Präsident Hendrik Hering:

Für die Landesregierung antwortet Herr Staatssekretär Stich.

Randolf Stich, Staatssekretär:

Sehr geehrter Herr Präsident, meine sehr geehrten Damen und Herren Abgeordnete! Zu den Fragen kann ich wie folgt berichten.

Ich komme zunächst zu Frage 1: Angriffe auf den Deutschen Bundestag 2015, die CDU-Zentrale in Berlin im Mai 2016, Cyberattacken auf den Parteivorstand der US-Demokraten, auch die Attacken auf das Wahlkampfteam von Emmanuel Macron haben innerhalb der letzten beiden Jahre doch für ein erhebliches öffentliches Aufsehen gesorgt. Die Beispiele zeigen, die Gefahr einer Einflussnahme auf die Bundestagswahl im September muss als durchaus realistisches Szenario eingestuft werden.

Zur Absicherung sowohl der Politik als auch der Verwaltung verfolgt die Landesregierung eine ganzheitliche Informationssicherheitsstrategie. Diese setzt zum einen auf die Absicherung der zentralen IT-Infrastrukturen, aber auch zum anderen auf den zentralen Betrieb gerade geschäftskritischer Infrastrukturen im Landesbetrieb Dateninformation, also in diesen abgesicherten IT- Infrastrukturen. So wurde im Fall der staatlichen Wahlserver entschieden, dass der Zugang zu diesen auf Landesseite nur über das rheinland-pfälzische Landesnetz, das rlp-Netz, erfolgen kann und auch die Wahlserver selbst im Rechenzentrum des LDI betrieben werden.

Von besonderer Bedeutung ist hierbei das flächendeckende, hoch sichere und hoch verfügbare Rheinland-Pfalz-Netz. Das ist das gemeinsame Datennetz sowohl der Landesverwaltung, der Landesregierung als auch des Landtags. Lange vor Bekanntwerden dieser Angriffsszenarien hat die Landesregierung erkannt, wie wichtig eine eingehende Überprüfung der Konzepte für Schutz und Sicherheit der Daten durch externe Gutachter und externe Auditoren ist.

Die gesamte technische Umsetzung und der Betrieb des Rheinland-Pfalz-Netzes wurden durch das Bundesamt für Sicherheit in der Informationstechnik im Rahmen einer Zertifizierung untersucht. Noch im April diesen Jahres – also ganz aktuell – wurde durch das BSI bzw. von ihm zertifizierte Auditoren auf der Basis von IT-Grundschutz noch einmal eine Reauditierung durchgeführt und das bestehende sogenannte ISO 27001-Zertifikat – das ist das IT-Grundschutz-Zertifikat – erneuert. Damit bestätigen uns die externen Gutachter, die IT-Basisinfrastruktur in Rheinland-Pfalz, das rlp-Netz, ist eine sichere Basis für die Verarbeitung, aber auch für die Speicherung der Daten der rheinland-pfälzischen Landesregierung, der Landesverwaltung und auch des Landtags.

Rheinland-Pfalz ist – das möchte ich noch einmal betonen, das haben wir an vielen Stellen schon gesagt – das zweite Bundesland, das überhaupt diesen Nachweis erbringen kann und erbringen konnte. Auch das rlp-Netz ist regelmäßig Ziel von Cyberangriffen; im Schnitt haben wir pro Tag zwei bis ungefähr fünf schwerwiegende Angriffe festzustellen, die sich teilweise in die Angriffsländer zurückverfolgen lassen. Diese Angriffe werden von den Angriffserkennungssystemen des LDI erkannt und von der dort angesiedelten professionellen CERT-Kopfstelle – das ist das sogenannte Computer Emergency Response Team – professionell bearbeitet.

Da die Cyberangriffe immer gezielter ausgeführt werden und ihre Häufigkeit stetig zunimmt, hat die Landesregierung weitere Maßnahmen zur Erhöhung der Informationssicherheit eingeleitet, unter anderem wird derzeit ein einheitliches verwaltungsübergreifendes Informationssicherheitsmanagement in der Landesverwaltung aufgebaut. Außerdem werden IT-Informationssicherheitsstrukturen in der Landesverwaltung unter Berücksichtigung entsprechender Empfehlungen des BSI und auf der Grundlage einer Empfehlung des IT-Planungsrats im Moment eingeführt und fortlaufend optimiert. Durch diese Maßnahmen seien sie technischer, aber auch – genauso wichtig – organisatorischer Struktur, werden auch die staatlichen Wahlserver vor Angriffen und Manipulationen hinreichend geschützt.

