Abgeordnetenhaus BERLIN

18. Wahlperiode

Plenar- und Ausschussdienst

Wortprotokoll

Öffentliche Sitzung

**Ausschuss für Kommunikations-
technologie und Datenschutz**

27. Sitzung
9. Dezember 2019

Beginn: 15.03 Uhr
Schluss: 17.45 Uhr
Vorsitz: Marc Vallendar (AfD)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung (neu)

Verfahrensregeln

Siehe Inhaltsprotokoll.

Punkt 2 (neu) der Tagesordnung

Aktuelle Viertelstunde

Siehe Inhaltsprotokoll.

Punkt 3 (neu) der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs — 0120
Datenschutzverstöße der Deutsche Wohnen SE — KTDat
(auf Antrag der Fraktionen der SPD, Die Linke und Bündnis 90/Die Grünen)

Siehe Inhaltsprotokoll.

Punkt 4 (neu) der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs 0123
Schlussfolgerungen des Senats aus dem Cyberangriff auf das Kammergericht KTDat
(auf Antrag der Fraktion der CDU)

Vorsitzender Marc Vallendar: Zu diesem Tagesordnungspunkt begrüße Herrn Dr. Bernd Pickel, Präsident des Kammergerichts, dem wir heute das Rederecht in unserem Ausschuss für TOP 4 einräumen. – Wird die Anfertigung eines Wortprotokolls gewünscht? – Das ist der Fall. – Möchte die CDU den Besprechungsbedarf begründen? – Herr Lenz – bitte!

Stephan Lenz (CDU): Ich kann mich da kurz halten. Als zuständiger Ausschuss wären wir gern auf dem aktuellen Stand in diesen Fragen. Wir hätten gern den Sachstand. Es ist natürlich auch interessant, wenn Sie etwas sagen können im Hinblick auf die Arbeitsfähigkeit des Kammergerichts. Für uns ist auch die Frage ganz entscheidend, wie es jetzt weitergehen soll; das wird Sie nicht überraschen. Aber wenn wir da einen kurzen Ausblick bekommen könnten, wäre das für uns sehr hilfreich. Und wir würden gern auch besser das zukünftige Zusammenspiel und die zukünftige Rolle des ITDZ verstehen können. – Das sind meine Hauptfragen, und weitere Fragen richte ich gern nach Ihrem Vortrag an Sie. – Vielen Dank!

Vorsitzender Marc Vallendar: Möchte der Senat eine einleitende Stellungnahme abgeben? – Frau Smentek!

Staatssekretärin Sabine Smentek (SenInnDS): Herr Vorsitzender! Meine Damen und Herren! Sehr gerne, weil sich die Fragestellung zwar auf das Kammergericht bezog, aber ausdrücklich gefragt worden ist, welche Schlussfolgerungen der Senat aus dem Cyberangriff auf das Kammergericht zieht. Das ist eine Ebene darüber, weil wir beim Kammergericht durchaus einen Vorfall haben, aus dem alle Beteiligten etwas lernen, und zwar nicht nur für das Kammergericht.

Deswegen möchte ich gerne einleiten und Ihnen drei Zahlen nennen. Wir haben uns heute schon kurz bei einem anderen Tagesordnungspunkt über die Dynamik von Cyberkriminalität ausgetauscht. Im Jahr 2018 hat das ITDZ Berlin rund 31 Millionen Spam-Mails erfolgreich geblockt. Das ist die erste Zahl. Die zweite Zahl ist die, dass es daneben direkte Versuche gab, sich über die Online-Dienstleistungen der Berliner Verwaltung Zugang zur IT-Infrastruktur der Landesverwaltung zu verschaffen. Hier gibt es alleine 7 Millionen versuchter Angriffe im letzten Jahr. Das heißt, wir reden hier nicht über Peanuts, sondern über eine Bedrohungslage, die sich dynamisiert und die beim Kammergericht nun Folgen gehabt hat. Wir sind froh, dass wir mit dem ITDZ einen Dienstleister haben, der offensichtlich diese Angriffe erfolgreich blockieren kann, weil wir Auswirkungen wie im Kammergericht glücklicherweise nicht in jeder Verwaltung haben.

Aber wir haben tatsächlich eine stark steigende Bedrohungslage, und natürlich haben wir uns nicht nur wegen dem, was beim Kammergericht passiert ist, wegen der vielen Auswirkungen, die das konkret auf die Verwaltung hatte, gemeinsam mit dem ITDZ regelmäßig ausgetauscht – wir tun das nach wie vor –, wie wir dieser Angriffsszenarien und der Dynamik besser Herr werden können. Es ist so, dass wir eine Struktur zum Umgang mit der IT-Sicherheit haben,

wo das ITDZ eine ganz wesentliche Rolle spielt – auch mit dem CERT –, wo die Informationen über Angriffe zusammenlaufen und dann weiterverteilt werden, auch im direkten Austausch mit dem BSI. Interessanterweise kennen wir mittlerweile alle die Abkürzung, was BSI ist; das war vielleicht vor einem Jahr auch noch nicht so der Fall.

Diese Strukturen werden regelmäßig optimiert. Das heißt, es gibt systemimmanent einen direkten Austausch, wie man auf Bedrohungslagen sowohl technisch wie organisatorisch wie personell aktuell immer besser reagieren kann. Das heißt, es gibt eine regelmäßige Prüfführung auch der Regelungen für die Berliner Verwaltung, die regelmäßig aufgrund der aktuellen Bedrohungssituation weiterentwickelt werden. Und es gibt so etwas wie einen kontinuierlichen Verbesserungsprozess, der systemimmanent ist, zwischen allen Beteiligten.

Die Schlussfolgerungen werden dann in die Regelungen zur IT-Sicherheit aufgenommen, und es gibt auch regelmäßige Zusammenkünfte mit den IT-Sicherheitsbeauftragten der Verwaltungen. Aufgrund der Vorfälle, die wir hier leider zu beklagen haben, insbesondere auch beim Kammergericht, kann man sagen, dass das Interesse an solchen Austauschveranstaltungen durchaus zunimmt. Also die Bedrohungslage wird tatsächlich bei vielen mittlerweile als Auftrag angenommen, sich um die Datensicherheit des Landes Berlin zentral und dezentral zu kümmern.

Man muss eins sagen: Die technologische Herausforderung, vor der das ITDZ steht, ist nur ein Teil der Veranstaltung. Wir haben vor allen Dingen aufgrund der vielen E-Mails mit Filtern, wo wir versuchen, die Datensicherheit herzustellen, auch Angriffsversuche, wo gezielt Nutzerinnen und Nutzer mit Links zu Schadsoftware angesprochen werden. Wir merken in der Senatsverwaltung für Inneres – da kenne ich das als Amtschefin noch mal ein bisschen besser – auch, dass das Bewusstsein der Beschäftigten zunimmt, weil in unserer IT-Verbindungsstelle in der Senatsverwaltung für Inneres immer mehr merkwürdige E-Mails ankommen, die ganz normale Beschäftigte zur Prüfung weiterleiten. Genau so muss es sein. Alle Beschäftigten müssen das Thema IT-Sicherheit als ihren eigenen Auftrag wahrnehmen und dürfen nicht einfach nur der Technik vertrauen und auf jeden Link klicken, der da kommt. Da merken wir, dass sich das Bewusstsein ändert.

Was wir aber auch merken, ist, dass wir angesichts der Bedrohungssituation vor der Herausforderung stehen, bestimmte Dinge einfach zu verbieten. Wir haben z. B. hier davon gesprochen, dass wir im Augenblick wegen der Vorfälle im Bereich der Bildungsverwaltung nicht mehr Zip-Datei-Anhänge in E-Mails akzeptieren. Desgleichen haben wir, was die komfortable Nutzung von E-Mails für den Nutzer ein bisschen einschränkt, gesagt: Toll gestaltete und illustrierte HTML-Nachrichten werden nur noch als Textnachrichten dargestellt! – Das macht für die Nutzerin und den Nutzer in jeder Berlin Verwaltung erst mal keinen Spaß, weil sie mit einer Funktionseinschränkung leben müssen. Wir müssen dies aber tun, weil wir ansonsten, wenn wir diese Regelungen nicht verschärfen würden, der Cyberkriminalität Tür und Tor öffnen würden.

Von daher haben wir bei jedem dieser Vorfälle immer wieder die Frage: Müssen wir jetzt die Funktionalität weiter einschränken? Oder können wir Funktionalitäten weiter nutzen, wenn wir andere technologische Standards finden, um zentral bestimmte Angriffe abzublocken? – Das ist nicht mit einer Verordnung geklärt, sondern eine ständige Aufgabe sowohl des IT-Sicherheitsbeauftragten bei mir in der Verwaltung gemeinsam mit dem CERT, dem ITDZ wie

auch allen dezentralen IT-Sicherheitsverantwortlichen. Die Zusammenarbeit läuft immer besser, sodass ich zuversichtlich bin, dass unsere Regelungen, die wir, wie ich gerade ausgeführt habe, ständig verbessern, auch weiterhin wirksam dazu beitragen werden, dass wir das Thema IT-Sicherheit in der Berliner Verwaltung hoffentlich nicht mit so vielen Auswirkungen haben, wie es leider im Kammergericht passiert ist. Es bleibt eine ständige Herausforderung, und es kann morgen etwas passieren, womit wir heute alle nicht gerechnet haben, weil es keinen hundertprozentigen Schutz vor Cyberkriminalität geben wird.

Vorsitzender Marc Vallendar: Dann beginnen wir nun mit der Stellungnahme von Herrn Dr. Pickel, mit einer Redezeit von maximal fünf Minuten. – Bitte, Sie haben das Wort!

Dr. Bernd Pickel (Präsident des Kammergerichts Berlin): Frau Smentek hat es schon vorweggenommen: Wir haben eine erhöhte Bedrohungslage, und wir haben es, glaube ich, nicht nur mit mehr Angriffen, sondern mit Angriffen einer neuen Qualität zu tun. Dennoch möchte ich sagen: Das Eindringen des Trojaners in unser EDV-System – obwohl unser Anti-Viren-Hersteller in der Expertise dann gesagt hat: Wir haben das System ordnungsgemäß betrieben und aufgestellt. Wir hatten Firewalls. Wir haben auch in einem Umfang, den man sicher noch hätte erweitern können, Awareness-Schulungen bei den Mitarbeitern gemacht – war, ich möchte jetzt nicht sagen, wie ein Blitzschlag auf der Straße, dennoch war das, was uns passiert ist, schicksalshaft. Wir hatten einfach, und das muss ich im Nachhinein bekennen, vielleicht sogar weniger, um den Angriff als solchen und das Eindringen eines Trojaners zu verhindern – – Frau Smentek, Sie haben ja gesagt, dass es hundertprozentigen Schutz nicht gibt. Aber wir haben eben ganz massive Folgen gehabt oder haben sie immer noch bis heute.

Als eine kleine Vorrede auf Ihre Frage, wie der Stand ist: Wir haben bis heute immer noch die Situation, dass nicht nur nicht jeder Mitarbeiter einen Einzelplatz-PC mit der ganz normalen Ausstattung – Fachverfahren, E-Mail-Verkehr, Bürokommunikationssoftware, die vernetzt ist – hat, sondern sich sieben, acht, neun Kollegen in der Notfallumgebung, in der wir von ehemals 550 PCs jetzt im Augenblick 60 am Start haben, die Arbeitsplätze teilen müssen. Der wesentliche Grund, den wir darin sehen, dass es uns so hart getroffen hat und es immer noch ist, war, dass unsere Struktur nicht ordnungsgemäß aufgelegt war. Es war nicht das Problem – das muss ich auch sagen –, das immer durch die Presse geistert, dass es Nachlässigkeiten bei den Mitarbeitern in der IT-Stelle gegeben hat, dass Back-Ups nicht ausgeführt worden seien oder dass das AV-System nicht upgedatet worden war, sondern der Hauptgrund für diese massiven Ausbrüche war, dass wir eine nichtadäquate Struktur hatten.

