LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/2479**
8. Wahlperiode **21.08.2023**

KLEINE ANFRAGE

des Abgeordneten David Wulff, Fraktion der FDP

Cybersicherheit in Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

1. Welche Infrastrukturen – staatliche, aber auch private – stuft die Landesregierung als sogenannte „kritische Infrastrukturen“ ein?

Es wird auf die Antwort der Landesregierung zu den Fragen 1 bis 3 der Kleinen Anfrage auf Drucksache 8/1191 verwiesen.

2. Von wie vielen Cyberattacken hat die Landesregierung im Zeitraum von Januar 2019 bis Juni 2023 Kenntnis erhalten?

   a) Welche Infrastrukturen, Behörden und Unternehmen waren von Cyberattacken betroffen?
   b) Auf welche Art und Weise haben diese Angriffe stattgefunden?

Der Begriff „Cyberattacken“ ist polizeilich nicht definiert. Gerade im Bereich der Cybercrime zuzuordnenden Straftaten ist ein Rückgriff auf die Polizeiliche Kriminalstatistik (PKS) problematisch. Diese bildet diese Straftaten unzureichend und unkorrekt ab, da aus dem Ausland begangene Straftaten und Straftaten mit ungeklärten Tatort (bezogen auf den Staat) nicht in der PKS abgebildet werden. Maßnahmen zur Erfassung dieser Taten liefern bislang keine validen Daten.

Der Minister für Inneres, Bau und Digitalisierung hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 18. August 2023 beantwortet.

Unter Berücksichtigung der vorangegangenen Hinweise wird auf die Kapitel „Cybercrime“ der Jahresberichte zur PKS unter https://www.polizei.mvnet.de/Presse/Statistiken/ verwiesen. Aus Gründen des Datenschutzes können keine konkreten Angaben zu den Geschädigten gemacht werden. Daneben gibt es eine Dunkelziffer an nicht gemeldeten oder gar erkannten Angriffen.

Im Übrigen wird auf die Antwort der Landesregierung zu Frage 4 der Kleinen Anfrage auf Drucksache 8/18 verwiesen.

Zu den IT-Sicherheitsvorfällen besteht eine Meldepflicht der öffentlichen Verwaltung des Landes gegenüber dem CERT (Computer Emergency Response Team) Mecklenburg-Vorpommern. Darüber wurden folgende Vorfälle gemeldet:

Jahr	**Anzahl der gemeldeten Sicherheitsvorfälle**
2019	15
2020	20
2021	22
2022	31
bis Juni 2023	14

Zu a)

Von den Cyberangriffen waren überwiegend kleine und mittelständische Unternehmen, Arztpraxen, Schulen, mehrere öffentliche Verwaltungen und Dienstleister für den öffentlichen Sektor sowie eingetragene Vereine betroffen.

Zu b)

Aus polizeilicher Sicht reicht das Angriffsspektrum vom Ausspähen von Daten, über DDoS-Attacken und Erpressungen bis zur Computersabotage durch Verschlüsselung (Ransomware).

Vom CERT werden folgende Angriffsmuster verstärkt detektiert:
1. Versand von schadhaften SPAM-E-Mails in der Hoffnung, dass Beschäftigte die E-Mail öffnen und den enthaltenen Schadcode (Drive-by-Download oder direkt innerhalb der E-Mail) zur Ausführung bringt.
2. Versand von Phishing-E-Mails, um Zugangsdaten der Beschäftigten über nachgebaute Webseiten (Fake-Webseiten) abzufangen.
3. Ausnutzung von fehlerhaft konfigurierten Systemen, welche unter Umständen vom Internet aus erreichbar sind.
4. Ausnutzung von Sicherheitsschwachstellen (zum Beispiel Zero-Day).

3. Welche Schäden und Störungen haben die Attacken jeweils verursacht, die im Sinne der Initiatoren erfolgreich waren?

   a) Wie hoch waren die Kosten zur Behebung der jeweiligen Schäden?
   b) Konnten die Schäden durch die Behörden/Unternehmen/Infrastrukturen selbst behoben werden?
   c) Wenn nicht, welche zusätzlichen Kapazitäten/Ressourcen waren notwendig?

