**LANDTAG MECKLENBURG-VORPOMMERN** **Drucksache 8/24**
**8. Wahlperiode** **09.12.2021**

# KLEINE ANFRAGE

**des Abgeordneten Sebastian Ehlers, Fraktion der CDU**

## Sicherheit der IT-Systeme des Landes Mecklenburg-Vorpommern

**und**

# ANTWORT

**der Landesregierung**

Aufgrund der Umsetzung des Onlinezugangsgesetzes werden Verwaltungsdienstleistungen zunehmend ins Internet verlagert. Damit verbunden ist auch eine zunehmende Komplexität und Vernetzung der IT-Systeme und IT-Infrastrukturen der Verwaltung, die verlässlichere, robuste und wirkungsvolle IT-Sicherheitskonzepte notwendig machen. Dabei sind auch die zusätzlichen Angriffsvektoren durch die Anbindung von Homeoffice-Arbeitsplätzen zu berücksichtigen.

Vor dem Hintergrund eines erfolgreichen Cyberangriffs auf die IT-Systeme des kommunalen IT-Dienstleisters KSM am 15. Oktober 2021 und des damit verbundenen Ausfalls der IT-Systeme der Landeshauptstadt Schwerin und des Landkreises Ludwigslust-Parchims ist auch das Bedrohungsszenario für die IT-Systeme der Landesverwaltung Mecklenburg-Vorpommerns gewachsen. Erfolgreiche Hackerangriffe auf die IT-Systeme der Verwaltung können das Vertrauen der Bürger und Unternehmen in die neuen Online-Bürgerdienste und den verantwortungsvollen Umgang der Verwaltung mit ihren Daten massiv schädigen.

---

Der Minister für Inneres, Bau und Digitalisierung hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 8. Dezember 2021 beantwortet.

1. Verfügt die Landesregierung über ein Verzeichnis für die in der Landesverwaltung im Einsatz befindlichen IT-Fachverfahren, welches auch das Vorhandensein und die Aktualität der jeweiligen IT-Sicherheitskonzepte erfasst?

Nach den Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik muss eine IT-Dokumentation inklusive Betriebshandbuch, Sicherheits- und gegebenenfalls Datenschutzkonzept für alle in der Landesverwaltung eingesetzten IT-Verfahren gepflegt und vollständig sein. Die jeweiligen Behörden sind für ihre Netzsegmente, Systeme, fachspezifischen Verfahren verantwortlich.

Auf der Grundlage des Kabinettsbeschlusses vom 12. Mai 2021 betreibt das für Digitalisierung zuständige Ministerium das IT-Verfahrensverzeichnis als zentrale, datenbankbasierte Anwendung.

Die Ressorts der Landesregierung sind verpflichtet, bis zum Ende dieses Jahres ihre IT-Fachverfahren in diesem Verzeichnis zu dokumentieren und danach fortlaufend zu aktualisieren. Besonderes Augenmerk liegt dabei in der Erfassung von Metainformationen, wie beispielsweise die Dokumentation zur IT-Verantwortlichkeit, der technischen Architektur sowie Angaben zum Sicherheitskonzept. Weitere Datenfelder beziehungsweise Themenfelder können in der Zukunft durch das Ministerium für Inneres, Bau und Digitalisierung ergänzt werden, sodass der Informationsstand kontinuierlich weiter ausgebaut wird.

Im Themenfeld „Sicherheit und Datenschutz“ wird das Vorhandensein eines Sicherheitskonzepts sowie das Datum der letzten Aktualisierung des Sicherheitskonzepts erfasst. Auch hierfür sind die jeweiligen Ressorts in eigener Zuständigkeit verantwortlich. Für die Erstellung, Aktualisierung, Fortschreibung und Dokumentation zur Umsetzung der Sicherheitskonzepte setzt die Landesverwaltung seit 2015 zum Beispiel die Open Source-Software „verinice.“ ein. Verinice. unterstützt die Informationssicherheitsbeauftragten sowohl in der Landes- als auch in der Kommunalverwaltung beim Management der Informationssicherheit auf Basis der Methodik des IT-Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in der jeweils gültigen Fassung der BSI-Standards und des IT-Grundschutz-Kompendiums.

