**Jan Korte**

(A) kanntermaßen eine Ausgründung aus dem BND gewesen. Deswegen sagt die Linke: Wir brauchen hier eine Generalüberprüfung der Rolle des BSI, wir brauchen vor allem eine Offenlegung des Tätigkeitsberichts – der sollte nicht eingestuft sein –, und wir brauchen hier eine grundsätzliche Debatte darüber, was wir mit dem BSI eigentlich anfangen wollen.

(Beifall bei der LINKEN sowie bei Abgeordneten des BÜNDNISSES 90/DIE GRÜNEN)

In diesem Zusammenhang will ich – durchaus im Sinne des BSI, wie ich glaube – etwas anmerken. Das BSI ist dem Bundesinnenministerium untergeordnet, was zu Recht immer kritisiert wird, aber natürlich eine bestimmte Linie in der inneren Sicherheit hat. Insofern wäre es doch, glaube ich, im Zuge der Beratung über das IT-Sicherheitsgesetz eine hervorragende Idee, darüber nachzudenken, wie wir zunächst einmal die Unabhängigkeit des BSI herstellen können. Wir haben das gerade erst vor kurzem bei der Bundesbeauftragten für den Datenschutz gelöst, indem wir das BfDI zu einer obersten Bundesbehörde gemacht haben. Es wäre doch wirklich ein Fortschritt, das BSI dem Zugriff des Innenministeriums zu entziehen, was grundsätzlich sinnvoll ist, und es zu einer obersten Bundesbehörde zu machen, um eine wirkliche Unabhängigkeit herzustellen. Das wäre etwas, was wirklich sinnvoll wäre.

(Beifall bei der LINKEN sowie bei Abgeordneten des BÜNDNISSES 90/DIE GRÜNEN)

(B) Ich fasse zusammen: Ein IT-Sicherheitsgesetz ist eine grundsätzlich gute Idee; das ist anzuerkennen. Die Ausführung, so wie Sie sie angehen, ist leider mangelhaft. Wenn Sie allerdings jetzt im Zuge der Beratung auf die Hinweise der Opposition hören würden und könnten, dann könnte es ein fortschrittliches IT-Sicherheitsgesetz geben, und wir hätten im Bereich der Innenpolitik einmal etwas Richtiges im Falschen erreicht.

(Heiterkeit bei Abgeordneten der LINKEN)

Solange aber die Bundesregierung bei der staatlichen Ausspähung und Kompromittierung von IT-Systemen mitmacht oder sie zumindest hinnimmt, ohne etwas dagegen zu tun, so lange befindet sie sich auf der Seite der Gefährder von IT-Sicherheit. Wenn Ihnen IT-Sicherheit also so doll am Herzen liegt, wie Sie es gerade engagiert vorgetragen haben, dann fordere ich Sie auf, die Seiten zu wechseln und unsere Vorschläge aufzunehmen. Dann würden wir ein ganzes Stück weiterkommen.

Vielen Dank.

(Beifall bei der LINKEN sowie bei Abgeordneten des BÜNDNISSES 90/DIE GRÜNEN)

**Vizepräsidentin Edelgard Bulmahn:**

Vielen Dank. – Als nächster Redner spricht Gerold Reichenbach von der SPD-Fraktion.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

**Gerold Reichenbach** (SPD): (C)

Sehr geehrte Frau Präsidentin! Sehr geehrte Damen und Herren! Liebe Kolleginnen und Kollegen! Dass die Digitalisierung und die digitale Vernetzung immer weitere Lebensbereiche durchdringen, ist inzwischen ein Allgemeinplatz geworden; aber das ist keine Banalität. Während der heutigen Debatte werden wir erleben, dass es dunkel wird. Das hat eine natürliche Ursache, nämlich die Sonnenfinsternis, die im Laufe des Vormittags eintritt. Es könnte aber auch andere Gründe haben. Im Rahmen einer Veranstaltung zum Thema „Vernetzung und IT-Sicherheit“ erzählte neulich ein Professor, dass man sich unter Kollegen darüber unterhielt, wie man von Wien aus die Jalousien beim Deutschen Bundestag herauf- und herunterfährt. Das hört sich zunächst sehr lustig an, Herr Korte,

