Datum: 01. Dezember 2024

Johannes Kuhn im Gespräch mit Claudia Plattner, Präsidentin des Bundesamts für Sicherheit in der Informationstechnik

Äußerungen unserer Gesprächspartner geben deren eigene Auffassungen wieder. Deutschlandfunk macht sich Äußerungen seiner Gesprächspartner in Interviews und Diskussionen nicht zu eigen.

Kuhn: Am Mikrofon ist Johannes Kuhn, und mir zugeschaltet ist Claudia Plattner, die Präsidentin von Deutschlands Cyber-Sicherheitsbehörde, dem Bundesamt für die Sicherheit in der Informationstechnik, kurz BSI. Hallo, Frau Plattner.

Plattner: Hallo, ich grüße Sie.

Kuhn: Frau Plattner, Cybersicherheit, das ist ja nicht nur ein Thema für Experten, sondern letztlich für die ganze Bevölkerung. Sie sind jetzt fast anderthalb Jahre im Amt. Vorher waren Sie nicht im BSI tätig und sind da wahrscheinlich auch mit bestimmten Vorstellungen reingegangen, also wie naiv oder wie bewusst wir hier in Deutschland mit dem Thema Cybersicherheit umgehen. Wo sind denn aus Ihrer Sicht wir Endnutzer wachsamer bei der Computersicherheit, als Sie geglaubt haben, und wo fehlt uns noch das Bewusstsein?

Plattner: Also ich denke, insgesamt haben sich da meine Erwartungen, wenn Sie so wollen, durchaus erfüllt. Ich hatte mich da keinen Illusionen hingegeben, dass das schon alles erledigt wäre, gar keine Frage. Ich hatte aber jetzt auch nicht gedacht, dass umgekehrt wir da quasi nichts mehr zu tun haben. Also insofern, das hat die Erwartung durchaus getroffen. Was man feststellen kann, ist, wir sind insgesamt durchaus noch zu sorglos unterwegs. Wir haben da alle noch ein bisschen was zu lernen und auch, wie sagt man so schön, eine Schippe draufzulegen, aber ich glaube, wir sind auf einem guten Weg. Das Bewusstsein wächst, und das ist auch das, was wir erreichen wollen und müssen.

Kuhn: Bevor wir ins Fachpolitische gehen, lassen Sie es uns vielleicht einmal konkret machen: Was sind denn drei Schutzmaßnahmen, bei denen Sie sagen, das können unsere Hörerinnen und Hörer nach der Sendung schnell umsetzen, also wenn sie am Sonntagnachmittag vom Weihnachtsmarkt oder vom Spaziergang oder von der Autofahrt oder vom Sonntagsdienst kommen, einfach das Handy in die Hand nehmen oder den Computer anschalten und sagen, okay, ich will jetzt sicherer werden?

Plattner: Punkt Nummer 1, wenn ihr einmal drei Minuten Zeit habt, schaltet bitte, bitte, bitte die automatischen Updates auf euren Devices ein, also auf den Handys,

auf den Tablets. Das hilft schon ganz viel, wenn man die einfach eingeschaltet hat. Das geht richtig schnell. Der zweite Punkt dauert schon einen Ticken länger. Das ist nämlich, eure vielen Passwörter, packt die doch gerne einmal in so einen Passwort Safe, weil wenn man so einen Passwort Safe hat, dann nutzt man den nämlich auch, und dann ist auch so dieses „nimm mal ein gutes Passwort, auch eines, was du sonst noch nicht verwendet hast“, viel einfacher. Also Passwort Safe wäre Wunsch Nummer 2. Und wenn ihr richtig einmal ein bisschen länger Zeit habt, euch damit zu beschäftigen, dann wäre natürlich so etwas wie ein Umstieg auf Passkeys mein ganz großer Traum, weil danach habt ihr nämlich wirklich Ruhe und könnt euch ziemlich sicher sein, dass das vernünftig geregelt wird und dass eure Passwörter und alles, was damit zu tun hat, in sogenannten Passkeys, also in so neuen Methoden, untergebracht sind. Es ist sehr sicher, und das könnt ihr dann mit Biometrie, also zum Beispiel mit Face-ID oder mit Fingerabdruck, ganz wunderbar verwenden. Damit ist es nämlich auch wirklich super einfach. Das wären so Sachen, die sind mir ganz wichtig. Und wenn ihr eine Firma seid oder aber viel auf Social Media unterwegs seid und Ähnlichem, ist das ganze Thema Zwei-Faktor-Authentisierung jetzt auch noch ein dickes Ding. Ich weiß, das waren jetzt schon vier Wünsche, und bei drei heißt es schon, das geht doch eigentlich gar nicht, aber trotzdem, das wären so ein paar, die mir dazu einfallen.