2. In welchem Jahr wurde für die zentralen E-Government-Basisdienste des Landes Mecklenburg-Vorpommerns zuletzt die Wirksamkeit der eingeleiteten Sicherheits- und Schutzmaßnahmen durch
   a) eine IT-Notfallübung,
   b) ein Penetrationstest (Schwachstellenanalyse und kontrollierte Durchführung von Angriffen aus der Sichtweise eines Angreifers) und
   c) eine Sicherheitsprüfung/Audit überprüft?
   [Bitte Darstellung für die Prüfmaßnahmen a), b) und c) für jeden der 13 E-Government-Basisdienste gemäß Anlage der BasDi LVO M-V vom 4. Oktober 2020]

Die Fragen 2, a), b) und c) werden zusammenhängend beantwortet.

Die Landesverordnung über die Bereitstellung, Ausgestaltung und Nutzung von E-Government-Basisdiensten im Land Mecklenburg-Vorpommern (BasDi LVO M-V) ist zum 4. Oktober 2021 in Kraft getreten. Zur Veröffentlichung des MV-Serviceportals 2019 wurde ein Sicherheitskonzept unter Beachtung des DSGVO unter Anwendung des Standarddatenschutzmodells und Beachtung der Betroffenenrechte für einen „hohen“ Schutzbedarf erstellt. Im Anschluss hierzu wurden auch die vorhandenen Sicherheitskonzepte zu den Basisdiensten neu unter Beachtung der DSGVO mit Anwendung des Standarddatenschutzmodells s. o. neu erstellt. Diese Arbeiten wurden zum Jahresbeginn 2021 abgeschlossen. Im Anschluss wurde mit der Umsetzung von offenen optionalen oder neuen Schutz- und Sicherheitsmaßnahmen begonnen, die sich insbesondere durch eine weitere Härtung und Fortentwicklung der Maßnahmenkataloge des BSI Grundschutzes ergeben haben. Das Informationssicherheitsmanagement hat zur Wirksamkeitsprüfung von Sicherheitskonzepten seit 2019 ein Auditprogramm aufgesetzt. Penetrationstests sind Bestandteil dieses Auditprogramms.

Derzeit wurden die Basisdienste noch keiner der in den Fragen 2 a) bis c) genannten Maßnahmen unterzogen. Dies ist jedoch Teil des Auditprogramms, das vom Informationssicherheitsmanagement seit dem Jahr 2019 durchgeführt wird.

3. Wie entwickelte sich die personelle Ausstattung des in der Landesregierung verorteten Computer-Notfall-Teams (Computer Emergency Response Team, kurz CERT) Mecklenburg-Vorpommerns, dessen Spezialisten seit 2015 für die IT-Sicherheit in den kommunalen und staatlichen Stellen des Landes sorgen (bitte jahresweise Darstellung mit Vollzeitäquivalenten Stand: 31. Dezember 2015 bis 2020)?

Das Computer-Notfall-Team (Computer Emergency Response Team, CERT M-V) mit seinen CERT-Basisdiensten wurde beginnend ab 2015 sukzessiv in mehreren Phasen aufgebaut. Ausgehend von den im „Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ (ISM M-V) festgelegten Aufgaben leitet sich die personelle Ausstattung des CERT M-V ab. Demnach bietet das CERT M-V seine CERT-Basisdienste primär für die Landesverwaltung an. Die Kommunalverwaltung ist insofern in den CERT-Basisdiensten berücksichtigt, wenn zentrale Sicherheitssysteme, gemeinsam genutzte IT-Verfahren oder IT-Infrastrukturen betroffen sind.

Im Rahmen der Weiterentwicklung der CERT-Basisdienste wurden einzelne CERT-Aufgaben, wie beispielsweise die kontinuierliche Bereitstellung von Informationen über Schwachstellen in Hard- und Softwareprodukten und deren Bewertung an einen externen Dienstleister im Rahmen eines Outsourcings ausgelagert.

