

## „Update Verfügbar – ein Podcast des BSI“

### **Transkription für Folge 11, 18.08.2021:**

Cyber-Sicherheit für die Bundestagswahl 2021

*Moderation: Ute Lange, Michael Münz*

*Gast: Anders Kölligan, BSI*

*Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)*



---

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

**Münz:** Mein Name ist Michael Münz. Wir melden uns heute aus dem Home-Office mit einer Sonderausgabe von „Update verfügbar“, denn für uns alle steht ein großes Update an – die Bundestagswahl am Sonntag, den 26. September. Eine der Institutionen, die für einen ordnungsgemäßen und vor allem sicheren Ablauf der Wahl sorgt, ist das Bundesamt für Sicherheit in der Informationstechnik. Darüber, was das BSI im Rahmen der Bundestagswahl macht, sprechen wir heute mit Anders Kölligan.

**Lange:** Ja, herzlich willkommen Anders! Schön, dass du dir Zeit nimmst. Wo arbeitest du im BSI? Und was macht ihr da?

**Kölligan:** Erst einmal sehr schön, dass ich heute hier sein kann! Vielen Dank, dass ich hier im Podcast mitmachen kann! Mein Name wurde schon mehrfach genannt, aber ihr habt noch nicht gesagt, in welchem Referat ich tätig bin. Das ist das Referat OC 18 und „O-C“ steht für operative Cyber-Sicherheit. Wir beschäftigen uns mit Sicherheit im Internet, in Infrastrukturen und Diensten. Unter diese Internetdienste fallen auch die sozialen Netzwerke. Da sind wir natürlich auch in der Wahlabsicherung beschäftigt.

**Münz:** Da würde ich gern einhaken, weil für mich ist eine Wahl erst einmal ein Zettel und Stift. Ich überlege in der Wahlkabine – nachdem ich vorher einen Brief bekommen habe, dass ich dahinkommen soll, was ich wähle. Wie genau setzt das BSI da an, weil wahrnehmen tue ich das in dem Moment der Wahl ja nicht?

**Kölligan:** Ja, das ist richtig. Du hast es auch schon richtig gesagt: Ich überlege mir vorher, was ich wählen werde. Da ist auch schon ein Teil, bei dem das BSI durchaus beteiligt wird. Gerade die sozialen Netzwerke sind da auch ganz wichtig. Wen wähle ich denn am Ende und wie kommt diese Meinung von mir zustande, dass das die Richtigen sind, die ich da wähle? Wir sind eigentlich im Vorfeld schon damit beschäftigt, dass genau dieser Meinungsbildungsprozess reibungslos ablaufen kann. Das heißt, wir setzen uns mit den sozialen Netzwerken zusammen und sorgen dafür, dass Politikerinnen und Politiker und die verschiedenen Parteien ihre Informationen, ihre Parteiprogramme, so austragen können, wie

sie möchten, und dass das nicht in irgendeiner Weise manipuliert werden kann. Abgesehen davon gibt es natürlich nicht nur diesen analogen Prozess auf Papier, sondern es gibt dazu ja auch noch die Schnellmeldungen und Hochrechnungen, die tatsächlich auch auf digitalem Wege kommuniziert werden. Aber du hast natürlich Recht: Der amtliche Teil der Wahl findet vollständig auf Papier statt und unterliegt im Prinzip keinen großen digitalen Einflüssen. Das heißt, wir Wählerinnen und Wähler werfen unsere Wahlzettel ein oder schicken die per Briefwahl ab. Die werden dann von Menschen ausgezählt. Diese Menschen notieren diese Ergebnisse dann auch auf Papier. Es soll alles nachvollziehbar sein und auf Papier vorliegen. Am Ende der Wahl findet dann die Stimmenaushölung statt. Dieses amtliche Endergebnis liegt tatsächlich erst nach Wochen vor. Das dauert einfach so lange, weil das ein physikalischer, ein analoger Prozess ist.

**Münz:** Okay! Das hat also eine technische Komponente, was ihr macht. Ihr guckt, dass Parteien ihre Informationen technisch einwandfrei zum Beispiel in sozialen Netzwerken übermitteln können. Was kann denn an der Stelle schiefgehen, dass das nicht mehr der Fall ist, dass ihr eingreifen müsstet?

