Landtag von Baden-Württemberg **Drucksache 16 / 6583**

16. Wahlperiode **15. 07. 2019**

Kleine Anfrage

des Abg. Dr. Rainer Podeswa AfD

und

Antwort

des Ministeriums für Inneres, Digitalisierung und Migration

Einsatz von Ransomware gegen Städte, Gemeinden, Behörden oder die Regierung

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie sind die Städte und Gemeinden in Baden-Württemberg auf Ransomware-Angriffe und Lösegeld-Forderungen vorbereitet, insbesondere da die Angriffe laut ihren Angaben (siehe Drucksache 16/2076) zunehmen?

2. Wie oft und auf welche Art wird die IT der Städte und Gemeinden gesichert bzw. falls dies in Selbstverwaltung durch die Städte organisiert wird: wie oft und auf welche Art wird die IT der Großstädte in Baden-Württemberg gesichert?

3. Ist sichergestellt, dass die IT-Sicherungen nicht ebenfalls durch eine Ransomware beschädigt werden könnten?

4. Wie sind die Regierungseinrichtungen, die Ministerien und weitere kritische und relevante staatliche Einrichtungen wie das Landesamt für Besoldung auf Ransomware-Angriffe und Lösegeld-Forderungen vorbereitet?

5. Hält sie die Landesverwaltung den baden-württembergischen Unternehmen für technisch weit überlegen oder wie kommt sie in Drucksache 16/2076 zu der Aussage, dass die Mailserver der Landesverwaltung verdächtige Anhänge quasi einfach herausfiltern, was Unternehmen mit Sicherheit genauso versuchen?

6. Wie oft wurden in der aktuellen Legislaturperiode schon Systeme aufgrund einer Infizierung bei den Landesbehörden neu installiert (vergleiche ebenfalls ihre Aussagen in Drucksache 16/2076)?

7. Hätten die Städte und Gemeinden die Möglichkeit, kurzfristig an Kryptowährungen wie Bitcoins für Lösegeldzahlungen zu kommen?

Eingegangen: 15. 07. 2019 / Ausgegeben: 23. 08. 2019

8. Gibt es Empfehlungen seitens der Landesregierung bezüglich dem Umgang mit Erpressungsversuchen?

9. Hält sie die in Ziffer 13 von Drucksache 16/2076 genannten nur drei Experten beim Landesamt für Verfassungsschutz im Themenfeld nachrichtendienstlich gesteuerter Cyberspionage und -sabotage weiterhin für ausreichend, insbesondere im Hinblick auf die zunehmende Internetkriminalität und Staaten, die (angeblich oder tatsächlich) ganze Cyberarmeen aufstellen?

10. Was kennzeichnet einen, wie sie in der vorgenannten Drucksache schreibt, „extrem qualifizierten“ Mitarbeiter in diesem Tätigkeitsfeld?

10. 07. 2019

Dr. Podeswa AfD

Begründung

Unbekannte Kriminelle forderten nach einem Ransomware-Angriff auf die Stadtverwaltung von Baltimore Lösegeld von mehreren zehntausend Dollar – sonst würden wichtige Dokumente zerstört. Die Stadt Greenville in North Carolina wurde im April vermutlich mit demselben Virus angegriffen und zu erpressen versucht. Im vorigen Jahr griffen zwei Iraner die Informatik der Großstadt Atlanta in Georgia an (siehe z. B. NZZ vom 23. Mai 2019).

Städte scheinen nach Auffassung des Fragestellers daher zunehmend zum Angriffsziel Krimineller zu werden, die Lösegeld erpressen wollen. Die Kleine Anfrage soll der Situation in Baden-Württemberg nachgehen. Wie sind die Städte und Gemeinden hier vorbereitet? Da unsere Städte, im Gegensatz zu vielen US-Städten, häufig solventer sind, sollte man nach Auffassung des Fragestellers auf entsprechende Risiken vorbereitet sein.

