LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/2624**
8. Wahlperiode **05.10.2023**

KLEINE ANFRAGE

des Abgeordneten Paul-Joachim Timm, Fraktion der AfD

Cyberangriffe in Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

Im Cyber-Brief Nr. 02/2023 des Bundesamtes für Verfassungsschutz wird von aktuellen Hinweisen berichtet, die auf die Bedrohung deutscher kleiner und mittelständischer Unternehmen (KMU) sowie von Privathaushalten durch Cyberangriffe hindeuten. Auch private Haushalte werden deswegen aufgefordert, Maßnahmen zu ergreifen, um die Nutzung ihrer Geräte für sog. Verschleierungsnetzwerke auszuschließen.

1. Wie oft kam es seit 2020 zu sog. Spionageattacken oder Cyberattacken mit Hilfe sog. Verschleierungsnetze über den Zugriff auf Netzwerkgeräte privater Haushalte?

Aufgrund einer großen Anzahl von täglichen Angriffsversuchen, die von den Sicherheitsexperten der Landesverwaltung und ihrer IT-Dienstleister als sogenanntes Grundrauschen im Tagesgeschäft (sicherheitsrelevantes Ereignis) klassifiziert werden, ist es kaum möglich, eine konkrete Anzahl von Cyberattacken, die mithilfe von Verschleierungsnetzwerken durchgeführt werden, zu benennen. Viele Angriffsversuche werden automatisiert durch die verschiedenartig wirkenden Schutzsysteme der Landesverwaltung entweder direkt beim Internetprovider oder am äußeren Schutzperimeter des Landesrechenzentrums beim Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ) abgewehrt. In den letzten drei Jahren hat das Computer-Notfall-Team (Computer Emergency Response Team, kurz CERT M-V) eine deutliche Zunahme von Angriffen auf die Verfügbarkeit (DDoS-Angriffe) gegen die IT-Infrastruktur der Landesverwaltung festgestellt. Die CERTs anderer Bundesländer bestätigen diese Entwicklung.

Der Minister für Inneres, Bau und Digitalisierung hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 3. Oktober 2023 beantwortet.

Bei der Analyse des Angriffsvektors DDoS fällt auf, dass die Angreifer für ihre großangelegten DDoS-Angriffe oftmals kompromittierte private IT-Systeme, aber auch schlecht gesicherte oder nicht gepatchte „Internet-of-Things-Geräte“ (IoT-Geräte) mit bekannten Sicherheitslücken nutzen. Ziel der Angreifer ist es, die Kapazität des Internetanschlusses ihrer Opfer und ihrer dedizierten IP-Adressen zu nutzen, um ihrem Angriff eine höhere Bandbreite zu verleihen und Rückschlüsse auf sich selbst zu verschleiern. Für die Opfer bedeuten diese Angriffe einen Verlust der Verfügbarkeit ihrer IT-Systeme beziehungsweise ihrer E-Commerce-Plattformen und durch die Digitalisierung ihrer Geschäftsprozesse gegebenenfalls einen Umsatzverlust.
Eine Trennung zwischen Spionageattacken, also Angriffen mit nachrichtendienstlichem Hintergrund, und anderen Cyberattacken ist nur schwer möglich. Dies gilt besonders, wenn „Verschleierungsnetze“ genutzt werden. Bei DDoS-Angriffen ist in der Regel kein Spionagehintergrund zu erwarten, da hier das Ziel nicht die Erlangung von Daten ist.

2. Welche Informationen hat die Landesregierung über Cyberangriffe auf Netzwerke privater Haushalte oder die Nutzung privater Geräte zum Aufbau sog. Verschleierungsnetzwerke in Mecklenburg-Vorpommern (bitte nach Art und Anzahl aufschlüsseln)?

Die Sicherheitsexperten der Landesverwaltung sowie das CERT M-V stehen im ständigen, engen Austausch mit den Sicherheitsexperten anderer Bundesländer und dem Bund.
Die Zielgruppe der Länder-CERTs sind die jeweiligen Landesverwaltungen und gegebenenfalls partiell die Kommunalverwaltungen.
Private Haushalte stehen nicht im Fokus der staatlichen und/oder kommunalen CERTs.

3. Welche konkreten Maßnahmen plant die Landesregierung, um die Nutzung von Geräten privater Haushalte in Zukunft zu erschweren und Geräte der Bürger besser gegen Missbrauch zu schützen?

Um das Sicherheitsniveau von IT-Systemen beziehungsweise von IoT-Geräten für die Bürgerinnen und Bürger transparenter zu gestalten, hat der Gesetzgeber Ende 2021 ein IT-Sicherheitskennzeichen eingeführt.
Bei dem IT-Sicherheitskennzeichen handelt es sich um ein freiwilliges Etikett, das Herstellern von IT-Produkten sowie IT-Diensteanbietern die Möglichkeit bietet, Transparenz zu schaffen und den Bürgerinnen und Bürgern zu beweisen, dass deren Produkte und Dienstleistungen über definierte Sicherheitseigenschaften verfügen. Neben den Sicherheitseigenschaften von Produkten sind jedoch auch die Bürgerinnen und Bürger gefordert, die durch die Hersteller bereitgestellten Sicherheitsupdates für ihre IT-Produkte zu installieren.
Analog zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) plant die Regierung der Vereinigten Staaten von Amerika (USA) ebenfalls die Einführung eines neuen Gütesiegels, das den Verbrauchern zeigt, bei welchen IoT-Geräten das Thema IoT-Sicherheit besonders berücksichtigt wird.