Kuhn: In Ihrem Lagebericht schreiben Sie, dass auch eine zunehmende Verwundbarkeit bei Googles Android festzustellen ist. Android, das ist ja das gängige Handy-Betriebssystem hier in Deutschland. Zwei Drittel aller Smartphones haben das hier. Was heißt denn das für mich als Endnutzer?

Plattner: Also für Sie als Endnutzer heißt das vor allen Dingen, dass es darum geht, wirklich die Updates einzuschalten. Ich komme immer wieder zu den gleichen Punkten zurück, Verzeihung. Das ist nicht, weil mir nichts Neues einfällt, sondern einfach wirklich, weil das so Basissachen sind, die echt helfen. Also Android selber ist ein Betriebssystem, das im Moment massiv angegriffen wird. Das ist so, und die haben einfach auch noch ein paar Themen, um die sie sich auch kümmern müssen. Das passiert da durchaus auch, aber nichtsdestotrotz sehen wir da einen deutlichen Zuwachs, weil natürlich die Mobile Devices da immer mehr auch im Fokus stehen. Und bei Apple, bei iPhone, bei manch anderen haben wir da noch eine etwas andere Situation. Android ist das, wo wir im Moment wirklich einen Zuwachs sehen. Also hier bitte unbedingt die automatischen Updates, damit man immer schnell geschützt ist, sobald etwas Neues bekannt wird.

Kuhn: Der jährliche Lagebericht des BSI kam vor ein paar Wochen heraus. Der Tenor ist ja eigentlich jedes Jahr, die Bedrohungslage ist angespannt. Vielleicht können Sie einmal ein paar Schlagworte nennen, was Ihnen im Moment besonders Sorgen macht.

Plattner: Ein paar Dinge, die uns da wirklich umtreiben, sind natürlich ganz vorne mit dabei, das Thema Ransomware-Angriffe, also wenn jemand quasi in die Systeme einer Firma oder einer Behörde, einer Kommune eindringt und dort dann im Prinzip alles verschlüsselt. Und dann kommt man montagmorgens dahin und findet einfach nur einen blauen Bildschirm oder einen roten Bildschirm, und auf dem steht drauf, du wurdest gehackt. Bitte so und so viel Euro auf das und das Bitcoin-Konto überweisen. Das ist im Prinzip das, was uns richtig, richtig Sorgen macht. Und die Idee ist quasi, dass man dann ein Lösegeld bezahlt auf dieses Bitcoin-Konto und der Angreifer einem dann sozusagen die Schlüssel gibt, damit man alles wieder entschlüsseln kann.

Kuhn: Wenn ich da einmal hineingehen darf, da hat man ja immer bei den bekannt gewordenen Fällen, und das sind ja eigentlich wenige Fälle im Vergleich zur Verbreitung solcher Angriffe, da hat man ja immer so einen Eindruck von Hilflosigkeit in den vergangenen Jahren bei den betroffenen Organisationen gehabt. Hat sich das inzwischen geändert, oder ist man da inzwischen besser vorbereitet? Tut sich da etwas?

Plattner: Also die gute Nachricht ist, an vielen Stellen ja. Die schlechte Nachricht, an vielen Stellen ist es auch weiterhin immer noch so, dass man da eine ziemliche Hilflosigkeit hat. Man sitzt da wirklich montagmorgens und weiß überhaupt nicht, was man da machen soll. So, und das ist dann im Prinzip die Situation, die wir vermeiden wollen, und viele Firmen schaffen das inzwischen auch. Also die schaffen es, sich früher vorzubereiten, zum Beispiel indem sie Backups haben, indem sie üben, wie diese Backups wieder eingespielt werden müssen. Und dann verliert es so einen Schrecken von, da hat jemand die Systeme angegriffen, sehr schnell den Schrecken, wenn man einfach weiß, hier, man kann das auch relativ schnell selber wieder herstellen, weil man Backups hat, weil man weiß, wie man die wieder einspielt.

Kuhn: Was sind denn Branchen oder Firmengrößen, wo Sie sagen, die sind gut vorbereitet, und wo sagen Sie, na, da wird zu wenig getan?

Plattner: Also definitiv gut vorbereitet sind natürlich die vor allen Dingen größeren Firmen, weil die einfach auch die Ressourcen haben und die Möglichkeiten, sich da entsprechend vorzubereiten. Da ist das schon ein bisschen geordneter. Das ist auch klar. Was uns weiterhin Sorgen macht, ist, ich sage einmal, das sind die KMOs, nicht KMUs, sondern KMOs, also die kleinen und mittlere Organisationen, also alle kleinen und mittleren Unternehmen, aber eben halt auch zum Beispiel Kommunen, Behörden, politische Institutionen, also alles, was da sozusagen spannende, interessante Ziele sind, das sind die, die uns wirklich Sorgen machen, die eben halt nicht die Größe haben, um sich gut zu schützen.