Antwort

Mit Schreiben vom 9. August 2019 Nr. 5-0141.5/1 beantwortet das Ministerium für Inneres, Digitalisierung und Migration im Einvernehmen mit dem Ministerium für Finanzen die Kleine Anfrage wie folgt:

1. Wie sind die Städte und Gemeinden in Baden-Württemberg auf Ransomware-Angriffe und Lösegeld-Forderungen vorbereitet, insbesondere da die Angriffe laut ihren Angaben (siehe Drucksache 16/2076) zunehmen?

2. Wie oft und auf welche Art wird die IT der Städte und Gemeinden gesichert bzw. falls dies in Selbstverwaltung durch die Städte organisiert wird: wie oft und auf welche Art wird die IT der Großstädte in Baden-Württemberg gesichert?

3. Ist sichergestellt, dass die IT-Sicherungen nicht ebenfalls durch eine Ransomware beschädigt werden könnten?

Zu 1. bis 3.:

Die Fragen 1 bis 3 betreffen Themen der kommunalen Selbstverwaltung im unmittelbaren Verantwortungsbereich der Städte und Gemeinden. Eine Beantwortung der gestellten Fragen durch die Landesregierung ist daher nicht möglich. Be-

stehende Unterstützungsangebote der Landesverwaltung für Kommunen im Bereich der IT-Sicherheit sind in der Stellungnahme zu Ziffer 18 der Großen Anfrage der Fraktion der FDP/DVP – IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und Institutionen im besonderen staatlichen Interesse (INSI) – Drucksache 16/3345 vom 24. Januar 2018 aufgeführt.

4. Wie sind die Regierungseinrichtungen, die Ministerien und weitere kritische und relevante staatliche Einrichtungen wie das Landesamt für Besoldung auf Ransomware-Angriffe und Lösegeld-Forderungen vorbereitet?

Zu 4.:

Hinsichtlich präventiver technischer und strategischer Maßnahmen wird auf die Antworten zu Ziffer 3 des Antrags der Abg. Rainer Stickelberger u. a. SPD – Cybersicherheit in Baden-Württemberg – Drucksache 16/2129 vom 24. Mai 2017 und die Antworten zu Ziffer 4, Abschnitt „Sektor Staat und Verwaltung“ der Großen Anfrage der Fraktion der FDP/DVP – IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und Institutionen im besonderen staatlichen Interesse (INSI) – Drucksache 16/3345 vom 24. Januar 2018 verwiesen. Hierbei ist die Anwendung der Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hervorzuheben. Diese umfassen sowohl präventive als auch reaktive Maßnahmen ebenso wie die Ausgestaltung eines entsprechenden Notfallmanagements. Für festgestellte Sicherheitsvorfälle – darunter fallen auch Ransomware-Angriffe – sind entsprechende Melde- und Eskalationswege etabliert, sodass eine Beteiligung aller erforderlichen Stellen sichergestellt ist.

5. Hält sie die Landesverwaltung den baden-württembergischen Unternehmen für technisch weit überlegen oder wie kommt sie in Drucksache 16/2076 zu der Aussage, dass die Mailserver der Landesverwaltung verdächtige Anhänge quasi einfach herausfiltern, was Unternehmen mit Sicherheit genauso versuchen?

Zu 5.:

Die in der Antwort zum Antrag der Abg. Dr. Timm Kern u. a. FDP/DVP – Cybersicherheit in Baden-Württemberg – Drucksache 16/2076 vom 17. Mai 2017 getroffene Aussage *„Die Mailserver der Landesverwaltung Baden-Württemberg filtern verdächtige Anhänge heraus“* bezog sich in erster Linie auf die zum Zeitpunkt der Anfragestellung im Frühjahr 2017 sehr aktuelle, weltweit erfolgte und medial präsente Wannacry-Attacke. Diese Aussage stellt keinerlei Wertung gegenüber anderen IT-Betreibern in Behörden oder Unternehmen dar. Die Mechanismen der Landesverwaltung zur Ausfilterung von Schadsoftware weisen eine hohe Effizienz auf, hundertprozentige Sicherheit gibt es weder in der Verwaltung noch in Unternehmen.

6. Wie oft wurden in der aktuellen Legislaturperiode schon Systeme aufgrund einer Infizierung bei den Landesbehörden neu installiert (vergleiche ebenfalls ihre Aussagen in Drucksache 16/2076)?

