Abgeordnetenhaus BERLIN

Drucksache 19 / 11 670
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Tobias Schulze (LINKE)

vom 22. April 2022 (Eingang beim Abgeordnetenhaus am 22. April 2022)

zum Thema:

Samma hackt's?! Zum Angriff auf die IT-Systeme der TU Berlin

und **Antwort** vom 10. Mai 2022 (Eingang beim Abgeordnetenhaus am 11. Mai 2022)

Senatsverwaltung für Wissenschaft,
Gesundheit, Pflege und Gleichstellung

Herrn Abgeordneten Tobias Schulze (LINKE)

über

den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 19/11 670
vom 22. April 2022
über „Samma hackt's?! Zum Angriff auf die IT-Systeme der TU Berlin“

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

Die Schriftliche Anfrage betrifft Sachverhalte, die der Senat nicht ohne Beiziehung der Technischen Universität Berlin (TUB) beantworten kann. Diese wurde um Stellungnahme zu den Fragen 1 bis 13 gebeten.

1. Vor einem Jahr wurde die TU Berlin Ziel eines Angriffs auf die gesamte IT-Infrastruktur. Sind immer noch Dienste, oder IT-Ressourcen nicht nutzbar oder nur eingeschränkt nutzbar? Wenn ja, um welche Software- oder Systemkomponenten sowie Dienste handelt es sich und wann ist voraussichtlich wieder mit einer uneingeschränkten Nutzung zu rechnen?

Zu 1.:

Nach Auskunft der TUB sei der (Wieder-)Aufbau einer in Teilen modifizierten IT-Infrastruktur in den wesentlichen Teilen abgeschlossen. In Arbeit seien noch Anpassungen bzw. Verbesserungen vor allem im Bereich des Identifikationsmanagements sowie der Prozesslogik, die dem Umbau der IT-Architektur geschuldet sind. Betroffen seien hiervon noch die vor dem Angriff verfügbaren Self-Services für die dezentralen Bereiche. Der Anpassungsaufwand durch den gleichzeitig mit der Behebung der Schäden durchgeführten Wechsel des Identitätsmanagement-Systems sei nicht unerheblich und werde für die TUB deshalb noch einige Zeit in Anspruch nehmen.
Die TUB hat sich außerdem dafür entschieden, parallel zur Behebung der Schäden zusätzliche neue IT-Dienstleistungen einzuführen, die es vor dem Vorfall nicht gab.

2. Wie lange nach dem Angriff waren welche Software- und Systemkomponenten sowie Dienste der TU Berlin nicht nutzbar?

Zu 2.:
Eine Dokumentation dazu, welcher Dienst - in vollem oder zunächst nur eingeschränktem Umfang - zu welchem Zeitpunkt wieder angeboten wurde, hat die TU Berlin zum Abschluss ihrer ab 30. April 2021 laufenden aktualisierten Nachrichten nicht erstellt. Die Mitglieder der TU Berlin konnten sich auf der zentralen Webseite über den jeweils aktuellen Stand informieren (https://www.tu.berlin/themen/einschraenkung-it-services/).

Als Beispiele können genannt werden: Die Dienste für den Lehr- und Studienbetrieb inkl. Videokonferenzmöglichkeiten standen den Angehörigen der TUB ab dem zweiten Werktag nach der angriffsbedingten Abschaltung wieder zur Verfügung, die Nutzung der tubCloud und eines temporären Not-Mail-Systems ab etwa Mitte Mai. Der Exchange-Service stand nach etwa drei Monaten zur Verfügung. Die Finanzbuchhaltung war bis Juli 2021 stark eingeschränkt (prioritäre Vorgänge wie z.B. Buchungen von Gehaltszahlungen und Rechnungen konnten manuell, z.T. verzögert, durchgeführt werden). Mit Beginn des Wintersemesters 2021/2022 standen die meisten der Dienste und Services wieder zur Verfügung. Die Wiedereinsetzung der integrierten digitalen Verwaltungssysteme für die Bereiche Ressourcenmanagement und Studierendenverwaltung konnte nach sechs Wochen beginnen und nahm mehrere Monate in Anspruch. Immatrikulationen, Prüfungsanmeldungen und Zeugnisausstellungen waren z.T. bis in das Wintersemester 2021/22 hinein beeinträchtigt; dem wurde mit entsprechenden Fristverlängerungen begegnet.

