Landtag
Nordrhein-Westfalen
16. Wahlperiode

Ausschussprotokoll
APr 16/1319
01.06.2016

Ausschuss für Arbeit, Gesundheit und Soziales

106. Sitzung (öffentlich)

1. Juni 2016

Düsseldorf – Haus des Landtags

13:30 Uhr bis 15:25 Uhr

Vorsitz: Günter Garbrecht (SPD)

Protokoll: Ricarda Lampret

Verhandlungspunkt:

Die IT-Infrastruktur der Krankenhäuser in Nordrhein-Westfalen muss sicher sein – die Gesundheit der Patientinnen und Patienten darf nicht zum Spielball von Kriminellen im Netz werden! **3**

Antrag
der Fraktion der PIRATEN
Drucksache 16/11216

– öffentliche Anhörung
(Teilnehmende Sachverständige und Stellungnahmen siehe Anlage.)

* * *

Vorsitzender Günter Garbrecht: Willkommen zur 106. Sitzung des Ausschusses für Arbeit, Gesundheit und Soziales, heute zu einer Anhörung! Ich begrüße insbesondere die Sachverständigen, die unserer Einladung gefolgt sind, sowie die Zuhörerinnen und Zuhörer! Herzlich willkommen auch Herr Hermann-Josef Arentz! Er ist ein ehemaliger Kollege und hat in der letzten Reihe Platz genommen.

Ich rufe auf:

Die IT-Infrastruktur der Krankenhäuser in Nordrhein-Westfalen muss sicher sein – die Gesundheit der Patientinnen und Patienten darf nicht zum Spielball von Kriminellen im Netz werden!

Antrag
der Fraktion der PIRATEN
Drucksache 16/11216

Der Antrag ist in der 106. Plenarsitzung am 2. März beraten und an unseren Ausschuss überwiesen worden. Wir haben ihn bereits im Ausschuss behandelt und diese Anhörung aufgrund des Anliegens der antragstellenden Fraktion anberaumt.

Im Namen des Ausschusses bedanke ich mich für die übersandten Stellungnahmen. Abgeordnete arbeiten insbesondere mit Papier. Daher sind wir auch in der Lage, kurzfristig eingegangene Stellungnahmen umfangreicher Provenienz zu verarbeiten. Wir sind im Thema. Das werden wir unter Beweis stellen, indem sich die Damen und Herren Abgeordnete direkt mit Fragen an Sie wenden werden. Damit ist überprüfbar, ob sie die übersandten Stellungnahmen im entsprechenden Maße aufgenommen haben.

Nach dieser Vorrede gucke ich in die Runde. Traditionsgemäß macht die Fraktion, die den Antrag gestellt hat, den Aufschlag. Ich erteile dem Kollegen Sommer von der Fraktion der Piraten als erstem Redner das Wort.

Torsten Sommer (PIRATEN): Vielen Dank Herr Vorsitzender! – Vielen Dank für die eingereichten Stellungnahmen und dass Sie hier erschienen sind, um ein paar Fragen zu beantworten. Das Thema ist durchaus wichtig.

Meine erste Frage richtet sich an Herrn Dr. Walther und an Herrn Spyra: Vor welcher Herausforderung stehen die Krankenhäuser in Nordrhein-Westfalen vor dem Hintergrund der Digitalisierung in den letzten zehn, 15 Jahren?

An Herrn Dr. Walther habe die folgende Frage: In der IT-Verantwortung und IT-Sicherheit gibt es noch andere Aspekte außer dem monetären, die den Verantwortlichen das Leben leichter machen können. Vielleicht können Sie ausführen, was den IT-Verantwortlichen in den Krankenhäusern das Leben leichter machen kann, abgesehen von finanziellen Maßnahmen? Welchen Rahmenbedingungen könnten verbessert werden?

Herr Spyra, welche Pflichten haben die Hersteller und Betreiber von Medizinprodukten im Hinblick auf die Informationssicherheit? Wieso kann es an dieser Stelle zu Konflikten kommen? An welcher Stelle ist hier die Landesregierung aufgefordert, tätig zu werden? Wer ist Ihrer Meinung nach für die Aufsicht über die IT-Sicherheit in den Krankenhäusern zuständig?

Dann kommen wir mit meiner Frage an die Krankenhausgesellschaft zum monetären Bereich: Wenn Krankenhäuser einen entsprechenden IT-Bedarf von zum Beispiel 2,5 % des Gesamtbudgets haben, wie hoch wäre dann der aktuelle Gesamtinvestitionsbedarf für alle Krankenhäuser in NRW? Würden 500 Millionen € dafür überhaupt ausreichen?

Ich gehe davon aus, dass es zwei Fragerunden gibt, Herr Vorsitzender.

Vorsitzender Günter Garbrecht: Das ist eine weise Voraussicht.

Torsten Sommer (PIRATEN): Danke.

Vorsitzender Günter Garbrecht: Herr Kollege Ünal.

Arif Ünal (GRÜNE): Vielen Dank! – Herr Vorsitzender! Liebe Kolleginnen und Kollegen! Ich danke auch für Ihre Stellungnahmen.

Ich habe drei Fragen. Die erste richtet sich an die Krankenhausgesellschaft. Wie ist die IT-Sicherheit in den Krankenhäusern? Können Sie zum Beispiel der Aussage, die IT-Infrastruktur in den Krankenhäusern sei marode und veraltet, zustimmen? Wenn nicht, können Sie beschreiben, wie sich die Situation darstellt?

Die zweite Frage richtet sich an Dr. Häger vom Bundesamt für Sicherheit in der Informationstechnik. Die Maßnahmen zur IT-Sicherheit in den Krankenhäusern haben Sie in technische, infrastrukturelle und personelle unterteilt. Können Sie darauf eingehen, welche technischen und infrastrukturellen Maßnahmen notwendig sind, um die IT-Sicherheit in den Krankenhäusern sicherzustellen? Sind die Administratoren darauf vorbereitet? Gibt es eine einheitliche Schulung oder Zertifizierung? Oder gibt es unterschiedliche Ausbildungsgänge?

Meine dritte Frage richtet sich an Herrn Appel; leider hatte ich keine Gelegenheit, Ihre Stellungnahme ausführlich zu lesen. Aber welche technischen Möglichkeiten sind nach jetzigem Wissensstand notwendig, um die IT-Sicherheit sicherzustellen? – Danke.

Vorsitzender Günter Garbrecht: Herzlichen Dank, Herr Kollege Ünal. – Herr Kollege Yüksel.

Serdar Yüksel (SPD): Herr Vorsitzender! Namens der SPD-Fraktion bedanke ich mich bei allen Sachverständigen für die eingereichten Unterlagen.

Ich habe drei Fragen. Die erste richtet sich an die Krankenhausgesellschaft Nordrhein-Westfalen. In Ihrer Stellungnahme 16/3962 führen Sie aus, dass es keinen 100%igen Schutz gibt. Pentagon, Bundestag und große Banken würden auch entsprechend angegriffen. Diese Auffassung teile ich ausdrücklich. Sie sagen, in 99 % der Fälle komme es nicht zu Schäden. Allerdings informierten Sie die Krankenhäuser nicht regelmäßig über erfolgte Cyberangriffe. Halten Sie eine solche Meldung an Sie für sinnvoll? Sollte man nicht initiieren, dass die Krankenhäuser solche Angriffe der Krankenhausgesellschaft automatisch melden? Das ist meine Frage an die Krankenhausgesellschaft.

Meine zweite Frage richtet sich an Herrn Dr. Stefan Walther. Sie schreiben in Ihrer Stellungnahme 26/3959, innerhalb der Krankenhäuser sei die IT-Sicherheit oft politisch schwach aufgestellt. Das heißt, im Verteilungskampf um Investitionen gewinnt meist die Medizin, da diese als Primärgeschäft betrachtet wird. Es scheint eine Prioritätensetzung in den Krankenhäusern zu geben, dass der Chefarzt eher seine apparative Neuausstattung durchsetzt und die Verantwortung für die IT-Sicherheit delegiert und beim Land sieht. Vielleicht können Sie näher ausführen, wie Sie zu dieser Erkenntnis kommen.

Meine dritte Frage richtet sich an Herrn Spyra. Herr Spyra, Sie schreiben in Ihrer Stellungnahme 19/3961, Informationssicherheit bestehe in Krankenhäusern oftmals aus Insellösungen, denen kein ganzheitliches Konzept zugrunde liege. Wie könnte so ein ganzheitliches Konzept aussehen? Wo sehen Sie die Defizite?

Vorsitzender Günter Garbrecht: Danke schön, Herr Kollege Yüksel. – Herr Kollege Preuß.

Peter Preuß (CDU): Herr Vorsitzender! Meine Damen und Herren! Auch von unserer Seite zunächst einmal herzlichen Dank für Ihre Stellungnahmen! Ich denke, grundsätzlich besteht Einigkeit darüber, dass die Digitalisierung unaufhaltsam fortschreitet. Damit einher geht die Frage nach der IT-Sicherheit. Wir müssen uns darüber im Klaren sein, dass Menschen, die Computer bedienen, auch Fehler machen können. Was die IT-Sicherheit angeht, müssen sie auch eine gewisse Einstellung zu haben.

Deshalb würde ich an Herrn Appel gern die Frage richten, welche Bedeutung die IT-Sicherheit für die Krankenhäuser hat. Was muss getan werden, um die Mitarbeiter entsprechend darauf einzustellen? Was muss das Management tun, um hierfür die richtige Einstellung zu entwickeln?

Die zweite Frage, die ich in diesem Zusammenhang habe, ist: Was erwarten Sie von der Politik, damit sich die Krankenhäuser auf die mehrfach angesprochenen Herausforderungen im Zusammenhang mit der IT-Sicherheit einstellen können?

Vorsitzender Günter Garbrecht: Herzlichen Dank, Herr Kollege Preuß. – Herr Kollege Alda.

Ulrich Alda (FDP): Danke, Herr Vorsitzender! – Auch von der FDP-Fraktion danke für Ihre Stellungnahmen!

Ich habe drei Fragen, und zwar an die Herren Spyra, Dr. Walther und Herr Blum. Sie alle drei haben die Notwendigkeit ausreichender Investitionen in die IT-Infrastruktur betont. Daher habe ich meine folgenden drei Fragen.

Erstens: Wie wirkt sich die derzeitige Krankenhausfinanzierung auf die IT-Sicherheit aus?

Zweitens: Wie bewerten Sie in diesem Zusammenhang die Investitionsförderung des Landes, auch im Vergleich zu anderen Bundesländern?

Drittens: Wie sollte aus Ihrer Sicht eine zweckgebundene Förderung der IT-Sicherheit eingeführt werden? – Danke.

Vorsitzender Günter Garbrecht: Danke schön, Herr Kollege Alda. – Wir gehen bei der Beantwortung der Fragen nach der Reihenfolge der Ansprache vor. Wir beginnen mit Herrn Dr. Walther, bitte schön.

Dr. Stefan Walther (Chief Information Officer): Danke schön. – Sehr geehrte Frau Landtagspräsidentin! Sehr geehrter Herr Garbrecht! Sehr geehrte Damen und Herren Abgeordnete! Vielen Dank für die Einladung! Das Thema ist wichtig, und ich begrüße sehr, dass es hier zur Sprache kommt.

In der IT hat sich innerhalb der letzten fünf Jahre extrem viel verändert. Wir leben de facto in einer Revolution. Lange Zeit war IT ein Mangelsystem: ITler haben versucht, die Computer an die Nutzer zu bringen und die Nutzer zu den Computern zu bringen. Lange Zeit hatte man eine Mangelverwaltung. Man hat versucht, Kompromisse zu schließen und den Nutzern das Ganze einigermaßen schmackhaft zu machen. Seit etwa fünf Jahre sind alle Wünsche, die wir hatten, wahr geworden. Das ist eigentlich eine sehr schöne Situation. Die Systeme können genau das, was die Nutzer haben wollen; wir können sie so konfigurieren, wie wir sie haben wollen. Die Durchdringungstiefe ist gegeben. Ich muss es nicht mehr an die Nutzer herantragen. Die Nutzer fordern das, was sie haben wollen. Eigentlich ist es eine traumhaft schöne Welt. Es gibt nur einen kleinen Nachteil für die IT: Die Systeme sind dermaßen komplex geworden, dass wir anfangen, sie nicht mehr zu beherrschen. Jetzt dreht sich der Spieß um. Die IT trägt nicht mehr heran, sondern ist der Getriebene. Die Außenwelt fordert immer mehr an immer mehr Stellen. Plötzlich schlagen an irgendwelchen Ecken IT-Bereiche auf, die man vorher noch nicht geahnt hat. Man wird mehr oder minder gejagt. Jetzt ist noch nicht ganz klar, wie wir damit umgehen.

Die Sparmaßnahmen, die in den Krankenhäusern zwangsläufig getroffen werden, betreffen auch die IT. Die IT muss sich an dieser Stelle politisch durchsetzen und versuchen, das hinzukriegen. Das ist aber unverhältnismäßig. Selbst eine gut aufgestellte IT hat noch zu wenige Ressourcen mit Blick auf die Komplexität, die in letzter Zeit zugenommen hat.

Wenn wir uns nicht genug darum kümmern, werden die Systeme instabil. Die Sicherheit läuft der gejagten IT sozusagen ein Stück weit hinterher. Sicherheit gehört mittlerweile ein Stück weit zum Routinegeschäft, zum Beispiel Datensicherheit und Ähnliches. Da reduziert man eher mal die Qualität, um das Tagesgeschäft zu überstehen.

Damit ist die Flanke offen. Probleme bei der IT-Sicherheit führen inzwischen, anders als Probleme in vielen anderen Bereiche, dazu, dass ein ganzes Krankenhaus auf einmal lahmgelegt werden kann. Wenn dort wirklich etwas aufschlägt, ist ein Krankenhaus unter Umständen bewegungsunfähig. Das zu den Herausforderungen, vor denen wir jetzt gerade stehen.

