Freie und Hansestadt Hamburg
Bezirksversammlung Altona

Drucksachen–Nr.: **21-3126**

Kleine Anfrage öffentlich

Beratungsfolge		
	Gremium	**Datum**
Öffentlich	Bezirksversammlung	25.05.2022

Ist Altona gegen Cyberangriffe gewappnet?
Kleine Anfrage von Wolf Achim Wiegand (FDP-Fraktion)

Die internationale Lage nach dem Angriffskrieg Russlands gegen die Ukraine hat den Fokus erneut auf die Cybersicherheit gelenkt. Experten befürchten, dass sich die schon vor der Invasion gehäuften Netzangriffe nochmals potenzieren könnten.

Unter anderem war im vergangenen Dezember die kritische Zero-Day-Schwachstelle Log4Shell entdeckt worden. Millionen von Java-Anwendungen seien noch immer anfällig für Angriffe, fanden Forscher des israelischen Sicherheitsunternehmens Rezilion kürzlich heraus. Dabei lasse sich die Schwachstelle leicht ausnutzen und könne die vollständige Übernahme des Servers ermöglichen. Mögliche Attacken werden in China oder Iran verortet.

Die Bedrohung durch Späh- oder Schadangriffe kommt nicht nur von militärisch oder politisch motivierten Angreifern, sondern in großer Zahl von Kriminellen. Diese Eindringlinge sind in der Regel global aktive und hochprofessionelle Erpresserbanden der Organisierten Kriminalität. Sie operieren von Standorten rund um den Globus aus. Dabei verfeinern und verbessern sie ihre Methoden ständig, um immer besseren Zugang zu verschlüsselten Systemen zu bekommen.

Im besonderen Fokus von Cyberangriffen stehen Behörden, da sie kritische Infrastruktur und für das Funktionieren des Staates nötige Daten verwalten bzw. nutzen. Eine Attacke auf staatliche Stellen kann unermessliche Schäden bewirken - bis hin zur realen Bedrohung von Leib und Leben der Bevölkerung.

Das Bezirksamt Altona beantwortet die Fragen wie folgt:

1. *Wie erstellt das Bezirksamt Altona eine vollständige, zeitnahe Sicherungskopie (Back-up) seiner Systeme, damit die korrekten Daten im Angriffsfall nach Neustart aller Systeme unverzüglich zurückgespielt werden können?*

a. *Gibt es dafür ein offline Back-up?*

Zu 1.a:
Seit 2007 ist Dataport der zentrale IT-Dienstleister für die öffentliche Verwaltung und damit auch für das Bezirksamt Altona. Das Bezirksamt Altona erstellt von sich aus keine eigenen Sicherungskopien der Systeme. In welchen Abständen durch Dataport Sicherungskopien angefertigt werden, ist dem Bezirksamt Altona nicht bekannt.

2. *Wie sensibilisiert das Bezirksamt Altona alle Mitarbeiter für Cyber-Angriffe, damit sie nicht auf Mails oder Chats potenzieller Angreifer reinfallen und Passwörter etc. bekannt geben?*

Zu 2:
Der Abschnitt IT-Angelegenheiten und -Projekte des Bezirksamtes Altona versendet regelmäßig E-Mails an alle Beschäftigten des Bezirksamtes, um vor potentiell schädlichen Mails (und insbesondere den Anhänge in diesen) zu warnen. Dataport informiert entsprechend über aktuelle Gefahren und Hinweise, die durch uns dann jeweils an die Beschäftigten weitergegeben werden. Des Weiteren stehen Informationen über die potentiellen Gefahren von externen Mails auf unserem internen SharePoint jederzeit zur Verfügung.

3. *Wie stellt das Bezirksamt Altona sicher, dass alle Systeme auf dem aktuellen Patchstand sind?*

Zu 3:
Seit 2007 ist Dataport der zentrale IT-Dienstleister für die öffentliche Verwaltung und damit auch für das Bezirksamt Altona. Die regelmäßigen Aktualisierungen werden über Dataport angestoßen. Das Bezirksamt Altona hat hierauf keinen Einfluss.

4. *Wie stellt das Bezirksamt sicher, dass Altsysteme, die nicht mehr gewartet werden, durch aktuelle Versionen oder andere Software ersetzt werden?*

Zu 4:
Auch hierauf hat das Bezirksamt Altona keinen Einfluss. Dataport prüft die Software und stellt diese der FHH zur Verfügung. Das Bezirksamt Altona hat keine Möglichkeit, selbständig Software zu installieren, ohne dass Dataport diese Software über den Dataport Warenkorb zugänglich macht. Das heißt, dass das Bezirksamt Altona zwar Software installieren kann, aber nur jene, die sich im Dataport Warenkorb befindet.