3. Ist die Analyse des Angriffs mittlerweile abgeschlossen und konnte ein komplettes Schadensbild erstellt werden?

Zu 3.:
Auf Grund der Vielzahl der betroffenen Systeme wurde die forensische Analyse auf den Angriffsweg und die Identifikation der kompromittierten zentralen Systeme beschränkt. Diese Analyse der wesentlichen Aspekte des Angriffs ist nach Auskunft der TUB abgeschlossen. Die daraus resultierenden Ergebnisse beschreiben einen Angriffsweg, bei dem die TUB und ihr Dienstleister davon ausgehen, dass dessen vollständige Erfassung gelungen ist. Die forensischen Arbeiten wurden von einem laut Bundesamt für Sicherheit in der Informationstechnik (BSI) qualifizierten Dienstleister durchgeführt.

4. Welche Daten wurden während des Angriffs entwendet?

Zu 4.:
Die TUB hatte bereits frühzeitig bekannt gemacht, dass das Active Directory (Gliederung der Netzwerkstruktur) kopiert wurde. Außerdem gibt die TU Berlin an, dass insgesamt 5566 Dateien gemäß folgender Aufstellung entwendet oder beschädigt wurden. Betroffene wurden entsprechend den Datenschutzrichtlinien informiert.

Art der Dateien (Informationen zu Inhalten bzw. zur Einschätzung des TU-Datenschutzteams)	Anzahl
Dokumente, die als unkritisch eingeschätzt werden (Fotos ohne Personen, datenschutzrechtlich unbedenkliche Dokumente)	3.221
Systemdateien (ohne datenschutzrechtliche Relevanz)	1.148
beschädigte Dokumente (technische Wiederherstellung erfolglos)	36
passwortgeschützte Dokumente (Prüfung durch Bereich)	132
Dokumente, die Passwörter enthalten	26
Dokumente aus Berufungsverfahren (Bewerbungsunterlagen, Gutachten, Sitzungsprotokolle)	190
Dokumente mit Gesundheitsdaten (nur einzelne Informationen zu Personen-dosimetrien aus TU-Laboren)	5
Dokumente zu Lehraufträgen (nur Namen und Vergütung, nur einzelne Aufträge)	12
Dokumente mit Matrikelnummern (Kursteilnehmerlisten, 169 Personen)	1
Dokumente sortiert nach Beschäftigten (5 Beschäftigte, einzelne Personalverwaltungsdateien, entwendet aus deren persönlichen Laufwerken, nicht von der TU-Personalverwaltung)	173
IR- und Fak-Rat Protokolle mit vertraulichem Teil (eine Fakultät)	98
Dokumente zu Promotionsverfahren (Zulassungen, Zeugnisse)	82
Dokumente mit Personalia (Anträge zur Verlängerung von Gastprofessuren etc.)	47
Dokumente zum Strahlenschutz (Personallisten, Fachkundebescheinigungen)	207
Übertragung selbst. Aufgaben in der Lehre (nicht vertraulich)	5
Mitschnitte aus Videokonferenzen (Mitschnitterlaubnisse waren vorhanden)	6
Fotos mit Personen (ein Fachbereich, u.a. Lehr-/Laborfotos)	70
20 Zip-Ordner (113 Dateien, teilweise Doubletten)	82
Insgesamt:	5.566

5. Betrafen die Ausfälle der TU auch andere Hochschulen, die gemeinsame IT-Dienste oder Software nutzen?

Zu 5.:
Im Rahmen gemeinsamer Forschungsvorhaben stellt die TUB IT-Dienste für andere Hochschulen im Bereich der Sync-and-Share-Dienste zur Verfügung. Diese wurden im Rahmen der Analyse des Vorfalls und der Gefahrenabwehr abgeschaltet. Außerdem betreut die TUB für andere Hochschulen bzw. Einrichtungen des Landes Berlin Dienstleistungen im Bereich Personalabrechnung, die ebenfalls betroffen gewesen seien.

