspricht oder ob dieses Label vielleicht gar nicht mehr gültig ist? Also steht da zum Beispiel das Datum drauf, von wann das Label ist? Oder gibt es andere Kennzeichen, an denen ich erkennen kann: Ah ja, da hat das BSI noch ein Auge drauf. Da kann ich mich jetzt beim Kauf drauf verlassen.

Paul Trinks: Das ist eine superspannende Frage, weil das tatsächlich auch etwas ist, was wir beim IT-Sicherheitskennzeichen ein bisschen als Innovation sehen. Also, es ist eben so, dass ganz viele Gütesiegel, Produktkennzeichen, Zertifikate, die wir irgendwie am Markt

kennen, in der Regel zu einem Stichtag X irgendetwas prüfen. Dann kommen die an das Produkt, und dann hat die Produkte in der Regel niemand mehr im Blick. Und das funktioniert aber nicht für IT-Sicherheit, weil sich da die Lage eben ständig verändern kann. Und genau deshalb besteht unser IT-Sicherheitskennzeichen aus zwei verschiedenen Komponenten. Also wir haben einmal das statische Label, das, was man am Produkt findet. Dort ist auch nochmal ganz klar abgebildet: Was ist das Sicherheitsversprechen, was hier hinter dem Kennzeichen steht? Und dann – und das ist das eigentlich Spannende und Innovative am IT-Sicherheitskennzeichen – ist jedes Kennzeichen mit einem QR-Code versehen. Und was wir beim IT-Sicherheitskennzeichen und beim BSI machen: Wir pflegen zu jedem gekennzeichneten Produkt bei uns auf der Website vom BSI eine sogenannte Produktinformationsseite. Und auf dieser Produktinformationsseite finden Verbraucherinnen und Verbraucher ganz transparent aufgelistet: Welche Sicherheitsanforderungen hat der Hersteller hier zugesichert? Ist das Kennzeichen noch gültig? Welche Laufzeit hat das Kennzeichen?

Aber ich hatte vorhin über die Marktaufsicht geredet. Wenn wir jetzt beispielsweise Schwachstellen bei so einem Produkt finden würden, die nicht geschlossen werden können oder die besonders kritisch sind, dann hätten wir auch die Möglichkeit, auf dieser Produktinformationsseite eine Sicherheitsinformation oder einen Hinweis auf das zugehörige Update zu platzieren, sodass Verbraucherinnen und Verbraucher im Supermarkt stehen können oder im Onlineshop unterwegs sind, den QR-Code scannen und dann direkt sehen: Was wird mir hier versprochen von diesem Produkt? Welche Eigenschaften werden mir hier zugesichert? Gibt es aktuelle Hinweise beim BSI auf Schwachstellen? Und das ist eine Dynamik, die wir da reingebracht haben, auf die wir tatsächlich auch sehr stolz sind.

Ute Lange: Hättest du denn noch ein ganz konkretes Beispiel zu solchen Schwachstellen, Paul?

Paul Trinks: Tatsächlich nicht zu Schwachstellen, aber ich kann vielleicht mal erzählen, wie unsere Marktaufsicht arbeitet. Eine konkrete Anforderung, die wir für smarte Verbrauchergeräte stellen, ist beispielsweise das Thema Transparenz von Sensoren. Also Produkte, die das IT-Sicherheitskennzeichen tragen, die müssen gegenüber Verbraucherinnen und Verbrauchern transparent machen, welche Sensoren in so einem Produkt verbaut sind. Und das war ein Learning aus diesem Fall mit der Puppe Cayla. Ich weiß nicht, ob der euch bekannt ist. Da ging es im Prinzip um eine Puppe, und diese Puppe hatte ein Mikrofon verbaut, ohne dass dieses Mikrofon in irgendeiner Art und Weise dokumentiert gewesen ist. Also man wusste als Verbraucherin, Verbraucher schlichtweg nicht, dass in dieser Puppe ein Mikrofon drinsteckt, was imstande ist, im Prinzip Aufnahmen zu fertigen. Und genau deshalb fordern wir beispielsweise beim Kennzeichen auch unter anderem Transparenz beim Thema Sensoren. Und wenn wir jetzt im Rahmen eines Testkaufs so ein Produkt uns anschauen und würden dort sehen, da ist ein Mikrofon drin, von dem uns der Hersteller nichts gesagt hat, was nicht transparent gemacht ist, dann würde genau dieser Marktaufsichtsprozess im Prinzip starten.

