Kleine Anfrage zur schriftlichen Beantwortung
gemäß § 46 Abs. 1 GO LT
mit Antwort der Landesregierung

Anfrage der Abgeordneten Dr. Marco Genthe, Lars Alt, Jörg Bode und Horst Kortlang (FDP)

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung

IT-Sicherheit der kommunalen Verwaltung

Anfrage der Abgeordneten Dr. Marco Genthe, Lars Alt, Jörg Bode und Horst Kortlang (FDP), eingegangen am 23.09.2021 - Drs. 18/9975
an die Staatskanzlei übersandt am 28.09.2021

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung vom 28.10.2021

Vorbemerkung der Abgeordneten

Im Juli 2021 berichteten unterschiedliche Medien über einen Hackerangriff auf die IT-Systeme der Landkreisverwaltung Anhalt-Bitterfeld in Sachsen-Anhalt. Bei diesem Angriff wurde ein Trojaner in die Serverstrukturen der Kommune eingeschleust, und es wurden große Datenmengen verschlüsselt. Der Bürgerservice und viele weitere öffentliche Verwaltungsaufgaben konnten nicht mehr aufrechterhalten und wahrgenommen werden. (https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/anhalt/hackerangriff-auf-kreisverwaltung-100.html)

Insbesondere durch die Auswirkungen der Corona-Pandemie und der daraus folgenden Umstellung vieler Prozesse auf digitale Formate sowie Plattformen, erhöht sich derzeit das Risiko von sogenannten Cyber-Angriffen. Der Behörden Spiegel schreibt dazu: „Für öffentliche Organisationen und Unternehmen wird es immer aufwendiger, effektive und dabei wirtschaftliche IT-Sicherheitslösungen einzusetzen, um sich zuverlässig gegen Risiken schützen zu können. Cyber-Resilienz muss deshalb in Zukunft als zentrales Leitbild innerhalb jeder IT-Strategie etabliert werden. Das gilt auch und besonders für staatliche Institutionen. Cyber-Resilienz bedeutet, zentrale Prozesse und Infrastrukturen auch unter außergewöhnlichen Umständen auf ausreichendem Niveau funktionsfähig zu halten. Resilienz bezieht sich außerdem auf die Fähigkeit, eine schnelle Recovery zur vollen Leistung zu erreichen. Der Fokus liegt dabei nicht auf hundertprozentiger, sondern adäquater Sicherheit.“

(https://www.behoerden-spiegel.de/2021/03/08/cyber-resilienz-als-leitbild-fuer-zukuenftige-it-sicherheit/)

Vorbemerkung der Landesregierung

Die Landesregierung stuft auf Basis der Erkenntnisse sowohl des Niedersächsischen Computer Emergency Response Teams (N-CERT) als auch der Sicherheitsbehörden die Bedrohungslage durch Hackerattacken für die IT-Infrastruktur der öffentlichen Verwaltung in Niedersachsen unverändert auf erhöhtem Niveau ein, siehe hierzu auch die Vorbemerkung der Landesregierung in der Antwort auf die Kleine Anfrage zur kurzfristigen schriftlichen Beantwortung - Drs. 18/9852.

Im Bereich der Cyberkriminalität ist in den letzten Jahren der Bereich der Lösegelderpressung im Zusammenhang mit Verschlüsselungstrojanern (sogenannte Ransomware-Attacken) immer bedeutender geworden. In diesem Zusammenhang nimmt auch die Bedrohung der öffentlichen digitalen Infrastrukturen durch kriminelle Gruppierungen weiter zu.

Neben direkten Angriffen auf die Infrastruktur, bei denen die Schadsoftware beispielsweise über E-Mail verteilt wird, stellen Angriffe auf Software-Lieferanten (Supply-Chain-Angriffe) eine ernstzu-

nehmende Bedrohung für die IT-Sicherheit dar. Hierbei wird Schadsoftware über manipulierte Anwendungen von grundsätzlich vertrauenswürdigen Vertragspartnern in eine Organisation eingebracht.

