„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 31, 31.05.2023:

Darknet – Die dunkle Seite des Internets

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

Ute Lange: Hallo und herzlich willkommen zu einer neuen Folge von Update Verfügbar. Mein Name ist Ute Lange.

Michael Münz: Mein Name ist Michel Münz und auch von mir ein herzliches Willkommen zur neuen Folge. Ihr könnt dabei zuhören, wie sich bei mir eine richtig große Bildungslücke schließt, weil ich habe endlich jemanden gefunden, der mir alle meine Fragen zum Thema Darknet beantworten kann.

Ute Lange: Ja, aber nicht nur deine, sondern auch die von unseren Hörerinnen und Hörern, die uns ja immer mal wieder ihre Fragen zukommen lassen. Vielen Dank übrigens dafür, dass ihr das macht, und ich habe auch die eine oder andere Frage. Ich hoffe, ich komme bei deinen vielen Fragen dann auch irgendwie noch dazwischen heute.

Michael Münz: Ich will mal nicht so sein. Ich meine, wir arbeiten ja jetzt schon lange gut zusammen. Da darf ich mir auch mal die eine oder andere Frage erlauben, denke ich mal. Aber mal im Ernst, du hast also auch viele Fragen zum Thema Darknet ja?

Ute Lange: Ja, auch eine ganze Menge, weil gefühlt lese ich nahezu täglich darüber, oft über die Straftaten, die offensichtlich da ihr Zuhause gefunden haben. Aber auch unsere Gäste erwähnen es ja immer mal wieder. Ich erinnere mich vor allen Dingen an, das war glaube ich die vorletzte Folge mit Carsten Meywirth vom BKA, der uns einen richtig guten Einblick gegeben hat, vor allen Dingen, was dann polizeilich ermittelt wird in diesem Bereich, und ich finde es wird deswegen höchste Zeit, dass wir bei Update Verfügbar mal Licht in dieses Dunkel bringen.

Michael Münz: Dann würde ich sagen, lass doch gleich starten und unsere Expertin begrüßen in der Hoffnung, dass sie unsere Neugier zum Thema Darknet befriedigen kann. Hallo Jasmin Kreutz, schön, dass du da bist!

Jasmin Kreutz: Hallo zusammen.

Ute Lange: Ja, auch von mir. Hallo Jasmin, schön, dass du dir die Zeit nimmst für uns, unsere Fragen und die von unseren Hörern und Hörerinnen. Bevor wir dich löchern, magst du uns mal kurz erzählen, was du beim BSI machst und wie du dort gelandet bist.

Jasmin Kreutz: Gelandet bin ich nach dem Studium Informatik natürlich, und wo arbeitet man dann besser als in einer Sicherheitsbehörde? Und da bin ich jetzt seit 11 Jahren, seit drei Jahren bin ich bei Sicherheit in den Informationsstrukturen und -diensten. Ja und da beschäftige ich mich jetzt hauptsächlich mit Botnetzen, und deswegen bin ich bei euch, weil Botnetze und Darknet dann nicht so weit auseinander sind.

Ute Lange: Ja schön, warum beschäftigt sich denn das BSI überhaupt mit dem Darknet? Wir haben es ja eher so von der dunklen Seite kennengelernt bisher hier.

Jasmin Kreutz: Nun, das BSI beschäftigt sich in ganz vielen Bereichen mit dem Darknet. Also wir bei Botnetzen beschäftigen uns damit, weil wir müssen natürlich einen guten Überblick haben, welche Malware und Botnetze da draußen kursieren, und wo findet man eher Informationen als an der Quelle?

Ute Lange: Und ich als Privatperson, warum sollte ich zumindest ein Grundwissen über das Darknet haben?

Jasmin Kreuz: Man sollte immer Wissen haben, allein um sich auch ein bisschen schützen zu können. Das Darknet ist Teil des Internets und alle Daten, die man im Internet hat, landen früher oder später auch im Darknet. Man kennt die ganzen Leaks, die da draußen sind, und es ist gut zu wissen, wo die Daten liegen könnten.