Wir hatten für 550 Leute – – Das klingt viel, aber wenn mal sieht: Das ITDZ hat etwa 80 000, die sie betreuen, und eine entsprechende personelle Ausstattung dafür. Andere Verbünde, länderübergreifende Verbünde, die jetzt auch in der Justiz zunehmen, haben sechsstellige Zahlen. Die haben eine ganze andere Power, aber auch ganz andere Möglichkeiten, sich aufzustellen. Und entscheidend ist es für uns: Wir hatten für einen kleinen Eigenbetrieb, den wir hatten, der aber – auch wenn er immer zusammengearbeitet hat mit dem Berliner Landesbetrieb – dann funktionieren muss, damit die Mitarbeitenden ihre Standard-IT-Konfigurationen vorfinden und mit denen arbeiten können – – Für einen beschränkten Eigenbetrieb ist es schwierig, eine Struktur aufzubauen, die mit der, die ein professioneller Dienstleister halten kann, standhalten kann, aber auch die Folgen zu begrenzen.

Eine wesentliche Kritik, die wir jetzt aus der Forensik mitgenommen haben: Wir haben z. B. kaum eine Netzwerk-Segmentierung. Das heißt: Wenn ein Angriff durchschlägt, schlägt er potenziell gegen alle Mitarbeiter, die da sind, durch. Es ist – das muss man auch sagen – bei einem gewachsenen Betrieb, wo immer ein Verfahren nach dem nächsten angedockt und betreut worden ist, sehr schwierig, eine vollständige Konformität von BSI-Prozessen oder BSI-Empfehlungen durchzusetzen. Deswegen war die Vorgabe: Wir mussten uns – Sie haben in Ihrer Tagesordnung ja auch nach Schlussfolgerungen gefragt – jetzt darauf konzentrieren, zu sagen: Wir müssen neu aufbauen! Wir müssen generell eine kritische Überprüfung aller IT-Systeme, die wir haben, bezüglich IT-Sicherheit und Datenschutz machen und auch konkrete Maßnahmen ins Auge fassen wie z. B. Netzwerk-Segmentierungen, aber auch solche, die dahin gehen, ein IT-Sicherheitskonzept so aufzustellen, dass es in sich konsistent ist, dass es State of the Art ist und dass es dem entspricht, was heute das Verständnis moderner IT ist. Also kurze Release-Wechsel, agile Entwicklung, anforderungsgerechte Standardisierung!

Das haben wir auf einer abstrakten Ebene mit unserer Senatsverwaltung besprochen, oder man kann auch sagen, die hat uns nach dem Vorfall – – Sie hatten sich ja gemeinsam mit unserer Staatsekretärin entschieden, uns von allen Netzen zu trennen. Zu dieser Entscheidung stehe ich auch, obwohl sie für uns sehr hart war. Aber es gab keine andere Möglichkeit. Da hieß es, Vorgabe eben, einen wirklich professionellen IT-Betrieb – professionell in dem Sinne, wie es ein großer Dienstleister versteht – aufzubauen, externe Unterstützung zu beanspruchen – man kann heute nicht mehr alles selber machen – und – das ist heute auch in einem anderen Zusammenhang gefallen – zu gucken, dass auch unser System beim Kammergericht insgesamt der aktuellen Referenzarchitektur entspricht, dass wir also auch Datenschutzkonzepte und IT-Sicherheitskonzepte haben und umsetzen können, die dem entsprechen, was der Standard in der Berliner Verwaltung ist.

Das klingt ein bisschen theoretisch. Ich will jetzt versuchen, in der Kürze der Zeit ganz kurz zu sagen, wie wir das konkret umgesetzt haben. Das Wichtigste vorweg: Wir haben uns eigentlich bereits wenige Tage nach dem Sicherheitsvorfall entschieden, unser bisheriges System, das ein Mischbetrieb aus einem Eigenbetrieb und dem Betrieb beim ITDZ war, wo wir viele Datenhaltungen auch damals schon hatten – – Dieses alte System wollen und werden wir nicht wieder aufbauen. Wir haben uns vielmehr schon in dieser Phase, in der wir jetzt immer noch stecken, gesagt, dass wir jetzt einen Notbetrieb einrichten müssen, uns aber auch schon mit Blick auf die Zukunft gesagt: Wir wollen alles, was wir produktive Systeme nennen – das heißt also die Systeme, die die Bürokommunikation betreffen, die die Arbeit der Richterinnen und Richter, aber auch der Geschäftsstellenmitarbeiter, beispielsweise der Rechtspfleger in den Fachverfahren betreffen, auch in den Verwaltungsbereichen, die Fachverfahren, die erforderlich sind, um unsere Rechnungen zu betreiben, unser Personal zu betreuen, alles, was produktiv ist in dem Sinne – ich komme später noch darauf –, was nicht reine Pilotierungs-, Entwicklungs- und vielleicht auch noch Schulungsumgebungen sind – – Alles soll zum ITDZ.

Da war es für uns eine große Hilfe – – Wir haben ja als Kammergericht, als Oberlandesgericht die Verantwortung für die elf Berliner Amtsgerichte und das Landgericht Berlin, die schon beim ITDZ waren. Wir sind jetzt also in einem Prozess, wo wir sagen: Wir gehen in das ITDZ, aber nicht nur mit dem, was die reine Technik betrifft, sondern auch mit allem, was, ich sage mal, diesem Thema BSI-Konformität entspricht. – Das heißt, wir adaptieren

auch unsere Konzepte wie zentrale Infrastrukturkonzeption, Netzsicherheit, Notfallkonzepte, allgemeine Sicherheitskonzepte an das, was der Dienstleister dort vorgibt.

Für das alte, herkömmliche Kammergerichtseigenbetriebssystem heißt das: Es bleibt im Augenblick eingefroren, und wir werden es so auch nicht wieder an das Berliner Landesnetz anhängen. Wir konzentrieren uns jetzt erst mal, gerade in der letzten Woche – – Ich habe Herrn Waniek hier hinten gesehen. Wir hatten in der letzten Woche zwei große Gespräche, wo wir gesagt haben: Um die Verbindung zwischen dem Kammergericht und dem ITDZ herzustellen, nehmen wir Netze des ITDZ mit deren Netzwerkarchitektur, gemanagt vom ITDZ, und schließen neue, im Wege des IT-Sellings bestehende, frische Rechner an, die wir jetzt schon beschafft haben und die praktisch die Netzanbindung haben. Unser bisheriges System bleibt eingefroren.

Wir haben es relativ bald, um die Rechtsprechung zu sichern, ermöglicht, dass die Daten von den Kolleginnen und Kollegen lesend gesehen werden. Also sie können jetzt z. B. Texte sehen, die sie geschrieben haben. Da haben wir eigene PCs stehen, die in einer abgeschotteten Umgebung sind, also in einem Netz, das vom Berliner Landesnetz getrennt ist. Sie können sie ausdrucken, sie können sie lesen. Sie können sie im Augenblick aber nicht elektronisch weiter bearbeiten. Ich muss auch sagen: Dabei wird es eine gewisse Zeit lang bleiben, weil es uns immer noch darum geht, diese Grundarbeitsfähigkeit mit Einzelplatz-PCs und unter den Konformitätsregelungen des BSI zusammen mit unseren Partnern beim ITDZ herzustellen.

In einer zweiten Phase werden wir überlegen, ob und wie wir diese Daten doch in der einen oder anderen Form migrieren können. Auch da sagen wir jetzt aber: BSI-konformer Prozess. Es spricht einiges dafür, dass die Unternehmensdaten nach den bisherigen forensischen Ergebnissen – also die Daten, die unseren Laufwerken gespeichert sind – nicht kompromittiert sind. Trotzdem müssen wir natürlich jede Möglichkeit, dass eine potenzielle Infektion weitergetragen wird, ausschließen, und wollen externe Hilfe einholen. Wir haben Spezialisten, die uns auch bei der Forensik geholfen haben, ein Auftragsangebot rausgeschickt. Per heute ist es noch nicht zurückgekommen, aber ich rechne damit. Wir wollen uns da auch Konzepte vorschlagen lassen, wie wir diese Daten in der einen oder anderen Form – ich sage es mal untechnisch – waschen können, sodass wir dann vom CERT und auch von Ihnen, Herr Waniek, in der IKT-Steuerung, Frau Smentek, ein Go bekommen und insgesamt einen dann ordnungsgemäßen Prozess haben.

Was wir noch zusätzlich machen: Ich habe es eingangs gesagt. Wir sind auch verantwortlich, auch wenn wir dort keine Administrationsaufgaben, sondern im Grunde Organisationsaufgaben und Auftraggeberfunktionen wahrgenommen haben, für die IT in der ordentlichen Gerichtsbarkeit, also bei elf Amtsgerichten und dem Landgericht. Auch da überprüfen wir entsprechend der Vorgabe die Prozesse. Es ist in der Presse vielfach angesprochen worden, dass wir – ich will es mal so sagen – vor dem Vorfall einen relativ liberalen Umgang mit USB-Sticks hatten. Es gibt keine Erkenntnisse dafür – das muss man auch sagen –, und auch die forensischen Ergebnisse – es liegen uns im Augenblick nur Entwürfe von Gutachten vor – sprechen nicht dafür, dass diese Infektion etwas mit USB-Sticks zu tun hatte. Trotzdem haben wir im Zusammenwirken mit dem ITDZ entschieden, weil wir bei dieser Überprüfung aller Systeme, die wir gemacht haben, gesehen haben – insgesamt ist es kein vom Dienstleister gemanagter Vorgang gewesen –, dass die Sticks hier frei genutzt werden konnten – – Wir haben uns entschieden, auch auf eine Anregung aus Ihrem Haus, Frau Smoltczyk, dann zu

sagen: Wir müssen diese Möglichkeit erst einmal sperren und gucken, ob und in welcher Form und wie wir hier zu einem wirklich sicheren, gemanagten Prozess kommen. – Deswegen haben wir jetzt die Entscheidung getroffen, dass die USB-Sticks nicht nur im Kammergericht – da haben wir sie sowieso nach dem Sicherheitsvorfall sofort bei den verbliebenen Rechnern gesperrt –, sondern insgesamt gesperrt werden, bis wir so einen neuen Prozess etabliert haben.

Ganz kurz noch, weil Sie auch gefragt haben, wie es weitergeht: Es geht uns bei dem Vorgehen, das wir jetzt gemacht haben – ich glaube, das ist deutlich geworden –, nicht nur darum, zu einem Dienstleister, zum ITDZ zu gehen, um irgendwie aus den aktuellen Schwierigkeiten herauszukommen, dann unseren Eigenbetrieb wiederaufzubauen und zurückzugehen, sondern wir wollen perspektivisch beim ITDZ bleiben. Also diese Struktur, die wir jetzt in der Notfallumgebung gefunden haben, soll vorbehaltlich aller Fragen, die im politischen Raum diskutiert werden – dass es irgendwann später vielleicht noch andere Dienstleister gibt, die uns professionell managen könnten im Rahmen von Justizverbünden –, eine dauerhafte Sache sein. Das ist also für uns etwas, was wir als dauerhafte Entscheidung ansehen.

Eine Frage wird sein, ob alle Verfahren, die wir haben, vom ITDZ auch gehostet werden: Das ist eher zweifelhaft. Wir werden uns ein paar Sachen aufgabenkritisch angucken müssen. Ein Problem, das auch wir hatten, ist heute auch in einem anderen Zusammenhang angesprochen worden: Ja, wir haben teilweise sehr alte Verfahren in der Justiz; z. B. ist unser zentrales Fachverfahren AULAK sehr alt. Da haben wir versucht, Aktualisierungen vorzuziehen. Wir hatten ursprünglich geplant, bis Ende des Jahres auf ein neues Fachverfahren „forumSTAR“ zu wechseln. Das wird jetzt im ersten Quartal vorgezogen werden, damit wir bei so einer zentralen Anwendung, die für uns unverzichtbar ist, wie etwa ein Fachverfahren – –

Vorsitzender Marc Vallendar: Herr Dr. Pickel! Ich würde ungern unterbrechen, aber wir sind mittlerweile bei 15 Minuten, und wir wollen noch eine Fragerunde machen.