Michael Münz: Ja, an die Puppe kann ich mich auch noch sehr gut erinnern, weil wir über die in der Smart-Toys-Folge gesprochen haben, die Ute ganz am Anfang der Folge erwähnt hat. Also hört da noch mal rein. Die Geschichte ist echt gruselig und es ist gut zu wissen, dass da jemand ein Auge draufhat, dass sowas nicht nochmal passiert.

Ute Lange: Du hast eben gerade gesagt, also, wenn euch dann was auffällt, könnt ihr das auf der Seite bekannt geben. Dass ich, wenn ich so ein Produkt habe und ich dieses Label bei mir am Produkt eben auch erkenne und denke, ich will jetzt mal gucken, ist das noch alles in Ordnung? Was sind denn so Schritte, wenn euch so eine Lücke auffällt? Du hast ja vorhin gesagt, ihr habt damals, als ihr darüber nachgedacht habt, sechs Produkte gekauft und 7.000 Schwachstellen gefunden. Also unterschiedlich gravierende, hattest du ja schon erwähnt. Da ist meine Mathematik noch nicht ganz am Ende, was das pro Produkt heißt. Aber was wären denn so klassische Fälle, wo ihr dann einschreitet, und wie geht ihr dann vor? Also wann kommt dann die Information bei mir an? Müssen die Hersteller nicht zunächst was machen? Ist ja deren Verantwortung, denke ich als Verbraucherin, dafür zu sorgen, dass das sicher bleibt.

Paul Trinks: Natürlich, das IT-Sicherheitskennzeichen und das Herstellerversprechen, was damit einhergeht, umfasst natürlich erstmal das Versprechen, dass das Produkt unseren Sicherheitsanforderungen entspricht. Hersteller, die das Kennzeichen tragen, verpflichten sich aber auch zu mehr, beispielsweise dass sie eben das Produkt über die gesamte Laufzeit des Kennzeichens mit Updates versorgen, aber auch das BSI darüber informieren, wenn ihnen bei dem Produkt Schwachstellen bekannt werden. Also dann ist mit dem Kennzeichen durchaus auch eine Meldepflicht verbunden. Also, Hersteller, die das Kennzeichen haben, müssen uns unaufgefordert über Schwachstellen am Produkt informieren und diese auch beheben. Das ist ein ganz wichtiger Punkt. Wenn wir jetzt über solch eine Meldung, aber beispielsweise auch über eine Stichprobe, Hinweise auf eine Sicherheitslücke bekommen bei einem gekennzeichneten Produkt, dann schauen wir uns die natürlich in dem ersten Schritt bei uns im BSI an. Also unsere Kolleginnen und Kollegen aus der Marktaufsicht schauen sich dann die Schwachstelle an, schätzen ein, wie kritisch die ist, und dann gehen die in einem ersten Schritt natürlich auf den Hersteller oder Anbieter zu. Da wird quasi im Gespräch mit dem Hersteller geschaut, wie kann diese Sicherheitslücke geschlossen werden, welchen Zeithorizont hat das, sodass dann der Hersteller oder Dienstanbieter genügend Zeit hat, um genau diese Schwachstelle auch zu schließen. Jetzt kann es natürlich passieren, dass die Schwachstelle entweder besonders kritisch ist, weil sie beispielsweise schon öffentlich bekannt geworden ist, auf anderem Weg. Oder aber der Hersteller – das wird die Minderheit sein – sich beispielsweise weigert, die Schwachstelle zu schließen. Und genau das wäre dann der Moment, wo wir eben diese Sicherheitsinformation auf der Produktinformationsseite platzieren würden.

