LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/10733**

17.09.2024

Kleine Anfrage 4510

der Abgeordneten Angela Freimuth und Marc Lürbke FDP

Ein Jahr nach dem Cyberangriff auf die Südwestfalen-IT: Hat die Landesregierung Sicherheitsbeschlüsse des Parlaments umgesetzt?

In der Nacht auf den 30. Oktober 2023 wurde bei der Südwestfalen-IT (SIT) ein Cyberangriff entdeckt. Infolgedessen wurde die kommunale Infrastruktur von 72 Kommunen lahmgelegt, die bei der SIT ihre IT-Dienstleistungen abwickeln. In der Akutphase waren für die Bürgerinnen und Bürger zahlreiche öffentliche Dienstleistungen nicht verfügbar. Die Wiederherstellung aller Leistungen hat leider Monate benötigt.[1]

Die Fraktionen von CDU und Grünen hatten bereits am 17. Januar 2023 einen Antrag in das Plenum eingebracht, der sich ausführlich mit IT-Sicherheit befasst und acht Arbeitsaufträge an die Regierung formuliert.[2] Der Antrag wurde in der Sitzung des Ausschusses für Bauen, Wohnen und Digitales am 02. März 2023 ohne Expertenanhörung mit den Stimmen von CDU und Grünen bei Enthaltung der FDP beschlossen.[3]

Vor diesem Hintergrund fragen wir die Landesregierung, wie sie den Beschluss umgesetzt hat, insbesondere mit Blick auf die folgenden Fragen:

1. Mit welchem Ergebnis hat die Landesregierung geprüft, ob Backupsysteme nach dem Vorbild der Hochschulen für Land und Kommunen einen Mehrwert bieten?

2. In welchem Umfang hat die Landesverwaltung Pläne bzw. Übungen umgesetzt, um die Reaktionszeit auf IT-Schadensfälle wie Cyberangriffe oder Softwarelücken auf wenige Stunden zu verkürzen?

---

[1] KommunalWiki: Cyberangriff auf die Südwestfalen-IT 2023, abrufbar unter: https://kommunalwiki.boell.de/index.php/Cyberangriff_auf_die_S%C3%BCdwestfalen-IT_2023#:~:text=In%20der%20Nacht%20auf%20den,einige%20weitere%20Kund%3Ainnen%20betreibt. (Letzter Zugriff: 04.09.2024). Ausführliche Darstellung in einer Reihe vom Deutschlandfunk, vgl. Annabell Brockhues und Felicitas Boeselager: Zero Day in Südwestfalen, Teile 1 bis 5, 17. Juni 2024, abrufbar unter: https://www.deutschlandfunk.de/zero-day-in-suedwestfalen-folge-1-hackeralarm-bei-nacht-dlf-cab9c129-100.html (letzter Zugriff: 04.09.2024).

[2] Fraktionen von CDU und Grünen: Aktuellen und zukünftigen Herausforderungen der IT-Sicherheit strukturiert begegnen, Drucksache 18/2543.

[3] Ausschussprotokoll, APr 18/182, abrufbar unter: https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMA18-181.pdf, Seite 16 bis 18.

Datum des Originals: 17.09.2024/Ausgegeben: 18.09.2024

3. Welche Maßnahmen hat die Landesregierung ergriffen, um die kommunale IT-Sicherheitsstruktur mit einem kommunalen CERT 2.0 zu stärken?

4. Welche Fortschritte hat die Landesregierung bei der Entwicklung eines Konzepts gemacht, damit Mitarbeiterinnen und Mitarbeiter der Landes- und Kommunalverwaltungen für IT-Fragen sensibilisiert werden und daraus resultierend IT-Sicherheitsmaßnahmen einfacher angewandt werden können?

5. Welche konkreten Schritte hat die Landesregierung unternommen, um die IT-Sicherheit in der Landes- und Kommunalverwaltung im Rahmen des beschlossenen PDCA-Zyklus (Plan-Do-Check-Act) umzustrukturieren?

Angela Freimuth
Marc Lürbke

LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/11349**

05.11.2024

Antwort

der Landesregierung

auf die Kleine Anfrage 4510 vom 17. September 2024
der Abgeordneten Angela Freimuth und Marc Lürbke FDP
Drucksache 18/10733

Ein Jahr nach dem Cyberangriff auf die Südwestfalen-IT: Hat die Landesregierung Sicherheitsbeschlüsse des Parlaments umgesetzt?

