Abgeordnetenhaus BERLIN

Drucksache 18 / 24 389
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Florian Graf (CDU)

vom 04. Aug. 2020 (Eingang beim Abgeordnetenhaus am 05. August 2020)

zum Thema:
Sicherheitslücken bei den Berliner Wasserbetrieben

und **Antwort** vom 17. August 2020 (Eingang beim Abgeordnetenhaus am 20. Aug. 2020)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Wirtschaft,
Energie und Betriebe

Herrn Abgeordneten Florian Graf (CDU)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 18/24 389
vom 4. August 2020
über Sicherheitslücken bei den Berliner Wasserbetrieben

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Die Schriftliche Anfrage betrifft überwiegend Sachverhalte, die der Senat nicht in eigener Zuständigkeit und Kenntnis beantworten kann. Er ist gleichwohl bemüht, Ihnen eine Atwort auf Ihre Anfrage zukommen zu lassen und hat daher die Berliner Wasserbetriebe (BWB) Anstalt öffentlichen Rechts um eine Stellungnahme gebeten, die von dort in eigener Verantwortung erstellt und dem Senat übermittelt wurde. Sie wird nachfolgend wiedergegeben.

1. Wann wurde die „Security Analyse“ durch das Sicherheitsberatungsunternehmen Alpha Strike Labs im Bereich Abwasser und bei der Informationstechnik der Berliner Wasserbetrieb in Auftrag gegeben? (Bitte auch Details zur etwaigen Ausschreibung etc.)

Zu 1.: Nach Angaben der BWB sei Alpha Strike Labs GmbH aus einer vom Bundesamt für Sicherheit in der Informationstechnik (BSI) übermittelten Liste möglicher Unternehmen ausgewählt worden. Der Auftrag an das Unternehmen sei am 9. April 2020 erteilt worden.

2. Wer hat die „Security Analyse“ in Auftrag gegeben?

Zu 2.: Die Berliner Wasserbetriebe.

3. Wurde die Analyse in Absprache mit der Senatsverwaltung für Wirtschaft, Energie und Betriebe in Auftrag gegeben?

Zu 3.: Nein.

4. Warum wurde ein externes Sicherheitsberatungsunternehmen mit einer „Security Analyse“ beauftragt?

Zu 4.: Die BWB teilten mit, dass sie ihre Werke und Systeme mit einer umfassenden Sicherheitsarchitektur schützen. Diese sei nie fertig und werde stetig verbessert. Sie stressen ihre Systeme routine- und regelmäßig und lassen die Wirksamkeit der Schutzmaßnahmen überprüfen.

Vor einiger Zeit habe ein Mitarbeiter der BWB zur Vorbereitung eines Updates des Virenschutzes im Leit- und Informationssystem Abwasser (LISA) sensible Daten an das beauftragte Unternehmen verschickt. Diese Daten betrafen einen Teilbereich der Abwasserentsorgung, nicht das gesamte Unternehmen.

Nach Bekanntwerden sei ein externer Dienstleister - wie auch sonst regelmäßig - damit beauftragt worden, sofort zu überprüfen, ob Dritte Zugriff auf die Daten in der Mail hatten. Das sei nicht der Fall gewesen.

Die Üerprüfung habe dennoch eine Vielzahl von Erkenntnissen und bisweilen erheblichen Nachholbedarf ergeben.

5. Waren den Berliner Wasserbetrieben bereits vor der Beauftragung des Unternehmens Sicherheitsmängel bekannt?

Zu 5.: Sicherheitsmängel seien den BWB vor der eigenen Beauftragung des Gutachtens nicht in dem dort beschriebenen Umfang bekannt gewesen.

6. Seit wann liegt das Ergebnis der Analyse vor?

Zu 6.: Der Abschlussbericht sei den BWB am 25. Mai 2020 übermittelt worden.