Hinzu kommen natürlich neue Gesetze und Ähnliches. Das gibt es schon lange. Die Gesetze laufen im Mittel in die richtige Richtung. Die strategische Ausrichtung der Gesetze zum Gesundheitswesen aus den letzten 15 Jahren – plus/minus – hat, unabhängig von der Regierung zu der jeweiligen Zeit, einen roten Faden. Das besteht eine saubere strategische Linie. Das ist gut aufgebaut. Man begrüßt es, aber schafft es zum Teil nicht mehr. Diese Schwierigkeit besteht dabei einfach.

Es gibt ein paar nicht monetäre Punkte, die das Leben auch schwer machen. Die VOL – ich weiß, das ist ein kritischer Punkt – hat sich jetzt gerade etwas geändert. In der bisherigen Form war sie an vielen Stellen nicht für die heutige IT gemacht. Die neuen Grundlagen des Landes zur sind sinnvoll. In der Praxis sind aber Angebote nicht mehr gültig, wenn die Mittel genehmigt sind. Das heißt, es bedarf zweier oder dreier Runden, weil die Angebote allein aufgrund der Schwankungen des Dollarkurses nicht mehr gültig sind. Hier könnte man das eine oder andere vereinfachen. Es könnte zum Beispiel erlaubt werden, Vorentscheidungen zu treffen.

Ein weiterer Punkt – es tut mir leid, dass ich das anspreche; ich weiß, dass es auch ein heißes Thema ist – ist die Mitbestimmung. Das Tempo einer klassischen Mitbestimmung passt an vielen Stellen nicht mehr zur Bewegung der Außenwelt. Neue Sicherheitssysteme müssen unter Umständen sehr schnell eingebaut werden. Es bestehen in diesem Fall nur zwei Möglichkeiten: Entweder ich übergehe die Mitbestimmung und werde mit den Konsequenzen fertig, oder ich lasse das System unsicher. Das ist wirklich noch einmal anzugehen, damit man an diesen Stellen etwas mehr Bewegungs- und Entscheidungsmöglichkeiten hat. Das heißt nicht, dass ich kein Freund von Mitbestimmung bin. Darum geht es nicht. Aber die Außenwelt und das, was in den Sitzungen geschieht, divergieren stark. Die Einigungsstelle tagt nur zwei Mal im Jahr – hier wird richterlich über die Fälle von allen Unikliniken bestimmt –; das ist zu wenig. Die Frequenz muss deutlich höher werden.

Die dritte Frage, die mir gestellt wurde, war, ob die IT unter Umständen schwach aufgestellt sei. Die Situation betreffend die Finanztöpfe ist in allen Kliniken angespannt. Das liegt daran, dass neue Geräte schick und teuer sind, der Bedarf hoch ist, und Kosten für neue Chefärzte und Neuberufungen von Professoren – das sind meist kostspielige Verhandlungen, weil es sich hier um einen direkten Wettbewerb handelt – hinzukommen. Man sollte die Aufgabe der Leitung einer Klinik nicht unterschätzen. Das ist eine hohe Managementaufgabe. Das Spektrum – die monetären Bereiche, die Bereiche Personalführung, Wissenschaft und das operative Geschäft, ein guter Chirurg oder Internist sein, Forschung und Lehre zu bedienen – ist breit. Es gibt nicht viele, die dieses breite Spektrum einigermaßen abdecken können. Diese Leute muss man hegen und pflegen.

Die IT ist zunächst ein Kostenfaktor. Wenn ich mitteile, dass die Speicherkapazität nicht mehr genügt und mehr benötigt wird, wird gefragt, wie viel das kostet. Dann muss

ich sagen: „Aufwendungen unter 300.000 € machen keinen Sinn.“ Dann wird geseufzt. Im besten Fall ist bei einer Bewilligung der Mittel in Höhe von 300.000 € erreicht, dass ich erstens meinen Ruf ruiniert habe und zweitens der Status vorher noch dem Status nachher entspricht; man kann dann nämlich Daten speichern. Ab einer gewissen Speichermenge teile ich mit: „Ich brauche noch zusätzliche Ressourcen; denn die Datensicherung wird schwierig.“ Komplexität kann nicht linear skaliert werden. Das heißt, eine Speicherkapazität von 10 GB ist etwas anderes als ein Speicher von 10 TB oder 10 PB. Das kann nicht linear skaliert werden. Das jemandem beizubringen, ist ein undankbares Geschäft. Ich bin im entsprechenden Fall automatisch in einer passiven Situation, die dann oft recht wenig Spaß macht. – So weit von mir.

Vorsitzender Günter Garbrecht: Ich leite über. Herrn Spyra habe ich vorhin leider übergangen. Bitte antworten Sie nun auf die Fragen, die an Sie gerichtet worden sind.

Gerald Spyra (Kanzlei Spyra): Sehr gerne. – Zur ersten Frage, zur Evolution der IT und ihren Herausforderungen: Ich denke, man sollte sich vor Augen führen, was für eine wahnsinnige Evolution die Krankenhäuser diesbezüglich eigentlich mitgemacht haben. Früher war alles – daher kommt auch der Begriff „Medizintechnik“ – technisch, mechanisch. IT wurde nur eingesetzt, um Prozesse für ein Gerät abzubilden. Heutzutage soll aber alles miteinander vernetzt sein. Die Daten sollen alle untereinander ausgetauscht werden können. Das bedingt wiederum, dass die Komplexität allein in der Netzwerkinfrastruktur extrem ist. Das führt dazu, dass die Daten irgendwo entlang fließen. Wir können diese Daten aber kaum mehr greifen. Das heißt, es besteht eine Intransparenz bei der Datenverarbeitung. Das macht es kompliziert, das Kritische zu benennen. Wie können wir auf kritische Ereignisse reagieren?

Es gibt im Krankenhaus unterschiedliche Bereiche. Im administrativen Bereich werden Windows-Office-Produkte eingesetzt. Die meisten der Angriffe heute – so war es wahrscheinlich auch beim Angriff im Krankenhaus in Neuss –, kommen über diese Office-Produkte. Das heißt im Endeffekt, jemand erhält eine E-Mail, öffnet diese und der Rechner wird mit einem Virus infiziert. Aufgrund der ganzen Vernetzung ist dadurch letztlich das ganze Krankenhaus infiziert. Die Auswirkungen haben wir mitbekommen.

Schauen wir uns an, welche Geräte es alles in Krankenhäusern gibt. Ärzte, Chefärzte bringen sogar noch ihr eigenes Smartphone mit. Das private Smartphone wird für dienstliche Zwecke eingesetzt, um Patienten zu behandeln. All das muss im Netzwerke eingebunden sein, denn es wird dokumentiert usw. Niemand weiß im Endeffekt mehr damit Klarzukommen. Wie soll das alles noch dokumentiert werden? Wie soll das abgesichert werden? Das heißt, es besteht Intransparenz und keine Transparenz mehr.

Damit bin ich beim ganzheitlichen Ansatz. Ein ganzheitlicher Ansatz kann nur funktionieren, wenn die Prozesse transparent sind. Wenn wir diese nicht identifizieren, wenn wir gar nicht wissen, wie die Daten verlaufen, können wir auch keine Absicherungsmaßnahmen treffen. Ein ganzheitlicher Ansatz bedeutet für mich auch, dass alle Bereiche adressiert werden.

Informationssicherheit ist für mich der Oberbegriff dafür. Darunter fällt auch der Datenschutz, die Medizinproduktesicherheit in einem Krankenhaus usw. Das ist sehr komplex und betrifft viele Bereiche.

Über eine E-Mail wird das System infiziert. Das betrifft das sogenannte Social Engineering: Ein Mitarbeiter wird dazu gebracht, eine E-Mail zu öffnen. Das Problem ist sehr groß. Es geht hier um psychologische Aspekte; den menschlichen Aspekt dürfen wir nie außenvorlassen.

Dann gibt es noch die Prozesse. Wir müssen wissen, wer wofür verantwortlich ist. Nicht jeder Mitarbeiter darf auf alle Daten zugreifen. Das besagt bereits das Patientengeheimnis, die ärztliche Verschwiegenheitspflicht. Hier kommt möglicherweise der menschliche Aspekt hinzu; es geht immer auch um die Patienten.

Damit bin ich bei den Medizinprodukten. Dieser Punkt wird heutzutage noch viel zu wenig adressiert. In meiner Stellungnahme 16/3961 habe ich von einer rechtlichen Unsicherheit gesprochen. Ich würde das gern an einem Beispiel zeigen, damit Sie sehen, wie desolat die Lage ist: Medizinprodukte zeichnet aus, dass von diesen Produkten die Gesundheit und das Leben von Patienten abhängen. Das bedeutet, dass Hersteller von Medizinprodukten die volle Verantwortung für die ordnungsgemäße Funktionsfähigkeit ihrer Produkte übernehmen. Man muss sich den Hintergrund anschauen; das geht aus der Medizintechnik hervor. Es gab damals noch keine großartige Software. Es kam wirklich nur auf die Safety, auf die ordnungsgemäße Funktionsfähigkeit von Produkten an. Jetzt aber gibt es den Unsicherheitsfaktor Software und Vernetzung. Jeder von uns kennt Windowsprodukte und weiß, wie löchrig diese sind, wie oft wir Patches einspielen müssen. Bei Medizinprodukten ist das aber nicht so einfach möglich. Warum? Mit dem Einspielen eines Patches übernimmt der Hersteller nicht mehr die Gewährleistung, dass sein Produkt sicher ist und ordnungsgemäß funktionieren kann.

Vor ein paar Wochen kam heraus, dass ein Virenscanner eine Herzoperation lahmgelegt hat. Das war nur ein Virenscanner! Das heißt, ein Hersteller von Medizinprodukten muss all das adressieren. Nur dann kann er die Haftung übernehmen. Das Problem ist, dass ein Krankenhaus, das eigenständig Patches einspielt, um sein System sicher zu machen, von Gesetztes wegen sozusagen zum Hersteller der Produkte wird; das heißt, das Krankenhaus muss damit die volle Haftungsverantwortung übernehmen.

Das ist der Grund, weshalb die Krankenhäuser sagen: „Dieses Risiko gehe ich nicht ein. Wir warten, bis der Hersteller die Patches freigibt.“ Das heißt, das muss validiert werden. Das dauert bei kritischen Sicherheitspatches um die drei Monate, wenn nicht noch länger. Es muss überprüft werden, ob sich dadurch nicht etwas verändert.

Das ist ein Riesenproblem, das wir heute bei der Informationssicherheit in den Krankenhäusern haben, gerade aufgrund dieser ganzen Vernetzung. Es reicht, wenn ein System angegriffen werden kann; dann kann ein ganzes Netzwerk übernommen werden.

Martin Wundram, ein guter Bekannter von mir, ist öffentlich vereidigter IT-Forensiker. Er hat von einem Krankenhaus den Auftrag erhalten, einen Penetrationstest vorzunehmen: „Geh mal auf unser System und schau, ob du reinkommst.“ Er hat dafür nur eine

relativ kurze Zeit benötigt. An dem Krankenhaussystem waren noch vier andere Krankenhäuser angeschlossen. Er konnte die volle Kontrolle über diese Krankenhäuser übernehmen, über alle Systeme. Das müsste uns, glaube ich, zum Nachdenken bringen.

Deswegen sage ich: Wir brauchen die Verschleierungstaktiken, die im Moment auch die Softwarehersteller vornehmen, nicht. Es wird immer – das habe ich in meiner Stellungnahme als „Security by Obscurity“ bezeichnet – gesagt: „Wenn die Angreifer unsere Sicherheitsmaßnahmen nicht kennen, wissen sie auch nicht, wie sie uns gefährden können.“ Dieser Ansatz ist aber sehr gefährlich. Die Angriffe werden immer intelligenter, und die Angreifer können die Lücken in der Software immer besser herausfinden. Wenn wir wissen, dass Systeme nicht gepatcht sind, muss sich ein Angreifer nur den Patch anschauen, um zu wissen, wie er ein Krankenhaus angreifen kann. Das ist ein Riesenproblem.

Deswegen stehe ich dafür ein, Transparenz – auch hinsichtlich der Software – zu schaffen. Wenn Software für sicherheitskritisch relevante Bereiche geschaffen wird, muss sie auditierbar sein. Sie muss theoretisch von jedem eingesehen werden können. Es geht nicht darum, zu sagen: „Das ist ein Geschäftsgeheimnis.“ Es geht um uns – wir alle sind Patienten – und um unsere Sicherheit.

Zur Frage, wer für die Aufsicht über die IT-Sicherheit zuständig ist: Wir müssen uns erst einmal anschauen, was Informationssicherheit für uns ist. Es gibt unterschiedliche Aufsichtsbehörden. Zum Beispiel gibt es eine Landesbeauftragte für Datenschutz und Informationsfreiheit. Diese ist für die Aufsicht im Bereich Datenschutz zuständig. Es gibt die Bezirksregierungen; diese sind für die Aufsicht über die ordnungsgemäße Funktionsfähigkeit im Bereich Medizinprodukte zuständig. Es gibt unterschiedlichste andere Bereiche, in denen es um Daten und Informationen geht. Deswegen habe ich etwas gegen den Begriff „Cyber“. „Cyber“ ist ein sehr undefinierter Begriff, sodass wir keine Zuständigkeiten definieren können. Das sehen Sie bereits hinsichtlich der Informationssicherheit. Dafür gibt es keine eindeutige Zuständigkeit. Für das Patientengeheimnis sind die Ärztekammern zuständig. Theoretisch dürfte keine Aufsichtsbehörde Patientendaten anschauen. Sie sehen, an welchen Stellen wir hier Probleme haben. Diese bestehen aufgrund der Daten und der unterschiedlichen Verantwortlichkeiten. Das gilt es zu adressieren: Wer ist wofür verantwortlich? – Ich danke Ihnen.

Vorsitzender Günter Garbrecht: Als nächstes werde ich Herrn Appel das Wort erteilen, dann Herrn Blum, Herrn Dr. Häger sowie Herrn Röhrl.

