China-hackte US-Finanzamt: Schwerer Sicherheitsvorfall

China-unterstützte Hacker haben in einem schwerwiegenden Vorfall US-Schatzamt-Arbeitsstationen infiltriert. Das Sicherheitsproblem wurde durch einen gestohlenen Schlüssel ermöglicht. Weitere Ermittlungen laufen.

Das US-Finanzministerium hat die Gesetzgeber am Montag darüber informiert, dass ein von China unterstützter Akteur in die Arbeitsstationen des Ministeriums eingedrungen ist, was von den Beamten als ein „großes Ereignis“ beschrieben wird.

Details zum Eindringen in das Finanzministerium

In einem von CNN eingesehenen Schreiben teilte ein Beamter des Finanzministeriums mit, dass man am 8. Dezember von einem Drittanbieter für Softwaredienstleistungen informiert wurde, dass ein Bedrohungsakteur mithilfe eines gestohlenen

Schlüssels aus der Ferne auf bestimmte Arbeitsstationen und unklassifizierte Dokumente des Ministeriums zugegriffen hatte.

Zuordnung des Vorfalls zu staatlichen Akteuren

„Basierend auf den verfügbaren Indikatoren wurde der Vorfall einem von China unterstützten Advanced Persistent Threat (APT)-Akteur zugeordnet“, schrieb Aditi Hardikar, die stellvertretende Sekretärin für Management im US-Finanzministerium, in dem Schreiben.

Maßnahmen nach dem Vorfall

Ein Sprecher des Ministeriums erklärte gegenüber CNN, dass der betroffene Dienst offline genommen wurde und die Beamten mit den Strafverfolgungsbehörden sowie der Cybersecurity and Infrastructure Security Agency (CISA) zusammenarbeiten.

„Es gibt keine Hinweise darauf, dass der Bedrohungsakteur weiterhin Zugang zu den Systemen oder Informationen des Finanzministeriums hat“, so der Sprecher weiter.

Geheime Meldung an den Finanzdienstleistungsausschuss

Beamte des Finanzministeriums planen nächste Woche eine vertrauliche Informationssitzung zu dem Vorfall mit Mitarbeitern des Ausschusses für Finanzdienstleistungen des Repräsentantenhauses, wie ein leitender Mitarbeiter des Ausschusses CNN mitteilte. Der genaue Zeitpunkt der Sitzung steht noch nicht fest.

Zugang durch gestohlenen Schlüssel

Laut dem Schreiben an die Führung des Senate Banking

Committee gab der Drittanbieter BeyondTrust bekannt, dass Hacker Zugang zu einem Schlüssel erlangt hatten, der vom Anbieter verwendet wurde, um einen cloudbasierten Dienst für technische Unterstützung, den das Finanzministerium nutzt, abzusichern.

Reaktion von BeyondTrust auf den Sicherheitsvorfall

„Durch den Zugang zum gestohlenen Schlüssel konnte der Bedrohungsakteur die Sicherheitsvorkehrungen des Dienstes übergehen, auf bestimmte Arbeitsstationen der Mitarbeiter des Finanzministeriums zugreifen und bestimmte unklassifizierte Dokumente einsehen, die von diesen Nutzern verwaltet werden“, heißt es in dem Schreiben des Ministeriums.

BeyondTrust erklärte, dass man am 2. Dezember einen Sicherheitsvorfall festgestellt habe, der das Produkt „Remote Support“ betraf, und habe die betroffenen Kunden informiert, nachdem das Unternehmen am 5. Dezember „anormales Verhalten“ in dem Produkt bestätigt hatte.

Am 8. Dezember veröffentlichte das Unternehmen **Informationsmaterial** zu dem Vorfall auf seiner Webseite und hat laufend über den Fortschritt seiner Untersuchungen berichtet, um zukünftige Bedrohungen zu mildern. Das Unternehmen gab an, die betroffenen Instanzen des Produkts außer Betrieb genommen und ein externes Cybersicherheitsteam zur Untersuchung engagiert zu haben.

Identifizierung der betroffenen Systeme

„Es waren keine anderen Produkte von BeyondTrust betroffen“, sagte ein Sprecher des Unternehmens. „Die Strafverfolgungsbehörden wurden benachrichtigt, und BeyondTrust unterstützt die Ermittlungsbemühungen.“

Es ist unklar, wie viele Arbeitsstationen infiltriert wurden. Der Sprecher des Finanzministeriums teilte jedoch mit, dass „mehrere“ Arbeitsstationen von Nutzern des Ministeriums betroffen seien.

Klassifizierung des Vorfalls als große Cybersecurity-Bedrohung

Hardikar erklärte in dem Schreiben, dass gemäß den Richtlinien des Finanzministeriums Eindringlinge, die mit fortschrittlichen Bedrohungsakteuren in Verbindung stehen, als „großes Cybersecurity-Ereignis“ eingestuft werden. Die Beamten des Finanzministeriums sind verpflichtet, innerhalb von 30 Tagen einen aktualisierten Bericht vorzulegen.

Umfang der Schäden und weitere Untersuchungen

Es ist noch unklar, ob das Finanzministerium den Umfang der durch den Vorfall verursachten Schäden vollständig ermittelt hat. Hardikar schrieb in dem Schreiben, dass das Finanzministerium in einem Bemühen, den Vorfall „vollständig zu charakterisieren und seine Gesamtauswirkungen zu bestimmen“, mit CISA, dem FBI, US-Geheimdiensten und externen forensischen Ermittlern zusammenarbeitet.

„CISA wurde sofort in Kenntnis gesetzt, nachdem das Finanzministerium von dem Angriff erfahren hatte, und die verbleibenden zuständigen Behörden wurden kontaktiert, sobald das Ausmaß des Angriffs offensichtlich wurde“, heißt es in dem Schreiben.

Details