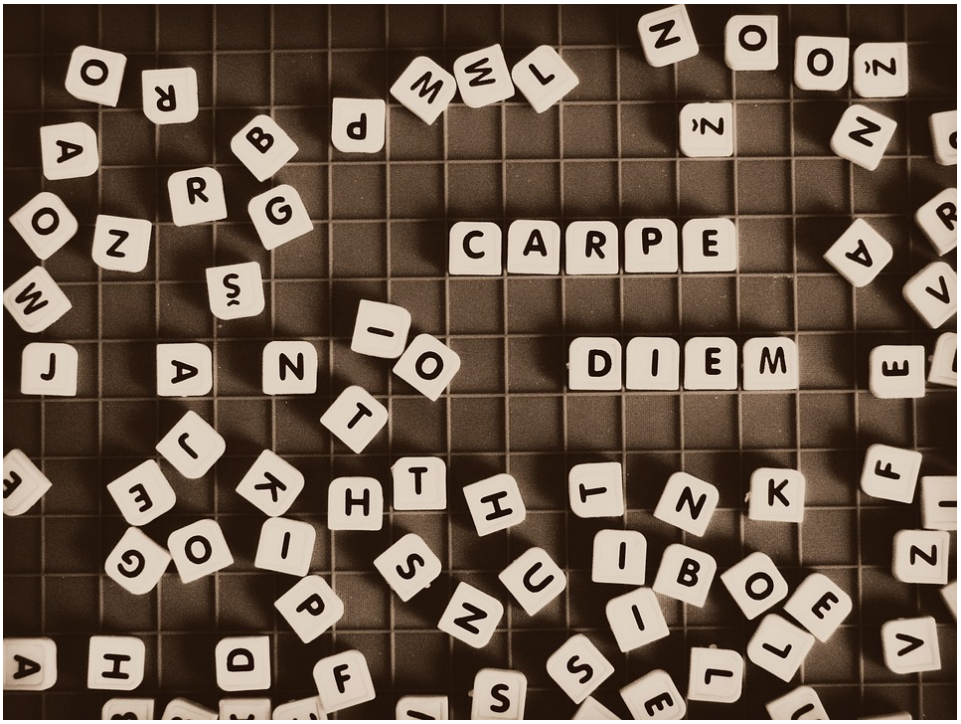
NACHRICHTEN AG
Deutschland

US untersucht Sicherheitsrisiken durch Internet-Router für Millionen Nutzer

US-Behörden untersuchen potenzielle Sicherheitsrisiken von TP-Link-Routern, die Millionen nutzen. Diese Maßnahmen zielen darauf ab, Chinas Einfluss im amerikanischen Telekommunikationssektor zu begrenzen.



US-Behörden untersuchen potenzielle nationalstaatliche Sicherheitsrisiken im Zusammenhang mit einem Telekommunikationsunternehmen, das in **China** gegründet wurde und dessen Internet-Router von Millionen genutzt werden, wie mehrere informierte Quellen gegenüber CNN berichteten.

Risiko durch TP-Link-Router

Die US-Behörden sind besorgt, dass die kostengünstigen und weit verbreiteten Router von TP-Link möglicherweise als

Sprungbrett für von China unterstützte Hacker in die US-Infrastruktur dienen könnten, so die Quellen. Das Handelsministerium hat eine Untersuchung des Unternehmens eingeleitet, die sich noch in einem frühen Stadium befindet. Eine mögliche Folge dieser Ermittlungen könnte ein Verkaufsverbot für TP-Link-Router in den USA sein, erklärten zwei der Quellen.

Aktionen der Biden-Administration

Dies ist nur eine von zahlreichen Maßnahmen, die die Biden-Administration in ihren letzten Tagen ergriffen hat, um Chinas Fähigkeit zur Cyberkriminalität im amerikanischen Telekommunikationssektor einzuschränken. Diese Initiativen werden auch in die Trump-Administration übernommen, die vor der schwierigen Aufgabe steht, Chinas aggressiven Einsatz von Cyberoperationen zur Informationsbeschaffung zu kontern.

Das Handelsministerium hat in der vergangenen Woche auch ein „vorläufiges Ergebnis“ im Rahmen einer separaten Untersuchung zu einem anderen Unternehmen, der US-Tochtergesellschaft von China Telecom, dem staatlichen Telekommunikationsgiganten, veröffentlicht. Diese steht im Zusammenhang mit nationalen Sicherheitsrisiken, die US-Behörden bei der Nutzung von dessen Ausrüstung durch amerikanische Telekom-Firmen vermuten. Dies ist der erste Schritt in Richtung einer möglichen Säuberung aller verbleibenden China Telecom-Geräte von US-Anbietern.

Cyber-Espionage und Schutzmaßnahmen

All dies geschieht, während große US-Telekommunikationsanbieter weiterhin daran arbeiten, chinesische Hacker aus ihren Netzwerken zu vertreiben, die im Rahmen einer Cyber-Espionagekampagne Hochrangige US-Politiker, einschließlich des Präsidenten-elect Donald Trump, ins Visier nahmen. Der Wall Street Journal berichtete zuerst über die Untersuchung des Handelsministeriums gegen TP-Link.

