Bundesamt
für Sicherheit in der
Informationstechnik

# BSI warnt: Kritische Schwachstellen in Exchange-Servern

Sofortiges Handeln notwendig!

**Ort**Bonn**Datum**05.03.2021

Zehntausende Exchange-Server in Deutschland sind nach Informationen des IT-Dienstleisters Shodan über das Internet angreifbar und mit hoher Wahrscheinlichkeit bereits mit Schadsoftware infiziert. Betroffen sind Organisationen jeder Größe. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat begonnen, potentiell Betroffene zu informieren. Es empfiehlt allen Betreibern von betroffenen Exchange-Servern, sofort die von Microsoft bereitgestellten Patches einzuspielen.

In der Nacht auf Mittwoch, den 3. März 2021, hat Microsoft kurzfristig neue Sicherheitsupdates für das Produkt „Exchange-Server“ veröffentlicht, mit dem vier Schwachstellen geschlossen werden. Diese werden derzeit aktiv von einer Angreifergruppe ausgenutzt. Sie können über einen Fernzugriff aus dem Internet ausgenutzt werden. Zusätzlich besitzen Exchange-Server standardmäßig in vielen Infrastrukturen hohe Rechte im Active Directory. Es ist denkbar, dass weitergehende Angriffe mit den Rechten eines übernommenen Exchange-Servers potentiell mit geringem Aufwand auch die gesamte Domäne kompromittieren können. Bei Systemen, die bis dato nicht gepatched wurden, sollte von einer Kompromittierung ausgegangen werden. Aufgrund der öffentlichen Verfügbarkeit von sogenannten Proof-of-Concept Exploit-Codes sowie starken weltweiten Scan-Aktivitäten sieht das BSI aktuell ein sehr hohes Angriffsrisiko.

Das BSI empfiehlt dringend das Einspielen der von Microsoft bereitgestellten Sicherheitsupdates. Anfällige Exchange-Systeme sollten aufgrund des sehr hohen Angriffsrisikos dringend auf entsprechende Auffälligkeiten geprüft werden.
Das BSI Lagezentrum arbeitet 24/7. Betroffene Organisationen finden **hier** Informationen.
Informationen zur Warnung finden Sie **hier**.

Erschwerend kommt aktuell hinzu, dass tausende Systeme noch Schwachstellen aufweisen, die seit über einem Jahr bekannt sind und noch nicht gepatched wurden. Insbesondere Kleine und Mittelständische Unternehmen (KMU) könnten hiervon betroffen sein. Neben

dem Zugriff auf die E-Mail-Kommunikation der jeweiligen Unternehmen lässt sich von Angreifern über solche verwundbaren Server-Systeme oftmals auch der Zugriff auf das komplette Unternehmensnetzwerk erlangen.

Im Rahmen seines Engagements zur Erhöhung der IT-Sicherheit bei KMU hat sich das BSI daher heute in einem postalischen Schreiben direkt an die Geschäftsführungen derjenigen Unternehmen gewandt, deren Exchange-Server nach Kenntnis des BSI betroffen sind und darin Empfehlungen für Gegenmaßnahmen gegeben. Kontaktiert wurden mehr als 9.000 Unternehmen. Die tatsächliche Anzahl verwundbarer Systeme in Deutschland dürfte noch deutlich höher liegen.

# Pressekontakt:

*Bundesamt für Sicherheit in der Informationstechnik*
*Postfach 200363*
*53133 Bonn*
*Telefon: +49 228 99 9582-5777*
*Telefax: +49 228 99 9582-5455*
*E-Mail: **presse@bsi.bund.de***