**Kölligan:** Ja, da kann eigentlich relativ viel schiefgehen. Deswegen halten wir auch immer dazu an, dass die Leute ihre Accounts sicher machen, und dass die eine kurze Zeit investieren, um die Empfehlungen des BSI umzusetzen. Da gibt es eine vielfältige Palette an Angriffsmöglichkeiten, was da schiefgehen könnte. Es könnte sich zum Beispiel jemand als eine von diesen Parteien ausgeben und in deren Namen irgendwelchen Unsinn verbreiten. Natürlich kann man sich auch als kandidierende Person ausgeben und in deren Namen falsche Informationen verbreiten. Es ist tatsächlich möglich, dass diese Accounts gehackt sind, gerade wenn diese Sicherheitseinstellungen nicht so sind, wie das BSI sie empfiehlt. Immer wenn so etwas passiert, dann greifen wir ein zusammen mit den sozialen Netzwerken und können in den meisten Fällen sehr schnell helfen.

**Lange:** Wie helfst ihr denn konkret, wenn so etwas passiert? Hast du ein Beispiel?

**Kölligan:** Wenn zum Beispiel so ein Account gehackt wurde, ist es unsere Hauptaufgabe, zu helfen. Wir sind die zentrale Anlaufstelle. Das heißt, wir versuchen möglichst vorher – auch schon vor der Wahl – dafür zu sorgen, dass die Parteien und die Kandidierenden alle wissen, dass sie sich im Zweifelsfall an das BSI wenden können, auch wenn Sachen in sozialen Netzwerken passieren. Wir haben die direkten Kommunikationskanäle zu den sozialen Netzwerken. Normalerweise läuft das dann wesentlich schneller, als wenn die das über die Plattformen selbst lösen. Das kann man natürlich auch machen, das funktioniert auch. Aber wir können noch einmal gucken, wer das wirklich ist. Wir checken das noch einmal gegen und das können wir dann direkt an die sozialen Netzwerke verteilen. Wir haben da 24/7-Kontakte. Dann reagieren die auch innerhalb von Minuten darauf und können erste Hilfe einleiten. Eventuell können wir auch selbst schon irgendetwas tun, um den Betroffenen dabei zu helfen.

**Münz:** Das heißt, im Wesentlichen sind die Kandidierenden ja dann genauso angehalten, so zu handeln, wie wir es auch im Podcast eigentlich für Privatpersonen propagieren: sichere

Passwörter, nicht auf jeden Phishing-Versuch gleich reagieren; sondern sich vielleicht anzuschauen, was da ankommt, ob man die Adresse kennt. Das sind im Wesentlichen die gängigen Ratschläge, die ihr dann auch den Kandidierenden gebt? In welcher Form übermittelt ihr das? Habt ihr für die auch speziell Informationsmaterial, das ihr denen zur Verfügung stellt?

**Kölligan:** Ich antworte einfach mal auf die zweite Frage zuerst. Ja, wir sammeln Informationsmaterialien auch von den sozialen Netzwerken, damit die diese auch wirklich für die entsprechende Plattform, die sie dann nutzen, vorfinden können. Wir sammeln die auf einer Webseite für Kandidierende, die ist auch im Internet zu finden. Wir haben außerdem weitere Informationsmaterialien, die zum Beispiel im Intranet des Bundestages veröffentlicht werden. Wir führen auch Informationsveranstaltungen für Mitglieder des Bundestages durch. Wir haben verschiedene Kanäle, wie wir das dann möglichst heraustragen. Wir schreiben auch die Generalsekretärinnen der Parteien an und hoffen, dass die die Informationen, die wir haben, an ihre Mitglieder weitertragen. Wir versuchen im Großen und Ganzen diese Sensibilisierung hinzubekommen, dass Accountsicherheit, IT-Sicherheit, wichtig ist. Und wie du schon gesagt hast: Das fängt bei Phishing an, mit E-Mail Accounts. Es geht wirklich so weiter. Es zieht sich halt so durch!

**Lange:** Wie nachgefragt ist denn das Angebot jetzt so kurz vor der Wahl oder ist der Run auf das Material schon vor einigen Monaten gewesen?