Roland Appel (Bornheim): Herr Vorsitzender! Meine Damen und Herren Abgeordnete! Liebe Kollegen! Zunächst einmal vielen Dank für die Einladung! Es ist mir eine große Freude, hier vortragen zu dürfen.

Vielleicht ein Wort vorweg. Mein Kollege hat es vorhin richtig dargestellt: Es gibt im Bereich der Krankenhausdaten eine große Unsicherheit. Man muss der Politik aber auch sagen, was sie im Rahmen ihrer Kompetenzen tun kann und was nicht, was möglich ist und was meines Erachtens nicht geht. Vielleicht hilft dabei, dass ich diesem Hause vor langer Zeit angehört habe.

Es kommt bei der Beherrschbarkeit von Angriffen im Bereich der Krankenhäuser zutage, dass die IT heute eine große Schwachstelle ist. Sie ist von vielen Seiten angreifbar. Das können Sie im Einzelnen in meiner Stellungnahme 16/3964 nachlesen. Das Bundesamt für Sicherheit in der Informationstechnik hat in seinem Bedrohungsbericht festgestellt, dass die Mehrzahl der Bedrohungen keine gezielten Angriffe seien, sondern tägliche Spam-E-Mails und Schadsoftware. Deren Anzahl hat sich von 100 Millionen Programmen 2012 auf 400 Millionen Programme Stand Anfang 2016 erhöht. Es werden sozusagen täglich und jährlich mehr. Die meisten Angriffe – die Methodik im Falle des Krankenhauses in Neuss war ähnlich – wurden durch menschliche Naivität und Versagen begünstigt. Man öffnet eine E-Mail, kann sie nicht als Spam oder Schadstoffware erkennen, und das System ist – zack – infiziert.

Interessant ist vielleicht auch, dass in 42 % der Fälle, die das BSI aufgelistet hat, der Virenangriff nicht abgewehrt wurde. In der Mehrzahl der Fälle – über 54 % – war menschliches Versagen der Auslöser. Es ist also nicht unbedingt eine Frage der Technik. Meist sind die Virenscanner aktuell. Dem Faktor Mensch kommt meines Erachtens eine zu geringe Bedeutung zu, wenn wir über die IT-Sicherheit im Krankenhaus reden.

Vor zwei Jahren habe ich eine große interne Untersuchung zum Datenschutz innerhalb der Bundesagentur für Arbeit durchgeführt. In dieser wurde deutlich: Es ist ganz wichtig, dass die IT-Sicherheit und die IT überhaupt im Vorstand einer Institution – das gilt für die BA genauso wie für Krankenhäuser – angesiedelt ist. Der IT-Berater mit Kompetenzen, der Datenschutzbeauftragte – diese gibt es in den Krankenhäusern ebenfalls – sollten beim Vorstand angesiedelt sind; besser noch – das halte ich heute für unabdingbar – ist, wenn es einen IT-Vorstand gibt. Dieser sollte für die IT-Sicherheit und die Struktur der IT verantwortlich sein. Das ist eine Organisationsentscheidung.

Die Kollegen haben es deutlich gemacht: Wir sind technikgetrieben. Dann entstehen in den meisten Krankenhäusern – diese unterscheiden sich nicht von der freien Wirtschaft, für die ich viel arbeite – Insellösungen. Das heißt, ein Professor hat die Mittel für ein tolles neues Gerät bekommen – vielleicht über Drittmittel –, und das steht dann im Krankenhaus. Möglicherweise passt es nicht in die gesamte Krankenhausarchitektur. Dieses Problem zu lösen, ist zunächst unmöglich. Dafür gibt es sogenannte IT- oder Datenschutzmanagementsysteme. Das heißt, es muss anhand der Prozesse, die es im Krankenhaus gibt, systematisch von entsprechendem Personal – das kann man sich einkaufen – eine Struktur geschaffen werden, in der alle Teile der IT, der IT-Sicherheit und – am besten auch – des Datenschutzes aufgenommen werden. Bekannt ist zum Beispiel der Grundschutz nach der BSI-Empfehlung. Diese Struktur muss man implementieren und durchziehen. Da sollte es auch Notfallpläne geben: Am Wochenende oder wenn der IT-Spezialist im Urlaub ist, weiß man dann, wer für diese Dinge zuständig ist.

Ich halte es darüber hinaus für wichtig, dass man die Mitarbeiter schult. In der Wirtschaft läuft das übrigens genauso wie in den Krankenhäusern. Zunächst werden die Dinge angeschafft, die die Produktivität steigern, die Maschinen. Dann werden die Mitarbeiter an den Maschinen geschult. An den Datenschutz und Datensicherheit denkt man dann ganz zuletzt; wir haben es hier sogar mit dem Patientengeheimnis, also mit strafbewehrten Daten, zu tun. Leider ist das in der Praxis so.

Deswegen ist eine meiner Hauptforderungen: Wir müssen der Politik sagen: Datenschutz und Datensicherheit sind Chefsache. Der Chief Information Officer, der CIO – so nennt man ihn auf Neudeutsch –, sollte beim Vorstand angesiedelt sein. Er sollte ausreichend Sensibilität in den Vorständen der Krankenhäuser und Krankenhausgesellschaften für dieses Thema herstellen.

Man sollte Managementsysteme einführen. Außerdem sollten die Mitarbeiter geschult werden. Heute ist das eigentlich kein wichtiges Ding. Ich habe in meiner Stellungnahme geschrieben, dass 1,4 Millionen der im National Health System in England Beschäftigten 2003 den europäischen Computerführerschein – dieser enthält in Deutschland auch Module in Informationssicherheit und Datenschutz – erhalten haben; das haben sie durchgezogen. Sie haben dabei festgestellt – das zum Thema „Gewerkschaften“ –: Die Mitarbeiter haben mehr Zeit für die Pflege, und zwar 39 Minuten pro Tag, und sie sind – auch ganz wichtig – der Einführung neuer Technik gegenüber positiver aufgeschlossen. Das heißt, entsprechende Probleme mit dem Betriebsrat würde es viel seltener geben, wenn die Menschen kompetent sind und verstehen, was auf sie zukommt.

Ich bin der Meinung, die Landesregierung wäre damit gut beraten. Die Förderpauschalen sind, wie sie sind. Es ist ja nicht mehr Geld vorhanden. Die Piraten fordern in ihrem Antrag, man solle die Mittel einfach erhöhen. Das ist klar; die Piraten sind Freibeuter, sie müssen sich nicht an Gesetze halten.

(Heiterkeit)

Aber wenn die Fallpauschalen erhöht werden, ist die Gefahr groß, dass die Mittel in den allgemeinen Investitionshaushalt fließen. Deswegen empfehle ich, dass die Landesregierung sagt: „Um den Nachholbedarf aufzuholen…“ Die anderen Kollegen werden das auch noch sagen: Der Nachholbedarf ist enorm. Ich nenne ein vergleichbares Beispiel: Derzeit werden von Daimler autonome Fahrzeuge entwickelt; ich finde dieses Daimler-Projekt sehr spannend. Dabei werden die Datenflüsse und der Datenschutz bedacht. Sie können sich nicht vorstellen, wer alles diese Daten haben und handeln möchte. Alles muss anonymisiert und datenschutzfreundlich sein. Das werden wir im Krankenhaus auch bekommen. Wir werden in wenigen Jahren die Situation haben, dass die Pharmaindustrie oder die Geräteindustrie sagt: „Gebt uns anonymisierte Forschungsdaten, damit wir unsere Produkte weiterentwickeln können.“ Wenn diese wirklich anonymisiert sind, finde ich das richtig. Das ist Kapital für die Krankenhäuser. Aber davon können Sie mit der heutigen Technik, mit den heutigen Sicherheitssystemen, mit dem heutigen Datenschutzstandard nur träumen. So etwas heute zu machen, wäre absolut unverantwortlich.

Deswegen müssen wir eigentlich jetzt handeln und ein Programm auflegen, um diesen Rückstand, den die Krankenhäuser auch im Vergleich zur Wirtschaft haben, aufzuholen. Sonst können wir uns die Wirtschaft 4.0 von der Backe putzen. – Danke schön.

Vorsitzender Günter Garbrecht: Sie haben eine schöne Vorlage für Herrn Blum geliefert, dessen Krankenhaus bereits einen IT-Vorstand hat. Sie haben bereits die Empfehlung herausgegeben, dass die Chefärzte ihre Smartphones an der Pforte abzugeben haben, Herr Blum. – Bitte.

Matthias Blum (Krankenhausgesellschaft Nordrhein-Westfalen e. V.): Vielen Dank! – Herr Vorsitzender! Meine sehr geehrten Damen und Herren Abgeordnete! Meine sehr geehrten Damen und Herren! Zunächst herzlichen Dank, dass wir heute hier eingeladen worden sind. Es ist schon so viel gesagt worden, dass ich versuchen werde, anhand der Fragen zu antworten. Ich habe mir diese auch notiert. Im Bedarfsfall bitte ich die Fragenden, nachzuhaken. Ich versuche, meine Redezeit zu beschränken und nichts zu wiederholen, was schon gesagt worden ist.

Ich glaube, die Komplexität der gesamten Fragestellung zeigt, dass diese Anhörung sehr sinnvoll war, dass es sinnvoll war, sich mit diesem Thema auseinanderzusetzen. Wir hatten schon am 9. März die Ehre, in einer Sitzung des Ausschusses zu berichten, wie sich die Situation darstellt. Ich will davon im Einzelnen nur die Dinge wiederholen, die sich in den Fragen wiedergefunden haben.

Die erste Frage war von Herrn Sommer von der Piraten-Fraktion; er fragte: Wie hoch ist der gesamte Investitionsbedarf im Bereich der IT? Wir haben versucht, das in unserer Stellungnahme 16/3962 auszudrücken. Derzeit geben die Krankenhäuser etwa 1,5 % ihres Budgets für Personal und Sachkosten in diesem Bereich aus; Banken und Versicherungen geben etwa 10 % bis 15 % dafür aus. Das gibt uns einen gewissen Aha-Effekt. Wir können davon ausgehen, dass die 364 Klinken mit 18,3 Milliarden € Gesamtbudget im Durchschnitt etwa 750.000 € pro Krankenhaus für – wohlgemerkt – Personal und Sachkosten ausgeben. Personal und Sachkosten muss man zusammen sehen. Wenn Sie diese Mitarbeiter auf dem Markt suchen, müssen Sie feststellen, dass sie in der heutigen Zeit übrigens nicht günstig sind. Darüber hinaus hat mein Kollege Herr Baum ausgerechnet, dass eine sachgerechte IT-Ausstattung der Krankenhäuser bundesweit etwa 600 Millionen € jährlich kosten würde. Die Investitionskosten, die bundesweit von der DKG genannt worden sind – sie decken sich mit den INEK-Zahlen – entsprechen etwa 10 % davon. Sie können das auf das Investitionsbarometer in NRW – ich glaube, das haben Sie hier schon hinlänglich erörtert – beziehen. 10 % von 1,5 Milliarden € entspricht 150 Millionen €; da sind die Personalkosten noch nicht drin; das ist der reine Investitionsbedarf. Darüber muss man sich im Klaren sein.

Wie sieht die IT-Struktur – ich komme auf die Frage von Herrn Ünal zu sprechen – in den Krankenhäusern aus? Ist sie überall marode und veraltet? Wir haben keine 364 Ortstermine durchgeführt, um uns die IT jeweils vor Ort anzuschauen. Die IT in den Krankenhäusern läuft. Wir müssen uns aber darüber im Klaren sein, dass die IT letztlich ein hoch investiver Bereich ist. Wenn Sie auf Dauer à jour bleiben wollen, müssen Sie dauerhaft investieren. Sie kennen das von ihren privaten Programmen; da müssen Sie auch immer irgendwelche Sicherheitsupdates durchführen. Entweder Sie haben diese bereits beim Kauf mitbezahlt, oder Sie müssen das immer wieder nachkaufen. Viele Programme sind auch in der sogenannten Beta-Version; die Programme reifen bei Ihnen und werden entsprechend nachgerüstet.

Zusammenfassend kann man sagen: Die Investitionsmittel, die im Moment vorhanden sind, reichen nicht für die Herausforderungen, die im Rahmen der Digitalisierung auf die Krankenhäuser zukommen. Ich nenne das IT-Sicherheitsgesetz und das E-Health-Gesetz, das die Krankenhäuser indirekt betrifft, Stichwort „Medikationsplan“. Ich glaube, das ist auch in den anderen Reden relativ deutlich geworden.

Ich glaube, dass sich das Land seiner Verantwortung bewusst ist. In den Rahmenvorgaben zum Krankenhausplan ist zum Ausdruck gekommen, dass man in dieser Richtung unterwegs ist, dass man auch Telematik, Infrastruktur etc. aufbauen will.

Wir müssen uns nur im Klaren darüber sein – in den Beiträgen meiner Vorredner ist das auch zum Ausdruck gekommen –: In den letzten fünf Jahren hat sich merklich etwas getan. Wir sind von einer eher unterstützenden in eine beherrschende Stellung gekommen. Auch im Bereich der Medizinprodukte ist das, glaube ich, sehr deutlich geworden. Den angesprochenen Fall, dass einer die Systeme von vier Krankenhäusern übernommen hat, kannten wir noch nicht; vielleicht können wir anschließend noch darüber sprechen.

Nichtsdestotrotz – wir haben es schon einmal gesagt –: Eine 100%ige Sicherheit wird es in diesem Bereich nicht geben. Wir können heute sagen: Es ist noch zu keiner Patientengefährdung gekommen; jedenfalls ist uns keine bekannt. Aber wir können nicht mit Sicherheit sagen, dass es nie dazu kommen wird.