Kuhn: Cybersicherheit hat ja nicht nur mit Hackerangriffen zu tun, sondern auch mit Stabilität. Wir hatten im Juli den CrowdStrike-Ausfall, 8,5 Millionen Windows-Rechner lahmgelegt, damit auch Fluggesellschaften, Krankenhäuser, Einzelhändler, und das einfach nur, weil die Firma CrowdStrike ein fehlerhaftes Update eingespielt hat. Am

Donnerstag hatten wir auch in Dänemark teilweise Ausfälle von Teilen des Mobilfunknetztes, auch von Bahnsignalen, weil da ein Provider auch ein fehlerhaftes Update eingespielt hat. Gehen Sie davon aus, dass wir jetzt mit solchen Vorfällen regelmäßig leben müssen?

Plattner: Also wir müssen auf jeden Fall lernen, damit so umzugehen, dass uns das nicht passiert, aber das ist einmal ganz klar. Das war nicht nur die Firma CrowdStrike. Also CrowdStrike hat sicherlich an der Stelle nicht mit der notwendigen Sorgfalt gearbeitet, gar keine Frage. Wir reden aber auch davon, dass am Ende des Tages das auf dem Betriebssystem Microsoft passiert ist. Das heißt, hier ist also auch noch einiges in der Betriebssystemsicherheit, also dem sogenannten Kernel zu machen. Da passiert noch ein bisschen was und muss auch noch etwas passieren. Da sind wir auch durchaus hinterher als BSI. Da reden wir sehr intensiv mit all diesen Herstellern auf der Sicherheitsheitsseite, aber eben halt auch auf der Microsoft-Seite und nicht zuletzt, nicht zu vergessen, natürlich auch auf der Betreiberseite. Wenn ich kritische Infrastrukturen habe und ich davon abhängig bin, dass gewisse Rechner funktionieren, dann habe ich dafür auch ein Back-up. Und die hängen dann vielleicht auch nicht an automatischen Updates, zumindest nicht in der ersten Schleife. Also ich glaube, an verschiedenen Stellen haben wir da Punkte, wo wir sehen, dass wir noch etwas verbessern können und müssen, aber es ist eben halt nicht nur Crowdstrike gewesen, es war durchaus noch ein bisschen mehr, was da zusammengekommen ist.

Kuhn: Sie hören das Interview der Woche im Deutschlandfunk, zu Gast ist die BSI-Präsidentin Claudia Plattner. Frau Plattner, wir können natürlich nicht über Digitalthemen reden, ohne über künstliche Intelligenz ganz kurz zu reden. Es ist ja derzeit das große Thema in der Technologiebranche. Ist KI für die IT-Sicherheit im Moment eher eine Bedrohung oder eher eine Chance?

Plattner: Also die Antwort lautet natürlich beides. Also das ist tatsächlich das Thema. Wir merken, die Angreifer professionalisieren sich immer mehr. Die werden immer schneller, immer besser. Die arbeiten hervorragend arbeitsteilig zusammen. Die nutzen Hochtechnologie, keine Frage, und die nutzen natürlich auch KI. Also KI nutzt man dann zum Beispiel, um Schwachstellen schnell zu finden und sie auch schnell auszunutzen, große Datenmengen zu durchforsten. Das heißt, wir müssen genau das Gleiche tun. Das heißt, wir müssen lernen, wie können wir KI nutzen, um uns auch ganz schnell zu verteidigen, das heißt, dieselbe Schwachstelle finden, aber halt schließen, bevor sie ausgenutzt werden kann, zum Beispiel feststellen, wenn in unseren Systemen irgendetwas passiert, was eben halt nicht normal ist. KI kann solche Themen finden und dann auch wirklich ganz schnell idealerweise automatisiert auch Gegenmaßnahmen einleiten. Auch da kann KI helfen. Es geht darum, wer von uns wird schneller besser, die Angreifer oder die Verteidiger. Und ich möchte an dieser Stelle dafür plädieren, dass wir unsere Hausaufgaben machen, dass wir Technologie uns zunutze machen, um schneller besser zu werden, als es die Angreifer tun.