Michael Münz: Das heißt, ich, wenn ich dann den QR-Code scanne, würde dann dabei gleich sehen: Hier stimmt was nicht mit dem Gerät. Okay, ich weiß nicht Ute, wie das bei dir ist, aber vor meinem geistigen Auge habe ich gerade so ein Labor wie bei James Bond mit Q, wo so fünf Leute in Kitteln an Mobiltelefonen oder irgendwelchen Heizungsthermostaten rumdrehen. Also trifft die schöne Vorstellung zu, ist das so ein Tüftler-Job beim BSI?

Paul Trinks: Mit Sicherheit auch. Es ist so, dass wir tatsächlich auch im Haus einzelne Produkte testen können, wir aber auch ganz, ganz stark natürlich mit externen Dienstleistern und Prüfstellen zusammenarbeiten. Das liegt einfach an der Masse an Produkten, die wir auf lang oder kurz kennzeichnen werden. Das wird man zu einem gewissen Prozentsatz natürlich bei uns im BSI machen können. Das lassen wir aber durchaus auch durch externe Prüfstellen machen.

Michael Münz: Ich würde gerne nochmal ein bisschen zu den Herstellern kommen. Wie war denn so die Resonanz bei Herstellern, als ihr das Kennzeichen vorgestellt habt? Hattet ihr das Gefühl, da gibt's eine große Kooperationsbereitschaft? Ich kann mir ja auch vorstellen, wenn ich mich jetzt als Hersteller an einen bestimmten Standard halte, dass die Entwicklung oder vielleicht auch die Absicherung des Geräts ein bisschen mehr kostet als ursprünglich geplant. Wie ist das da mit den Kosten? Wie ist so die Resonanz bei den Herstellern der Produkte, die ihr euch jetzt anguckt?

Paul Trinks: Man muss natürlich erst mal verstehen, dass das IT-Sicherheitskennzeichen eine freiwillige Maßnahme ist. Das heißt, Hersteller beantragen dieses Kennzeichen aus einer Freiwilligkeit heraus, sodass man natürlich erst mal davon ausgeht, dass das im wesentlichen Hersteller machen werden, die ohnehin schon sehr viel Wert auf das Thema Cybersicherheit und IT-Sicherheit legen. Aber genau das soll das Kennzeichen eben auch bieten. Also, wir haben jetzt ganz viel über Verbraucherinnen und Verbraucher geredet. Natürlich profitieren die enorm vom Kennzeichen, weil es eben Orientierung gibt, weil es Transparenz schafft. Aber gleichermaßen profitieren Hersteller und Anbieter von diesem Kennzeichen, weil die jetzt zum ersten Mal die Möglichkeit bekommen, eben ihre Produkte am Markt hervorzuheben, mit dem Thema Cybersicherheit. Sie bekommen im Prinzip die Möglichkeit, IT-Sicherheit zu einem Kaufargument zu machen. Das ist was, was wir auch unterstützen und was wir befürworten. Wir sind ganz, ganz eng im Austausch mit Herstellern, aber durchaus auch mit Branchenverbänden. Wir bekommen von denjenigen, die das Kennzeichnen schon an ihrem Produkt tragen, sehr, sehr positives Feedback. Ich bin regelmäßig im Austausch mit Herstellern, die mir sagen: „Hey, seitdem wir das Kennzeichen bei uns am Produkt haben, haben wir tolles Kundenfeedback bekommen, haben wir teilweise sogar einen Anstieg in den Verkaufszahlen gesehen.“ Also, das hat durchaus auch Auswirkungen auf das Kaufverhalten von Verbraucherinnen und Verbrauchern. Und insofern geben wir auch unseren Herstellern immer eine kleine Bühne, um sich eben auch mit ihrem Produkt und dem Thema Cybersicherheit zu präsentieren, indem wir beispielsweise auch Veranstaltungen zusammen machen, wo wir dann über das Kennzeichen berichten, aber eben auch Herstellern nochmal quasi ihrer Peergroup, ihrem Gegenüber signalisieren können: Für uns hat das funktioniert, wir haben tolle Erfahrungen mit dem Kennzeichen gemacht. Und genau das wünschen wir uns eigentlich auch.