6. Wie hoch ist in etwa der gesamte finanzielle Schaden, der durch den Angriff auf die IT-Systeme der TU entstanden ist?

Zu 6.:
Eine Gesamtsumme ist nach Angaben der TUB nicht feststellbar, da mögliche Folgekosten außerhalb der betroffenen zentralen Systeme nicht gesondert ermittelt oder verbucht wurden. Für die Wiederherstellung und die Umsetzung aktualisierter technischer und organisatorischer Sicherheitsstandards in den zentralen TU-

Systemen der Zentraleinrichtung Campusmanagement (ZECM) sind Kosten i.H.v. 445.552,21 Euro angefallen, darin sind die in Frage 7 dargelegten Kosten enthalten.

7. Welche finanziellen Mittel mussten für externe IT-Dienstleister*innen aufgewendet werden, um den Angriff zu analysieren, Sicherheitslücken zu schließen, den angerichteten Schaden zu beheben usw.?

Zu 7.:
In den in Frage 6 benannten Kosten sind 351.860,95 Euro für externe IT-Beratungen und Dienstleistungen enthalten, die für forensische Untersuchungen und die Konzeption des neuen Sicherheitskonzeptes sowie für die Unterstützung beim technischen Wiederaufbau der digitalen Verwaltungssysteme angefallen sind.

8. Wie viele Arbeitsstunden wurden circa von IT-Mitarbeiter*innen der TU aufgrund des Angriffs bis heute geleistet? Wie viele Überstunden wurden im Zuge des Angriffs und der Wiederherstellung der IT-Dienste bisher angewiesen?

Zu 8.:
Eine Gesamtzahl ist nach Angaben der TUB nicht ermittelbar. Als Beispiel wird angegeben, dass die Zentraleinrichtung Campusmanagement (ZECM) als zentraler Dienstleister der TUB (2021 ca. 85 Stellen) allein im arbeitsintensiven, auf den Angriff folgenden Monat Mai 2021 940 Überstunden beantragt und bewilligt bekommen habe. Für die dezentralen IT-Beschäftigten sei eine Überstundenzahl nicht ermittelbar (vgl. Antwort zu Frage 9).

9. Wie viele Arbeitsstunden mussten von anderen Mitarbeiter*innen der TU-Verwaltung schätzungsweise geleistet werden, um die ausgefallene IT der TU zu kompensieren? Wie viele Überstunden wurden angewiesen?

Zu 9.:
Nach Angaben der TUB sei weder eine Gesamtzahl der schadensbedingten Überstunden ermittelbar noch sei eine Schätzung möglich. Dies liege u.a. daran, dass auch bei den wegen des Schadens notwendigen oder aber nicht möglichen Arbeitszeiten eine Gleitzeitregelung galt. Gleitzeitguthaben und –abbau werden nur dezentral erfasst. Angeordnete Überstunden können nicht nach Sachgründen getrennt ermittelt werden. Aufgrund Personalmangels in mehreren zentralen und dezentralen Bereichen der TUB seien im gleichen Zeitraum auch Überstunden angefallen, die nicht mit dem IT-Schaden im Zusammenhang stehen.

10. Welchen Stand hat das polizeiliche Ermittlungsverfahren? Ist es abgeschlossen? Konnten Individuen identifiziert werden? Wo werden diese vermutet?

