Bayerischer Landtag

18. Wahlperiode 03.08.2020 Drucksache 18/8840

Schriftliche Anfrage

der Abgeordneten **Ludwig Hartmann, Katharina Schulze, Benjamin Adjei**
BÜNDNIS 90/DIE GRÜNEN
vom 13.03.2020

Sicherheit der Videokonferenzsysteme der Staatsministerien

Das Staatsministerium des Innern, für Sport und Integration hat kürzlich offenbar nicht für die Öffentlichkeit bestimmte Videokonferenzen durchgeführt, die von außen bei Kenntnis der URL der genutzten virtuellen Konferenzräume frei zugänglich waren (vgl. https://www.heise.de/ct/artikel/c-t-deckt-auf-Bayerischer-Innenminister-bespricht-Corona-Krise-in-ungeschuetzter-Videokonferenz-4680288.html).

Ich frage die Staatsregierung:

Hinweis des Landtagsamts: Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

Antwort

des Staatsministeriums der Finanzen und für Heimat
vom 29.06.2020

1. a) Wie lange wurden vom Staatsministerium des Innern, für Sport und Integration (StMI) oder einem anderen Staatsministerium Videokonferenzen ohne Sicherheitsvorkehrungen (Teilnahme nur per VPN, Passwortschutz etc.) durchgeführt (bitte genauen Zeitraum angeben)?

Videokonferenzen über dieses System wurden im Staatsministerium für Gesundheit und Pflege (StMGP) seit Januar 2018 ohne Zwischenfall geführt.

Es handelt sich dabei nicht um eine Sicherheitslücke des Systems. Voraussetzung für eine Teilnahme an einer Videokonferenz ist die Kenntnis des benutzten virtuellen Konferenzraums. Im angesprochenen Fall wurde nach Einschätzung des Informationssicherheitsbeauftragten (ISB) des StMGP diese Information unbefugt nach außen gegeben. Für einen solchen Fall helfen auch PIN-Schutz usw. nicht weiter (PIN kann weitergegeben werden – nötig zur Teilnahme an einer Konferenz). Die Sicherheit der Verbindung zur zentralen Videokonferenz ist durch TLS-Verschlüsselung sichergestellt. Niemand kann unerkannt an einer Besprechung teilnehmen. Es ertönt immer ein Tonsignal und es erscheint zusätzlich ein Symbol- oder Videobild.

b) Welche in diesem Zeitraum abgehaltenen Videokonferenzen wurden wie im Bericht beschrieben ohne Sicherheitsvorkehrungen durchgeführt (bitte einzeln angeben, sofern möglich unter Angabe der Teilnehmenden)?

Alle Konferenzen, die vom StMGP über einen virtuellen Konferenzraum abgehalten wurden. Dabei wurden oben genannte Vorkehrungen getroffen. Aufzeichnungen über die Teilnehmer werden nicht geführt.

2. a) Seit wann genau nutzen das Staatsministerium für Gesundheit und Pflege, bzw. das Staatsministerium des Innern, für Sport und Integration das im Vorspruch genannte Videokonferenzsystem (bitte konkreten Zeitpunkt angeben)?

Siehe Antwort zu Frage 1 a.

b) Warum wurde der Schutz durch ein Passwort bzw. eine PIN erst im Nachgang dieses Falles aktiviert?

Aus Sicht des StMGP wurden die Sicherheitsmaßnahmen (nicht sprechender Name für den Videokonferenzraum, Verschlüsselung, Ton- und Bild-Signal bei Einwahl) grundsätzlich als ausreichend angesehen.

c) Welche weiteren Sicherheitsvorkehrungen traf die Staatsregierung nach Bekanntwerden der frei zugänglichen Videokonferenz?

Das IT-Dienstleistungszentrum (IT-DLZ) hat zusätzlich zu den bereits vorhandenen Sicherheitsmaßnahmen (Application Level Gateway, Intrusion Detection, optionaler PIN-Schutz) weitere Maßnahmen ergriffen: Der Zugang zum Videokonferenzsystem per Jabber Guest aus dem Internet wurde vorübergehend geblockt und alle Behörden wurden gebeten, zu prüfen, ob weitere Videoräume mit einer PIN geschützt werden sollen.

Das StMGP gibt PINs nur telefonisch an die geplanten Teilnehmer bis 15 min vor Konferenzbeginn weiter.

3. a) Kann die Staatsregierung ausschließen, dass sicherheitsrelevante interne Informationen durch die Lücke von Unberechtigten abgegriffen werden konnten?

Es sind keine derartigen Fälle bekannt.

b) Welche (regelmäßigen) Besprechungen, Meetings etc. wurden bzw. werden seitens der Staatsregierung grundsätzlich per Videokonferenz durchgeführt (bitte einzeln und möglichst genau aufführen)?

Videokonferenzen werden von der Staatskanzlei (StK) und den einzelnen Staatsministerien situativ und in unterschiedlicher Intensität genutzt. Es erfolgt keine zentrale Erfassung der Videokonferenzen in den Ressorts.

4. a) Welche weiteren Staatsministerien nutzen das im Bericht genannte Videokonferenzsystem?

Die StK und folgende Staatsministerien nutzen das Videokonferenzsystem: StMI, Staatsministerium für Unterricht und Kultus (StMUK), Staatsministerium der Finanzen und für Heimat (StMFH), Staatsministerium der Justiz (StMJ), Staatsministerium für Umwelt und Verbraucherschutz (StMUV), Staatsministerium für Wissenschaft und Kunst (StMWK), Staatsministerium für Ernährung, Landwirtschaft und Forsten (StMELF), Staatsministerium für Familie, Arbeit und Soziales (StMAS), Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi), StMGP, Staatsministerium für Digitales (StMD), Staatsministerium für Wohnen, Bau und Verkehr (StMB).

b) Wurden auch in diesen Staatsministerien ohne Sicherheitsvorkehrungen (Teilnahme nur per VPN, Passwortschutz etc.) Videokonferenzen durchgeführt?