5. *Welche Sicherheitssoftware setzt das Bezirksamt Altona ein, um Viren und andere Ereignisse (Security Information & Event Management – SIEM) rechtzeitig zu erkennen?*

Zu 5:
Welche Sicherheitssoftware seitens Dataport an die FHH angebunden ist, kann das Bezirksamt Altona nicht beantworten. Hierzu kann lediglich mitgeteilt werden, dass als SPAM erkannte eingehende Mails auch direkt als SPAM markiert werden. Mails, die (noch) nicht als SPAM erkannt wurden, bei denen es sich aber offensichtlich um SPAM handelt (bspw. durch den Absender oder den Betreff erkennbar), können an eine eigene Maildresse bei Dataport weitergeleitet werden (spam@dataport.de). Dort wird die SPAM-Mail dann geprüft, um zukünftig ggf. den Absender zu sperren o.ä. Weitere Informationen hierzu kann Ihnen sicherlich Dataport direkt geben.

a. *Wie oft und regelmäßig wertet das Bezirksamt Altona die Log-Files und die Ergebnisse der Sicherheitssoftware aus?*

Zu 5.a:
Das Bezirksamt Altona wertet keine Log-Files oder Ergebnisse einer Sicherheitssoftware aus. Auch hier liegt die Zuständigkeit bei Dataport als zentraler IT-Dienstleister.

b. *Wie stellt das Bezirksamt Altona sicher, dass Alarmen unverzüglich und zu jeder Zeit nachgegangen werden kann?*

Zu 5.b:
Auch zu diesem Punkt liegt die Zuständigkeit bei Dataport als zentraler IT-Dienstleister für die FHH.

6. *Wie üben die Mitarbeiter des Bezirksamtes solche Katastrophenfälle, damit alle wissen, wie man auf Cyber-Angriffe reagieren muss?*

Zu 6:
Das Bezirksamt Altona führt keine Katastrophenübungen für den Fall eines Cyberangriffes durch, da hierzu auch die Zugriffe fehlen würden. Die Zuständigkeit liegt hier bei Dataport und in für den Katastrophenschutz bei der Behörde für Inneres und Sport.

a. Welche Schulungen mit Mitarbeitern führt das Bezirksamt Altona speziell zur Beherrschung von Ransomware-Angriffen durch?

Zu 6.a:
Das Bezirksamt Altona führt keine Schulungen zur Beherrschung von Ransomware-Angriffen durch.

b. Werden Cyberangriffe zu Schulungszwecken simuliert?

Zu 6.b:
Das Bezirksamt Altona simuliert keine Cyberangriffe zu Schulungszwecken.

7. Welche Versicherung gegen Cyberangriffe hat das Bezirksamt Altona und was deckt sie (nicht) ab?

Zu 7:
Die benötigten Sicherheitsanforderungen und Sicherheitsbedürfnisse werden durch Dataport (nach zentraler Entscheidung durch die Senatskanzlei) umgesetzt. Ob es zwischen der FHH und Dataport hierzu eine Versicherung, Verträge o.ä. gibt, ist dem Bezirksamt Altona nicht bekannt.

8. Wie lässt das Bezirksamt Altona sein IT-Sicherheitsniveau professionell bewerten – nicht nur mit ‚Penetration Tests' von innen und außen, sondern auch in Bezug auf die Verschlüsselung der Kommunikation?

Zu 8:
Das Bezirksamt Altona bewertet das IT-Sicherheitsniveau nicht selbständig, da auch dies in die Zuständigkeit des zentralen IT-Dienstleisters Dataport fällt. Wie das IT-Sicherheitsniveau seitens Dataport bewertet wird, kann das Bezirksamt Altona nicht mitteilen.

9. Wie stellt das Bezirksamt Altona sicher, dass nicht nur automatisierte Tests zur Identifizierung potenzieller Sicherheitslücken durchgeführt werden, sondern insbesondere auch folgende Spezialprüfungen:

a. Vulnerability Scans der Systeme zur Identifizierung veröffentlichter Sicherheitslücken.

Zu 9.a:
Zu diesem Punkt muss erneut auf Dataport verwiesen werden.

b. Identifizierung unveröffentlichter Sicherheitslücken.

Zu 9.b:
Zu diesem Punkt muss erneut auf Dataport verwiesen werden.

c. Händische Untersuchung aller Systeme auf veraltete und ungepatchte Softwareversionen.

Zu 9.c:
Zu diesem Punkt muss erneut auf Dataport verwiesen werden.

d. *Untersuchung auf inkorrekte und damit unsichere Parametrisierung von Software wie z. B. Virtual Private Networks (VPN) und Mailverschlüsselung*.

Zu 9.d:
Zu diesem Punkt muss erneut auf Dataport verwiesen werden.

Petitum:
Die Bezirksversammlung wird um Kenntnisnahme gebeten.

Anlage/n:
ohne