



HESSISCHER LANDTAG

31. 07. 2024

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 27.05.2024

Cyberangriff auf HöMS

und

Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Im Februar 2024 ereignete sich ein Cyberangriff auf die Hessische Hochschule für öffentliches Management und Sicherheit (HöMS), bei dem sensible Daten von Studierenden und Beschäftigten entwendet wurden. Betroffen sind u. a. Namen, Wohnanschriften, E-Mail-Adressen, Bankdaten und Gesundheitsinformationen. Der Angriff, eine Ransomware-Attacke, führte zur Verschlüsselung der Daten und einer Lösegeldforderung. Die Hochschule hat betroffene Systeme abgeschaltet, ein Servicepostfach und eine Hotline für Betroffene eingerichtet und Strafanzeige erstattet. Die Ermittlungen dauern an.

Diese Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

- Frage 1 Welche konkreten IT-Sicherheitsmaßnahmen waren vor dem Angriff an der HöMS implementiert und warum waren diese Maßnahmen nicht ausreichend, um den Cyberangriff zu verhindern?
- Frage 5 Welche spezifischen Schwachstellen im IT-System der HöMS wurden durch den Cyberangriff ausgenutzt?
- Frage 9 Welche langfristigen Auswirkungen erwartet die Landesregierung durch diesen Cyberangriff auf den Hochschulbetrieb?

Die Fragen 1, 5 und 9 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Im ehemaligen Netz der Hessischen Hochschule für Polizei und Verwaltung (HfPV) wurden einzelne Servicedienstleistungen betrieben, die noch nicht in das Hessennetz (itshessen) überführt werden konnten. Zum Schutz des Netzes war der Virens Scanner „McAfee/Trellix“ installiert; die Aktualisierung erfolgte mittels McAfee-EPO-Server automatisiert. Das Eindringen der Ransomware wurde von diesem Virens Scanner nicht erkannt. Die Firewall „Cisco asa“ wurde von der Ransomware umgangen, da diese vermutlich über eine Phishing-Mail in das Netz eindringen konnte.

Zum Zeitpunkt des Cyberangriffs war die Migration des alten Netzes auf das itshessen-Netz der Hochschule für öffentliches Management und Sicherheit (HöMS) bis auf die erwähnten Servicedienstleistungen bereits abgeschlossen, sodass mit langfristigen Auswirkungen auf den Hochschulbetrieb der HöMS nicht gerechnet wird.

- Frage 2 Welche sofortigen Maßnahmen wurden ergriffen, um den Schaden zu begrenzen und die betroffenen Systeme zu sichern?

Im Einklang mit den Empfehlungen des BSI wurde das betroffene Netz unmittelbar nach Bekanntwerden des Angriffs vom Internet getrennt und abgeschaltet. Das Innenministerium, einschließlich Hessen3C, der Ressort-Informationssicherheitsbeauftragte, die HZD und das Hessische Landeskriminalamt (HLKA) wurden informiert und die Nutzung von Datenträgern im HöMS- und im Polizeinetz der HöMS technisch unterbunden. Die Endgeräte des Netzes wurden außer Betrieb genommen bzw. deren Nutzung untersagt. Betroffene Hardware wurde mit BSI-zertifizierter Löschsoftware gelöscht.

Frage 3 Warum wurden die betroffenen Studierenden, Beschäftigten und Geschäftspartner erst verspätet über den Datenleak informiert?

Die Beschäftigten der HöMS wurden am Tag nach Bekanntwerden, am 13.02.2024, zunächst per E-Mail über den Ransomware-Angriff und die Abschaltung des HfPV-Netzes informiert sowie am 14.02.2024 über den Umgang mit E-Mails oder Anhängen aus dem ehemaligen HfPV-Netz sensibilisiert. Als verlässliche Informationen über Umfang und Wahrscheinlichkeit eines möglichen Datenabflusses vorlagen, wurde der betroffene Personenkreis nach den Vorgaben der Datenschutzgrundverordnung informiert.

Frage 4 Wie viele Personen waren insgesamt von dem Angriff betroffen?

Da die Dateien bei dem Cyberangriff zum Teil verschlüsselt worden sind, kann die Frage nicht abschließend beantwortet werden. Es ist davon auszugehen, dass es sich insbesondere um Daten von ehemaligen Studierenden, von Beschäftigten, Lehrbeauftragten und weiteren Betroffenen der ehemaligen HfPV aus den Fachbereichen Polizei und Verwaltung handelt.

Frage 6 Welche Maßnahmen plant die Landesregierung konkret, um ähnliche Cyberangriffe in Zukunft zu verhindern?

Die forensische Analyse und Nachbereitung des Vorfalls dauern an. Erst nach deren Abschluss kann eine konkrete Bewertung einschließlich etwaig notwendiger Anpassungen der IT-Sicherheitsmaßnahmen vorgenommen werden.

Frage 7 Wie genau gestaltet sich die Zusammenarbeit der HöMS mit den Sicherheitsbehörden, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik (BSI), im Rahmen der Ermittlungen?

Die HöMS steht mit den Sicherheitsbehörden in einem regelmäßigen Austausch. Insbesondere wurde nach dem Cyberangriff u. a. das Innenministerium, einschließlich Hessen3C und der Ressort-Informationssicherheitsbeauftragte informiert. Durch Hessen3C wurde die Zentrale Ansprechstelle Cybercrime (ZAC) des HLKA in Kenntnis gesetzt. Bei der Analyse der Schadsoftware stand das Hessen3C über das CERT-Hessen im Rahmen des VerwaltungsCertVerbundes auch mit dem BSI in Kontakt.

Frage 8 Welche Richtlinien bestehen im Umgang mit Lösegeldforderungen seitens der Landesregierung?

Die Regelungen des Landes zum Umgang mit Lösegeldforderungen sind nach der Verschlusssachenanweisung eingestuft. Es entspricht allerdings den Empfehlungen des BSI und des Bundeskriminalamtes, Lösegeldforderungen nicht nachzukommen.

Frage 10 Welche spezifischen Unterstützungsmöglichkeiten bietet die Landesregierung den Betroffenen des Datenlecks an, insbesondere in Bezug auf mögliche Identitätsdiebstähle und andere Datenschutzverletzungen?

Hessen3C beobachtet das Darknet hinsichtlich veröffentlichter Daten mit Bezug zur HöMS. Sollten diesbezüglich Informationen detektiert werden, werden die zuständigen Stellen informiert.

Wiesbaden, 18. Juli 2024

Prof. Dr. Roman Poseck