Kuhn: Jetzt gibt es ja die ersten KI-Agenten, OpenAir und Google werden da sehr wahrscheinlich demnächst eigene Systeme vorstellen. Was ist ein KI-Agent? Um es zu erklären, das ist eine künstliche Intelligenz, die für mich automatisch zum Beispiel einen Flug buchen kann, wenn ich ihr den Befehl dazu gebe. Es gibt ja erste Prototypen, die machen das, indem sie quasi den Browser bedienen. Da fährt dann der Mauszeiger automatisch herum. Die KI füllt die Textkästchen aus, also bedient quasi die Tastatur. Aber im Kern lautet ja das Versprechen, die künstliche Intelligenz wird mein Assistent und darf dann auch den Computer bedienen oder zumindest den Browser. Wie sehen Sie so etwas aus Cyber-Sicherheitssicht?

Plattner: Also aus Cyber-Sicherheitssicht müssen wir da viel tun, um das gut abzusichern, gar keine Frage. Ich meine, die Vorstellung ist natürlich attraktiv. Ich habe auch keine Lust, die Sachen immer selber zu machen und in kleinteiligen Sessions vor dem Rechner irgendwie einen Flug zu buchen und noch einmal den Termin zu checken und da noch einmal etwas zu verschicken. Klar ist es toll, wenn das ein KI-Agent für mich tun kann, aber es ist auch klar, ein KI-Agent, der entsprechend auch sehr viel tun kann bzw. auch andere KI-Agenten dann wieder steuern kann, der muss halt auch entsprechend dafür sorgen, dass er die Rechte hat, mit denen er das tun kann, und dann müssen wir da schon sehr genau schauen, wie kriegen wir da vernünftige Absicherungsmechanismen herein. Ich glaube, da werden wir noch viel darüber lernen. Vor allem im nächsten halben bis ein Jahr, glaube ich, wird da ganz, ganz viel passieren.

Kuhn: Um einmal den Blick in das Geopolitische zu wenden, wie blicken Sie auf künstliche Intelligenz als Teil der sogenannten hybriden Kriegsführung, also dass die Technik von Akteuren wie Russland oder China eingesetzt wird, zum Beispiel um hier Desinformationen in den Umlauf zu bringen?

Plattner: Also das sind natürlich Themen, die uns sehr, sehr große Sorgen machen. Also gerade im hybriden Bereich sehen wir da Tendenzen, alles rund um Desinformationen ist ein Riesenthema. Natürlich ist es mit KI heutzutage möglich, Inhalte zu produzieren, die täuschend echt sind. Die kann man als Mensch kaum noch unterscheiden. Und hier sind zwei Dinge uns ganz, ganz wichtig. Punkt Nummer 1, wir müssen es schaffen, die Menschen zu sensibilisieren für diese Themen. Es ist leider so, wir können unseren Augen und Ohren heutzutage nicht mehr uneingeschränkt glauben. Und da sage ich immer, schaut noch einmal auf die Information. Ist es wirklich wahrscheinlich? Kann das sein? Sucht euch eine zweite Quelle, eine unabhängige Quelle, die nicht nur in der eigenen Social-Media-Bubble stattfindet. Das ist mir ganz wichtig, dass wir es schaffen, als Gesellschaft da resilient zu werden. Und der zweite Punkt ist ein technischer, ich bin ja Tekkie, wir brauchen auch technische Methoden, um Material und Absender zu verifizieren, das heißt, wirklich zu erkennen, etwas ist Fake, zum Beispiel weil es schon so gekennzeichnet ist, oder auch etwas ist definitiv echt, zum Beispiel weil jemand das, in Anführungsstrichen, unterschrie-

ben hat, also digital signiert. Und das möchte ich, dass unsere Bürgerinnen und Bürger, unsere Verbraucherinnen und Verbraucher das auf dem Bildschirm auch unterschieden und sehen können und dann auch ihre eigenen Schlüsse daraus ziehen.

Kuhn: Gehen Sie davon aus, dass so etwas im Bundestagswahlkampf eine größere Rolle spielt, also Deepfakes zum Beispiel? Sie haben es angesprochen, Videos, Fotos, Sprachaufzeichnungen, die künstlich erstellt sind, aber echt wirken, dann auch sozusagen Doppelgänger von echten Personen darstellen, da muss ich auch kein Experte sein und muss auch nicht unbedingt in Russland sitzen, um so etwas zu produzieren inzwischen.