(Jan Korte [DIE LINKE]: Ich habe nicht gelacht!)

aber das ist eine neue Qualität, mit der wir es zu tun haben: dass unsere Systeme nämlich vom Ausland aus angreifbar sind, weil immer mehr unserer Lebenssysteme von Rechneranlagen digital gesteuert werden und international vernetzt sind. Das erklärt dann vielleicht auch für Sie, warum wir auch die präventive Seite gegenüber solchen Angriffen stärken müssen. Damit haben Sie die Erklärung, warum wir auch die Dienste in diesem Bereich und hinsichtlich dieser Fähigkeiten stärken müssen.

(Beifall bei Abgeordneten der SPD und der CDU/CSU)

(D)

Unsere Kraftwerksbetreiber bereiten sich seit Monaten darauf vor, einen Blackout zu verhindern, der aufgrund der Stromschwankungen, induziert durch die Sonnenfinsternis, bei den Solaranlagen auftreten könnte. Aber was wäre, wenn solche Schwankungen nicht durch ein vorhersehbares Ereignis, sondern durch eine Cyberattacke ausgelöst würden? Ein Blackout wäre vermutlich nicht mehr zu vermeiden, und es drohten für die Bürger der Bundesrepublik Deutschland drastische Folgen, wie wir sie gemeinsam im Grünbuch über die „Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland“ beschrieben haben und wie es auch in der TAB-Studie im Auftrag des Deutschen Bundestages dargelegt wurde.

Wir sind zunehmend von Datenverarbeitung und funktionierenden, sicheren Infrastrukturen und Kommunikationsinfrastrukturen abhängig. Ob Lebensmittelversorgung, Wasser-, Strom- und Energieversorgung, Logistik und Entsorgung, Gesundheitswesen oder öffentliche Sicherheit, aber auch Behörden und Verwaltung: Alle sind sie heute von funktionierenden IT-Strukturen und Kommunikationssystemen abhängig. Und diese sind in Bezug auf kriminelle oder staatliche Angriffe von außen in hohem Maße gefährdet.

Gleiches gilt übrigens für die Unternehmen und selbst für private Haushalte. Wir bewegen uns auch privat immer mehr in einer digital vernetzten Welt. Zukünftig werden immer mehr Funktionen davon abhängig sein: unser Auto, unsere Heizung, unsere Geld- und Warenge-

**Gerold Reichenbach**

(A) schäfte, nicht zuletzt unsere Brandsicherheit, wenn Toaster und Herd über IT-Kommunikation gesteuert werden.

Darum müssen wir uns verstärkt der IT-Sicherheit widmen, und dazu gehören mehr Kapazitäten zur Bekämpfung von Cyberkriminalität, ein besserer Schutz kritischer Infrastrukturen, einschließlich – das sage ich ausdrücklich – staatlicher Einrichtungen,

(Jan Korte [DIE LINKE]: Genau!)

und mehr Investitionen in IT-Sicherheit sowohl im privaten als auch im öffentlichen Bereich.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Liebe Kolleginnen und Kollegen, nicht zuletzt deshalb hat die Koalition vereinbart – ich zitiere mit Erlaubnis der Präsidentin –, „ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle“ zu schaffen. Wir haben geliefert. Ein entsprechender Gesetzentwurf liegt nun vor.

Wir wollen mit dem Gesetz für mehr Schutz der Bürgerinnen und Bürger im Netz sorgen. Deswegen werden wir die Ermittlungszuständigkeiten und Ermittlungsfähigkeiten des Bundeskriminalamtes im Bereich Cybercrime stärken und ausbauen; denn Gelegenheit macht Diebe.

