NACHRICHTEN
Österreich
21. Juli 2025

Hacker-Angriff gefährdet Behörden und Firmen: Microsoft-Software betroffen!

Cyberangriffe auf Behörden und Unternehmen in Wien: Sicherheitslücke in Microsoft SharePoint gefährdet Daten. Sofortige Maßnahmen empfohlen.

Vienna, AT - In den letzten Tagen hat die US-Technologiefirma Microsoft eine alarmierende Sicherheitslücke in seiner SharePoint-Software entdeckt, die bereits zu Angriffen auf viele Organisationen, sowohl im Wirtschafts- als auch im Regierungsbereich, geführt hat. Diese Schwachstelle betrifft lokale Server, die für das Teilen von Dateien über SharePoint genutzt werden. Angreifer haben bereits erfolgreichen Zugriff auf die Systeme „Dutzender“ Organisationen erlangt, wobei die IT-Sicherheitsfirma Palo Alto Networks von umfangreichen Aktivitäten berichtete. Der Zugang zu den Servern könnte potenziell zum Diebstahl von sensiblen Daten und Passwörtern führen, einschließlich digitaler Schlüssel, die den Angreifern späteren Zugang zu geschlossenen Systemen gewähren

könnten. Sicherheitsfirma Crowdstrike beschreibt die Schwachstelle als „bedeutend“.

Microsoft hat die Problematik in einem Blogeintrag eingeräumt und veröffentlichte umgehend Updates zur Beherrschung der Sicherheitslücke. Die US-IT-Sicherheitsbehörde CISA äußerte sich ebenfalls und forderte betroffene Stellen sowie Unternehmen zu schnellem Handeln auf. Erste Indizien für die Attacken wurden am Freitag festgestellt, wobei noch unklar bleibt, wer hinter den Angriffen steckt. Besonders besorgniserregend ist, dass in den USA Server von zwei Bundesbehörden erfolgreich kompromittiert wurden, jedoch keine spezifischen Angaben zu den betroffenen Behörden gemacht werden.

Details zur Sicherheitslücke

Diese spezifische Schwachstelle, bekannt als CVE-2025-53770, ermöglicht es Angreifern, unbefugten Zugriff auf lokal betriebene SharePoint-Server zu erlangen. Laut CISA erlaubt die Sicherheitsanfälligkeit die Remote-Codeausführung (RCE). Exploit-Tools wie „ToolShell“ ermöglichen den Zugriff auf vertrauliche Daten und die Ausführung beliebigen Codes. Die Bedrohung ist erheblich und das vollständige Ausmaß wird weiterhin untersucht. CISA hat empfohlen, Prozesse zur Sicherheitsüberprüfung und -überwachung zu implementieren, um die Systeme zu schützen.

CISA empfiehlt unter anderem Folgendes:

- Konfigurierung des Antimalware Scan Interface (AMSI) in SharePoint, um die Sicherheit zu erhöhen.
- Implementierung von Microsoft Defender AV auf allen SharePoint-Servern.
- Trennung der betroffenen Produkte vom Dienst, wenn AMSI nicht aktiv sein kann.
- Anwendung offizieller Abhilfemaßnahmen, sobald diese verfügbar sind.

- Befolgung der BOD 22-01-Richtlinien speziell für Bundesbehörden.

Vorbeugende Maßnahmen und Reaktion der Behörden

CISA hat CVE-2025-53770 am 20. Juli 2025 in ihren Katalog der „Known Exploited Vulnerabilities” aufgenommen. Um die Bedrohung zu minimieren, rät CISA allen Organisationen, Vorfälle unverzüglich zu melden. Unternehmen wird nahegelegt, ein umfassendes Protokollierungs- und Überwachungssystem zur Identifizierung von Exploit-Aktivitäten zu implementieren sowie die Layout- und Administratorrechte zu überprüfen und zu minimieren. Zudem wurden spezifische IP-Adressen identifiziert, von denen aus zwischen dem 18. und 19. Juli 2025 verdächtige Aktivitäten stattfanden.

Die kontinuierliche Behebung von bekannten Schwachstellen bleibt entscheidend, um Organisationen vor Cyberangriffen zu schützen. CISA stellt klar, dass alle betroffenen Stellen und Unternehmen schnellstmöglich handeln müssen, um Folgeschäden zu vermeiden.
Lesen Sie mehr zu diesem Thema bei **Vienna.at**, **All About Security** und **Cyber Security News**.

Details	
Vorfall	Cyberkriminalität
Ort	Vienna, AT
Quellen	• **www.vienna.at** • **www.all-about-security.de** • **cybersecuritynews.com**