Zu 10.:
Die TUB hat angegeben, vom Landeskriminalamt (LKA) bislang noch keine Information erhalten zu haben, dass das Verfahren abgeschlossen oder eingestellt worden sei. Inhaltliche Informationen zu den Erkenntnissen aus dem Ermittlungsverfahren habe das LKA der TUB nicht zur Verfügung gestellt, dies sei auch nicht üblich.

11. Wird die Gruppe, die den Angriff ausgeführt hat, mit weiteren Angriffen auf andere Einrichtungen in Verbindung gebracht?

Zu 11.:
Nach Auskunft der TUB sei dies zu vermuten, soweit es sich aus dem Teil der Ermittlungen schließen lasse, an dem TU-Angehörige mitgewirkt haben.

12. Welche Maßnahmen wurden unternommen, um die IT der TU nach diesem Angriff besser abzusichern? Gibt es bspw. Änderungen in der Organisation und im Stellenplan?

Zu 12.:
Nach Auskunft der TUB wurden auf Basis der Erkenntnisse aus diesem Vorfall und aufgrund der entsprechenden Beratung erste Maßnahmen ergriffen: Die grundsätzliche Architektur der Systemverknüpfungen wurde sowohl bezüglich des Aufbaus als auch der Administration verändert. Das Monitoring der zentralen IT-Systeme inklusive Netzwerk wurde um weitere Aspekte ergänzt. Es wurden neue Handlungsanweisungen inklusive entsprechender Sicherheitsvorgaben für die Systemadministration konzipiert. Der Authentisierungsprozess wurde geändert, u.a. der Einsatz einer Zwei-Faktor-Authentisierung vorangetrieben.

Die beratende Fa. HiSolutions habe sich in ihren Empfehlungen für eine Verdoppelung der Stellenanzahl von Systemadministratoren für kritische Dienste ausgesprochen sowie für die Einrichtung von zwei weiteren Stellen für das Aufgabengebiet Intrusion Detection. Diese insgesamt fünf Stellen wurden von der TUB eingerichtet und stehen vor der öffentlichen Ausschreibung.

13. Konnte die Stelle des IT-Sicherheitsbeauftragten mittlerweile besetzt werden? Seit wann ist die Stelle des CIO (Chief Information Officer / IT-Leiter*in) unbesetzt und zu wann rechnet die TU mit einer Neubesetzung?

Zu 13.:
Die Stelle der bzw. des zentralen IT-Sicherheitsbeauftragten der TUB konnte nach Auskunft der TUB bislang noch nicht besetzt werden. Sie wurde mehrfach erfolglos ausgeschrieben und steht nun nach tariflicher Neubewertung kurz vor einer erneuten Ausschreibung mit einer verbesserten tariflichen Einstufung.

Die Stelle der bzw. des Chief Information Officers der TUB ist seit dem 19. Januar 2022 unbesetzt, werde aktuell neu ausgerichtet und solle zeitnah intern besetzt oder ausgeschrieben werden.

14. Wie stärkt der Berliner Senat die Sicherheit der IT-Infrastruktur der Berliner Hochschulen?

Zu 14.:
Die Regierungsparteien haben sich im Koalitionsvertrag darauf geeinigt, dass der Senat den Bereich IT-Sicherheit an Hochschulen durch die Besetzung von hauptamtlichen IT-Sicherheitsbeauftragten stärkt. Es wird ein unabhängiges Forum der Hochschul-IT-Sicherheitsbeauftragten eingerichtet, das eine gemeinsame Berichtspflicht an den Senat hat.

In der aktuellen Qualitäts- und Innovationsoffensive der Berliner Hochschulen ist eine Förderlinie für den Bereich Digitalisierung enthalten (Fördervolumen: 22 Mio. €), in deren Projekten die Frage der IT-Sicherheit ebenfalls immer eine Rolle spielt.

Berlin, den 10. Mai 2022

In Vertretung
Armaghan Naghipour
Senatsverwaltung für Wissenschaft,
Gesundheit, Pflege und Gleichstellung