Michael Münz: Dann fange ich jetzt mal an und steig ein mit meinen ersten Fragen. Ich würde gerne mal die Begriffe klären. Darknet, das impliziert für mich so ein bisschen, das ist so ein besonderer, abgesicherter Bereich. Aber gleichzeitig denke ich auch so, wenn es Darknet gibt, gibt es auch ein Brightnet, also ein helles Netz, und ist es das, was wir so im Alltag nutzen? Und warum ist das Darknet dunkel? Und gibt es außer dem normalen Netz und dem Darknet noch andere Internetbereiche, die ich vielleicht noch gar nicht erwähnt habe?

Jasmin Kreutz: Hm, ja, also das, was wir alle so als Internet kennen, ist eigentlich, wenn wir bei den Begrifflichkeiten bleiben, das Clear Web. Das sind ungefähr 10 Prozent des Internets, die wir kennen und sehen, und das ist natürlich nicht viel. Das meiste Internet ist das Deep Web, also die 90 Prozent, die dann fehlen, die man so nicht sieht. Da liegen dann die ganzen Datenbanken, Firmen, Infrastrukturen, Dinge, die mit Passwort verschlüsselt sind oder speziell gesichert sind, wo man einfach nicht so dran kommt über Google Suche, und das Darknet ist dann ein Teil des Deep Webs. Da muss man nochmal bestimmte Sicherheitsbedingungen erfüllen, also einen Tor-Browser haben beispielsweise, um darauf zugreifen zu können.

Ute Lange: Jetzt hast du schon gleich so ein Wort benutzt, wo ich gar nicht genau weiß, wofür das steht, Tor-Browser.

Jasmin Kreutz: Also, Tor steht für den The-Onion-Routing, und das ist im Prinzip eine bestimmte Art von Kommunikation, die der Browser macht, wenn man sich einen installiert, ist er ähnlich wie ein Firefox von der Optik her, bietet also alles, was ein normaler Nutzer auch so kennt, hat da aber im Hintergrund ganz viele andere Technik, um Kommunikation aufzunehmen, Technik, die dafür sicher steht, dass man danach anonym bleibt, also relativ anonym. 100 prozentig Anonymität gibt es ja nicht.

Michael Münz: Das heißt, ich benutze einen anderen Browser, der dann sozusagen Zugang zu weiteren Daten hat, die ich mit meinem normalen Browser, den ich im Alltag nutze, nicht bekomme. Richtig?

Jasmin Kreutz: Ja, der Tor-Browser kann aber auch genutzt werden, um normal im Internet zu surfen, wenn man halt anonym bleiben möchte. Er ist dadurch etwas langsamer, weil er dieses Onion-Routing-Prinzip hat, das heißt, dass er über mehrere Notes verbindet, aber dafür hat man die Sicherheit, dass man nicht so einfach nachverfolgt werden kann.

Michael Münz: Das heißt, Notes sind so Knotenpunkte, über die dann die Verbindung läuft und es keine direkte Verbindung von mir und den abgerufenen Daten gibt.

Jasmin Kreutz: Genau, in der Regel sind das drei Notes, entre, middle und excess, und so wird halt sichergestellt, dass kein Knoten an sich die komplette Information hat. Das heißt, wenn irgendwie die Polizei oder Gott weiß wer der böse Übeltäter Informationen von einem Knoten abgreifen kann, dann weiß er halt immer noch nicht sehr viel.

Ute Lange: Das heißt also, wenn ich mich jetzt entscheiden würde, ich möchte im Darknet mal ein bisschen gucken gehen, weil mich das interessiert, da ich sonst nur die anderen 10 Prozent sehe, dann brauche ich erstmal diesen Browser. Und wenn ich dann diesen Browser habe, gebe ich dann, wenn ich zum Beispiel jetzt auch ein Paar dunkle Sachen rausfinden will, URLs wie Waffenhändler24.de, oder was mache ich dann also, wenn ich jetzt wirklich sehr neugierig bin?