Dr. Bernd Pickel (Präsident des Kammergerichts Berlin): Nur noch eins: Wie gesagt, Aktualisierung ist ein großes Thema für uns. Das zweite ist, ob wir einen Eigenbetrieb oder so etwas für die verbleibenden Fachverfahren haben und wie wir ihn gestalten. Das ist völlig offen – wenn, dann BSI-konform und in Abstimmung mit dem ITDZ und allen, die Verantwortung für das Berliner Landesnetz tragen. – Vielen Dank!

Vorsitzender Marc Vallendar: Vielen herzlichen Dank für Ihre Stellungnahme! Jetzt kommen wir zur Fragerunde. Im Anschluss haben Sie noch mal Gelegenheit, die Fragen zu beantworten. – Ich gehe in der Reihenfolge der Meldungen vor: Herr Kohlmeier von der SPD hat sich als Erster gemeldet. – Bitte!

Sven Kohlmeier (SPD): Danke schön, Herr Vorsitzender! – Ich will damit beginnen: Aus Respekt vor dem Kammergerichtspräsidenten sage ich nicht, was ich nach dem, was ich gerade von Ihnen gehört habe, gerade denke, Herr Dr. Pickel, auch weil ich Sie persönlich schätze. Nur so viel: Was Sie uns hier darstellen, beunruhigt mich in deutlicher, erheblicher Weise, und zwar im Hinblick, wie offenbar in der Vergangenheit die IT beim Kammergericht organisiert war, wie wenig Kenntnis offenbar besteht beim Kammergericht und wie fahrlässig man da umgegangen ist im Hinblick auf die Sicherstellung, dass da zumindest ein Grundansatz von Sicherheit bei der Verarbeitung personenbezogener Daten und auch bei der Verarbeitung von Richterdaten usw. gewährleistet wird. Da geht es mir gar nicht darum, dass Sie den liberalen Umgang mit USB-Sticks pflegen, über den hier jeder lacht; das kann man im Jahr 2019 so machen. Das hätte man schon gehört, dass das nicht State of the Art ist. Ich glaube auch nicht, dass sich Emotet – jedenfalls nach meiner Kenntnis, wie das System funktioniert – darüber ausgetauscht hat, sondern der Angriff passiert auf ganz andere Weise. Aber die Unkenntnis oder die Unzulänglichkeiten, die da bestanden, beunruhigen mich ganz deutlich.

Ich bin dankbar, dass Sie sich offenbar derzeit entschieden haben, zum ITDZ zu wechseln und da einen Dienstleister des Landes Berlin in Anspruch zu nehmen, der jedenfalls in der Lage war – bei aller Kritik, die wir in der Vergangenheit am ITDZ gehört haben –, erstens diesen Angriff zu erkennen und zweitens Sie kurzfristig auf einen Stand zu bringen, dass Sie überhaupt arbeitsfähig sind. Ich möchte mir nicht ausdenken, wie Sie hätten arbeiten wollen, wenn das ITDZ nicht gewesen wäre – ob Sie Ihre Schreibmaschinen wieder herausgeholt und irgendwelche Urteile mit der Schreibmaschine geschrieben hätten. Sie lächeln dazu, aber ich finde das tatsächlich nicht witzig. Ich finde es hochgradig schwierig – wir sind hier nicht im Rechtsausschuss, auch da haben wir das ja miteinander diskutiert –, dass der Rechtsstaat nicht in der Lage ist, sich so zu organisieren, dass Sie eine ordentliche judikative Arbeit machen können. Das finde ich deutlich beunruhigend, und ich bin dem ITDZ – Frau Fiedler ist, glaube ich, nicht da – hochgradig dankbar, dass sie in der Lage ist, mit ihrem Team die judikative Arbeit des Kammergerichts aufrechtzuerhalten.

Ich habe einige Fragen an Sie, Herr Dr. Pickel, und ich würde empfehlen, dass man die mitschreibt, nicht, weil ich glaube, dass Sie sich die nicht merken könnten, aber es sind einige; vielleicht schreiben Sie stichpunktartig mit. Mich interessiert, ob Sie wissen, wie der Trojaner Emotet funktioniert.

Zweitens ist meine Frage: Was hat das Kammergericht infolge der Warnungen des BSI getan, um die IT an die Gefahrenlage anzupassen? – Ich möchte daran erinnern, dass das BSI im Jahr 2018 bereits vor Angriffen von Emotet gewarnt hat, u. a. Behörden und IT-Infrastrukturen, und Unternehmen dazu aufgefordert hat, sich entsprechend vorzubereiten.

Dann die dritte Frage: Emotet wurde durch den ausgehenden Traffic beim Kammergericht entdeckt. Wissen Sie, was das für Traffic war, wohin der geflossen ist und wie viel Traffic es war?

Vierte Frage: Welche Daten sind konkret abgeflossen, und ist bekannt, ob E-Mail-Adressen und Inhalte von Kontaktpartner abgeflossen sind? – In dem Zusammenhang die Frage, die im Rechtsausschuss schon eine Rolle gespielt hat: Da wurde ja mitgeteilt, dass datenschutzrechtlich jedenfalls keine Veranlassung war, eine Meldung zu machen, weil keine Daten abgeflossen sind. Mein Grundverständnis von IT ist so, dass dann, wenn E-Mail-Adressen, und zwar

aus E-Mail-Clients heraus, abfließen, das datenschutzrechtlich ein Abfluss von Daten ist. Aber da könnte vielleicht die Datenschutzbeauftragte mir juristische Nachhilfe geben. Ich würde das so verstehen, aber im Rechtsausschuss wurde das anders diskutiert. Da wäre dann die Frage, inwieweit die Datenschutzbeauftragte einzuschalten war.

Fünfte Frage: Die Antivirenprogramme erkennen häufig die nachgeladenen Schadprogramme nicht. Wurde eine aktive Suche nach Emotet oder Trojanern von Seiten Ihrer IT-Abteilung durchgeführt?

Sechste Frage: Wer hatte am Kammergericht Zugriff auf die Admin-Konten, und wurde an dem System etwas geändert?

Siebte Frage: Wurde eine Strafanzeige bei der zentralen Ansprechstelle Cybercrime der Polizei gestellt, und wenn nein, warum nicht?

Achte Frage: Wurden alle Kontaktpartner des Kammergerichts über die Infektion mit Emotet informiert, um sie zu sensibilisieren, dass es zu ähnlich gespooften E-Mails kommen kann, die scheinbar vom Kammergericht kommen und auf eine existierende Kommunikation hinweisen?

Neunte Frage: Wie wird das Risiko gemindert, dass Emotet die geklauten E-Mail-Daten vom Kammergericht nutzt, um vermeintlich vom Kammergericht gesendete E-Mails zu versenden und sich so weiter auf Kontaktpartner und Institutionen des Kammergerichts auszubreiten?

Zehnte Frage: Warum wird die komplette Hardware ausgetauscht, obwohl das BSI empfohlen hat, dass man das System neu aufsetzen kann? – So war es jedenfalls bei heise.de, die ebenfalls von dem Emotet-Angriff betroffen waren. Und dann die Folgefrage, ob die Kosten für das Neu-Aufsetzen geringer gewesen wären, als wenn man eine neue IT beschafft hätte.

Dann die Frage: Irgendwie ist mir zugetragen worden, dass es ein T-Systems-Gutachten gibt, das Sie wohl als Kammergericht in Auftrag gegeben haben und wo relativ deutlich die Schwachstellen bei Ihnen dargestellt wurden. Da das offenbar irgendwo in der Weltgeschichte existiert, hätte ich als Abgeordneter gern eine Kopie von diesem Gutachten, um es mir nicht anderweitig beschaffen zu müssen. Daher wäre meine Bitte an den Senat, dem Ausschuss oder mir als Abgeordnetem eine Fassung dieses Gutachtens zur Verfügung zu stellen.

Dann noch eine Frage an Herrn Dr. Pickel: Ist es so, dass Sie Back-Ups von den Daten erstellt haben? Sind diese Back-Ups nutzbar und wieder aufrufbar, oder sind Daten unwiederbringlich verloren? – Letzte Anmerkung von mir zu dem T-Systems-Gutachten: Ist es zutreffend, dass Sie ein weiteres Gutachten beauftragt haben in Hinblick auf die Datensicherheit beim Kammergericht? Wird es dem Ausschuss zur Verfügung gestellt, wenn das Ergebnis vorliegt?

Vorsitzender Marc Vallendar: Dann als Nächste auf meiner Liste Frau Dr. Brinker von der AfD-Fraktion. – Bitte!

Dr. Kristin Brinker (AfD): Vielen Dank, Herr Vorsitzender! – Ich fasse mich kurz, und zwar zum einen in Richtung Frau Smentek: Ja, einen hundertprozentigen Schutz gibt es nicht. Trotzdem muss man alle Vorkehrungen treffen, soweit es geht, damit nichts Gravierendes

passiert. Insofern begrüßen wir Ihre HTML-Lösung, den Umgang mit HTML-Dokumenten; das ist schon mal gut. – Es ist schade, dass heute Frau Fiedler vom ITDZ nicht da ist; das hatte Herr Kollege Kohlmeier schon angemerkt. Wir hatten Frau Fiedler genau zu diesem Aspekt „Kammergericht“ im Unterausschuss Beteiligungsmanagement und Controlling zu Gast. Da das ein vertraulicher Ausschuss ist, kann ich jetzt hier über die Inhalte nichts weiter sagen, außer vielleicht so viel, dass nach unserer Einschätzung das ITDZ hier als Feuerwehr wunderbar funktioniert hat und im Prinzip vieles geleistet hat, was man so in der Öffentlichkeit gar nicht wahrnimmt.

Ich habe auch aus dem Ausschuss damals mitgenommen – so viel kann man sicher sagen –, dass keinerlei Daten aus dem Kammergerichtspool heraus nach außen gedrungen sind. Es ist die Frage an Dr. Pickel, ob er das bestätigen kann, dass tatsächlich keinerlei Daten – was man auch immer unter Daten versteht – rausgegangen sind und dass entsprechend der Schutz durch das ITDZ letztlich gezielt und schnell gegriffen hat. Das ist die eine Frage.

Die zweite Frage an Herrn Dr. Pickel: Sie haben freundlicherweise ausgeführt, dass Sie mit dem ITDZ in Zukunft zusammenarbeiten werden. Wie ist denn da die genaue Zeitplanung? Gibt es da eine konkrete Zeitplanung? – Wenn sie noch nicht so konkret ist, dann ist das vielleicht eine Berichtsbitte an den Senat, dass Sie uns, sobald der Zeitplan vorliegt – in den nächsten zwei Monaten, man kann einen Termin festlegen –, mitteilen, wie das Ganze gestaffelt ablaufen soll.

Noch eine letzte Frage an Dr. Pickel: Sie haben von Ihrem Software-Hersteller berichtet, der die Software für Sie betrieben hat. Hatte der denn auch einen wirksamen Viren- und Malware-Schutz? Haben Sie noch weitere Softwareprodukte eingesetzt, oder war das nur ein Hersteller? – Ich frage das einfach nur, damit man das Problem eingrenzen kann, in der Erwartung, dass das Thema, wenn Sie zum ITDZ wechseln, wirklich ein für alle Mal gegessen ist. – Vielen Dank!

Vorsitzender Marc Vallendar: Dann Herr Schlüsselburg von der Linken – bitte!

Sebastian Schlüsselburg (LINKE): Vielen Dank, Herr Vorsitzender! – Ich werde mich vor dem Hintergrund der auch schon im Rechtsausschuss erfolgten Besprechung hier auf die Frage beschränken, was sich seitdem verbessert hat. Erste Frage ist die nach der internen Kommunikation unter Ihren Beschäftigten: Kollege Kohlmeier und ich waren unlängst bei der Mitgliederversammlung der Jugend- und Auszubildendenvertretung bei Ihnen und haben am Schwarzen Brett einen analogen Newsletter gesehen, mit dem die interne Behördenkommunikation gewährleistet werden sollte. Deswegen meine Frage, ob und inwieweit sich inzwischen und insbesondere seit der Erörterung im Rechtsausschuss die interne digitale Kommunikation verbessert hat.