Vorbemerkung der Kleinen Anfrage

In der Nacht auf den 30. Oktober 2023 wurde bei der Südwestfalen-IT (SIT) ein Cyberangriff entdeckt. Infolgedessen wurde die kommunale Infrastruktur von 72 Kommunen lahmgelegt, die bei der SIT ihre IT-Dienstleistungen abwickeln. In der Akutphase waren für die Bürgerinnen und Bürger zahlreiche öffentliche Dienstleistungen nicht verfügbar. Die Wiederherstellung aller Leistungen hat leider Monate benötigt.[1]

Die Fraktionen von CDU und Grünen hatten bereits am 17. Januar 2023 einen Antrag in das Plenum eingebracht, der sich ausführlich mit IT-Sicherheit befasst und acht Arbeitsaufträge an die Regierung formuliert.[2] Der Antrag wurde in der Sitzung des Ausschusses für Bauen, Wohnen und Digitales am 02. März 2023 ohne Expertenanhörung mit den Stimmen von CDU und Grünen bei Enthaltung der FDP beschlossen.[3]

Vor diesem Hintergrund fragen wir die Landesregierung, wie sie den Beschluss umgesetzt hat, insbesondere mit Blick auf die folgenden Fragen.

Die Ministerin für Heimat, Kommunales, Bau und Digitalisierung hat die Kleine Anfrage 4510 mit Schreiben vom 5. November 2024 namens der Landesregierung im Einvernehmen mit dem Minister des Innern beantwortet.

---

[1] KommunalWiki: Cyberangriff auf die Südwestfalen-IT 2023, abrufbar unter: https://kommunal-wiki.boell.de/index.php/Cyberangriff_auf_die_S%C3%BCdwestfalen-IT_2023#:~:text=In%20der%20Nacht%20auf%20den,einige%20weitere%20Kund%3Ainnen%20betreibt. (Letzter Zugriff: 04.09.2024). Ausführliche Darstellung in einer Reihe vom Deutschlandfunk, vgl. Annabell Brockhues und Felicitas Boeselager: Zero Day in Südwestfalen, Teile 1 bis 5, 17. Juni 2024, abrufbar unter: https://www.deutschlandfunk.de/zero-day-in-suedwestfalen-folge-1-hackeralarm-bei-nacht-dlf-cab9c129-100.html (letzter Zugriff: 04.09.2024).

[2] Fraktionen von CDU und Grünen: Aktuellen und zukünftigen Herausforderungen der IT-Sicherheit strukturiert begegnen, Drucksache 18/2543.

[3] Ausschussprotokoll, APr 18/182, abrufbar unter: https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMA18-181.pdf, Seite 16 bis 18.

Datum des Originals: 05.11.2024/Ausgegeben: 11.11.2024

1. Mit welchem Ergebnis hat die Landesregierung geprüft, ob Backupsysteme nach dem Vorbild der Hochschulen für Land und Kommunen einen Mehrwert bieten?

Die Hochschulen in NRW verfolgen bei dem Backupsystem einen cloudbasierten Ansatz. Die Prüfung hat ergeben, dass aufgrund des Schutzbedarfes der Daten der Landesverwaltung eine identische Lösung nicht anwendbar ist. Einschlägige, interne Regelungen und Empfehlungen des BSI-IT-Grundschutzes stehen diesem Lösungsansatz entgegen.

Die Landesverwaltung besitzt unter Einbeziehung der Landesrechenzentren eine krisensichere Backupstrategie, in die kontinuierlich Erkenntnisse aus Bedrohungslagen einfließen und zur Prüfung der Wirksamkeit der vorgesehenen Maßnahmen herangezogen werden.

2. In welchem Umfang hat die Landesverwaltung Pläne bzw. Übungen umgesetzt, um die Reaktionszeit auf IT-Schadensfälle wie Cyberangriffe oder Softwarelücken auf wenige Stunden zu verkürzen?

IT.NRW als zentraler IT-Dienstleister führt intern regelmäßige Ausfalltests durch. Hierzu gehören**:**

- Ausfallübungen der Rechenzentrumsstandorte mit den Phasen Wiederanlauf, Organisation des Notbetriebs sowie Überführung in den Regelbetrieb.
- Tests zur Betriebsübernahme von Anwendungen an einem anderen Rechenzentrumsstandort nach einem Ausfall.
- Blackbuilding-Tests mit kontrolliertem Abschalten der Energieversorgung vom Stromversorger zum Test der Redundanzsysteme des Gebäudes.
- Cool-Down-Tests in den Rechnersälen der Rechenzentren mit temporärer Abschaltung der Klimatisierung.

