Abgeordnetenhaus BERLIN

Drucksache 18 / 21 197
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Bernd Schlömer (FDP)

vom 08. Oktober 2019 (Eingang beim Abgeordnetenhaus am 08. Oktober 2019)

zum Thema:
IT-Sicherheitsvorfall im Kammergericht

und **Antwort** vom 28. Oktober 2019 (Eingang beim Abgeordnetenhaus am 29. Okt. 2019)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Justiz, Verbraucherschutz
und Antidiskriminierung

Herrn Abgeordneten Bernd Schlömer (FDP)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 18 / 21 197
vom 8. Oktober 2019
über **IT-Sicherheitsvorfall im Kammergericht**

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorwort des Abgeordneten: Am 2. Oktober 2019 wurde durch die Presse bekannt, dass Hacker das Kammergericht in Berlin angegriffen haben und dass daher das Gericht seit dem 27. September 2019 vom Landesnetz getrennt wurde.

1. Laut Informationen des "Tagesspiegel Checkpoint" vom 5. Oktober 2019 soll bereits am 10. September vom ITDZ Berlin eine Infektion mit einer Schadsoftware festgestellt worden sein, aber erst am 23. September 2019 eine offizielle Information an das Kammergericht ergangen sein.

a.) Warum wurde so lange mit der Information gewartet?

Zu 1. a.): Am 25. September 2019 wurde nach Information des Sicherheitsbeauftragten des Kammergerichts Berlin dieses erstmals über das IT Dienstleistungszentrum (ITDZ)/Cyber Emergency Response Team (CERT) von einem verdächtigen „Traffic" aus dem Kammergericht heraus über das Berliner Landesnetz in Kenntnis gesetzt. Im Kammergericht eingesetzte Fremdfirmen zur Bestandsanalyse sollen später darüber berichtet haben, dass der dort festgestellte Trojaner EMOTET am 10. September 2019 entwickelt worden sei. Wann konkret eine Kontaminierung der Systeme erfolgt ist, lässt sich im Nachhinein leider nicht feststellen. Von daher lässt sich derzeit ein langes Warten mit der Information nicht bestätigen. Als ersten Schritt wurde über die Einstellung im Proxy des Kammergerichts nach Aussage des Sicherheitsbeauftragten der E-Mailverkehr unterbrochen.

b.) Wie ist das Berichtswesen zu besonderen Vorfällen in der IT-Sicherheit im Land Berlin organisiert?

Zu 1. b.): Die Meldeprozesse zu IKT-Sicherheitsvorfällen sind in einer landesweit abgestimmten Beschreibung zu IKT-Sicherheitsvorfällen dokumentiert. Diese Beschreibung und die zugehörigen Formulare sind auf der Intranetseite des CERT u.a für die Annahme von sicherheitsrelevanten Informationen veröffentlicht.

Entsprechend der beschriebenen Meldeprozesse liegt die ereignisbezogene und regelmäßige Meldepflicht bei der betroffenen Behörde bzw. Einrichtung.
Die Verteilung von sicherheitsrelevanten Informationen und Empfehlungen vom CERT erfolgen entsprechend der Aufgabenbeschreibung des CERT. Die Aufgabenbeschreibung ist in der Informationssicherheitsleitlinie der Landesverwaltung des Landes enthalten.
Sofern das CERT im ITDZ Berlin als Landesdienstleister ein Sicherheitsereignis feststellt, wird die betroffene Einrichtung, vorliegend das Kammergericht Berlin, darüber unverzüglich in Kenntnis gesetzt.
Das CERT unterstützt die betroffenen Behörden und Einrichtungen bei der weiteren Bearbeitung und Reaktion auf Vorfälle gemäß seiner Aufgabenbeschreibung.

c.) Wer meldet wie an wen und zu welchem Zeitpunkt IT-Sicherheitsvorfälle?