Die zweite Frage ist ähnlich gerichtet, aber nach außen: Wie sieht es inzwischen aus mit der Erreichbarkeit des Kammergerichts für Anwälte, aber auf für Bürgerinnen und Bürger? – Wenn Sie vielleicht dazu etwas sagen können? – Dann habe ich noch eine Frage: Hat sich an dem Prognosezeitraum für die volle Arbeitsfähigkeit im Vergleich zu Ihrer Äußerung im Rechtsausschuss – da hatten Sie kein konkretes Datum genannt, aber einen Zeitraum – etwas geändert? Nach welcher aktuellen Prognose schätzen Sie, wieder voll arbeitsfähig sein zu können?

Dann noch die Frage, wie viele Rechner – also Arbeitsgeräte, Server oder auch Netzwerkrechner – inzwischen ausgetauscht wurden. Das ist ja ein Prozess, der läuft. Können sie dazu etwas sagen? Und dann habe ich noch die Frage, ob Sie uns zumindest eine Prognose geben können, wann alle Richterinnen und Richter mit dienstlichen Laptops ausgestattet sein werden. Das ist ja auch eine der Konsequenzen aus dem Vorfall.

Die letzte Frage geht wahrscheinlich eher an den Senat: Ich würde ganz gern wissen, wie der aktuelle Stand in Bezug auf die Vorbereitung einer möglichen Änderung von § 23 Ausführungsgesetz GVG aussieht. Das ist die Rechtsgrundlage, die in Berlin zumindest den Richterinnen und Richtern erlaubt, eigene, private IT-Geräte für die Arbeit zu verwenden. Letzten Endes ist es natürlich Aufgabe des Gesetzgebers. Aber ich würde gern wissen, ob es da schon einen Stand gibt, ob zumindest von Seiten des Senats an der Stelle eine Gesetzesinitiative zu erwarten ist. – Vielen Dank!

Vorsitzender Marc Vallendar: Jetzt Herr Schlömer von der FDP-Fraktion – bitte!

Bernd Schlömer (FDP): Vielen Dank, Herr Vorsitzender! – Vielen Dank für Ihre Ausführungen, Herr Dr. Pickel! Natürlich ist es so, wenn man den Impuls vom Senat und Ihre anfängliche Stellungnahmen hört, dass sich die Bedrohungslage potenziell vervielfacht hat, dass man dem Rechnung tragen muss. Auf der anderen Seite ist ganz deutlich leichtfertiges Verhalten bei diesem Fall in den Fokus zu nehmen. Ich kann aber den Ausführungen nicht deutlich entnehmen, dass Sie in irgendeiner Art und Weise Maßnahmen ergriffen haben, dass der Sensibilisierung und Belehrung auch von Richtern in Ihrem Zuständigkeitsbereich konsequent nachgegangen wird.

Vor diesem Hintergrund habe ich folgende Fragen: Liegen von allen Beschäftigten des Kammergerichts dokumentierbare Nachweise vor, dass eine Sensibilisierung zu Datenschutz und IT-Sicherheit vorgenommen worden ist, wie es üblich und Usus in der öffentlichen Verwaltung ist? – Zum Zweiten muss ich mit Erstaunen feststellen, dass sich durch alle Ihre Ausführungen hindurchzieht: „Wir prüfen“, „befristet“, „mal schauen, was wir machen, und dann machen wir es wieder selber“. Das muss insofern sehr erstaunen, weil Sie nachgewiesen haben, dass Sie nicht in der Lage sind, einen IT-Betrieb für mehrere Gerichte verantwortungsvoll wahrzunehmen. Da würde ich gern vom Senat hören, ob es, wenn Herr Dr. Pickel von Eigenbetrieb spricht, auch die Intention des Senats sein kann, dass man das Kammergericht nach einer befristeten Phase wieder in die eigene Zuständigkeit entlässt.

Mich würde auch interessieren, welche Rolle eigentlich die Justizverwaltung derzeit spielt. Welche Maßnahmen hat denn die Justizverwaltung ergriffen, um Sie bei der Behebung der Probleme zu unterstützen? – Und ich möchte wissen, welche disziplinar- und personalrechtlichen Maßnahmen Sie eingeleitet haben, die infolge des Bruchs von Amtsverschwiegenheit – denn als solchen kann man das deklarieren – von Ihrer Seite zumindest angeschoben worden sind, weil ja vielleicht jemand vorsätzlich gehandelt haben kann. Das können Sie ja nicht ausschließen.

Schließlich würde mich auch interessieren – Sie sprachen von einem Firewall-Gutachten, einer externen Stellungnahme –: Wer hat diese externe Stellungnahme verfasst? Was steht dort drin? Wie kann diese Stellungnahme an uns weitergegeben werden? – Sie sprachen auch

von einem Gutachten, dass Sie an externe Spezialisten geben wollen oder wo Sie kurz davor sind: Was ist das für ein Gutachten? Was ist Zweck und Zielrichtung des Gutachtens? Welche Handlungsleitlinien wollen Sie daraus ziehen und sich zunutze machen? – Das sind erst einmal meine Fragen. – Vielen Dank!

Vorsitzender Marc Vallendar: Herr Ziller von den Grünen – bitte!

Stefan Ziller (GRÜNE): Vielen Dank! – Ich will mit dem Dank anfangen: Danke, dass Ihnen dieser Vorfall passiert ist und wir deswegen eine ganze Menge diskutieren können! – Spaß bei Seite! Aber ohne solche Vorfälle kriegen wir die Berliner IT-Architektur nicht voran. Insofern steht über allen meinen Fragen: Was nehmen Sie auch für andere Behörden mit? – Dieses Gutachten öffentlich zu machen, damit andere davon lernen können, wäre ein Wert. Und vielleicht aus Ihren Gesprächen jetzt: Was empfehlen Sie den anderen Behörden, Bezirken, Landesunternehmen zu tun, bevor solch ein Vorfall aufkommt? Was hätte Ihnen vor diesem Vorfall geholfen, in Ihrer Behörde, mit Ihrem Amt genau diese Gutachten und Untersuchungen zu machen, um proaktiv auf eine sichere IT-Architektur umzustellen, und nicht erst, dass so ein Vorfall passieren muss? Wenn Sie da Hinweise haben, wäre das super, weil ich glaube, die Staatssekretärin hat recht, dass es inzwischen mehr Interesse gibt. Viele interessieren sich für IT-Sicherheit, aber leider nicht alle und nicht genug.

Ich glaube, dass wir im Land Berlin deswegen insgesamt nicht genug tun und unsere IT-Architektur einfach nicht dem Stand der Technik entspricht, wie es möglich wäre, wenn das alles vom ITDZ gemacht würde. Das ist auch keine Bösartigkeit. Das liegt einfach daran, wenn man halt nicht einen, sondern 27 Leute hat, die diese BSI-Sachen alle lesen müssen, und dann gibt es eine Empfehlung, und man setzt die um, aber dann hat man einfach zu viele Leute in der Kette, und es kommt am Ende später an, als wenn man das zentral steuert, wie das heute eigentlich gang und gäbe ist. Insofern haben wir in Berlin für die nächsten Jahre noch ein Problem, weil wir mit dem Übergang und der Umsetzung des E-Government-Gesetzes einfach lange brauchen; es ist leider so. – Aber die Frage: Was können wir aus Ihrer Sicht den anderen Behörden und den anderen Unternehmen, die betroffen sind, sagen, damit die vor so einem Vorfall schneller werden und agieren?

Das Zweite – Sie haben über Ihre Fachverfahren gesprochen –: Gibt es bei Ihnen eine Liste, welche dieser Fachverfahren der IKT-Architektur entsprechen und welche nicht? Haben Sie für Ihre Arbeit da eine Übersicht? Gibt es Fachverfahren, die unter einem Berlin-PC unter Standard Windows 10 nur laufen, wenn man irgendwelche Sicherheitseinstellungen runterstuft? Oder sind die alle up to date? Wie wäre gegebenenfalls der Zeitplan, die auf den neusten Stand der Technik zu bringen?

Die letzte Frage, weil sie uns im Rahmen des Einzelplans 25 und E-Government immer wieder betrifft – diese Sonderrolle der Justiz, dass Sie Teile der Verantwortung nicht unter das E-Government-Gesetz einordnen wollen, sondern immer eine Extra-Rolle haben –: Halten Sie das auch nach den gegebenen Vorfällen weiter im bestehenden Modus für sinnvoll? Oder sehen Sie, dass es Bereiche gibt, in denen man sich der Zentralisierung und Standardisierung anschließen sollte, wo es eben um den Betrieb der IT-Sachen geht und nicht um die richterliche Entscheidung? Hat durch den Vorfall bei Ihnen oder den Kolleginnen und Kollegen ein Umdenken eingesetzt?

Vorsitzender Marc Vallendar: Herr Stettner von der CDU – bitte!

Dirk Stettner (CDU): Viele Fragen sind Ihnen gestellt worden, Herr Dr. Pickel, und die will ich nicht wiederholen. Ich bin auf die Antworten sehr gespannt. Ich möchte auch nicht zu genau das wiederholen, was Kollege Kohlmeier gesagt, aber mir fällt schon sehr deutlich auf, dass Sie in Bezug auf die IT-Sicherheit jedenfalls der falsche Mann an der falschen Stelle sind – was wahrscheinlich klar ist, weil das nicht Ihr Hauptjob ist. Das zeigt auch Ihre Erläuterung dazu: Eine kleine Struktur kann für keine IT-Sicherheit sorgen. Ich stelle mir gerade ein Privatunternehmen in entsprechender Größenordnung vor, das nach zwei Jahren Zeit, umzustellen, nach zwei Jahren Information darüber, dass seine Software rettungslos veraltet ist, nichts tut, dann angegriffen wird und sagt: „Ich bin eine zu kleine Struktur, um das in Ordnung zu bringen!“, und frage mich, was mit diesem Unternehmen passiert wäre. Da haben Sie schon eine ganz besondere Stellung, dass überhaupt so freundlich mit Ihnen umgegangen wird.

Ich wundere mich zweitens, dass wir hier nach Schlussfolgerungen fragen und es offenbar Untersuchungen Ihrerseits gibt, aber es gibt keinerlei handfeste, belastbare Informationen, die uns hier vorgelegt werden. Sie sind hier im Fachausschuss, und Ihre Ausführungen sind dafür nicht ausreichend, ganz freundlich ausgedrückt. Das ist sehr allgemein gehalten. Ich habe es mir aufgeschrieben: Wie gesagt, die Fragen sind alle schon gestellt worden, aber Sie haben auf keine einzige meiner Fragen eine Antwort in Ihrem Vortrag bereitgehalten, und das hätte ich mir bei dem Aufruf mit Ankündigung doch anders erbeten. Ich bitte ganz deutlich darum, dass wir etwas Schriftliches bekommen, wie Sie in Zukunft ausschließen wollen, dass Sie ein so offenes Haus sind. Das habe ich bisher Ihrerseits gar nicht gehört.

Ich glaube, Sie sind jetzt seit ungefähr drei Monaten nicht arbeitsfähig. Ein Privatunternehmen wäre mittlerweile pleite. Für uns heißt das nur, dass das wichtigste Gericht nicht arbeitsfähig ist. Ich war nicht im Rechtsausschuss, und daher kenne ich im Gegensatz zu manch anderem hier leider nicht die Zeitschiene, die Sie da benannt haben. Wann stellen Sie die volle Arbeitsfähigkeit wieder her? Wie geht das zukünftig mit dem Zugriff von außen? – Es ist ja keine Rocket Science, dass man einen vernünftigen Zugriff, Arbeitsfähigkeit für den Mitarbeiter von außen herstellen kann. Dazu habe ich von Ihnen nichts gehört außer der Betrachtung retrospektiv, dass Sie einen etwas laxen Umgang mit Sticks gehabt haben. Das ist strafbar, wenn man das ganz klar betrachtet im normalen privaten Umfeld, wenn ich so mit meiner IT-Struktur umgehe. Also was ist da die Planung für die Zukunft?