(Beifall bei der SPD und der CDU/CSU)

(B) Deswegen werden wir das BSI stärken und ausbauen und ihm die Möglichkeit bieten, Marktprodukte zu analysieren und auf ihre Sicherheit zu überprüfen. Diese verstärkten Befugnisse binden wir ausdrücklich und klar an den Zweck, den Bürgerinnen und Bürgern sowie Unternehmen und Behörden Hilfestellungen sowie Hinweise für ihre IT-Sicherheit zu geben. Wir tun das nicht, wie Sie gerade unterstellt haben, um Lücken auszuforschen und diese zu nutzen.

Wir wollen mit dem Gesetz den Schutz der Informationstechnik des Bundes weiter vorantreiben und für das Funktionieren einer zunehmend digitalisierten öffentlichen Verwaltung Sicherheitsstandards setzen.

Damit einhergehend – last, but not least – wollen wir die IT-Sicherheit bei Unternehmen und vor allem bei kritischen Infrastrukturen stärken. Kritische Infrastrukturen sind im Wandel. Im 19. Jahrhundert waren Postkutschenstationen kritische Infrastrukturen. Heute sind es Flughäfen, die man damals nicht kannte und vermutlich nicht einmal erahnte. Während sich dieser Wandel in der Vergangenheit in längeren Zeiträumen vollzog, sind es heute nur noch wenige Jahre. Gleichzeitig schreitet die Vernetzung rasant voran.

Bleiben wir beim Beispiel der Verkehrs- und Logistikbranche. Der Flughafen Frankfurt ist mit einem Cargoaufkommen von 2,2 Millionen Tonnen der führende Cargoflughafen in Europa. In Frankfurt werden fast 50 Prozent des gesamten Luftfrachtvolumens abgewickelt. Frankfurt verfügt aber auch über hochspezialisierte Einrichtungen für das Handling von Pharma. Zahlreiche Spediteure verfügen am und um den Flughafen über eigene Pharmabereiche. Ein Ausfall dieser kritischen Infrastruktur hätte kaum absehbare Folgen, nicht nur für den Güter- und Personenverkehr, sondern auch für die Arzneimittelversorgung der Bevölkerung in der Bundesrepublik Deutschland. (C)

Die Logistikketten sind nämlich über ITK-Systeme und intelligente Steuerung längst eng miteinander verknüpft. Auch wenn die Spediteure, die die Produkte zu den Flug- und Seehäfen bringen, nach wie vor überwiegend kleine und mittlere Unternehmen sind und damit selbst wohl keine kritische Infrastruktur sind: Die dahinter stehenden vernetzten ITK-Systeme sind es sehr wohl. Wenn die IT-Steuerung der Seehäfen durch eine Cyberattacke lahmgelegt würde, dann litte Deutschland ganz schnell im wahrsten Sinne des Wortes unter Speiseröhrenverengung und Darmverschluss. Darum ist der Gesetzentwurf gerade in Bezug auf die kritischen Infrastrukturen bewusst so gestaltet, dass er mit der rasanten technischen Entwicklung Schritt halten kann.

Im Gesetzesvorschlag werden die kritischen Infrastrukturen in ihrer Sektorenzugehörigkeit und Funktionalität für die öffentliche Sicherheit und die Versorgung sowie die Funktionsfähigkeit des Gemeinwesens definiert. Herr Korte, ich kenne kein Gesetz – von der Seveso-Richtlinie bis zu anderen Gesetzen –, bei dem der Gesetzgeber vorher bis zum kleinsten Unternehmen gewusst hätte, wer letztendlich davon betroffen sein würde.

(Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]: Aber so ein bisschen würde es helfen! – Jan Korte [DIE LINKE]: Eine Ahnung könnte man ja haben!) (D)

– Die haben wir ja. Ich habe es gerade eben beschrieben.