Wenn die Digitalisierung weitergeht, ist die Vernetzung immer größer. Dann muss nur jemand von den niedergelassenen Ärzten seine MRT-CD ins Krankenhaus mitnehmen; das Krankenhaus kann dann sagen: „Damit fange ich mir möglicherweise einen Virus.“ Ich will damit sagen: Die Digitalisierung ist Fluch und Segen. Darüber müssen wir uns alle im Klaren sein. Allerdings werden, glaube ich, die Aspekte des Segens überwiegen. Deswegen werden wir mit dem Fluch fertigwerden müssen.

Herr Yüksel hat dazu nachgefragt: In 99 % der Fälle erfahren wir nichts von den Angriffen. Wenn wir das in 99 % der Fälle erfahren würden, könnten wir, glaube ich, drei Mitarbeiter einstellen, die die Mitteilungen entgegennähmen. Die Krankenhäuser werden täglich, minütlich, 24 Stunden an 365 Tagen im Jahr angegriffen. Das ist so. Die Angriffe sind nicht unbedingt gezielt, sondern kommen oft zufällig. So war es auch im Falle des Krankenhauses in Neuss: Es wurde eine E-Mail geöffnet. Deswegen heißt es auch immer, man müsse Back-ups machen und die Sache entsprechend aufstellen; das wäre aus meiner Sicht nicht zu leisten.

Wir können Sie beruhigen. Nachdem der Bundestag gehackt worden ist, wurde das IT-Sicherheitsgesetz verabschiedet. Es gibt nun eine sogenannten Kontaktstellen, und alle Krankenhäuser, die zur kritischen Infrastruktur gehören werden – wir haben gehört, dann in Nordrhein-Westfalen zwischen 20 und 50 dazugehören werden, das muss noch festgelegt werden –, sind verpflichtet, jegliche Angriffe sofort zu melden. Die anderen Krankenhäuser sind aber mit Sicherheit auch gut beraten, wenn sie schwerwiegendere Dinge – nicht die täglichen Angriffen, mit denen sie fertig werden – auch melden müssen.

Von Herrn Preuß habe ich keine Frage an mich in Erinnerung.

Herr Alda, Sie hatten mir eine dreigeteilte Frage gestellt. Ich versuche, diese im Zusammenhang zu beantworten. Sie haben mich zunächst gefragt, welche Auswirkungen die Krankenhausfinanzierung in diesem Zusammenhang habe. Die Finanzierung ist dual. Für die Betriebskosten und die Instandhaltung sind die Krankenkassen zuständig. Daneben gibt es die Investitionskosten.

Welche Auswirkungen gibt es im Bereich der Betriebskosten und der Instandhaltung? Dafür werden – das geht aus dem Investitionsbarometer hervor – knapp 700 Millionen € ausgegeben. Damit liegt NRW im Vergleich dieser Ausgaben für die Krankenhäuser im Bundesdurchschnitt. Man kann nicht sagen, dass hier Geld falsch ausgegeben werde.

Das Krankenhausstrukturgesetz hat die Krankenhäuser hier unterstützt. Dafür waren wir dankbar. Das haben wir den entsprechenden Fraktionen auf Bundes- und Landesebene auch gesagt. Die Krankenhäuser haben diese Unterstützung bei den Betriebskosten dringend gebraucht.

Die Probleme im Bereich der Investitionskosten sind im Rahmen des KSG bekanntermaßen noch nicht gelöst worden. Man hat einen Strukturfonds aufgelegt, der sicherlich eine Hilfe ist; aber das Grundproblem der zu geringen Investitionskostenfinanzierung der Länder löst er nicht. Das Problem werden wir also weiterhin haben.

Zur Investitionsfinanzierung des Landes im Vergleich mit der Investitionsfinanzierung der anderen Bundesländer: Dieser Bereich betraf die kurzfristigen Anlagengüter. Ich habe die aktuellen Zahlen, die wir auch am 9. März vorgetragen haben, mitgebracht. NRW liegt mit 317 Millionen € – also 2.882,73 € je Bett – im Vergleich der Bundesländer, wenn wir es richtig recherchiert haben, zwischen Mecklenburg-Vorpommern und Bayern und demnach etwas über dem bundesweiten Durchschnitt.

Diese schicke Tabelle bringt zum Ausdruck, wo die Krankenhäuser im Vergleich stehen. Aber alle Krankenhäuser sind in Bezug auf die Investitionskosten unterfinanziert. Kein Land ist an dieser Stelle gut aufgestellt. Sich in der Tabelle im Mittelfeld zu befinden, heißt nicht, dass wir unsere Arme hochreißen und sagen können: „Das ist alles prima.“ Vielmehr befinden wir uns damit im Mittelfeld im Vergleich der unzureichenden Finanzierung der Krankenhäuser. Das kann uns nicht beruhigen, schon gar nicht im Hinblick auf unseren Anspruch bezüglich der Patienten.

Die letzte Frage, die Sie gestellt haben, betraf, ob die zweckgebundene Förderung eine Lösung des Problems darstellen könnte. Ich will diese Frage vorsichtig beantworten: Meinen Sie, dass die Krankenhäuser verpflichtet werden sollen, einen bestimmten Anteil der 317 Millionen € für einen bestimmten Bereich aufzuwenden? Davor kann ich nur dringend warnen. Wenn Sie das machen würden, würden Sie im Prinzip zwar ein Loch stopfen, aber andere Löcher aufreißen. Das betrifft irgendwann den Bereich der Hygiene; diese kann dann irgendwann nicht mehr gewährleistet werden.

Im Moment machen die Krankenhäuser das Allernotwendigste, um den Betrieb vernünftig am Laufen zu halten. Aber wir können von einer Vorgabe wie beschrieben nur warnen. Auch die Eigenmittel der Krankenhäuser sind stark zurückgegangen. Das belegt auch das Investitionsbarometer. 2014 sind die Mittel um mehr als ein Viertel zurückgegangen; 2014 lagen diese noch bei 430 Millionen €. Darüber muss man sich

einfach im Klaren sein. Wir meinen, dass hinlänglich zum Ausdruck kommt, dass hier Handlungsbedarf besteht. Wir haben das anhand dessen, was wir hier letztens erörtert haben, auch verstanden. Das Ministerium wollte sich in den nächsten zwei, drei Wochen – so haben wir es verstanden – zum Investitionsbarometer NRW äußern. Wir hoffen, dass das Land die Verantwortung, die es in den Rahmenvorgaben zum Krankenhausplan zum Ausdruck gebracht hat, in die Tat umsetzt. – Vielen Dank.

Vorsitzender Günter Garbrecht: Danke schön, Herr Blum. – Herr Dr. Häger, bitte schön.

Dr. Dirk Häger (Bundesamt für Sicherheit in der Informationstechnik, Referat Kritische Infrastruktur): Danke! – Herr Vorsitzender! Sehr geehrte Damen und Herren! Ich bin von Herrn Ünal nach der Aufrechterhaltung des IT-Sicherheitsniveaus gefragt worden. Bevor ich ein paar exemplarische Beispiele nenne, möchte ich den Grundsatz erläutern: Das IT-Sicherheitsgesetz gibt IT-spezifische Sicherheitsstandards vor. Das ist auch in der Stellungnahme 16/3962 der Krankenhausgesellschaft angesprochen worden. Die Krankenhäuser erarbeiten diese Standards selbst und stimmen diese mit dem BSI und anderen Verbänden ab.

In einem Jahr können wir uns, glaube ich, genau darüber unterhalten, wie das aussehen wird. Daher will ich nur ein paar exemplarische Beispiele nennen, nach denen Sie gefragt hatten.

Technische Maßnahmen, die obligatorisch sind: Patches sind eine typische Maßnahme aus Büronetzen. Das ist der Stand der Technik. Darauf bestehen wir natürlich. Das Einsetzen von Patches in Industrial Control Systems – die Geräte in den Krankenhäusern sind genannt wurden – ist nicht immer ganz einfach. In den letzten Jahren ist in den Krankenhäusern Folgendes passiert: Durch die zunehmende Vernetzung sind auf einmal Systeme, die den Gefahren des Internets eigentlich gar nicht ausgesetzt werden dürften, ans Internet angeschlossen worden. Für die Probleme in diesem Zusammenhang muss man natürlich Lösungen finden. Der Angriffssektor in den Krankenhäusern betrifft die Bürokommunikation – das Lesen von E-Mails und Browsen im Internet. Sichergestellt werden muss – das ist eigentlich obligatorisch –, dass man von einem System, das ans Internet angebunden ist, kein Zugriff auf eine Herzlungenmaschine haben darf. Wir können nicht verhindern, dass Angreifer ins Netz eindringen. Aber die Auswirkungen müssen begrenzt werden. Ich nenne das Stichwort „Netzwerksegmentierung“. Man muss stark darauf achten, was ein Angreifer machen kann, wenn er einen PC übernommen hat.

Ich will eine beispielhafte organisatorische Maßnahme nennen, von der sicher ist, dass sie im IT-Sicherheitsgesetz stehen wird – Sicherheit muss nicht nur umgesetzt werden, sie muss regelmäßig geprüft werden –, und zwar die Maßnahme, alle zwei Jahre Audits durchzuführen. Die 20 bis 50 Krankenhäuser im NRW – wenn die genannten Zahlen stimmen – werden entsprechend verpflichtet. Das kann auch auf die anderen Krankenhäuser ausgeweitet werden, die von der KRITIS nicht erfasst werden. Wir erleben immer wieder, dass zwar ein Sicherheitskonzept besteht, aber seine Wirksamkeit nicht vorhanden ist. Eine regelmäßige Prüfung rate ich Ihnen durchaus an.

Wir brauchen – das ist auch schon einmal gefallen – einen für die IT-Sicherheit Verantwortlichen. Sie, Herr Appel, hatten den CIO genannt. Eigentlich will ich aber einen CISO haben; der CIO ist nämlich für die IT verantwortlich. Er hat mit Übernahme der Sicherheitsaufgabe automatisch einen Interessenkonflikt, da er die Systeme am Laufen halten möchte. Sicherheit und Betrieb von IT müssen nicht immer miteinander einhergehen. Der CISO muss im Vorstand angesiedelt sein und sich über den CIO beschweren können, der etwas bei Kosteneinsparung schnell umgesetzt haben möchte. Jemand muss für die IT-Sicherheit verantwortlich sein, nämlich der CISO. Es muss ganz klar sein, dass das seine Aufgabe ist. Er muss schreien, wenn die Sicherheit nicht gewährleistet wird.

Die üblichen organisatorischen Sachen wurden auch schon genannt. Da kann man eine Menge Sachen machen, zum Beispiel private IT verbieten.

Sie hatte noch gefragt, ob die Admins geeignet ausgebildet seien, ob es noch personelle Fragen gebe. Die Antwort ist ganz klar: nein. Das ist nicht krankenhausspezifisch. Die Behörden, denke ich, haben generell Schwierigkeiten, über ihre Tarife gute Adminis zu bezahlen. Auch die Wirtschaft hat momentan Schwierigkeiten – das wurde auch genannt –, gute IT-Leute zu bekommen. Das ist schwierig. Ich weiß nicht, wie die Admins im Krankenhaus bezahlt werden. Sind sie im mittleren Dienst?

(Torsten Sommer [PIRATEN]: A 12!)

– Okay. Das ist der gehobene Dienst. – Auch wir bei den Bundesbehörden haben Schwierigkeiten, gute Admins zu bekommen. Ich habe keine richtige Lösung für dieses Problem, außer diesen mehr Geld zu geben. Das sorgt aber für Unzufriedenheit bei den Alteingesessenen im mittleren Dienst, die gute Arbeit machen. Es gibt keine schnelle Lösung.

Nichtsdestotrotz muss man in die Leute, die man hat, investieren.

Das Beispiel kommt immer wieder hoch: Der dumme Mitarbeiter klickt auf einen Link. Ich bin dagegen, das den Mitarbeitern vorzuwerfen. Es bedarf – ich erwähne es – Wissen bei den Admins. Denn wenn ein Mitarbeiter durch den Klick auf einen Link die Krankenhaus-IT nachhaltig gefährdet, ist etwas mit der Krankenhaus-IT nicht in Ordnung. Die Admins sind dafür zuständig, dass böse Anhänge an E-Mails nicht ins System dringen können. Die Admins benötigen etwas Zeit, sich die Log-Daten anzuschauen, damit ein Angriff auch detektiert wird. Investieren Sie also in Ihre Admins! Sie bekommen gute ausgebildete Admins nicht günstig auf dem Markt. Also nehmen Sie die, die Sie kriegen, und investieren Sie in diese. – Das war’s. Danke.

Vorsitzender Günter Garbrecht: Als letzter in dieser Runde spricht der Vertreter des Landeskriminalamts, bitte schön.

Markus Röhrl (Cybercrime-Kompetenzzentrum, Landeskriminalamt NRW): Vielen Dank! – Herr Vorsitzender! Meine Damen und Herren! Mir ist keine konkrete Frage gestellt worden. Ich bin in der Lage, auf alles etwas sagen zu können, aber das tue ich natürlich nicht; all das, was bisher schon gesagt worden ist, ist aus meiner Erfahrung heraus absolut richtig.

Vielleicht darf ich kurz darstellen, um was für ein Phänomen es sich hier handelt. Ich möchte vor allem sagen: Die Bedrohung berührt nicht allein die Krankenhäuser. Das, was im Krankenhaus in Neuss zum Problem geworden ist – über Ransomware werden typischerweise Daten verschlüsselt, die nach Lösegeldzahlungen wieder entschlüsselt werden –, geht über Spams massenweise – das ist eben bereits gesagt worden – rein.

