

Chinesische Hacker verdächtigt: Cyberangriff auf US-Kanzlei

Chinesische Hacker sollen in die E-Mail-Konten einer renommierten Kanzlei in Washington, DC, eingedrungen sein. Die Cyber-Attacke zielt offenbar auf Geheimdienstinformationen ab.



Verdächtige chinesische Hacker haben sich den E-Mail-Accounts von Anwälten und Beratern einer einflussreichen Washingtoner Kanzlei, Wiley Rein, Zugriff verschafft. Dies wurde in einem Memo bekannt, das von der Kanzlei in dieser Woche an ihre Kunden versandt wurde, und das von CNN eingesehen wurde.

Hackerangriff auf wichtige Rechtskanzlei

Die verantwortlichen Hacker sind dafür bekannt, Informationen zu Handelsfragen, Taiwan und US-Regierungsbehörden, die für Zollfragen und die Überprüfung ausländischer Investitionen zuständig sind, anzuvisieren. In dem Memo teilte die Kanzlei mit: „Wir glauben, basierend auf den bisher ausgewerteten Beweisen, dass eine Gruppe, die möglicherweise mit der chinesischen Regierung verbunden ist, auf Nachrichten in den Microsoft 365-Konten bestimmter Mitarbeiter von Wiley zugegriffen hat, um Informationen zu sammeln.“

Kontext des Cyberangriffs

Der Angriff erfolgt in einem Kontext, in dem die Trump-Regierung in diesem Frühjahr den Handelskrieg mit China durch die Verhängung beispielloser Zölle auf chinesische Exporte in die USA verschärft hat. Diese Zollmaßnahmen führten auf beiden Seiten zu einem intensiven Bemühen, die Positionen des jeweiligen Gegenübers zu verstehen.

Wiley Rein und ihre Rolle im Handelskrieg

Wiley Rein hat Kunden, die in der Fortune 500 gelistet sind, und verfügt über ein Team von erstklassigen Handelsanwälten. Die Kanzlei ist ein bedeutender Akteur, der US-Unternehmen und der Regierung hilft, den Handelskonflikt mit China zu navigieren. Sie beschreibt sich selbst als „eng mit Washington verbunden“ und betont, „unvergleichliche Einblicke in die sich wandelnden Prioritäten von Behörden, Regulierungsbehörden und Gesetzgebern“ zu bieten.

Zusammenarbeit mit den Behörden

Die Kanzlei hat mitgeteilt, dass sie noch dabei ist zu klären, auf welche Informationen die Hacker zugegriffen haben. „Wir haben auch die Strafverfolgungsbehörden informiert und koordinieren uns mit ihnen“, heißt es in dem Memo. CNN hat um einen Kommentar von Wiley Rein und dem FBI gebeten, das in der

Regel hochkarätige Hacks mit nationalen Sicherheitsimplikationen untersucht. Die Sicherheitsfirma Mandiant, die zu Google gehört, ist mit der Behebung des Hacks beauftragt, wie das Memo von Wiley Rein vermerkt.

Verdächtige Aktivitäten und weitere Untersuchungen

Dieser Vorfall ist nur die jüngste vermutete chinesische Einbruchsaktion in eine US-Organisation, die mit sensiblen Handels- oder Investitionsangelegenheiten befasst ist. CNN berichtete im Januar, dass chinesische Hacker in das US-Regierungsbüro eingedrungen sind, das ausländische Investitionen auf nationale Sicherheitsrisiken überprüft.

Bewertungen von ausländischen Investitionen spielen eine wichtige Rolle in der Beziehung zwischen den beiden größten Volkswirtschaften der Welt. Am Freitag gab die Trump-Regierung bekannt, dass sie die Übernahme von Jupiter Systems, einem Anbieter von audiovisuellen Geräten, durch ein in Hongkong ansässiges Unternehmen blockiert hat, da sie die „potenzielle Gefährdung von Jupiters Produkten, die in militärischen und kritischen Infrastrukturmgebungen verwendet werden“, befürchtet.

Langfristige Cyberstrategie Chinas

Über Jahre hinweg haben US-Beamte, unabhängig von Parteien, versucht, Chinas formidable Cyberfähigkeiten zu begreifen. Das FBI hat festgestellt, dass China ein größeres Hackerprogramm betreibt als alle anderen ausländischen Regierungen zusammen. Der Hack bei Wiley Rein könnte eine von vielen laufenden Ermittlungen des FBI in Bezug auf cyber-spionage mit Verbindungen nach Peking erweitern.

Das FBI hat weiterhin mit der umfassenden Kompromittierung US-amerikanischer Telekommunikationsanbieter zu kämpfen,

die die Telefonkommunikation hochrangiger US-Führungskräfte, einschließlich des damaligen Präsidentschaftskandidaten Trump, ins Visier genommen hat und die im letzten Jahr öffentlich wurde. AT&T, Verizon und andere große Kommunikationsunternehmen wurden gehackt.

„Wir wissen nicht, ob wir mit der Identifizierung der Opfer bereits fertig sind oder ob es mehr gibt“, sagte Brett Leatherman, der stellvertretende Direktor der Cyber-Division des FBI. „Die Telekommunikationsunternehmen glauben jedoch, dass sie die Hacker nach vielen Monaten der Untersuchung eingedämmt haben“, fügte er hinzu.

Leatherman betonte: „Chinas Cyberdoktrin geht über den Zugang hinaus. Es geht darum, langfristige Einflussmöglichkeiten zu schaffen.“

Details

Besuchen Sie uns auf: [die-nachrichten.at](https://www.die-nachrichten.at)