Pressekonferenz Potsdamer Konferenz für Nationale Cyber-Sicherheit 2015

Datum: 11.6.2015, 12:40 bis 13:40 Uhr, Ort: Hörsaal 2 des Hasso-Plattner-Instituts (HPI)

Teilnehmer: Prof. Dr. Jamie Shea, NATO, Rob Wainright, Europol, Dr. Hans-Georg Maaßen (BfV), Michael Hange (BSI), Prof. Dr. Christoph Meinel, HPI, und Hans-Joachim Allgaier (Moderator)

Dieser Text beruht auf einer Transkription von Stefanie Saier, Berlin, die sprachlich geringfügig redigiert wurde von HPI-Pressesprecher Hans-Joachim Allgaier, Potsdam.

Moderator: Meine Damen und Herren, liebe Kolleginnen und Kollegen, ich begrüße Sie ganz herzlich zur Pressekonferenz anlässlich der dritten Potsdamer Sicherheitskonferenz, die offiziell heißt: Potsdamer Konferenz für Nationale CyberSicherheit. Mein Name ist Hans-Joachim Allgaier, ich bin der Pressesprecher des Instituts. Die Konferenzsprache ist Deutsch. Für unsere internationalen Gäste, den NATO-Vizegeneralsekretär Jamie Shea und den Europol-Direktor Rob Wainwright werden Ihre Fragen, wenn Sie sie nicht in Englisch stellen, ins Englische übersetzt. Die Antworten bekommen Sie auf Deutsch – Jamie Shea spricht sehr gut Deutsch, wie ich gerade festgestellt habe – oder in Englisch. Je nachdem. Ich denke, das ist okay so. Wir begrüßen auch die Zuschauer von N24, die live zugeschaltet sind wegen der Bedeutung der Pressekonferenz an diesem Tag. Dieser Tag ist natürlich für uns in Deutschland ein wenig geprägt von dem, was unter den Begriffen „Bundestag“ und „IT“ rangiert. Aber ich hoffe, wir beschäftigen uns heute nicht nur bzw. nicht hauptsächlich damit, sondern es geht um das große Generalthema Cyber-Sicherheit. Die Verunsicherung wächst, und wir wollten gerne heute unsere Teilnehmer kurze Statements geben lassen, in denen sie zusammenfassen, was sie entweder schon gesagt haben oder nachher direkt im Anschluss ab 14 Uhr noch sagen werden. Dann kommen wir zur Frage-Antwort-Runde. Material finden Sie in unserer Pressemappe. Es liegen auch noch einige auf dem Tisch dort. Es wird auch vorgestellt heute Nachmittag, und Prof. Meinel wird sicher dazu nachher noch etwas sagen, ein Secure Identity Lab, das von Bundesdruckerei und Hasso-Plattner-Institut entwickelt und eröffnet wird. Näheres dazu also gleich. Wir bitten um Verständnis dafür, dass Mr. Wainwright pünktlich um 13 Uhr abreisen muss wegen Verpflichtungen, die er im Ausland hat. Insoweit bitte ich um Handzeichen, wenn es ganz konkrete Fragen schon im Vorfeld für Mr. Wainwright gibt. Ansonsten würde ich mit der Einleitungsfrage an den NATO-Vizegeneralsekretär beginnen.

Mr. Shea, Sie haben vorhin von der Bedrohung der NATO durch einen Cyber-Angriff gesprochen und der Möglichkeit, dass sich alle Mitgliedsstaaten aufgerufen fühlen könnten, dies als Beistandsmoment, als Fall einer Beistandsverpflichtung zu sehen, ich glaube gemäß Paragraph 5 der NATO-Charta. Können Sie das ein wenig ausführen? Das ist natürlich besonders interessant.

Jamie Shea: Herr Allgaier, vielen Dank für diese sehr gute und aktuelle Frage. Please, I will answer in English, because I can speak four times as fast and the technological vocabulary comes easier to me. Thank you. We hope in the alliance, as it has been recently said on a NATO-Summit in Wales, that a cyber attack at a certain degree of severity could be considered the equivalent of an armed attack. In other words, armed attacks under international law do not only come in the form of tanks, missiles, or aircraft, but also could come in the form of electrons as well. And therefore, yes, NATO would consider a cyber attack potentially under article 5. However, there is no automaticity, obviously; it would depend upon the collective decision and the appreciation of the allies. We have left open

what that threshold for an armed attack would be, because clearly it is best for deterrence when you keep your potential adversaries guessing, as to your response.

But we do believe, looking at some recent examples, that cyber attacks are not just an inconvenience. They are not just about credit card theft or minor damage. We see increasingly that cyber attacks are very sophisticated, very well-financed, very well orchestrated, and that they are designed to real and lasting damage that can cost countries, that can cost industries billions of dollars to recover from. So this is a threat that we need to take very seriously indeed.

With that said, final answer: At NATO, we also don't want to be in a position where we do nothing unless there is a article 5, because allies are experiencing major cyber attacks every day of the week. So we are trying to make NATO into a cyber defence community. We do this through exchange of intelligence, through training, through exercises, through setting capability targets, designing cyber capability packages, like our malware information sharing platform and forming partnerships with the European Union—Rob Wainwright is here—and with industry as well. So we don't just wait for the attack. We are trying to improve the cyber resilience of all our allies on a 24-7 basis. Thank you.

Moderator: Dann schnell zu Rob Wainwright. Die Frage an Sie ist: Was kann Europol über die Unterschiedlichkeit der Bedrohung der Bevölkerung durch Cybercrime in den verschiedenen EU-Staaten feststellen? Und sind Sie eigentlich als Europol in der Lage, Ihren Aufgaben so nachzukommen, wie Sie sich das eigentlich idealerweise vorstellen?

Rob Wainwright: Thank you very much. At Europol we have the European Cybercrime Centre for the last two years, which is a unique, very dynamic operational platform, bringing together all the major policing agencies in Europe, plus many of the international partners, such as the United States, an increasing industry, the large tech firms, investing now in an operational centre that has conducted 700 major international operations in the last two years against the cybercrime threat. What we can see from that is that the scale of the threat is certainly increasing, the level of sophistication as well. What worries me the most is not that we are on a very strong upward curve, but the way in which the cybercrime area, with the Internet in particular, is transforming the criminal landscape as a whole, having almost a revolutionary effect, moving traditional criminal problems like drug dealing into the online environment. That is important, because the police powers online are much lower than they are on the streets.

Therefore today's drug dealer is not on your street corner; he is actually trading almost any type of illicit drug, almost any quantity from the comfort and privacy of his own home with almost zero risk of being identified. The same for today's bank robber, who is not carrying a gun anymore and wearing a balaclava going into a bank; he is doing it in virtual form, stealing even more money, using highly sophisticated malware to do so. In some of the most recent operations that we had, we have been very surprised at just how sophisticated the cybercrime capability is and the millions, in some cases a billion dollar of losses, on multiple banks. So we are dealing with a new age of criminality that also has connotations in the terrorist domain as well. It is requiring a different kind of response, a much more concerted international community of law enforcement agencies, increasingly including the private sector as well. I think the Europol Cybercrime Centre is part of the response. I think we are having an effect in dealing with this problem. I would like to thank in particular our German colleagues who are playing a leading role in our centre.