Wir im Landeskriminalamt sind davon fast selbst betroffen worden. Die erste Hürde hatte die Ransomware bereits übersprungen; Virenscanner und Firewalls können solche Schadcodes häufig gar nicht aufhalten, weil die Signaturen so neu sind, dass die herkömmlichen Virenscanner diese noch gar nicht kennen. In der Regel dauert es vom erstmaligen Auftreten solcher Malware 14 Tage, bis Kaspersky und Norton das analysiert und darauf reagiert haben. Das heißt, seit dem erstmaligen Auftreten gibt es immer 14 Tage, in denen das System unsicher ist. Ihr System kann dann noch so sicher sein; der Schadcode kann im System ankommen. Dann passiert das, was Herr Dr. Häger gesagt hat: Ein Mitarbeiter öffnet eine E-Mail – dadurch passiert in der Regel noch nichts – und ihren Anhang, sodass möglicherweise eine Zip-Datei, eine Java-Datei ins System dringt und aus dem Internet gegebenenfalls weitere Schadprogramme nachlädt, ohne dass Sie das merken.

Bei der Ransomware, die auch im Krankenhaus in Neuss eingesetzt worden war, ging es der Tätergruppe – das möchte ich bestätigen – mit fast 100%iger Sicherheit nicht darum, eine kritische Infrastruktur anzugreifen und Patientendaten zu kompromittieren oder abzufischen. Wie bei allen anderen Behörden, Unternehmen und Krankenhäusern in Nordrhein-Westfalen, die ebenso von dieser Welle betroffen waren, ging es schlicht und einfach darum, Lösegeld zu erpressen. Die Forderungen waren nicht wahnsinnig hoch; die betroffenen Opfer sollten durch die geringe Höhe der Lösegeldforderung sogar dazu animiert werden, das Lösegeld zu zahlen. Nach Schätzungen von Sicherheitsunternehmen tun das durchaus 30 % bis 40 % der betroffenen Haushalte, Unternehmen und kritischen Infrastrukturen; das kann ich letztendlich nicht belegen.

Wir haben hier einen kriminellen Akt, es gibt Täter. Wenn diese nicht ermittelt und gestoppt werden, dann bedeutet das, dass sich Betroffene mit einem geringen Lösegeld freigekauft haben und, wenn sie Glück haben, einen Entschlüsselungscode erhalten. Andere Opfer werden dann aber weiter malträtiert. Deswegen appellieren wir – unabhängig davon, ob es sich um ein Unternehmen, einen Privathaushalt oder insbesondere um eine kritische Infrastruktur oder Behörde handelt –, dass die Polizei über einen solchen Vorfall informiert wird. „Informiert wird“ bedeutet für mich, dass Strafanzeige erstattet wird. Denn nur dann sind wir zuständig und können auch ermitteln.

Im Falle des Krankenhauses in Neuss ist das geschehen. Allerdings geschah dies auf unser Anraten hin. Die Woche war sehr turbulent. Wir haben, glaube ich, am 10. oder 11. Februar aus der Presse von diesem Sicherheitsvorfall Kenntnis bekommen und sofort mit dem Krankenhaus in Neuss Kontakt aufgenommen. Wir hatten dann einen ganz ausgezeichneten Kontakt zur Geschäftsleitung des Krankenhauses, zum IT-Verantwortlichen, zur Justiziarin. Alle waren sich darin einig, dass es gut sei, die Polizei so schnell wie möglich ins Haus zu bekommen. Dr. Häger und das BSI waren dann

am Abend und die ganze Nacht über auch da und haben gearbeitet, weil ein Krankenhaus in solch einem dicht besiedelten Bereich – auch wenn es hier viele Krankenhäuser gibt – eine kritische Infrastruktur darstellt. Für uns, die Polizei war es daher nicht uninteressant.

Man kann sagen: Das war der erste – zumindest mir bekannte – Angriff auf eine kritische Infrastruktur in Nordrhein-Westfalen, der einen schädigenden Erfolg hatte. Der Vorfall war zumindest monetär schädigend; die Patienten sind nicht geschädigt worden. Zwar mussten Operationen verschoben werden, aber das konnte durch die umliegenden Krankenhäuser aufgefangen werden, gar keine Frage.

Insoweit war der Sachverhalt für uns sehr interessant. Deswegen haben wir uns, das Cybercrime-Kompetenzzentrum des Landeskriminalamts, in diese Ermittlungen eingebracht. Für uns war das ein herausragender Fall. Wir konnten hier gegebenenfalls viel für die Zukunft lernen. Wir, das Landeskriminalamt, ermitteln nicht nur, sondern betreiben auch Awareness. Wir sind tagein tagaus in Nordrhein-Westfalen unterwegs, in Unternehmen, in Industrieverbänden, in Behörden. Wir machen – zum Teil zusammen mit anderen Partnern – Awarenessveranstaltungen, um Punkte anzusprechen, die aus unserer Sicht notwendig sind, um ein möglichst großes Maß an IT-Sicherheit im Unternehmen zu garantieren.

Wir sind keine Fachleute für IT-Sicherheit. Aber wir stellen bei allen Ermittlungen fest – insbesondere bei kleineren und mittleren Unternehmen in Nordrhein-Westfalen –, dass es an allen Ecken und Enden fehlt. Es gibt Unternehmen, bei denen der CIO oder der CISO nach wie vor der Hausmeister ist, weil er sich mit Technik auskennt; deswegen verwaltet und managt er das Netzwerk des betreffenden Unternehmens. Über das Netzwerk, über das Internet wird die Automatisation betrieben usw. Das funktioniert natürlich nicht.

Das Beispiel ist banal. Das war beim Krankenhaus in Neuss auch nicht der Fall. Die IT-Struktur, die wir dort gesehen haben, war hoch professionell, aber auch hoch komplex. Diese Komplexität – das hat der eine oder andere Vorredner bereits ausgeführt – führt dazu, dass es keine 100%ige Sicherheit gibt. Fachleute sagen, es gebe heutzutage keine Software und keine Hardware mehr, die zu 100 % sicher sei. Ich glaube, das verwundert uns auch nicht. Es gibt wahrscheinlich auch kein Flugzeug, kein Auto, von dem behauptet werden kann, es sei in den nächsten zehn Jahren zu 100 % sicher. Das geht einfach nicht.

Wir sagen in unseren Veranstaltungen aber immer, dass die Unternehmen – insbesondere wenn es sich um kritische Infrastruktur handelt – investieren müssen – Herr Dr. Walther hat dies bereits angesprochen –, und zwar ständig. Man muss sich – das ist unser Rat – immer professionelle IT-Dienstleister leisten. Ein DAX-Unternehmen hat eine IT-Abteilung mit 300 oder 500 Mitarbeitern, die nicht nur nach A 12 bezahlt werden, sondern zum Teil deutlich höher. Für ein solches Unternehmen ist das in der Regel kein Problem. Aber ein mittelständisches Unternehmen, ein Krankenhaus muss sich auf einen externen IT-Dienstleister stützen, damit die IT-Sicherheit – bis hin zum Penetrationstest – vernünftig ist; denn ansonsten steigt das Risiko.

IT-Security zur Chefsache machen, empfehlen wir natürlich auch immer. Dazu gehört, dass es einen strengen Verhaltenscodex, eine Cyber-Compliance-Strategie geben muss; das gibt es nicht so häufig. Oft darf jeder mehr oder weniger machen, was er will. Es gibt offene USB-Anschlüsse, sodass man über einen USB-Stick seine Bilder auf den dienstlichen Rechner hochladen kann. Wenn über eine solche Stelle Malware übertragen wird, hat diese gute Chancen, sich durch das Netzwerk zu arbeiten.

Wenn man schon keine 100%ige Sicherheit erreichen kann, dann muss man Planentscheidungen treffen. Man muss auf den Notfall vorbereitet sein. Dieser kommt, so sicher wie das Amen in der Kirche. Das haben wir im Krankenhaus in Neuss gesehen. Beim nächsten Mal betrifft es vielleicht ein anderes Krankenhaus. Zwischen Dezember 2015 und März 2016 – da gab es diese Welle – waren elf Krankenhäuser in Nordrhein-Westfalen betroffen. Wahrscheinlich gibt es eine hohe Dunkelziffer, die darüber hinausgeht.

Wir brauchen auf jeden Fall strenge Verhaltenscodizes in den Unternehmen, bei einer kritischen Infrastruktur, in den Krankenhäusern. So etwas muss monitored, controlled, überwacht werden.

Ein wesentlicher Appel von uns ist, kein Lösegeld zu zahlen. Ich habe das eben angesprochen; manche zahlen, weil sie sagen: „Das ist das geringste Übel. Ich muss wieder arbeitsfähig werden.“ Es gibt andere Möglichkeiten. Eine vernünftige Back-up-Strategie, das Neuaufsetzen von Systemen ist sicherlich nicht ganz billig und kostet Zeit. Die Back-ups müssen natürlich vom Netzwerk getrennt sein, sonst ist der Back-up-Server auch von der Malware betroffen. Dann bin ich in der Lage, mich relativ schnell wieder arbeitsfähig zu machen und habe dann keine Daten verloren.

Bitte zahlen Sie kein Lösegeld und stellen Sie in jedem Fall Strafanzeige.

Vorsitzender Günter Garbrecht: Herzlichen Dank! – Wir gehen jetzt in die zweite Fragerunde. Diese fängt auch mit Herrn Kollegen Sommer an, bitte schön.

Torsten Sommer (PIRATEN): Vielen Dank, Herr Vorsitzender! – Ich habe noch ein paar zusätzliche Fragen! Herr Appel, Best Buddy der Gesundheitsministerin, wollte mit seinem Wortwitz über Freibeuter und uns Piraten das Investitionsvolumen kleinreden oder als lächerlich darstellen. An Herrn Blum habe ich daher die Frage: Sind aktuell genug Mittel vorhanden, um der hier geschilderten Sicherheitslage im IT-Bereich Herr zu werden? Oder sind mehr Mittel für die Investitionen in den Krankenhäusern notwendig und nicht nur wünschenswert?

Dann habe ich noch weitere Fragen an Herrn Blum, Herrn Spyra, Herrn Dr. Walther und Herrn Dr. Häger: Gerade hieß es, 20 Krankenhäuser würden zur kritischen Infrastruktur erklärt. Der Hauptpunkt ist aber die Vernetzung. Was haben wir also davon, wenn von den 364 Krankenhäusern 20 zur kritischen Infrastruktur erklärt werden, in diesen eine hervorragende Sicherheit besteht, diese aber durch zentralisierte Dienste und sonstiges – ein einem Krankenhaus läuft die Buchhaltung für das andere gleich mit – mit anderen vernetzt sind? Im Endeffekt hört es sich für mich so an, als ob es

sinnvoll wäre, bei allen Krankenhäusern entsprechend Wert darauf zu legen. Ist es sinnvoll, da wirklich zu unterscheiden?

Nächste Frage an Herrn Dr. Häger, Herrn Spyra, Herrn Dr. Walther: Herr Dr. Häger sprach davon, den Einsatz privater IT in Krankenhäusern zu verbieten. Für wie realistisch halten Sie die Durchsetzung? Herr Dr. Häger sprach auch von segmentierten Netzen, Netzen, die wahrscheinlich nur eine Anbindung ans Intranet und keinen Internetzugang haben. Ein medizintechnischer Automat – ich glaube, Herr Spyra nannte dieses Beispiel – kann aber zwangsläufig eine Anbindung ans Internet brauchen, um aktualisiert zu werden, sonst stellt er die Arbeit ein und sagt: „Ich kann das Update nicht abrufen. Ich bin nicht betriebssicher. Ich fahre herunter.“ Wie realistisch ist es also, das wirklich zu segmentieren?

Ich hätte von Herrn Spyra – er sprach es gerade nur sehr beiläufig an – und Herrn Dr. Walther gern etwas zu öffentlich auditierbaren Sicherheitsstrukturen und auditierbare Software gehört. Wir erleben, dass die IT-Software so konfektioniert ist, dass der Hersteller externen Zugriff darauf hat und bestimmt, wann Updates usw. vorgenommen werden. Wir haben letztens erst erlebt, dass eine große Firma eine Präsentation im Internet abgespielt hat, das Video 300.000 Besucher hatte, aber dann der Windowsrechner runtergefahren ist, er hat ein Update installiert und ist wieder hochgefahren. Stellen Sie sich das bei der kritischen Struktur in den Krankenhäusern vor, dass eine Beatmungsmaschine in einer zehnstündigen neurochirurgischen Operation ein Update installiert und runterfährt. Wie wichtig ist tatsächlich auditierbare Software? Das hätte ich gern gewusst.

Wir haben die ganze Zeit davon geredet, dass beim Lukaskrankenhaus in Neuss nur ein geringer monetärer Schaden entstanden ist. Ich hätte dazu eine Frage an Herrn Röhrl, Herrn Dr. Häger, Herrn Spyra und Herrn Dr. Walther. Bei dem Beifangangriff sind Daten verschlüsselt worden. Welche Sicherheit haben wir, dass nicht auch Daten abgeflossen sind? Welche Sicherheit haben die Patienten des Krankenhauses, dass ihre Daten, die verschlüsselt worden sind, nicht an den Angreifer gesendet worden sind, sodass sich diese ihre medizinischen Daten – das höchste Private – nicht nächstes Jahr von den gleichen Angreifern zurückkaufen müssen, der dafür verspricht, die Daten zu löschen?

Herr Kollege Yüksel, Sie sprachen eben an, dass selbst das Netzwerk des Bundestags gehackt worden ist. An Herrn Röhrl und Herrn Dr. Häger hätte ich meine Frage: Der genannte Hack hat speziell den Bundestag getroffen; jemand hat die Anleitung aus einer bekannten Computerzeitschrift – der CT – Schritt für Schritt abarbeitet. Wenn selbst der Bundestag mit öffentlich zugänglichen Informationen so einfach hackbar ist, wie sieht dass dann bei einem Tailored Access, bei einem auf unsere Krankenhäuser zugeschnittenem Angriff aus? – Vielen Dank.

Vorsitzender Günter Garbrecht: Sie könnten diese Anhörung alleine beschreiten. – Jetzt noch als Garnierung die Fragen des Kollegen Wegner. – Wir haben aber im Hinterkopf, dass um 15:30 Uhr die nächste Ausschusssitzung beginnt.

Olaf Wegner (PIRATEN): Vielen Dank, Herr Vorsitzender. – Ich habe nur eine Frage.