Zu Frage 2: Spätestens seit der US-Wahl im November 2016 und der Präsidentschaftswahl in Frankreich, die mit Cyberattacken und unwahren Behauptungen in sozialen Medien einhergingen, gilt die Streuung von Fake News und die Verunstaltung von Internetauftritten, das sogenannte Website-Defacement, als ein übler Auswuchs von sozialen Netzwerken. Meistens soll mit Hilfe von Fake News die politische Diskussion verschoben werden, oder es soll gezielt Angst und Hass gegenüber bestimmten Personengruppen verbreitet werden.

Laut Medienberichten – das ist ein sehr interessanter Umstand – waren gezielte politisch motivierte Falschmeldungen in den Wochen vor der US-Wahl auf Facebook erfolgreicher als Meldungen etablierter Medien. Beim sogenannten Website-Defacement werden die Inhalte von politischen Webseiten mutwillig verändert und politische Botschaften sowie diffamierende und verleumderische Inhalte auf den angegriffenen Webseiten hinterlegt.

Auch in Rheinland-Pfalz wurden dem rheinland-pfälzischen Verfassungsschutz in den letzten Wochen Fälle von Webseiten-Defacements einiger rheinland-pfälzischer Parteiverbände bekannt. Vor diesem Hintergrund ist immer zu befürchten, dass auch im Rahmen der Bundestagswahl entsprechende Angriffe zu verzeichnen sind.

Im Hinblick auf die anstehende Bundestagswahl sensibilisiert der rheinland-pfälzische Verfassungsschutz die Landtagsfraktionen in einer Informationsveranstaltung, die demnächst zu den Folgen von Fake-News und Webseiten-Defacement stattfindet. Er stellt selbstverständlich – das ist das zentrale Element – auch Maßnahmen zum Schutz vor entsprechenden Attacken dar.

Im Hinblick auf die bekannt gewordenen Website-Defacements mehrerer rheinland-pfälzischer Parteiverbände wurde seitens des Verfassungsschutzes umgehend Kontakt zu den betreffenden Parteiverbänden aufgenommen. Die Verantwortlichen der Web-Präsenzen wurden über die erfolgten Sicherheitsvorfälle informiert, und es wurden ihnen auch Maßnahmen zur Behebung der Sicherheitsvorfälle aufgezeigt.

Zu Frage 3: Ransomware, also Verschlüsselungstrojaner, gefährden weltweit Unternehmen, Behörden und auch Gesundheitseinrichtungen. Die meisten Ransomware-Angriffe sind schlichtweg und einfach auf das Betriebssystem Microsoft-Windows gerichtet, weil es das am weitesten verbreitete ist. Aber auch andere Betriebssysteme sind nicht sicher. Wir haben heute genauso bei Android-Geräten, bei Mac OS oder bei Linux-Server entsprechende Vorfälle zu berichten.

Obwohl viele Unternehmen und Behörden umfangreiche Sicherheitsmaßnahmen eingeleitet haben, haben wir nach wie vor eine große Zahl von Infektionen. Gründe hierfür sind oft fehlende oder veraltete Sicherheitspatches, das heißt Sicherheitsupdates, aber auch schwache Administrator-Passwörter und Ähnliches. Hier kann es zu enormen Schäden für die betroffenen Unternehmen und Behörden kommen.

Wir haben jetzt einen sehr spektakulären Fall einer dänischen Reederei, die über Wochen nicht mehr in der Lage war, ihre Logistiksysteme entsprechend einzurichten. Es wurde ein Schaden von 200 bis 300 Millionen Dollar durch einen einzigen Verschlüsselungstrojaner-Angriff prognostiziert.

