BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
21. Wahlperiode

Drucksache 21/5288
22.07.16

Schriftliche Kleine Anfrage

der Abgeordneten Carsten Ovens und Birgit Stöver (CDU) vom 14.07.16

und Antwort des Senats

Betr.: Wurden die Computersysteme der Hamburger Kliniken gehackt?

In der Sendung „report München“ vom 12.07.2016 wurde berichtet, dass ab Februar 2016 die Computersysteme verschiedener Krankenhäuser gehackt wurden. Es seien hohe Kosten entstanden und auf die Daten von Patienten zugegriffen worden. Teilweise wurden die Krankenhäuser mit den gehackten Daten erpresst. Auch beim UKE Hamburg seien Fehler im Backupsystem der Klinik gefunden worden. Diese Vorgänge werfen Fragen nach der Sicherheit von Patientendaten an den insgesamt 57 Hamburger Kliniken (32 Krankenhäuser und 25 konzessionierte Privatkliniken) auf.

Vor diesem Hintergrund fragen wir den Senat:

In den Hamburger Plankrankenhäusern, die im Zuständigkeitsbereich der Behörde für Gesundheit und Verbraucherschutz angesiedelt sind, hat es seit 2013 eine große Zahl nicht erfolgreicher Hackerangriffe auf die Computersysteme gegeben. Statistiken werden von den Plankrankenhäusern dazu nicht geführt. Nach deren Aussagen sind die Computernetze der Plankrankenhäuser mit mehreren Firewalls und Proxy-Servern gesichert, auf denen unterschiedliche Virenscanner alle Aktivitäten prüfen. Auf diese Weise werden jeden Monat Tausende von verdächtigen Dateien und Mails abgefangen, die gar nicht erst in die Computersysteme hineingelassen werden. Die Protokolle der Überprüfungen (auch auf den Anwender-PCs) werden regelmäßig geprüft. Das Jahr 2016 ist, verursacht durch die Schadsoftware Locky, nach Darstellung einzelner Plankrankenhäuser ein außergewöhnliches Jahr mit vielen Hackerangriffen.

Bei dem in der Sendung „report München“ vom 12. Juli 2016 erwähnten Computersystem des Universitätsklinikums Hamburg-Eppendorf (UKE) handelt es sich um einen Ausfall- beziehungsweise Backupserver des UKE-Internetauftritts www.uke.de. Dieser ist bis zum Schließen der in dem Bericht erwähnten Lücke nicht aktiv genutzt worden. Dieses – technisch abgeschottet von den klinischen Systemen betriebene – System hält keine eigenen Daten vor. Es ist lediglich für das „Ausliefern“ der Informationen an die Nutzer verantwortlich. Die über den Server laufenden Informationen sind identisch mit den Daten, die im Internetauftritt www.uke.de ohnehin für jeden Nutzer frei zugänglich sind. Somit bestand zu keiner Zeit eine Gefährdung der patientenführenden Systeme oder anderer kritischer Daten.

Dies vorausgeschickt, beantwortet der Senat die Fragen – teilweise auf der Grundlage von Auskünften der Hamburger Plankrankenhäuser einschließlich des UKE – wie folgt:

1. *Wie viele Hackerangriffe auf die Computersysteme der Hamburger Krankenhäuser und Kliniken gab es in den Jahren 2013, 2014, 2015 und 2016? Bitte differenziert nach Klinik und Jahr auflisten.*

a) Wie viele der oben genannten Hackerangriffe waren erfolgreich beziehungsweise bei wie vielen dieser Angriffe kam es zu Datenverlusten und/oder Datenentwendungen? Bitte differenziert nach Klinik und Jahr auflisten.

b) In wie vielen und welchen Fällen der unter 1. a) genannten Hackerangriffe waren Patientendaten betroffen?

Im Jahr 2013 ist es in einem Plankrankenhaus gelungen, in einem Einzelfall Zugriff auf eine Patientenakte zu nehmen. Das Plankrankenhaus hat daraufhin sein IT-Sicherheitskonzept überprüft, verstärkt und die Mitarbeiterinnen und Mitarbeiter informiert und geschult. Die zuständige Behörde verzichtet aus Sicherheitsgründen auf die Nennung des Plankrankenhauses.

Nach einer im UKE in der zur Verfügung stehenden Zeit durchgeführten manuellen Auswertung der regelmäßigen IT-Managementberichte wurden folgende „externe Hackerangriffe“ auf die zentralen IT-Systeme des UKE erkannt und erfasst:

Jahr	**Anzahl**
2013	2
2014	4
2015	18
2016	5

Bei den Fällen aus den Jahren 2015 und 2016 handelte es sich nahezu ausschließlich um solche im Rahmen des Verschlüsselungstrojaners „Ransomware“ und dessen Derivaten. Nach im UKE vorhandenen Erkenntnissen erfolgten diese Angriffe nicht zielgerichtet auf die Institution „UKE“: Vielmehr handelte es sich um breit („wahllos“) gestreute Angriffe, die zufällig auch das Verwaltungsnetz des UKE trafen. Auch bei den Vorfällen in den Jahren 2013 und 2014 wurden Trojaner oder ähnliche Schadsoftware detektiert. Über die Zahl der bereits an den „Außengrenzen“ durch die vorhandenen Sicherheitseinrichtungen (Firewalls, Proxy, Intrusiondetection, Antivirenlösungen und andere mehr) des UKE erfolgreich abgewehrten Angriffsversuche liegen für den von der Anfrage umfassten Zeitraum im UKE keine Erkenntnisse vor.