Faktoren wie IT-Sicherheitsvorkehrungen, Größe der Infra- bzw. Netzwerkstrukturen und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter spielen eine wesentliche Rolle für den Schutz gegen Cyberangriffe. Wichtig ist hervorzuheben, dass im genannten Beispiel der Anfrage die Landkreisverwaltung Anhalt-Bitterfeld oder auch die Stadt Neustadt am Rübenberge nicht deshalb Opfer eines solchen Ransomware-Angriffs geworden sind, weil die Cyberkriminellen dort besonders sensible Informationen erbeuten wollten. Vielmehr verfolgen nach hiesigen Erkenntnissen die Angreifenden mit ihrem „Geschäftsmodell“, das u. a. gegen Wirtschaftsunternehmen eingesetzt wird, das Ziel, Lösegeld zu erpressen, häufig gekoppelt mit der Möglichkeit der anonymen Lösegeldüberweisung mittels Krypto-Währungen wie Bitcoin. Der Diebstahl sensibler Daten ist hier nur von nachrangiger Bedeutung.

Die zunehmende Verflechtung zwischen physischer und digitaler Welt erfordert robuste Resilienzmaßnahmen gegen Bedrohungen aller Art. Hierbei sind grundsätzlich alle Verwaltungsbereiche einzubeziehen, insbesondere solche, die den Kritischen Infrastrukturen (KRITIS) zugerechnet werden. In diesem Kontext wird auf bestehende gesetzliche und untergesetzliche Regelungen hingewiesen.

Mit dem Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) hat der Landtag die Initiative der Landesregierung aufgegriffen, für die Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, einen Sicherheitsverbund zu definieren. Jedes Mitglied des Sicherheitsverbundes hat auf der Basis von Risikoanalysen eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene Informationssicherheit, auch im Hinblick auf andere Mitglieder des Sicherheitsverbundes, zu gewährleisten. Für weite Bereiche der Verwaltung sind durch die niedersächsische Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) und das darauf basierende Informationssicherheitsmanagementsystem (ISMS) der Landesverwaltung untergesetzliche Regelungen getroffen worden, die der Gewährleistung der Informationssicherheit für die unmittelbare Landesverwaltung dienen. Der Bundesgesetzgeber hat mit dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) u. a. eine Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen und Regelungen für Unternehmen im besonderen öffentlichen Interesse getroffen. In diesem Zusammenhang ist auch die Datenschutzgrundverordnung zu nennen, die für die Verarbeitung personenbezogener Daten festlegt, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Mit Blick auf die Betroffenheit der Kommunalverwaltungen sei vorausgeschickt, dass die Kommunen ihre IT im Rahmen der kommunalen Selbstverwaltung eigenständig betreiben und daher auch eigenverantwortlich die IT-Sicherheit zu organisieren haben. Das Land unterstützt lediglich beratend. IT-Sicherheitsvorfälle im kommunalen Bereich werden gegenüber dem Land in der Regel nur dann bekannt, wenn diese seitens der betroffenen Kommune gemeldet werden. In Niedersachsen sind der Polizei bisher keine Fälle bekannt geworden, bei denen betroffene Kommunen oder öffentliche Verwaltungen die im Rahmen von Erpressungshandlungen im digitalen Raum geforderten Beträge gezahlt haben.

1. Wie beurteilt die Landesregierung die Gefahr von Hackerattacken auf die öffentliche digitale Infrastruktur in Niedersachsen?

Siehe Vorbemerkung.

2. Hat die Landesregierung Kenntnis über etwaige Angriffe im digitalen Raum? Wenn ja, wie viele waren es seit dem Jahr 2019 (bitte nach Jahren aufschlüsseln)?

Wie bereits eingangs erläutert, sind nur solche Vorfälle bekannt, die von einer betroffenen Kommune gemeldet oder zur Anzeige gebracht werden.

Im Betrachtungszeitraum vom 1. Januar 2019 bis zum 1. Oktober 2021 sind dem Landeskriminalamt Niedersachsen (LKA) insgesamt 14 Angriffe im digitalen Raum auf die öffentliche Infrastruktur niedersächsischer Kommunen bekannt geworden. Diese Angriffe erfolgten durch den Einsatz von Ransomware, die Nutzung von CEO-Fraud/Business, E-Mail-Compromise, das Kompromittieren einer Website, das Ausnutzen einer Sicherheitslücke im Mail-Server-System, Erpressungen per E-Mail bis hin zur Kompromittierung mittels Update-Software.