**Kölligan:** Ich denke der Run auf das Material findet tatsächlich immer dann statt, wenn wir neues Material haben. Ich glaube, die Nachfrage ist zumindest nach meinem Gefühl sehr groß. Die eben angesprochenen Informationsveranstaltungen waren mit über 100 Teilnehmerinnen sehr gut besucht. Die letzte Veranstaltung hatte einiges an Andrang erlebt. Wir sehen auch, dass diese Informationsdokumente rege heruntergeladen werden. Wir gehen davon aus, dass die Nachfrage besteht und deswegen auch schon einiges an Sensibilisierung stattgefunden haben muss. Wir sind immer glücklich, wenn wir unsere Informationen an den Mann oder an die Frau bringen, wo sie hingehören.

**Münz:** Arbeitet ihr mit anderen Institutionen zusammen, die mit der Wahl beschäftigt sind und bei der Vorbereitung beitragen? Funktioniert auch die Kommunikation in diese Richtung?

**Kölligan:** Auf jeden Fall! Wir haben im Vorfeld der Wahl mit dem Innenministerium und auch mit dem Bundeswahlleiter direkte Drähte und die können direkt mit uns kommunizieren. Aber wir haben auch noch eine andere Institution, das sogenannte Cyber-Abwehrzentrum, wo wir dann mit den Strafverfolgungsbehörden, mit den Geheimdiensten und anderen Behörden, anderen Bundesbehörden, die noch involviert sein könnten, direkt sprechen können und die auch mit uns. Das heißt, wenn das Bundeskriminalamt zum Beispiel feststellt, dass sie einen Vorfall haben, der bearbeitet werden muss, und dass es die Unterstützung des BSI braucht, dann kann es genauso auf uns zu gehen wie wir auf das Bundeskriminalamt.

**Lange:** Du hast gerade den Geheimdienst und andere Sachen erwähnt. Da sind mir ein paar Schlagzeilen aus den letzten Wochen in Erinnerung gekommen. Es wird ja davon ausgegangen, dass es tatsächlich andere Staaten geben könnte, die ein Interesse daran haben, unsere Wahl zu beeinflussen, wie das ja auch schon in anderen Ländern diskutiert wurde oder auch nachträglich untersucht wurde: Wie ist denn da der Stand der Dinge? Ist das auch ein Teil eurer Aufgabe? Gibt es da Diskussionen im Hintergrund und darfst du uns überhaupt etwas darüber sagen?

**Kölligan:** Ich würde jetzt nicht alles erzählen, wovon ich weiß. Aber natürlich ist das eine Bedrohung beziehungsweise eine realistische Bedrohung, dass es auch Staaten gibt, die gern Einfluss auf unsere Politik nehmen möchten und die gern beeinflussen möchten, wie das Wahlergebnis ist. Tatsächlich glaube ich aber, dass Deutschland da sehr gut gerüstet ist und im internationalen Vergleich nicht das primäre Ziel ist. Abgesehen davon haben wir das natürlich im Auge. Immer wenn wir irgendwie bedrohliche Gruppen identifizieren, die so etwas machen könnten, dann sind die auf jeden Fall in unserer Aufmerksamkeit. Und wir tun natürlich, was wir dagegen tun können. Aber davon geht eigentlich keine große Gefahr aus unserer Einschätzung nach.

**Münz:** Dann vermute ich mal, dass aber auf jeden Fall ein Ziel dieser Aktion ist, die politische Willensbildung zu beeinflussen, also Wählerinnen und Wähler zu erreichen? Wahrscheinlich über soziale Netzwerke und über Inhalte dann deren politische Meinungsprozesse zu beeinflussen und damit dann auch die Wahl? Dann kommen wir zum Thema Desinformation: Wie sieht es denn damit aus? Könnt ihr da schon etwas beobachten? Was sind die gängigen Wege, um solche Desinformationen in sozialen Netzwerken unterzubringen?