TP-Link, 1996 in China gegründet, hat sich zu einem dominierenden Akteur auf dem globalen Markt für drahtlose Internet-Router entwickelt. Die genaue Marktanteil von TP-Link in den USA ist unklar (ein Sprecher des Unternehmens reagierte nicht auf eine Anfrage nach Marktanteilen), aber die breite Nutzung der Geräte in den USA ist ein Grund für die laufenden Ermittlungen.

Reaktionen und Stellungnahmen von TP-Link

In diesem Jahr kündigte TP-Link eine Unternehmensumstrukturierung an und errichtete einen Firmensitz in Kalifornien, TP-Link Systems, der eigenen Aussagen zufolge von den chinesischen Operationen getrennt ist. „Als in den USA ansässiges Unternehmen entsprechen die Sicherheitspraktiken von TP-Link Systems Inc. vollständig den branchenspezifischen Sicherheitsstandards in den USA“, sagte ein Sprecher von TP-Link Systems gegenüber CNN.

„Wir begrüßen Gelegenheiten, um mit der Bundesregierung in Kontakt zu treten und zu zeigen, dass unsere Sicherheitspraktiken den branchenspezifischen Sicherheitsstandards entsprechen. Zudem drücken wir unser fortwährendes Engagement für den amerikanischen Markt und die amerikanischen Verbraucher aus und möchten US-nationale Sicherheitsrisiken angehen“, heißt es in der Erklärung. Das Unternehmen wurde jedoch nicht wegen Fehlverhaltens beschuldigt.

Expertise und Cyberbedrohungen

China verfügt über eine Vielzahl von Hackergruppen, die geschickt in der Ausnutzung von Internet- und Telefonanbietern sind, um sensible Benutzerinformationen zu erfassen, so private Experten und US-Behörden. Diese Hacker haben nicht nur TP-Link-Router ausgenutzt, sondern auch Geräte amerikanischer

Anbieter wie Cisco.

Die chinesische Regierung bestreitet regelmäßig US-Vorwürfe über Cyberangriffe. „Wir fordern die USA auf, zu verhindern, dass der Begriff der nationalen Sicherheit ausgeweitet wird, und die Missbrauch nationaler Macht zu stoppen, um chinesische Unternehmen zu unterdrücken“, erklärte Liu Pengyu, ein Sprecher der chinesischen Botschaft in Washington, DC, in einer E-Mail.

Ermittlungen und Sicherheitsmaßnahmen

Eine umfassende Hacking-Kampagne, die auf die Telefonate von Trump, Vizepräsident-elect JD Vance und hochrangige Beamte der Biden-Administration abzielte, hat die Dringlichkeit der Untersuchungen des Handelsministeriums in Bezug auf chinesische Telekommunikationsgeräte verstärkt.

US-Beamte glauben, dass die chinesischen Hacker mindestens acht US-Telekommunikationsanbieter in ihrem Bestreben, hochrangige US-Politiker auszuspionieren, infiltriert haben. Diese aktuelle Cyber-Spionage hat auch die angespannten US-chinesischen Cyber-Beziehungen weiter belastet, die selten ruhig sind.

Verantwortung und Reformen

In einigen Fällen hat ein Mangel an starken Sicherheitsvorkehrungen bei einigen Telekommunikationsanbietern und Geräteherstellern wahrscheinlich die Schäden der mutmaßlichen chinesischen Hackerangriffe verschärft und dafür gesorgt, dass die Hacker nicht früher entdeckt wurden. Das Weiße Haus hat den Telekommunikationsanbietern die Schuld für den Vorfall zugewiesen, was einige Telekom-Führungskräfte verärgert hat, die angeben, dass sie erheblich in Verteidigungsmaßnahmen investiert haben und gegen eine extrem fähige Hackergruppe antreten.

US-Beamte und Telekom-Führungskräfte hatten Schwierigkeiten, vorherzusehen, wie die mutmaßlichen chinesischen Spione das gesamte Telekommunikationssystem, einschließlich seiner Verbindungen, sowie die erforderliche Software und Hardware studieren und ausnutzen würden. „Der Status quo muss sich ändern“, erklärte Senat Ron Wyden.

„Dies ist ein Wendepunkt, und man kann entweder bei einem gebrochenen System bleiben oder bereit sein, Maßnahmen zu ergreifen, um dies zu verbessern“, fügte Wyden hinzu. Seine Gesetzgebung würde erfordern, dass die Führungskräfte der Anbieter unterzeichnete Erklärungen vorlegen, in denen sie bestätigen, dass sie den FCC-Cybersicherheitsregeln entsprechen.

Die großen Telekommunikationsanbieter finden im Allgemeinen schnell heraus, wenn jemand versucht hat, in ihre Netzwerke einzudringen, so Marcus Sachs, ehemaliger Vizepräsident für nationale Sicherheitsstrategie bei Verizon. „Der schlimmste Fall ist, wenn der Eindringling Monate oder Jahre unentdeckt bleibt und innerhalb des Netzwerks Informationen überwacht und sammelt“, erklärte Sachs.

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