Zu 6.:

In rund 20 unterschiedlichen Fällen mussten Systeme wegen Infizierung mit Schadsoftware neu installiert werden.

7. Hätten die Städte und Gemeinden die Möglichkeit, kurzfristig an Kryptowährungen wie Bitcoins für Lösegeldzahlungen zu kommen?

Zu 7.:

Auf die Antwort zu den Fragen 1 bis 3 wird verwiesen.

8. Gibt es Empfehlungen seitens der Landesregierung bezüglich dem Umgang mit Erpressungsversuchen?

Zu 8.:

Bei Erpressungsversuchen wird empfohlen, schnellstmöglich Kontakt mit der Polizei aufzunehmen und Anzeige zu erstatten. So steht beispielsweise mit der Zentralen Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt rund um die Uhr eine Kompetenzstelle zur Verfügung, die im Falle eines Angriffs auf Computer oder Netzwerke weiterhelfen kann. Städte und Gemeinden, Behörden und Wirtschaftsunternehmen können sich bei IT-Sicherheitsvorfällen direkt an die ZAC wenden. Die ausgewiesenen Experten nehmen die Anzeige entgegen und leiten sofort polizeiliche Erstmaßnahmen ein oder vermitteln an Ansprechpartner bei den eng vernetzten örtlichen Dienststellen. Darüber hinaus ist eine Anzeigeerstattung bei jeder Polizeidienststelle möglich. Von dort werden die weiteren Schritte, wie beispielsweise die Einschaltung von Experten zur Bewältigung von Erpressungslagen, veranlasst.

Auch außerhalb akuter Erpressungslagen bieten die Experten der ZAC Beratungs- und Unterstützungsleistung an. Die Erfahrungen zeigen, dass es für Behörden und Unternehmen wichtig ist, sich frühzeitig mit möglichen Bedrohungsszenarien vertraut zu machen, um die erforderlichen Schutzmöglichkeiten zu kennen und im Ernstfall die richtigen Maßnahmen ergreifen zu können.

9. Hält sie die in Ziffer 13 von Drucksache 16/2076 genannten nur drei Experten beim Landesamt für Verfassungsschutz im Themenfeld nachrichtendienstlich gesteuerter Cyberspionage und -sabotage weiterhin für ausreichend, insbesondere im Hinblick auf die zunehmende Internetkriminalität und Staaten, die (angeblich oder tatsächlich) ganze Cyberarmeen aufstellen?

Zu 9.:

Wie in der Stellungnahme zu Ziffer 6 des Antrags der Abg. Nico Weinmann u. a. FDP/DVP – Die sogenannte Cyberwehr in der Sicherheitsarchitektur des Landes – Drucksache 16/2737 vom 26. September 2017 dargestellt, werden die Experten des Landesamtes für Verfassungsschutz Baden-Württemberg (LfV) im Einzelfall von weiteren Mitarbeitern des IT-Sicherheitsmanagements und des beratend tätigen Wirtschaftsschutzteams fachtechnisch unterstützt. Unabhängig davon erfolgt laufend eine Ermittlung des Personalbedarfs, so auch im Bereich der nachrichtendienstlich gesteuerten Cyberspionage und -sabotage.

10. Was kennzeichnet einen, wie sie in der vorgenannten Drucksache schreibt, „extrem qualifizierten“ Mitarbeiter in diesem Tätigkeitsfeld?

Zu 10.:

In der referenzierten Antwort zur Drucksache 16/2076 wurde hinsichtlich der beschriebenen Herausforderungen der Begriff „extern qualifizierten Mitarbeiter“ verwendet, nicht das Wort „extrem“.

Für die Aufgabenbereiche der Cyberabwehr beim LfV sind insbesondere Praktiker aus nachfolgenden Berufsbildern bzw. Absolventen entsprechender Studiengänge, sowohl mit Hochschul-/Masterabschluss wie auch mit Fachhochschul-/Bachelorabschluss besonders qualifiziert und geeignet: Cyberforensiker/-innen, Netzwerkforensiker/-innen, Netzwerktechniker/-innen, Informatiker/-innen und Ingenieure/-innen.

In Vertretung

Krebs

Ministerialdirektor