BSI

Viele Exchange-Server ungeschützt

[27.03.2024] Microsoft Exchange ist ein weit verbreiteter E-Mail- und Groupware-Server. Veraltete Systeme und nicht eingespielte Updates eröffnen kritische Sicherheitslücken. Das BSI geht davon aus, dass etwa die Hälfte aller Exchange-Server in Deutschland verwundbar ist und rät dringend, den Patch-Stand zu prüfen und zu aktualisieren.

Mindestens 17.000 Instanzen von Microsoft-Exchange-Servern in Deutschland sind durch eine oder mehrere kritische Schwachstellen verwundbar. Hinzu kommt eine Dunkelziffer an Exchange-Servern in vergleichbarer Größe, die potenziell verwundbar sind. Das geht aus einer aktuellen Untersuchung des Bundesamts für Sicherheit in der Informationstechnik (BSI) hervor. Daher ruft das BSI die Betreiber der Instanzen dazu auf, aktuelle Exchange-Versionen einzusetzen, verfügbare Sicherheitsupdates einzuspielen und die Instanzen sicher zu konfigurieren. Weitere Informationen stellt das BSI in einer aktuellen Warnung zur Verfügung.
Cyber-Kriminelle sowie staatliche Akteure nutzen nach BSI-Angaben mehrere dieser Schwachstellen bereits aktiv zur Verbreitung von Schad-Software, zur Cyber-Spionage oder für Ransomware-Angriffe aus. Betroffen sind insbesondere Schulen und Hochschulen, Kliniken, Arztpraxen, Pflegedienste und andere medizinische Einrichtungen, Rechtsanwälte und Steuerberater, Kommunalverwaltungen sowie viele mittelständische Unternehmen. Dazu sagt BSI-Präsidentin Claudia Plattner: „Dass es in Deutschland von einer derart relevanten Software zigtausende angreifbare Installationen gibt, darf nicht passieren. Unternehmen, Organisationen und Behörden gefährden ohne Not ihre IT-Systeme und damit ihre Wertschöpfung, ihre Dienstleistungen oder eigene und fremde Daten, die womöglich hochsensibel sind. Cyber-Sicherheit muss endlich hoch oben auf die Agenda. Es besteht dringender Handlungsbedarf.“

Hoher Anteil der Microsoft-Exchange-Server verwundbar

Rund 45.000 Microsoft-Exchange-Server in Deutschland sind derzeit ohne Beschränkungen aus dem Internet erreichbar. Nach aktuellen Erkenntnissen des BSI sind etwa zwölf Prozent davon so veraltet, dass für sie keine Sicherheitsupdates mehr angeboten werden. Rund 25 Prozent aller Server werden zwar mit den aktuellen Versionen Exchange 2016 und 2019 betrieben, verfügen aber über einen veralteten Patch-Stand. In beiden Fällen sind die Server für mehrere kritische Schwachstellen anfällig. Damit sind mindestens 37 Prozent aller offen aus dem Internet erreichbaren Microsoft-Exchange-Server verwundbar. Für weitere 48 Prozent der Exchange-Server kann keine eindeutige Aussage hinsichtlich der Verwundbarkeit für die kritische Schwachstelle CVE-2024-21410 getroffen werden. Diese Systeme sind noch verwundbar, sofern die Betreiber nicht die seit August 2022 zur Verfügung stehende Extended Protection aktiviert oder andere Schutzmaßnahmen getroffen haben. Inwieweit dies zutrifft, können nur die jeweiligen Betreiber beurteilen.
Darüber hinaus besteht eine weitere Schwachstelle in Microsoft Exchange, für die jüngst Sicherheitsupdates zur Verfügung gestellt wurden. Werden diese Updates nicht eingespielt, erhöht sich die Bedrohungslage weiter. Das CERT-Bund des BSI informiert Netzbetreiber in Deutschland bereits seit längerer Zeit tagesaktuell automatisiert per E-Mail zu IP-Adressen in ihren Netzen, unter denen sich bekannte verwundbare Exchange-Server befinden.

(sib)

BSI-Warnung Microsoft-Exchange-Server

Stichwörter: IT-Sicherheit, BSI, Microsoft, Exchange, Cyber-Sicherheit