Plattner: Also wir gehen definitiv davon aus, dass es Gruppierungen gibt, die Interesse daran haben, illegitimen Einfluss auf die Wahlen zu nehmen. Davon müssen wir ausgehen, damit müssen wir arbeiten, mit dieser Annahme. Und das tun wir auch. Also wir machen genau die Sachen, die man hier an dieser Stelle, Stand jetzt, tun kann. Das heißt, wir gehen definitiv heraus in die Bevölkerung und versuchen, denen zu erklären, hey, da kann ganz, ganz viel auch wirklich nicht wahr sein, das wird auch so sein. Da gibt es ein Interesse daran, uns zu beeinflussen. Nicht alles, was jetzt furchtbar schlimm klingt, ist auch wirklich schlimm. Hier werden Themen wirklich genommen undeutlich übertrieben. Das sind alles Themen, die wir machen. Wir gehen natürlich auch zu den Social-Media-Providern und sehen zu, dass wir dort möglichst diese ganzen Fake-Accounts herauskriegen, aber das ist alles so eine langwierige Arbeit. Wir kommen da gut vorwärts, keine Frage, aber wir müssen davon ausgehen, dass hier auch ein entsprechender Einfluss genommen werden will. Das heißt, dort gibt es Gruppen, die in der Tat versuchen, illegitimen Einfluss zu nehmen.

Kuhn: Wie bereiten Sie sich denn auf die Bundestagswahl vor? Also der Verfassungsschutz warnt zum Beispiel in einem aktuellen Papier vor Hack-and-Leak-Operationen. Also man hackt sich bei einer Partei ein, um dort belastendes Material zu finden oder vermeintlich belastendes Material oder Material, wo man dann Sachen verändert und veröffentlicht das dann. Wie bereiten Sie sich darauf vor, und wie bereiten Sie auch letztendlich die Parteien darauf vor?

Plattner: Also zunächst einmal machen wir das alles zusammen. Das ist erst einmal die gute Nachricht. Wir arbeiten da alle zusammen, ziehen da alle an einem Strang. Die Wahl an sich ist immer unter der Führung der Bundeswahlleiterin, auch klar, und wir selber geben da an der Stelle auch eine entsprechende technische Expertise hinein. Um ganz konkret auf die Hack-and-Leak-Thematiken einzugehen, und ich fand die Formulierung sehr schön, vermeintlich, genauso ist es nämlich. Man sucht dann irgendwas, was man dann als Narrativ verspinnen kann und irgendeine große Story daraus machen kann. Ganz konkret dazu gehen wir zum Beispiel mit den Persönlichkeiten, die in der Öffentlichkeit stehen, mit den Politikern, mit den Parteien, mit den politischen Stiftungen, da machen wir entsprechende Webinare, in denen wir ihnen

quasi zeigen, wie sie sich schützen können, wie sie zum Beispiel ihre Privatgeräte absichern können etc. pp. Normalerweise hätten wir das durchaus auch gerne vor Ort gemacht und in persönlicher Ansprache. Jetzt müssen wir das eher auf die Webinare verlegen, einfach weil wir nicht ganz so viel Vorbereitungszeit hatten, wie wir uns das gedacht haben. Nichtsdestotrotz die Angebote sind da, und die werden auch angenommen.

Kuhn: Gibt es ein Thema, bei dem Sie Bauchschmerzen haben? Weil, Sie haben es ja angesprochen, es ist ja ein sehr verkürzter Prozess jetzt auch bis zur Bundestagswahl.

Plattner: Nein, also Bauchschmerzen habe ich da an der Stelle nicht. Das Thema ist für uns eher, wie viel könnten wir noch tun, um das Ganze, ich sage einmal, noch formvollendeter zu machen, aber bei der Frage, ist die Wahl gefährdet, ein klares Nein. Wir wählen in Deutschland bis auf wirklich ganz wenige Ausnahmen auf Papier. Das heißt, die Durchführung der Bundestageswahl an sich ist nicht abhängig von Informationstechnik, aber was eben halt am Ende des Tages eine Rolle spielt, ist, Sie kennen das, Sie sitzen vor dem Fernseher kurz nach 18:00 Uhr. Die ersten Hochrechnungen kommen. Dann kommen irgendwann die ersten Ergebnisse. Das wird natürlich alles auch ein Stück weit übertragen. Und da wollen wir natürlich auch sicherstellen, dass genau dieser Prozess und diese Information wirklich hundertprozentig integer da auch ankommt, wo sie hin muss. Und da engagieren wir uns auf jeden Fall auch mit unserer technischen Expertise, weil wir definitiv sicherstellen wollen, dass nicht nur die Wahl sicher ist, sondern eben halt auch das Vertrauen der Menschen in die Wahl wirklich gegeben ist, und das machen wir.

Kuhn: Sie haben es gesagt, wir wählen auf Papier. Es gibt aber auch Länder wie Estland, die wählen digital. Gehen Sie davon aus, dass wir den Esten irgendwann einmal folgen? Sollten wir ihnen folgen, oder sagen Sie, na ja, Papier hat sozusagen im Kontext Cybersicherheit in dem Fall auch seine Vorteile?