Zu 1. c.): Siehe 1. b.) Vorliegend erfolgte die Information telefonisch über einen Mitarbeiter des CERT.

d.) Existiert ein 24/7-Service zur Gefahrenabwehr und zur Gewährleistung der IT-Sicherheit im Land Berlin?

Zu 1. d.): Die technische Gefahrenabwehr für die IKT der Berliner Landesverwaltung wird beim ITDZ in einem 24/7-Service betrieben.

e.) Wie ist die ämter- bzw. ressortübergreifende Information konkret organisiert?

Zu 1. e.): Die ämter- und ressortübergreifende Information erfolgt mittels des Warn- und Informationsdienstes (WID) des CERT. Das schließt die Verteilung von Informationen mit ein, die im Rahmen der Meldepflicht der Behörden und Einrichtungen unverzüglich an das CERT zu melden sind.

2. Wann wurde die IT-Ausstattung des Kammergerichts zuletzt erneuert? Wurden die USB-Sticks, mit denen die Richter und Richterinnen arbeiten (Checkpoint vom 5. Oktober 2019) vom Kammergericht zur Verfügung gestellt oder werden private USB-Sticks benutzt?

Zu 2.): Das Kammergericht Berlin befindet sich im Status eines Eigenbetriebs in Form der Verbindung von (Fat-) Clients über dort betriebene Server im Rahmen eines eigenen Netzwerks. Es besteht eine Datenverbindung zum Berliner Landesnetz. Alle bezeichneten Komponenten befinden sich im üblichen Release Zyklus von maximal fünf Jahren.

Den Richterinnen und Richtern wie auch den übrigen Mitarbeitern des Kammergerichts wurden bei Bedarf USB-Sticks zu dienstlichen Zwecken zur Verfügung gestellt. Die Nutzung privater USB-Sticks war bis zum festgestellten Sicherheitsvorfall möglich.

3. Welche Verfahrensvorschrift im Land Berlin sieht vor, dass Wechseldatenträger für dienstlich bereit gestellte Rechner frei genutzt werden können?

Zu 3.: Eine solche Verfahrensvorschrift ist zumindest der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung nicht bekannt.

4. Wie ist die regelmäßig durchzuführende IT-Sicherheitsbelehrung im Justizwesen des Landes Berlin geregelt? Wer ist konkret mit der Durchführung beauftragt? Existieren Verfahrensvorschriften hierzu, wenn ja, wie heißen diese und welches Datum tragen diese? Wie wird die Regelmäßigkeit der IT-Sicherheitsbelehrung im Justizwesen im Allgemeinen und im Kammergericht im Besonderen kontrolliert?

Zu 4.: Eine Verfahrensvorschrift zur regelmäßigen Durchführung einer IT-Sicherheitsbelehrung im Justizwesen des Landes Berlin ist nicht bekannt. Eine Überprüfung der Durchführung der Regelmäßigkeit von IT-Sicherheitsbelehrungen im Geschäftsbereich der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung findet nicht statt.

Der Präsident des Kammergerichts hat für sein Haus Folgendes mitgeteilt: „Im Zuge des Inkrafttretens der DSGVO sind die Leiter/innen der verschiedenen Arbeitsbereiche des Kammergerichts (Geschäftsleitung, Leitung der Dezernate u.a.) in mehreren Info-Veranstaltungen in Fragen der IT-Sicherheit und des Datenschutzes als Multiplikator/innen unterwiesen worden. Hierzu wurden intern und externe Experten herangezogen, ebenso der Sicherheitskoordinator des Kammergerichts und der örtliche Datenschutzbeauftragte.

5. Wann fand die letzte IT-Sicherheitsbelehrung im Kammergericht statt? Wie werden Nachweise hierüber geführt? Welche Personengruppen unter den Mitarbeitenden werden angesprochen? Ist die IT-Sicherheitsbelehrung auch für Richter und Richterinnen verpflichtend?

Zu 5.: Siehe Punkt 4.