Jasmin Kreutz: Also erstmal würde ich raten, nachdem man den Browser installiert hat, die Einstellung prüfen, denn das Darknet ist nicht unbedingt der Ort, wo man fahrlässig mit Sicherheitseinstellungen umgehen sollte. Also gerade Dinge wie der Cache sollten auf jeden Fall gelehrt werden, sobald man die Browser Session beendet, denn man möchte nicht hinterher irgendwelche Bilder, die vielleicht illegal sind, auf seinem Rechner zwischengespeichert haben. Aber wenn man das dann gemacht hat und zufrieden ist mit den Einstellungen, dann öffnet man diesen Browser, stellt die Verbindung her. Das, was du gerade gesagt hast, ist eine typische Clear Web Domain. Im Darknet gibt es onions, die Domains heißen dort onions, die Bestehen aus 16 oder

32 Zeichen oder einer zahlenlange Kombination. So einen sprechenden Namen, wie du ihn gerade gegeben hast, gibt es da einfach nicht.

Michael Münz: Und wie finde ich dann die Sachen, die ich suche? Also, das können ja unterschiedliche Dinge sein, das können Güter sein, es können aber auch Daten sein, oder es können ja aber vielleicht auch Informationen sein, an die ich nicht dran komme aus geografischen Gründen zum Beispiel. Also wie komme ich an Informationen, wenn ich im Darknet bin? Wie finde ich die Inhalte, die ich suche?

Jasmin Kreutz: Auch im Darknet gibt es Suchmaschinen. Ähnlich wie Google beispielsweise gibt es da Torch, das ist die Abkürzung für Tor-Search. Da ist natürlich alles mit viel Werbung gespickt, aber es funktioniert ähnlich. Da gibt man halt ein, was man sucht, und kriegt dann verschiedene Vorschläge, die dann alle mehr oder weniger kryptisch aussehen. Das ist auch der Grund, warum man eigentlich, wenn man nicht genau im Thema ist, kaum etwas findet. Also, man kann sich nicht so vorstellen, man geht da rein, sucht danach, ich sag jetzt mal, Waffenhändler, und findet direkt den zuversichtlichen Waffenshop.

Michael Münz: Jetzt hast du ja gesagt, du interessierst dich für das Darknet, zum Beispiel wegen Malware oder auch Botnetzen, die aufgebaut werden. Kannst du ein bisschen beschreiben, ob du ins Darknet gehst und wie du dich da zurecht findest und wie du dann sozusagen ein Gefühl dafür kriegst, was gerade so an Schadsoftware unterwegs ist?

Jasmin Kreutz: Nun im Darknet wird alles angeboten, was mehr oder weniger nicht angeboten werden sollte. Das heißt, da kann man sich auch Malware zusammenstellen lassen, Dienste zusammenstellen lassen, Angriffe planen, und wenn man dann eine Zeitlang da drin rumsurft, kriegt man schon ein bisschen Gefühl dafür, welche Seiten eher plausibel klingen oder nicht. Man kann natürlich auch ein bisschen vergleichen. Viele machen auch Werbung. Im Darknet gibt es alles, was es im Clear Web auch gibt. Das heißt, da gibt es dann auch Feedbackfunktionen, Bewertungsfunktionen. Da kann man dann auch so ein bisschen recherchieren, ob Sachen stimmen oder nicht stimmen oder weder etwas angekommen ist. So kann man sich halbwegs gut zurechtfinden.

Ute Lange: Wir hatten hier immer noch mal einen anderen Begriff für sichere Verbindung. Ich weiß jetzt nicht, welches Netz, aber das kannst du uns ja beantworten, und zwar VPN, sind jetzt VPN und Darknet Synonyme oder nicht?

Jasmin Kreutz: Nein, sind es nicht. Das VPN kann man nutzen, um im Clear Web zu bleiben. Das kann man auch nutzen zusammen mit Tor, wenn man nochmal eine Stufe sicherer sein würde, also im Prinzip, wenn man es mal ganz einfach erklären will, ist das VPN eine verschlüsselte Kommunikation zwischen zwei Partnern über einen Hop, und das Darknet macht das ganze halt über drei Hops, ist aber zwar verschlüsselt im Sinne von der Hop, der nächste weiß nicht, was kommt, aber die eigentliche Nachricht

ist nicht Ende zu Ende verschlüsselt. Das heißt, wenn man so 100 Prozent sicher sein will, müsste man das auch miteinander verbinden. Man kann ja auch eine VPN nehmen und dann über den Tor vorgehen.