Moderator: Herzlichen Dank. Ich denke, es macht Sinn, dass wir jetzt an dieser Stelle, da Mr. Wainwright nur bis 13 Uhr bei uns sein kann, vielleicht Fragen von Ihnen an ihn direkt richten lassen. Gibt es Fragen?

Frage: The recent attack on the German parliament, its IT—was Europol involved in that case?

Rob Wainwright: No, we are not involved in that case, at least not yet. We stand ready through our Cybercrime Centre to provide the German authorities with any help that we can, of course. It is fair to say though, when we monitor the ability of police and security authorities around Europe to deal with such attacks, our observation is that Germany is relatively advanced in its national capability. Herr Maaßen, of course, and Herr Hange are in a better position to reply to that. From my observation, at a European level, I don't think Germany particularly needs the help of Europol in this attack, but of course we are always ready to play any part it wishes.

Frage: Britta Hilpert from ZDF. From your observation, is what we have seen at the Bundestag something that is an all day occurrence, or do you observe that other parliaments in the EU or in Europe have been attacked in the same way?

Rob Wainwright: Certainly an all day occurrence around the world are multiple similar attacks on a range of institutions, both public and private institutions; five in every six major international companies are the victims of a breach every year. Regarding public institutions we have heard of similar data breaches from public records in the United States, for example. So, I would not say that every parliament in Europe is under such attack, but I think what it tells us it that in the public domain and the private domain, we have to expect that we are now living in an age where such cyber security attacks are at least attempted on a regular scale. We also have to accept that even the most well respected, well protected institutions, for example in the financial industry, can expect to be breached sometimes. Therefore, we shouldn't talk about trying ever to get to a point of zero risk, where we can completely eliminate the threat; it is beyond that now. We should be talking about resilience, about developing better awareness and more sophisticated layers of defence mechanisms that can build a better level of resilience. I am not surprised, therefore, that we have seen an attack such as this. But at the moment we don't see it every day on every parliament in Europe, of course.

Moderator: Sie haben die Möglichkeit zu weiteren Fragen an Rob Wainwright, den Direktor von Europol. Sie bekommen ein Mikrofon angereicht.

Frage: Sonja Peteranderl von Wired Germany. I want to ask how the political situation with Russia hampers also the fight against cybercrime?

Rob Wainwright: Good question. We recognise that in a large proportion of all the investigations we are involved in, we are dealing with the Russian-speaking criminal—Russian-speaking, so not necessarily from Russia itself. Therefore, that requires a certain level of cooperation with our counterparts in Russia. Therefore, in an ideal state, we would prefer to have better cooperation with the authorities than we have at the moment. We understand, however, it is not possible for obvious reasons. We still, find alternative means by which to work on this case, in particular by building our capability inside Europe and with the United States especially.

Moderator: Any other questions concerning Europol? No. Thank you, Mr Wainwright for being our guest.

Rob Wainwright: Goodbye.

Moderator: Ja, meine Damen und Herren, wir gehen weiter in unserer Pressekonferenz anlässlich der Potsdamer Sicherheitskonferenz. Wir haben zu Gast bei uns auf dem Podium auch den Präsidenten des Bundesverfassungsschutzes, Dr. Hans-Georg Maaßen, und den Präsidenten des Bundesamts für die Sicherheit in der Informationstechnologie, Herrn Michael Hange, und wir haben bei uns den Gastgeber der Konferenz, Prof. Christoph Meinel. Meine Fragen an Dr. Maaßen: Sie sind gleich der Keynote Speaker, etwa ab 14 Uhr. Wollen Sie uns jetzt schon verraten, wie Sie zusammenfassend die Cyber-Sicherheitslage in Deutschland in Hinblick sicherlich auch auf die aktuellen Ereignisse sehen?

Hans-Georg Maaßen: Wir stellen fest, dass die Konflikte in der Realwelt auch in der Cyber-Welt ausgetragen werden. Es ist eigentlich eine Welt, Cyber-Welt und Realwelt. Das wurde ganz deutlich mit dem Angriff auf TV5 Monde, der mutmaßlich – wir müssen immer noch mutmaßlich sagen – vom Umfeld des Cyber-Kalifats oder von IS-Unterstützern durchgeführt wurde. Wir haben es auch gesehen mit Blick auf den Angriff auf Charlie Hebdo in Paris, wo es in der Folge mehr als 20.000 Defacements gegeben hat im Cyber-Raum. Das heißt, die Auseinandersetzungen, die Terroranschläge und extremistischen Gewalttaten in der Realwelt spiegeln sich auch im Cyber-Raum wider. Wir sehen auch die Auseinandersetzung von Ost und West im Cyber-Raum. Denken Sie an die DDoS-Angriffe auf die Website der Bundeskanzlerin im Januar, die mutmaßlich einen ukrainischen Hintergrund hatten. Das heißt also, wir können nicht sagen: Auf der einen Seite haben wir den Cyber-Raum, um dessen Sicherheit wir uns kümmern, und dann die Realwelt, um die kümmern sich dann die inländischen Behörden oder die Bundeswehr, sondern es ist ein Raum. Und wenn sich in dem einen Raum in der Realwelt etwas verändert, wird sich auch etwas in der virtuellen Welt verändern. Wir sehen auch, dass der Cyber-Raum eine immense Attraktivität für unsere Gegner in der Realwelt hat, weil es ein asymmetrischer Raum ist. Das ist beim Angriff auf Sony Pictures Entertainment deutlich geworden, der mutmaßlich von Nordkorea gesteuert wurde. Denken Sie daran: Nordkorea ist ein bitterarmes Land, Nordkorea hat mutmaßlich noch nicht mal einen einzigen Geldcomputer und wohl nur drei Zugänge zum internationalen Internet. Aber die haben hochentwickelte Hacker, die in der Lage sind, Cyber-Angriffe zu fahren und Großunternehmen in die Knie zu zwingen bzw. zu erpressen. Sie sind in der Lage, die westliche Industrieinfrastruktur anzugreifen. Wir können im Gegenzug nichts gegen Nordkorea im Cyber-Bereich machen, weil Nordkorea nichts hat. Das ist eine Asymmetrie. Also Nordkorea kann mit relativ wenig sehr, sehr viel Schaden bei uns anrichten, und wir können nicht auf der gleichen Ebene zurückschlagen. Dieser Cyber-Raum führt dazu, dass es eine Neuverteilung auch der Waffen gibt. Staaten, die wir immer als schwach angesehen haben, haben die Möglichkeit, uns anzugreifen, uns wehrlos zu machen. Dazu kommt, dass der Cyber-Raum auch ein Raum der Anonymisierung ist. Wir wissen letztendlich nicht hundertprozentig, ob es Nordkorea war, oder ob hinter dem mutmaßlichen Attentäter nicht noch ein anderer steht. Es sind also erhebliche Bedrohungen, die wir sehen, eine Veränderung auch der Gewichte, diese Asymmetrie, die dieser Cyber-Raum bietet. Aber alles in allem muss man sagen, ist es eine Welt - die Realwelt und die Cyber-Welt - und Konflikte in der einen Welt, in der Realwelt werden in der Cyber-Welt ausgetragen. Das ist für uns derzeit eine ausgesprochene Herausforderung.

