



# HESSISCHER LANDTAG

24. 06. 2024

## Kleine Anfrage

**Oliver Stirböck (Freie Demokraten) vom 26.03.2024****Sicherheitslücken in der Microsoft-Kommunikationsplattform Exchange****und****Antwort****Ministerin für Digitalisierung und Innovation**

### Vorbemerkung Fragesteller:

Laut Mitteilung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vom 26.03.2024 gibt es erhebliche Sicherheitslücken in der Microsoft-Kommunikationsplattform Exchange. Die Server-Software verwaltet E-Mails, Termine, Kontakte und Aufgaben. Mindestens 17.000 Versionen von Microsoft-Exchange-Servern in Deutschland seien von kritischen Schwachstellen betroffen. Die Dunkelziffer sei noch deutlich größer. Neben Cyberkriminellen seien staatliche Akteure als Angreifer zu vermuten, die dadurch Schadsoftware verbreiten. Betroffen seien insbesondere Schulen und Hochschulen, Kliniken, Arztpraxen, Pflegedienste und andere medizinische Einrichtungen und Kommunalverwaltungen.

### Vorbemerkung Ministerin für Digitalisierung und Innovation:

Im Rahmen ihrer Funktion als zentraler IT-Dienstleister betreibt die Hessische Zentrale für Datenverarbeitung (HZD) für die Ressorts und Dienststellen der hessischen Landesverwaltung vier voneinander abgegrenzte Microsoft-Exchange-Server-Umgebungen. Die Antworten beziehen sich nur auf die Microsoft-Exchange-Umgebungen, die von der HZD betrieben werden.

In Anbetracht der Notwendigkeit, die Integrität und Sicherheit der Infrastrukturen zu wahren, ist es gemäß den geltenden Sicherheitsrichtlinien untersagt, spezifische Informationen bezüglich der betroffenen Infrastrukturen sowie der diese nutzenden Ressorts öffentlich zu machen.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister des Innern, für Sicherheit und Heimatschutz wie folgt:

Frage 1 Wie viele Microsoft-Exchange-Server in Hessen sind von den identifizierten Sicherheitslücken betroffen, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgestellt hat?

Die Microsoft-Exchange-Server-Umgebungen bei der HZD sind nicht direkt über das Internet zugänglich. Demzufolge fallen sie nicht unter die direkt betroffenen Systeme im Kontext der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) berichteten Sicherheitslücken.

Frage 2 Welche konkreten Auswirkungen haben die Sicherheitslücken in der Microsoft-Kommunikationsplattform Exchange auf die IT-Systeme und Daten von Organisationen und Behörden in Hessen?

Frage 4 Welche Maßnahmen wurden bereits ergriffen, um die betroffenen Microsoft-Exchange-Server in Hessen zu schützen und potenzielle Angriffe abzuwehren?

Die Fragen 2 und 4 werden im Sachzusammenhang gemeinsam beantwortet.

Für die Microsoft-Exchange-Server-Umgebungen der Landesverwaltung, für die die HZD verantwortlich ist, besteht gemäß der aktuellen Sicherheitseinschätzung keine unmittelbare Möglichkeit für direkte Angriffe über die vom BSI gemeldeten Sicherheitslücken. Bei diesen wurden weitere Schutzmaßnahmen (z. B. Zugriff über VPN) bereits in der Planungsphase berücksichtigt und umgesetzt. Diese Schutzmaßnahmen minimieren die Angriffsfläche auf die IT-Systeme der hessischen Landesverwaltung erheblich, so dass auch schwere Sicherheitslücken nicht unmittelbar zu einer Gefährdung der Daten führen.

Frage 3 Welche Branchen und Einrichtungen in Hessen sind besonders stark von den Sicherheitslücken betroffen?

Hinsichtlich spezifischer Informationen zu betroffenen Systemen außerhalb ihres Zuständigkeitsbereiches verfügt die HZD über keine Kenntnisse.

Frage 5 Welche Maßnahmen wurden bereits ergriffen, um die betroffenen Microsoft-Exchange-Server in Hessen zu schützen und potenzielle Angriffe abzuwehren?

Das Hessen CyberCompetenceCenter (Hessen3C) arbeitet eng mit Polizei und Verfassungsschutz zusammen. Es unterstützt neben der Landesverwaltung und Kommunen auch kleine und mittlere Unternehmen (KMU) sowie Betreiber von Kritischen Infrastrukturen bei der Erkennung, Untersuchung und Abwehr von Cyber-Bedrohungen.

Zu den von dem Fragesteller angesprochenen Sicherheitslücken in der Microsoft-Kommunikationsplattform Exchange wurden Warnmeldungen mit konkreten Informationen hinsichtlich Prüfung auf Betroffenheit und Maßnahmenempfehlungen zum Schließen der Sicherheitslücken an registrierte Empfänger versandt. Die Nutzung des Warnmeldedienstes steht allen interessierten Behörden offen und kann über die Hessen3C-Website abonniert werden. Die konkreten Schwachstellen können durch das Einspielen der aktuellsten Software-Versionen (Sicherheitsaktualisierungen) geschlossen werden. Dies ist eine Regelaufgabe der örtlich zuständigen IT-Administration.

Frage 6 Wie unterstützt die Landesregierung Schulen, Hochschulen, Kliniken, Arztpraxen, Pflegedienste konkret bei der Behebung der Sicherheitslücken?

Bei konkreten Sicherheitsvorfällen können sich Schulen, Hochschulen, Kliniken, Arztpraxen und Pflegedienste über eine 24/7-besetzte Notfallrufnummer direkt an das dem Hessen3C zugehörige CERT-Hessen wenden. Dieses berät zur Erkennung und Analyse von Sicherheitsvorfällen sowie zum IT-Krisenmanagement. Bei Bedarf kann ein Mobile Incident Response Team (MIRT) vor Ort bei der Vorfallsbearbeitung und beim Krisenmanagement unterstützen.

Frage 7 In welcher Weise sind die hessischen Ministerien unmittelbar betroffen?

Für die Ministerien des Landes Hessen, deren elektronische Postfächer innerhalb der von der HZD verwalteten Exchange-Server-Umgebungen angesiedelt sind, ergibt sich keine direkte Betroffenheit durch die aktuell diskutierten Sicherheitsrisiken.

Wiesbaden, 15. Juni 2024

**Prof. Dr. Kristina Sinemus**