Ute Lange: Also, ich brauche, um ganz sicher zu sein, zum Beispiel, wenn ich im Homeoffice arbeite und den Kontakt mit meiner Firma halten will, eine VPN-Verschlüsselung. Das hatten wir schon öfter, und ich hab im Darknet dann die Möglichkeit, das miteinander zu verknüpfen, nämlich das, was das Darknet bietet. Die drei Hops, und mein VPN-Machen ist dann noch mal extra sicher, und du hast aber vorhin schon gesagt, so ganz anonym geht es vielleicht doch nicht. Wo sind dann noch Herausforderungen? Weil es gibt ja vielleicht Kontexte, in denen ich unbedingt anonym bleiben möchte. Also denken wir an Menschenrechtsaktivisten in Ländern, wo sie durch ihre eigene Regierung gefährdet sind oder so. Das ist ja dann vielleicht auch die hellere Seite dieses Netzes. Wie kann ich denn meine Anonymität, wenn ich in so einer Situation bin, gut absichern?

Jasmin Kreutz: Man selbst hat da wenig Möglichkeiten, das zu machen, denn Tor wählt tatsächlich willkürlich drei Knoten. Die Sache ist mit der Anonymität. Jeder kann potenziell einen Knoten spendieren. Das heißt, auch ich könnte mir hier ein Server hinstellen und könnte sagen, das ist jetzt demnächst ein Tor Knoten, der gewählt werden kann. Das heißt, man ist natürlich nicht sicher, ob der Tor Knoten, über den man jetzt sich einwählt, tatsächlich ein freier ist, der alles nur gute Dinge im Hinterkopf hat, oder ob da vielleicht doch irgendwie jemand hintersteckt, sei es jetzt die Polizei, weil man in einem verfolgten Staat ist, oder sei es vielleicht sogar irgendwie jemand, der Malware macht oder an die Daten herkommen will. Also, da gibt es halt viele Möglichkeiten. Deswegen sage ich, so ganz anonym ist man da auch nicht und ganz sicher auch nicht. Abgesehen von der Anonymität und der Sicherheit gibt es natürlich noch andere Risiken. Ich meine im Darknet gibt es alles das, was es im Clear Web auch gibt, hier diese drive-by-exploits, Man-in-the-Middle Attacken, alles, was man an Angriffen kennt. Auch da sollte man nicht auf irgendwelche Links einfach draufklicken, um mal zu gucken, was dahinter ist. Man muss halt mit sehr, sehr viel, wahrscheinlich noch mit mehr gesunden Menschenverstand agieren, als man es im Clear Web tut.

Michael Münz: Und habt ihr irgendwie eine Zahl, wie viele Leute so im Darknet unterwegs sind? Also, du hattest vorhin gesagt, das Clear Web sind 10 Prozent, und verteilt sich dann die Nutzungszahl auch so? Gibt es da eine Unterscheidung, wie viele Menschen im Darknet unterwegs sind? Sind es mehr oder weniger als im Clear Web?

Jasmin Kreutz: Um einiges weniger, aber ich muss gestehen, richtige Zahlen habe ich nicht parat.

Michael Münz: Okay, aber das ist ja schon mal ein guter Anhaltspunkt zu wissen, dass es nicht da irgendwie eine Party gibt, von der ich noch nichts gehört habe, wo alle anderen sind, außer mir. Das ist schon mal gut so!

Jasmin Kreutz: Tatsächlich ist es sogar extrem schwer, im Darknet irgendwas zu finden, was nicht illegal ist. Also wenn man da beispielsweise mal Suchbegriffe eingibt wie keine Ahnung, Schmuck, Jewelery oder sonst was, man kriegt immer wieder die Seiten, die dann doch eher auf die dunkle Seite tendieren.

Michael Münz: Und kommen wir nochmal zu deiner Arbeit zurück, und das, was dann vielleicht aus dem Darknet ins Clear Web, rüberspringt. Also dort kriegst du dann Hinweise darauf, dass es neue Malware gibt, die zum Beispiel Botnetze zusammenbaut. Also dort prahlen dann vielleicht doch Leute damit, dass sie Datenbanken gehackt haben, und das sind so für dich dann die Anhaltspunkte, wo du weißt, das könnte dann eine potenzielle Gefahr werden für auch Leute, die eigentlich nicht im Darknet sind.