Moderator: Herzlichen Dank. Kommen wir in der Reihe der Opening Statements zu Ihrem Nachbarn zur Linken, zu Herrn Hange. Herr Hange, Sie werden sicher gleich gefragt werden: Was haben Sie heute Morgen dem Bundestag, der IuK-Kommission gesagt? Wir sind schon gespannt, ob Sie etwas

sagen. Aber wenn Sie es zunächst vielleicht ein bisschen grundsätzlicher sehen: Wie wollen Sie vom Bundesamt für Sicherheit in der Informationstechnik dazu beitragen, dass die gefühlte und die tatsächliche Sicherheit der Internetnutzer in Deutschland zunimmt oder wieder zunimmt?

Michael Hange: Also gefühlt und tatsächlich… wir gehen erst mal von der tatsächlichen Sicherheit aus. Aber Sie haben Recht: Gefühlte Sicherheit hat auch etwas mit Vertrauen zu tun, Vertrauen in Technologie. Damit würde ich einfach mal anfangen. Wir leben von der Technologie, wie sie sich entwickelt und laufend weiterentwickelt. Während wir hier sitzen werden neue Apps entwickelt. Industrie 4.0 ist ja nichts, wofür ein Startschuss gegeben wird durch Politiker, sondern das läuft schon längst. Also das Internet und Internet-Mechanismen durchdringen immer mehr die Welt. Aus dem Rollenverständnis des BSI ist es so: Wir haben eine Beratungsfunktion, wir haben eine Schutzfunktion und wir haben eine Warnfunktion. Warnung auch, wenn etwas passiert. Wir ergänzen uns in dem Kontext auch mit den klassischen Sicherheitsbehörden. Die Gefährdungslage, wie sie sich darstellt, ist in der Tat so - Herr Maaßen sprach von Asymmetrie zwischen Angreifern und Verteidigern; man kann es in der Cyber-Welt wirklich auch von den Angriffsmöglichkeiten her so sehen. Ein Angreifer kann sich den Punkt aussuchen, die Schwachstelle aussuchen, wo er reingeht; der Verteidiger muss sehen, dass er das System in der ganzen Breite wie eine Kette, bei der man das schwächste Glied herausfinden kann, schützt. Software ist Menschenwerk und ist, weil es Menschenwerk ist, mit genug Schwachstellen ausgestattet. Wenn man eine Zahl nennt für gute Software, vom Hasso-Plattner-Institut begleitet, dann hat diese vielleicht 0,3 Promille Fehler, Standardsoftware 3 bis 5 Promille. Das heißt, Sie finden Tausende von Schwachstellen, die man ausnutzen kann. Und das zeigt die Situation, wie sie sich heute darstellt. Das war noch ein Ponyhof um 2000 herum, heute gibt es eine Szene, die das ganz systematisch ausbeutet und ausnutzt und damit Schwachansatzpunkte findet. Der zweite Punkt ist der, dass natürlich immer noch eine gewisse digitale Sorglosigkeit da ist – da sind wir bei der gefühlten Sicherheit –, dass wir nicht direkt betroffen sind, und Sicherheit lebt von Vorfällen. Also wenn es normal läuft, fühlt man sich nicht betroffen, aber wenn etwas passiert… Sie haben heute ein Ereignis angesprochen. Wenn man mal den Loveletter-Virus unter Stuxnet nimmt für die NATO: Das sind Fanale gewesen. Da sind Signale gesetzt worden, die das einfach deutlich machen. Was heute wesentlich ist: Wir werden nicht mehr Sicherheit garantieren können mit Prävention. Kryptographie ist ein sehr starker Mechanismus, das ist klassisch. Aber heute in der Cyber-Welt können wir es nicht mehr garantieren. Das heißt, wir brauchen einen Mix von präventiven Maßnahmen, wir brauchen aber auch eine effiziente Detektion, und wir brauchen auch ein professionelles Reagieren, wenn etwas passiert. Denn das unterscheidet unsere Aufgaben: Wir interessieren uns für die technischen Ursachen von Cyber-Angriffen, Herr Maaßen dann für die Folgen, wenn etwas passiert, oder das Bundeskriminalamt für die Kriminalität. Deshalb ist auch die Zusammenarbeit, der Kooperationsaspekt heute so zentral, denn wir werden das Thema nur in Zusammenarbeit mit den Sicherheitsbehörden bewältigen. Deshalb haben wir auch das Cyber-Abwehrzentrum, wir kümmern uns um die technische Analyse. Aber wir dürfen den Cyber-Raum für den Angreifer nicht so attraktiv machen, dass er sich sicher fühlt, dass er nicht entdeckt wird. Das heißt, wir müssen auch die Fälle haben, und zwar häufig, wo eine Tat dann zur Verhaftung eines Täters oder zur Benennung eines Täters führt, um einfach deutlich zu machen: Es ist kein risikoloses Geschäft. Aber was wesentlich ist: Auch aus Detektion - das ist unsere Aufgabe, eine Kernaufgabe, die in den letzten Jahren immer wichtiger geworden ist - lernen, was wir für die Prävention besser machen können. Es gibt keine staatlichen Sicherheitskonzepte mehr, sondern wir müssen in dynamischen Prozessen leben. Da arbeiten wir auch intensiv zusammen mit dem Hasso-Plattner-Institut, denn das ist eine Herausforderung für Wissenschaft und Wirtschaft. Wir brauchen

Kooperationsmodelle, um dieses Thema anzugehen. Einen Lichtblick habe ich: Wenn man alle Sicherheitsmaßnahmen, die man ableitet aus Angriffen, wirklich konzentriert auf ein System, dann hat man einen ziemlich hohen Grad von Sicherheit für Standardangriffe. Auch Angreifer haben ein Kosten-Nutzen-Modell, so dass sie sagen: Wenn wir leicht reinkommen, tun wir es. Leider müssen wir feststellen: Es sind oft sehr simple Maßnahmen, mit denen man schon Erfolg hat. Aber das müsste unser Ansatz sein. Und insofern darf man jetzt nicht nur – so ist das manchmal in der Presse, muss ich sagen – von den Vorfällen reden, sondern wir müssen auch ein Auge auf die Lösungsansätze werfen, die sich anbieten, und sie auch aufzeigen, und da sind wir bei der gefühlten Sicherheit, dass jeder etwas tun kann: der Bürger selbst, aber auch ein Unternehmen, auch die Verwaltung selbst.

Moderator: Vielen Dank für den zugespielten Ball. Wir sind beim Wissenschaftler in der Runde, bei Prof. Christoph Meinel, der nicht nur der Direktor des Hasso-Plattner-Instituts ist, sondern auch der Leiter des Fachgebiets Internet-Technologien und Systeme, das sich schwerpunktmäßig auch mit dem Feld der IT-Sicherheit beschäftigt. Sie sind heute Morgen auf ein interessantes System eingegangen, bei dem ich mich gefragt habe: Wenn der Bundestag es gehabt hätte, hätte er mit hoher Sicherheit das abwehren können, was jetzt passiert ist? Es geht um die Erkennung und Analyse von Cyber-Angriffen in dem Augenblick, wo sie ausgeführt werden. Können Sie dazu noch ein paar mehr Details sagen? Ich denke, das ist sehr, sehr spannend. Wahrscheinlich interessiert die Öffentlichkeit auch, was die Wissenschaft dazu beitragen kann durch Ausbildung der Experten, so dass diese sicheren Anwendungen, die jeder fordert, dann auch wirklich benutzerfreundlich werden und das es nicht so schwierig ist, an vielen Stellen etwas zu verändern, damit ich einen besseren Sicherheitslevel in meiner Software und vielleicht auch in meiner Hardware habe.

