NACHRICHTEN AG
Deutschland

11. Januar 2025

Chinesische Hacker plündern US-Büro für ausländische Investitionen

Chinesische Hacker haben das US-Büro für ausländische Investitionen infiltriert, das nationale Sicherheitsrisiken bewertet. Dies wirft Bedenken wegen Cyberspionage und den aktuellen US-China-Spannungen auf.

Chinesische Hacker haben ein US-Regierungsbüro infiltriert, das ausländische Investitionen auf nationale Sicherheitsrisiken überprüft, wie drei US-Beamte gegenüber CNN bestätigten. Dieser Vorfall, der bisher nicht berichtet wurde, verdeutlicht Chinas Interesse am Spionieren eines Büros, das weitreichende Befugnisse hat, chinesische Investitionen in den USA zu blockieren. Dies geschieht inmitten zunehmender Spannungen zwischen den beiden Supermächten.

Details des Hacks

Der Cyberangriff war Teil einer größeren Offensive der Hacker in das unklassifizierte System des Finanzministeriums. Das angegriffene Büro, das Komitee für ausländische Investitionen in den USA (CFIUS), erhielt im Dezember erweiterte Befugnisse zur Überprüfung von Immobilienverkäufen in der Nähe von US-Militärbasen. US-Gesetzgeber und Sicherheitsbeamte sind zunehmend besorgt, dass die chinesische Regierung oder deren Stellvertreter Landkäufe nutzen könnten, um Informationen über diese Basen zu sammeln.

Folgen für die nationale Sicherheit

Dieser Vorfall ist nur einer in einer Reihe angeblicher Cyber-

Spionagekampagnen aus China, die die US-Regierung im vergangenen Jahr erschüttert haben und die die anstehende Trump-Administration herausfordern werden. Ein anderer Hackerangriff von China drang tief in US-Telekommunikationsnetzwerke ein, um die Telefonkommunikation hochrangiger US-Politiker, darunter auch den designierten Präsidenten Donald Trump, zu überwachen.

US-Beamte sind nun dabei, die Auswirkungen des Hacks auf die nationale Sicherheit zu bewerten, nachdem das Finanzministerium diese Informationen letzte Woche den Gesetzgebern mitgeteilt hatte. Die Hacker hatten auch das Büro für Sanktionen des Finanzministeriums im Visier, das gerade erst eine chinesische Firma wegen ihres angeblichen Engagements in Cyberangriffen bestraft hatte. Es ist unklar, welche Informationen die Hacker letztendlich von den Computern des Finanzministeriums erbeuten konnten.

Überprüfung der gestohlenen Informationen

US-Beamte überprüfen die Dokumente, auf die die Hacker Zugriff hatten, und analysieren die nationalen Sicherheitsauswirkungen der gestohlenen Informationen. Es gibt zwar keine Beweise dafür, dass klassifizierte Daten zugänglich waren, jedoch besteht die Sorge, dass unklassifizierte Informationen in Kombination nützliche Erkenntnisse für die Chinesen liefern könnten.

Ein Sprecher des Finanzministeriums äußerte sich nicht direkt zu den Hackerangriffen auf das CFIUS, sondern verwies auf eine frühere Erklärung des Ministeriums. Laut dem Sprecher hatten die Hacker einen „Drittanbieter“ kompromittiert und konnten „von mehreren Arbeitsstationen der Nutzer des Finanzministeriums aus auf bestimmte unklassifizierte Dokumente zugreifen“. Das Ministerium hat mit Strafverfolgungsbehörden zusammengearbeitet, um die Auswirkungen dieses Vorfalls zu ermitteln, und es gibt keine

Hinweise darauf, dass die Hacker weiterhin Zugang zu den Systemen des Finanzministeriums haben.

Reaktionen aus China

Liu Pengyu, Sprecher der chinesischen Botschaft in Washington, DC, wiederholte Chinas langjährige Ablehnung, an Hackeroperationen beteiligt zu sein. „Während seines Treffens mit Präsident Biden in Lima im vergangenen Jahr erklärte Präsident Xi Jinping, dass es keine Beweise für die irrationalen Behauptungen über die angeblichen ‚Cyberangriffe aus China' gibt", so Liu in einer E-Mail.

Finanzministerin Janet Yellen erklärte gegenüber CNBC, dass der Hack „kein Vertrauen in unsere Beziehung [zu China] aufbaut" und dass sie dieses Thema in einem Anruf mit ihrem chinesischen Kollegen angesprochen habe. Yellen leitet das CFIUS, das auch andere Kabinettsmitglieder umfasst, wie die Minister für Verteidigung und Innere Sicherheit. In den letzten Jahren hat CFIUS an Bedeutung gewonnen, da der Wettbewerb zwischen den USA und China komplizierter geworden ist und sich auch auf Geschäftstransaktionen in abgelegenen Teilen der USA ausdehnt.

Ausblick auf künftige Maßnahmen

Die bevorstehende Trump-Administration wird Mitglieder oder andere hochrangige Mitarbeiter umfassen, die strengere Maßnahmen gegen China aufgrund von nationalen Sicherheitsbedenken gefordert haben, darunter der designierte nationale Sicherheitsberater Rep. Mike Waltz und Sen. Marco Rubio, Trumps Auswahl für das Außenministerium. US-Militär- und Geheimdienste führen bereits offensive Cyberoperationen gegen China durch, aber Waltz fordert zusätzliches Handeln.

„Amerika kann es sich nicht mehr leisten, im Cyberraum nur defensiv zu agieren", postete Waltz letzten Monat auf X. „Wir müssen offensiv vorgehen und Kosten für diejenigen auferlegen,

die unsere Technologie stehlen und unsere Infrastruktur angreifen.“

Details	
Quellen	• **edition.cnn.com**