Abgeordnetenhaus BERLIN

Drucksache 19 / 18 456
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Marc Vallendar (AfD)

vom 29. Februar 2024 (Eingang beim Abgeordnetenhaus am 1. März 2024)

zum Thema:

Jurassic Hack - Cyberattacke auf Berliner Naturkundemuseum

und **Antwort** vom 13. März 2024 (Eingang beim Abgeordnetenhaus am 15. März 2024)

Senatsverwaltung für Wissenschaft,
Gesundheit und Pflege

Herrn Abgeordneten Marc Vallendar (AfD)

über

die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 19/18 456
vom 29. Februar 2024
über Jurassic Hack - Cyberattacke auf Berliner Naturkundemuseum

---

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

Vorbemerkung der Verwaltung:
Die Anfrage betrifft Sachverhalte, die der Senat nicht ohne Beiziehung des Museums für Naturkunde (MfN) beantworten kann. Das MfN wurde daher um Stellungnahme und Beantwortung zu den Fragen 1-4 gebeten.

Vorbemerkung des Abgeordneten:
Im Oktober 2023 wurde das Berliner Naturkundemuseum Ziel eines gravierenden Cyberangriffs, bei dem personenbezogene Daten von Kunden, einschließlich sensibler PayPal-Informationen, entwendet wurden.[1] Dieser Vorfall offenbart nicht nur die Verletzlichkeit unserer öffentlichen Institutionen gegenüber digitalen Bedrohungen, sondern stellt auch ein erhebliches Risiko für die Privatsphäre und finanzielle Sicherheit der Betroffenen dar. Angesichts der Schwere des Angriffs, der zum Diebstahl kritischer Daten und zur Arbeitsunfähigkeit von 450 Mitarbeitenden führte,[2] sowie der anschließenden Veröffentlichung eines Teils dieser Daten im Internet, ist es von entscheidender Bedeutung, die Umstände dieses Vorfalls gründlich zu untersuchen und Maßnahmen zur Verbesserung der Cybersicherheit und zum Schutz der Bürger Berlins zu ergreifen.

---

[1] https://www.rbb24.de/panorama/beitrag/2024/02/naturkundemuseum-cyberattacke-kundendaten-hacker-berlin.html
[2] https://www.rbb24.de/panorama/beitrag/2023/11/berlin-naturkundemuseum-cyberangriff-computersystem

1.Welche Maßnahmen wurden ergriffen, um die Quelle des Cyberangriffs zu identifizieren und die Verantwortlichen zur Rechenschaft zu ziehen?

Zu 1.:

Unmittelbar nach der Entdeckung des Cyberangriffs wurde ein spezialisierter und renommierter First Response Cybersecurity Dienstleister mit der Analyse des Angriffs beauftragt. Er konnte den Angreifer, eine russische Hackergruppe, eindeutig identifizieren. Parallel dazu erstattete das Museum Strafanzeige beim Landeskriminalamt (LKA) und informierte die Beauftragte für Datenschutz und Informationsfreiheit des Landes Berlin. Darüber hinaus wurde das Bundesamt für die Sicherheit in der Informationstechnik (BSI) um Beratung gebeten. Die Ermittlungen des LKA dauern an.

2. In welchem Ausmaß waren die Schäden, die durch den Angriff entstanden sind, und welche Schritte wurden unternommen, um diese Schäden abzumildern?

Zu 2.:

Durch den Angriff wurde die gesamte IT-Infrastruktur kompromittiert und muss vollständig neu aufgesetzt werden, da sich die Angreifer vollen Zugriff auf das Netzwerk und deren Komponenten (Server und Endgeräte der Benutzer) verschaffen konnten. Hierdurch entstanden Kosten in Millionenhöhe, die sich zusammensetzen aus den notwendigen Dienstleistungen, der Schaffung eines neuen Sicherheitslevels und der notwendigen Beschaffung von Ersatztechnik zum Wiederaufbau einer sicheren IT-Infrastruktur.
Zusätzlich entstanden weitere Schäden durch eine monatelange Betriebsunterbrechung, Verluste durch verschlüsselte und aktuell nicht wiederherstellbare Forschungsdaten, sowie ein hoher Aufwand zur Wiederherstellung der gesamten Kommunikation, Geschäftsprozesse, Arbeitsfähigkeit und Forschungstätigkeiten.
Es wurden alle Sofortmaßnahmen zur Schadensbegrenzung ergriffen, darunter die Isolierung infizierter Systeme, das Sperren sämtlicher Zugriffe von außen und von innen sowie das Abschalten aller kritischen Systeme. Es wurde ein Modell für den Notbetrieb etabliert, um die basalen Geschäftsprozesse wiederaufzunehmen. Es wurde begonnen, verlorene oder beschädigte Daten wiederherzustellen, unter Verwendung von Backup- und Restore-Verfahren. Diese Aktivitäten dauern weiterhin an.