Die Angriffe verteilen sich auf die Jahre 2019 bis 2021 wie folgt:

– Jahr 2019: 4 Angriffe,

– Jahr 2020: 4 Angriffe,

– Jahr 2021: 6 Angriffe.

Dem N-CERT werden mehrere Hundert sogenannter Hochrisikoobjekte pro Monat gemeldet, die unterschiedliche Schadsoftwaretypen enthalten können. Die Anzahl schwankt je nach Aktivität einer „Angriffswelle“. Es kann sich dabei beispielsweise um unerlaubte Zugriffsversuche auf Bestandteile der IT-Infrastruktur handeln oder auch um Schadsoftware, die direkt an Empfängerinnen und Empfänger in den Behörden per E-Mail oder andere Kommunikations-Kanäle adressiert werden.

Im Jahr 2019 wurden in der Landesverwaltung Vorfallsmeldungen mit der Ransomware Emotet an das N-CERT übermittelt, die sich auf vereinzelte und lokal begrenzte Schadensereignisse bezogen. Die Ereignisse wurden schnell erkannt und eine Ausbreitung konnte verhindert werden. Im Laufe des Jahres 2019 wurden die Abwehrmaßnahmen deutlich verstärkt. Die Schutzeinrichtungen in der Landesverwaltung sind in mehreren Kaskaden so aufgebaut, dass eine Schadsoftware möglichst frühzeitig erkannt und blockiert wird. Aufgrund dieses resilienten Aufbaus wurden im Betrachtungszeitraum keine erfolgreichen Cyberangriffe in der Landesverwaltung verzeichnet.

3. Welche Bereiche der öffentlichen digitalen Infrastruktur sind aus Sicht der Landesregierung besonders bedroht?

Wie bereits in der Vorbemerkung dargestellt, greifen Cyberkriminelle neben Unternehmen oder Privatpersonen auch öffentliche Institutionen an. Eine Fokussierung auf bestimmte Bereiche der digitalen Infrastruktur öffentlicher Institutionen ist dabei nicht erkennbar.

4. Sind der Landesregierung Fälle bekannt, in denen Kommunen in Niedersachsen durch Cyber-Attacken geschädigt wurden? Wenn ja, wie groß waren die Schäden?

Siehe Antwort zur Frage 2. Wie bereits in den Vorbemerkungen ausgeführt, besteht seitens der Kommunen grundsätzlich keine Meldeverpflichtung gegenüber dem Land. Daher liegen der Landesregierung keine umfassenden und detaillierten Informationen über das jeweilige Schadensausmaß vor.

Mittels einer Abfrage bei den jeweiligen Kommunen ist seitens des Ministeriums für Inneres und Sport vorgesehen, konkrete Angaben zur jeweiligen Schadenshöhe nachzureichen. Dies war im Rahmen der für die Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Zeit nicht möglich.

5. Was tut die Landesregierung konkret, um die Cyber-Resilienz der Kommunen zu stärken?

Die Gewährleistung der Cybersicherheit kommunaler Einrichtungen ist eine eigenverantwortliche Aufgabe der jeweiligen Kommune. Aufgrund des Prinzips der kommunalen Selbstverwaltung besteht hier keine Zuständigkeit der Landesverwaltung. Gleichwohl bietet die Landesverwaltung im Bereich der Cybersicherheit eine Reihe von Unterstützungsleistungen, welche auch den Kommunen angeboten werden. Bereits seit 2014 stellt das Land Niedersachsen den niedersächsischen Kommunen die Leistungen des N-CERT zur Unterstützung von Maßnahmen zur Verhinderung, Erkennung und Bewältigung von Cyber-Angriffen kostenlos zur Verfügung.