**Kölligan:** Wir beobachten eigentlich konstant, was da passiert. Wir gucken nicht direkt in die Inhalte hinein. Wir beobachten, wie sich diese Informationen verbreiten. Wir gucken uns an, wie die Techniken dahinter sind. Wie sind vielleicht die psychologischen Effekte und wie können sich diese Informationen verbreiten? Ganz wichtig dabei sind auch die Algorithmen, die dahinter stehen bei den sozialen Netzwerken und auch zu so etwas führen können. Einerseits ist man mit bestimmten Leuten befreundet oder in irgendeiner Weise vernetzt. Das können auch Follower sein, die eine ähnliche Meinung vertreten. Wenn ich dann meine Meinung da äußere, selbst wenn sie noch so abstrus ist, bin ich ja schon mit den Leuten vernetzt, die eine ähnliche Meinung und Weltanschauung vielleicht teilen. Das bestärkt mich und die anderen dann weiter in meiner Meinung, was problematisch sein kann. Zum anderen gibt es Algorithmen, die dafür sorgen, dass – und davon leben ja im Prinzip auch die sozialen Netzwerke – für mich interessante Posts oder Inhalte angezeigt werden. Das kann im politischen Kontext missbraucht werden von Akteuren, wenn man schon in einem bestimmten Weltbild irgendwie verhaftet ist; dass man dann auch Informationen bekommt, die genau dieses weiter unterstützen. Was auch ganz besonders problematisch daran sein kann, ist nicht nur, dass die Meinung dieser Personen beeinflusst werden kann, sondern dass auch deren Vertrauen in unsere funktionierende Demokratie unterminiert werden kann. Am

Ende können die irgendwelchen Verschwörungstheorien aufsitzen, dass die Bundesrepublik vielleicht doch nicht so gut funktioniert. Das ist ein Szenario, was man im Auge haben muss.

**Lange:** Im Auge haben heißt ihr beobachtet – das ist ja eine eurer Aufgaben. Das hatte uns Meike aus dem Lagezentrum schon erzählt. Ihr beobachtet, um zu schauen, was sich da im Netz tut und wo man dann gegebenenfalls eingreifen muss. Was tut ihr denn konkret bzw. was können wir denn auch tun, wenn wir Nutzer und Nutzerinnen der sozialen Medien sind und uns zum Beispiel Informationen im Moment anschauen, weil wir noch nicht ganz entschieden haben, was wir am 26. September in der Wahlkabine ankreuzen? Das sind ja zwei Aspekte, um diese Wahl sicher zu machen.

**Kölligan:** Das ist auf jeden Fall eine sehr gute Frage, weil wir als BSI gar nicht in die Inhalte gucken können. Wir gucken uns die Inhalte auch gar nicht an. Wir sind keine Meinungspolizei oder ähnliches. Ich glaube, auch die anderen Bundesbehörden gucken nicht so in die Inhalte hinein. Aber deswegen ist es umso wichtiger, dass man als mündige Bürgerin und mündiger Bürger und als Nutzerin den sozialen Netzwerke selbst ein bisschen Fürsorge betreibt; wenn man zum Beispiel einen bestimmten Post teilt; dass man sich den vielleicht noch einmal anguckt, sich die Quelle ansieht und nachschaut, ob man dieser Quelle wirklich vertrauen kann und wo diese Informationen herkommen. Man sollte seinen Verstand einschalten und noch einmal darauf schauen: „Ist das wirklich eine Information, der ich vertrauen kann? Möchte ich die wirklich teilen?“. Es ist im Prinzip einer der wichtigsten Prozesse, dass die Bürgerinnen und Bürger wirklich gucken, woher diese Information kommt. Ist die glaubhaft? Da sind wir gerade in einem demokratischen Staat als Behörden mehr oder weniger machtlos, wenn das nicht sonst stattfindet.

**Münz:** Ich wollte an der Stelle noch einmal einhaken, weil mir der Punkt noch wichtig ist. Wenn ich zum Beispiel ein soziales Netzwerk gucke und die Überschriften und geteilten Inhalte sehe, dann ist es ja nicht so wie bei einem Zeitschriftenkiosk, wo ich vor einer Wand stehe und die alle nebeneinander gleichberechtigt – das ganze politische Spektrum wahrscheinlich – im Regal stehen. Was ich im sozialen Netzwerk sehe, ist schon vorausgewählt worden, und zwar anhand dessen, wovon das soziale Netzwerk glaubt, dass es mich mehr interessiert als anderes. Das heißt, zum einen bekomme ich im Zweifelsfall gar nicht das ganze breite Meinungsspektrum angezeigt. Zum anderen gibt es auch noch den Teil der Sponsored Posts, bei denen jemand dafür sorgt, indem er dafür bezahlt, dass mir ein Inhalt angezeigt wird. Habt ihr denn das Gefühl, dass die Mündigkeit der Bürgerinnen und Bürger gefestigt ist?