Christoph Meinel: Als Institut, das junge Leute ausbildet, die in dieser IT-Welt tätig werden als Programmierer, als Architekten, als IT-Ingenieure, als Information Officer, haben wir das Privileg, ein Stück weiter zu sehen, was auf uns zukommt. Die Digitalisierung - Herr Maaßen, Sie sprechen schon von einer Welt, ich würde sogar fast noch von zwei Welten reden, nämlich unserer physikalischen Welt, die in all ihren Dingen einen digitalen Spiegel, einen digitalen Oberbau kriegt, der mit der realen Welt immer mehr verkoppelt ist. So entsteht eine zweite Welt, die aber natürlich in ihren Auswirkungen als eine Welt funktioniert. Es besteht dort die Möglichkeit, Eingriffe gar nicht mehr über physikalische Dinge, sondern über Steuerungsmechanismen vorzunehmen. Genau das ist auch die Idee dieser Konferenz: Es wird nicht die Technik geben, bei der wir mit einem Fingerschnipsen sicher sind. Sondern das ist ein so komplexes System, das fängt an, wie sich Menschen verhalten, wie wählen sie Passwörter aus, bis hin dazu, welche Systeme kommen zum Einsatz, welche Architekturen kommen zum Einsatz, wie wird sichergestellt, dass bei allen Sicherheitsarchitekturen auch der laufende Betrieb immer untersucht wird? Denn da haben wir natürlich ein Wettrüsten: auf der einen Seite neue Techniken, digitale Sicherheit zu gewährleisten, Angriffe zu erkennen, und auf der anderen Seite natürlich auch die Möglichkeiten, neue Angriffe zu fahren. Sie haben die Schwachstellen erwähnt. Das muss man vielleicht auch noch ein bisschen deutlicher sagen. Diese Schwachstellen in der Software, das sind die vorhersehbaren Punkte für Angriffe, die es - geschickt kombiniert - ermöglichen, zum Beispiel Zugang zu irgendwelchen sensiblen Daten zu bekommen, die man dann mitlesen kann, also Wirtschaftsspionage. Die man manipulieren kann, um irgendwelche Dinge durcheinander zu bringen, zu beeinflussen, Missgunst, Misstrauen zu säen. Das ist die Palette, und da muss jeder an seiner Stelle tätig werden. Insofern wieder dieser Universitätsgedanke: Wir müssen all die, die beteiligt sind, zusammenbringen auf neutralem Boden, wie das unser Institut sein kann, und wir müssen auch Informationen bereitstellen, glaubend, dass wenn die Menschen wissen,

was sich technisch abspielt, sie ihr eigenes Verhalten reflektierter durchführen. Ich komme noch mal auf dieses Beispiel der Passwörter zurück. Vielleicht haben Sie gesehen, es sind von solchen ganz sensiblen Daten wie Passwort oder Bank-Account 200 Millionen im Internet frei verfügbar. Gestohlen irgendwoher, zum Beispiel von Sony. Wenn man dann analysiert, welche Passwörter haben die Menschen – dann ist das am häufigsten verwendete Passwort: 123456. Wenn das als Passwort eingesetzt wird, dann ist das ein Zeichen, dass derjenige, der dieses Passwort nutzt, aber auch gar nicht verstanden hat, dass es nicht um Bequemlichkeit geht, sondern dass es um den Schutz seiner Daten, um den Schutz seines eigenen Systems geht. Denn ein solch simples Passwort kann jeder leicht erraten, und jeder, der das erraten kann, kann dann im Namen dieses Menschen Dinge tun, Angriffe fahren, einkaufen, was immer. Also diese Awareness-Schulung halten wir für sehr wichtig. Insofern ist das die Kehrseite, denn wir können nicht auf eine Regierung warten, wir können nicht auf ein Produkt einer Firma warten, das für uns das Sicherheitsproblem löst. Wir müssen jeder an seiner Stelle seinen Beitrag leisten und mitwirken.

Moderator: Das war die Runde der Eingangsstatements. Ich hoffe, das war eine ganze Menge Munition. Sie haben noch eigene. Einer der Ersten, der sich gemeldet hat, war Herr Sagurna vom MDR. Bitteschön. Melden Sie sich bitte, sagen Sie Ihren Namen und zeigen Sie, dass Sie ein Mikrofon brauchen. Unsere jungen Herren links und rechts reichen Ihnen eines an.

Frage: Meine Frage geht an Herrn Hange: Sie sind nicht zuständig für die IT-Infrastruktur des Bundestages, dennoch haben sie eine beratende Funktion. Sind Sie schon um Ihren Rat gefragt worden, und wenn ja, welchen haben sie dem Bundestagspräsidenten Lammert gegeben oder werden ihm geben bezüglich seines Problems?

Michael Hange: Im Bundestag gibt es Gremien, die sich damit befassen. Wir sind in der Tat beratend tätig, aber Beratung bedeutet auch ein besonderes Vertrauensverhältnis; gerade in diesem Fall deshalb möchte ich zu Details jetzt nichts sagen

Moderator: Weitere Fragen? Ich sehe dort hinten eine Frage.

Frage: Können Sie uns eine Orientierung geben, weil zu viel durch die Medien schwirrt, und wir wissen gar nicht genau, was eigentlich genau passiert ist im Deutschen Bundestag. Können Sie uns eine Idee geben?

Michael Hange: In welche Richtung?

Frage: In der Richtung von: Wie sicher oder unsicher ist das System? Müssen Hardware und Software komplett ausgetauscht werden? Welche Dimensionen hat das finanziell? Und auch welche Folgen kann es haben aus Ihrer Sicht?

Michael Hange: Ich muss dazu sagen: Der Bundestag ist selbst verantwortlich für die IT. Insofern trifft der Bundestag die Entscheidungen, die zu treffen sind, selbst. Wir haben ein beratendes Mandat ihm zu helfen. Das gebietet es, auch dieses Vertrauensverhältnis besonders zu respektieren.

Moderator: Frau Steger vom Rundfunk Berlin-Brandenburg.

Frage: My question is addressed to Dr. Jamie Shea. You say in your sheet here: NATO considers that a cyber attack could be the equivalent of an armed aggression and therefore trigger a paragraph 5

collective defence response. What specific attack could this be? I think we agree that this could not be a minor attack, but what is in your eyes a severe attack, which would legitimate such a response?