Um entsprechende Angriffe zu verhindern, hat die Landesregierung umfangreiche technische und organisatorische Maßnahmen getroffen, um die Eintrittswahrscheinlichkeit eines Ransomware-Vorfalls im Rheinland-Pfalz-Netz zu minimieren. So werden im zentralen E-Mail-Eingang des Rheinland-Pfalz-Netzes bekannte Typen von E-Mail-Anhängen mit ausführbaren Inhalten konsequent und sofort gelöscht. Ich nehme an, jeder von Ihnen hat schon einmal eine entsprechende Mail mit der Meldung des LDI bekommen, dass entsprechender Anhang herausgenommen wurde. Hinter diesen Anhängen verstecken sich dann in der Regel entsprechende Angriffsszenarien.

Die im LDI betriebenen Wahlserver haben selbst keine aktive Zugriffsmöglichkeit auf das Internet. Das verringert zusätzlich die Wahrscheinlichkeit eines entsprechenden Angriffs, weil bei einer Infektion in der Regel der eigentliche Schadcode erst über das Internet nachgeladen wird, sodass man damit auch noch einmal zusätzlich Sicherheit schafft.

Der Betrieb der gesamten staatlichen Infrastruktur steht im Wahlserver-Bereich in der zentralen zertifizierten Umgebung. Wir haben hier die notwendigen organisatorischen, strukturellen und personellen Maßnahmen getroffen. Zudem wurden die Wahlserver im LDI im Vorfeld der Wahlen einem Penetrationstest unterzogen und weitere Härtungsmaßnahmen abgeleitet. Von daher können wir im Rahmen der staatlichen Infrastruktur von einem hohen Sicherheitsniveau ausgehen.

Vielen Dank.

Präsident Hendrik Hering:

Eine Zusatzfrage des Herrn Abgeordneten Schäffner.

Abg. Daniel Schäffner, SPD:

Herr Staatssekretär, vielen Dank für die Ausführungen zu dem ganzheitlichen Sicherheitssystem, das im Land die EDV schützt. Meine Frage geht in die Richtung, wie wir den Kommunen helfen, die auch betroffen sein können. Was bietet das Land den Kommunen an Unterstützung zur Sicherheit ihrer EDV-Systeme an?

Randolf Stich, Staatssekretär:

Herzlichen Dank. Das Land steht auch in dem Bereich an der Seite der Kommunen. Wir haben schon vor vielen Jahren gemeinsam mit den Kommunen eine Netzinfrastruktur aufgebaut, die jetzt von kommunaler Seite eigenständig weitergeschrieben wird. Das ist das sogenannte Kommunalnetz, das auch verschlüsselt läuft.

Wir haben jetzt gerade, nachdem wir im Bereich der IT-Sicherheit seit vielen Jahren eine enge Kooperation haben, die nächste Stufe gestartet. Das heißt, Anfang des Jahres ist das sogenannte CERT-kommunal, das Computer Emergency Response Team-kommunal, geschaffen worden, das in enger Zusammenarbeit mit dem staatlichen CERT arbeitet.

Sämtliche Sicherheitsmeldungen, Sicherheitswarnungen, aber auch Konzepte zur Erhöhung des Sicherheitsniveaus, die staatlichen Behörden gegeben werden, werden auch dem CERT-kommunal weitergeleitet, sodass hier auch weiterhin ein Schritt gegangen wird, um ein einheitliches Sicherheitsniveau festzustellen. Das heißt, auch die staatlich-kommunale Zusammenarbeit im Sicherheitsbereich ist auf einem sehr hohen Niveau. Wir geben den Kommunen auch immer aktuelle Stände.

Präsident Hendrik Hering:

Eine Zusatzfrage des Herrn Abgeordneten Junge.

Abg. Uwe Junge, AfD:

Vielen Dank, Herr Präsident. Herr Staatssekretär, herzlichen Dank für die Ausführungen. Ich habe noch eine Nachfrage zu Frage 2. Sie haben in erster Linie dargestellt, welche physikalischen Maßnahmen wir treffen, um Angriffe zu vermeiden. Die Frage 2 bezieht sich aber in erster Linie aber auch auf Desinformationskampagnen – so steht es hier – und Propaganda. Ich meine, Propaganda machen wir alle.

(Zuruf des Abg. Martin Haller, SPD)

Propaganda ist Werbung über unsere politischen Überzeugungen.

– Nein, schauen Sie einmal genau nach, was das heißt.