Die personelle Ausstattung des CERT M-V (Kernteam) entwickelte sich in den Jahren 2015 bis 2020 wie folgt:

| **Jahr** | **Stunden/Monat** | **Vollzeitäquivalente** |
|---|---|---|
| 2015 | 238 | 1,75 |
| 2016 | 340 | 2,50 |
| 2017 | 380 | 2,79 |
| 2018 | 380 | 2,79 |
| 2019 | 380 | 2,79 |
| 2020 | 436 | 3,20 |

Ein Vollzeitäquivalent (VZÄ) beträgt, bezogen auf ein Kalenderjahr unter Berücksichtigung von Urlaub, Ausfall durch Krankheit sowie durch Fort- und Weiterbildungsmaßnahmen, im Monatsdurchschnitt 136 Stunden.

Anlassbezogen, beispielsweise bei einem schwerwiegenden oder ressortübergreifenden Sicherheitsvorfall, wächst das CERT M-V durch weitere, kooptiere Mitglieder temporär auf. Zu diesen Mitgliedern gehören beispielsweise das Landeskriminalamt, das DVZ-Sicherheitsteam, das Security Operation Team im DVZ (DVZ-SOC) oder das Mobile Incident Response Team (MIRT) vom BSI.

4. Wie viele IT-Sicherheitsvorfälle wurden gemäß „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ (IS-Leitlinie) seit 2015 gemeldet (bitte jahresweise Darstellung für 2015 bis 2020)?

Die dem CERT M-V von der Landesverwaltung gemeldeten Sicherheitsvorfälle beinhalten ressortinterne, möglichweise ressortübergreifende oder ressortübergreifende Vorfälle. Diese Klassifizierung wird seitens der kommunalen Zielgruppe des CERT M-V nicht angewendet. Eine allgemeine Meldepflicht der Kommunen gegenüber dem CERT M-V existiert seit 2020.

| **Jahr** | **Anzahl der gemeldeten Sicherheitsvorfälle** |
|---|---|
| 2015 | keine Zahlen vorhanden |
| 2016 | 9 |
| 2017 | 6 |
| 2018 | 16 |
| 2019 | 15 |
| 2020 | 20 |

5. Welche Awareness-Maßnahmen zur Sensibilisierung der Mitarbeitenden der Landesverwaltung für die Bedrohung durch Schadsoftware hat das CERT M-V seit dem 1. März 2020 durchgeführt, um das Risiko durch das verstärkte Arbeiten im Homeoffice seit der Corona-Pandemie zu mindern?

Durch das CERT M-V wird ein Warn- und Informationsdienst betrieben, der die Zielgruppen des CERT M-V (Landes- und Kommunalverwaltung) auf mögliche Schwachstellen informiert und hinweist. Darin enthalten sind zudem Bewertungen zur Schwere der Schwachstelle bzw. zur Sicherheitslücke. Es werden Möglichkeiten zur Schließung beziehungsweise Risikoreduzierung aufgezeigt. Darüber hinaus informiert das CERT M-V über diesen CERT-Basisdienst sowie über das CERT-Portal regelmäßig über neue Angriffsvektoren und neue Bedrohungen. Dies umfasst auch Informationen zu den neuen Risiken, die durch das Arbeiten im Homeoffice entstehen.

Gemäß der CERT-Dienstespezifikation zu den CERT-Basisdiensten unterstützt das CERT M-V die Informationssicherheitsbeauftragten der Ressorts bei der Sensibilisierung der Beschäftigten in ihren Behörden, Einrichtungen oder Institutionen. Für die Durchführung von Schulungen und Awareness-Veranstaltungen in den Ressorts sind die jeweiligen Informationssicherheitsbeauftragten zuständig.

Über den IT-Planungsrat werden der Zielgruppe jährlich drei Awareness-Veranstaltungen angeboten, die dann durch externe spezialisierte Dienstleister sowohl in der Landes- als auch in der Kommunalverwaltung durchgeführt werden. Des Weiteren bietet das Referat „Ressortübergreifendes Informationssicherheitsmanagement“ regelmäßig Schulungen für die Informationssicherheitsbeauftragten an.