Eine Frage wiederhole ich doch: Wie kommen Sie zu der Idee, eigene IT-Struktur im Haus behalten zu wollen, nach diesen Erfahrungen, die Sie damit gemacht haben? Also wie kann man auf diese Idee kommen? Haben Sie 50 neue IT-Experten einkaufen können, die das für Sie demnächst erfolgreich tun? Oder glauben Sie, dass dann Ihre Struktur plötzlich besser funktioniert?

Das Thema Fortbildung, Unterweisung – Herr Schlömer hat es schon angesprochen; ich glaube, wir hatten das auch schon in der ersten Runde –: Gibt es bei Ihnen standardisiert und dokumentiert regelmäßige IT-Unterweisung, Datensicherheitsunterweisung? Werden die dokumentiert, werden die unterschrieben, dass die auch durchgeführt worden sind? Wer trägt dafür die Verantwortung? – Das ist alles Ihre Pflicht, das in der Struktur zu organisieren. Dazu habe ich noch nichts gehört.

Mich interessiert, was die Datenschutzbeauftragte zu diesen Vorgängen sagt. Auch da hätte ich gern den Vergleich zu einem privaten Unternehmen. Bitte ziehen Sie diesen Vergleich einmal. Ich habe dazu eine Vorstellung. Und inwieweit läuft ein Echtzeit-Monitoring Ihrer Struktur jetzt, und zwar Ihrer kompletten Struktur, nicht nur der Teile, die schon vorher beim ITDZ gewesen sind? – Danke schön!

Vorsitzender Marc Vallendar: Frau Dr. Vandrey von den Grünen – bitte!

Dr. Petra Vandrey (GRÜNE): Erst mal möchte ich festhalten: Natürlich dürfen solche Vorfälle wie im Kammergericht nicht passieren, auch möglichst nicht, damit wir erst dadurch lernen, sondern wir sollten vorher versuchen, auch hinsichtlich der anderen Gerichte die IT der Berliner Justiz so aufzustellen, dass sie funktioniert. Es wird sehr viel auf dem Kammergericht und Herrn Dr. Pickel herumgehackt. Ich möchte betonen: Herr Dr. Pickel ist meines Wissens nach Jurist und Richter. Es wäre vielleicht sinnvoll, auch die IT-Abteilung des Kammergerichts mal näher dazu zu befragen oder um eine schriftliche Beantwortung dieser vielen Fragen zu bitten.

Ich habe leichte Zweifel, ob das Ganze nicht genauso gut einem anderen Gericht in Berlin passieren könnte. Ich würde es gut finden, wenn wir jetzt aufhören, uns nur das Kammergericht anzugucken, weil das jetzt dem Kammergericht passiert ist. Es ist schlimm genug; das will ich gar nicht abmildern. Aber wir sollten nicht so tun, als ob wir es hier nur mit einem Problem des Kammergerichts zu tun hätten. Wir haben insgesamt ein Problem mit der IT der Berliner Justiz, und wir sollten gucken, dass wir uns die Justiz insgesamt angucken, damit wir nicht morgen hier das Landgericht oder irgendein anderes Berliner Gericht sitzen haben und dann genauso, wie wir es jetzt mit dem Kammergericht tun, auf dem nächsten Gericht herumhacken.

Ich möchte auch ausdrücklich betonen, dass aus meiner Sicht als Anwältin – ich bin ja hier in Berlin als Anwältin tätig – die Arbeitsfähigkeit des Kammergerichts durchaus da ist. Ich bin im Familienrecht tätig, das heißt, ich habe schon in zweiter Instanz die Verfahren immer vor dem Kammergericht. Daher habe ich relativ viele kammergerichtliche Verfahren, auch im Moment. Im Moment läuft es so. Da gebührt mein ausdrücklicher Dank den Geschäftsstellen des Kammergerichts und auch den dort zuständigen Richterinnen und Richtern, die wahnsinnig hilfsbereit sind, und die Verfahren laufen einigermaßen. Es trifft zu, dass wir im Moment handgeschriebene Zettel mit irgendwelchen Hinweisen kriegen. Wir kriegen handschriftlich korrigierte Terminsladungen. Das ist kein guter Zustand, das möchte ich überhaupt nicht so sagen, aber es gibt eine sehr große Hilfsbereitschaft der Geschäftsstellen, die ständig mit uns telefonieren, einfach anrufen und darauf hinweisen, wenn irgendwo ein Tippfehler drin war, der schriftlich in irgendeinem Fax – oder was da jetzt benutzt wird – rausgegangen ist. Also ich sehe nicht, dass wir ein komplett arbeitsunfähiges Kammergericht haben. Ich kann aus meiner eigenen Anwaltskanzlei sagen, dass die Verfahren, die ich beim Kammergericht habe, im Moment etwas stolpern, aber die Verfahren laufen alle.

Dann wollte ich aber auch fragen, weil ich durchaus sensibel bin in diesen Datenschutzfragen und mir schon ein bisschen Sorge mache, wie die Zukunft aussieht: Sie haben ja freundlicherweise gesagt, Herr Dr. Pickel, dass Sie unter den Mantel des ITDZ gehen wollen. Darauf bezogen sich schon einige Fragen meiner Vorredner. Das haben Sie auch schon im Rechtsausschuss, dem ich angehöre, ausgeführt. Meine Frage ist: Welche Bereiche – Sie ha-

ben gesagt, der produktive Bereich geht in das ITDZ – sind jetzt genau die, die beim Kammergericht Ihrer Auffassung nach bleiben sollen? – Das habe ich Ihren Ausführungen vorhin nicht ganz entnommen. Und dann würde mich vor allem auch interessieren: Wann ist der Übergang zum ITDZ geplant? Wie lange dauert es dann, bis die routinierte Arbeitsfähigkeit des Kammergerichts wieder so hergestellt ist, dass sie voll funktioniert?

Als Letztes hätte ich noch die Frage hinsichtlich der finanziellen Auswirkungen der ganzen Angelegenheit: Wenn Sie neue IT-Fachkräfte einstellen müssen, wenn Sie zum ITDZ gehen, wenn Sie Ihre eigene IT neu aufstellen wollen, ist das wahrscheinlich mit vielen finanziellen Auswirkungen verbunden. Wie schätzen Sie die ein? Denken Sie im Übrigen, dass in unserem Haushalt – Einzelplan 06 zur Justiz – genug Mittel für die IT der Justiz eingestellt sind? Oder sehen Sie da noch Handlungsbedarf hinsichtlich der finanziellen Auswirkungen der gesamten Situation am Kammergericht? – Vielen Dank!

Vorsitzender Marc Vallendar: Herr Lenz hat sich noch gemeldet – von der CDU-Fraktion. – Bitte!

Stephan Lenz (CDU): Ich versuche, es kurz zu machen, weil wahnsinnig viele Fragen schon gestellt worden sind. Ich weiß gar nicht, wie Sie darauf antworten sollen. Ich bin auch gern bereit, wie Frau Vandrey das gesagt hat: Man muss wahrscheinlich die gesamte Berliner Justiz in den Blick nehmen, um das auf ein konstruktives Gleis zu setzen. Aber ich möchte noch einmal – und mit dem Gefühl möchte ich hier rausgehen – darauf hinweisen: Sie sind der Leiter eines ganz besonderen Gerichts. Sie haben hochsensible Verfahren. Das sind nicht nur familienrechtliche Verfahren. Sie haben Verfahren mit sehr heiklen Daten, wo es Sicherheitsgefährdungen gibt. Sie haben Angeklagte, die bestimmten Spektren angehören. Das ist teilweise hochsensibel, da geht es um Menschenleben. Das ist nicht dramatisiert. Insofern wäre es für mich schon sehr wichtig, hier rauszugehen mit einer gewissen Sicherheit dahingehend – ich habe mir gemerkt –: Es gab keine Datenabflüsse.

Jetzt hat Kollege Kohlmeier herausgearbeitet, dass es unsicher ist, ob es nicht doch Datenabflüsse derart gab, dass E-Mail-Adressen und damit Personen identifiziert worden sind. Ist das so? Das würde ich gerne wissen, wenn ich hier rausgehe. Oder ist das nicht so? Das ist für mich ein ganz entscheidender Punkt, weil das dann nicht nur ein Lernbeispiel ist, sondern dann haben wir daraus, glaube ich, Schlussfolgerungen zu ziehen, die auch mit der Gefährdung der betroffenen Personen zu tun haben. Wenn ja, würde ich auch gern direkt wissen – weil Sie nun mal der Präsident sind –: Wie agieren Sie, um die Leute zu schützen?

Und der zweite Punkt – es sind, wie gesagt, einfach andere Verfahren, die mich umtreiben, Frau Kollegin –: Wie ist es mit der Arbeitsfähigkeit? Wann ist die voll wiederhergestellt? Sie nehmen einfach ganz zentrale Aufgaben für unser Land wahr. Wann ist es wieder sichergestellt, wann laufen Sie wieder auf allen Zylindern? Es geht ja nicht nur darum, Datenschutzbelange zu schützen, sondern es geht darum, diese Verfahren erfolgreich zum Ende zu bringen und im Idealfall die Betroffenen ihrer Verurteilung zuzuführen und damit letztlich unser Land zu schützen.

Vorsitzender Marc Vallendar: Dann hat sich die Datenschutzbeauftragte, Frau Smoltzcyk, gemeldet. – Bitte!

Maja Smoltzcyk (Berliner Beauftragte für Datenschutz und Informationsfreiheit): Vielen Dank! – Zur Frage, ob es hätte gemeldet werden müssen: Ja, natürlich hätte es gemeldet werden müssen. Es wurde auch gemeldet, ein bisschen zu spät. Es ist eine Datenpanne, und natürlich muss das gemeldet werden, zumal überhaupt nicht absehbar ist, inwieweit tatsächlich Daten abgeflossen sind oder nicht. Das kann man, glaube ich, gar nicht feststellen. Ich meine, hier war ja ein Konglomerat von technischen Geräten. Es wurden Privatgeräte benutzt. Wie soll man wissen, ob die auch befallen sind oder was darüber für Daten vielleicht abgeflossen sind?

Ich glaube, man sollte das Problem aber tatsächlich ein bisschen weiter fassen: Wir haben das Kammergericht. Wir haben aber kurz danach auch die HU und die TU gehabt, und bei HU und TU ist sehr viel weniger beherzt agiert worden als im Kammergericht. Das möchte ich an dieser Stelle auch mal sagen. Da ist man sehr viel laxer damit umgegangen. Ich glaube, was wir wirklich im Augenblick brauchen oder was wir unbedingt in Angriff nehmen müssen, ist die Erstellung von Handlungsleitfäden für den öffentlichen Bereich insgesamt, wo auf der einen Seite die Handlungsmaßgaben aufgeführt werden, um solche Datenpannen zu vermeiden, und auf der anderen Seite Handlungsempfehlungen gegeben werden, wie man sich verhält, wenn es zu solchen Datenpannen kommt. Das ist das eine. Ich halte es für absolut existenziell, dass das passiert.

In der Tat: Es kann überall passieren, und unser Bestreben sollte dahin gehen, dass man versucht, das für das Land Berlin insgesamt so weit wie möglich in den Griff zu kriegen und auszuschließen. Es wird Erfordernisse geben, ein paar technisch-organisatorische Maßnahmen zu ergreifen. Das geht von der Überprüfung von E-Mail-Eingängen bis zu einem Verschlüsselungssystem für ganz Berlin. Das halte ich für absolut zwingend, dass das im Zusammenhang mit dem E-Government in Angriff genommen wird. Man wird da technische Möglichkeiten finden müssen. Wenn E-Mails verschlüsselt verschickt werden, kann man natürlich auch nicht erkennen, ob eine Schadsoftware drin ist. Das heißt, wenn die beim Empfänger ankommen, muss das zunächst von einer Maschine entschlüsselt werden. Dann muss es überprüft werden, und erst dann darf es in den Eingang der Empfänger kommen. Das ist eine Art Quarantänestation, um die Infiltrierung von Rechnern zu vermeiden. – Ich würde gern Herrn Dr. Vollmer das Wort geben, der das technisch ein bisschen genauer erklären kann, wenn es Ihnen recht ist.

