

## **KLEINE ANFRAGE**

**des Abgeordneten Thomas des Jesus Fernandes, Fraktion der AfD**

**Sicherheitslage vor Cyberangriffen auf Bürger-Datensysteme**

**und**

## **ANTWORT**

**der Landesregierung**

Unter Bezugnahme auf den Bericht des NDR-MV vom 16. Oktober 2021 stellen sich Fragen (NDR - Cyberangriff: Auswirkungen auch auf andere Landesteile).

1. Ist der Landesregierung die Grundlage bekannt, auf die sich die Aussage des Schweriner Oberbürgermeisters Dr. Rico Badenschier, dass ... „zwar die eigenen Daten verschlüsselt worden seien, diese aber nicht an externe Stellen weitergegeben wurden“ stützt?

Nein.

2. Ist der Landesregierung bekannt, ob in diesem aktuellen Fall bereits Lösegeldforderungen eingegangen sind?

Der Landesregierung sind solche Lösegeldforderungen nicht bekannt.

3. Gab es in der Vergangenheit in Mecklenburg-Vorpommern bereits ähnliche Cyberangriffe?  
Wenn ja, welche öffentlichen Einrichtungen und sensiblen Infrastruktureinrichtungen waren von Cyberangriffen betroffen?

Für den Zeitraum 2015 bis 2021 sind aktuell insgesamt 13 Angriffe mittels Ransomware auf staatliche oder öffentliche Einrichtungen des Landes MV polizeilich bekannt geworden.

Betroffen waren zwei Schulen, ein Reha-Zentrum, eine rechtsfähige Teilkörperschaft einer Universität, regionale Einrichtungen von Hilfs- und Wohlfahrtsorganisationen, ein Nahverkehrsunternehmen, eine Landtagsfraktion sowie eine Stadt- und Landkreisverwaltung. Eine weitere Konkretisierung ist zum Schutz der betroffenen Einrichtungen nicht möglich.

Eine Einordnung von Unternehmen als „sensibile Infrastruktureinrichtungen“ gibt es in der polizeilichen Kriminalstatistik nicht, weshalb auch keine diesbezüglichen Zahlen benannt werden können.

Es wird zudem darauf verwiesen, dass im Phänomenbereich Cybercrime ein sehr hohes Dunkelfeld besteht, das heißt nicht alle Delikte werden den Ermittlungsbehörden bekannt.

4. Welche Rechtsgrundlage regelt die Höhe der in der Vergangenheit gezahlten Lösegelder?

Keine.

Die Landesregierung folgt der Empfehlung seitens der Polizei und des Bundesamtes für Sicherheit in der Informationstechnik, grundsätzlich nicht auf Lösegeldforderungen einzugehen.

5. Welchem Haushaltsposten wurden Lösegelder bislang entnommen?

Es wird auf die Antwort zu Frage 4 verwiesen.

6. Welche zusätzlichen Maßnahmen gedenkt die Landesregierung zu ergreifen, um Cyberangriffe in Zukunft auszuschließen?

Die Landesregierung wird weiterhin die bestehenden technischen, organisatorischen und infrastrukturellen Schutz- und Sicherheitsmaßnahmen auf ihre Wirksamkeit prüfen sowie gegebenenfalls neue Maßnahmen aufgrund der sich stets ändernden Bedrohungslage entwickeln und implementieren.

Dazu gehören die fortlaufende Sensibilisierung und Schulung der Beschäftigten der öffentlichen Verwaltung, eine konsequente Umsetzung und Aufrechterhaltung eines Sicherheitsniveaus unter anderem im Landesdatennetz CN LAVINE sowie der Ausbau des Computersicherheits-Ereignis- und Reaktionsteam Mecklenburg-Vorpommern (CERT M-V).

Dennoch ist sich die Landesregierung bewusst, dass sich Cyberangriffe auch in Zukunft nicht vollständig verhindern lassen. Die bereits getroffenen und zukünftig ergänzend wirkenden Maßnahmen können jedoch die möglichen Auswirkungen derartiger Cyberangriffe signifikant reduzieren.

Zusätzlich flankiert wird dieser Prozess durch umfangreiche Maßnahmen seitens der Landespolizei, die seit 2011 über kompetente Ansprechpartner im Bereich der Cybercrimebekämpfung verfügt. So ist die Zentrale Ansprechstelle Cybercrime Mecklenburg-Vorpommern (ZAC MV) im Landeskriminalamt angegliedert und fungiert als Ansprechpartner für Unternehmen sowie öffentliche und nicht öffentliche Institutionen.

Die Mitarbeiterinnen und Mitarbeiter des Landeskriminalamtes beraten und unterstützen hier rund um das Thema Cybercrime. Sie informieren zielgruppengerecht auf verschiedenen Veranstaltungen über Sicherheitsrisiken, geben Verhaltensempfehlungen in Hinblick auf den aktuellen Handlungsbedarf und stimmen im Schadensfall die erforderlichen Maßnahmen ab.

Im Rahmen der Sicherheitspartnerschaft Mecklenburg-Vorpommern werden zudem regelmäßig Veranstaltungen angeboten. Hier kommt es zum einen zu fachlichen Diskussionen, zum anderen aber auch zum Austausch von Erfahrungen mit klein- und mittelständischen Unternehmen sowie größeren Firmen.

In der vom Bundeskriminalamt herausgegebenen Schrift „Cybercrime - Handlungsempfehlungen für die Wirtschaft“, unter Nennung der Zentralen Ansprechstellen Cybercrime sowie der Broschüre „Ransomware - Unternehmen und Institutionen als Zielscheibe“ wird seitens des Landeskriminalamts insbesondere auf folgende Maßnahmen aufmerksam gemacht:

- Absicherung gegen Schadsoftware,
- regelmäßige Schulungen zur Thematik und aktuellen Modus Operandi Verschlüsselung nutzen bei der Übermittlung von personenbezogenen Daten,
- regelmäßige (offline) Backups.

Im Übrigen wird auf die Antwort der Landesregierung zu Frage 1 der Kleinen Anfrage auf Drucksache 8/18 verwiesen.