

KLEINE ANFRAGE

der Abgeordneten Eva-Maria Kröger, Fraktion DIE LINKE

**Angriffe auf die Informationstechnik und das Datennetzwerk des Landes
Mecklenburg-Vorpommern**

und

ANTWORT

der Landesregierung

Vorbemerkung

Für die Landesregierung sind die Gewährleistung und Aufrechterhaltung der Informationssicherheit ein kontinuierlicher Prozess. Unter diesem Aspekt spiegelt sich die Kernproblematik der Informationssicherheit beziehungsweise IT-Sicherheit sehr gut wider: Die mit der Informationssicherheit assoziierten Aufgaben und Tätigkeiten müssen regelmäßig wiederholt und neu durchlaufen werden. Nur unter dieser Prämisse wird ein bestmöglicher Schutz für die informationstechnischen Systeme der Landesverwaltung mit Blick auf die drei Grundwerte der Informationssicherheit - Vertraulichkeit, Verfügbarkeit und Integrität - auch bei sich verändernden Gefährdungslagen erreicht.

Bislang geht die Landesregierung davon aus, dass es keine erfolgreichen, zielgerichteten Cyberangriffe auf die informationstechnischen Systeme der Landesverwaltung gab. Aufgrund geltender IT-Sicherheitsrichtlinien und umgesetzter Sicherheitsmaßnahmen ist es grundsätzlich nicht möglich, vom Internet oder von anderen Netzen aus direkt auf die informationstechnischen Systeme der Landesverwaltung zuzugreifen. In diesem Zusammenhang haben die kürzlich veröffentlichten Cyberangriffe auf das Auswärtige Amt keine unmittelbaren Auswirkungen auf die IT-Sicherheit der informationstechnischen Systeme der Landesverwaltung.

1. Wie ist das Datennetz des Landes Mecklenburg-Vorpommern - einschließlich des Daten-netzwerks des Landtages sowie das Datennetzwerk von Landesbehörden - vor möglichen Cyberattacken geschützt?

Das Datennetz des Landes, das Corporate Network Landeskommunikationsvermittlungs- und Informationsnetz (CN LAVINE) ist ein nicht-öffentliches, geschlossenes Transportnetz. Es wird durch die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) im Auftrag des Landes betrieben. Die geltenden Regularien einschließlich IT-Sicherheitsrichtlinien für den Zugang zum Datennetz des Landes sind im Rahmenvertrag CN LAVINE, in den jeweiligen Leistungsscheinen mit den CN LAVINE-Teilnehmern vertraglich vereinbart.

Für die Netzsicherheit im Datennetz des Landes sind sowohl technische und als auch organisatorische Sicherheitsmaßnahmen auf Basis des Sicherheitsstandards BSI IT-Grundschutz (wie zum Beispiel eine Phalanx von Anti-Virus-Lösungen, Netzsegmentierung) implementiert. Am zentralen Netzübergang des CN LAVINE wird durch die DVZ M-V GmbH eine mehrstufige Firewall-Lösung betrieben. In ihrer Gesamtheit sollen diese Sicherheitsmaßnahmen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und IT-Systemen innerhalb des CN LAVINE gewährleisten.

Ergänzend zu diesen zentralen Sicherheitsmaßnahmen sind die lokalen Netzwerke der CN LAVINE-Teilnehmer durch weitere, in der Regel technische Sicherheitsmaßnahmen, wie beispielsweise Firewall-Lösungen mit Web-Proxy geschützt. Parallel hierzu existieren zentral verwaltete Anti-Virus-Lösungen für den Schutz der Arbeitsplatzrechner.

Konkrete Informationen zu technischen und organisatorischen Sicherheitsmaßnahmen für das Datennetzwerk des Landtages einschließlich des Landesrechnungshofes liegen der Landesregierung nicht vor.