Vorsitzender Marc Vallendar: Dann Herr Dr. Vollmer – bitte, Sie haben das Wort!

Dr. Ulrich Vollmer (BlnBDI): Herzlichen Dank! – Ich möchte das ein klein wenig näher ausführen in dem Sinne, dass ein Grundübel hier schon angesprochen wurde: das der Nutzung von privaten Geräten. Die Ausgestaltung der Verarbeitung von sensiblen Daten in privaten Gerät ist höchst komplex, und wir haben hier ein schlechtes Beispiel vor uns. Wir raten dringend dazu, dass private Geräte für solche Verarbeitungen gar nicht erst eingesetzt werden, und wenn es da eine entsprechende Änderung der gesetzlichen Grundlagen gibt, würden wir das auf jeden Fall begrüßen.

Wir hatten schon gesagt, dass es Handlungsleitfäden geben muss. Es gab den Begriff des ITDZ als Feuerwehr. Wir begrüßen es, wenn es ein schnelles Eingreifteam gibt, das bei den Behörden vor Ort sein kann, um die Gegenmaßnahmen mitzusteuern, Beweismittel zu sichern und zu ermöglichen, dass man hinterher feststellen kann, auf welchem Weg diese Schadsoft-

ware überhaupt in das System eingedrungen ist. Man muss ja wissen, woher es kommt, um entsprechend darauf reagieren zu können und andere zu warnen, die eventuell in der Folge genauso davon betroffen sein können.

Wir haben – das hat sich weniger im Fall des Kammergerichts als im Fall der Universitäten gezeigt; das ist vielleicht auch in der Hauptverwaltung weniger ein Problem, aber in anderen Bereichen durchaus – dann Probleme, wenn sich private Daten und dienstliche Daten mischen. Es kommt also sehr darauf an, dass man das eine von dem anderen trennt, dass man wirklich in die Daten hineinschauen kann und schauen kann, ob sie von Schadsoftware befallen oder nicht befallen sind.

Es kommt darauf daran, dass wir die Technik schärfen. Im Augenblick wird eine solche Anti-Viren-Software eingesetzt. Aber diejenigen, die Schadsoftware herstellen, trainieren ihre Schadsoftware so, dass sie gerade von den Anti-Viren-Programmen nicht erkannt werden. Es gibt aber Verfahren, die schlauer sind als unser Anti-Viren-Programm, die einfach darauf schauen, was für Techniken die Schadsoftware einsetzt. Um ein Beispiel zu nennen, das vielen von Ihnen vielleicht noch bekannt ist: In der normalen Bürosoftware Microsoft Word ist ein Makro drin, und aus diesem Makro kommt dann die ganze Schadsoftware, die wird dann mit einem Faden herausgezogen. Aber so etwas kann man an der Grenze zu einem Netz erkennen und von vorneherein herausfiltern. Es gibt wenige Bereiche, wo solche Funktionen überhaupt benötigt werden.

Wir brauchen auch ein Konzept, das über die Filterung, die jetzt schon vom ITDZ durchgeführt wird – – Dass Spam ausgefiltert wird, ist richtig, dass bestimmte Standardangriffe ausgefiltert werden ist, richtig und notwendig, dass Anti-Viren-Software über die Eingänge läuft, ist richtig und notwendig, aber es ist leider nicht ausreichend. Wir brauchen bei den einzelnen Stellen Beratung – das ist schon angesprochen worden –, was die Struktur der Netzwerke betrifft, das Verständnis dessen, was überhaupt ein Risiko darstellt. Eine Vorgabe, eine Architektur ist eine gute Sache, Beratung ist aber notwendig, um eine Struktur oder Architektur, die vorgegeben ist, in eine tatsächlich sichere Software-Umgebung umzusetzen. Das kann eine einzelne Behörde nicht alleine tun. Je mehr wir hier zentralisieren, je mehr wir beim Vorgang des Übergangs zur Datenverarbeitung im Auftrag durch das ITDZ voranschreiten, desto besser wird das Land Berlin aufgestellt sein. Aber bis dahin ist noch eine gewisse Zeit zu gehen.

Maja Smoltczyk (BlnBDI): Ich möchte noch kurz auf die Frage mit den Unternehmen eingehen, ob die in Konkurs gehen würden, wenn sie sich so verhalten würden: Im Bereich der Unternehmen gibt es alles. Es gibt Unternehmen, die genauso sorglos mit der IT-Technik umgehen, wie das in der Verwaltung häufig anzutreffen ist. Es gibt aber selbstverständlich auch Unternehmen, die das nicht tun, die sehr gut darauf vorbereitet sind. Erlauben Sie mir, dass ich hier einflechte, dass Unternehmen mit Bußgeldern zu rechnen haben, öffentliche Einrichtungen haben das nicht. Ich glaube schon, dass das auch einen Unterschied macht.

Vorsitzender Marc Vallendar: Dann hat sich noch Frau Smentek gemeldet. – Bitte!

Staatssekretärin Sabine Smentek (SenInnDS): Ich denke über die Sache mit den Bußgeldern noch nach, aber das Parlament hat ja in der Tat auch einen – – Wir haben eine Evaluation des E-Government-Gesetzes vor uns, aber ich befürchte, dass wir an ein paar Grenzen stoßen, was das Verhältnis der Verwaltungen untereinander betrifft. – Ich wollte etwas anderes

sagen: Es ist die Frage gestellt worden, wie wir die Haltung: „Eigenbetrieb – ja oder nein?“ sehen. Sie wissen, dass wir bei den Verwaltungen, die unter das E-Government-Gesetz fallen, selbstverständlich an der Migration des Betriebs zum ITDZ arbeiten. Das betrifft die verfahrungsunabhängige IKT.

Ausgenommen davon ist ausdrücklich nach § 1 des E-Government-Gesetzes die Gerichtsbarkeit. Das bedeutet, wir können das gut finden, wenn die Gerichtsbarkeit sagt: Wir würden gern die verfahrensunabhängige IKT zum ITDZ migrieren. – Natürlich unterstützen wir diesen Weg, aber wir können es, anders als in anderen Verwaltungen, nicht entscheiden. Das ist so. Ich habe aber den Eindruck – ich habe ja Herrn Dr. Pickel jetzt erneut zuhören dürfen –, dass wir in der Frage von Kooperation und beim Finden von Lösungen im Sinne der Datensicherheit und der Modernität und auch der Anschlussfähigkeit an die Berliner Verwaltung dort einen neuen Kooperationspartner gefunden haben. Das ist auch mein Eindruck von der Justizverwaltung in den letzten drei Jahren insgesamt, dass, obwohl dieser § 1 – Geltungsbereichs des E-Government-Gesetzes – für den Bereich der Justiz nur eingeschränkt gilt, dort durchaus eine Form der Zusammenarbeit gesucht wird. An dem, was Herr Dr. Pickel gerade dargestellt hat, sieht man auch, dass hier eine sehr starke Anbindung an die Standards des Landes Berlin gewünscht ist.

Was durchaus auch für die Gerichtsbarkeit gilt, sind die Regelungen zur IT-Sicherheit – nur, um das hier auch deutlich zu sagen. Die Regelungen zur IT-Sicherheit erlässt die Innenverwaltung nicht unter dem Stichwort „Verfahrensunabhängige IKT“, sondern alle Regelungen zum Thema IT-Sicherheit gelten für alle Berliner Verwaltungen. Das möchte ich an der Stelle auch sagen. Dass wir hier noch einiges zu tun haben, habe ich auch in meinen Eingangsstatement gesagt. Also Eigenbetrieb – das können wir an der Stelle leider für die Gerichtsbarkeit aufgrund der geltenden Gesetz nicht ganz so festlegen. Da bin ich mal gespannt.

Was ich gerne mitnehme würde, ist die Frage nach dem § 23 AGGVG: Ob da eine Änderung in Planung ist, kann ich im Augenblick nicht sagen. Aber ich glaube, wir haben an der Stelle ein ähnliches Interesse, zumindest mal die Diskussion zu führen.

Vorsitzender Marc Vallendar: Dann jetzt zur Beantwortung der vielen Fragen Herr Dr. Pickel. – Bitte!

Dr. Bernd Pickel (Präsident des Kammergerichts Berlin): Ich versuche es mal, und damit es nicht völlig durcheinandergeht, werde ich versuchen, das in drei Gruppen zu beantworten: Fragen, die die Vergangenheit betreffen, also was bei uns passiert ist; dann als Nächstes, was wir zur Schadensbeseitigung getan haben und was die Situation ist, und alles andere ist dann die Zukunft und die Zukunftseinschätzung. Teilweise haben mir Frau Smoltczyk und Frau Smentek beim letzten Punkt schon geholfen, aber vielleicht kann ich auch noch unsere Position sagen.

Ich fange mal mit der allerersten Frage an, weil sie für mich so typisch ist, und es ist eine Gretchenfrage: Wissen Sie, wie Emotet funktioniert? – Ich muss sagen, vor dem Vorfall wusste ich es nicht. Jetzt habe ich, glaube ich, durch diesen Vorfall eine ganze Menge gelernt. Aber das Grundproblem bleibt: Ich bin – irgendwer hat es auch gesagt; Sie, Frau Dr. Vandrey, glaube ich – Richter von Hause aus. Ich kann ganz gut beurteilen, was meine Kollegen juristisch machen.

Diese Situation mit dem Eigenbetrieb, so wie wir sie bisher hatten, das ist kein reiner Eigenbetrieb. Wir haben immer mit dem ITDZ zusammengearbeitet, und unsere Datenhaltung z. B. bei unserem Fachverfahren funktionierte ja auch über das ITDZ, und auch der E-Mail-Verkehr des Berliner Landesnetzes. Ich glaube, das Grundproblem an der Struktur, die wir hatten, ist eben, dass wir in der Situation, wie wir sind, IT nebenbei gemacht haben. Frau Fiedler weiß als Leiterin des ITDZ sicher mehr. Wir haben gute Kräfte gehabt, aber wir konnten in der Situation nicht ständig alle Anforderungen ordnungsgemäß so erfüllen – und dabei bleibe ich einfach –, wie es ein professioneller, großer Dienstleister schaffen kann. Deswegen kann ich auch die Frage, was wir getan haben, um uns vorbeugend an Emotet anzupassen, sehr schwer beantworten.

Ich habe, als ich es vorgefunden habe, gesehen, dass ein paar Strukturen bei uns nicht stimmten. Wir hatten z. B. eine behördliche Datenschutzbeauftragte, die zugleich stellvertretende Geschäftsleiterin ist und die das in einem ganz kleinen Umfang im Nebenamt gemacht hat. Da ist nicht viel passiert. Wir haben dann gerade wegen dieser großen IT-Verantwortung, die wir haben, einen Datenschutzbeauftragten, der ganz weitgehend freigestellt ist – und auch hier ist–, was zeigt, dass da einiges hineinkommt. Wir haben einen Informationssicherheitsbeauftragten bestellt, der auch bei dieser Frage – – ausgehende Daten beobachtet hat das ITDZ, also bei dem Vorfall – – Aber das Zusammenarbeiten war dann agil, auch zwischen den Mitarbeitern des ITDZ und z. B. unserem Sicherheitsbeauftragten. Der hat diesen Verdacht, der aus dem Haus von Frau Smentek kam, dass es Emotet war, nachweisen können, war eine große Hilfe und ist jetzt federführend in dem Prozess, dass wir externe Gutachter hingestellt haben.

Aber unser Grundproblem bleibt: Wir können uns nicht so auf IT konzentrieren und vor allem – das ist immer die Schwierigkeit – nicht durch eine Führung der Dienststelle, durch mich, so up to date bleiben in Entwicklungen, die gekommen sind, wie das ein normaler Dienstleister kann. Deswegen bin ich persönlich der Meinung, dass ein Eigenbetrieb keine große Zukunft hat, ohne dass ich deswegen jetzt über meine Mitarbeiter in der IT-Stelle den Stab brechen möchte. Wir haben das AV-System so konfiguriert, wie es ist. Wir haben in den letzten Jahren auch in dem Bereich irgendwie ausgerechnet, aber wir müssen einfach sehen: Es hat nicht gereicht.