Jasmin Kreutz: Korrekt, aber es geht in beide Richtungen. Es ist auch so, dass die meisten Leaks, die man im öffentlichen sieht, dann irgendwann später oder zeitgleich, sie haben natürlich durch die Veröffentlichung Verzögerungen, auch im Darknet auftauchen. Also Daten gehen eher vom Clear Web ins Darknet als umgekehrt.

Ute Lange: Das heißt also auch, selbst wenn ich noch nie im Darknet war und auch vielleicht nach dieser Folge gar nicht mehr die Neugier hätte, da reingehen zu wollen, könnten dort Daten von mir liegen, weil sie irgendwo anders geleakt wurden und dann dort praktisch zum Kauf angeboten werden. Oder was machen die Menschen im Darknet dann mit meinen Daten?

Jasmin Kreutz: Ja, also, mit Daten wird ganz normal wie mit Gütern auch gehandelt. Es gibt ja, diese schöne Seite, “Have I Been Pwned?, und da kann man halt gucken. Es gibt ja unzählig viele Leaks, weil mittlerweile unzählig viele Dienste im Internet sind, und mit den Daten kann man halt richtig gut Geld machen, und das ist natürlich auch nichts legales. Da will man auch eine gewisse Sicherheit hinter haben, dass man nicht die der Polizei verkauft, und deswegen sind solche Daten, Verkaufsaktionen natürlich auch fast ausschließlich im Darknet.

Michael Münz: Und wenn du sagst, verkauft, dann gibt man sich ja wahrscheinlich nicht das Geld über einen online Bezahldienst mit sechs Buchstaben oder mehr, sondern da gibt es dann andere Dienste, die man benutzt, und da kann man sich auch sicher sein, dass man dann am Ende auch das Geld für die Ware bekommt. Wie funktioniert das dann da bei denen?

Jasmin Kreutz: Also, da wird hauptsächlich mit Crypto-Währung gehandelt, Bitcoins, aber sicher sein, dass man die Ware kriegt, kann man sich eigentlich nicht, wenn wie das Darknet schon sagt, und wie ich auch schon erwähnt habe, da sind eher die schwarzen Schafe unterwegs, muss also wirklich ganz, ganz sorgfältig sein, wenn man da irgendwas erwirbt. Diese Dienste haben natürlich auch keinen Verkäuferschutz

oder so etwas in der Art. Es kann also gut sein, man kauft was, und das Geld ist einfach weg danach, passiert.

Ute Lange: Also, das heißt, selbst in der Gesellschaft, die ich im Darknet finde, muss ich damit rechnen, dass ich dann auch wieder übers Ohr gehauen werde. Das heißt, all das, was du mir jetzt erklärst, führt bei mir dazu, dass ich denke, ach ja, das ist ganz gut, dass ich jetzt weiß, dass ich da nicht rein will. Aber wenn ich nun trotzdem neugieriger sein sollte, was kann mir denn passieren? Reinkommen scheint ja einigermaßen okay. Wie komme ich denn daraus, beziehungsweise weiß ich, ob ich sicher da rauskomme, weil du sagtest, vorhin schon Cache löschen, weil vielleicht illegale Fotos dann auf meinem Rechner sind? Kannst du darauf nochmal eingehen? Was könnte mir denn da im schlimmsten Fall auch noch passieren, was ich nicht möchte?

