Bayerischer Landtag

18. Wahlperiode 04.12.2020 Drucksache 18/10302

Schriftliche Anfrage

des Abgeordneten **Benjamin Adjei BÜNDNIS 90/DIE GRÜNEN**
vom 29.07.2020

Sicherheit der Videokonferenzsystemen der Staatsministerien – Erneute Nachfrage

Am 11.03.2020 berichtete Heise online in einem Artikel darüber, wie es Journalistinnen bzw. Journalisten mit einfachsten Mitteln möglich war, unbemerkt an einer nichtöffentlichen Sitzung des Staatsministeriums des Innern, für Sport und Integration (StMI) teilzunehmen (https://www.heise.de/ct/artikel/c-t-deckt-auf-Bayerischer-Innenminister-bespricht-Corona-Krise-in-ungeschuetzter-Videokonferenz-4680288.html). Diese Anfrage bezieht sich auf die Antwort der Staatsregierung zu einer früheren Anfrage zum Thema „Sicherheit der Videokonferenzsysteme der Staatsministerien" vom 13.03.2020 (Drucksache 18/8840).

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 nach Beteiligung des Staatsministeriums für Gesundheit und Pflege und des Staatsministeriums des Innern, für Sport und Integration
vom 07.10.2020

1.1 Wie kommt der Informationssicherheitsbeauftragte des Staatsministeriums für Gesundheit und Pflege (StMGP) zu der Einschätzung, dass Informationen über den verwendeten virtuellen Konferenzraum „unbefugt nach außen gegeben“ wurden, obwohl im Bericht von Heise steht, dass durch einfaches „try-and-error“ die entsprechende URL ermittelt wurde?

Um die Adresse des virtuellen Konferenzraumes manuell in akzeptabler Zeit zu erraten, bedarf es nach Experteneinschätzung Insiderinformationen wie den Aufbau der Adressen und des verwendeten Systems, welche anscheinend vorlagen. Eine automatisierte Ermittlung ohne Vorkenntnisse mittels „brute forceW wäre nach fachlicher Einschätzung z. B. durch Performance-Einbußen des Systems wegen der erhöhten Zugriffszahlen aufgefallen und hätte ebenfalls sehr lange Zeit in Anspruch genommen und erheblichen Aufwand für Heise verursacht.

1.2 Wie kommt die Staatsregierung zu der Einschätzung, dass im entsprechenden Fall die Verwendung eines PIN-Schutzes die unautorisierte Teilnahme nicht verhindert hätte?

Wie dargestellt, gehen die Fachexperten davon aus, dass Heise Insiderinformationen wie die Raumadresse bewusst zugeleitet wurden. Es erscheint naheliegend, dass dabei eine PIN ebenfalls weitergereicht worden sein könnte.

2.1 Wie erklärt die Staatsregierung den Widerspruch in ihrer Antwort, dass zwar einerseits ein PIN-Schutz in dem konkreten Fall nichts genützt hätte (Antwort zu Frage 1 a), aber dennoch als eine der ersten Maßnahmen geprüft wurde, welche Räume mit einer PIN geschützt werden sollen (Antwort zu Frage 2 c)?

Grundsätzlich stellt eine PIN einen verbesserten Schutz bei versehentlichem Bekanntwerden der Adresse dar.

Da im konkreten Fall der Verdacht einer bewussten Weitergabe vorlag, hätte in diesem konkreten Fall ein PIN-Schutz keine Wirkung gehabt, weil auch die PIN weitergereicht werden kann.

2.2 Wie erklärt die Staatsregierung, dass im konkreten Fall keine PIN verwendet wurde, obwohl nur in Einzelfällen keine PIN genutzt wird (Antwort zu Frage 4 b) und auf die Verwendung einer PIN nur verzichtet wird, wenn explizit gewünscht ist, dass externe Personen an der Sitzung teilnehmen können (Antwort zu Frage 7 c)?

Siehe Antwort zu Frage 2 b der ersten Anfrage: „Aus Sicht des StMGP wurden die Sicherheitsmaßnahmen (nicht sprechender Name für den ViKo-Raum, Verschlüsselung, Ton- und Bild-Signal bei Einwahl) grundsätzlich als ausreichend angesehen."

