Große Anfrage

Fraktion der AfD

Sicherheit der IT-Systeme in Wirtschaft und Verwaltung in Niedersachsen

Anfrage der Fraktion der AfD an die Landesregierung, eingegangen am 07.08.2024

Die Absicherung von IT-Systemen gewinnt im Zusammenhang mit einer rasanten Digitalisierung und den damit einhergehenden Risiken verschiedenster Cyberangriffsmöglichkeiten eine immer größere Bedeutung.

In einer repräsentativen Umfrage[1] aus den Jahren 2018 und 2019 des Kriminologischen Forschungsinstituts Niedersachsen e. V., in welcher 5 000 Unternehmen befragt wurden, gaben damals rund 41 % der befragten Unternehmen an, in den vorhergehenden zwölf Monaten Ziel eines Cyberangriffs gewesen zu sein, auf den reagiert werden musste.

Angriffe mittels Schadsoftware bilden bei den unterschiedlichen Cyberangriffsarten neben den sogenannten Phishing-Angriffen einen Schwerpunkt der Bedrohungen. Von diesen Ransomware-Angriffen waren laut der Befragung in den vorangegangenen Monaten rund 12 % der Unternehmen betroffen.

Im Koalitionsvertrag der Regierungsparteien ist zu lesen, dass die Digitalisierung eine große Chance für unsere Gesellschaft ist. Mit dieser Großen Anfrage soll festgestellt werden, wie die Situation rund um das Thema Cybersicherheit für niedersächsische Unternehmen ist. Außerdem soll ermittelt werden, welche Maßnahmen, Programme oder finanzielle Hilfen sich bisher bewährt haben und welche noch notwendig sind, um niedersächsische Unternehmen wirksam gegen Cyberangriffe zu schützen und wirtschaftliche Schäden zu vermeiden oder in engen Ausmaßen zu begrenzen.

Im dritten Teil dieser in drei Bereiche aufgeteilten Anfrage soll die Sicherheitslage und der Umgang von Behörden mit Cyberangriffen beleuchtet werden.

I. Cyberangriffe und Cybersicherheit bei Unternehmen, an denen das Land Niedersachsen beteiligt ist

1. Welche Kenntnisse hat die Landesregierung über Cyberangriffe auf die IT bei Unternehmen im Zeitraum von 2018 bis 2023, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist (bitte aufschlüsseln nach Jahren und Art der Angriffe, wie beispielsweise Ransomware-Angriffe oder Angriffe über Schadprogramme)?
2. Welche Schäden sind den in Frage 1 benannten Unternehmen im besagten Zeitraum entstanden (bitte jeweils aufschlüsseln nach Jahren)?
3. Was sind nach Kenntnis der Landesregierung die am häufigsten aufgetretenen Schwachstellen in der Cybersicherheit dieser Unternehmen?
4. Bei welchen Cloud-Betreibern sind die Daten gespeichert, auf die die Unternehmen Zugriff haben, und welche der Cloud-Betreiber haben ihren Sitz in Deutschland bzw. der Europäischen Union (bitte für jedes Unternehmen, an dem das Land Niedersachsen beteiligt ist, einzeln aufschlüsseln)?
5. Hat die Landesregierung auf die Unternehmen, an denen das Land Niedersachsen beteiligt ist, eingewirkt, die Cloud eines deutschen oder europäischen Betreibers zu nutzen?
6. Wie viele und welche IT-Schulungen fanden im Zeitraum von 2018 bis 2023 in den Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, statt?

[1] https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf

7. In welcher Höhe geben die Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, jährlich Geld für Cybersicherheit aus (bitte aufschlüsseln nach Jahren für den Zeitraum der letzten fünf Jahre)?

8. Welche Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, nutzen „HoneySens“ bzw. haben sich diese Lösung in Form einer Open-Source-Lizenz entsprechend ihren Kundenbedürfnissen anpassen lassen?

9. Ist der Landesregierung bekannt, ob und, falls ja, mit welchen Maßnahmen die Betriebe, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, ihre Mitarbeiter für das Thema Cybersicherheit sensibilisieren?

10. Ist der Landesregierung bekannt, inwieweit Homeoffice-Arbeitsplätze in den Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist, in den Jahren 2020 und 2021 von Cyberangriffen betroffen waren (bitte aufschlüsseln nach Jahren und Anzahl, sofern es Cyberangriffe gab)?

11. Ist der Landesregierung bekannt, ob die Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist, gegen Cyberangriffe versichert sind? Falls ja, welche Unternehmen sind in welchem Umfang versichert?

12. Welche Kenntnisse besitzt die Landesregierung über den gegenwärtigen Investitionsbedarf in IT-Sicherheit bei den Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist?

II. Cyberangriffe und Cybersicherheit bei kleinen und mittleren Unternehmen (KMU)

13. Beabsichtigt die Landesregierung, bei den KMU in Niedersachsen in nächster Zeit Unternehmensbefragungen zur Cybersicherheit durchzuführen, bzw. wurden in den Jahren 2020 und 2021 Unternehmensbefragungen in dieser Gruppe durchgeführt? Falls ja, mit welchen Ergebnissen, bzw. welche Handlungsempfehlungen sind aus den Befragungsergebnissen abzuleiten?

14. Welche IT-Fachfirmen haben in den Jahren 2022 und 2023 niedersächsische KMU zum Thema Cybersicherheit beraten, und wie hoch waren die Kosten dafür?

15. Wie viele Veranstaltungen hat die Zentrale Ansprechstelle Cybercrime für die niedersächsische Wirtschaft (ZAC) für niedersächsische Unternehmen im Bereich Cybersicherheit im Jahr 2023 durchgeführt, und welche Schwerpunkte wurden thematisch bei diesen Veranstaltungen gesetzt?

