NACHRICHTEN
Österreich

21. Juli 2025

Microsoft-Warnung: Hackerangriffe auf Behörden alarmieren die Nation!

Microsoft warnt vor Angriffen auf US-Behörden durch Hacker, nachdem Sicherheitslücken entdeckt wurden. Dringende Updates erforderlich.

USA - Microsoft hat ein ernstes Sicherheitsproblem in seiner Software identifiziert. Am 21.07.2025 bestätigte das Unternehmen in einem Blogeintrag die Entdeckung einer Schwachstelle, die sowohl lokale Server als auch SharePoint betrifft. Diese Sicherheitslücke hat bereits dazu geführt, dass Hacker in die Systeme „Dutzender“ Organisationen, darunter sowohl wirtschaftliche als auch staatliche Stellen, eindringen konnten. Laut Berichten von der **Krone** und **ZDF** fordert die amerikanische Cyber-Sicherheitsbehörde CISA alle betroffenen Behörden und Unternehmen zu schnellem Handeln auf.

Die Schwachstelle ermöglicht potenziell den Diebstahl von Daten, Passwörtern sowie digitaler Schlüssel, was den

Angreifern späteren Zugang zu geschlossenen Sicherheitslücken eröffnet. Microsoft hat Updates veröffentlicht, um das Problem zu beheben. Dennoch bleibt die Identität der Angreifer unklar, und es gibt hierzu keine spezifischen Angaben über die betroffenen US-Bundesbehörden, die laut der „Washington Post“ erfolgreich angegriffen wurden.

Ermittlungen und Bedrohungslage

Ermittler in mehreren Ländern haben bereits verschiedene Varianten von Schadsoftware unschädlich gemacht und die Täter identifiziert. Aktivisten und Forscher der Sicherheitsfirma Crowdstrike warnen vor der signifikanten Bedrohung, die diese Sicherheitslücke darstellt. Im Jahr 2023 hatten mutmaßlich chinesische Hacker über eine Schwachstelle in Microsoft-Software Zugang zu E-Mails in einigen US-Behörden erlangt, was das Vertrauen in die Sicherheitsinfrastruktur weiter erschüttert hat.

Der Manager von Crowdstrike bezeichnete die neu entdeckte Schwachstelle als „bedeutend“ und riet dazu, betroffene SharePoint-Server entweder zu isolieren oder abzuschalten, um die Risiken zu minimieren. Auch in Deutschland hat die Cyberkriminalität im Jahr 2023 zugenommen, wie das Bundeslagebild 2023 des Bundeskriminalamts zeigt. Die Diskussion über Sicherheitsstrategien und regulatorische Maßnahmen wird intensiver.

Regulatorische Maßnahmen und ihre Auswirkungen

Die Notwendigkeit, kritische Infrastrukturen widerstandsfähiger zu machen, wird von Regierungen zunehmend erkannt. Einem Bericht von **PwC** zufolge haben gesetzliche Vorschriften zur Cybersicherheit bereits signifikante Auswirkungen auf die Unternehmensinvestitionen. 89 % der deutschen Organisationen berichten von einem moderaten bis signifikanten Einfluss auf

ihre Cyberausgaben. In der EMEA-Region liegt dieser Wert bei 80 %.

Die Debatte über regulatorische Lasten gewinnt insbesondere in der Europäischen Union an Fahrt, besonders nach den Ergebnissen der US-Wahlen. Kurz- bis mittelfristig ist jedoch keine regulatorische Entlastung zu erwarten. Dies lässt die Frage offen, ob alle EU-Mitgliedstaaten den gleichen Weg gehen oder ob einigen die notwendigen Schritte schwerfallen werden.

Zusammenfassend lässt sich sagen, dass die Situation rund um die Microsoft-Sicherheitsproblematik und die damit verbundenen Cyberbedrohungen eine dringende und koordinierte Antwort auf politischer und wirtschaftlicher Ebene erfordert. Die Entwicklungen in diesem Bereich werden sowohl Unternehmen als auch Regierungen weiterhin beschäftigen.

Details	
Vorfall	Cyberkriminalität
Ursache	Sicherheitslücke
Ort	USA
Quellen	• **www.krone.at** • **www.zdfheute.de** • **www.pwc.de**