NACHRICHTEN
Österreich

US-Sicherheitsbehörden beraten Telecom-Chefs über chinesischen Cyber-Diebstahl

US-Telekom-Manager treffen sich mit nationalen Sicherheitsbehörden, um Informationen über eine chinesische Cyber-Spionagekampagne auszutauschen. Sicherheitsbedenken wachsen, während Ermittlungen laufen.

(CNN) — Am Freitag trafen sich hochrangige Führungskräfte der Telekommunikationsbranche mit US-Nationalen Sicherheitsbehörden im Weißen Haus, da die Bedenken bezüglich einer langfristigen chinesischen Cyber-Spionagekampagne, die einige der höchsten politischen Figuren der USA ins Visier genommen hat, zunehmen.

Die Bedrohung durch Cyber-Spionage

Die Hacker haben sich tief in einige der großen US-Telekommunikationsanbieter eingegraben, um Telefonanrufe und Textnachrichten auszuspionieren. Laut informierten Personen war es schwierig, die Eindringlinge aus einigen Netzwerken zu entfernen.

Beratung für bessere Sicherheitsvorkehrungen

Die Treffen boten den Telekommunikationsvertretern die Gelegenheit, der Regierung Ratschläge zu erteilen, wie sie ihre Verteidigung gegen ausgeklügelte Hacks verbessern könnte. Die verschiedenen Gruppen tauschten auch

Geheimdienstinformationen über die Operation aus.

Herausforderung für die kommende Regierung

Der Hack entwickelt sich zu einer der größten Herausforderungen im Bereich Cyber- und nationale Sicherheit, mit denen die kommende Trump-Administration konfrontiert ist.

Geheime Informationen im Senat

Als weiteres Zeichen für die wachsenden Bedenken bezüglich der Cyber-Spionagekampagne ist für den 4. Dezember eine geheime Bürgerversammlung für alle Senatoren angesetzt, nachdem der Kongress im nächsten Monat aus der Pause zurückkehrt, so ein Mitarbeiter des Senats.

Umfang des Hacks und betroffene Personen

Der Hack ist laut Sen. Mark Warner, Demokrat aus Virginia und Vorsitzender des Geheimdienstkomitees, „bei weitem“ der „schlimmste Telekom-Hack in der Geschichte unserer Nation.“ Der vollständige Umfang des Hacks und die Auswirkungen auf die nationale Sicherheit werden derzeit noch untersucht.

Anzahl der betroffenen Telekommunikationsunternehmen

Das FBI hat weniger als 150 Opfer benachrichtigt, meist aus der Region Washington, D.C., so Warner. Allerdings haben all diese Opfer wahrscheinlich zahlreichen Personen Anrufe getätigt oder Textnachrichten gesendet, was bedeutet, dass die Zahl der von den Hackern Zugriff erlangten Aufzeichnungen wahrscheinlich viel höher ist. Die Hacker könnten die Anrufe bestimmter Zielpersonen über bestimmte Zeiträume hinweg überwachen, berichtete Warner.

Zielgerichtete Angriffe auf politische Persönlichkeiten

US-Offizielle sowie private Cybersicherheitsexperten führen Buch über die Anzahl der angegriffenen Telekommunikationsunternehmen. Die US-Breitband- und Internetanbieter AT&T, Verizon und Lumen wurden alle in dem Hackerangriff ins Visier genommen, wie CNN zuvor berichtete.

Angriff auf Politiker beider Parteien

Die Hacker hatten die Telefonkommunikation hochrangiger Persönlichkeiten sowohl der Republikanischen als auch der Demokratischen Partei im Visier, darunter **der gewählte Präsident Donald Trump**, den gewählten Vizepräsidenten JD Vance sowie **Jared Kushner und Eric Trump**.

Chinas Reaktion und US-amerikanische Cyberfähigkeiten

China hat die Vorwürfe des Hackens zurückgewiesen. US-Geheimdienstbehörden verfügen ebenfalls über umfassende Hackerfähigkeiten und haben den Telekommunikationssektor Chinas ins Visier genommen, wie Unterlagen zeigen, die vor über einem Jahrzehnt vom ehemaligen NSA-Auftragnehmer Edward Snowden geleakt wurden.

Künftige Sicherheitswarnungen

US-Offizielle haben seit Jahren vor Chinas Hacking-Programm gewarnt, das laut FBI-Direktor Christopher Wray größer ist als die Programme aller anderen großen Länder zusammen. Diese Warnungen sind im Laufe des letzten Jahres dringlicher geworden, da die Bedenken bezüglich einer möglichen chinesischen Invasion Taiwans zugenommen haben.

Cyberstrategie der USA

„Chinesische, mit der Regierung verbundene Hacker werden nicht aufhören, da dies Teil ihrer umfassenden nationalen Ziele ist. Cyber-Aktivitäten sind zu einem ihrer mächtigsten Instrumente nationaler Macht geworden“, sagte Morgan Adamski, Executive Director des US Cyber Command, der militärischen Offensive und defensiven Cyber-Einheit, in einer Rede am Freitag.

Die US-Regierung, einschließlich des Cyber Command, hat offensive und defensive Operationen durchgeführt, die darauf abzielen, Chinas Cyber-Operationen weltweit zu „schwächen und zu stören“, fügte Adamski auf der CYBERWARCON-Konferenz in Arlington, Virginia, hinzu.

Diese Geschichte wurde mit zusätzlichen Informationen aktualisiert.
CNNs Morgan Rimmer hat zu diesem Bericht beigetragen.

Details