Zu 3, a), b) und c)

Zu den Schäden und Auswirkungen im Einzelnen werden von der Landesverwaltung keine Daten erhoben. Vor allem liegen keine Informationen zur Behebung von Schäden außerhalb der Landesverwaltung vor. Es ist polizeilich bekannt, dass vor allem von größeren Unternehmen regelmäßig externe IT-Dienstleister hinzugezogen werden. Die Kostenstruktur dieser und die tatsächlichen Leistungsabrechnungen sind jedoch nicht bekannt.

Aber auch innerhalb der Landesverwaltung sind die Schäden oder Störungen in ihren Ausmaßen höchst unterschiedlich. Bis dato jedoch ist es den IT-Experten und dessen IT-Dienstleistern gelungen, weiterreichende Kompromittierungen von IT-Infrastrukturkomponenten bei erfolgreichen Angriffen entgegenzuwirken. Bis dato konnten die Schäden an IT-Systemen der Landesverwaltung auch mit Hilfe des Landes-IT-Dienstleisters selbst behoben werden. Für die forensische Analyse der Restsysteme auf eine mögliche Betroffenheit wurde unter anderem auf externe Expertise zurückgegriffen (Hiscox, Telekom), um die eventuelle Down-Time von Systemen drastisch zu verkürzen.

4. Inwiefern hat sich nach Auffassung der Landesregierung seit 2019 die Gefährdungslage für kritische Infrastrukturen, Behörden und Unternehmen, Opfer von Cyberattacken zu werden, insbesondere auch vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine verändert?

Es wird auf die Vorbemerkung und die Antwort der Landesregierung zu Frage 1 der Kleinen Anfrage auf Drucksache 8/2048 verwiesen.

5. Welche zusätzlichen Maßnahmen sind seit 2019 ergriffen worden, um den Ausfall kritischer Infrastrukturen, beispielsweise Strom-, Gas-, Fernwärme- und Wasserversorgung durch Cyberattacken vorzubeugen?

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz–BSIG) und die zugehörige Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) beschreiben unter anderem verpflichtende Schutzmaßnahmen vor IT-Gefahren, die Unternehmen Kritischer Infrastruktur im Sinne der Verordnung umsetzen müssen. Alle anderen Unternehmen sollten intrinsisch motiviert sein, um eigene Schutzmaßnahmen zu treffen.

Zudem wird auf die Antwort der Landesregierung zur Frage 3 der Kleinen Anfrage auf Drucksache 8/2048 verwiesen.

6. Wie sind die für die Cybersicherheit zuständigen Behörden im Land personell und finanziell ausgestattet?

   a) Ist diese Ausstattung angesichts der gegenwärtigen Bedrohungslage noch ausreichend?
   b) Wenn nicht, wo muss mit welchen Mitteln nachgebessert werden?

Die Fragen 6, a) und b) werden zusammenhängend beantwortet.

In den Ansätzen der Titel der Maßnahmegruppe 59 „Informationstechnik“ sowie der Maßnahmegruppe 58 „IT-Bedarf für ressortübergreifende DV-Verfahren“ der Einzelpläne sind anteilig Ausgaben für IT-Sicherheitsmaßnahmen enthalten, die sich aber nicht näher spezifizieren lassen. Darüber hinaus wurden beim Ministerium für Inneres, Bau und Digitalisierung aus dem MV-Schutzfonds im Kapitel 0481 2 800 000 Euro beim Titel 511.22 „IT-Sicherheit“ (MG 07) und 146 000 Euro beim Titel 525.07 „Fortbildung für Informationssicherheit“ (MG 07) für die Jahre 2023/2024 bereitgestellt. Für die IT-Sicherheit stehen vier (Plan-)Stellen zur Verfügung.