6. Werden spezielle Schulungen zum Thema “Social Engineering” im Berliner Justizwesen durchgeführt? Wenn ja, welche Personengruppen unter den Mitarbeitenden werden angesprochen? Sind diese Schulungen verpflichtend? Wenn nein, warum nicht? Wenn ja, wie werden hierüber Nachweise geführt?

Zu 6.: In der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung werden spezielle Schulungen zum Thema „Social Engineering“ nicht angeboten.

Der Sicherheitsbeauftragte des Kammergerichts hat Schulungen der genannten Art für den allgemeinen Justizdienst auf freiwilliger Basis in der Vergangenheit wiederholt unter eigener Federführung angeboten.

7. Wie plant der Senat zukünftig regelmäßige IT-Sicherheitssensibilisierungen – unabhängig von der aktuellen Beschlusslage des AGH - umzusetzen?

Zu 7.: Nach der Vorgabe der Informationssicherheitsleitlinie der Senatsverwaltung für Inneres und Sport von Berlin hat das Informationssicherheitsmanagement nach den Standards des BSI in den Behörden zu erfolgen. Das beinhaltet zugleich die Umsetzung der Anforderungen des Grundschutzkompendiums in der Verantwortung der jeweiligen Behördenleitungen. Der konkrete Vorfall im Kammergericht Berlin ist ein Hinweis, dass der Grundschutz-Baustein "ORP.3 Sensibilisierung und Schulung" zusätzlich zu den bestehenden fachlich geprägten Schulungsinhalten zukünftig mit dem Fokus Sensibilisierung äquivalent umzusetzen ist. Die landesweiten Planungen dazu wurden auch mit den Schwerpunkten zur Umsetzung der Beschlüsse des Abgeordnetenhauses 18/1674 "IT-Sicherheitsstrategie für die Berliner Verwaltung" und 18/1823 " IT-Sicherheit durch Aus-, Fort- und Weiterbildung gewährleisten – IT-Sicherheitsübungen und Cyber-Sicherheitstag durchführen" bereits aufgenommen.

8. Wie hoch ist der durch die Schadsoftware “Emotet” entstandene Schaden? Wer haftet für diesen? Gibt es eine Lösegeldforderung?

Zu 8.: Der Schaden lässt sich noch nicht beziffern. Inwieweit die vorhandene Hardware – Clients und Server sowie Peripheriegeräte –betroffen ist, lässt sich noch nicht abschätzen. Ein konkreter Verantwortlicher für die Kontaminierung ist (noch) nicht feststellbar, so dass auch die Haftungsfrage derzeit nicht beantwortet werden kann.

Eine Lösegeldforderung gibt es bislang nicht.

9. Sollte es eine Lösegeldforderung geben, wird der Senat dieser nachkommen? Hat der Senat Bitcoins, um diese mit dieser Kryptowährung zu bezahlen?

Zu 9.: Nein. Der Senat verfügt über keine Bitcoins.

10. Sind personenbezogene Daten von Bürgerinnen und Bürgern Berlins betroffen?

Zu 10.: Im Rahmen der umfangreichen Überprüfungen konnte bislang nicht festgestellt werden, dass personenbezogene Daten von Bürgerinnen und Bürger Berlins betroffen sind.

11. Welche Stellen wurden innerhalb des Landes Berlin und bundesweit vom Senat, dem Kammergericht und dem ITDZ mit einbezogen?

Zu 11.: Innerhalb des Landes Berlin wurden das ITDZ Berlin/CERT, Senatsverwaltung für Inneres und Sport/IKT-Steuerung, das Landeskriminalamt (LKA) sowie alle Gerichte, Strafverfolgungsbehörden und Justizvollzugsanstalten sowie die Berliner Beauftragte für Datenschutz informiert; ferner das Bundesamt für Sicherheit in der Informationstechnik sowie die IT-Verantwortlichen des Landes Brandenburg.

Berlin, den 28. Oktober 2019

In Vertretung

Brückner
Senatsverwaltung für Justiz,
Verbraucherschutz und Antidiskriminierung