2.3 Muss davon ausgegangen werden, dass es vom Staatsministerium des Innern, für Sport und Integration gewollt war, dass externe Personen an der Videokonferenz teilnehmen?

Nach Mitteilung vom StMI und StMGP befindet sich die Diakonie, von wo aus der Staatsminister des Innern, für Sport und Integration Joachim Herrmann teilgenommen hat, nicht im bayerischen Behördennetz und wird daher als extern eingestuft, die Teilnahme von unbefugten Dritten war zu keinem Zeitpunkt intendiert.

3.1 Wie erklärt die Staatsregierung, dass es der c't-Redaktion möglich war, mehrere Minuten unbemerkt an der Sitzung teilzunehmen, obwohl laut Antwort der Staatsregierung „niemand […] unerkannt an einer Sitzung teilnehmen" kann (Antwort zu Frage 1 a)?

Wie das von Heise aus der eigenen Perspektive veröffentlichte Bild zum einen zeigt, waren alle nicht aktiven Teilnehmer am unteren Bildschirmrand zu sehen. Nach Mitteilung des StMGP kann insoweit dahingestellt bleiben, was unter einer mehrminütigen unbemerkten Teilnahme konkret zu verstehen ist. Zum anderen ist in Erinnerung zu rufen, dass die Lage zum Besprechungszeitpunkt aufgrund der sich zuspitzenden Pandemie dramatisch war. Die Entfernung der meisten der ca. 40 Teilnehmer vom Bildschirm war so groß, dass Einzelheiten bei den nicht aktiven Teilnehmern nicht erkannt werden konnten. Daher geht die Staatsregierung davon aus, dass die Aufmerksamkeit der Besprechungsteilnehmer vollständig von dem seinerzeit extrem beunruhigenden Infektionsgeschehen in Anspruch genommen war. In dieser ernsten Situation dürften die Besprechungsteilnehmer nicht mit vorsätzlich unberechtigten Teilnehmern gerechnet haben.

3.2 Wie erklärt die Staatsregierung, dass die c't-Redaktion trotz „ertöntem Tonsignal und angezeigtem Symbol- bzw. Videobild" (Antwort zu Frage 1 a) nicht sofort aus der Videokonferenz entfernt wurde?

Siehe Antwort zu Frage 3.1.

3.3 Wie erklärt sich die Staatsregierung, dass es der c't-Redaktion möglich war, den Zugang zum Videokonferenzraum zu finden, obwohl laut Antwort der Staatsregierung für die Teilnahme ein „nicht sprechender Name für den ViKo-Raum" benötigt wird (Antwort zu Frage 2 b)?

Siehe Antwort zu Frage 1.1.

4.1 In wie vielen Fällen wurde bisher mithilfe von Logdateien eine nachträgliche Ermittlung von unautorisierten Teilnehmerinnen bzw. Teilnehmern ermittelt?

Bislang wurde von keinem Besprechungsorganisator ein entsprechender Antrag im Rechenzentrum gestellt, daher wurden bisher auch keine Ermittlungen durchgeführt. Für den Fall, dass ein derartiger Antrag gestellt wird, hat das IT-Dienstleistungszentrum (IT-DLZ) einen festen Prozess unter Beteiligung des Datenschutzbeauftragten des IT-DLZ mit den Strafverfolgungsbehörden vereinbart.

4.2 Weshalb wurde jeweils im konkreten Fall von der Möglichkeit der nachträglichen Ermittlung mithilfe von Logdateien Gebrauch gemacht?

Entfällt.

4.3 Wird eine stichprobenartige Untersuchung der Logdateien durchgeführt, um sicherzustellen, dass keine unautorisierte Teilnahme an einer Videokonferenz erfolgt ist?

Der Aufwand anlassloser Stichproben stünde in keinem Verhältnis zum Nutzen, zudem sind die dafür benötigten Daten ihrer Natur nach personenbezogen und unterliegen daher dem Datenschutz. Eine anlasslose Ermittlung dieser Daten wäre unangemessen.