Ute Lange: Michael hat das ja eben schon angesprochen. Ich bin jetzt wieder Verbraucherin. Das ist ja ein Prozess, da fließt ja Arbeit rein. Diese Arbeit wird Geld kosten und wird das Produkt dann dadurch teurer oder was kann ich da als Verbraucherin erwarten? Also, das ist ja auch immer ein Kaufargument, nicht nur IT-Sicherheit, sondern, wenn die Kosten in die Höhe schießen. Dann ist das für den einen oder anderen vielleicht gar nicht mehr erschwinglich.

Paul Trinks: Dazu haben wir tatsächlich keine Erkenntnisse. Also, wir haben bisher keine Rückmeldung in die Richtung bekommen, dass Produkte teurer dadurch werden, dass sie das IT-Sicherheitskennzeichen tragen. Man muss auch dazu sagen, die Kosten, die für so ein Kennzeichen bei uns, beim BSI entstehen, sind aus unternehmerischer Sicht wirklich überschaubar. Also, das richtet sich ein bisschen nach dem Aufwand, den wir haben. Aber erfahrungsgemäß liegt die Erteilung so eines Kennzeichens in der Bearbeitungsgebühr zwischen 1.000 und 2.000 Euro. Also, das sind wirklich keine astronomischen Summen, über die wir hier reden. Ich war vor kurzem mit Kolleginnen und Kollegen aus den USA im

Gespräch. Die planen nämlich gerade, ein sehr ähnliches Kennzeichen einzuführen, und dort wurde auf eine Studie verwiesen. Die ist vielleicht ein bisschen mit Vorsicht zu genießen, aber in dieser kleinen Studie wurde für den US-Markt zumindest rausgefunden, dass Kundinnen und Kunden bereit sind, bis zu 30 Prozent mehr für ein Produkt zu bezahlen, wenn es eben ein Kennzeichen für Cybersicherheit trägt. Wie gesagt, das würde ich mit Vorsicht genießen, würde ich so auch nicht eins zu eins auf den deutschen Markt übertragen. Aber ich kann mir schon vorstellen, dass Verbraucherinnen und Verbraucher grundsätzlich bereit sind, ein paar Euro mehr zu bezahlen, wenn sie im Gegenzug ein Produkt haben, was eben Mindestanforderungen an die IT-Sicherheit einhält.

Michael Münz: Ja, also ich für meinen Fall kann, glaube ich, sagen, dass ich lieber dann fünf oder zehn Euro mehr bezahlen würde, um dann sicher zu sein, dass mein Gerät dann auch datensicher ist. Aber ich bin ja auch befangen, muss ich an dieser Stelle sagen. Aber wie auch immer, aus Verbrauchersicht finde ich das auf jeden Fall eine gute Idee. Jetzt haben wir schon recht lange darüber gesprochen. Ich glaube, wir haben es hingekriegt, noch gar nicht konkret zu benennen, was für Geräte denn gerade mit so einem Kennzeichen versehen sind. Vielleicht kannst du, Paul, dann ja auch noch ein bisschen in die Zukunft gucken. Also auf welchen Geräten oder auf welchen Diensten werden wir das Kennzeichen künftig auch noch sehen?