Plattner: Also die Entscheidung darüber, wie man sozusagen hier die Richtung einschlägt, liegt natürlich ganz, ganz klar bei der Bundeswahlleitung. Also da sind wir sozusagen die Enabler. Wenn irgendwie gesagt wird, wir wollen in die Richtung gehen, dann sind wir da natürlich dabei oder entsprechend auch zu helfen, wenn es um die Absicherung geht. Stand jetzt haben wir genau den aktuellen Prozess. Ich glaube, der hat sich auch bewährt, und gerade jetzt, wo wir auch vielleicht einmal ein bisschen weniger Zeit als Vorbereitung haben, bin ich in diesem Moment tatsächlich gar nicht so undankbar dafür.

Kuhn: Ich will noch einmal mit Ihnen über das Thema NIS-2 reden. Wenn ich über NIS-2 Drei-Minuten-Radiobeiträge mache, muss ich erst einmal eine Minute lang erklären, was das ist. Vielleicht können Sie einmal kurz in Ihren eigenen Worten den Menschen da draußen beschreiben, was diese europäische NIS-2-Richtlinie regeln soll und warum das für Sie als BSI wichtig ist, aber auch für uns als Bevölkerung.

Plattner: Die NIS-2-Richtlinie aus der EU regelt, dass alle diejenigen, die IT betreiben, also Firmen, die IT haben, Behörden, die IT haben, eine Kommune, die Systeme hat, die sie einsetzt, dass alle diejenigen sich darum kümmern müssen, dass das gut abgesichert ist. Das heißt, sie werden so ein Stück weit verpflichtet, sich so sozusagen um ihre eigene Sicherheit zu kümmern. Das ist das, was die NIS-2-Richtlinie tut, und das eben auf einem europäischen Niveau. Das heißt wirklich alle, nicht nur Deutschland, sondern eben halt auch Zypern, Schweden, Frankreich und was auch immer, wir sind alle mit dabei, weil wir uns auch wirklich europaweit darum kümmern müssen. Und das ist natürlich erst einmal eine Veränderung, wenn sozusagen auch von außen gesagt wird, nicht nur, es wäre besser für dich, schütze dich bitte, sondern du musst dich sogar schützen.

Kuhn: Jetzt diskutieren wir in Deutschland im Moment sehr viel über Bürokratie, und aus der Wirtschaft ist einerseits zu hören, gut, dass jetzt das Cyber-Sicherheitsniveau angehoben wird. Auf der anderen Seite gibt es natürlich jetzt deutlich mehr Branchen, die als wichtig oder sehr wichtig und im öffentlichen Interesse eingestuft werden als zuvor. Ich glaube, vorher waren es 6.000 Betreiber. Jetzt sind es 29.000 Firmen, Organisationen, Verwaltungen. Also das ist ja nicht nur deutlich mehr Arbeit für Sie, sondern auch deutlich mehr Organisationen, die betroffen sind. Können Sie nachvollziehen, wenn zum Beispiel gesagt wird: Gut, dass die Lebensmittelbranche jetzt irgendwie für besonders relevant gehalten wird, ist klar, es ist ja auch eine Lehre aus Corona so ein bisschen - aber dass jetzt zum Beispiel eine Molkerei mit 51 Mitarbeitenden im Allgäu wirklich irgendwelche Cyber-Audits machen muss, vielleicht sich Beratung holen muss, mit mehr Bürokratie zu tun hat, das ist ein bisschen übertrieben?

Plattner: Also zunächst einmal ist natürlich immer schwierig, da irgendwo auch vernünftige Grenzen zu ziehen, aber jetzt einmal die Grenzen zur Seite, ich halte es grundsätzlich für wichtig, dass wir das Gesetz haben, weil es ist einfach Ausdruck von der Notwendigkeit und der Dringlichkeit. Das Problem ist einfach akut. Wir müssen uns darum kümmern, und insofern bin ich da erst einmal sehr dafür. Ich kann die Ängste auf der anderen Seite natürlich auch total verstehen. Ich habe ja selber IT auf der anderen Seite sozusagen gemacht und das auch für viele, viele Jahre. Und ich kenne die Probleme, und ich kenne auch die Ausprägungen, die das annehmen kann. Wir als BSI, die ja diejenigen sind, die dafür verantwortlich sind, das auch hier mit den Firmen zusammen zu machen, haben für uns ganz, ganz klar den Fokus gesetzt auf Kooperation, auf Hilfe und etwas weniger auf wie können wir jetzt möglichst bürokratisch vollständig hier vorgehen. Das ist uns ganz wichtig. Und dann bleibt für die Firmen als Allererstes einmal übrig, zumindest aus unserer Sicht, aus der, in Anführungsstrichen, bürokratischen Sicht, ja, ihr müsst euch registrieren, ihr müsst euch melden. Ja, wenn wir ein Security Incident habt, dann müsst ihr ihn tatsächlich auch melden. Das kommt noch mit dazu, und das sind erst einmal die beiden wirklich

wichtigen Pflichten, und ansonsten könnt ihr euch auf jeden Fall auch erst einmal darauf konzentrieren, euch jetzt wirklich sicherer zu machen. Uns geht es nicht darum, die spärlichen Ressourcen für Bürokratie und für Dokumentation auszugeben, das braucht man auch, aber das Wichtigste ist, uns erst einmal wirklich absichern bitte.

