



00:51 Min

Behörden und Firmen betroffen

Hackerangriff deckt Microsoft-Schwachstelle auf

Stand: 21.07.2025 09:00 Uhr

IT-Experten warnen vor einer bisher unbekannten Sicherheitslücke bei Microsoft-Servern. Betroffen ist das Programm SharePoint, das weltweit Firmen, Behörden und Universitäten nutzen, um Daten auszutauschen. Das FBI ermittelt.

Angesichts eines Hackerangriffs auf ein viel genutztes Programm von Microsoft hat sich in den USA die Bundespolizei eingeschaltet. Das FBI teilte mit, es arbeite wegen der Attacken eng mit verschiedenen Behörden und Unternehmen zusammen. Einzelheiten nannten die Ermittlerinnen und Ermittler zunächst nicht.

Zuvor hatte Microsoft vor aktiven Angriffen auf seine Server-Software SharePoint gewarnt. Das Programm wird zur gemeinsamen Nutzung von Dokumenten verwendet. Microsoft empfahl seinen Kundinnen und Kunden, umgehend Sicherheitsupdates zu installieren. Dem Konzern zufolge handelt es sich um eine Schwachstelle, die Angriffe mittels "Spoofing" ermöglicht. Dabei kann ein Angreifer seine Identität verschleiern und sich als vertrauenswürdige Person ausgeben.

Betroffen seien nur SharePoint-Server, die von den Organisationen selbst betrieben werden, erklärte Microsoft weiter. Die Cloud-Version SharePoint Online in Microsoft 365 sei verschont geblieben. Man stimme sich bei der Reaktion mit mehreren US-Behörden ab, darunter auch dem Cyber-Kommando des Verteidigungsministeriums.

Dutzende Firmen und Behörden angegriffen

Hacker hätten die Sicherheitslücke in den letzten Tagen schon genutzt und seien auf Server "Dutzender" Firmen und Behörden eingedrungen. Das sagte ein Manager der IT-Sicherheitsfirma Palo Alto Networks. Laut Washington Post sind auch zwei US-Bundesbehörden angegriffen worden. Zehntausende Server seien gefährdet.

Der Zugang zu den Servern eröffne potenziell die Möglichkeit, Daten zu stehlen und Passwörter abzugreifen, warnte das niederländische Unternehmen Eye Security. Schlimmer noch: Nach Erkenntnissen der Expertinnen und Experten können Angreifer auch digitale Schlüssel stehlen, mit denen sie sich später auch wieder Zugang zu Computersystemen mit geschlossener Sicherheitslücke verschaffen könnten.

Jeder, der einen SharePoint-Server betreibe, habe ein Problem, sagte ein Vertreter der Sicherheitsfirma CrowdStrike. "Es ist eine bedeutende Schwachstelle." Eye Security empfiehlt angesichts der Attacken auf "Tausende" Server, diese zu isolieren oder abzuschalten.

Software-Update soll helfen

Das Problem sei bekannt, schreibt Microsoft unterdessen in einem Blogeintrag und forderte Betroffene auf, ein Software-Update schnellstmöglich zu installieren. Das soll die Sicherheitslücke schließen. Wenn Kundinnen und Kunden den empfohlenen Malware-Schutz nicht aktivieren könnten, sollten sie ihre Server vom Internet trennen, bis ein Sicherheitsupdate verfügbar ist.

Microsoft hatte erst kürzlich mit einem Update mehrere Schwachstellen geschlossen. Die Angreifer fanden danach eine ähnliche Sicherheitslücke an anderer Stelle. Die amerikanische IT-Sicherheitsbehörde CISA rief betroffene staatliche Stellen und Unternehmen zu schnellem Handeln auf.

Zuletzt hatten sich im Jahr 2023 mutmaßlich chinesische Hacker Zugang zu E-Mails in einigen US-Behörden über eine Schwachstelle in Microsoft-Software verschafft.

Mit Informationen von Nils Dampz, ARD-Studio Los Angeles

[Zur Startseite](#)