Paul Trinks: Ja, sehr gerne. Aktuell arbeiten wir eben genau diesen drei Produktkategorien, von denen ich vorhin schon sprach. Wir haben aktuell Breitbandrouter, E-Mail-Dienste und eben smarte Verbrauchergeräte. Und natürlich wollen wir den Anwendungsbereich des Kennzeichens auch perspektivisch noch ausbauen. Wir decken schon sehr, sehr viel ab. Also, die meisten Verbraucherprodukte, die man physisch im Regal findet, können tatsächlich aktuell schon gekennzeichnet werden, und wir wollen aber genau diese Produktkategorien auch ausbauen. Ich kann dafür das kommende Jahr schon mal ein bisschen spoilern. Also, wir planen beispielsweise für das kommende Jahr noch eine neue Produktkategorie für Videokonferenzsysteme, weil wir auch gemerkt haben, dass das über die Pandemiezeit durchaus ein größeres Thema auch für Verbraucherinnen und Verbraucher geworden ist, eben Videocalls zu machen. Also, dafür wird es im kommenden Jahr voraussichtlich eine Produktkategorie geben. Und wir arbeiten auch an einer Produktkategorie für Smartphones, weil das natürlich das Produkt ist, was Verbraucherinnen und Verbraucher tagtäglich in der Hand haben. Da haben wir jetzt sehr viel Zeit und sehr viel Energie in einen geeigneten Standard gesteckt. Das muss man immer sehen. Also, bevor wir eine neue Produktkategorie einführen, müssen wir natürlich einen entsprechenden Anforderungskatalog, entsprechende Sicherheitsanforderungen haben. Da haben wir jetzt sehr viel Zeit und Arbeit rein investiert, sodass wir im kommenden Jahr voraussichtlich auch die Produktkategorie Smartphones einführen werden.

Michael Münz: Cool, das klingt super! Und noch ein zweiter kleiner Blick in die Zukunft, auch noch mal aus Verbrauchersicht. Wenn ich jetzt zum Beispiel einen Käse kaufe, habe ich drei Käse vor mir liegen. Der eine hat so ein Tierhaltungs-Siegel, der andere ein Ernährungssiegel und der dritte, keine Ahnung, noch irgendwie ein Verpackungssiegel. Und dann stehe ich da, und es gibt jetzt mittlerweile ja so viele – also bei Lebensmitteln – für mich verwirrende Kennzeichnungen, dass ich am Ende ja schon gar nicht mehr weiß: Warte, entscheide ich mich jetzt für dieses, oder wo kommt das eigentlich her, und wer hat diese Siegel eigentlich vergeben? Also angenommen, jemand anderes käme jetzt auch noch auf

die Idee, so eine Gerätekennzeichnung zu entwickeln und darauf zu machen. Denkt ihr dann so: Oh nein, die klauen uns die Idee und verwässern die Intention! Oder seid ihr da eher gelassen mit?

Paul Trinks: Da sind wir tatsächlich eher gelassen. Also, du hast natürlich Recht, wir haben keinen Einfluss darauf, was private Akteure am Markt anbieten. Und wenn private Organisationen auf die Idee kommen, vergleichbare Label einzuführen, dann müssen wir das natürlich hinnehmen. Für das IT-Sicherheitskennzeichen gilt aber: Es ist das staatliche Kennzeichen für IT-Sicherheit. Das wird es auch auf absehbare Zeit bleiben, und da können sich die Verbraucherinnen und Verbraucher auch darauf verlassen, dass wir als herausgebende Stelle oder als kennzeichnende Stelle eben nicht von wirtschaftlichen Interessen geleitet sind, sondern uns geht es um das Thema Sicherheit. Wir sind der Cybersicherheit verpflichtet. Und wir informieren eben auch über diese Produktinformationsseite als unabhängige Stelle über das Produkt, was die Hersteller und Dienstanbieter angeht. Die können sich natürlich bei uns auch ein bisschen stärker darauf verlassen, dass wir auch internationale Entwicklungen im Blick haben. Natürlich behalten wir als Behörde regulatorische Entwicklungen im Blick, internationale Entwicklungen im Blick und würden dann das Kennzeichen eben auch anpassen, wenn das irgendwie geboten ist.