Die Definition dessen, was nach dem gegenwärtigen Entwicklungsstand – das ist die entscheidende Frage; wir als Gesetzgeber haben uns nicht nur nach dem gegenwärtigen Entwicklungsstand zu richten – im Einzelnen unter kritischer Infrastruktur zu verstehen ist, wollen wir bewusst dem Instrument der Rechtsverordnung überlassen, um die nötige Flexibilität zu haben, auf die schnellen technologischen Entwicklungen reagieren zu können. Dazu werden wir einen Identifikationsprozess aufsetzen, in den wir die Betreiber und Branchen mit einbeziehen werden.

Ein wesentliches Element des Gesetzes sind die Meldepflichten. Meldungen können anonym erfolgen, wenn es um ein Lagebild über die Cybersicherheitslage geht. Bei bestimmten Vorfällen machen anonyme Meldungen allerdings keinen Sinn mehr. Man stelle sich vor, beim Kraftfahrzeugbundesamt ginge die anonyme Meldung ein, dass es Fahrzeuge mit nicht funktionierenden Bremsen gebe, aber es würde nicht gesagt, welche Fahrzeuge und welche Hersteller es sind. Genauso wie im Automobilverkehr und bei der Sicherheit im Straßenverkehr können von der Funktionsfähigkeit kritischer Infrastrukturen Menschenleben abhängen. Diese sind höherrangig zu bewerten als die Interessen der Wirtschaft. Darum dürfen Meldungen nicht mehr anonym erfolgen, wenn es

**Gerold Reichenbach**

(A) zu Ausfällen oder Beeinträchtigungen der Funktionsfähigkeit kritischer Infrastruktur kommt.

(Beifall bei der SPD und der CDU/CSU)

Ich finde, wir sollten den jetzt aufgesetzten Mechanismus auch auf seine Wirksamkeit hin überprüfen und für das Gesetz eine Evaluierung nach einem angemessenen Zeitraum vorsehen.

IT-Sicherheit und Schutz von kritischen Infrastrukturen ist nicht nur eine Frage der Sicherheit der Bürger heute, sie wird immer mehr zur entscheidenden Frage für die Wachstumsmöglichkeiten und die Chancen der Digitalisierung selbst. Denn die Menschen würden es nicht akzeptieren, in immer mehr wichtigen Lebensbereichen von unsicheren IT-Infrastrukturen abhängig zu sein. Als Staat und Gesellschaft können wir es nicht einfach hinnehmen, für Angriffe und Bedrohungen von außen immer anfälliger zu werden. Vertrauen und Sicherheit werden die entscheidenden Faktoren für die weitere digitale Entwicklung unserer Wirtschaft und Gesellschaft sein. Natürlich ist zuvörderst die Wirtschaft in der Pflicht, in die Sicherheit von IT-Strukturen zu investieren. Dort aber, wo die Schadenswirkung über das eigene Unternehmen oder die eigene Branche hinausgeht, wo Sicherheitslücken auch Dritte in erheblichem Umfang schädigen oder gefährden können, ist der Gesetzgeber in der Pflicht, die notwendigen Sicherheitsrahmenbedingungen vorzugeben.

(Beifall bei Abgeordneten der SPD und der
(B) CDU/CSU)

So haben wir es übrigens – der Minister hat es erwähnt – in der alten industriellen Welt völlig selbstverständlich immer wieder getan und tun es auch heute noch. Dies gilt es auch für die digitale und vernetzte Welt zu gestalten.

IT-Sicherheit und Vertrauen in kritische Infrastrukturen werden zu immer wesentlicheren Standortfaktoren. Ich habe viele Gespräche mit Betreibern kritischer Infrastrukturen geführt, mit Vertretern der Wirtschaft und auch mit Vertretern von ausländischen Unternehmen, die dies bestätigten. Gerade auch Vertreter aus dem Ausland sahen – aus ihrer Sicht manchmal etwas neidisch – die Chance, dass dieses weltweit eines der ersten IT-Sicherheitsgesetze zu einem echten Standortvorteil für die Bundesrepublik Deutschland werden kann.