Jamie Shea: Thank you for that. Well, first of all, I cannot give you a precise example, because we have not yet declared article 5 in response to a cyber attack. We have declared paragraph 5 once, as you remember, in response to a terrorist attack after 9-11. So this does demonstrate that the NATO "Bündnisfall" - as you say here - the paragraph 5, does apply to attacks more broadly than the Cold War scenario of tanks that we were thinking of 30 years ago. But I also said in my speech today that NATO has not defined the exact threshold, and for a good reason. Because if we define the precise threshold, we would send to an aggressor the kind of message that it is ok to attack NATO up to this levelnothing is going to happen. But if you go beyond it, then there will be a response. That would not serve deterrence, because trying to have deterrence against cyber attacks is also important. So it is a potential possibility, but it would depend upon the severity of the attack. It would also depend, of course, upon attribution of the aggression. Because after 9-11 it was when the United States was able to demonstrate that the attacks came from Afghanistan that NATO declared paragraph 5—and of course the collective appreciation by the allies. But it does demonstrate that we consider - if a cyber threat is sufficiently serious - that in certain cases NATO solidarity, as a response, would be called upon. But, as I said, I think it is best to keep potential aggressors guessing in that particular area.

Moderator: Die Nächste ist Britta Hilpert vom ZDF.

Frage: Noch mal eine Frage: Von allen Experten habe ich heute gehört, dass auch das Problem ist, dass viele User, viele Nutzer ein bisschen zu sorglos sind. Awareness ist ein ganz großes Thema hier. Auch noch mal an Sie, Herr Hange, natürlich vor dem Hintergrund der Attacke auf den Bundestag: Wie verbindlich sind denn eigentlich die Empfehlungen des BSI für Bundesbehörden, die Sie beraten, oder für Bundesinstitutionen wie den Bundestag, sich eben an Sicherheitsmaßnahmen im Cyber-Bereich zu halten?

Michael Hange: Es ist sehr unterschiedlich. Ich sagte ja, Rolle des BSI ist: Wir haben eine Schutzfunktion für das Regierungsnetz, und dort bestimmen wir auch Spielregeln für die angeschlossenen Behörden. Das bedeutet zum Beispiel beim Geheimschutz, dass man nur von uns zugelassene Kryptogeräte einsetzt. Das ist aus der Tradition sehr klar. Es ist aber auch so, dass die Macht von Empfehlungen nicht unterschätzt werden kann. Wir müssen einfach bedenken, Informationstechnik ist so innovativ, dass man sie nicht durchregulieren kann. Eine völlig durchregulierte Informationstechnik würde keinen Bestand haben, würde auch dem Innovationsfaktor, auch dem Marktfaktor Informationstechnik einfach völlig zuwiderlaufen. Das heißt, wir haben regulativ an sich relativ wenige Rechte. Wir haben in der Bundesverwaltung, wir haben für Geheimschutz diese Woche, Frau Staatssekretärin Rogall-Grothe hat es erwähnt, das IT-Sicherheitsgesetz in der Verabschiedung. Das weist uns auch eine Funktion zu für den Schutz von kritischen Infrastrukturen. Aber auch dieser Ansatz ist kooperativ angedacht. Denn Informationstechnik ist so komplex, wie Prof. Meinel das auch erläutert hat, insofern: Digitale Sorglosigkeit hat zwei Facetten. Das ist zum einen die Komplexität der Informationstechnik, zum anderen ist es aber auch das Nichtwissen um die Gefährdung oder auch um Schutzmöglichkeiten. Das sind die zwei Facetten. Aber wenn man hier den Bereich [kritische Infrastrukturen] nimmt, stellt man fest, dass da, wo von den Schäden her ein Regulierungsbedarf da ist, dass man es dort angeht. Alle Industrienationen, Also das IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen ist nicht

alleine eine deutsche Erfindung, sondern findet in Europa statt, Frankreich hat auch schon ein entsprechendes Gesetz. Insofern will ich die Frage so beantworten: Jeder ist für seine Informationstechnik erst mal selbst verantwortlich und damit auch für den Schutz. Wichtig ist dort, wo man feststellt, dass das Know-how nicht da ist, dass das Wissen nicht da ist, dass man Hilfestellung gibt. Insofern hat das BSI umfangreiche Empfehlungen wie das Grundschutzhandbuch oder die Allianz für Cyber-Sicherheit, das machen wir mit 1200 Institutionen aus Wissenschaft und Wirtschaft, so dass man hier versucht, Empfehlungen heranzutragen. Da ist der fruchtbare Boden, einfach das Bewusstsein dafür, also Awareness. Sicherheit fängt auf der Chef-Ebene an. Es ist nicht nur eine Frage der Techniker oder der Nutzer, sondern die IT-Sicherheit muss in jedem Unternehmen organisiert werden

Frage: Eine kurze Nachfrage: Es sind Empfehlungen, keine Verpflichtungen?

Michael Hange: Empfehlungen. Zum Teil haben wir aber auch den Fall zum Beispiel im Grundschutzhandbuch, dass bestimmte Bereiche als Selbstverpflichtung gelten, wenn etwa die Verwaltungen sagen: Wir setzen das - wie die Polizeien - als Standardgrundschutz ein und gehen danach vor. Da hat dann im Grunde die gleiche Wirkung.

Moderator: Auf meiner Liste stehen jetzt Frau Binsch, DPA Netzwelt, Herr Wenk, Potsdamer Neueste Nachrichten, und Jan Rähm, Deutschlandfunk. Herr Sagurna anschließend. Bitte, Frau Binsch.

Frage: Dann mache ich mal weiter. Der Herr Wainwright hat ja jetzt auch gerade noch mal erklärt, dass man eigentlich solche Eingriffe sehr häufig sieht und auch Sie beide, Herr Maaßen und Herr Hange, warnen ja regelmäßig davor. Da muss ich sagen, es überrascht doch etwas, dass der Bundestag jetzt so vollkommen überrollt wird von dieser Attacke. Können Sie das noch mal einordnen, wurden Sie davon wirklich so überrascht, und könnte das auch anderen Behörden des Bundes passieren?

Michael Hange: Ich fange mal an, und die Sicherheitsbewertung wird dann von Herrn Maaßen kommen. Also es ist so wie Herr Wainwright gesagt hat, Cyber-Angriffe sind heute alltäglich. Im Jahresbericht haben wir es erwähnt - wir haben zum Beispiel inzwischen 17.000 DDoS-Angriffe in einem Vierteljahr. 17.000, wo versucht wird, Websites im Grunde zu blockieren, wo man Server blockiert. Es wird nicht festgestellt, weil es kein großer Angriff ist, sondern viele kleine. Im Jahresbericht haben wir auch gestohlene Identitäten. Wir haben mal diese großen Fälle gehabt, aber wir bekommen jetzt täglich bis zu 20.000 gestohlene Identitäten, die wir an Provider weiterreichen, wo dann die Provider ihre Kunden warnen. So ist es auch mit den Angriffen als solche, Phänomen Angriff. Welche Schäden dann entstehen, das ist Aufgabe von Herrn Maaßen, das zu bewerten. Es ist keine Überraschung, dass so etwas passiert. Ist es ist sicherlich dann aber für eine Institution, und da komme ich auf die Qualität der Angriffe: Es gibt Normalangriffe, die man auch mit normalen Mechanismen abwehrt. Aber wenn es sehr komplexe Angriffe sind, ist es natürlich so, dass es sehr schwierig ist, dem zu begegnen, und dass man auch dann mit fremder Hilfe im Grunde nur effizient, also professionell reagieren kann. Und diese Dimension hat zugenommen, ist nicht nur im nachrichtendienstlichen Umfeld zu verorten, sondern inzwischen sind kriminelle Organisationen arbeitsteilig international auch viel besser aufgestellt und nutzen dann sehr avancierte Angriffsmethoden.