Ute Lange: Ich habe noch eine Frage, vielleicht ist es auch die letzte. Wir sprechen ja auch oft über Fake, also Fake Shops, Deep Fakes. Woran erkenne ich, wenn ich dieses IT-Kennzeichen vom BSI sehe, dass es das echte ist und nicht irgendjemand damit Schabernack getrieben hat?

Paul Trinks: Immer über das Scannen des QR-Codes. Also hier ist tatsächlich der QR-Code der Schlüssel zum Erfolg. Dafür werben wir auch immer: Nicht nur das Kennzeichen angucken, sondern immer auch den QR-Code dazu scannen, weil man eben dann tatsächlich auf eine Website des BSI geleitet wird. Da auch immer mal wieder auf den Link beispielsweise achten, dass es sich da auch wirklich um eine Website des BSI handelt. Das erkennt man an dem Link. Wir stellen im Übrigen auch auf unserer Website eine Liste mit allen gekennzeichneten Produkten zur Verfügung. Also auch über diesen Weg kann man da nochmal querprüfen. Ich will ganz ehrlich sein, auch wir sind nicht vor krimineller Energie geschützt. Natürlich kann es vorkommen, dass jemand zum Beispiel diesen QR-Code missbraucht oder aber auch ohne Berechtigung das Kennzeichen trägt. Das verfolgen wir aber dann auch als Ordnungswidrigkeit. Also die unberechtigte Verwendung des Kennzeichens ist eine Ordnungswidrigkeit, die wir auch als Behörde verfolgen, mit einem Bußgeld von bis zu 500.000 Euro. Also, das sind durchaus auch empfindliche Strafen, die da dahinterstecken. Und beim OR-Code immer auf den Link achten, darauf achten, dass es eine sichere Verbindung zum BSI ist, oder im Zweifelsfall auch mal unseren online verfügbaren Katalog von gekennzeichneten Produkten querprüfen.

Michael Münz: Danke dir, Paul. Also für mich klingt das alles sehr hilfreich. Und ich denke, dass ich künftig auch verstärkt darauf achten werde, dass dieses Kennzeichen auf Geräten drauf ist. Ich finde es auch cool, dass ihr es auf der Seite habt, dass ich im Prinzip auch mal gucken kann, was es denn schon gekennzeichnet. Wenn ich mich mit einer Neuanschaffung befasse, dann kann ich das ja auf dem Weg versuchen anzugehen. Ich glaube, dass wir dir auf jeden Fall locker das Label des kenntnisreichen und angenehmen Podcastgastes

verleihen können. Heute vielen Dank, dass du da warst und mit uns dein Wissen und deine Informationen geteilt hast. Das war super aufschlussreich, danke dir.

Paul Trinks: Sehr gerne, danke euch für die Einladung.

Ute Lange: Ja, danke auch von mir! Das Thema Sicherheit im Netz beschäftigt uns ja nicht nur hier in dem Podcast. Beziehungsweise es beschäftigt uns so viel, weil es so nötig ist, dass wir darüber umfassendes Wissen haben. Und es ist nicht nur unsere gefühlte Wahrheit hier. Wir wollten generell mal wissen, wie viele Menschen eigentlich von Cyberkriminalität betroffen sind und wie Menschen sich darüber informieren und auch schützen. Und Antworten haben wir gefunden, und zwar wo Michael?

Michael Münz: Im Cybersicherheitsmonitor 2023, das ist eine gemeinsame Bürgerbefragung vom BSI und dem Programm „Polizeiliche Kriminalprävention der Länder und des Bundes“, kurz ProPK. Ich habe das mal mit aufgenommen, weil mit Abkürzungen haben wir es ja auch in dieser Folge so ein bisschen gehabt. Diese Befragung bringt Zahlen mit, wo ich sage, auch nach drei Jahren Podcast sind die immer noch nicht beruhigend.