**Kölligan:** Ich denke schon, dass der Großteil der Bürgerinnen und Bürger eigentlich ein gutes Verständnis davon hat, was glaubhaft ist und was nicht. Tatsächlich muss man aber auch sagen, dass die sozialen Netzwerke spätestens seit der US-Präsidentenwahl 2016 viel dafür tun, um diese Situation zu verbessern, vor allem in politischen Kontexten. Die Algorithmen kommen natürlich daher, dass mir zum Beispiel irgendwie interessante Produkte angezeigt werden. Oder was du sagst: dieses Microtargeting, dass einer bestimmten Person die möglichst relevanten Inhalte angezeigt werden. Das können

Werbetreibende nutzen. Das hat einen legitimen Hintergrund. Es ist ja ein sinnvolles Geschäftsmodell, dass mir mein neues Haarpflege Produkt angezeigt wird, für das ich mich interessiere oder so. Dieser Mechanismus kann auch gerade von politischen Akteuren missbraucht werden. Tatsächlich haben deswegen die sozialen Netzwerke zur letzten Präsidentschaftswahl und auch schon davor die Algorithmen angepasst und haben Auflagen auferlegt für politische Werbetreibende. Mittlerweile wird auch immer angezeigt, wer tatsächlich diese Werbung macht. Das ist wichtig für den Kontext für die Bürgerinnen und Bürger. Die sollten das natürlich auch nutzen. Wenn daran steht, dass das von XY gesponsort ist, dann sollten sie sich auch angucken, wer das ist und welches Interesse dahinter stecken könnte. Das hilft tatsächlich. Das haben die sozialen Netzwerke verbessert. Auch verbessert haben sie den Umgang mit kontroversen Inhalten – man sagt Fake News. Diese werden mittlerweile auch hinterfragt. Das heißt, gerade gegen die Meinungsblasen, in denen man gefangen sein kann, tun die sozialen Netzwerke mittlerweile sinnvolle Dinge, um das zu verhindern. Die arbeiten mit unabhängigen Fact Checking Organisationen zusammen. Und Nutzerinnen und Nutzer können zum Beispiel auch Inhalte melden, die sie für nicht glaubwürdig erachten oder die wirklich in die Irre führen. Die werden dann durch Algorithmen und Menschen gecheckt und im Zweifelsfall an diese Fact Checking Organisationen weitergegeben. Wenn dann Inhalte als Falschmeldungen identifiziert worden sind, können die sozialen Netzwerke auch hingehen und diese kennzeichnen mit einem Warnhinweis; oder, je nachdem, in schlimmeren Fällen die Informationen direkt wegnehmen. Ich denke, dass das sehr sinnvoll ist, um Leute noch einmal mit einer anderen Meinung zu konfrontieren – gerade, wenn sie ein bisschen an so eine Verschwörungstheorie glauben.

**Münz:** Das heißt hier aber auch, dass letztendlich jeder von uns in sozialen Netzwerken oder grundsätzlich dazu beitragen kann a) Inhalte zu prüfen, die einem unter die Nase kommen, b) im Zweifelsfall die Inhalte als kritisch zu markieren, zu flaggen, und c) dafür zu sorgen, dass deren Verbreitung dann irgendwann mal aufhört.

**Kölligan:** Ganz genau! Ich denke, dass das eine der wichtigsten Messages ist, die wir hier verteilen können. Man kann auch Fake Accounts melden, wenn man zum Beispiel sieht, dass seltsame Informationen von einem vermeintlichen RKI oder so verteilt werden. Man sollte sich dann auch den Account angucken. Wenn man Fake Accounts findet, dann sollte man die auf jeden Fall melden. Das hilft allen anderen Nutzern. Das Gleiche kann man mit Informationen machen. Dazu ist diese Funktion da und die sollte man auch nutzen. Da tut man wirklich etwas für die Gesellschaft und natürlich für die sozialen Netzwerke und für alle, die dort sind. So kann man selbst sogar das Internet und die sozialen Netzwerke ein Stückchen sicherer machen.

**Lange:** Ich habe noch eine Frage. Du hast vorhin gesagt, dass ihr so eine Art 24/7-Kontakt zu den sozialen Netzwerken habt: Wie gestaltet sich denn die Zusammenarbeit und zu welchen Themen arbeitet ihr zusammen? Kannst du uns ein paar Beispiele nennen?

