KASTEL

KASTEL erklärt

03 | 2024

Die Taurus-Abhöraffaire

Vergangene Woche veröffentlichte Russland einen 40-minütigen Mitschnitt einer Webex-Konferenz hochrangiger deutscher Offiziere, die mögliche Einsatzszenarien für Taurus-Marschflugkörper diskutierten. Die Abhöraffäre hat zu heftigen Debatten geführt. Experten der **KASTEL Security Research Labs** geben eine Einschätzung zu aktuellen sicherheitsrelevanten Fragen.

Derzeit wird über einen Anwendungsfehler eines der der Beteiligten spekuliert, der das Abhören ermöglichte. Ist das plausibel?

Es gibt keine detaillierten Informationen über die tatsächlich ausgenutzte Schwachstelle. Da laut Aussage der Bundeswehr ein intern betriebenes Webex-Konferenzsystem von Cisco eingesetzt wurde, ist nicht unbedingt eine Schwachstelle seitens externer Betreiber zu vermuten. Auch die Erklärung, dass ein Teilnehmer aus einem ungeschützten Hotelnetzwerk per Telefon teilgenommen habe, erhöht die Wahrscheinlichkeit, dass die Schwachstelle hier liegt – also in dem Versäumnis, die unsichere Internetverbindung mit Verschlüsselung abzusichern.

Wo könnte eine potenzielle Sicherheitslücke liegen?

Grundsätzlich sind cloudbasierte Video-Konferenzsysteme wie Zoom, Teams, oder auch Webex, insbesondere dann als eher unsicher einzuschätzen, wenn ihre Implementierungen nicht quelloffen vorliegen. Daher wären ihnen offene Systeme, wie etwa Jitsi, BigBlueButton oder sogar Matrix, das offiziell von der Bundeswehr eingesetzt wird, solchen Lösungen vorzuziehen.

Dennoch ist im vorliegenden Fall wohl nicht davon auszugehen, dass es sich um eine Schwachstelle oder einen Datenabfluss aus dem System handelt, sondern eher um das Versäumnis, vom Handy über eine gesicherte Verbindung zu kommunizieren.

Sind Online-Konferenzsysteme für die Nutzung wie zum Beispiel durch Behörden, Forschungseinrichtungen, Unternehmen und Privatpersonen noch sicher?

Cloudbasierte Konferenzsysteme sind grundsätzlich gegenüber ihrem Betreiber unsicher. Geschäftsgeheimnisse oder anderweitig sensible

Informationen sollten grundsätzlich nicht auf diesem Weg ausgetauscht werden. Quelloffene, selbst betriebene Systeme mit Verschlüsselung sind entsprechend immer vorzuziehen. Dennoch gibt es hier natürlich Unterschiede in Bezug auf die Vertrauenswürdigkeit der Anbieter. Wer Office 365 Online benutzt, hat die Entscheidung, einem Anbieter zu vertrauen, bereits getroffen und braucht sich auch nach diesen neuen Vorkommnissen eigentlich keine weitergehenden Gedanken zu machen

.

Könnten Sicherheitslücken künftig vermieden werden?

Grundsätzlich ist immer darauf zu achten, die Systeme auf dem aktuellsten Stand zu halten – und wo es geht, auf cloudbasierte Konferenzsysteme zu verzichten. Systeme, die selbst betrieben werden, und bei denen eine verschlüsselte Kommunikation erzwungen wird, sind frei verfügbar und bieten die gleiche Qualität und den gleichen Komfort wie kommerzielle Anbieter. Dennoch besteht natürlich immer die Möglichkeit, dass Schwachstellen in Systemen gefunden werden. Im konkreten Fall handelte es sich wohl um einen Bedienungsfehler. Diese Fehler zu vermeiden, ist durch bessere Benutzerschnittstellen möglich, ausschließen lassen sie sich aber kaum.

Kann die Forschung zukünftig helfen, das Risiko zu minimieren?

Gerade in Bezug auf die Bedienbarkeit von sicheren Systemen ist noch viel zu tun. Natürlich müssen wir auch weiterhin daran forschen, wie eine sichere Verschlüsselung umsetzbar ist, wie Kommunikation über Netze und auch die Endsysteme abgesichert werden können. Der vorliegende Fall scheint aber erneut darauf hinzuweisen, dass insbesondere Fehler in der Bedienung zu Sicherheitslücken führen. Hier ist klar, daran zu forschen, wie das Bewusstsein geschärft und die Kompetenz im Umgang mit IT-Systemen verbessert bzw. der Umgang systematisch vereinfacht werden kann.

www.kastel-labs.de