7. Zu welchen Ergebnissen kommt Alpha Strike Labs in Bezug auf die Sicherheit der IT und das Leit- und Informationssystem Abwasser (LISA)? (Bitte detaillierte Darstellung)

8. Welche Mängel wurden festgestellt? (Bitte detaillierte Auflistung mit Einstufung des Gefahrenpotentials und Erläuterung)

Zu 7. und 8.: Nach Angaben der BWB sei zum Zeitpunkt des beauftragten Tests im Frühjahr 2020 der IT-/ OT-Sicherheitszustand (Informationstechnik/operative Technik) des LISA-Systems fehlerhaft und die Gefährdung des Systems hoch gewesen. Insgesamt habe es folgende Feststellungen gegeben:

- Acht Feststellungen der Kategorie Kritisch
- Neun Feststellungen der Kategorie Hoch
- Elf Feststellungen der Kategorie Mittel
- Fünf Feststellungen der Kategorie Niedrig

Bei dem in Teilen an die Öffentlichkeit gelangten Inhalt des Sicherheitsgutachtens handele es sich um als „vertraulich“ eingestufte Informationen bzw. um hochsensible Daten über Struktur, Schutzkonzepte- und Maßnahmen eines Unternehmens der kritischen Infrastruktur. Eine weitere Detailierung der Feststellungen würde den bestmöglichen Schutz der Systeme und Anlagen vor Cyber-Angriffen gefährden.

9. Wie bewertet Alpha Strike Laps den IT-Sicherheitszustand der Berliner Wasserbetriebe und die aktuelle Gefährdungslage?

Zu 9.: Nach Auskunft der BWB schätze Alpha Strike Labs GmbH den Sicherheitszustand von LISA per 31. Juli 2020 wieder als befriedigend ein. Johannes Klick, Geschäftsführer der Alpha Strike Labs GmbH, bewertet den aktuellen Projektfortschritt zum o.g. Zeitpunkt so: „Die in unserem Bericht zum Penetrationstest dargestellten Szenarien sind nicht mehr möglich.“ (vgl. auch https://www.bwb.de/de/24762.php).

10.Welche Maßnahmen haben die Berliner Wasserbetriebe nach der Vorlage des Berichts durch Alpha Strike Laps ergriffen?

Zu 10.: Nach interner Analyse und Bewertung der Ergebnisse des beauftragten Sicherheitsgutachtens (vgl. gemeinsame Antwort zu den Fragen 7. und 8.) seien seitens der BWB 52 Maßnahmen abgeleitet worden. Mit der Abarbeitung der Maßnahmen sei kurzfristig eine Task Force im Unternehmen beauftragt worden.

Eine weitere Detailierung der konkret ergriffenen Maßnahmen würde den bestmöglichen Schutz der Systeme und Anlagen vor Cyber-Angriffen gefährden.

11.Wie begründen die Berliner Wasserbetriebe die gravierenden Mängel bei der IT und dem Leit- und Informationssystem Abwasser (LISA)?

Zu 11.: Die Analyse laufe und sei noch nicht abgeschlossen. Die BWB tragen wie alle Unternehmen der kritischen Infrastruktur in und für Berlin eine hohe Verantwortung. Deshalb schützen sie ihre Werke und Systeme mit einer umfassenden Sicherheitsarchitektur. Im Wettstreit mit der organisierten Kriminalität sowie Hackerinnen und Hackern sei diese nie fertig und werde stetig verbessert.

12.Haben die Berliner Wasserbetriebe bereits einen Masterplan zur Beseitigung der Mängel erarbeitet?

Zu 12.: vgl. hierzu Antwort zur Frage 10.

Im Übrigen ergänze ein mittel- und langfristiges Maßnahmenpaket der BWB die aktuellen Aufgaben, u.a. mit folgenden Schwerpunkten:

- Prüfen und ggf. Erstellen der IT- und OT-Strategien und Architekturen,
- Roadmap Cybersicherheit - Sicherheitsleitstand,
- Schwachstellenmanagement,
- Identity Management System,
- Datenklassifizierung,
- Erhöhung des Bewusstseins für Sicherheit bei den Beschäftigten

13.Werden zur Beseitigung der Mängel externe Unternehmen hinzugezogen?

Zu 13.: Ja.

14.In welcher Art und Weise wird das Sicherheitsberatungsunternehmen Alpha Strike Laps bei der Behebung der Mängel involviert sein?

Zu 14.: Alpha Strike Labs GmbH begleite nach Auskunft der BWB die Task Force bei der Abarbeitung der Feststellungen und prüfe die jeweiligen Umsetzungsergebnisse auf ihre Wirksamkeit.

15.Wann werden die Mängel laut der Berliner Wasserbetriebe behoben sein?

Zu 15.: Zum Zeitpunkt 4. August 2020 seien von den 52 eingeleiteten Maßnahmen (vgl. hierzu Antwort zur Frage 10.) 32 bereits im Review oder abgeschlossen, 18 Maßnahmen in Arbeit und zwei Maßnahmen noch offen. Ziel sei es, alle eingeleiteten Maßnahmen unverzüglich abzuschließen.