7. Inwiefern werden die in den Fragen 5 und 6 adressierten Präventionsmaßnahmen regelmäßig einer Evaluation in Bezug auf ihre Wirksamkeit unterzogen?

Es wird auf die Antworten der Landesregierung zu Frage 6 der Kleinen Anfrage auf Drucksache 8/21 und zu Frage 5 der Kleinen Anfrage auf Drucksache 8/24 verwiesen.

Des Weiteren erfolgen zahlreiche Penetrationstests auf IT-Infrastrukturkomponenten der Landesverwaltung. Bei einem Penetrationstest übernimmt die testende Person die Rolle eines Angreifers und versucht, das zu testende Netzwerk oder System zu infiltrieren. Diese Art von Test ist extrem realitätsnah und gibt neue Aufschlüsse über eventuelle Schwachstellen und mögliche Migrationsmaßnahmen.

8. Wie hat sich die Zahl von Cyberattacken insbesondere auf kleinere und mittlere Unternehmen im Land seit 2019 entwickelt?
   Ist seit dem 24. Februar 2022 eine auffällige Entwicklung bei der Zahl der Attacken festzustellen?

Es wird auf die Antwort zu Frage 2 und im Übrigen auf die Antwort der Landesregierung zu der Kleinen Anfrage auf Drucksache 8/2048 verwiesen.

9. Welche Aus- und Fortbildungsmöglichkeiten werden Polizeivollzugsbeamtinnen und -beamten angeboten, um die Aufgaben im Rahmen ihres Einsatzes gegen Cybercrime entsprechend wahrzunehmen?

Die Nachwuchskräfte der Polizei werden an der Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege auch auf dem Gebiet der Bekämpfung von Internetkriminalität geschult und erwerben damit bereits im Vorbereitungsdienst Kompetenzen im Umgang mit Cyberkriminalität. Die Ausbildungspläne und die Modulhandbücher werden regelmäßig evaluiert und an die Erfordernisse der Praxis angepasst.

Die Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege bietet im Rahmen der Fortbildung folgende Lehrgänge mit thematischem Bezug an:

- OZ 6840 Cybercrime–Forensik Grundlagen Cellebrite Reader
- OZ 6841 Ersteinsteiger Cybercrime
- OZ 6842 Phyton Grundlagen
- OZ 6843 Cybercrime–Ermittlungen im Internet
- OZ 6844 Tatmittel Internet
- OZ 6846 Ermittlungsmöglichkeiten bei Kryptowährungen
- OZ 6847 Cybercrime Speziallehrgang–CTB Notepad++ Dir3ctory.

Zusätzlich finden Schulungen in den Dienststellen statt und es werden Angebote externer Anbieter von entsprechenden Fortbildungsmaßnahmen wahrgenommen.

Darüber hinaus werden in den Ermittlungsbereichen, welche sich mit Cybercrime befassen, nach Bedarf IT-Fachkräfte mit entsprechenden externen Hochschulabschlüssen auf der Grundlage von § 16 der Polizeilaufbahnverordnung als sogenannte Seiteneinsteiger in den Polizeivollzugsdienst des Landes eingestellt.

10. Wie viele Ermittlungsverfahren hat es aufgrund welcher Delikte im Bereich Cyberkriminalität seit 2019 bei der Staatsanwaltschaft zusätzlich gegeben (sofern die Verfahren abgeschlossen sind, den Ausgang der jeweiligen Verfahren mitteilen).

Im Rahmen der bei den Staatsanwaltschaften des Landes geführten amtlichen Justizgeschäftsstatistik erfolgt keine gesonderte Erfassung von Cyberkriminalität innerhalb der jeweiligen Delikte oder Sachgebiete. Eine händische Auswertung der Akten wäre mit Aufwand verbunden, der schon mit der aus Artikel 40 Absatz 1 Satz 1 der Verfassung des Landes Mecklenburg-Vorpommern folgenden Pflicht zur unverzüglichen Beantwortung Kleiner Anfragen nicht zu vereinbaren wäre.