Die Frage ist, um es zu versachlichen: Welche Maßnahmen treffen Sie, wenn Sie die Dinge tatsächlich umsetzen wollen, um bei der Bewertung die Neutralität zu wahren? Was ist Desinformation, und was ist Propaganda? Das ist relativ schwierig und eine Grauzone. Wie halten Sie die Neutralität ein?

Randolf Stich, Staatssekretär:

Bei den Webseiten-Defacements kann man deutliche Veränderungen von Webseiten feststellen. Das heißt, in der Regel werden im Rahmen von Angriffen Netzwerkordner auf den Servern untersucht. Es werden zusätzliche falsche Inhalte eingebracht. Das lässt sich bei einer Untersuchung recht schnell erkennen. Es ist so, dass Facebook in der Zwischenzeit sehr eng in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik auch verstärkt die Konten untersucht.

Es wird bewusst – das wird immer wieder in den Meldungen hervorgehoben – erst einmal keine Inhaltskontrolle durchgeführt, sondern man sucht anhand eines Posts gleichbleibende Inhalte in einer hohen Frequenz. In einer hohen Frequenz von Meldungen identifiziert man auffällige Accounts und stellt fest, dass hinter den Accounts in

der Regel ein Bot sitzen muss, das heißt ein Roboter, der entsprechende Informationen gibt. Diese werden dann gezielt untersucht.

Das heißt, dieses Untersuchungsszenario in den sozialen Netzwerken, das Facebook in Absprache mit dem BSI durchführt, wird anhand einer mechanischen Kontrolle, die aber sehr verlässlich eine mechanische Antwortwahrscheinlichkeit hinten dran vermuten lässt, durchgeführt. Der Schritt, der eine Auffälligkeitskontrolle durchführt, ist keine inhaltliche Bewertung, sondern eine technisch-mechanische Bewertung, die dazu führt.

Präsident Hendrik Hering:

Eine Zusatzfrage des Herrn Kollegen Haller.

Abg. Martin Haller, SPD:

Herr Staatssekretär, Sie haben das Thema Defacement angesprochen, und dass auch Parteiverbände in Rheinland-Pfalz betroffen waren. Es würde uns doch interessieren, welche es waren. Wie muss ich mir das konkret vorstellen? Können Sie irgendein Beispiel nennen?

Randolf Stich, Staatssekretär:

Das waren Angriffsszenarien, die im Rahmen des Verfassungsschutzverbundes aufgefallen sind. Das wurde dem rheinland-pfälzischen Verfassungsschutz entsprechend gemeldet. Es waren Verbände einer Partei. Es waren CDU-Parteiverbände, die betroffen waren. Die betroffenen Parteiverbände wurden, nachdem das dem Verfassungsschutz bekannt wurde, umgehend informiert. Mit den Verantwortlichen wurde Kontakt aufgenommen. Die Betreiber der entsprechenden Infrastruktur wurden darauf hingewiesen, dass ein Angriffsszenario vorliegt. Sie wurden auch darauf hingewiesen, wie man das beheben kann.

Präsident Hendrik Hering:

Eine Zusatzfrage des Herrn Kollegen Wäschenbach.

Abg. Michael Wäschenbach, CDU:

Herr Staatssekretär, auf welche Art und Weise informiert die Landesregierung die Wirtschaft, die auch von vergleichbaren Angriffen wie in der Politik getroffen werden kann, zum Beispiel im Rahmen der Industriespionage oder Proliferation? Welche Wege geht die Landesregierung?

Randolf Stich, Staatssekretär:

Der rheinland-pfälzische Verfassungsschutz hat in dem Bereich einen klaren Beratungsauftrag, der sich auch aus dem Verfassungsschutzgesetz ergibt. Dieser wird in vielfältiger Weise wahrgenommen.

Zum einen haben wir in den letzten Jahren umfassende und vielfältige Informationsveranstaltungen gemeinsam mit den Industrie- und Handelskammern im Bereich der Sicherheit und der Spionage durchgeführt. In diesen wurden Unternehmen gezielt darauf hingewiesen, in welchem Umfang Angriffsszenarien im Bereich der Wirtschaftsspionage zu erwarten sind und welche Maßnahmen dagegen ergriffen werden können.

