Kleine Anfrage zur kurzfristigen schriftlichen Beantwortung
gemäß § 46 Abs. 2 GO LT
mit Antwort der Landesregierung

Anfrage der Abgeordneten Dr. Marco Genthe und Dr. Stefan Birkner (FDP)

Antwort des Niedersächsischen Justizministeriums namens der Landesregierung

Cyberangriffe auf niedersächsische Gerichte?

Anfrage der Abgeordneten Dr. Marco Genthe und Dr. Stefan Birkner (FDP), eingegangen am 11.02.2020 - Drs. 18/5792
an die Staatskanzlei übersandt am 13.02.2020

Antwort des Niedersächsischen Justizministeriums namens der Landesregierung vom 27.02.2020

Vorbemerkung der Abgeordneten

Im September 2019 kam es zu einem Cyberangriff auf das Berliner Kammergericht, der vermutlich aus Reihen der organisierten Kriminalität verübt wurde (rbb24, 28.01.2020). Laut einem Gutachten hatte der Urheber des Angriffs vollen Zugriff auf die Daten des u. a. für Terrorprozesse zuständigen Gerichts (*Der Tagesspiegel*, 29.01.2020).

„Datenschützer sprachen hinterher von einem ‚Totalschaden' für das Kammergericht. IT-Experten äußerten sich schockiert über die Missstände in der vom Gericht selbst verwalteten IT-Infrastruktur" (*Der Tagesspiegel*, 29.01.2020).

Vorbemerkung der Landesregierung

Alle niedersächsischen Gerichte und sonstigen Justizbehörden sind Bestandteil der vom Zentralen IT-Betrieb niedersächsische Justiz (ZIB) verwalteten IT-Infrastruktur und insoweit durch umfassende technische und organisatorische Maßnahmen vor Cyberangriffen geschützt.

1. Wie viele Cyberangriffe auf niedersächsische Gerichte gab es seit 2013 (bitte nach Gerichten aufschlüsseln)?

Die Landesregierung hat keine Anhaltspunkte für die Annahme, niedersächsische Gerichte seien bisher gezielt aus dem Cyberraum angegriffen worden. Die regelmäßig identifizierten Angriffe sind eher als Bestandteil von groß angelegten Streu- oder Flächenangriffen zu werten.

Eine strukturierte und nachvollziehbare Dokumentation von Cyberangriffen auf die niedersächsischen Gerichte ist erst ab 2015 möglich.

Im Zeitraum von 2015 bis heute wurden insgesamt 21 Angriffsversuche auf Gerichte registriert, die sich wie folgt aufteilen:

Justiz gesamt bzw. nicht differenziert:	6 (Massenmails, Kampagnen)
Amtsgericht Braunschweig	2
Amtsgericht Holzminden	1
Amtsgericht Lehrte	1
Amtsgericht Osnabrück	2
Amtsgericht Otterndorf	1
Amtsgericht Syke	1
Landgericht Hannover	1
Landgericht Lüneburg	1
Landessozialgericht Niedersachsen-Bremen	1
Oberlandesgericht Celle	1

Sozialgericht Hildesheim	1
Verwaltungsgericht Hannover	2

Bei den vorgenannten Angriffsversuchen handelt es sich jeweils um klassifizierte Informationssicherheitsvorfälle mit dem Verdacht auf oder tatsächlichen Infektionen mit Schadcode (Viren, Würmer, Trojaner), welche die in den Gerichten betriebenen Endgeräte (PC, Notebooks etc.) hätten schädigen können, wenn sie nicht von den lokalen Virenschutzsystemen erkannt worden wären.

Daneben wird von den zentral gelagerten Virenschutzsystemen des ZIB täglich eine Vielzahl von verdächtigen E-Mails abgefangen, die in der niedersächsischen Justiz jährlich im sechsstelligen Bereich liegen. Diese werden jedoch gleich an zentraler Stelle gelöscht oder in Quarantäneordner verschoben und dringen somit nicht bis in die Hausnetze der Gerichte vor.

2. Welchen Schaden haben die jeweiligen Angriffe angerichtet, bzw. welche Daten waren gefährdet (bitte nach Gerichten aufschlüsseln)?

Ein konkreter Schaden durch Cyberangriffe, wie z. B. die erpresserische Verschlüsselung von Daten oder ein unkontrollierter Datenabfluss, wurde nach den vorliegenden Erkenntnissen in der niedersächsischen Justiz nicht verursacht. Die Behandlung von vermuteten oder bestätigten Informationssicherheitsvorfällen sieht daher in aller Regel eine Neuinstallation der betroffenen Systeme vor. Bisher stellt sich der Aufwand für die aus diesem Grund notwendigen Neuinstallationen von Systemen als zu vernachlässigende Größe dar.

3. Wie sind die niedersächsischen Gerichte vor derartigen Angriffen geschützt?

Neben klassischen Sicherheitskomponenten (wie dem Einsatz von Firewalls sowie von zentralen und lokalen Virenschutzsystemen) begegnet die niedersächsische Justiz der steigenden Professionalität der Angreifer sowie deren psychologischer und technischer Aufrüstung durch den Einsatz fortschrittlicher IT-Sicherheitstechnologien und Erkennungssysteme sowie differenzierter Betriebs- und Administrationskonzepte. Zudem werden für die in der Justiz verwendeten Hard- und Softwaresysteme fortlaufend Risiken analysiert, Sicherheitskonzepte erstellt und die daraus resultierende Maßnahmenumsetzung vorangetrieben.

Um auch die E-Mail-Kommunikation vor fremden Zugriffen oder Manipulationen Dritter zu schützen, wurden neben dem Virenscanner auf den E-Mail-Servern der Justiz weitere Schutzmaßnahmen eingeführt. Der Zugriff auf Webinhalte im Internet wird durch ein professionelles, permanent aktualisiertes System geschützt, indem der Zugriff auf bekannte Schadcode behaftete Webseiten verhindert wird.

Neben den technischen Schutzmaßnahmen werden die Mitarbeiterinnen und Mitarbeiter der Justiz regelmäßig per E-Mail oder im Intranet über aktuelle Bedrohungen informiert. In Form von Präsenzveranstaltungen, für die eine Teilnahme verpflichtend ist, werden sämtliche Justizbeschäftigten turnusmäßig über die Gefahren sensibilisiert und erhalten Ratschläge und Verhaltensmaßregeln.

Die niedersächsische Justiz ist Bestandteil des Informationssicherheitsmanagement-Systems der niedersächsischen Landesverwaltung, und alle Justizbehörden werden durch den ZIB betreut und verwaltet. So ist gewährleistet, dass alle technischen und organisatorischen Maßnahmen auf alle Justizbehörden wirken.

Der ZIB arbeitet fortlaufend an der Weiterentwicklung der IT-Infrastruktur und der vorhandenen sowie neuen Schutzmaßnahmen. So sind mit dem Sondervermögen Digitalisierung für das Jahr 2020 zusätzlich 1 Million Euro zur Stärkung der Informationssicherheit eingeplant.

(Verteilt am 28.02.2020)