Vorsitzender Günter Garbrecht: Sehr gut, Herr Kollege.

Olaf Wegner (PIRATEN): Im Prinzip ergänzt diese die Fragen des Kollegen Sommer. Meine Frage richtet sich an Herrn Spyra, Dr. Walther und Herrn Röhrl. Herr Röhrl hat geschildert, dass es sich im Falle des Lukaskrankenhauses aller Wahrscheinlichkeit nach um keinen gezielten Angriff auf dieses Krankenhaus gehandelt hat, sondern dass es – ich drücke mich einmal so aus – ein zufälliger Angriff war. Wahrscheinlich hat jemand eine bestimmte Anzahl an E-Mails in die Welt gesendet und geschaut, wo diese einschlagen. Stimmen Sie den folgenden Fragen zu: Wenn bereits Zufallsangriffe einen solch fatalen Erfolg haben, ist einem gezielten Angriff dann nicht Tür und Tor geöffnet? Kann ich dann von einem absolut unsicheren System sprechen?

Vorsitzender Günter Garbrecht: Danke schön. – Herr Kollege Burkert.

Oskar Burkert (CDU): Ich habe mehrere Fragen. Wie eben schon gesagt, sind die Verfahren, wie man auf bestimmte Daten in den Krankenhäusern oder anderen Einrichtungen zugreift, kompliziert. Von einigen wurde gesagt – so habe ich diese verstanden –, dass es sehr einfache Methoden gibt, einzugreifen. Herr Appel sagte, Nutzung von den privaten und dienstlichen Geräten sollte getrennt werden. Ich kenne ein großes deutsches Unternehmen, bei dem es strengstens verboten ist, eigene Laptops, Tablets oder I-Phones zu benutzen. Diese werden alle gestellt, um auszuschließen, dass jemand zum Beispiel einen USB-Stick mit entsprechenden Viren verwendet.

Sie, Herr Blum – an Sie ist diese Frage gerichtet –, haben in Ihrer Stellungnahme 16/3962 im letzten Absatz geschrieben: „Die Medizinhersteller sind gefordert.“ Verstehe ich es richtig, dass viele Geräte für die Narkose oder Beatmung mit separater Software ausgestattet sind, die nicht ins Krankenhaussystem eingebunden ist und nicht angegriffen werden kann, da – so schreiben Sie – die IT-Dienstleister nicht darauf zugreifen dürften; das dürfe nur der Hersteller? Also wäre es die Empfehlung – vielleicht haben Sie diese schon herausgegeben –, dass nur noch Geräte angeschafft werden, auf die kein Zugriff von außen erfolgen kann. Ist das richtig?

Gibt es Ihrerseits Überlegungen, den Krankenhäusern zu empfehlen, im Krankenhaus keine privaten Geräte zu nutzen, keine Daten aufzuspielen oder zu überspielen?

Vorsitzender Günter Garbrecht: Das werden wir klären, Herr Kollege. – Frau Kollegin Schneider.

Susanne Schneider (FDP): Vielen Dank, Herr Vorsitzender! – Ich habe zunächst zwei Fragen an Herrn Spyra. Wie schätzen Sie den aktuellen Umfang von veralteten Betriebssystemen – explizit von Windows XP – in den Krankenhäusern ein? Sie verweisen auf gezielte Angriffe auf Medizinprodukte in den USA; diese stehen im Gegensatz zu den ungezielten Angriffen in NRW. Können Sie Ihre Beispiel bitte etwas konkreter ausführen?

Dann habe ich noch eine Frage an Herrn Spyra, Herrn Blum, Herrn Dr. Walther und Herrn Appel, und zwar: Wie bewerten Sie das Risikomanagement und die Notfallpläne der Krankenhäuser, speziell der Krankenhäuser in Nordrhein-Westfalen? – Danke schön.

Vorsitzender Günter Garbrecht: Gibt es weitere Wortmeldungen von den Damen und Herren Abgeordneten? – Das ist nicht der Fall. Herr Spyra, wir beginnen mit Ihnen.

Gerald Spyra (Kanzlei Spyra): Sehr gerne. – Ich arbeite die Fragen ab. Wir reden hier von einer ubiquitären Vernetzung, wenn ich das so sagen darf. Ich habe auf einer Veranstaltung gesagt: Wenn alles miteinander vernetzt werden soll – das ist auch die Idee von Industrie 4.0 –, dann können wir nicht mehr von einzelnen Bereichen sprechen. In Amerika gibt es prominente Hacks. Zum Beispiel wurde bei Target ein Lieferant für Kühlsysteme angegriffen; dieser hatte Zugriff auf das Supermarktsystem, sodass sich die Angreifer bis zu den Point of Sales vorarbeiten konnten. Das heißt, wir müssen dieser ubiquitären Vernetzung ausreichend Rechnung tragen. Wir müssen eigentlich alles sicher machen. Es reicht nur ein Angriffspunkt, und wir alle sind verwundbar. Dieses Problem haben wir meiner Ansicht nach auch heutzutage mit den KV-SafeNets; unsere Patientendaten, unsere Gesundheitsakte, all das wird da gespeichert. Wir haben eben gehört, dass die Systeme unsicher seien. Wenn aber nur ein System gehackt wird, kann man auf dieses System aufgrund dieser bisher unbekannten Lücke, die noch nicht veröffentlicht wurde, zugreifen. Dieses Problem schaffen wir uns im Endeffekt mit dieser ubiquitären Vernetzung.

Daher ist es meiner Ansicht nach ein bisschen zu kurzgesprungen, wenn nur 20 oder 50 von fast 400 Krankenhäusern in Nordrhein-Westfalen zur sicheren Infrastruktur erklärt werden; die Krankenhäuser tauschen sich – auch über Forschungseinrichtungen – deutschlandweit, in ganz Europa, weltweit aus. Dieses Problem haben wir heutzutage.

Wie realistisch ist das Verbot privater Geräte im Krankenhaus? Es ist unrealistisch. Krankenhäuser wissen um ihre Stellung. Sie müssen ihren Mitarbeitern etwas geben, und wenn es nur das Gefühl ist, sich wie zu Hause zu fühlen und Facebook nutzen zu dürfen. Das hat zur Konsequenz, dass Fotos von Patienten gemacht und über WhatsApp geteilt werden. Das ist die Realität. Das müssen wir auch adressieren. Deswegen sollte ein Krankenhaus private Geräte verbieten; das sollte auch in die Betriebsvereinbarung aufgenommen werden, allein aufgrund von möglichen Haftungsfällen. Das ist die Problematik; Mitarbeiter bringen ihre privaten Geräte mit. Damit einher geht ein Rattenschwanz an Haftungsproblematiken, die ich in dieser Zeit gar nicht aufzählen kann. Deswegen wäre es am besten, die Geräte zu verbieten – aber hinter verschlossenen Türen wird es gestattet, damit die Leute nicht nur für die Arbeit da sind, sondern ihr Privates mitnehmen können.

Zu öffentlich auditierbaren Softwaregeräten: Meiner Ansicht nach ist das essenziell, wenn von diesen Geräten unsere Gesundheit abhängt. Deswegen müsste alles von öffentlichen Forschungseinrichtungen usw. auditiert werden.

Verschlüsselung bedeutet nicht gleich Verschlüsselung. Verschlüsselte Daten sind sicher; aber wenn die Verschlüsselung nicht vernünftig implementiert wird, nutzt die beste Verschlüsselung nichts. Das heißt, es muss auditiert werden können, wie es gemacht ist. Einige Konzerne aus Amerika vertreten die Wild-Garden-Philosophie, dass wir diesen Geräten vertrauen müssen. Aber seien wir ehrlich: Wir vertrauen diesen Geräten unsere intimsten Daten an. Ihrem besten Freund würden Sie diese Daten nicht einmal anvertrauen, vertrauen sie aber Apple an. Das ist ein Riesenproblem, dass wir in der heutigen Zeit haben.

Wie viel Sicherheit haben wir, dass im Krankenhaus in Neuss keine Daten abgeflossen sind? Meiner Ansicht nach haben wir dafür gar keine Sicherheit. Wir wissen nicht, was beim Angriff mitgekommen ist. Wahrscheinlich sind nicht alle Systeme neu aufgesetzt worden. Daher wissen wir nicht, ob sich darauf – ich will mich vorsichtig ausdrücken – etwas manifestiert hat. Das heißt, möglicherweise können Daten abfließen. Aufgrund der Intransparenz finden wir dafür keinen Beleg.

Ich habe es angesprochen: Es gibt unterschiedliche Protokollstandards. Weil es keinen einheitlichen Standard gibt, ist es nicht möglich, sich anzuschauen, welche Daten herausgekommen sind. Wir wissen es nicht. Das heißt, wir müssen Vertrauen. Und es gibt eine absolute Intransparenz. Sie wissen selbst, wie toll es ist, einem intransparenten System zu vertrauen.

Wie sieht es mit einem gezielten Angriff aus? Meiner Ansicht nach sieht es dann schlecht aus. Ich habe den Penetrationstest nicht umsonst genannt. Wenn ein Angreifer es wirklich auf eine Institution abgesehen hat… In Amerika ist es leider schon vorgekommen, dass jemand mit Kenntnissen von Medizinproduktesoftware diese Produkte angegriffen und das ganze Krankenhaus lahmgelegt hat. Ich will keine Angst machen. Ich verweise aber auf den Fall, dass die Firmenware, die eine Infusionspumpe steuerte, gehackt werden konnte. Damit hätten die Werte verändert werden können, also eine andere Insulinmenge gespritzt werden können. Das wäre praktisch der perfekte digitale Mord. Leider ist das Realität. Theoretisch können Sie das dann so darstellen, dass die Krankenschwester nicht sieht, was geschieht. Das ist kein Horrorszenario. Das ist die Realität. Davor darf man die Augen nicht verschließen.

Ich habe ein paar Beispiele aus den USA genannt. Diese sind in Deutschland leider nicht publik geworden. Aber ich würde mir wünschen, dass einige dieser Angriffe in den USA in Deutschland publik würden.

Ein Beispiel des Community Health Systems: Ich weiß nicht, ob Sie sich an die Lücke Heartbleed erinnern? Das war eine Lücke in einer Verschlüsselung. Aufgrund dieser Lücke – man mutmaßt, es waren chinesische Hacker –, wurden im Community Health System 4,5 Millionen Patientendaten abgegriffen. Bei einer Versicherung im Bereich Gesundheit sind 81 Millionen Daten abgegriffen worden. Daten – das müssen wir uns vor Augen führen – sind Gold wert. Auf dem Schwarzmarkt werden Datensätze für jeweils etwa 500 US-Dollar gehandelt. Rechnen Sie 4,5 Millionen Datensätze mal 500 US-Dollar. Damit kann ein hübsches Sümmchen verdient werden. Daher ist das, glaube ich, nicht ohne Probleme.

Zum Risikomanagement in den Krankenhäusern: Im Endeffekt – ich habe versucht, das in meiner Stellungnahme 16/3961 anzudeuten – gibt es Insellösungen. Es gibt keinen ganzheitlichen Ansatz. Weil die Prozesse so komplex sind, haben wir eigentlich keine Möglichkeit, Transparenz zu schaffen. Die Mitarbeiter werden von den Leitungen oftmals nicht ermächtigt, sich alle Prozesse anzuschauen. Das ist auch eine organisatorische Sache.

Damit komme ich auf das Problem der externen Dienstleister zu sprechen. Externe Dienstleister dürfen eigentlich nicht auf Patientendaten zugreifen, weil das möglicherweise eine Verletzung des Patientengeheimnisses ist. Das ist ein Riesenproblem. Sie sehen Anspruch und Wirklichkeit: Die Ärzte müssen ihre Daten, die das Vertrauensverhältnis zwischen Arzt und Patient betreffen, eigentlich für sich behalten. Aber sie können das nicht, weil sie die entsprechende IT einsetzen und letztlich immer welche darauf zugreifen. Gerade die Hersteller von Medizinprodukten brauchen diesen Zugriff. Wenn selbst die Hersteller über das Internet Zugriff darauf haben, können Sie sich vorstellen, wer noch Zugriff darauf haben könnte. – Damit bin ich am Ende. Vielen Dank.

Vorsitzender Günter Garbrecht: Herr Dr. Walther.

Dr. Stefan Walther (Chief Information Officer): Danke. – Ich werde versuchen, die Fragen zusammenzufassen, damit ich mich einigermaßen kurzfassen kann.

In Bezug auf das Thema „Private Daten“: Grundsätzlich halte ich es nicht für möglich, private Daten zu verbieten – wenn ein IT-Leiter seinen Job behalten möchte. Das lässt sich an vielen Stellen politisch nicht durchsetzen. Es gibt Gegenmaßnahmen; darauf komme ich gleich zu sprechen. Wenn man private Daten verbietet – in vielen Unternehmen wird das gemacht; an manchen Stellen wäre das auch wünschenswert –, würde ein ganzer Teil der Infrastruktur genommen. „IT“ ist für die Nutzer ein hoch emotionales Thema; das sollte man nicht vergessen. Die private und die Arbeitswelt werden mehr oder minder ununterbrochen vermischt. Das kann ich nicht mehr trennen. Vonseiten der IT wäre es wünschenswert, dass die dienstlichen Daten in einem eigenen Container gespeichert würden; diese Technik gibt es. Sie kostet aber schlicht und ergreifend Geld, Zeit und Ressourcen. Damit können auf einem normalen Handy oder Laptop die dienstlichen Daten in einem Container belassen werden; damit sind sie in sich geschützt und können extern vernichtet werden, wenn ich es will. Damit wird dem Nutzer die Möglichkeit eröffnet, beides zusammenzuführen und trotzdem ein hohes Maß an Sicherheit gewährleistet.

Überhaupt würde vieles in dieser Diskussion einfacher, wenn wir die bestehenden Techniken anwenden würden. Wir haben dafür im Tagesgeschäft aber weder die Zeit noch die Ressourcen. Die Technik ist vorhanden, aber wir können sie nicht anwenden.