Wenn Unternehmen gezielt auf den Verfassungsschutz zukommen und eine Information möchten über die Wahrscheinlichkeit von Angriffen, die Erkennbarkeit von Angriffen, aber auch die Art und Weise, wie so etwas behoben oder eine Vorbeugung durchgeführt werden kann, führen wir gern mit diesen Unternehmen unmittelbare Einzelgespräche, in denen wir sie entsprechend sensibilisieren, aber auch aufzeigen, wie eine gute und gezielte Absicherung erfolgen kann.

Das geht im Endeffekt von organisatorischen Maßnahmen auf der einen Seite bis hin zu technischen Schutzszenarien auf der anderen Seite. Da haben wir entsprechend gut ausgebildete Mitarbeiter im Bereich des Verfassungsschutzes, die sehr umfassend beraten können. Das ist ein Angebot, das gern wahrgenommen wird.

Präsident Hendrik Hering:

Eine Zusatzfrage des Herrn Abgeordneten Schweitzer.

Abg. Alexander Schweitzer, SPD:

Ich möchte einmal nachfragen, was die Frage der Angriffe auf Webseiten von Parteiverbänden oder die Gliederung von Parteien angeht. Kann man davon ausgehen, dass die aufgetretenen Fälle – Sie haben die Partei CDU genannt – von ausländischen Hackern kommen, oder kommen diese aus dem Land selbst? Welchen Ermittlungsstand hat der Verfassungsschutz?

Randolf Stich, Staatssekretär:

Die Fälle, die jetzt bekannt geworden sind, und die aktuell da waren, ließen sich ins Ausland zurückverfolgen.

Präsident Hendrik Hering:

Eine weitere Zusatzfrage des Herrn Abgeordneten Junge.

Abg. Uwe Junge, AfD:

Vielen Dank, Herr Präsident. Das Thema „Socialbots“ haben Sie gar nicht angesprochen. Das haben wir im Parlament besprochen. Es gab eine Initiative der CDU, dass wir uns gemeinschaftlich darauf einigen, diese Dinge nicht einzusetzen. Ist das in Ihren Überlegungen aufgenommen worden? Ich denke, wir haben uns alle entsprechend geäußert und gesagt, wir wollen diese Dinge nicht einbringen. Ich nehme an, das haben Sie mit der Beantwortung der Frage 2 gemeint. Ich möchte nur noch einmal eine Bestätigung haben.

Randolf Stich, Staatssekretär:

Ich glaube, es ist für uns selbstverständlich, dass wir keine Socialbots einsetzen. Es geht hier um die Unterrichtung über die aktuelle Entwicklung, dass gerade die sozialen Netzwerke in der Zwischenzeit sehr stark auch im Hinblick auf den Bundestagswahlkampf für diese Thematik sensibilisiert sind. Sie haben gerade noch einmal organisatorische Maßnahme ergriffen, um dieser Thematik zunehmend Herr zu werden. Facebook hat vermeldet, dass es ein zusätzliches Löschzentrum gegründet hat, in dem sich die Mitarbeiter ausschließlich nach Erkennung entsprechender Inhalte um eine entsprechende Überprüfung der Accounts kümmern.

Das Ganze führt erst einmal nicht zu einer Inhaltskontrolle. Die Erkennung läuft auf einer technisch-organisatorischen Basis und wird auf dieser Grundlage dann erst umgesetzt.

Präsident Hendrik Hering:

Eine weitere Zusatzfrage des Herrn Kollegen Wäschenbach.

Abg. Michael Wäschenbach, CDU:

Herr Staatssekretär, wie steht die Landesregierung zur Nutzung von Cloud-Computing und Cloud-Speicher in der öffentlichen Verwaltung im Land und bei den Kommunen?

Randolf Stich, Staatssekretär:

Die Cloud bietet für die öffentliche Verwaltung eine große Chance. Man muss nur an der Stelle sehen, dass Cloud nicht gleich Cloud ist, sondern man muss ganz klar zwischen einer Public Cloud und einer Private Cloud unterscheiden. Eine Public Cloud für öffentliche Daten wäre sicher ein Umstand, der mit dem Datenschutzbeauftragten schwer zu vereinbaren wäre, weil wir hier schlichtweg andere Speicherungsvoraussetzungen haben, als das im privaten Bereich für private Belange der Fall ist.