Moderator: Dr. Maaßen, wollen Sie gleich dazu ergänzen?

Hans-Georg Maaßen: Ja. Wir schauen uns als Bundesverfassungsschutz die Normalangriffe normalerweise auch gar nicht an. Die Normalangriffe können normalerweise auch von jeder fortgeschrittenen IT-Infrastruktur abgewiesen werden. Wir interessieren uns in erster Linie für nachrichtendienstliche Angriffe, seien es Angriffe, die von Nachrichtendiensten direkt lanciert werden, oder wo wir den Eindruck haben, dass organisierte Kriminalität oder Hackergruppen zwischengeschaltet werden. Wie Herr Hange schon sagte: Es gibt fortgeschrittene Hackergruppen, die hochqualifizierte Angriffe fahren, wo wir den Eindruck haben, dass es Nachrichtendienste gibt, die diese Angriffe outsourcen an diese Hackergruppen. Was wir im Bundestag gesehen haben, ist in meiner Wahrnehmung schon ein beachtlicher Angriff. Aber ich muss es mit aller Zurückhaltung sagen, weil wir zwar für die Spionageabwehr die zuständige Behörde sind, den Bundestag auch aufmerksam gemacht haben am 12. Mai auf diesen Angriff, aber bisher in die Aufklärung des Vorfalls noch nicht eingebunden sind.

Moderator: Erik Wenk von den Potsdamer Neuesten Nachrichten.

Frage: Auch noch mal gleich eine Frage an Herrn Maaßen: Welche Rolle kann der Verfassungsschutz in Deutschland eigentlich spielen für Cyber-Sicherheit? Inwiefern ist der Verfassungsschutz in der Lage oder kann das leisten, solche Angriffe abzuwehren? Und ist das die Hauptbehörde, die damit befasst ist, oder muss da auch mit BKA, mit BND … Also wie ist der Verfassungsschutz dazu verorten?

Hans-Georg Maaßen: Wir sind ein Netzwerk im Bereich der Cyber-Abwehr. Jeder hat seine eigene Rolle zu spielen. Herr Hanges Behörde ist in erster Linie für die Technik zuständig. Wir sind für die Aufklärung zuständig. Wer könnte dahinter stecken? Was könnte derjenige vorhaben? Und wer könnte als Nächster angegriffen werden? Wenn wir zum Beispiel einen Cyber-Angriff gegen einen Zulieferer in der Wirtschaft feststellen und Herr Hange uns mit seiner Behörde berichtet, was die technischen Parameter und Hintergründe sind, können wir dann aufklären, inwieweit vielleicht in der Realwelt ein paralleler Angriff läuft, ob vielleicht ein anderer Zulieferer auch betroffen ist, ob wir vergleichbare Parameter auch bei einem Angriff gegen das Hauptunternehmen sehen. Wir können auch aufklären, ob wir vielleicht in der Vergangenheit derartige Angriffsparameter in einem ganz anderen Zusammenhang gesehen haben, und Rückschlüsse ziehen, ob es einen chinesischen, einen russischen oder wie auch immer gearteten Hintergrund hat. Aber wir sind auch nur ein Spieler. Wir brauchen beispielsweise auch den Bundesnachrichtendienst, der sehr gute Kenntnisse hat über die technische Leistungsfähigkeit unseres Gegenübers im Ausland, der uns zum Beispiel auch sagen kann: Aufpassen, auf der Einkaufsliste der Chinesen steht derzeit - sage ich mal willkürlich und salopp - die optische Industrie in Deutschland. So etwas kann der Auslandsnachrichtendienst mitteilen. Daraus können wir Rückschlüsse auch ziehen auf die jeweiligen Industrieunternehmen und dann branchenspezifische oder unternehmensspezifische Beratung durchführen, was die Awareness angeht. Und das BSI kann dann, was die IT-Infrastruktur von derartigen Branchen angeht, Hinweise geben.

Moderator: Jan Rähm vom Deutschlandfunk.

Frage: Meine Frage geht vorrangig erst mal an Herrn Hange, aber auch gerne an Herrn Maaßen: Sie haben ja eben schon angesprochen das IT-Sicherheitsgesetz, und wir haben ja jetzt gerade den großen Vorfall im Bundestag. Das IT-Sicherheitsgesetz ist ja weiterhin sehr reaktiv. Die Vorsorgekomponente fehlt meiner Ansicht nach dann doch ein bisschen. Worüber wir seit vielen Jahren sprechen, ist eine Meldepflicht für Sicherheitslücken. Die findet sich immer noch nicht, nicht

mal annähernd. Wir haben eine Meldepflicht für irgendwelche Vorfälle, die aber auch nicht ganz konkret beschrieben sind, eigentlich nur, wenn es richtig weh tut, wie jetzt, dass es gemeldet werden muss. Müssten wir das nicht eigentlich ein bisschen mehr vorantreiben? Oder um bei „schwammig“ zu bleiben: Es steht wieder drin „Sicherheit auf dem Stand der Technik, also die Geräte sollen dem technischen Stand entsprechen. Wer bestimmt denn, was der technische Stand ist? Es ist alles ein bisschen arg schwammig, was in diesem Gesetz drin steht, und es ist halt keine Vorsorgekomponente in dem Sinne erkennbar.

Michael Hange: Ich übernehme die Antwort. Das IT-Sicherheitsgesetz ist zum einen der Einstieg überhaupt in eine Kooperation auf einer gesetzlichen Basis mit der Wirtschaft. Und zwar der Wirtschaft mit den kritischen Infrastrukturen. Sie müssen einfach auch sehen, da prallen natürlich auch Meinungen politisch aufeinander. Also wenn Sie die ersten Stellungnahmen der Wirtschaftsverbände gesehen haben, dann wird das als sehr große Belastung empfunden. Es ist wichtig und so hat es auch Minister de Maizière gesehen, dass das jetzt die Antwort auf die Bedrohung zurzeit ist und die im Grunde einen Einstieg darstellt. Wo wir in 15 Jahren sind - keiner kann Cyber-Angriffe genau vorhersagen oder wen es trifft. Man kann nur sagen, es wird sich weiterentwickeln. Ich glaube aber, dieser Viertakt ist wichtig: Mindeststandards durch die Branchen selbst formuliert. Sie dürfen ja nicht vergessen, es handelt sich hier nicht nur um Bürokommunikation, sondern es handelt sich um Industriesteuerungssysteme, die gesteuert werden, wo also die Sicherheit auch etwas anders formuliert wird. Und das ist ein wichtiger Punkt. Die Orientierung gibt zum Beispiel der IT-Grundschutz, um zu sagen: Wie verstehen wir Sicherheit? Denn auch dort ist das ein Prozess mit der Wirtschaft. Natürlich: Hundertprozentige Sicherheit lässt sich mit Standards nicht verbinden. Der Begriff „Stand der Technik“ ist übrigens dem Umweltrecht entnommen. Dort spricht man auch bei entsprechenden Maßnahmen vom Stand der Technik. Stand der Technik hat insbesondere folgenden Vorteil, dass – und da kommen die Meldepflichten rein – wenn Sie Angriffe beobachten, dem BSI auch gemeldet wird, in welcher technischen Ausprägung. Dann können Sie nachsteuern. Und das ist die Erfahrung heute. In den 90er Jahren, sozusagen dem Goldfischteich, haben wir noch Sicherheitskonzepte präventiv gemacht mit der Perspektive von drei bis vier Jahren. Heute macht man Konzepte und weiß aber, dass man bei den Sicherheitskonzepten nachsteuern muss, je nachdem, was passiert. Es ist also eine permanente Lernkurve dabei. Was wir zusätzlich noch machen: Das Amt gibt jährlich einen Lagebericht. Dieser Lagebericht wird mit Informationen gefüttert von dem, was passiert, sodass auch alle anderen in der Wirtschaft eine Vorstellung bekommen. Ich sage noch mal: Die Zusammenarbeit der Behörden ist wichtig. Sie dürfen nicht nur jeden einzelnen Angriff sehen. Herr Maaßen hat auch gesagt: Wir müssen ganze Komplexe betrachten. Also wenn einer ein Ziel im Auge hat, dann versucht er das auf verschiedenen Wegen in der Realwelt, aber auch in der Cyber-Welt. So ist es ganz wichtig, dass wir Fälle zusammenbündeln mit gleicher Methodik und dann auch Rückschlüsse auf Täter ziehen können. Wir müssen also viel stärker auch das Denken der Angreifer mit in die Abwehr einbeziehen. Denn hundertprozentiger Schutz wäre heute nicht mehr finanzierbar, sondern wir müssen einen angemessenen Schutz finden, der natürlich genau die Bedrohungslage im Auge hat. Insofern ist, da kritische Infrastruktur unser Gemeinwohl berührt, das eine wesentliche Komponente auch der Daseinsvorsorge.