2. Wie viele Cyberattacken auf die Informationstechnik und das Datennetzwerk des Landes Mecklenburg-Vorpommern wurden in den letzten fünf Jahren registriert (bitte nach Jahren, Landesbehörden/ Landtag und Art der Attacke getrennt aufschlüsseln)?

Zum Schutz vor IT-Angriffen nutzen die Behörden der Landesverwaltung für ihre Internetzugänge unter anderem ein zentrales Sicherheitssystem, das aus mehreren Firewall- und Viruswallsystemen besteht und durch die DVZ M-V GmbH betrieben wird. Dieses zentrale Sicherheitssystem ermöglicht eine konzentrierte Gefahrenkontrolle und Gefahrenabwehr.

Nach Auskunft der DVZ M-V GmbH verarbeiten die zentralen Firewall-Systeme der Landesregierung je nach Aufkommen bis zu 150.000 Datenpakete je Sekunde. In jeder Sekunde verursachen durchschnittlich rund 20 dieser Pakete Warnmeldungen, die von den Herstellern der Firewall-Systeme mit dem Level „kritisch“ eingestuft sind. Auf diese Weise summiert sich die Zahl der pro Tag möglichen Angriffsversuche auf mehrere Hunderttausend.

Zu den Angriffsversuchen zählen unter anderem die folgenden Angriffsarten:

- SPAM/E-Mail mit schadhaften Anhängen, zum Beispiel Viren, Trojanern oder Würmern: An einem durchschnittlichen Arbeitstag erreichen circa 350.000 E-Mails das zentrale Sicherheitssystem in der DVZ M-V GmbH. Von diesen E-Mails werden durch das zentrale Sicherheitssystem circa 302.500 E-Mails als SPAM erkannt; 2.500 E-Mails sind mit gefährlichen Anlagen belastet. Lediglich 45.000 E-Mails (rund 12,85 Prozent) stellen das „normale“ E-Mailaufkommen der Landesverwaltung dar. In Spitzenzeiten (Feiertage, Wahlen, bundesweite/internationale Kongresse oder Besuche von Staatsoberhäuptern) potenzieren sich diese Zahlen um ein Vielfaches.
- Port-Scans: Hacker suchen gezielt nach verwundbaren IT-Systemen, um diese unter anderem für den SPAM-Versand, für die Verbreitung von zumeist urheberrechtlich geschützten Inhalten oder zur Vorbereitung von Denial-of-Service-Angriffen (Verfügbarkeitsangriffen) gegen Dritte zu missbrauchen. Bei Denial-of-Service-Angriffen soll durch Überlastung der IT-Infrastruktursysteme ein Ausfall von Netzwerkdiensten erreicht werden.

Konkrete Statistiken darüber, wie viele Cyberattacken, welcher Art und in welchem Zeitraum festgestellt wurden, liegen nicht vor. Aufgrund der hohen IT-Sicherheitsstandards konnten die Angriffsversuche auf das zentrale Sicherheitssystem bisher abgewehrt werden.

3. Welche Kommunikations- bzw. Informationswege sind bei Angriffen auf die Informationstechnik und das Datennetzwerk des Landes Mecklenburg-Vorpommern einzuhalten?

Eine Meldepflicht bei erkannten IT-Angriffen beziehungsweise IT-Sicherheitsvorfällen für die Behörden und Einrichtungen des Landes ergibt sich aus der „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ (IS-Leitlinie). Die auf dieser Meldepflicht aufbauenden Kommunikationswege beziehungsweise Informationswege sind im „Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ (ISM-MV) weiterführend beschrieben.

Ein ganzheitlicher Prozess für die Behandlung von IT-Sicherheitsvorfällen mit einer engen Zusammenarbeit mit dem Computer Emergency Response Team Mecklenburg-Vorpommern (CERT M-V) wurde in der ressortübergreifenden Informationssicherheitsorganisation des Landes, in der Kommission für Informationssicherheit diskutiert, abgestimmt und etabliert. Er wird im Rahmen des kontinuierlichen Verbesserungsprozesses fortlaufend überprüft und aktualisiert.