**Kölligan:** Ja, auf jeden Fall! Jetzt gerade im Vorfeld der Wahl tauschen wir uns regelmäßig dazu aus, was aktuelle Bedrohungen sind, die möglicherweise passieren können. Wir besprechen irgendwelche Vorfallszenarien und besprechen zusammen, was wir tun könnten, wenn ein bestimmter Vorfall passiert. Wir haben auch Kontakt zu sonstigen aktuellen Themen, die wir besprechen müssen. Wie gesagt, wir treffen uns regelmäßig und sprechen darüber, was aktuell ansteht und was es aktuell zu bearbeiten gibt. Wenn wir identifizieren, dass wir gemeinsam irgendetwas zu entwickeln haben, dann tun wir das auch. Die Kommunikation mit den sozialen Netzwerken ist sehr gut und die Kooperation funktioniert.

**Münz:** Wenn wir jetzt auf die die verbleibenden Wochen bis zur Bundestagswahl gucken: Was sind die Schritte, die auf jeden Fall noch abgehakt werden müssen? Gibt es wichtige Meilensteine für dich als der, der diesen Prozess, dieses Projekt, mitbetreut?

**Kölligan:** Wir haben schon sehr viel erreicht für den Kernwahlprozess. Das heißt, um zum Beispiel diese Schnellmeldungen abzusichern, haben wir schon Informationen herausgegeben an die Gemeinden, damit die wissen, was ein sicheres informationstechnisches System zur Verarbeitung der Wahlergebnisse und für die Schnellmeldungen auszeichnet. Wir haben Beratungsangebote herausgegeben für die Kandidierenden. Wir haben auch verschiedene Sicherheitschecks für die Webseiten der Parteien, zum Beispiel. Diese ganzen Angebote haben wir schon herausgetragen und wir sind sehr gut auf die Wahl vorbereitet. Wir haben schon seit Ende letzten Jahres die ersten Maßnahmen für die Wahlen in Angriff genommen. Was jetzt noch ansteht, ist wirklich die Wahl selbst. Im Vorfeld haben wir natürlich auch noch ein paar Veranstaltungen, zum Beispiel Gespräche. Wir im Referat und mit anderen aus dem BSI treffen uns jetzt auch noch einmal mit großen sozialen Netzwerken und gehen im Prinzip solche Vorfallszenarien durch. Die bringen Szenarien mit, wir bringen Szenarien mit. Wir unterhalten uns darüber, was wir machen würden und gucken, ob wirklich jeder Bescheid weiß, was man im Zweifelsfall tun muss und wie wir das verbessern können. Das machen wir tatsächlich noch vor der Wahl. Wir setzen das dann natürlich auch noch um, damit das dann alles reibungslos steht.

**Münz:** Vielen Dank! Ich werde daran denken, wenn ich an der Wahlurne stehe und meinen Zettel einwerfen.

**Lange:** Ich habe aber jetzt noch eine Frage zu dir und deinem Hintergrund, Anders. Du hast jetzt so engagiert darüber erzählt – auch über diese gesellschaftlichen und politischen Verknüpfungen; nicht nur mit der Wahl, sondern auch mit deiner Arbeit beim BSI. Was hast du denn gelernt? Bist du Politikwissenschaftler oder Wahlexperte? Es klingt, als ob das deine Leidenschaft wäre, aber bei BSI fällt mir immer eher Technik oder Informatik ein. Magst uns verraten, was dich zum BSI geführt hat?

**Kölligan:** Ja, auf jeden Fall! Man hört ja schon heraus, dass das viele Aspekte hat. Wie du schon richtig gesagt hast, hat es natürlich politische Aspekte, aber auch viele technische Aspekte. Ich bin tatsächlich aus einer technischen Richtung hergekommen. Ich bin eigentlich Physiker. Das habe ich gelernt, sozusagen. Ich habe vorher Simulationen gemacht von sich bildenden wasserreichen Sternen. Ich habe viel mit Computern gearbeitet. Ich habe auf