Im Übrigen siehe Vorbemerkung.

c) In wie vielen und welchen Fällen der unter 1. a) genannten Hackerangriffe kam es im Verlauf zu Erpressungsversuchen den Kliniken beziehungsweise einzelnen Pateinten gegenüber, und mit welchen Folgen?

Laut Auskunft der Plankrankenhäuser und des UKE hat es keine Erpressungsversuche gegeben.

d) Was tut der Senat beziehungsweise tun die zuständigen Behörden und die Hamburger Krankenhäuser, um solche Hackerangriffe in Zukunft zu vermeiden beziehungsweise welche Vorkehrungen wurden wann getroffen?

Durch die Rundschreiben der Hamburgischen Krankenhausgesellschaft (HKG Nummer 84/16 vom 15. Februar 2016) wurden die Hamburger Mitgliedskrankenhäuser über aktuelle Hackerangriffe informiert. Unter anderem vor diesem Hintergrund wurden in den Hamburger Plankrankenhäusern sämtliche Systeme auf ihre sicherheitsrelevanten Aspekte geprüft und bei Bedarf auf den aktuellen Stand gebracht (IT-Sicherheitskonzepte). Es obliegt den Trägern der Plankrankenhäuser, mit entsprechenden IT-Sicherheitskonzepten unter anderem die Patientendaten zu schützen. Das wird regelhaft im Rahmen der Qualitätssicherung überprüft.

In den zentralen IT-Systemen des UKE sind die verschiedenen Systeme für Verwaltung und Klinik technisch voneinander getrennt. Eine Kommunikation erfolgt ausschließlich über mehrfach abgesicherte und kontrollierte Übergänge. Aufgrund der konkreten „Ransomware“-Fälle im Jahr 2015 erfolgte Ende 2015 eine erneute Aufrüstung der Absicherung des Internetzugangs durch einen neuen Webproxy. Dieser überprüft sämtliche ein- und ausgehenden Verbindungen aus dem und in das Internet auf mögliche Bedrohungen und blockiert diese.

Das UKE hat im Geschäftsbereich IT für die Informationssicherheit eine spezielle Organisation und ein Managementsystem etabliert. Risiken und auch Vorfälle werden strukturiert erfasst, bewertet und Maßnahmen nachverfolgt. Es erfolgen zudem jährliche Audits durch das Bundesamt für Sicherheit in der Informationstechnologie und regelmäßig sogenannte Penetrations-Tests, bei denen ein externer Dienstleister systematisch die möglichen Angriffsvektoren aus dem Internet auf das UKE untersucht.

Im Übrigen siehe Vorbemerkung.

2. Um welchen Fehler beziehungsweise um welche Lücken im Computersystem des UKE, über den beziehungsweise über die „report München" berichtete, handelt es sich genau?

Aus sicherheitsrelevanten Gründen sieht der Senat davon ab, die Sicherheitslücke genauer zu benennen. Im Übrigen siehe Vorbemerkung.

a) Von wann bis wann bestand dieser Fehler beziehungsweise diese Lücke?

Der betroffene Server wurde ab dem 15. Dezember 2015 als Test- und Reservesystem installiert. Die Tests erfolgten mit einem externen Dienstleister, weshalb der Server von außen erreichbar sein musste. Die Lücke wurde durch ein Update am 17. Mai 2016 geschlossen. In den Echtbetrieb wurde der Server erst am 25. Mai 2016, also nach Schließen der Lücke, überführt.

b) Wann wurden die zuständigen Behörden über diesen Fehler durch wen informiert?

Das UKE wurde am Freitag, den 13. Mai 2016, durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) selbst auf diese Schwachstelle hingewiesen. Eine Information hamburgischer Behörden ist nicht erfolgt. Das UKE hat sie als entbehrlich angesehen, da der Fehler lediglich ein potenzielles Risiko in einem nicht als kritisch zu bewertenden System bedeutet hatte.

c) Welche Maßnahmen ergriffen der Senat, die zuständigen Behörden und das UKE, um diese Fehler beziehungsweise Lücken zu beheben? Und wie lange dauerte die Behebung dieser Fehler beziehungsweise Lücken?

Siehe Antwort zu 2. a).

d) Welche weiteren Fehler und Lücken gab es im Computerbetriebssystem des UKE in den Jahren 2013 bis 2016? Wann hatten der Senat beziehungsweise die zuständigen Behörden von diesen Fehlern und Lücken Kenntnis? Wann und wie wurden diese Fehler und Lücken behoben? Bitte differenziert nach Klinik und Jahr auflisten.

Weitere Fehler und Lücken im Computerbetriebssystem des UKE in den Jahren 2013 bis 2016 sind nicht bekannt.

e) Gab es an den anderen Hamburger Krankenhäusern und Kliniken ähnliche Fehler und Lücken im Computerbetriebssystem während der Jahre 2013 bis 2016?

Wenn ja: Um welche Fehler und Lücken handelte es sich? Wann hatten der Senat beziehungsweise die zuständigen Behörden von diesen Fehlern und Lücken Kenntnis? Wann und wie wurden diese Fehler und Lücken behoben? Bitte differenziert nach Klinik und Jahr auflisten.

Siehe Vorbemerkung.