Landtag von Baden-Württemberg **Drucksache 17 / 4278**
17. Wahlperiode **27.2.2023**

Kleine Anfrage

des Abg. Ansgar Mayr CDU

und

Antwort

des Ministeriums für Kultus, Jugend und Sport

Cyber-Angriffe auf Schulen

Kleine Anfrage

Ich frage die Landesregierung:

1. Welche Karlsruher Schulen waren am Wochenende vom 11./12. Februar 2023 von einem Hackerangriff betroffen?

2. Gab es im gleichen Zeitraum oder kurz davor bzw. danach ähnliche Cyberattacken auf andere Schulen in Baden-Württemberg?

3. Welche, vom Angriff betroffenen Systeme, haben die betroffenen Schulen benutzt und wie hoch ist der Verbreitungsgrad dieser Systeme an allen Schulen in Baden-Württemberg?

4. Welche Folgeschäden durch die Attacke sind für die Systeme sowie Datensätze bekannt und wurden durch den Angriff Daten abgezogen?

5. Welche Auswirkungen hatte der Hackerangriff auf den Schulbetrieb an den betroffenen Schulen, sowie an weiteren, nicht direkt betroffenen Schulen im Stadt- und Landkreis Karlsruhe?

6. Welche Erkenntnisse hat die Landesregierung über den Ursprung der Angriffe?

7. Wie unterstützt das Land Baden-Württemberg die Schulträger in diesem ganz konkreten Fall, um die Folgen der Cyberangriffe zu bewältigen und welche weiteren Lehren werden aus diesem Fall gezogen?

8. Wie ist der Stand bei der neuen digitalen Bildungsplattform für die Schulen in Baden-Württemberg?

16.2.2023

Mayr CDU

Eingegangen: 27.2.2023 / Ausgegeben: 31.3.2023

Begründung

Immer mehr Bereiche im Schulalltag werden in Baden-Württemberg digital abgewickelt, unter anderem auch sensible personenbezogene Daten. Hackerangriffe auf Schulen stören deshalb nicht nur den Unterrichtsablauf, sondern können auch erhebliche Schäden verursachen. Es ist nach Ansicht des Fragestellers davon auszugehen, dass Cyberangriffe auf öffentliche Einrichtungen u. a. auch Schulen in Zukunft zunehmen könnten. Deshalb ist es wichtig zu analysieren, welche Systeme besonders anfällig sind und wie sich das Land auf kommende Gefahrensituationen in Schulen vorbereiten kann.

Antwort

Mit Schreiben vom 24. März 2023 Nr. KMZ-0141.5-1/23/1 beantwortet das Ministerium für Kultus, Jugend und Sport im Einvernehmen mit dem Ministerium des Inneren, für Digitalisierung und Kommunen die Kleine Anfrage wie folgt:

Ich frage die Landesregierung:

1. Welche Karlsruher Schulen waren am Wochenende vom 11./12. Februar 2023 von einem Hackerangriff betroffen?

Es waren folgende Schulen betroffen:

- Erich-Kästner-Schule
- Grundschule Wolfartsweier
- Hardtschule
- Hebel Grundschule
- Marie-Luise-Kaschnitz-Schule
- Markgrafen Gymnasium
- Realschule am Rennbuckel (erfolgloser Versuch einer Attacke)
- Realschule Neureut
- Schule am Turmberg

2. Gab es im gleichen Zeitraum oder kurz davor bzw. danach ähnliche Cyberattacken auf andere Schulen in Baden-Württemberg?

Bei der Cybersicherheitsagentur Baden-Württemberg (CSBW) hat Anfang März eine weitere Schule einen Verdacht auf Schadsoftwarebefall auf einem System im Netzwerk der Schule gemeldet. Nach Untersuchung durch den IT-Dienstleister der Schule hat sich dieser Verdacht jedoch nicht bestätigt. Darüber hinaus liegen aktuell bei der CSBW keine weiteren Meldungen über ähnliche Cyberattacken auf Schulen vor. Beim Stadtmedienzentrum (SMZ) Karlsruhe und beim Landesmedienzentrum Baden-Württemberg liegen mit Stand 23. März 2023 ebenfalls keine weiteren Meldungen zu ähnlichen Cyberattacken auf andere Schulen in Baden-Württemberg vor.

3. Welche, vom Angriff betroffenen Systeme, haben die betroffenen Schulen benutzt und wie hoch ist der Verbreitungsgrad dieser Systeme an allen Schulen in Baden-Württemberg?

Bei den vom Angriff betroffenen Schulen wurden Daten in den Serversystemen und Speichersystemen des Schulverwaltungsnetzes und des pädagogischen Netzes verschlüsselt. Dabei fokussierte sich der Angriff auf eine Administrationskomponente, die auch an zahlreichen anderen Schulen in Baden-Württemberg zum Einsatz kommt.

4. Welche Folgeschäden durch die Attacke sind für die Systeme sowie Datensätze bekannt und wurden durch den Angriff Daten abgezogen?

Es bestanden und bestehen Backups der betroffenen Systeme, die nach gründlicher IT-forensischer Untersuchung auf neu beschaffte Hardware (Server) aufgespielt werden. Es kann davon ausgegangen werden, dass für die betroffenen Schulen keine Folgeschäden entstehen. Nach derzeitiger Sachlage gibt es somit keine Hinweise auf einen Datenabfluss und Datenverlust.

5. Welche Auswirkungen hatte der Hackerangriff auf den Schulbetrieb an den betroffenen Schulen, sowie an weiteren, nicht direkt betroffenen Schulen im Stadt- und Landkreis Karlsruhe?