Stichwort Vergangenheit: Was ist passiert? Was ist der Schaden? – Ich komme später bei der Frage der Zukunft darauf zurück, wie ich unsere Struktur da sehe. Daten abgeflossen? – Wir haben ein Gutachten von T-Systems, und der Entwurf eines Abschlussberichts liegt vor. Der wird aber noch diskutiert bei uns. Wir sind prinzipiell bereit – ich habe das auch immer gesagt –, die Erkenntnisse daraus zur Verfügung zu stellen, insbesondere Ihnen als Abgeordneten. Wir müssen allerdings eines sehen: Das ist ein Gutachten – das ist, glaube ich, von Ihnen angeführt worden –, das die Sicherheitsinfrastruktur betrifft. Wir müssen uns überlegen, in welcher Form und wie wir das weitergeben. Da steht z. B. auch drin, wie das Virus entdeckt wurde. Daraus kann jemand Schlüsse ziehen, der Viren herstellt, der Böses im Schilde führt, wie die IT des Kammergerichts aufgebaut war und wie sie aufgebaut sein soll. Wie sind Viren dann doch erkennbar? Wir haben hier vor, wenn wir das endgültige Gutachten haben – das hat auch unser Sicherheitsbeauftragter angemahnt –, über unseren Sicherheitsbeauftragten zu gucken, in welcher Form und wie wir das verfügbar machen können. Er hat schon angekündigt, er möchte da auch Empfehlungen des BSI zurate ziehen.

Deswegen sind Informationen, die ich jetzt habe, relativ vorläufig. Es spricht viel dafür – es ist eine klare Stelle in der Formulierung in dem Entwurf des Gutachtens –, dass es eine große Gefahr war und dass bei entsprechendem Vorsatz – so ist es dort beschrieben – mit Emotet und der eigentlichen Schadsoftware Trickbot, die dann nachgeladen wurde, die Möglichkeit bestanden hätte, große Datenbestände von uns zu exfiltrieren und Credentials abzugreifen. Es gibt keine Erkenntnisse darüber – auch in dem Gutachten –, dass es tatsächlich so einen Datenabfluss gegeben hat. Sie wissen alle – das ist auch irgendwie dokumentiert worden –, dass das Nachladen weiterer Schadsoftware durch die Trennung vom Internet verhindert wurde, dass unser altes System jetzt keine Netzanbindung mehr hat, dass es keine Verschlüsselungsaktivitäten gegeben hat.

Diese Firma, die dann dieses Gutachten erstellen soll nach unseren Vorstellungen über die Frage, wie wir diese Datenmigration sicher machen können, das ist ebenfalls T-Systems, weil die auf Empfehlung des BSI auch unseren Vorfall untersucht hat, deswegen kennt, was passiert ist, unsere Daten analysiert hat und dann eben auch sagen kann, wie man Herrn Waniek, Herrn Botschen vom CERT und letztlich Ihnen, Frau Smentek, eine Datenmigration anbieten und verantwortbar empfehlen kann. Aber da müssen wir noch die endgültigen Ergebnisse abwarten. Im Augenblick ist es so, dass wir davon ausgehen, dass es keinen Datenabfluss gegeben hat. Aber Genaues kann ich Ihnen dazu noch nicht sagen.

Die Frage ist vielfach gestellt worden: Wurden Backups erstellt, sind sie nutzbar? – Ja, es wurden Backups erstellt. Es gibt ein frühestes Infektionsdatum – das habe ich schon im Rechtsausschuss erwähnt –, das auf den 10. September deutet, tatsächlich bei uns wahrscheinlich deutlich später in der letzten September-Dekade anhand des T-Systems-Gutachtens festgestellt. Wir haben immer am letzten Freitag des Monats vollständige Backups hergestellt; das letzte vor dem Vorfall war der 30. August. Mit diesem Backup arbeiten wir.

Also Backups hat es gegeben. Das Problem unter Sicherheitsgesichtspunkten ist, dass es nicht so einfach ist, dieses Backup risikoarm einzuspielen und mit diesen Daten weiterzuarbeiten, weil man bei allen Prognosen, bei allen Wahrscheinlichkeiten nie sicher ist, dass dieses Datum nicht auch inkriminiert war. Wie gesagt: Von unserer Struktur her – das müssen wir einfach akzeptieren, und das muss ich auch irgendwie verantworten – müssen, selbst wenn dieser Emotet-Vorfall nicht jetzt zum Tragen gekommen ist, sich der IKT-Bereich oder das CERT Gedanken darüber machen, ob es nicht sonstige Infektionen gegeben haben könnte.

Ich komme zurück auf die Frage: Wissen Sie, wie Emotet funktioniert? – Eingeschränkt. So ähnlich ist es bei mir auch mit den Kenntnissen über die Beurteilung der Wirksamkeit von AV-Software, nach der ich gefragt worden bin von Ihnen, glaube ich, Herr Kohlmeier. Mein Eindruck ist – und das finde ich auch in dem Entwurf des Gutachtens von T-Systems bestätigt –, dass signaturbasierte AV-Systeme bei Viren wie Emotet Grenzen haben, dass es allein nicht mehr ausreicht und man sich darauf nicht verlassen kann. Es gibt andere Möglichkeiten, statt die üblichen Pattern, also die Bilder dieses Virus auszutauschen, sogenannte Hashwerte abzugleichen, die, sage ich jetzt mal so, das Verhalten des Virus betreffen.

Nach dem, was mir meine IT-Stelle gesagt hat und was ich auch sonst bestätigt gefunden habe, gibt es teilweise Schwierigkeiten – die aber im ganzen Landesnetz sind –, dass die entsprechenden Server nicht im Bereich der EU liegen. Vielleicht muss man da noch weitere Verteidigungsmöglichkeiten in Erwägung ziehen. Ich glaube aber – und das ist etwas, was

Sie, Frau Smoltczyk, gesagt haben –, dass das insgesamt ein Gesamtproblem der Berliner IT oder überhaupt der IT in Deutschland ist. Es hat ja auch noch andere prominente Emotet-Opfer gegeben, und ich glaube, diese Diskussion, was man noch tun kann, was man noch verstärken kann, kann nicht nur in Bezug auf das Kammergericht geführt werden, sondern muss bundesweit geführt werden.

Für uns ist wichtig, dass jetzt nicht jemand – – Wie gesagt, ich mache die Mitarbeiter nicht schlecht, aber es kann nicht sein, dass eine von Hunderten Behörden oder Gerichten – da können wir keinen großen Player spielen. Das muss an anderer Stelle von der IKT-Steuerung, von den großen Dienstleistern entschieden und uns dann vorgegeben werden. Insofern hoffe ich sehr, dass man bei allen Schwierigkeiten, die es durch diesen Vorfall bei uns gegeben hat, nicht auf so eine Klischee-Ebene zurückkommt und sagt: Ach, bei Gerichten ist alles alt, und die haben von Technik sowieso keine Ahnung, und uns, den anderen Bereichen, kann das nicht passieren! – Je mehr ich mit Leuten diskutiert habe, die hohe IT-Erfahrung, hohe IT-Kompetenz haben, bei unserem Dienstleister – ich habe auch Gespräche mit Dataport gehabt –, je mehr hört man: Bei Infektionen – was hier auch von Ihnen gesagt worden ist – gibt es keinen perfekten Schutz. – Aber wir müssen uns einfach gemeinsam anstrengen, dass wir die kompetenten Leute zusammenbringen, die das unterstützen. Aber wir werden das nicht alleine können.

Ich komme noch mal auf das Thema Vergangenheit: Was haben wir gemacht, um die Mitarbeiter fortzubilden, zu unterweisen in einem sicheren Umgang mit IT? – Wir haben Schulungen im Kammergericht gemacht, die sehr gut besucht waren, zu den allgemeinen Gefährdungen mit Hackern. Wir haben sie zu wenig und zu selten gemacht. Wir haben nach dem Vorfall – da kann man immer sagen, wenn man aus dem Rathaus kommt, ist man schlauer; das ist einfach so – eine neue Veranstaltungsserie – übrigens nicht nur für uns, sondern für die ganze ordentliche Gerichtsbarkeit – aufgelegt und machen sie verpflichtend.

Dokumente, die Mitarbeiter unterschreiben müssen, gibt es in der Justiz relativ viele. Wir haben recht viel Papier. Wir müssen uns jetzt aber noch gemeinsam überlegen – das gehört zu diesem neuen Sicherheitskonzept –, wie wir die Mitarbeiter wirklich erreichen, dass sie das ernst nehmen. Ein großes Bedürfnis ist bei unseren Mitarbeitern nicht erst seit dem Vorfall da, sondern überall. Wir haben z. B., gerade weil wir auch Kommunikation zwischen häuslichen und dienstlichen Rechnern haben – was aus meiner Sicht keine Spezialität der Gerichte ist, es wird viele Bereiche in der Berliner Verwaltung geben, wo sich jemand von zu Hause mal eine Mail in den Dienst hineinschickt; alles andere ist, glaube ich, Illusion –, gemerkt, dass ein großes Bedürfnis bei den Mitarbeitern im Haus bestand und haben sie da auch unterstützt, indem wir spezielle Analyse-Sticks, die auf Emotet geeicht waren, zur Verfügung gestellt haben. Wir haben dann gesagt: So könnt ihr auch eure häuslichen Rechner schützen, und bitte teilt uns vertraulich auf einer informellen Basis mit, was ihr dabei gefunden habt, damit wir reagieren können! – Das ist aus meiner Sicht gut angenommen worden.

Ich möchte ganz kurz noch einmal zur Schadensbeseitigung kommen – da kann ich nur unterstreichen, was insbesondere Dr. Vandrey gesagt hat, aber auch ein paar andere Kollegen –: Es ist nicht so, dass die Arbeitsfähigkeit des Kammergerichts nicht hergestellt war. Es ist auch nicht so, dass seit dem Vorfall nichts getan wurde, um die Arbeitsfähigkeit herzustellen. Sie haben, Herr Schlüsselburg, auch die Erreichbarkeit für Rechtsanwälte erwähnt. Da war ein Vorteil, dass es im Zusammenhang mit der Vorbereitung der E-Akte ein sehr gutes, ein sehr

schnell umsetzungsfähiges Notfallkonzept gab. Wir haben die Erreichbarkeit über das besondere elektronische Anwaltspostfach, das sogenannte „beA“, mit dem Anwälte anders als mit E-Mails rechtswirksam mit den Gerichten korrespondieren können. Das war praktisch ab dem ersten Tag verfügbar, und nach zwei oder drei Tagen konnte es bei uns auch im Kammergericht bedient werden, und wir mussten nicht zu einem anderen Bereich laufen.

Ich habe schon dargestellt, dass wir bis auf ein kleines Delta zwischen den Tagen unmittelbar um den Virusbefall die alten Daten sichtbar machen sollten. Wir haben es auch geschafft über das ITDZ – im Zusammenwirken. Unser Fachverfahren AULAK deckt etwa 80 bis 85 Prozent unserer Rechtsprechungsbereiche ab – daneben haben wir überwiegend nur noch Strafrecht –, dass man das verfügbar machen konnte. Wir haben es den Kollegen auch ermöglicht – – Die alten Rechner sind stehen geblieben. Dort, wo sie beim LKA – – Das ist hier auch eine Frage gewesen: Ist eine Strafanzeige gestellt worden? – Das habe ich schon im Rechtsausschuss bejaht. Ja, es gibt intensive Ermittlungsarbeit der Polizeibehörden, erst vom LKA, und jetzt hat das BKA übernommen.

Wir haben alle Rechner, die normale Bürokommunikationssoftware unterstützen, aber – und das ist unser großes Problem – wir haben eben kein internes Netz. Ich habe ja gesagt, das ist eben diese Konsequenz, wenn wir sagen: Wir wollen das alte, möglicherweise kontaminierte Netz und das neue, das wir im Augenblick noch notfallmäßig beim ITDZ haben, nicht vermischen. – Dann haben wir eben einfach die Situation, dass wir keine Netzkommunikation haben, und das ist vielleicht das, was uns rückblickend, Herr Schlüsselburg, in den letzten Monaten am meisten behindert hat.