Nach Angaben der Staatsministerien wurden Videokonferenzen ohne zusätzliche PIN-Absicherung überwiegend nur in Einzelfällen genutzt.

c) Wenn ja, jeweils seit wann?

Erste Videokonferenzen wurden im Jahr 2013 pilotiert. Die Einführung in den Ressorts erfolgte anschließend sukzessive bis zum Jahr 2018.

5. a) Werden über das im Vorspruch genannte System hinaus von den Staatsministerien weitere Systeme für Videokonferenzen eingesetzt?

Es werden innerhalb des vom Landesamt für Sicherheit in der Informationstechnik (LSI) geschützten Behördennetzes zudem Systeme wie Skype for Business der Firma Microsoft und Webex der Firma Cisco genutzt. Weiterhin werden externe Systeme genutzt, insbesondere wenn die Videokonferenz von externen Teilnehmern organisiert wird. Freischaltungen für externe Systeme müssen nach dem Minimalprinzip (so restriktiv wie möglich) erteilt werden. Die IT-Sicherheit wird vom LSI überwacht.

b) Inwiefern wurden bei der Auswahl der eingesetzten Video- und Telefonsysteme mögliche Sicherheitslücken geprüft?

Bei der Auswahl der Produkte wurde darauf geachtet, dass die Hersteller Prozesse zur Behandlung von Sicherheitslücken etabliert haben. Dazu zählen das Feststellen von etwaigen Sicherheitslücken sowie das Entwickeln und Bereitstellen von Patches zur Behebung der Sicherheitslücken.

Skype for Business ist nur innerhalb des geschlossenen und abgesicherten bayerischen Behördennetzes nutzbar. Bei der Auswahl wurde u. a. auch auf die Zertifizierung nach ISO 27001, BSI-Standard C5, Skyhigh CloudTrust, SSAe-16 geachtet.

c) Wird das im Bericht genannte Konferenzsystem auch für kritische und sicherheitsrelevante Kommunikation der Staatsministerien genutzt?

Das zentrale System wird im Umfang der normalen Dienstgeschäfte eingesetzt.

6. a) Können die betroffenen Staatsministerien im Nachgang ermitteln, wer unberechtigt an den ungesichert durchgeführten Videokonferenzen teilgenommen hat?

Eine nachträgliche Ermittlung kann im Bedarfsfall zeitnah mithilfe von Logdateien erfolgen.

b) Wer ist für die Videokonferenzsysteme der Staatsministerien verantwortlich (insbesondere im Hinblick auf die notwendige Sicherheit der Systeme)?

Die Verantwortung für Endgeräte und deren individuelle Einstellungen, wie z. B. das Beauftragen der Einrichtung einer PIN-Abfrage liegen bei den Staatsministerien (Clientmanagement und das Wissen über den Nutzungszweck liegen dort).

In wenigen Einzelfällen wurde das IT-DLZ mit dem Patch-Management beauftragt. Die Teilkomponente der zentralen Videokonferenzplattform wird vom IT-DLZ betreut.

Dezentrale Videokonferenzplattformen liegen in der Verantwortung der jeweiligen Ressorts.

7. a) Führt die Staatsregierung regelmäßig IT-Sicherheitsaudits in den Ministerialverwaltungen durch?

In den Staatsministerien wurden bereits IT-Sicherheitsaudits durchgeführt und ein bayernweites Information Security Management System befindet sich derzeit im Aufbau.

Seitens des IT-DLZ werden jährlich Audits nach ISO 27001 auf Basis IT-Grundschutz durchgeführt.

b) Falls ja, wann hat zuletzt ein Sicherheitsaudit stattgefunden?

Die letzten Audits fanden im März 2020 und am 26.Juni 2019 statt.

c) Warum ist die Sicherheitslücke bezüglich Videokonferenzen dabei nicht aufgefallen?

Es handelt sich dabei nicht um eine Sicherheitslücke. Virtuelle Videokonferenzräume können, wenn notwendig, ohne PIN-Schutz eingerichtet werden. Dieses Vorgehen wird z. B. gewählt, wenn der Wunsch besteht, Videokonferenzen für öffentliche Veranstaltungen zu nutzen. Solche und ähnliche Anforderungen bestehen auch weiterhin, sodass nach wie vor einige wenige Räume ohne PIN-Schutz, z. B. für Pressekonferenzen, vorhanden sind.

8. a) Welches System nutzen die Staatsministerien für Telefonkonferenzen?

Telefonanlagen liegen in der Verantwortung der jeweiligen Staatsministerien. Daher sind verschiedene Anlagen verschiedener Hersteller im Einsatz, z. B. von CISCO, Unify, Alcatel oder Vodafone.

b) Welche Sicherheitsvorkehrungen gibt es für die Telefonkonferenzen der Staatsministerien?

Aufgrund der Vielfalt an Anlagen gibt es u. a. folgende Sicherheitsvorkehrungen: Akustisches Signal beim Einklinken eines neuen Gesprächsteilnehmers und PIN-Schutz.

c) Gab es bei Telefonkonferenzen in der Vergangenheit ähnliche Sicherheitslücken wie im Falle der im Bericht genannten Videokonferenz der Staatsregierung?

Es sind keine Vorfälle bekannt.