Im Übrigen vgl. Antwort auf Frage 9.

16.Ist es zutreffend, dass die Berliner Wasserbetriebe auch die Sicherheit der Trinkwasserversorgung durch ein externes Unternehmen prüfen lassen werden?

Zu 16.: Ja. Die BWB haben mitgeteilt, dass sie auch schon in der Vergangenheit regel- und routinemäßig sowie in Abhängigkeit von der Kritikalität der Anlagen und Systeme die Wirksamkeit ihrer Schutzmaßnahmen überprüfe.

Hierzu zählen unter anderem:

- Monatliche automatisierte Testroutinen (sog. Vulnerability Scans), die u.a. auf aktuelle Releasestände, Patches und Sicherheitslücken prüfen sowie
- externe Penetrationstests im „Black Box-Verfahren“ (Angreifer erhält keine Informationen und greift von außen an) bzw. „White Box-Verfahren (Angreifer erhält Informationen und greift von innerhalb des Netzwerks an).

Zusätzlich seien die BWB nach § 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik - BSIG - („B3S“-Sicherheitsstandard) zertifiziert, hätten sich hierfür regelmäßig extern prüfen lassen, zuletzt im Jahr 2018.

17.Sind den Berliner Wasserbetrieben bereits Sicherheitslücken bei der Trinkwasserversorgung bekannt? Falls ja, welche?

Zu 17.: „Sicherheitslücken“, wie im Sicherheitsgutachten von Alpha Strike Labs GmbH vom 25. Mai 2020 beschrieben, seien den BWB für die Trinkwasserversorgung nicht bekannt. Die Systeme der Trinkwasserversorgung seien ihrer Natur nach in Art und Struktur auch nicht mit denen der Abwasserentsorgung vergleichbar.

18.Gedenken die Berliner Wasserbetriebe weitere „Systeme“ prüfen zu lassen? Falls ja, welche?

Zu 18.: Die BWB sicherten zu, dass sie alle ihre Systeme regel- und routinemäßig auf Verwundbarkeiten prüfen werden und dies auch in der Zukunft kontinuierlich fortzusetzen.

19.Wann hat Frau Senatorin Pop von den Missständen bei den Berliner Wasserbetrieben

Kenntnis erhalten?

Zu 19.: Senatorin Pop wurde über die Ergebnisse des Penetrationstests am LISA-Netzwerk der BWB durch den Vorstand der BWB im Rahmen einer Telefonkonferenz am 5. Juni informiert.

20.Welche Maßnahmen hat Frau Senatorin Pop eingeleitet, nachdem sie von den Missständen Kenntnis erhalten hat?

Zu 20.: Die Aufsichtsratsvorsitzende Senatorin Pop forderte den Vorstand der BWB auf, entsprechende Maßnahmen zu ergreifen und dem Aufsichtsrat regelmäßig sowie anlassbezogen über die Umsetzung der auf Basis der Ergebnisse des Penetrationstests am LISA-Netzwerk unternehmensseitig abgeleiteten Maßnahmen zu berichten.

21.Waren Frau Senatorin Pop bereits vor der „Security Analyse“ durch Alpha Strike Labs Mängel bei den Berliner Wasserbetrieben bekannt?

Zu 21.: Das Thema der Cybersicherheit bei den BWB ist regelmäßig Bestandteil der Berichterstattung des Vorstands an den Aufsichtsrat der BWB. Dies beruht darauf, dass die BWB zum Schutz der Cybersicherheit periodisch Risikoanalysen vornehmen. Über dabei etwa gefundene Risiken und abgeleitete Maßnahmen informiert der

Vorstand den Aufsichtsrat entsprechend.

22.Wann wurde der Aufsichtsrat über die gravierenden Mängel in Kenntnis gesetzt?

Zu 22.: Der Personalausschuss des Aufsichtsrates der BWB wurde am 8. Juni 2020 informiert, der Aufsichtsrat der BWB wurde im Rahmen der Aufsichtsratssitzung am 17. Juni 2020 über die Ergebnisse des Penetrationstests am LISA-Netzwerk und den Sachstand zur Umsetzung der unternehmensseitig abgeleiteten Maßnahmen informiert.

Berlin, den 17. August 2020

In Vertretung

Christian R i c k e r t s
.....
Senatsverwaltung für Wirtschaft,
Energie und Betriebe