Mit dem Bekanntwerden des Angriffs am 13. Februar 2023 wurden alle Server der Karlsruher Schulen vorsorglich heruntergefahren. Dies bedeutet, dass ab diesem Zeitpunkt keine IT-Dienste mehr verfügbar waren. Die Endgeräte des Verwaltungsnetzes sowie des pädagogischen Netzes waren ab diesem Zeitpunkt nicht mehr benutzbar. Da in der überwiegenden Anzahl auf den physikalischen Servern in den Schulen sowohl das pädagogische Netz als auch die Schulverwaltung bereitgestellt wird, waren mit Herunterfahren dieser Komponenten auch die genannten Netze nicht verfügbar. In enger Zusammenarbeit zwischen SMZ, Stadt und externen IT-Forensikern wurden beide Netze sorgfältig geprüft und sukzessive wieder in Betrieb genommen.

Aktuell stellt sich die Situation wie folgt dar:

- An allen Schulen, die nicht von der Attacke betroffen waren, sind die Server wieder in Betrieb und der Zustand vor der Attacke wurde wiederhergestellt.
- Für die kompromittierten Schulen wurden vorsorglich neue Server beschafft.
- Für alle betroffenen Schulen wurde neue Serverhardware bestellt. Aktuell wird auf die ausstehende Lieferung des letzten neu beschafften Servers gewartet, sodass auch die letzte verbleibende kompromittierte Schule wieder ans Netz gebracht werden kann. Dies sollte mit Abschluss der KW 13 erfolgt sein. An allen anderen betroffenen Schulen sind die neuen Server bereits in Betrieb.
- Somit sollten mit Abschluss der KW 13 alle Schulen wieder Zugang zum Verwaltungsnetz und zum pädagogischen Netz haben.

6. Welche Erkenntnisse hat die Landesregierung über den Ursprung der Angriffe?

Über den Ursprung der Angriffe können aktuell keine Aussagen getroffen werden. Die polizeilichen Ermittlungen hierzu dauern an und sind auch nach Wiederinbetriebnahme der Server der Schulen noch nicht abgeschlossen. Zum aktuellen Stand wird von einem automatisierten Angriff ausgegangen, hinter dem eine reale Lösegeldforderung steht.

7. Wie unterstützt das Land Baden-Württemberg die Schulträger in diesem ganz konkreten Fall, um die Folgen der Cyberangriffe zu bewältigen und welche weiteren Lehren werden aus diesem Fall gezogen?

Die CSBW nahm umgehend nach Bekanntwerden des Angriffs Kontakt zur Stadt auf und bot Hilfe an. Da bereits am ersten Tag des Angriffes ein internes Notfallteam aufgestellt war, konnte die Aufarbeitung des Angriffes ohne die CSBW erfolgen. Die Kriminalpolizei hat ebenfalls umgehend die Ermittlungen aufgenommen. Im Nachgang zur Cyberattacke vom 12. Februar 2023 werden das SMZ und die Stadt Karlsruhe mögliche Optimierungspotenziale (Netzwerkarchitektur, Administration) definieren und sukzessive umsetzen.

Die vom Warn- und Informationsdienst der CSBW erstellten Informationen zu Sicherheitslücken und die Handlungsempfehlungen sollen zeitnah auch allen Kommunen und damit einer Vielzahl von Schulträgern zur Verfügung gestellt werden.

8. Wie ist der Stand bei der neuen digitalen Bildungsplattform für die Schulen in Baden-Württemberg?

Zentrale Bausteine der Digitalen Bildungsplattform sind an den Schulen bereits erfolgreich im Einsatz. Die modulare Architektur hat sich bewährt. Öffentlichen Schulen im Geschäftsbereich des Kultusministeriums stehen die Lernmanagementsysteme itslearning und Moodle zur Verfügung und werden sehr gut angenommen. In beide ist ein Videokonferenzwerkzeug (Big Blue Button) und eine Officelösung (Collabora) eingebunden. Aktuell ist es allerdings nicht möglich, itslearning an allgemein bildenden Gymnasien anzubieten, da der Hauptpersonalrat der Gymnasien der Nutzung bisher nicht zugestimmt hat. Der sichere Messenger Threema ist bei über 52 000 Lehrkräften im Einsatz. Beim Digitalen Arbeitsplatz für Lehrkräfte (DAP) mit einheitlicher dienstlicher E-Mail arbeiten das Kultusministerium und die Landesoberbehörde IT Baden-Württemberg (BITBW) aus Datenschutzerwägungen intensiv an einer alternativen Lösung, die nicht auf dem Einsatz von Microsoft 365 beruht. Für den DAP wurde daher von November 2022 bis Februar 2023 erfolgreich ein Pilotprojekt mit mehreren hundert Lehrkräften durchgeführt. Basis dafür war die dPhoenix-Suite von Dataport AöR mit Open-Source Komponenten. Die im Piloten gewonnenen Erkenntnisse werden nun in das weitere Vorgehen einfließen.

Auch das Identitätsmanagementsystem (IdAM) mit seinem Dashboard als zentraler Einstieg in die Bildungsplattform zur Bündelung der Module und zur Rechteverwaltung aller Nutzenden wurde gemeinsam mit Schulen erfolgreich erprobt. Als nächstes steht die Umsetzung der schrittweisen Bereitstellung des IdAM an.

Mit der Digitalen Bildungsplattform sollen die Schulen und deren Lehrkräfte auch von administrativen, technischen und datenschutzrechtlichen Aufgaben entlastet werden.

Schopper

Ministerin für Kultus,
Jugend und Sport