Ute Lange: Nein, über ein Viertel der Befragten, ganz konkret sind es 27 Prozent, haben angegeben, dass sie schon mal von Kriminalität betroffen waren. Etwa jeder fünfte von diesen Betroffenen hat dabei sogar finanziellen Schaden genommen, um sich schützen zu können. Und – das ist die andere Zahl, die wir interessant fanden – es informieren sich außerdem 15 Prozent der Befragten regelmäßig zur Cybersicherheit. Und wenn Ihr diesen Podcast hört, gehört Ihr genau zu diesen 15 Prozent, und dafür danken wir Euch schon mal.

Michael Münz: Auch von mir Danke dafür und eine kleine Bitte im Anschluss. Wir könnten ja dann gemeinsam dafür sorgen, dass diese Zahl 15 Prozent beim nächsten Monitor vielleicht auch ein bisschen höher liegt: Wenn ihr diesen Podcast weiterempfehlt und sich mehr Leute über Cybersicherheit informieren, dann können wir dazu beitragen, dass diese Zahl auf jeden Fall steigt. Weitere Erkenntnisse aus dem Cybersicherheitsmonitor, zum Beispiel zu künstlicher Intelligenz und was die Leute dazu denken oder was sie sich vielleicht auch für Sorgen machen, die könnt ihr jetzt schon im Kurzbericht der Befragung nachlesen. Den Link packen wir auf die Shownotes. Oder wenn ihr sowieso schon auf der Liste nachguckt, welche Geräte gerade ein Kennzeichen haben, auf der Website des BSI findet ihr den auch.

Ute Lange: Und wir greifen uns in den nächsten Folgen immer mal Informationen und vor allen Dingen auch Zahlen heraus, damit wir die mit euch teilen können und euch besser informieren, also damit ihr vielleicht auch euren Bekannten- und Freundeskreis informieren könnt, wie man sich noch besser schützt.

Michael Münz: Zahlen ist übrigens ein super Stichwort. Ich habe gerade nochmal schnell ausgerechnet, wie viele Schwachstellen ein Gerät hat bei sechs zu 7.000: Also jedes Gerät hatte 1.166 Periode sechs Schwachstellen – also, wenn man die Ausgangsrechnung noch mal macht. Aber nichts destotrotz: Falls ihr bis dahin, also bis zur nächsten Folge, in den Monitor geschaut habt, und da sind Fragen oder Themen drin, die euch besonders interessieren, dann sagt uns Bescheid. Schreibt uns! Wir greifen eure Fragen natürlich super gerne hier auf.

Ute Lange: Ja, und schreiben könnt ihr uns über die BSI-Kanäle zum Beispiel auf Facebook, Instagram, X – das früher Twitter hieß – Mastodon sowie YouTube.

Michael Münz: Oder ihr schickt uns einfach eine Mail an: podcast@bsi.bund.de. Wir freuen uns über jede Post, die uns zu „Update verfügbar“ erreicht.

Ute Lange: Wir hören uns wieder im nächsten Monat. Und das wird dann eine Folge, die sich speziell an Eltern richtet. Natürlich können diese Eltern das auch mit ihren Kindern hören, aber es wird um das Thema gehen: Wie kann ich mein Kind im Netz schützen und ihm oder ihr einen sicheren Umgang vermitteln mit dem, was im Netz da draußen alles möglich ist? Wir werden eine Autorin zu Gast haben. Die hat sich mit dem Thema beschäftigt. Sie arbeitet im Schulbereich, kennt sich damit gut aus, erlebt täglich interessante Dinge, würde ich mal sagen. Und sie wird uns berichten, was da so los ist, und vor allen Dingen, welche Tipps sie hat, wie man die Kinder gut vorbereiten und schützen kann, damit sie sicher im Netz unterwegs sind.

Michael Münz: Mehr dazu und warum das auch Erwachsene betrifft, dann in der nächsten Folge.

Ute Lange: Ja, bis dahin likt und folgt „Update verfügbar“ auf euren Podcast-Plattformen. Erzählt es weiter, dass es hier interessante Informationen gibt. Und wir wünschen euch alles Gute bis dahin! Tschüss!