Frage: Ganz kurz die Nachfrage: Diese Meldepflicht für IT-Sicherheitslücken, da sind sie jetzt ein bisschen dran vorbeigeschrammt , da reden wir seit vielen Jahren drüber, seit vielen Jahren kommt die nicht, in keiner Art und Weise. Wir haben gesehen, teilweise dauert die Reaktion auf eine bekannte Sicherheitslücke anderthalb Jahre. Ich denke da an die Siematic bei Siemens, das hat knapp

anderthalb Jahre gedauert, ehe die Lücke dann geschlossen war. Brauchen wir diese Verpflichtung auch, Sicherheitslücken schnellstmöglich zu schließen? Oder, da kommt Herr Maaßen möglicherweise ins Spiel, sind die Dienste, die Geheimdienste, die Nachrichtendienste daran selber viel zu sehr interessiert?

Michael Hange: Also ich nehme mal das, was Herr Meinel gesagt hat: Es gibt so viele Schwachstellen in Software, dass man nicht auf bekannte Lücken alleine bauen kann, aber das verantwortungsvolle Schließen von Lücken ist ein Punkt. Für uns ist wichtig, dass man verantwortungsvoll vorgeht, dass man dem Hersteller, der in einer Verantwortung für sein Produkt ist, auch die Gelegenheit gibt, zu schließen. Dieser Prozess, eine Software zu updaten, diese Lücke zu schließen, das muss gründlich geschehen. Es dürfen sich dann nicht neue Lücken auftun oder sich dann Fehler einschleichen. Das ist ein Punkt. Das hat die Wirtschaft aber zum Teil selbst erkannt. Google hat eine Initiative gestartet, dass sie sagen, im Grunde müssten alle Hersteller nach 90 Tagen die Lücke spätestens geschlossen haben, ansonsten kündigen sie an, dass da eine Lücke ist, die noch nicht geschlossen ist. Im Gesetz ist es jetzt so - und das meint den Bereich der Industrie-IT - dass eine Produktionsstraße nach anderen Gesichtspunkten läuft. Also wenn Sie die klassische nehmen, ist es so, dass eine Produktionsstraße eingerichtet wird und dann ändert man nichts mehr daran. Wir leben aber im Internet, Industrie 4.0, es kommen immer mehr Internetstandards. Das heißt, das muss man mit berücksichtigen, auch hier im Industrieumfeld müssen SCADA-Systeme angepasst werden. Da sind wir gerade bei dem System, was Sie angesprochen haben. Das wird sich erschließen, dass wir SCADA-Systeme oder Prozesssteuerungssysteme auch hinsichtlich Erfassung von Schwachstellen stärker in den Blick nehmen werden. Auch bei der Beseitigung solcher Schwachstellen.

Christoph Meinel: Als Wissenschaftler und als nicht involviert in die Gesetzgebung würde ich da gerne eine Bemerkung zu machen. Also der Glaube, dass ein Gesetz dieses Thema regelt, ist ein Irrglaube. Mit dem Gesetz kann ein Rahmen geschaffen werden. Ich glaube, es ist gut, was jetzt an neuem Rahmen hinzukommt. Und es ist auch schon sichtbar, was dieser Rahmen nicht abdecken wird. Aber das muss sein in einem Thema, was sich rasant entwickelt, wo es alle fünf Jahre neue Technologien mit ganz neuen Ansätzen gibt. Ich will Ihnen ein Beispiel nennen mit unserem Datenschutz. Der ist philosophisch basiert auf dem Prinzip der Datensparsamkeit. In einer Zeit heute, wo praktisch alle Geschäfte auf Big Data basieren, kommen wir da absolut an Grenzen. Das heißt, hier hat sich die Technik weiterentwickelt, die Ansprüche weiterentwickelt, und es müssten ganz neue gesetzliche Regelungen her. Nun ist das mit den gesetzlichen Regelungen schwierig, das ist ein langsamer Prozess, der da weitergeht. Also insofern ist das Gesetzt eine Hilfestellung, aber das Heil davon zu erwarten: Bitte nicht.

Moderator: Herr Nölke, dann Herr Sagurna, dann Frau Budde vom Deutschlandradio.

Frage: Mal eine Frage an Herrn Maaßen: Bietet da nicht die geplante Vorratsdatenspeicherung, sofern sie in andere Hände gerät, gerade im Ausland, das per Gesetz in der Lage ist oder wo es erlaubt ist, die Daten auch wirtschaftlich auszuwerten, nicht eine große Gefahr? Wie schätzen Sie das ein?

Hans-Georg Maaßen: Zum Einen ist es so, dass die sogenannten Vorratsdaten bei Unternehmen gespeichert werden sollen, nicht bei Behörden. Es soll eine Pflicht sein, und in Teilen machen die Unternehmen das jetzt schon aus eigenen Interessen, zum Beispiel zu Abrechnungszwecken. So gibt es Unternehmen, die die Daten in Deutschland erheben, ins Ausland transferieren und im Ausland

die Rechnungsstellung durchführen. Und dann werden die Rechnungen in Deutschland versandt. Das heißt, was wir derzeit sehen, ist, dass schon in großem Umfang sogenannte Vorratsdaten erhoben werden im Telekommunikationsbereich aus eigenwirtschaftlichen Interessen der Unternehmen, ohne dass es da irgendeine rechtliche Begrenzung gibt; dass diese Daten ins Ausland transferiert werden können – und in Teilen werden sie es auch – und auch aufgrund des dortigen Rechts – dort gilt nicht das deutsche Rechtsregime – dann auch möglicherweise gebraucht oder missbraucht werden. Ich sehe jedenfalls durch eine gesetzliche Verpflichtung zur Mindestspeicherung dieser Daten keine Erhöhung eines Risikos des Missbrauchs der Daten.

