LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/2048**
8. Wahlperiode **10.05.2023**

KLEINE ANFRAGE

des Abgeordneten Michael Meister, Fraktion der AfD

Russische Cyberangriffe auf Polizei und Landesregierung in Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

Vorbemerkung

Die Auswirkungen des Angriffskrieges Russlands auf die Ukraine sind auch im Cyberraum zu spüren. Das CyberPeace-Institut in Genf hat im Jahr 2022 mehr als 850 Cyberattacken registriert. Daneben gibt es eine hohe Dunkelziffer an nicht gemeldeten oder gar erkannten Angriffen. Die Angreifer, die teils mit staatlicher Duldung oder auch Unterstützung operieren, sind gut ausgebildet und verfügen über entsprechend große Ressourcen. Daneben nutzen diese Gruppen auch immer öfter Crowdsourcing für Distributed Denial-of-Service (DDoS)-Angriffe. Dies bedeutet, dass Sympathisanten in der Bevölkerung umworben und deren Computer über Scripte automatisch für Attacken herangezogen oder die Scripte Sympathisanten zur Nutzung überlassen werden.

Durch das Bekanntwerden der „Vulcan Files“ zeigt sich die Strategie Russlands, wie im Cyberraum agiert werden soll (https://www.zdf.de/nachrichten/digitales/vulkan-files-cyberangriff-hacker-ukraine-krieg-russland-100.html).

> Laut Schweriner Volkszeitung kam es am 4. April 2023 zu massiven Cyberangriffen auf die staatlichen Sicherheitsorgane und die Landesregierung in Mecklenburg-Vorpommern. Mehrere Internetseiten des Regierungsportals Mecklenburg-Vorpommern waren nicht zu erreichen. Betroffen waren die Websites der Ministerien und der Landespolizei sowie das MV-Serviceportal. Das Ministerium für Inneres, Bau und Digitalisierung sieht seit dem vergangenen Jahr eine erhöhte Bedrohungslage.
> (SVZ.de - Cyberangriff in MV: Websites der Polizei und Regierung lahmgelegt)

Der Minister für Inneres, Bau und Digitalisierung hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 9. Mai 2023 beantwortet.

Daher ergeben sich zur Drucksache 8/723 Nachfragen.

1. Wie definiert beziehungsweise beurteilt die Landesregierung aktuell das Bedrohungspotenzial durch russische Nachrichtendienste und russische Hackergruppen (bitte detailliert begründen)?

Das Eskalationsrisiko im Cyberraum bleibt weiterhin auf hohem Niveau. Mögliche Auswirkungen auf Deutschland sind weiterhin wahrscheinlich. Im letzten Jahr wurde eine hohe Bedrohung durch Cyberangriffe beobachtet. Durch den russischen Angriffskrieg auf die Ukraine erhöhte sich das Bedrohungspotenzial unter anderem durch russische Nachrichtendienste sowie durch mehrere, neu in Erscheinung getretene Hacker-Gruppen.

2. Wie viele Spionage- oder Cyberangriffe auf das Land Mecklenburg-Vorpommern und deren Institutionen und Behörden sind seit dem Beginn des russischen Angriffskrieges auf die Ukraine registriert worden (bitte detailliert nach Datum, Angriffsmethode, angegriffener Behörde oder Institution und Erfolg beziehungsweise Misserfolg des Angriffs aufschlüsseln)?

Cyberangriffe gegen die IT-Infrastruktur der Landesverwaltung werden fortlaufend detektiert. Davon wird eine Vielzahl automatisiert abgewehrt. Bei besonders auffälligen Ereignissen ist eine Bewertung durch Analysten notwendig. Statistische Daten über Angriffe werden nicht erhoben. Die Mehrzahl der Angriffe besteht aus Scan-Aktivitäten, das heißt, die potenziellen Angreifer versuchen über verschiedene Methoden, Informationen über die aus dem Internet zugängliche IT-Infrastruktur mit den dortigen IT-Systemen zu gewinnen.

3. Welche Maßnahmen wurden durch die Landesregierung seit dem 24. Februar 2022 eingeleitet beziehungsweise umgesetzt, um das Bedrohungspotenzial für das Land Mecklenburg-Vorpommern signifikant zu reduzieren (bitte detailliert nach Maßnahme und Datum aufschlüsseln)?

Die Landesregierung hat zusammen mit dem IT-Landesdienstleister unterschiedlich wirkende Vorsorgemaßnahmen zur Abwehr verschiedener Angriffsformen auf die IT-Infrastruktur getroffen. Diese beinhalten unter anderem die Erhöhung der Detektions- und Reaktionsfähigkeit mit Maßnahmen, die durch den festgelegten Sicherheitsstandard IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik geprägt sind. Zu den Maßnahmen gehören insbesondere die erweiterte Betriebsüberwachung besonders sensibler und kritischer Komponenten der IT-Infrastruktur, die Protokollierung und Korrelation von Protokoll- und Ereignisdaten sowie das Härten der Systeme. Zudem werden bekannte IP-Adressen von Angreifern gesperrt und der Datenfluss auf bekannte Malware geprüft.

Die implementierten Maßnahmen werden laufend auf ihre Wirksamkeit überprüft und bei erkennbarem Bedarf angepasst. Zudem befindet sich das Computer Emergency Response Team (CERT) des Landes in engem Austausch mit anderen Landes-CERTs sowie dem CERT-Bund, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und anderen Dienststellen von Sicherheitsbehörden.

4. Auf Frage 4 der Kleinen Anfrage 8/723 antwortete die Landesregierung wie folgt: „Für Cyberangriffe gilt generell, dass nur gelegentlich der Urheber sicher festgestellt werden kann, sodass eine differenzierende Zuordnung bezüglich ausländischer Spionageaktivitäten oder anderer Angreifer nicht möglich ist.“
   Vertritt die Landesregierung auch heute noch diese Aussage?

Ja.

5. Konnten die russischen Hacker bei dem am 4. April 2023 durchgeführten Cyberangriff Daten erbeuten, beschädigen, löschen, manipulieren beziehungsweise digitale Infrastrukturen und Kommunikationssysteme infiltrieren?

Nach derzeit vorliegenden Informationen war dies den Angreifern nicht möglich, zumal die detektierte Angriffsmethode nicht auf die in der Fragestellung umrissenen Ziele abzielte.

6. Gibt es für alle Daten der Polizei und der Landesregierung Sicherheitsbackups, die vor Cyberangriffen geschützt sind?

Die Daten der Landesregierung werden nach den Anforderungen des BSI IT-Grundschutzes unter Berücksichtigung der Ergebnisse aus den Schutzbedarfsanalysen gesichert und regelmäßig in Wiederherstellungsprozeduren auf Funktionsfähigkeit geprüft.

Einen kompletten Schutz gibt es jedoch nicht. Mit ausreichenden Ressourcen und Berechtigungen ist es grundsätzlich möglich, sich zu jedem IT-System einen Zugang zu verschaffen.