Bei den hier beschriebenen Maßnahmen war das Museum im ständigen Austausch mit dem LKA und ist dessen Ratschlägen gefolgt. Die Ermittlungen des LKA wurden durch eine Datenbereitstellung unterstützt.

3. Wurde die Sicherheitssoftware des Naturkundemuseums aktualisiert, um ähnliche Angriffe in der Zukunft zu verhindern? Wenn ja, welche spezifischen Maßnahmen wurden ergriffen?

Die IT-Sicherheitslösungen des Museums wurden nach dem Cyberangriff erheblich verstärkt. So können sogenannte Zero-Day-Exploits schnell erkannt und behoben werden und die Effektivität zur Mitigierung von aktuellen Bedrohungen wurde deutlich verbessert. Die Integration von Intrusion Detection und Prevention Systemen wurde durchgeführt, um verdächtige Aktivitäten 24/7 zu monitoren, zu erkennen und sofortige Gegenmaßnahmen ergreifen zu können.
Die gesamte IT-Infrastruktur wird weiterhin parallel neu aufgebaut, um zukünftigen Bedrohungen standhalten zu können. Dies beinhaltet die Überprüfung aller Daten und die Erneuerung sämtlicher Server und Endgeräte.

4. Wie hat der Senat sichergestellt, dass die betroffenen Kunden rechtzeitig und effektiv über die Datenschutzverletzung informiert wurden? Wieviele Kunden waren insgesamt betroffen?

Das Museum für Naturkunde hat gem. Art. 34 DSGVO unverzüglich auf seiner Website über den Vorfall informiert. Sobald im Rahmen der Analyse des Angriffs von ihm Kunden identifiziert werden konnten, von denen sensible Daten betroffen waren, hat das Museum diese zusätzlich gezielt per E-Mail informiert. Bei sämtlichen Informationen hat sich das Museum bemüht, den Betroffenen möglichst umfangreiche und konkrete Hilfestellungen zu geben und Vorsichtsmaßnahmen zu empfehlen. Die in Bezug auf die Information der Betroffenen ergriffenen Maßnahmen wurden der zuständigen Datenschutzaufsichtsbehörde mehrmals mitgeteilt. Alle Maßnahmen wurden eng abgestimmt mit einem auf Datenschutzrecht spezialisierten Anwalt. Dabei wurden auch die von den deutschen und europäischen Aufsichtsbehörden veröffentlichten Orientierungshilfen zum Umgang mit Datenschutzvorfällen berücksichtigt.

Betroffen sind ein Teil der Kunden, die seit 2021 Tickets im Onlineshop des Museums erworben und mit PayPal gezahlt haben. Es handelt sich hierbei um 37.243 betroffene Kunden, das sind ca. 2 Prozent der Besuchenden des Museums.

5. Welche Maßnahmen wurden ergriffen, um ähnliche Angriffe auf andere öffentliche Einrichtungen in Berlin zu verhindern?

Die in dem zuständigen Referat betreuten außeruniversitären Forschungsinstitute sind rechtlich selbstständig und tragen insofern selbst die Verantwortung für eine funktionierende IT-Sicherheit.

Bei Einrichtungen, die als juristische Personen des öffentlichen Rechts organisiert sind, bestehen staatliche Eingriffsmöglichkeiten im Wege der Staats- und Rechtsaufsicht, soweit die Voraussetzungen hierfür gegeben wären.

Berlin, den 13. März 2024

In Vertretung
Dr. Henry Marx
Senatsverwaltung für Wissenschaft,
Gesundheit und Pflege