Das betrifft zum Beispiel auch die Frage von Herrn Sommer nach auditierbarer Software. Auditierbare Software wäre wünschenswert. Aber von allen Herstellern, von den großen und den kleinen, werde ich das nicht erhalten.

In einem normalen Krankenhaus wäre das sogenannte Wide Listing bereits ein guter Weg, also nur die Ausführung der Programme zu erlauben, die bekannt sind. Damit besagt nicht der Scann, welche Programme böse sind; vielmehr dürfen nur die Programme zugreifen, die gut sind; und das wird vorher überprüft. Das ist seit sieben Jahren in professioneller Version vorhanden. Das ist sehr teuer; das ist sehr aufwendig. Es wird aus diesen Gründen nicht gemacht.

Ein Punkt, den ich mir von dieser Anhörung erhoffe, ist, dass der Landtag und die Krankenhausgesellschaft den Krankenhäusern empfehlen, hierdrauf eine stärkere Priorität zu setzen und auf die Gefahren hinzuweisen. Nicht nur monetäre Aspekte spielen an dieser Stelle eine Rolle.

In Bezug darauf, ob Daten des Krankenhauses in Neuss abgeflossen sind: Es gibt schlicht und einfach keine Garantie. Ein Root ist ein Root, ein Admin ist ein Admin. Wenn ein Angreifer Zugriff hat, gehört das System ihm und der Nutzer eigentlich auch. Damit besteht de facto die vollständige Kontrolle. Bei zeitverzögerten Algorithmen kann man sich auch hinterher jeder Zeit wieder einklinken. Ist ein Angreifer einmal im System, kann er immer rein. Das heißt, wenn ein System einmal befallen ist, war’s das.

Bezüglich der Maßnahme, 20 Krankenhäuser zur kritischen Infrastruktur zu erklären: Als kurzfristige Lösung kann ich mir vorstellen, bestimmte Krankenhäuser mehr zu fördern – dass sie ein größeres Stück des Kuchens bekommen –, um ihnen die Möglichkeit zu geben, die bestehende Technik einzuführen, bestimmte Technologien zu verwenden und aufzusetzen. Damit kann noch eine Notversorgung aufrechterhalten werden. Das wäre aus meiner Sicht eine sinnvolle Idee. Das wäre auch etwas, was die Community vollständig mittragen würde.

Es ist keine Dauerlösung. Irgendwann besteht ein Durchsatzproblem. Die elektiven Eingriffe können eine Zeitlang verschoben werden; aber nach einem gewissen Punkt ist Schluss. Aber für die Notfallversorgung wäre die Idee aus meiner Sicht sinnvoll.

Zur Frage nach einem gezielten und einem nicht gezielten Angriff: Mit einem gezielten Angriff, denke ich, kann ein System angegriffen werden. Diese haben einen Vorteil für den Angreifer: Man sieht sie nicht. Bei einem gezielten Angriff ist der Angreifer für den Admin nicht erkennbar, außer, der Administrator ist wirklich sehr gut. Bei einem gezielten Angriff können die Spuren so weit verschleiert werden, dass dieser – davon müssen wir ausgehen, die ITs stehen hoch unter Druck – nicht auffällt.

Ich denke, dass die Trennung der Daten und Verwendung von Containern dazu führt, dass der gezielte Angriff nicht alle Bereiche durchdringt, sondern nur einen Container. Diese Lösung wäre zu propagieren. Das ist aber mit Sicherheit auch ein finanzielles, personelles Problem; die Firmen, die das anbieten, sind hoch spezialisiert.

Zum Thema „Risikomanagement“: Innerhalb der Krankenhäuser in Nordrhein-Westfalen gibt es aus meiner Sicht zu wenig Kommunikation über das Risikomanagement. Ich hätte an Herrn Fischer – er hat sich als Moderator sehr bewährt – die Bitte, das Thema zusammenzuführen, damit es eine Art grundlegendes Risikomanagementhandbuch gibt. Vorzustellen wäre es ähnlich einer Kladde. Bei bestimmten Verträgen

muss man Optionen ankreuzen, um zu wissen, dass man sich rechtlich in einem sicheren Raum bewegt, zum Beispiel bei EVB-IT-Verträgen. Ein Risikomanagementhandbuch zu arbeiten würde sich durchaus lohnen. Ich glaube, da könnte man wirklich mehr tun. Denn die Kommunikation zwischen den einzelnen Krankenhäusern ist diesbezüglich schlecht. Überall gibt es Fragmente, die mehr oder weniger gut ausgearbeitet sind. – Ich glaube, das waren die Fragen an mich. Danke schön.

Vorsitzender Günter Garbrecht: Herzlichen Dank. – Herr Röhrl, wollen Sie antworten?

Markus Röhrl (Cybercrime-Kompetenzzentrum, Landeskriminalamt NRW): Das kann ich gerne tun. – In der Tat gibt es keine 100%ige Sicherheit, dass nicht auch andere Daten abgefischt worden sind. Man muss allerdings sagen: Das Problem besteht derzeit bei jedem Krankenhaus.

Unsere Netzwerkforensiker, die des BSI und von G Data haben, glaube ich, keine Hinweise gefunden, dass auf andere Daten zugegriffen worden ist, dass Patientendaten abgefischt worden sind oder dass weitere Daten abgesendet wurden.

Wir haben sehr viel über Angriffe von außen geredet; das ist sicherlich eine ganz wichtige Geschichte. Wir haben festgestellt: Wir können uns nur bis zu einer bestimmten Ebene schützen. Ein gezielter Angriff auf einen Fernwartungszugriff, auf einen offenen Port kann tatsächlich dazu führen, dass gewisse Bereiche kontaminiert werden. Lösungen sind eben von Herrn Dr. Walther und Herrn Dr. Häger – er sprach die Segmentierung an – dargestellt worden. Zu 100 % werden wir diese Zugriffe aber nicht verhindern können.

Für solche Angriffe müssen Sie heutzutage kein Profi sein. Sie können sich einen Angriff im Internet konzipieren lassen – in der Underground Economy, meisten im Tornetz –, sodass wir an die Anbieter und Käufer solcher Software nicht herankommen. Sie können sich solche Software bestellen. Sie können auch dritte Personen instruieren, einen bestimmten Bereich anzugreifen, nach bestimmten Schwachstellen zu suchen. Das alles ist heutzutage kein Problem mehr. Das machen auch keine Script-Kiddies, sondern professionelle oder zumindest gewerbliche Täter.

Ich möchte den Blick noch einmal auf die Täter werfen. Sie werden das nie verhindern können. Bei großen Unternehmen in Nordrhein-Westfalen – nicht in der kritischen Infrastruktur – haben sich Mitarbeiter mit Administratorenrechten beispielsweise aufgrund der Unzufriedenheit mit dem Arbeitgeber – sie sind zum Beispiel nicht befördert worden oder sind nicht besser bezahlt worden – auf kriminelle Weise Daten – Kreditkartendaten usw. – von Kunden verschafft mit dem Ziel, diese weiter zu veräußern. Dazu ist eben auch etwas von Herrn Spyra gesagt worden.

Innentäter – also jemand aus dem Unternehmen; in der Politik ist das ein Spion – können Sie technisch nie ausschließen. Das Risiko, das von ihnen ausgeht, ist mindestens, glaube ich, genauso groß beziehungsweise quantitativ vielleicht noch viel größer als das technische Risiko, von außen gezielt angegriffen zu werden.

Zum Risikomanagement in Krankenhäusern: Ich habe vorhin gesagt, dass das, was für Krankenhäuser gilt, auch für alle anderen wichtigen Unternehmen und Behörden gilt. Man muss eine Notfallstrategie haben. Man muss wissen, was man machen muss, wenn so ein Fall eingetreten ist.

Im Krankenhaus in Neuss hat man sehr gut reagiert. Man hat die Ausführung des Trojaners sehr schnell erkannt und sehr schnell alle Systeme heruntergefahren. Das war sicherlich ein erster richtiger und wichtiger Schritt. Aber bei vielen Unternehmen – vielleicht auch Krankenhäusern – ist das nicht geklärt: „Wer darf die Anweisung geben, die Systeme herunterzufahren?“ Vielleicht ist die Geschäftsleitung dafür zuständig, vielleicht aber auch nicht; vielleicht hat man sich bis heute gar keine Gedanken darüber gemacht. Vielleicht erreichen Sie die zuständige Person in einem solchen Fall nicht.

Ich denke, dass sind ganz wesentliche Dinge, an denen man Arbeiten kann, nicht nur in den Krankenhäusern, sondern hinsichtlich aller kritischer Infrastrukturen und in allen großen Unternehmen und Behörden.

Vorsitzender Günter Garbrecht: Herzlichen Dank. – Herr Appel.

Roland Appel (Bornheim): Zunächst zu den Ausführungen des Herrn Abgeordneten Sommer: Sie haben mich als Best Buddy der Gesundheitsministerin bezeichnet. Ich bin stolz darauf, dass mich die CDU als Sachverständigen benannt hat. Im Übrigen zeigt mir das, dass Sie meine Stellungnahme nicht gelesen haben. Wenn Sie diese gelesen hätten, wüssten Sie, dass ich unterm Strich 600 Millionen € für ein Sonderprogramm fordere. Ich glaube nicht, dass das Frau Steffens gefällt. Ich glaube, wir sollten in der Sache ein bisschen auf dem Teppich bleiben.

Ich meine nicht – das unterscheidet mich von meinen Vorrednern –, dass nicht nur die 20 Krankenhäuser, die zur kritischen Infrastruktur erklärt werden sollen, ein Datenschutzmanagementsystem einführen sollten. Dies einzuführen kostet 100.000 €; für alle Krankenhäuser macht das 36 Millionen €. Schulungen kosten etwa 200 € pro Beschäftigtem; bei etwa 247.000 Beschäftigten in den Krankenhäusern sind das etwa 50 Millionen €. Insgesamt kostet es damit 86 Millionen €. Dann kommt noch die Hardware hinzu. Wir bewegen uns da in einem ziemlich offenen Feld. Die Angaben sind alles Schätzungen. Die Anschaffungen können 300 Millionen € kosten, aber auch 500 Millionen €. Die Ausgaben kann man auch über Jahre strecken. In den Krankenhäusern gibt es Innovationsbedarf. Die angesprochenen Windows-XP-Systeme werden auch noch verwendet.

Diese Ausgaben für Managementsysteme und Weiterbildungen sind – bezogen auf den Landeshaushalt – relativ kleines Geld. Hier ist mit wenig Geld viel Sicherheit zu schaffen. Ich finde, das sollte angegangen werden.

Herr Abgeordneter Burkert hat die Frage nach den Regeln angesprochen. Meinen beiden Vorrednern Herr Spyra und Herrn Dr. Walther möchte ich hier wiedersprechen. Ich hatte mit zwei Unternehmen – das eine ist ein öffentliches Unternehmen mit 160.000 IT-Arbeitsplätzen und das andere ist ein Privatunternehmen in Stuttgart mit

weltweit 270.000 Computerarbeitsplätzen – zu tun, die das im Griff haben. Die Beschäftigten dürfen keine privaten USB-Sticks verwenden. Die Tablet-Computer von Daimler haben eine dienstliche Partition, die sich bei Diebstahl automatisch zerstört. Sie dürfen auf den Tablets auch privat arbeiten, aber auf einer anderen Partition. Das alles geht.

Ich würde nie sagen: „Ich kann den Menschen nicht verbieten, Facebook oder WhatsApp zu verwenden.“ WhatsApp ist ja eine Datenschleuse ohne Ende. Ich würde das nie benutzen und auch nicht im Krankenhaus zulassen. Zur Verwendung sozialer Netzwerke kann man strenge Regeln erlassen; die müssen eingehalten werden. Anders können Sie Computersysteme überhaupt nicht beherrschbar machen.

Bring-Your-Own-Device geht gar nicht. In Einzelfällen geht das, aber dann bedarf es noch strengerer Regeln. Es muss dann vorgegeben werden, welcher Gerätetyp und welche Software verwendet werden dürfen; das muss normiert werden und kontrolliert werden. Sonst bekommt man das alles nicht in den Griff.

Man kann nicht blauäugig sagen: „Die nutzen das alle. Sonst kommen Sie gar nicht mehr und spielen nicht mehr.“ Übrigens sollen die Beschäftigten während der Arbeitszeit auch nicht auf Facebook sein. Da muss ich sehr vehement widersprechen. Aber ich muss auch sagen: Das alles ist beherrschbar. Die Regeln müssen natürlich gebildet und eingehalten werden. Es muss konsequent sein.

Deswegen noch einmal das Plädoyer: IT-Sicherheit und Datenschutz sind Chefsache.

Frau Abgeordnete Schneider, zum Risikomanagement in den Krankenhäusern in Nordrhein-Westfalen kann man da generell nicht so sagen. Im Vorfeld zu dieser Anhörung habe ich ein paar Telefonate geführt – völlig eklektisch ausgewählt. Einige Krankenhäuser sind richtig fit und durch die Vorfälle in Neuss richtig aufmerksam darauf geworden. Das hat zu Diskussionen bis hoch in den Vorstand geführt. Aber es gab auch andere, die sagen: „Naja, wenn wir ehrlich sind und anonym nachfragen: Wir haben nicht jeden Tag ein Back-up.“ Das ist natürlich tödlich. Aber das ist die Spannbreite; das ist die Realität. Damit muss man umgehen.

Managementsysteme sind eine Methode. Allerdings – da pflichte ich allen anderen bei –: 100%ige Sicherheit gibt es nicht.

Ich möchte auch bitten, zu unterscheiden: Es gibt keine privaten Daten; es gibt nur personenbezogene Daten. Diese sind durch das Datenschutzgesetz, die Datenschutzgrundverordnung oder durch das Patientengeheimnis geschützt. Daneben gibt es die private Computernutzung. Das ist aber etwas anders.