Frage: Eine kurze Nachfrage an Herrn Hange: Besteht die Möglichkeit, aus solchen Daten dann Verhalten, künftiges Verhalten, zu triangulieren? Also dass ich sagen kann, okay, diese Firma hat mit diesem Wissenschaftler dies vereinbart, damals telefoniert, und ich kann einen Blick in die Zukunft werfen?

Michael Hange: Das ist eine Frage, die über die Zuständigkeit unseres Amts hinausgeht - Profile zu bilden. Ich glaube, das ist wichtig. Diese Daten unterliegen ja nicht nur einer Zweckbindung, sondern auch einem gewissen Schutzbedarf. Es ist wichtig dass man natürlich die Daten dann auch so schützt, dass sie nicht in einen Zugriff geraten. Ich glaube, mit diesen beiden Aspekten ist es wesentlich, das anzugehen. Was sie mit Profilbildung meinen, Herr Meinel hat es angesprochen: Datensilos sind heute ein Thema. Das ist sicherlich vielfach stärker zu verorten im Rahmen von AGBs, dass man irgendeinem Anbieter die Möglichkeit gibt, für ein kostenloses Surface die Daten auch zu verwerten, dann nicht in Deutschland, sondern außerhalb, und daraus dann Profile zu erschließen für irgendwelche Geschäftsmodelle. Das ist, glaube ich, die größere Realität heute, als aus Vorratsdaten, aus Daten im Rahmen der Vorratsdatenspeicherung, dann Profile zu entwickeln.

Moderator: Jetzt Herr Sagurna. Dann würde ich mit der Frage von Frau Budde vom Deutschlandradio die Frageliste schließen, denn wir sollten den Keynote Speakern auch noch die Gelegenheit geben, ein wenig vom Lunch zu profitieren, denn sie müssen ja gleich um 14 Uhr auftreten. Bitte, Herr Sagurna, anschließend Frau Budde.

Frage: Herr Dr. Maaßen, Sie sprachen eben in Bezug auf den Bundestag von einem beachtlichen Angriff. Wenn ich Sie richtig verstanden habe, dann haben Sie den Bundestag gewarnt, offenbar vor Wochen. Dennoch sind Sie noch nicht in die Aufklärung eingebunden. Meine Frage: Warum ist das so? Da wundert man sich. Und können Sie zum jetzigen Zeitpunkt, das wäre ja dann auch ihre Zuständigkeit mit der Spionageabwehr, sagen, dass dieser Angriff von außen geführt wurde?

Hans-Georg Maaßen: Als ich sagte „ein beachtlicher Angriff“, beruhte meine Bewertung auf den Erkenntnissen, die ich auch von anderen Behörden oder aus den Medien erfahren habe. Wie gesagt, wir sind bisher nicht eingebunden. Ihre Frage zum Warum bitte ich an diejenigen zu richten, die die Entscheidung darüber zu treffen haben. Das ist nicht meine Dienststelle.

Frage: Außen- oder Innenangriff?

Hans-Georg Maaßen: Sie stellen die Frage danach, ob es ein Innentäter war?

Frage: Von außerhalb des Landes.

Hans-Georg Maaßen: Ach so. Auch diese Frage kann ich derzeit noch nicht beantworten, weil wir nicht in die Auswertung einbezogen sind.

Moderator: Damit sind wir beim Ende der Fragerunde und bei Frau Budde vom Deutschlandradio.

Frage: Herr Maaßen, meine Frage geht in eine ähnliche Richtung oder fast in die gleiche wie die des Kollegen. Was sagen Sie denn zu den Bedenken mancher Bundestagsabgeordneten, in die Aufklärung des größten Angriffs bisher aus dem Internet auf unser Parlament den Verfassungsschutz einzubinden? Das ist in unseren Augen doch eine recht absurde Situation. Wie sieht das bei Ihnen aus?

Hans-Georg Maaßen: Also ich kenne diese Bedenken so nicht, muss ich sagen. Dem Vernehmen nach soll es Bedenken geben - ich könnte sie jedenfalls nicht nachvollziehen - vor dem Hintergrund, dass ich die große Sorge habe, dass es sich um einen Cyber-Angriff eines ausländischen Nachrichtendienstes handelt, der, wie es sich mir darstellt, ein großer Angriff ist, wo auch Informationen abgeflossen sein könnten. Und ich denke, auch das Parlament sollte so viel Zutrauen zur Spionageabwehr haben, um geschützt zu werden vor ausländischen Diensten. Ich finde es nicht richtig, wenn man vielleicht größeres Vertrauen auf die Diskretion von ausländischen Nachrichtendiensten hat, die Cyber-Angriffe fahren gegen den Bundestag, als gegenüber der eigenen Spionageabwehr.

Moderator: Herzlichen Dank, meine Damen und Herren. Eine allerletzte Frage von Michael Sauerbier von der Bildzeitung.

Frage: Danke, Herr Allgaier, dass Sie noch eine Frage gestatten. Auch die geht an Herrn Maaßen. Herr Maaßen, Sie haben jetzt mehrfach bekundet, dass Sie nicht eingebunden sind in die Aufklärung dieses Angriffs auf den Deutschen Bundestag. Aber seit gestern Abend ist vermehrt in den Medien zu lesen, dahinter stecke wohl der russische Auslandsgeheimdienst. Jetzt mit der Außensicht, da können sie ja keine Geheimnisse verraten, als nicht Eingebundener: Für wie wahrscheinlich halten Sie diese seit gestern Abend immer wieder in den Medien aufflammende These?

Hans-Georg Maaßen: Wie gesagt, wir sind nicht in die Aufklärung eingebunden. Insoweit muss ich hier auch ein wenig spekulieren, weil ich hier keine eigenen Erkenntnisse habe. Aber mein Dienst hat immer wiederholt bestätigt, dass jedenfalls die Cyber-Angriffe gerade von Russland, von russischen Diensten, hochqualifiziert sind und uns große Sorge bereiten.

Moderator: Vielen Dank. Gestatten Sie uns als Gastgeber der dritten Potsdamer Sicherheitskonferenz noch, darauf hinzuweisen, dass um 17.45 Uhr – möglicherweise zu spät für einige von Ihnen – die Eröffnung eines Secure Identitiy Labs stattfindet. Prof. Meinel ist bei uns und kann uns zum Abschluss noch etwas sagen, was denn da erforscht wird, was uns in Zukunft hilft. Bitte.

Christoph Meinel: Wir haben über die digitalen Identitäten und die Passwortproblematik gesprochen. Natürlich ist Passwort nicht das technisch adäquate Mittel für den Identitätsschutz im Internet. Genau darum soll es in dem Lab gehen: neue Wege für den Schutz, für die Authentifizierung, Autorisierung im Netz bereitzustellen.

Moderator: Herzlichen Dank. Mehr darüber um 17:45 Uhr, auch über den Livestream, der zu sehen ist über www.tele-task.de. Damit ist das Ende der Pressekonferenz zur dritten Potsdamer Sicherheitskonferenz erreicht. Herzlichen Dank!

Ende der Pressekonferenz