Es ist eben dadurch alles schwierig, und wenn es nur darum geht, Kollegen zu einer Adventsfeier einzuladen, die Auszubildenden darauf hinzuweisen, dass es eine Veranstaltung für sie mit dem Abgeordnetenhaus gibt, dass die Kollegen in den Senaten sich zur Vorberatung einer Sache verabreden wollen. Wenn man an E-Mail gewohnt ist – und das hat entgegen manchen Vorstellungen auch bei den Gerichten längst Einzug gehalten und dominiert doch die Arbeit –, dann ist es eben sehr schwierig, darauf zu verzichten.

Mit den analogen Newslettern und Umläufen haben wir versucht, was möglich ist. Wir mussten es irgendwie kompensieren, so ähnlich, wie wir manchmal auch kompensieren müssen, dass es eben nicht so schön aussieht. Nicht nur wir sind betroffen, die ganze Berliner Justiz ist betroffen, und da muss man es manchmal hinnehmen, dass es einfacher ist, etwas handschriftlich zu kommentieren, durchzustreichen und zu ändern in einem Schreiben, als jetzt zu warten. Ich hatte Ihnen ja gesagt, dass wir im Augenblick – und das war auch eine Frage, die Sie hatten: Nach dem Rechtsausschuss, was hat sich verändert? – mehr Geräte im provisorischen Betrieb haben, als wir damals hatten – zum Zeitpunkt des Rechtsausschusses. Da hatten wir, glaube ich, 30, jetzt sind wir bei 60. Es hat eine gewisse Entlastung gegeben. Richter leben von der Recherche, viele recherchieren vor allem in Juris und in Beck-Online, und Datenbanklizenzen hatten wir den Kollegen schon immer zur Verfügung gestellt. Wir haben jetzt praktisch eine Vollausstattung mit WLAN bei uns im Gericht, sodass die Richter recherchieren können. Allerdings können sie natürlich ihre Recherche nicht unmittelbar in das System übertragen.

Dieses System, das wir jetzt haben, bedeutet aber, dass sich viele noch einen PC teilen müssen. Wir haben – auch das hat sich geändert – PCs und Notebooks beschafft. Sie stehen im Keller. Wir sind jetzt bei den letzten Schritten, die gemeinsam mit dem ITDZ und unter Rücksprache mit Herrn Botschen von CERT und Herrn Waniek von der IKT-Steuerung auf einem sicheren Weg im Netzwerkmanagement des ITDZ anzuschließen. Ich hoffe, dass wir dann – auch das war eine Frage – herauskommen jetzt in den nächsten Tagen hoffentlich – Ende im Januar –, dass wir diese Grundarbeitsfähigkeit wiederherstellen. Die bedeutet, dass jeder seinen eigenen PC wieder hat, jeder wieder an das Internet kommen kann, recherchieren kann und dass dann das allermeiste abgedeckt sein wird.

Das bringt mich auch zu der Frage – wir sind jetzt schon so langsam in der Zukunft –: Was bleibt dann eigentlich noch als Potenzial für einen Eigenbetrieb? Und wie kann man es verantworten – das war auch eine Frage –, überhaupt darüber nachzudenken, nachdem unser bisheriges System mit solchen Folgen angegriffen wurde? – Es gibt eine Menge von Verfahren, die wir vorgefunden haben, bei denen es mir teilweise verzichtbar erscheint, sie im Netz betreiben zu lassen. Ein Beispiel: Wir als Kammergericht steuern auch das Bibliothekswesen der ordentlichen Gerichtsbarkeit, die Beschaffungs- und Bestellvorgänge. Dazu brauchen Sie ein Verzeichnis, welche Bücher es gibt. Auch in den örtlichen Bibliotheken ist es wichtig, dass die irgendwelche Verzeichnisse haben. Das ist eines dieser berühmten alten Programme, die das ITDZ bestimmt nicht mehr hosten will und hosten soll. Man muss bei vielem über Stand-alone-Lösungen oder über kleine separate Netze nachdenken, zum Beispiel für die Bibliothek. Ähnliche Überlegungen muss man auch dort anstellen, wo es um Schulungskonzepte geht.

Zu dieser Frage: Was heißt produktiver Betrieb? – Das ist im Grunde alles, was wir außerhalb solcher Anwendungsbereiche zum täglichen Arbeiten brauchen, wo eben die Urteile gespeichert sind. Ich hatte vor der Fragerunde schon erzählt, wie wir unsere Verwaltung betreiben. Das gehört nicht mit hinein. Aber wir haben zum Beispiel häufiger Pilotierungsverfahren für die elektronische Akte, die wir vorbereiten, Testverfahren und Ähnliches. Darüber kann man nachdenken. Ich muss sagen, dass ich im Augenblick noch nicht viel darüber nachdenke. Im Augenblick denken wir darüber nach, wie wir unsere Grundarbeitsfähigkeit wiederherstellen und wieder zu normalen Arbeits- und Kommunikationsprozessen kommen.

Ich will noch mal zu den grundlegenden Fragen für die Zukunft kommen. § 23 AGGVG ist angesprochen worden, Änderung des AGGVG. Ich bin im Rechtsausschuss auch schon mal danach gefragt worden. Ich glaube, man muss einfach sehen: Richterinnen und Richter haben – ich will jetzt gar nicht so hoch greifen – nicht nur nach dem AGGVG das Recht, zu Hause zu arbeiten, sondern es ist auch einfach eine Notwendigkeit. Sie können ein umfangreiches Urteil nicht immer schreiben, wenn Sie in einem Bürostress sind. Es ist manchmal notwendig – das ist keine Erfindung von mir, sondern auch vom Bundesverfassungsgericht –, dass man sagt, man recherchiert mal in Ruhe zu Hause, gerade bei komplexen Sachen wie in einem Oberlandesgericht.

Ich glaube, es hilft weniger, jetzt am Gesetz etwas zu ändern, sondern wir müssen das, was wir den Kollegen bieten können, verändern. Wir haben deswegen 150 Laptops gekauft, das reicht für eine Vollausstattung der Richter. Das Entscheidende ist – und das wäre der erste Schritt, wo wir dann weiter wären als vorher –, dass wir die mit einer Mappingfunktion an das Netz bekommen. Dann kann eine Richterin, ein Richter, die oder der im Gericht zum Beispiel

begonnen hat zu arbeiten, dort auch recherchiert hat – das ist noch nicht die volle Onlineverfügbarkeit –, einfach dieses Gerät, das keine Anschlüsse nach außen hat, wo sich diese Frage USB-Stick gar nicht stellt, mit nach Hause nehmen, kann dann zu Hause weiterarbeiten und ihre Ergebnisse auch wieder mit dem Gerät zurückbringen. Also für mich ist eigentlich die Zukunft, dass das, was Sicherheitsrisiken bringt, was, wie hier ja auch gesagt wurde, mittelfristig so überhaupt nicht mehr vertretbar ist, gar nicht mehr notwendig wird. Das ist eigentlich das, was wir jetzt anstreben.

Auch noch mal zu dieser Frage der Zentralisierung und Standardisierung: Soll die Justiz sich jetzt noch abgrenzen von dem Bereich der allgemeinen Verwaltung? Wie soll die Kommunikation laufen? – Ich weiß, wir sind nicht der einzige Eigenbetrieb, wir sind auch mit den Kollegen aus anderen Gerichten, Gerichtsbarkeiten, die teilweise Eigenbetrieb haben, in der Diskussion. Ich persönlich möchte in einer Gerichtsbarkeit, die ich leite, keinen Eigenbetrieb mehr haben, also keinen Eigenbetrieb, in dem wirklich sensible Daten vorhanden sind, wo man einen Ausfall, wie wir ihn hatten, nicht haben kann. Vielleicht sehen das andere anders. Ich glaube, unsere Zukunft liegt darin – wie überhaupt die Zukunft in der IT –, dass wir standardisieren und Kompetenzen bündeln. Deswegen finde ich es gut, dass jetzt – wir haben immer kooperiert mit dem ITDZ – der Schulterschluss mit dem ITDZ enger wird.

Vorsitzender Marc Vallendar: Herr Dr. Pickel!

Dr. Bernd Pickel (Präsident des Kammergerichts Berlin): Darf ich noch ganz kurz etwas anfügen? – Was für mich trotzdem noch eine Chance hat, ist – weil wir eben auch verfassungsrechtliche Anforderungen haben –, dass wir uns perspektivisch zu Justizverbünden zusammenschließen. Das wäre es.

Ich würde dann zurückgeben, weil Sie mich schon gemahnt haben – mit Recht. Ich hoffe, dass ich die meisten Fragen beantwortet habe. Darf ich noch ganz kurz die finanziellen Auswirkungen betonen? – [Zuruf von Dr. Petra Vandrey (GRÜNE)] – Das wäre vielleicht einfacher für uns, weil unsere Haushaltsbeauftragte gerade einen Bericht schreibt. Es ist sehr schwer zu quantifizieren. Gerade im IT-Bereich haben wir geringe Innovationszyklen. Einen großen Teil der Rechner, die wir jetzt beschafft haben, hätten wir z. B. auch für den Windows-10-Release-Wechsel beschafft. Da konnten wir ein paar Sachen parallelisieren. Also das würden wir dann vielleicht noch mal zusammenfassend berichten.

Vorsitzender Marc Vallendar: Vielen Dank für Ihre Stellungnahme, Herr Dr. Pickel! – Wir sind jetzt schon 40 Minuten über unserer regulären Ausschusszeit. Herr Kohlmeier hatte sich noch gemeldet. – Bitte!

Sven Kohlmeier (SPD): Wir lernen das schon für das nächste Jahr, wo wir länger sitzen. – Die erste Frage an den Senat: Bekommen wir das T-Systems-Gutachten, im Zweifel im Geheimraum oder wie auch immer? Das können Sie ja klassifizieren. Das muss der Senat beantworten. Ansonsten müssen wir ihn anderweitig anfordern.

Die zweite Frage ist: Herr Pickel hat gesagt – das hat mich irritiert –, dass die Server, die genutzt werden, nicht in der EU liegen. Ist die Aussage so zutreffend? Auch die Frage geht an den Senat. Herr Pickel sagte während seiner Ausführungen, dass die Schwierigkeit sei – das wurde auch von der Datenschutzbehörde gehört –, dass die Server ja nicht in der EU liegen

würden. Das hat mich verwundert, weil ich bisher davon ausging, dass unsere Daten zumindest in Deutschland oder in Europa gespeichert werden. Vielleicht kann man die Auskunft nachreichen.

Dr. Bernd Pickel (Präsident des Kammergerichts Berlin): Es wird ja nicht genutzt. Es gab eine Empfehlung – wenn ich das jetzt noch mal erläutern darf, von unserem – – [Stefan Ziller (GRÜNE): Kann man das schriftlich nachreichen?] – Ja, ja.

Vorsitzender Marc Vallendar: Entschuldigung! Ich habe noch die Sitzungsleitung. Wir haben jetzt noch ein paar weitere Wortmeldungen. Die Frage, die sich jetzt stellt, ist: Wir sind jetzt schon lange über die Sitzungszeit hinaus. Wir können es vertagen und es so machen, dass die Fragen schriftlich eingereicht werden und dann von Herrn Dr. Pickel vom Kammergericht nach Möglichkeit dann an den Ausschuss beantwortet werden. Das würde ich jetzt vorschlagen, es sei denn, es gibt jetzt noch etwas Dringliches, was unbedingt sofort sein müsste. Aber wir sind weit über die Sitzungszeit hinaus. Deswegen würde ich vorschlagen, dass wir den Tagesordnungspunkt vertagen. – [Zurufe von Sven Kohlmeier (SPD) und Dirk Stettner (CDU)] – Das finden alle gut? – Dann verfahren wir so. – Vielen Dank, Herr Dr. Pickel, dass Sie da waren!

Punkt 5 (neu) der Tagesordnung

Vorlage – zur Beschlussfassung – Drucksache 18/1850 **Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen der Berliner Verwaltung (Onlinezugangsgesetz Berlin – OZG Bln)**	0104 KTDat Haupt

Vertagt.

Punkt 6 (neu) der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.