Supercomputern gerechnet. Ich finde auch das Internet sehr spannend als Konstrukt und wie das funktioniert. Damit habe ich mich auch auseinandergesetzt – zunächst erst einmal als Hobby. Aber dann habe ich mich weiter damit auseinandergesetzt, sodass ich auch einiges an Fachwissen hatte. Ich habe mich dann auf eine Stelle beim BSI beworben und bin da sehr glücklich. Das Schöne beim BSI ist, dass man wirklich etwas für die Realität der Leute erreichen kann. Man kann hier in diesem Amt jeden Tag das Internet ein Stückchen besser oder ein Stückchen sicherer machen. Man sieht an Stellen tatsächliche Ergebnisse. Immer, wenn man merkt, dass das, was man da tut, wirklich direkte, positive Konsequenzen hat, ist auf jeden Fall sehr motivierend. Das ist mit ein Aspekt, warum ich sehr gern beim BSI arbeite.

**Lange:** Das ist heute übergesprungen. Das habe ich auf jeden Fall gemerkt. Ganz herzlichen Dank, dass du dir die Zeit genommen hast! Ich denke, dass nicht nur für Michael und mich interessante Infos dabei waren, sondern auch für unsere Hörer und Hörerinnen. Damit sind wir schon fast am Ende der heutigen Folge. Aber auch nur fast!

**Münz:** Genau, denn zum einen wollen wir darauf hinweisen, dass sich unser BSI-Partner-Podcast „Cybersnacs“ in diesem Monat auch mit einer Folge dem Thema Cyber-Sicherheit bei Wahlen widmen wird. Simona Autolitano und Agnieszka Pawlowska haben Julia Schuetze zu Gast. Sie ist Projektleiterin für internationale Cyber-Sicherheitspolitik bei der Stiftung Neue Verantwortung. Ute ich kennen die Dame auch von einem Vortrag, für den wir sie bei einer Konferenz als Referentin eingeladen hatten. Ich bin mir ziemlich sicher, dass das auch ein sehr, sehr interessantes Gespräch wird, was Simona und Agnieszka mit ihr führen werden.

**Lange:** Das glaube ich auch. Ich habe mir das jetzt im Geiste notiert, dass ich da auch mal Reinhöre. Wir verraten Ihnen jetzt noch, was unsere nächste reguläre Folge zum Thema haben wird, in die Sie hoffentlich wieder Reinhören. Und zwar kommt die wie gewohnt zum Ende des Monats und beschäftigt sich anlässlich der diesjährigen Gamescom mit dem Thema Gaming. Wir haben einen Mitarbeiter des BSI zu Gast, der sich damit besonders auskennt. Es geht natürlich vor allen Dingen darum, wie man diese ganzen Computerspiele sicher spielen kann. Ich hoffe, Sie sind dann wieder dabei. Es wird eine spannende Folge, glaube ich!

**Münz:** Das glaube ich auch. Anders, hast du ein Computerspiel, das du immer mal wieder aufrufst zur Entspannung oder zum Aufregen?

**Kölligan:** Ich spiele eigentlich tatsächlich die ganze Palette. Ich spiele sehr gern Dark Souls und ich mag aber auch Autorennenspiele oder Civilization. Ich freue mich auch auf jeden Fall auf die Folge. Da gibt es bestimmt viele spannende Themen!

**Münz:** Das glaube ich auch! Ich bin eher der Beobachter: Ich kenne junge Menschen, die viel spielen. Da ist es, glaube ich, auch nicht verkehrt, die einzelnen Aspekte der Sicherheitsfragen zu kennen. Deswegen bin ich auch sehr neugierig darauf. Bevor wir uns verabschieden, noch der Hinweis, dass Sie uns natürlich gerne über die BSI-Kanäle auf Facebook, auf Instagram, auf Twitter oder YouTube kontaktieren können oder auch eine E-Mail schicken können an [bsi@bsi.bund.de](mailto:bsi@bsi.bund.de). Wir freuen uns über Post! Bis dahin weiterhin alles Gute, und vor allem Gesundheit, und bis zur nächsten Folge!



**Lange:** Ja! Liken und folgen Sie doch dem Podcast „Update verfügbar“ auf Ihrer Podcast-Plattform, dann verpassen Sie auch keine weiteren Folgen. Und auch von mir Tschüss und bis bald!

---

Besuchen Sie uns auch auf:

<https://www.bsi.bund.de/>

<https://www.facebook.com/bsi.fuer.buerger>

[https://twitter.com/BSI\\_Bund](https://twitter.com/BSI_Bund)

[https://www.instagram.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