Kuhn: Die NIS-2-Richtlinie sollte eigentlich schon im Oktober umgesetzt sein, das war die EU-Vorgabe. Am Donnerstag hat auch die EU-Kommission einen Vertragsverletzungsverfahren eingeleitet, denn das Gesetz hängt ja gerade im Bundestag, und wir kennen die politische Situation. Es ist unklar, ob es da vor der Bundestagswahl noch fertig herauskommt. Inwiefern sehen Sie jetzt bei diesem Thema, unabhängig davon, dass es vielleicht Strafzahlungen gibt, die Parteien in der Pflicht, das noch durchzubringen, speziell natürlich Parteien wie die FDP und die Union, ohne die es ja für die aktuelle Bundesregierung keine Mehrheit gibt?

Plattner: Also ich kann nur an alle Kolleginnen und Kollegen im Bundestag wirklich appellieren, zu sagen, hey, das ist ein ganz, ganz, ganz wichtiges Gesetz. Wenn wir das jetzt nicht mehr durchkriegen, dann werden wir wirklich einiges an Zeit verlieren, ob das jetzt ein Dreivierteljahr ist oder ein Jahr, sei einmal dahingestellt, aber der für mich wirklich wichtige Punkt ist, die Firmen da draußen hatten jetzt angefangen, sich darauf einzustellen. Die brauchen Planungssicherheit. Die müssen wissen, was kommt. Die müssen wissen, kommt dieses Gesetz oder noch einmal ein anderes. Wenn es nicht gut läuft und das wirklich lange dauert, dann werden die auch viele Dinge, die sie dann jetzt schon angefangen hatten zu planen, gegebenenfalls auch noch einmal auf die lange Bank schieben. Und das ist wirklich das Blödeste, was uns passieren kann. Wir müssen uns schützen. Wir müssen eine Schippe drauflegen, nicht eine Schippe runternehmen. Und insofern, wenn es irgendwie geht, lasst uns bitte versuchen, dieses Gesetz so schnell wie möglich, gerne jetzt sofort noch umzusetzen.

Kuhn: Was ja am Entwurf auffällt, die Bundesministerien sind künftig an die höheren NIS-2-Standards gebunden. Die Bundesbehörden, für die Sie als BSI ja auch zuständig sind, dagegen nicht. Das klingt jetzt erst einmal nicht logisch, dass man sagt: Ministerien ja, nachgelagerte Behörden, ja, warten wir erst einmal oder gucken wir halt einmal.

Plattner: Also das waren schon durchaus spannende Kompromisse, die da erzielt werden konnten. Da ist auch viel im Vorfeld, da hatten wir jetzt gar nicht so direkt etwas mit zu tun, aber da ist auch viel, viel gesprochen worden, aber für mich ist ganz klar, je mehr Organisationen wir hier reinnehmen können und je geordneter und standardisierter wir miteinander vorgehen können, desto sicherer kriegen wir auch alle in der Verwaltung des Bundes, und insofern würden wir uns natürlich freuen, wenn die auch noch da mit hineinkämen. Es ist tatsächlich schwer zu erklären. Das ist schwer, der Öffentlichkeit zu erklären, warum die dann da nicht mit drin sind. Da bin ich total bei Ihnen. Ich würde mir wünschen, dass sie es wären.

Kuhn: Was ja NIS-2 nicht ändern würde, ist die föderale Zuständigkeit, heißt also, BSI ist für den Bund zuständig, die Länder haben ihre eigenen Landessicherheitsämter, weil eben IT-Sicherheit auch ja Landesangelegenheit ist. Das ist sehr verwirrend und klar, es gibt schon Zusammenarbeit, aber wie groß sind denn die Reibungsverluste, wenn sich quasi 16+1 immer koordinieren müssen, auch gucken müssen, das wird ja bei NIS-2 auch eine große Rolle spielen, wie man es dann sozusagen auch wieder einheitlich hinkriegt, damit eben eine Firma, die zum Beispiel in Schleswig-Holstein und in Bayern betroffen ist sozusagen, dann nicht verschiedenen Standards folgen muss und letztendlich auch, um alert zu sein, bei Bedrohungen im Cyberraum.