Mittlerweile sind 106 Kommunen, ihre Verbände und IT-Dienstleister beim N-CERT registriert. Diese nutzen den Warn- und Informationsdienst und erhalten einen regelmäßigen Sicherheitslagebericht. Zudem können sie die Beratungsleistungen des N-CERT, etwa bei der Konzeption von Maßnahmen der IT-Sicherheit, oder auch akut im Rahmen der Bewältigung von Sicherheitsvorfällen, in Anspruch nehmen. In regelmäßigen Treffen mit den IT-Fachkräften in den Kommunen wird der Informationsaustausch gefördert und aktiv Feedback zu den Leistungen des N-CERT eingeholt.

Seit 2016 besteht ein kontinuierlicher fachlicher Austausch zwischen N-CERT und Kommunen im Rahmen des Kommunalen Sicherheitsbündnisses (KITSIN). Im Rahmen dieses Bündnisses wurden in der Vorpandemiezeit regelmäßig (mindestens zwei Mal im Jahr) Arbeitstreffen zwischen dem N-CERT und den niedersächsischen Kommunen sowie kommunalen Dienstleistern durchgeführt. Bei den Arbeitstreffen wurden Erfahrungen aus aktuellen Sicherheitsvorfällen und zum Umgang mit Sicherheitslücken ausgetauscht.

Seit 2020 hat das N-CERT ein eigens für die Kommunen konzipiertes und ebenfalls kostenloses Workshop-Angebot geschaffen. Die Zusammenarbeit zwischen N-CERT und den kommunalen Bereichen wird u. a. wegen der stetig wachsenden Nachfrage als sehr erfolgreich eingeschätzt. Derzeit weitet das N-CERT seine Leistungen an den kommunalen Bereich aus. Beispielsweise wird eine Informationsplattform über Schadsoftware und Cyberangriffe für den kommunalen Bereich mit ersten interessierten Kommunen erprobt.

Darüber hinaus besteht eine Reihe von Informationsangeboten seitens der Landesverwaltungen für interessierte Bürgerinnen, Bürger, Unternehmen und alle Bereiche der öffentlichen Verwaltung. Dazu zählen beispielsweise Sensibilisierungen über die Bedeutung der Informationssicherheit, Hinweise auf Informationsquellen oder über Hilfsangebote.

6. Bestehen innerhalb der Verwaltungshierarchie Backup-Systeme bei übergeordneten Behörden oder Kommunen, die die wesentlichen Aufgaben eines Verwaltungsorgans übernehmen können, welches durch einen Hackerangriff betroffen ist (Äquivalent zum Bankensystem)?

Im Bereich des Katastrophenschutzes sind nach § 23 Niedersächsisches Katastrophenschutzgesetz (NKatSG) andere Katastrophenschutzbehörden im Rahmen der Nachbarschaftshilfe und überörtlichen Hilfe untereinander zur Hilfeleistung verpflichtet, sofern dadurch nicht dringende eigene öffentliche Aufgaben beeinträchtigt werden. Sofern diese Nachbarschaftshilfe nicht ausreichend ist, wird seitens der Katastrophenschutzbehörde überörtliche Hilfe bei der für sie zuständigen Polizeidirektion angefordert.

Sollte im Rahmen eines Hackerangriffs oder aufgrund eines Ausfalls der IT-Systeme auf kommunaler Ebene der Katastrophenfall gemäß § 20 NKatSG festgestellt werden, wären Hilfeleistungen im Rahmen des NKatSG durch andere Behörden, Dienststellen oder Katastrophenschutzbehörden im Wege der Amtshilfe, Nachbarschaftshilfe oder überörtlichen Hilfe möglich, um beispielsweise kommunale Dienstleistungen aufrechtzuerhalten.

Des Weiteren verfolgt das Niedersächsische Landesamt für Brand- und Katastrophenschutz (NLBK) mit seinem Projekt „Katastrophenschutz Notfallnetz Niedersachsen“ den Aufbau eines auf Satellitentechnik basierenden Netzes, das bei Ausfall der IT-Kommunikationswege des Regelbetriebes die Kommunikation zwischen den Katastrophenschutzstäben des Landes und den Kommunen sicherstellt.

(Verteilt am 29.10.2021)