Liebe Kolleginnen und Kollegen, mit diesem Gesetz wird die Koalition nicht nur für mehr Sicherheit unserer Bürgerinnen und Bürger sorgen. Mit diesem Gesetz wird der Standort Deutschland fit für die digitale Zukunft.

Ich danke Ihnen für Ihre Aufmerksamkeit.

(Beifall bei der SPD und der CDU/CSU)

**Vizepräsidentin Edelgard Bulmahn:**

Vielen Dank. – Als nächster Redner hat Konstantin von Notz das Wort.

**Dr. Konstantin von Notz** (BÜNDNIS 90/DIE (C) GRÜNEN):

Frau Präsidentin! Liebe Kolleginnen und Kollegen! Meine sehr verehrten Damen und Herren! Das zentrale Thema der CeBIT in diesem Jahr ist die massive Gefährdung unserer digitalen Infrastruktur durch Massenausspähung und IT-Angriffe. Ohne Edward Snowden hätten wir heute nicht ansatzweise den Überblick über die tatsächliche Bedrohungslage.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
und bei der LINKEN – Widerspruch bei Abgeordneten der CDU/CSU)

IT-Sicherheit war immer wichtig. Aber spätestens seit Stuxnet, Regin, dem Heartbleed Bug und dem überwachten Handy der Kanzlerin ist völlig klar: Im Bereich der IT-Sicherheit brennt in Deutschland die Hütte lichterloh. Ein zentrales Risikoszenario für Betriebs- und Geschäftsgeheimnisse, für Kommunikation und Privatheit ist nicht nur die organisierte Kriminalität, es sind auch die sich verselbstständigenden Geheimdienste und ihnen gefällig zuarbeitende Unternehmen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
sowie bei Abgeordneten der LINKEN)

Das ist die Ausgangslage auch nach zehn Jahren Bundesinnenministerium unter CDU/CSU-Führung, meine Damen und Herren.

Jeder weiß: Wir brauchen einen verbesserten Grundrechtsschutz der Menschen und eine Erhöhung der IT-Sicherheit für Unternehmen und Behörden. Das sind zwei Themen, die man heute nicht mehr trennen kann. Und (D) sosehr Ihr Ministerium, Herr de Maizière, in den letzten Jahren für die grundrechtsfeindliche Vorratsdatenspeicherung gekämpft hat, so wenig Substanzielles haben Sie im letzten Jahrzehnt für den Bereich der IT-Sicherheit vorzuweisen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
sowie bei Abgeordneten der LINKEN)

Zur CeBIT 2015 legen Sie jetzt Ihren übereilten, unreifen Entwurf eines IT-Sicherheitsgesetzes vor, der völlig zu Recht von allen Seiten kritisiert wird. Weder bringt er mehr IT-Sicherheit für Deutschland, noch schafft er das notwendige Vertrauen in die Nutzung der Kommunikationsinfrastruktur unserer Zeit, das Internet. Wer IT-Strukturen schützen will, braucht zunächst eine differenzierte Einschätzung der Gefährdungslage; Kollege Korte hat es angesprochen. Diese haben Sie bis heute nicht vorgenommen.

(Gerold Reichenbach [SPD]: Das stimmt doch
gar nicht!)

Es ist deshalb vielleicht konsequent, aber eben inhaltlich falsch, hier lediglich mit weitgehend unbestimmten Verfahrensregelungen um die Ecke zu kommen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
sowie bei Abgeordneten der LINKEN)

Sie denken IT-Sicherheit eben nicht ganzheitlich, sondern stellen hier nur auf den Bereich kritischer Infrastrukturen ab. Selbst bei diesen Regelungen springen Sie