19. Wahlperiode

Drucksache **19/4923**

HESSISCHER LANDTAG

06. 07. 2017

Kleine Anfrage

der Abg. Özgüven, Hofmann, Grumbach, Kummer, Waschke, Weiß (SPD)
vom 23.05.2017

betreffend IT-Sicherheit an hessischen Justizbehörden

und

Antwort

der Ministerin der Justiz

Vorbemerkung der Fragesteller:

Anfang Dezember 2016 erfolgte ein großflächiger Cyberangriff auf die hessischen Justizbehörden, bei dem als Bewerbungen getarnte E-Mails an mindestens fünf hessische Justizbehörden verschickt wurden. Statt der bezeichneten Bewerbungsunterlagen hing den E-Mails eine sogenannte "Ransomeware" an. Beim Öffnen durch den Empfänger führte dies zum Herunterladen der sogenannten Schadsoftware "Goldeneye" aus dem Internet. Diese verschlüsselte unwiederbringlich Daten auf den Festplatten von insgesamt vier Computern hessischer Justizbehörden und machte diese unbrauchbar.

Diese Vorbemerkungen der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

Frage 1. Welche konkreten Konsequenzen wurden aus dem Angriff vom 06.12.2016 für die Mitarbeitenden der hessischen Justizbehörden gezogen? Gab es seitdem insbesondere gezielte Fortbildungen für die Angestellten der Behörden, die zur Sensibilisierung der Mitarbeitenden geführt haben?

Der IT-Sicherheitsbeauftragte hat die Abläufe während des Sicherheitsvorfalls in einem ausführlichen Bericht bewertet. Als Folgerungen aus dem Angriff vom 6. Dezember 2016 wurden insbesondere folgende Maßnahmen eingeleitet:

- Schulungs- und Sensibilisierungsmaßnahmen zur Stärkung des Sicherheitsbewusstseins bei IT-Funktionsträgern (insbesondere Vorortbetreuern) und Nutzern, die wegen des erforderlichen Planungsvorlaufs im 2. Halbjahr 2017 stattfinden werden. Diese Maßnahmen umfassen u.a. einen Block "IT-Sicherheit" im Rahmen der jährlichen Fortbildung der Vorortbetreuer im August/September 2017, eine eintägige Veranstaltung "IT-Sicherheit an den Dienststellen" für Vorortbetreuer und behördliche IT-Sicherheitsbeauftragte sowie eine flächendeckende Awareness-Kampagne zur IT-Sicherheit für alle Dienststellen und Nutzer in der Justiz.
- Herausgabe einer Kurzhandlungsanweisung für Nutzer und Vorortbetreuer bei Verdacht auf Befall mit Schadsoftware.
- Schärfung der Prozeduren zu den Melde- und Informationswegen im Notfallmanagement der Justiz in Abstimmung mit dem IT-Notfallmanagement der HZD. Dabei wird insbesondere das neu eingerichtete Zentrale User Helpdesk (ZUHD) der IT-Stelle eingebunden.
- Innerhalb der IT-Stelle wird im Referat IT-Infrastruktur ein neuer Bereich "Operative IT-Sicherheit (OPIS)" eingerichtet, der die technischen Einrichtungen der IT-Sicherheit administriert und bei Sicherheitsvorfällen und bei der Abwehr von Cyberangriffen als Taktisches Operationszentrum fungiert. Dies soll u.a. der logistischen Unterstützung des IT-Sicherheitsbeauftragten der hessischen Justiz (ITSiBJ) und der Leitung der IT-Stelle dienen. Die Rekrutierung von Personal wird durch Sondermittel des IT-Sicherheitsbeauftragten der Landesregierung (CISO) unterstützt.

Frage 2. Finden regelmäßige Überprüfungen statt, um Schwachstellen der IT-Infrastruktur an hessischen Justizbehörden identifizieren zu können
a) Falls ja, in welchem Umfang?
b) Falls nein, warum nicht?

Zur Durchführung regelmäßiger technischer Prüfungen der Funktionsfähigkeit von IT-Sicherheitsmaßnahmen (Pentests) wird von der Justiz auf externe Beratungsfirmen aus dem

Eingegangen am 6. Juli 2017 · Bearbeitet am 7. Juli 2017 · Ausgegeben am 11. Juli 2017
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Rahmenvertrag des Landes Hessen für IT-Sicherheits-Dienstleistungen zurückgegriffen. Im Zentrum der Aufmerksamkeit stehen dabei Systeme mit unmittelbarer Verbindung zum Internet, etwa das Zentrale Schutzschriftenregister.

Prüfungen der organisatorischen und technischen Infrastruktur (Audits) erfolgen durch den IT-Sicherheitsbeauftragten der Justiz im Zusammenwirken mit der IT-Kontrollkommission der Justiz unter Beauftragung externer Beratungsfirmen. Hierfür wurde ein sich über mehrere Jahre erstreckender Auditplan erstellt, der regelmäßige Audits mit jeweils konkreten Auditplänen vorsieht. Eine Auditierung der HZD Hünfeld wird im 2. Halbjahr 2017 stattfinden.

Frage 3. Wird der Mailserver des Justizministeriums bei eingehendem Mailverkehr auf Schadsoftware untersucht?
a) Falls ja, warum konnte die Schadsoftware nicht entdeckt werden?
b) Falls nein, warum nicht?