Jasmin Kreutz: Das waren jetzt sogar zwei Fragen an sich. Zum einen, so schlimm ist das Darknet nicht. Das hat auch durchaus viele positive Aspekte, sind nur für uns in Deutschland halt recht hintergründig, aber natürlich für Leute, die an Informationen kommen wollen, freie Meinung äußern wollen. Da ist das die absolut einzige Chance zu interagieren, wenn man nicht danach durch seinen Staat im Gefängnis landen möchte. Insofern, es gibt wirklich viele gute Methoden oder viele gute Dinge, wofür man das Darknet nutzen kann, auch für Journalisten und Meinungsfreiheit. Die einzige Sache ist nur, weil man so anonym ist, wurde es sehr schnell von der dunklen Seite gekapert, und da hatte ich am Anfang ja schon gesagt, Cache löschen. Denn auch im Darknet gibt es viel Werbung, und wenn man jetzt auf einer Seite ist, wo irgendwie Bildchen von nackten Kindern, also Kinderpornografie gewesen sind, landen die halt auf dem Rechner, und solche Bilder will man nicht haben, denn damit macht man sich auch, wenn man es eigentlich nicht absichtlich runtergeladen hat, ja trotzdem strafbar. Deswegen immer diese Sicherheitskriterien vorher prüfen, dass man keine Daten zwischenspeichert. Natürlich der gesunde Menschenverstand, nicht auf irgendwelche Links draufklicken, die man nicht kennt, möglichst auch nicht auf irgendwelche Webseiten drauf klicken, die man nicht kennt. Das ist natürlich extrem schwer, wenn man sich das erste mal da tummelt und weil die Links einem auch so wenig sagen. Sie sind halt absolut überhaupt nicht sprechend, und ob man da einen Link mit einer drei oder einer vier drin hat, da ist auch die Chance, sich zu verklicken und einen Link zu nehmen, der ähnlich klingt, sehr, sehr einfach. Deswegen sehr viel gesunder Menschenverstand und sehr viel Vorsicht.

Ute Lange: Mhm ja, aber du hast gerade die etwas hellere Seite angesprochen. Da würde ich gerne nochmal ein bisschen drauf eingehen, weil du gesagt hast, in Deutschland brauchen wir das ja nicht, weil wir kommen ja auch so an alle Informationen. Ist das vielleicht eine, ich sage mal, Idee der Gründung, des Darknets gewesen, diese gute Seite, oder wie ist es überhaupt dazu gekommen? Und dass man jede Technologie auf die eine oder die andere Seite anwenden kann, ist klar. Aber

dieses positive würde ich doch ganz gerne nochmal ein bisschen ausführlicher hören von dir.

Jasmin Kreutz: Ja, also tatsächlich ist das Darknet über das NRL, Naval Research Lab ausgesprochen, gegründet worden, und es war tatsächlich dafür da. Es sollte eine Technik sein, die halt Menschen in diesen Ländern, die Zensur sehr stark haben, hilft, das zu umgehen. Ich will nicht sagen, dass dadurch bestimmt auch irgendwelche Hintergedanken waren, von wegen die eigenen Agence irgendwie sichern und da die Kommunikation schützen. Aber die Idee war halt wirklich, den Leuten die Möglichkeit zu geben, ohne irgendwie verfolgt zu werden und Informationen heranzukommen, und das hat es ja geschafft irgendwie.

Michael Münz: Aber ich nehme für mich mit, dass ich für meinen Alltag und auch mit den Informationsbedürfnissen, die ich habe, eigentlich im Darknet nichts zu suchen habe. Es gibt eigentlich kein legalen oder auch rationalen Grund dafür, dass ich mir überlege, ich gucke mal danach, ob ich da nicht noch irgendwie eine schöne Nachrichtenseite finde oder einen tollen Online Shop für neue Schuhe oder Schallplatten.

Jasmin Kreutz: Ja, Nachrichtenseiten findet man da, aber da wir in Deutschland sind, findet man da dieselben Nachrichten, die man bei uns halt auch im Clear Web findet. Tatsächlich hat man keinen Grund, außer der Neugier, da mal reinzuschauen.

Ute Lange: Ich finde das sehr aufschlussreich. Also ich habe jetzt auch so ein bisschen die Schlussfolgerung wie Michael. Das ist für mich als Privatperson und mit meinen Informationen und vielleicht auch Interessen kein Grund gibt, da reinzugehen. Ich weiß jetzt auch, warum ich es vielleicht lieber nicht tue, weil ich mich gar nicht gut genug auskennen würde, um diese ganzen Gefahren, die du erwähnt hast, so zu umgehen, dass ich nicht hinterher vielleicht bei Carsten Meywirth und seinem Team auf irgendeiner Liste stande und man mich weiterhin polizeilich ermittelt, weil ich unwissentlich was eingesammelt habe, was ich gar nicht haben wollte. Also deswegen aus meiner Sicht ganz herzlichen Dank, dass du dir heute die Zeit genommen hast und uns da so ein Licht in dieses Dunkel gegeben hast. Das waren auch einige der Fragen unserer Hörer und Hörerinnen, die hoffentlich hiermit dann beantwortet sind. Michael, hast du noch ein weiteres Resümee der heutigen Folge?