Natürlich können Sie Administratoren und externe Unternehmen beschäftigen, die sich per Unterschrift auf das Daten- und Patientengeheimnis verpflichten und im Zweifelsfall in den Knast gehen. Das muss ich, wenn ich bei Unternehmen bin, auch unterschreiben. Dass das nicht möglich ist, ist eine etwas abenteuerliche Aussage.

Insofern bin ich eigentlich optimistisch, dass wir die Situation in den Krankenhäusern – wenn die notwendigen Schritte dafür getan werden – im Griff behalten. Zukunftsfähig – das betone ich noch einmal – gelingt das nur, wenn man die Lücke schließt und Geld

für wirklich diese Zwecke in die Hand nimmt. Da sehe ich Handlungsbedarf. – Danke schön.

Vorsitzender Günter Garbrecht: Herzlichen Dank. – Jetzt bitte ich Herrn Dr. Häger ums Wort. Herr Blum macht den Abschluss.

Dr. Dirk Häger (Bundesamt für Sicherheit in der Informationstechnik, Referat Kritische Infrastruktur): Ich versuche, ein paar Sachen wegzulassen, die schon gesagt wurden.

Warum sollen nur 20 Krankenhäuser herausgepickt und zur kritischen Infrastruktur erklärt werden? Das IT-Sicherheitsgesetz hat die Intention, den Markt zu schaffen. Irgendwelche kritischen Infrastrukturen haben immer wieder behauptet: „Wir würden gern diese Produkte kaufen; aber es gibt dafür keine Anbieter.“ Die Anbieter sagen: „Wir würden unsere Produkte gerne verkaufen; aber es gibt keine Kunden.“ Wenn es uns gelingt, dass ein paar hundert Krankenhäuser bundesweit die IT-Sicherheit implementieren und damit einen Standard setzen – die Krankenhäuser müssen natürlich auf die Hersteller zugehen –, hat das – so hoffen wir stark – Ausstrahlungseffekte auf alle anderen Krankenhäuser. Deswegen sind wir durchaus der Meinung, dass wir uns auf die großen Krankenhäuser beschränken sollten, da ein paar Jahre später die kleinen Krankenhäuser das automatisch auch anwenden.

Zur privaten IT, zum Datenschutz: Ich wollte nicht sagen, dass verboten werden soll, ein Handy mitzuführen; ich würde verbieten, dass private IT an berufliche IT angeschlossen wird. Mit Bring-Your-Own-Device ist ja eine Kopplung gemeint. Dass in manchen Bereichen in den Krankenhäusern auch kein Handy mitgeführt werden darf, ist eine Selbstverständlichkeit. Das jedenfalls steckte hinter meinen Ausführungen.

Sie hatten nach der Segmentierung gefragt, Herr Sommer. Segmentierung bedeutet für mich kein totales Abschalten der Systeme, sondern ein kontrollierter Übergang. Wenn ein Gerät eine Internetverbindung zum Hersteller aufbauen muss, dann muss das gescheit abgesichert sein, sodass nur diese Verbindung erlaubt wird. Idealerweise wird dies über einen Kryptotunnel sichergestellt. Wenn ein Hersteller ein Update im Klartext übers Internet bereitstellt, würde ich mir einen anderen Hersteller suchen. Man kann das absichern. Also: kein freier Zugang zum Internet.

Ich glaube, ich bin jetzt bei der Frage zum Angriff auf den Bundestag; das ist hier sicherlich nicht das Thema. Herr Sommer, wo auch immer Sie das gelesen haben, wenn Sie einen Link haben, schicken Sie ihn mir zu. Ich bin mir sehr sicher, dass kein gewöhnlicher CT-Leser den Bundestag erfolgreich angegriffen hat. Dahinter steckte etwas mehr als das Abschreiben einer Anleitung.

Dann würde ich noch gern auf eine Frage antworten, die mir gar nicht gestellt wurde. Mir ist kein Fall bekannt, in dem ein US-Krankenhaus erfolgreich angegriffen wurde und es entsprechende Effekte auf die Patienten gab. Wir suchen natürlich nach solchen Fällen. Die Beispiele von Herrn Spyra betreffen eher das Webhacking, das Datenbankhacking. Das betrifft nicht den reinen Krankenhausbetrieb. Die genannten Bereiche sind für das Krankenhaus natürlich auch wichtig; ich will das nicht kleinreden.

Bei Cybercrime reden wir davon, dass ein Angreifer Geld machen möchte. Ich kann mir natürlich einen Hollywoodfilm über das Manipulieren von Infusionspumpen vorstellen. Es gab einen ehemaligen US-Vizepräsident, der seinen ferngesteuerten Herzschrittmacher abgestellt hat, um so etwas zu vermeiden. Nichtsdestotrotz: Zumindest mir sind keine entsprechenden Fälle bekannt. Glauben Sie uns: Wir suchen danach. Wir hätten das gern für die Sensibilisierung. – Danke.

Vorsitzender Günter Garbrecht: Herzlichen Dank, Herr Dr. Häger. – Herr Blum, Sie sind jetzt dran. Sie müssen allerdings nicht die restlichen 16 Minuten bis zum Beginn der nächsten Sitzung in Anspruch nehmen; Sie können sich gern kürzer fassen.

Matthias Blum (Krankenhausgesellschaft Nordrhein-Westfalen e. V.): Herr Vorsitzender! Ich versuche, mich auf die Fragen zu beschränken, die mir gestellt worden sind. – Zunächst einmal gab es die Frage des Herrn Abgeordneten Sommer: Ist Geld im System? Ich meine, dass ich vorhin schon darauf geantwortet habe. Ich verweise dazu auf die Seiten 6 und 7 unserer Stellungahme 16/3962. Aus allen Beiträgen ist eigentlich hervorgegangen, dass die Investitionsmittel, die zur Verfügung gestellt werden, für die Herausforderungen im Hinblick auf die Digitalisierung nicht ausreichen. Ich warne aber davor, von den 317 Millionen € 150 Millionen € abzuziehen; dann wäre zwar ein Problem gelöst, aber es würden andere geschaffen. Ich glaube, dass ist nicht im Sinne der Patienten. Davor kann ich nur dringend warnen. Ich möchte das an dieser Stelle noch einmal ausdrücklich gesagt haben.

Herr Sommer fragte: „Ist es ausreichend, wenn 20 Krankenhäuser zur kritischen Infrastruktur erklärt werden?“ Ich möchte mich dazu den Ausführungen von Herrn Dr. Häger anschließen. Diese 20 bis 50 betreffenden Krankenhäuser müssen gegenüber der Behörde den Branchenstandard nachweisen. Wir gehen auch davon aus, dass die anderen Krankenhäuser, die nicht zur kritischen Infrastruktur erklärt werden, ebenfalls gut beraten sind, dies umzusetzen. In einem Haftungsfall würde der Richter ziemlich schnell sagen: „Den Branchenstandard habt ihr auch einzuhalten. Wie kann es sein, dass das an dieser Stelle nicht geschah?“ Wir haben keine Einzelberechnung vorgenommen, was das pro Krankenhaus kostet. Das ist enorm teuer; wir haben das heute gehört. Das ist ein hoch investiver Bereich. Nichtsdestotrotz wird den Krankenhäusern nicht anders übrig bleiben, als diesen Bereich zu bedienen.

Herr Burkert hat nach dem privaten und dienstlichen Datenzugriff gefragt. Ich kann mich letztlich dem anschließen, was schon dazu gesagt worden ist. Wir haben nur die Kenntnis, dass Krankenhäuser die private Nutzung in der Regel untersagen. Das heißt, die USB-Eingänge sind zu. CDs oder DVDs werden zentral eingelesen. Ich räume aber auch ein: Untersucht die IT in den 364 Krankenhäusern jedes Büro und ich weiß nicht wie viel tausende Arbeitsplätze? Sind die USB-Eingänge alle zu? Eine 100%ige Sicherheit können wir nicht zur Protokoll geben. Das wäre gelogen. Das werden wir an dieser Stelle auch nicht tun. Das ist aus unserer Sicht das, was die Krankenhäuser tun sollen.

Frau Schneider, zu Ihrer Frage nach Notfallkonzepten. Ich möchte die Veranstaltungen, die wir durchgeführt haben, nennen. Gibt es ein entsprechendes Umsetzungshandbuch? Wir hatten am 4. Oktober 2010 eine Fachtagung zum Thema „Risikomanagement in medizinischen IT-Netzwerken und Software als Medizinprodukt“. Am 27. Februar 2012 gab es die Fachtagung „Risikomanagement für IT-Netzwerke mit Medizinprodukten – Die Umsetzung der neuen DIN 800001-1:2011 im Krankenhaus“. Ich lese das vor, weil Herr Fischer, der neben mir sitzt, gemeinsam mit den Kollegen von der DKG ein Umsetzungshandbuch für die Krankenhäuser angefertigt hat. Vielen Dank für die Idee; wir haben schon eines.

Darüber hinaus haben wir am 13. Januar 2015 in Dortmund eine Tagung zum Thema „Praxisdialog Krankenhaus-IT und Medizintechnik“ durchgeführt mit den Schwerpunkten „KRITIS, Fokus: Gesundheitswesen, IT-Sicherheitsgesetz, BSI-Leitfaden, „Kritische Infrastrukturen“, Risikomanagement im Krankenhaus; Datenschutz im Krankenhaus: Orientierungshilfe Krankenhausinformationssysteme, Datenschutz in der Medizintechnik; Vernetzung im Krankenhaus: Mobile IT, Medizinische IT-Netzwerke, Vernetzte Medizintechnik“.

Last, not least, am 13. Januar gab es die Veranstaltung zum Thema „Praxisdialog Krankenhaus-Informationstechnik und -Medizintechnik 2016“, bei der wir auch darüber gesprochen haben.

Vorhin waren die Stichworte „Arzneimittelpumpen“ und „Narkoseautomaten“ gefallen; wir haben den Workshop „Alarmierung und (mobile) Vernetzung im Krankenhaus“ durchgeführt sowie das Fachforum „Sicher ist sicher: KRITIS, IT-Sicherheitsgesetz und Risikomanagement.“

Noch ein Wort zum Thema „Arzneimittelpumpen und Narkoseautomaten“: Diese sind natürlich in der Alarmierung eingebunden, aber sie sind nur mit dem Internet verbunden, wenn es nicht anders machbar ist; regelhaft sind sie über ein separiertes Netz angebunden. Im Prinzip hat ein Angreifer, der einmal ins System gekommen ist, nicht automatisch den Zugriff auf die Steuerung aller Geräte. Aber machen wir uns nichts vor: Wenn man das Handy der Kanzlerin der Bundesrepublik Deutschland knacken kann, kommt man auch in die genannten Systeme – im Zweifel auf einem Weg, den wir alle noch nicht kennen – rein. Das wird sich, glaube ich, nicht 100%ig ausschließen lassen.

Zum Thema „Notfallmanagement“: Wir haben dazu regelmäßig informiert, auch mittels zweier Rundschreiben in den ersten zwei Quartalen aufgrund der Vorfälle in den 28 Krankenhäusern; darüber haben wir bereits in der Sitzung am 9. März diskutiert.

Das Lukaskrankenhaus ist eines der wenigen, wenn nicht sogar das einzige Krankenhaus, das komplett auf IT umgestellt hat; daher waren sie mit Blick auf ihre Handlungsfähigkeit von den Vorfällen besonders betroffen. Andere Krankenhäuser sind dabei, umzustellen. Wir wissen von ein, zwei Krankenhäusern, dass sie Glück hatten, da sie die Bereiche, die angegriffen worden sind, noch nicht vernetzt hatten; daher konnten sie die andere Bereich weiterbetreiben und haben die Bereiche, die angegriffen worden sind, abgeschaltet. Informationen darüber, dass sich die Krankenhäuser bereits im Vorfeld aufgemacht haben, liegen uns nicht vor. Aber ich denke, dass die Vorfälle

– über diese haben wir vielfältig publiziert und eine Veranstaltung dazu durchgeführt – für das gesamte Thema noch einmal sensibilisiert haben. – Ich glaube, damit habe ich alle Fragen beantwortet, Herr Vorsitzender.

Vorsitzender Günter Garbrecht: Herzlichen Dank. – Meine Damen und Herren, das war ein informatives Gespräch. Wir treffen uns hier zur nächsten Sitzung in neun Minuten wieder. Die Sitzung ist geschlossen.

gez. Günter Garbrecht
Vorsitzender

Anlage

13.06.2016/15.06.2016

215

Stand: 1. Juni 2016

Anhörung
des Ausschusses für Arbeit, Gesundheit und Soziales
am Mittwoch, 1. Juni 2016, 13.30 Uhr, Raum E3 D01

Thema: **"Die IT-Infrastruktur in Nordrhein-Westfalen muss sicher sein - die Gesundheit der Patientinnen und Patienten darf nicht zum Spielball von Kriminellen im Netz werden!"**

Antrag der Fraktion der PIRATEN, Drucksache 16/11216

Tableau

eingeladen	**Redner/in** Weitere Teilnehmer/-innen	**Stellungnahme**
Gerald Spyra, LL.M. Kanzlei Spyra Wipperfürth	**Gerald Spyra**	**16/3961**
Dr. Stefan Walther Chief Information Officer (CIO) Düsseldorf	**Dr. Stefan Walther**	**16/3959**
Cybercrime-Kompetenzzentrum Landeskriminalamt NRW Düsseldorf	**Markus Röhrl**	
Krankenhausgesellschaft Nordrhein-Westfalen e. V. Jochen Brink Matthias Blum Düsseldorf	**Matthias Blum** Burkhard Fischer Lothar Kratz	**16/3962**
Bundesamt für Sicherheit in der Informationstechnik Referat Kritische Infrastruktur Bonn	**Dr. Dirk Häger** Daniel Mühlenberg	**16/3960**
Herrn Roland Appel Bornheim	**Roland Appel**	**16/3964**
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Frau Helga Block Düsseldorf	*keine Teilnahme*	**---**

* * *