Die zentrale E-Mail-Plattform der Landesverwaltung einschließlich der Justiz bzw. des Justizministeriums wird bei eingehendem Mailverkehr auf Schadsoftware geprüft. Dabei wird zur Beschleunigung des Prüfungsvorgangs auf die Datenbank eines Herstellers von Virenschutzsoftware zurückgegriffen. Eine erneute Prüfung durch klassische Virensignaturen findet beim Öffnen von Mails auf den einzelnen Endgeräten statt.

Die in den Vorbemerkungen der Fragestellerinnen und Fragesteller angesprochene Schadsoftware konnte dennoch nicht entdeckt werden, da es sich um einen sog. "Zero-Day-Exploit" handelte. Dabei wird die Schadsoftware auf Servern im Darknet für potenzielle Angreifer verfügbar gemacht, bevor die Virensignaturen und Virendatenbanken der Hersteller von Schutzsoftware sich auf die neue Schadsoftware eingestellt haben. In der Zwischenzeit sind IT-Systeme durch die Schadsoftware grundsätzlich angreifbar.

Frage 4. Wie bewertet die Hessische Landesregierung die Netzsicherheit der hessischen Justizbehörden und an welchen Kriterien macht sie das fest?

Die von der HZD für die Justiz betriebenen Netze und IT-Systeme sind aus Sicht der strategischen und operativen IT-Leitung und des IT-Sicherheitsbeauftragten der Justiz im Hinblick auf die für die jeweiligen Daten zu erwartenden Angriffsszenarien ausreichend geschützt, eine absolute Sicherheit kann allerdings nicht gewährleistet werden. Die Schutzmaßnahmen des IT-Sicherheitsmanagement-Systems (ISMS) betreffen im Sinne einer Rundumverteidigung das Justiznetz bzw. die Netze der HZD und damit alle Behörden der Justiz. Eine Auflistung der umgesetzten und laufend aktualisierten Maßnahmen ist wegen entgegenstehender Sicherheitsinteressen nicht möglich, da diese Angaben Dritten Angriffsvektoren eröffnen und Daten für Mal-Ware-Angriffe liefern könnten, wenn sie durch die Veröffentlichung der Antwort zu dieser Kleinen Anfrage an Dritte gelangen. Die Ausweitung des Schutzes durch Fortentwicklung des ISMS ist weiterhin anzustreben. Dies gilt insbesondere im Hinblick auf besonders potente Angreifer, wie zum Beispiel aus der Organisierten Kriminalität oder aus Einrichtungen von Fremdstaaten im Rahmen des Cyberwar.

Frage 5. Wie groß fallen die durchschnittlichen finanziellen Ressourcen aus, die den hessischen Justizbehörden für deren IT-Sicherheit zur Verfügung stehen?
Bitte nach jeweiliger Maßnahme und Ressource aufschlüsseln.

Das Budget für spezielle Maßnahmen der Informationssicherheit für den gesamten Geschäftsbereich ist konzentriert im Etat des IT-Sicherheitsbeauftragten der Justiz. Für das Jahr 2017 beläuft es sich auf 2,335 Mio. €. Zu berücksichtigen ist, dass dieser Betrag wegen der Beschränkung der Mittel für den elektronischen Rechtsverkehr auf die Jahre 2016/2017 nicht durchschnittlich in jedem Jahr verfügbar ist. Um die Gesamtsumme nicht zu verfälschen, sind in diesem Betrag zudem zusätzlich aus 2016 übertragene Mittel in Höhe von rund 1,5 Mio. € nicht berücksichtigt. Die mit der Frage erbetene Aufschlüsselung nach jeweiliger Maßnahme und Ressource ist aus Sicherheitsgründen nicht möglich, da diese Angaben eventuellen Angreifern Hinweise darauf geben könnten, in welchen Bereichen ein Angriff möglicherweise besonders Erfolg versprechend sein könnte.

Frage 6. Wie wird sichergestellt, dass hochsensible Daten der Behörden gegenüber Angriffen aus dem Internet vollständig geschützt werden?
Bitte nach Maßnahmen aufschlüsseln.

Um den größtmöglichen Schutz von Daten gegenüber Angriffen aus dem Internet zu ermöglichen, sind entsprechende Schutzmaßnahmen jeweils im Hinblick auf die für die jeweiligen

Daten zu erwartenden Angriffsszenarien und Risikoquellen abzustimmen und zu optimieren. Dabei sind insbesondere fünf Maßnahmengruppen relevant:

- Schaffung von Informationssicherheitsleitlinien und -richtlinien, welche den Funktionsträgern und Nutzern Vorgaben zum Umgang mit der von ihnen genutzten IT machen;
- Schaffung und Umsetzung von IT-Sicherheitskonzepten für Fachverfahren und Basisinfrastruktur und die Umsetzung der darin enthaltenen Schutzmaßnahmen;
- Technische Maßnahmen zur Rundumverteidigung des Justiznetzes einschließlich der stetigen Verbesserung der Notfallkonzepte und -prozesse zur Behandlung von Sicherheitsvorfällen;
- IT-Sicherheitsprüfungen im Hinblick auf die Effektivität bestehender Sicherheitsmaßnahmen (Audits und Pentests);
- Förderung des IT-Sicherheitsbewusstseins und Fortbildung der Nutzer und IT-Funktionsträger.

Wiesbaden, 27. Juni 2017

Eva Kühne-Hörmann