Michael Münz: Also, bei mir fügen sich diese ganzen Puzzleteile, die ich vorher hatte, jetzt echt ganz gut zusammen, also die Bestandteile des Internets, dann, wie ich bestimmte Bereiche besuchen kann, aber dann auch im Darknet, so ein bisschen die, ich nenne es jetzt mal Nutzerführung, also wie man da an die Informationen kommt und gleichzeitig auch wissend, dass es für mich eigentlich keinen Grund gibt, dort hineinzugehen. Von daher auch von mir, Jasmin vielen Dank dafür! Das war jetzt wirklich so Puzzleteile zusammen und da, wo es fehlt, hast du jetzt die ergänzenden Stücke noch eingesetzt. Super, danke dir dafür, und für euch, die ihr uns jeden Monat

einschaltet, waren hoffentlich auch ein paar relevante Infos dabei, also auch im Namen unserer Hörerinnen und Hörer. Vielen dank, Jasmin!

Jasmin Kreutz: Gerne.

Ute Lange: Ja, und in den kommenden Folgen werden wir weitere Fragen von euch aufgreifen. Wenn ihr noch eine stellen möchtet, dann schreibt uns gerne. Kontaktiert uns über die BSI Kanäle auf Facebook, Instagram, Twitter oder YouTube.

Michael Münz: Oder schickt uns eine Mail an die Adresse Podcast@bsi.bund.de, wir freuen uns immer über eure Posts.

Ute Lange: Ja, und weil jetzt langsam die Ferienzeit naht, kann es auch gerne Urlaubsspass von euch sein. Wir würden gerne wissen, wo ihr in diesem Sommer Update Verfügbar hört: auf eurem Balkon, am Strand, im Auto. Vielleicht habt ihr ein Segelschiff, mit dem ihr unterwegs seid.

Michael Münz: Oder ihr steht am Flughafen rum und wartet und euer Handy Akku verabschiedet sich. Da habe ich letztens noch was erfahren, was ich hier noch gerne teilen möchte, nämlich es gibt ja an Flughäfen manchmal diese Ladestation, wo so Kabel mit unterschiedlichen Anschlüssen rausgucken. Da sollte man sein Handy nicht dran anschließen, weil das Ding könnte im schlimmsten Fall nicht nur Strom liefern, sondern gleichzeitig auch Schadeware auf das Handy laden oder eben auch Daten abziehen, weil das Kabel eben für Strom und Daten Kommunikation dient. Ich hatte da eine Meldung des FBI gesehen, dass davor warnt, diese Stationen an Flughäfen zu nutzen, und wird das künftig auch nicht mehr tun, wobei ich es natürlich vorher auch schon mal gemacht habe. Aber naja, dass so ein kleiner Urlaubstipp von mir an dieser Stelle.

Ute Lange: Ja, dankeschön, ich war kürzlich unterwegs und habe es tatsächlich genutzt. Ich überlege mir, ob es noch mal so eine gute Idee ist. Wie man sonst seinen digitalen Urlaub absichern kann. Wenn ihr denn jetzt kurz davor seid, Koffer zu packen, könnt ihr unsere Folge 23 nachhören, da haben wir schon mal ausführlicher darüber gesprochen und auch über die vom BSI erstellte Checkliste IT-Sicherheit für Urlauber und Urlauberin. Die verlinken wir euch einfach nochmal in den Shownotes.

Michael Münz: Ich finde es immer noch verrückt, dass man vor dem Sommer jetzt auch solche Sachen sagen muss und es nicht mehr reicht, Sonnenmilch und Mückenschutz einzupacken. Aber ja, ich glaube, das ist der digitale Alltag, in dem wir alle angekommen sind und für den wir euch dann auch sicher machen wollen. Wir wünschen euch einen schönen Start in den Sommer und hören uns nächsten Monat wieder. Bis dahin folgt oder liket uns auf euren Podcast Plattformen, damit ihr auch im Urlaub nicht auf uns verzichten müsst. Macht's gut und bis bald!

Ute Lange: Ja, tschüß und genießt die Sonne!

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