4. Welche Datenbestände inklusive personenbezogener Daten waren aufgrund der in der Antwort zu Frage 2 benannten Fälle betroffen?

Der Landesregierung sind keine IT-Sicherheitsvorfälle mit personenbezogenen Daten bekannt.

5. Welche Schäden und in welcher Höhe wurden durch Cyberangriffe auf das Datennetzwerk des Landes hervorgerufen?

Die am Perimeter des Netzüberganges vom Landesdatennetz zum Internet eingesetzten IT-Systeme mit ihren Schutzfunktionen registrieren täglich eine Vielzahl von Angriffsversuchen.

Im ehemaligen Ministerium für Wirtschaft, Arbeit und Tourismus ist es im Jahr 2009 zu einem Vorfall mit dem Conficker-Virus gekommen. Durch den Virusbefall wurde das Netzwerk des Ministeriums für einen Tag blockiert. Schäden finanzieller Art traten nicht auf.

Im Jahr 2016 war ein primärer Angriffsvektor von Hackern oder von Cyberkriminellen der Versand von gefälschten und mit Schadsoftware behafteten E-Mails. In diesem Kontext gab es vereinzelt Infektionen, die vorsorglich eine Neuinstallation der betroffenen Rechnersysteme notwendig machten. Weitreichende Schäden, insbesondere Datenverluste durch Ransomware (Verschlüsselungstrojaner) konnten durch Datenrücksicherungen vermieden werden.

Durch einen IT-Sicherheitsvorfall im Jahr 2016 (erfolgreicher Befall mit Ransomware) ist zusätzliche Unterstützungsleistung durch die DVZ M-V GmbH notwendig gewesen. Dadurch ist ein finanzieller Schaden in Höhe von 2.811,38 Euro entstanden.

Innerhalb der Landesverwaltung werden IT-Sicherheitsvorfälle durch das CERT M-V statistisch erfasst, analysiert und ausgewertet; eine summarische Kostenaufstellung für interne und/oder externe Aufwände in Verbindung mit IT-Sicherheitsvorfällen existiert nicht.

6. Welche Maßnahmen zur Aufklärung und zum Schutz vor möglichen Cyberangriffen wurden bisher realisiert?
Welche weiteren Maßnahmen sind geplant?

Das im Jahr 2014 etablierte Landes-CERT (CERT M-V) tauscht sich kontinuierlich innerhalb des Verwaltungs-CERT-Verbundes zu möglichen Gefährdungen oder IT-Angriffen aus. Ebenso kommuniziert das CERT M-V regelmäßig mit den jeweiligen Stellen im Landeskriminalamt und der Abteilung Verfassungsschutz des Ministeriums für Inneres und Europa.

Aktuell ist im Rahmen der gesetzlichen Möglichkeiten der Aufbau eines IT-Systems zur Erkennung und Behandlung von cyberkriminellen IT-Infrastrukturen (Botnet, Command-and-Control-Server) geplant.

7. Welche konkreten Vorkehrungen wurden getroffen, um zukünftige Cyberangriffe zu parieren und den unbefugten Zugriff auf Datenbestände zu verhindern?

Sowohl technische als auch organisatorische Sicherheitsmaßnahmen, unter anderem zum Schutz vor Cyberangriffen, werden in Abhängigkeit von dem jeweiligen Schutzbedarf für ein IT-Verfahren in einem Sicherheitskonzept ausgearbeitet. Auf dessen Basis erfolgt die Umsetzung des Sicherheitskonzeptes durch den IT-Dienstleister.

Die Sicherheitskonzepte sowie die umgesetzten Sicherheitsmaßnahmen werden regelmäßig, insbesondere bei einer Änderung der Gefährdungslage aktualisiert und fortgeschrieben. Grundlage hierfür ist die BSI IT-Grundschutzmethodik; bei der Verarbeitung von personenbezogenen Daten wird die Methodik des Standarddatenschutzmodells angewendet.