



Die Ministerin

MHKBD Nordrhein-Westfalen | 40190 Düsseldorf

An den
Präsidenten des Landtags
Nordrhein-Westfalen
Herrn André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/1187

A20, A15

28. April 2023

für die Mitglieder des Ausschusses für
Bauen, Wohnen und Digitalisierung
des Landtags Nordrhein-Westfalen

**13. Sitzung des Ausschusses für Bauen, Wohnen und Digitalisierung
am Donnerstag, 27. April 2023**

hier: Übersendung des Sprechzettels zum TOP Fehlkonfigurierter Webservice
eines Drittanbieters im Zusammenhang mit Lightweight Directory Access Pro-
tocol (LDAP) Daten

Sehr geehrter Herr Landtagspräsident,

in der Anlage übersende ich Ihnen den Sprechzettel zum oben genannten Ta-
gesordnungspunkt mit der Bitte um Weiterleitung an die Mitglieder des ge-
nannten Ausschusses.

Mit freundlichem Gruß

Ina Scharrenbach MdL



Bericht der Landesregierung an den
Ausschuss für Bauen, Wohnen und Digitalisierung
des Landtags Nordrhein-Westfalen
für die Sitzung am 27. April 2023

Fehlkonfigurierter Webservice eines Drittanbieters im Zusammenhang mit Lightweight Directory Access Protocol (LDAP) Daten

Der Landesbetrieb IT.NRW betreibt seit 2005 das CERT NRW (Computer Emergency Response Team Nordrhein-Westfalen). Diese Einheit ist die landesweite Ansprechstelle für Vorfälle in der Informationssicherheit. Der Auftrag des CERT NRW umfasst insbesondere das Erkennen von Cyber-Bedrohungen und deren Abwehr sowie das Aufdecken und Abstellen von Schwachstellen. Dies bezieht sich auf den Schutz von Informationen in den IT-Systemen der Landesverwaltung Nordrhein-Westfalen.

Dem CERT NRW wurde am späten Abend des 18. April 2023 (dienstags) bekannt dass es eine Herausforderung beim Download der diesjährigen Abiturklausuren gebe. Die Zuständigkeit für die hieran beteiligten Server liegt im Auftrag des Ministeriums für Schule und Bildung des Landes Nordrhein-Westfalen bei der Qualitäts- und UnterstützungsAgentur - Landesinstitut für Schule (QUA-LiS). Eine unmittelbare Herausforderung für die IT innerhalb des Landesverwaltungsnetzes war nicht festzustellen.

Am Mittwoch, 19. April 2023, erfolgte durch das CERT NRW eine Recherche in öffentlich zugänglichen Quellen, bei der ein Eintrag von Dienstag, 18. April 2023 in einem sozialen Netzwerk auffiel. In diesem Beitrag wurde dargelegt, dass Abiturklausuren angeblich frei herunterladbar und entschlüsselbar seien. Bei dem in dem Beitrag genannten Server handelte es sich um einen Testdownload-Server, der physikalisch ohne Bezug zum Downloadsystem für das Zentralabitur von dem externen Auftragnehmer geführt wird. Insoweit wird auf den gestrigen Bericht des Ministeriums für Schule und Bildung des Landes Nordrhein-Westfalen im zuständigen Landtagsausschuss verwiesen.

In einem weiteren social media-Eintrag wurde darüber berichtet, dass Namen und E-Mail-Anschriften von Lehrerinnen und Lehrern über den Testdownload-Server herunterladbar seien. Nach Bewertung durch das CERT NRW entsprachen diese Daten sogenannten Funktionsträgerdaten, die in Regel öffentlich sind: Behörden und sonstige öffentliche Stellen sind juristische Personen, die erst über ihre Mitarbeiterinnen und Mitarbeiter handlungsfähig



sind. Bei der Erfüllung dienstlicher Aufgaben kommt es in verschiedenen Konstellationen zur Nennung von Namen und weiteren Daten der Beschäftigten (sogenannter Funktionsträgerdaten). Zu diesen Funktionsträgerdaten zählen in der Regel der Familienname, der Vorname, E-Mail-Anschriften, dienstliche Telefonnummern, Dienstadressen mit Zimmernummern und Organisationsbezeichnungen innerhalb der Verwaltungen, denen die Mitarbeitenden angehören.

Innerhalb des CERT NRW lag zu diesem Zeitpunkt (Mittwoch, 19. April 2023) der Schwerpunkt der Tätigkeit auf der vorgetragenen Behauptung, dass die Abiturklausuren kompromittiert seien: Bei der hiermit verbundenen Arbeit ging es darum, diese Behauptung zu erhärten oder zu widerlegen, um dem Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen eine Empfehlung zum weiteren Vorgehen geben zu können.

Am Mittwoch, 19. April 2023, informierte das CERT Bund um 15.06 Uhr per Anruf an die Hotline des CERT NRW über Datensätze von Lehrerinnen und Lehrern, die vom Testdownload-Server herunterladbar seien. Der Operator des CERT NRW bat - der Dienstanweisung folgend - das CERT Bund um Übermittlung einer E-Mail mit der Verschriftlichung des telefonisch avisierten Sachverhaltes. Diese E-Mail traf am Mittwoch, 19. April 2023, um 15.36 Uhr im CERT NRW ein.

Am Donnerstag, 20. April 2023, wurde die E-Mail des CERT Bund um 10.33 Uhr an das zuständige Funktionspostfach im Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen versandt.

Nach Einschätzung des BSI handelte es sich um ein „moving target grade“, welcher nur für eine begrenzte Zeit ausnutzbar war. Ein Zugriff auf Personendaten konnte durch das BSI nicht bestätigt werden. Ein Versuch die Daten durch das CERT NRW abzurufen war ebenfalls nicht möglich. Das BSI schlussfolgert daraus, dass die Sicherheitslücke nur temporär bestanden hat und mittlerweile geschlossen wurde.

Nach - noch nicht abgeschlossener - Aufklärung durch das Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen handelt es sich bei dem aufgetretenen Vorfall um eine Lücke in der Konfiguration der Benutzerverwaltung durch den externen Auftragnehmer.