Plattner: Also mir wäre es sehr, sehr, sehr wichtig, dass wir es schaffen, hier in eine Zusammenarbeit hineinzukommen und auch vom Gesetzgeber die Möglichkeit dieser Zusammenarbeit zu bekommen, die es uns erlaubt, da viel, viel, viel koordinierter miteinander zu arbeiten. Also wir schaffen es an vielen Stellen, wir haben jetzt auch entsprechend schon Zusammenarbeit mit ganz, ganz vielen Ländern. Das ist auch gut. Das ist auch eine sehr geschätzte Zusammenarbeit. Ich will mich da gar nicht beschweren. Das ist schon echt fine, aber es gibt drei Punkte, die mir wirklich wichtig sind, die uns fehlen und von denen wir im Moment gesagt kriegen, so können wir nicht vorgehen. Punkt Nummer 1, ich hätte gerne ein gemeinsames Lagebild, wirklich ein gemeinsames Lagebild für Deutschland. Hier passiert gerade das, und da passierte gerade das und das im Überblick. Das wird zum Beispiel spannend beim zweiten Punkt, nämlich dem Krisenmanagement. Jetzt stellen wir uns einmal vor, in München und in Hamburg gehen gleichzeitig die Lichter aus, das aufgrund eines Cybervorfalls und das vielleicht noch aus einer geopolitischen Spannung. Dann müssen wir ganz klar wissen, dass wir jetzt sofort ab Sekunde Null auch mit dem Krisenmanagement hineingehen. Das muss koordiniert sein, wirklich ab Sekunde Null. Dazu brauche ich ein Lagebild, in dem ich erst einmal sehe, dass in Hamburg und in München gerade das Licht ausgegangen ist, ohne vorher telefonieren zu müssen, sondern wirklich in dem Moment, und ich muss in dem Moment auch gemeinsam dann sofort loslaufen können, geübte Strukturen haben, gemeinsames Krisenmanagement. So, und dann habe ich vielleicht noch irgendwie die Möglichkeit, vorher schon zu sehen, dass das etwas schiefgehen könnte. Das kann ich vielleicht auch machen, weil mein Nachbarland oder der Bund ein Tool hat, mit dem ich schon erkennen kann, dass da ein Angreifer im System ist, also eine gemeinsame Toolnutzung. Und das ist der dritte Punkt. Diese drei Punkte fehlen uns heute in der Zusammenarbeit. Und die sind mir ganz, ganz wichtig, und da habe ich die Hoffnung, dass wir es dann jetzt auch irgendwann schaffen, auch mithilfe des Gesetzgebers, hierfür die Voraussetzungen zu schaffen, mit den Ländern zusammen auf Augenhöhe in diese Art von Zusammenarbeit auch hereinzukommen. Die meisten wollen und können das auch. Es ist tatsächlich einfach eine Frage von wie setzen wir es auf, wie passt es auch in das Staatsgefüge in Deutschland.

Kuhn: Das ist ja nicht einfach. Es gibt Widerstand aus den Ländern. Da muss man das Grundgesetz ändern. Jetzt wird bald neu gewählt. Inwiefern sagen Sie jetzt schon mit Blick auf die nächste Regierung, das muss kommen einfach, damit es einfacher wird?

Plattner: Das ist genau das, was ich gerade gesagt habe. Das ist firmiert unter dem Begriff Zentralstelle. Das ist dieses Zusammenarbeiten-Können in diesen wichtigen Feldern, und wir machen das ja heute schon. Also wir haben eine Zentralstelle zum Beispiel beim BKA. Das heißt, das Bundeskriminalamt arbeitet mit den Landeskriminalämtern entsprechend zusammen. Wir haben das auch bei den Verfassungsschutzämtern. Also das ist jetzt nichts Ungeübtes, das ist nichts Neues. Und das brauchen wir auch für den Bereich Cybersicherheit. Auch hier müssen wir es schaffen, dass ein BSI mit den LSIn, oder wie auch immer sie in den Ländern heißen, entsprechend zusammenarbeiten kann. Und ich glaube, dass das gut funktionieren kann. Ich bin auch durchaus zuversichtlich, dass wir Mittel und Wege finden, das in der nächsten Legislatur auch anzugehen und dafür auch Lösungen zu finden. Wie die aussehen, da muss natürlich auch der Gesetzgeber sich überlegen, wie er das gestalten möchte, aber ich bin da eigentlich sehr zuversichtlich, weil wir sind uns alle, wirklich alle darüber einig, dass wir diese Probleme miteinander gelöst bekommen, sodass wir dann auch richtig zusammenarbeiten können.

Kuhn: Frau Plattner, vielen Dank für das Gespräch.

Plattner: Sehr gerne.