3. Welche Maßnahmen hat die Landesregierung ergriffen, um die kommunale IT-Sicherheitsstruktur mit einem kommunalen CERT 2.0 zu stärken?

Das Land bietet den Kommunen über den kommunalen Warn- und Informationsdienst des CERT NRW (KWID) zeitnah und zielgruppengerecht aufbereitete sicherheitsrelevante Informationen über Schwachstellen und Sicherheitspatches an.

4. Welche Fortschritte hat die Landesregierung bei der Entwicklung eines Konzepts gemacht, damit Mitarbeiterinnen und Mitarbeiter der Landes- und Kommunalverwaltungen für IT-Fragen sensibilisiert werden und daraus resultierend IT-Sicherheitsmaßnahmen einfacher angewandt werden können?

Seit über sieben Jahren nutzt die Landesverwaltung die landeseigene Plattform „Na sicher! NRW“, um den Beschäftigten der Landesverwaltung technisch niedrigschwellige Sensibilisierungsangebote anzubieten. Hierunter fallen auch Awareness Kampagnen wie "Die Hacker kommen", welche beispielsweise am 11.09.2024 im MHKBD durchgeführt wurde. Ein mit den Personalvertretungen abgestimmtes Schulungskonzept ist weitgehend umgesetzt.

Die Durchführung des Informationssicherheitstages 2023 ist erfolgt. In diesem Rahmen wurde den NRW Kommunen die "Na Sicher! NRW" Plattform mit positiver Resonanz vorgestellt.
Schon seit langem werden den Beschäftigten der Landesverwaltung über das IT-Fortbildungsprogramm des Landes Präsenzschulungen zum Thema IT-Sicherheit in unterschiedlichen Schwierigkeitsgraden angeboten. Diese Schulungen stehen auch den Beschäftigten in den Kommunen offen.

Der nordrhein-westfälische Verfassungsschutz hat mit Schreiben vom Februar 2024 noch einmal alle Kommunen und somit mittelbar die kommunalen IT-Dienstleister über das Sensibilisierungs- und Präventionsprogramm des Wirtschaftsschutzes in Kenntnis gesetzt und seine Vortrags- und Beratungsangebote ausdrücklich auf die Kommunalverwaltungen und kommunalen Eigenbetriebe ausgeweitet. Ziel dieser Maßnahme ist es, die Sensibilität aller Beschäftigten für Gefahren durch Spionage, Sabotage und Cyberangriffe zu erhöhen. Zudem soll nahegelegt werden, die beim Umgang mit Verschlusssachen bereits bestehende Sensibilität auch beim Umgang mit IT-Systemen und Geschäftsabläufen zu wahren. Dies kann sowohl durch allgemein gehaltene Vorträge für die komplette Mitarbeiterschaft, über spezialisierte Vorträge für gesonderte Bereiche (IT-Systemhaus, Hauptamt, Leitungsebene) bis zur Einzelfallbetrachtung im Rahmen einer Initialberatung hinsichtlich eines Sicherheits- und Notfallkonzepts führen. Bis heute wurden zwölf Sensibilisierungsvorträge bzw. Initialberatungen abgerufen.

5. Welche konkreten Schritte hat die Landesregierung unternommen, um die IT-Sicherheit in der Landes- und Kommunalverwaltung im Rahmen des beschlossenen PDCA-Zyklus (Plan-Do-Check-Act) umzustrukturieren?

Seit 1998 sieht die Landesverwaltung dementsprechend für jede ihrer Behörden die Umsetzung des BSI-Grundschutzes vor. Diese Vorgabe wurde 2015 über den Aufbau eines landeseinheitlichen Informationssicherheitsmanagementsystems (ISMS) vertieft und durch die Verwaltungsvorschrift "Informationssicherheitsleitlinie NRW" als Strategie gefestigt. Der PDCA-Zyklus ist fester Bestandteil des in der Leitlinie beschriebenen Vorgehensmodells und sorgt für dessen Fortentwicklung und Anpassung an die jeweiligen Gefährdungssituationen.
Der durch das Ministerium für Heimat, Kommunales, Bau und Digitalisierung initiierte und landesseitig finanzierte „IT-Check Kommunen“ bietet den Kommunen die Möglichkeit, systemische Fehler in kommunaler IT zu identifizieren, zu clustern und darauf aufbauend weitere Handlungsschritte (und -notwendigkeiten) zu identifizieren.