Deswegen setzen wir im LDI auf den Bereich der sogenannten Private Cloud. Das heißt, wir setzen intern im Landesnetz Serversysteme um, die die Cloud-Technologie nutzen, um vereinfacht Server flexibel einsetzen zu können. Das Ganze geschieht in enger Absprache mit dem Landesdatenschutzbeauftragten und dem BSI.

Auch diese Systeme werden dann an dem hohen Datenschutzgrundniveau ausgerichtet. Das heißt, Cloud-Technologie sehen wir als eine wesentliche Zukunft für die öffentliche Verwaltung an. Hier muss man aber noch einmal deutlich unterscheiden, nicht im Bereich der Public Cloud, sondern hier muss im Endeffekt geschaut werden, dass die Technik auf eine Private Cloud umgebaut wird.

Das heißt – einfach gesprochen – Systeme, die im Rheinland-Pfalz-Netz entsprechend aufgebaut werden und hier keine Außenwirkung haben. Es gab eine Ausnahme von der Telekom. Da hat man in Absprache mit dem Landesdatenschutzbeauftragten auch eine Möglichkeit für Verfahren angeboten, die in einem geringeren Schutzbereich sind, so wie Daten auf Webseiten aufgebracht werden. Das sind aber definitiv immer Fälle, in denen keine schutzwürdigen Daten gehostet werden.

Präsident Hendrik Hering:

Eine weitere Zusatzfrage des Herrn Kollegen Schweitzer.

Abg. Alexander Schweitzer, SPD:

Herr Staatssekretär, Sie haben gesagt, es kam nicht aus dem Inland, sondern aus dem Ausland. Wir nähern uns also an. Ich frage mich, aus welchen Ländern im Ausland kamen dieser Angriffe auf die Webpräsenzen von deutschen und rheinland-pfälzischen Parteien? In diesem Falle die Fälle, die Sie mit Blick auf die CDU geschildert haben. Weiß man das?

Randolf Stich, Staatssekretär:

Das wird derzeit noch untersucht. Das Problem ist immer, dass die IP-Adressen, die hintendran sind, gerne manipuliert werden, sodass ein Angriff, den man zwar auf den ersten Blick gerne klar zugeordnet, vielleicht im Hintergrund dann doch aus einem anderen Bereich kommt, weil gezielt Webadressen umgeleitet worden sind. Ich werde hier gerne entsprechend weiter berichten.

Präsident Hendrik Hering:

Eine Zusatzfrage des Herrn Abgeordneten Denninghoff.

Abg. Jörg Denninghoff, SPD:

Herr Staatssekretär, meiner Information nach ist es beim LDI sogar gelungen, die BSI-Zertifizierung auch für die Cloud-Infrastruktur zu erreichen, und das wohl als erster deutschland-, wenn nicht weltweit. Für BSI kann man deutschlandweit sagen, aber es ist in dem Fall weltweit. Können Sie etwas zur Einordnung unseres LDI zu den ähnlichen Betrieben anderer Bundesländer sagen?

Randolf Stich, Staatssekretär:

Also ich kann an der Stelle immer nur sagen, egal auf welcher Veranstaltung wir bundesweit auftreten, der LDI hat nicht nur eine Spitzenstellung, er hat auch in vielen Bereichen ein Alleinstellungsmerkmal. Ich habe es eben schon einmal genannt. Gerade der wirklich wesentliche Bereich des Rheinland-Pfalz-Netzes, eines von zwei Bundesländern von allen, die entsprechend zertifiziert sind. Das sind wir auch ganz klar über dem Stand des Bundesnetzes. Eine Serverinfrastruktur, die entsprechend abgesichert ist, E-Government Anwendungen, die eine entsprechende Zertifizierung haben, diesen Stand hat sicherheitstechnisch im Moment so kein anderes Land aufzuweisen.

Präsident Hendrik Hering:

Vielen Dank. – Es gibt keine weiteren Zusatzfragen. Damit ist die Mündliche Anfrage beantwortet.

(Beifall der SPD, der FDP und des
BÜNDNIS 90/DIE GRÜNEN)