16. Wie ist die Studienlage zur Internetkriminalität und zu Cyberangriffen im Land Niedersachsen? Sind aktuelle Studien durch die Landesregierung in Auftrag gegeben? Werden Studien, bei denen die Auftraggeber Dritte sind, vom Land Niedersachsen finanziert?

17. Wie viele KMU in Niedersachsen, an denen das Land Niedersachsen nicht unmittelbar oder mittelbar beteiligt ist, nutzen „HoneySens“ bzw. haben sich diese Lösung in Form einer Open-Source-Lizenz entsprechend ihren Kundenbedürfnissen anpassen lassen?

18. Wie viele Cyberangriffe auf Unternehmen wurden in Niedersachen in den Jahren 2022 und 2023 sowie im ersten Halbjahr 2024 jeweils angezeigt?

19. Ist der Landesregierung bekannt, ob KMU in Niedersachsen in einer messbaren Größenordnung gegen Cyberangriffe versichert sind?

20. Welche politischen Maßnahmen erachtet die Landesregierung gegebenenfalls für sinnvoll, um zeitnah Cyberangriffe auf niedersächsische Unternehmen einzudämmen?

21. Inwiefern sind niedersächsische Behörden ausreichend vorbereitet und ausgestattet, um vor allem KMU bei Fragen zur IT-Sicherheit wirksam zu unterstützen?

22. Welche Förderungen für Mitarbeiterschulungen durch Landesmittel im Bereich der Cybersicherheit existieren für KMU, und inwieweit wurden die Mittel abgerufen (bitte aufschlüsseln für die Jahre 2022 und 2023)?

23. Sieht die Landesregierung bei der Bekämpfung der Cyberkriminalität Lücken beim Informationsaustausch zwischen Behörden und betroffenen Unternehmen? Falls ja, welche und wie sollen diese geschlossen werden?

24. Warum wurde das Problem „Cybercrime“ nicht als eine eigene Herausforderung in dem Kapitel „Wirtschaft“ im aktuellen Koalitionsvertrag aufgenommen?

25. Welche Kenntnisse besitzt die Landesregierung über die Kosten, die KMU in Niedersachsen für die Einrichtung, den Betrieb und die Instandhaltung von IT-Sicherheit monatlich aufbringen?

26. Welche Kenntnisse besitzt die Landesregierung über den gegenwärtigen Investitionsbedarf der niedersächsischen KMU in die IT-Sicherheit?

27. Wie viele KMU in Niedersachsen beschäftigen zur Cyberabwehr Informatiker bzw. verfügen über eine eigene IT-Abteilung, die entsprechend aufgestellt ist, um Cyberangriffe abzuwehren bzw. entstandene Schäden zu beheben?

28. Wie viele KMU in Niedersachsen haben in den Jahren 2022 und 2023 ihre Mitarbeiter im Umgang mit IT weiterqualifiziert bzw. geschult, um die Datensicherheit im jeweiligen Unternehmen zu verbessern, und gab es hierfür vom Land Niedersachsen gezielte Angebote?

29. Welche wirtschaftlichen Schäden sind niedersächsischen KMU in den Jahren 2021, 2022 und 2023 durch Cyberangriffe entstanden (bitte aufschlüsseln nach Jahren und Schadenshöhe)?

III. Cyberangriffe auf Behörden und Kritische Infrastruktur

30. Wie viele Angriffe auf niedersächsische Einrichtungen und Behörden sowie auf die Kritische Infrastruktur sind der Landesregierung seit dem Jahr 2021 bekannt (bitte aufschlüsseln nach Jahren sowie jeweils nach angegriffener Einrichtung, Behörde und Infrastruktur)?

31. Welche Schäden sind dabei entstanden, und welche Schadenshöhe ist der Landesregierung bekannt (bitte aufschlüsseln wie in Frage 1)?

32. Beabsichtigt die Landesregierung, eine Meldepflicht für Cyberangriffe auf kommunale Einrichtungen und niedersächsische Behörden einzuführen? Falls ja, wann? Falls nein, warum nicht?

33. Welche Software zur Abwehr von Cyberangriffen wird in niedersächsischen Behörden genutzt, und beabsichtigt die Landesregierung gegebenenfalls in niedersächsischen Behörden den Umstieg auf Open-Source-Software? Falls ja, ab wann?

34. Plant die Landesregierung für niedersächsische Einrichtungen und Behörden den Einstieg beim europäischen Clouddienst Gaia-X? Falls ja, ab wann?

35. Hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bisher niedersächsische Kommunalverwaltungen in Fragen der Cybersicherheit beraten? Falls ja, wann und in wie vielen Fällen?

36. Konnte das BSI niedersächsische Kommunalverwaltungen in Einzelfällen bei der Bewältigung von Vorfällen helfen? Falls ja, wann und in wie vielen Fällen?

37. Was spricht aus Sicht der Landesregierung gegebenenfalls dagegen, die Kommunen mit in die Liste der Kritischen Infrastruktur aufzunehmen? Falls nichts dagegenspricht, wann werden entsprechende Regelungen erarbeitet und umgesetzt?

38. Beabsichtigt die Landesregierung gegebenenfalls zur Aufnahme der Kommunen in die Liste der Kritischen Infrastruktur eine Bundesratsinitiative zum IT-Sicherheitsgesetz zu initiieren? Falls ja, wann?

Jens-Christoph Brockmann

Parlamentarischer Geschäftsführer

(Verteilt am 16.08.2024)