Weltweit Angriffe auf Microsoft Exchange Server

Der großflächige Angriff auf Microsoft Exchange Mailserver ist seit Tagen in verschiedenen Medien Thema. Lt. Informationen von Microsoft steckt die Gruppe Hafnium dahinter. Zahlreiche Server in Unternehmen sind davon betroffen. Doch wie schützt man die den Server und die Daten vor diesem Angriff?

Was passiert bei diesem Angriff?

Die Hacker nutzen die Sicherheitslücken, um sich mit Administratorrechten auf Ihrem Exchange Server anzumelden. In weiterer Folge wird diverse Schadsoftware (z.B. sogenannte Webshells) installiert und damit werden weitere Systeme in Ihrem Netzwerk attackiert. Sobald sich die Infektion ausgebreitet hat, beginnen die Hacker mit der Verschlüsselung der Daten und verlangen Lösegeld.

Welche Server sind betroffen?

Angreifbar sind Exchange-Server, die Unternehmen selbst betreiben. **Exchange Online (= Office 365) ist laut Angaben von Microsoft nicht betroffen.** Die Lücke betrifft alle unterstützten Exchange Versionen gleichermaßen. Die Sicherheitslücke wird für Ihren Server zum Problem, wenn die Funktion Outlook Web Access (OWA) aktiviert haben und die Weboberfläche daher über das Internet erreichbar ist.

Microsoft hat inzwischen ein Test-Skript veröffentlicht, mit welchem überprüft werden kann, ob Ihr Exchange-Server erfolgreich attackiert wurde. Dieses Skript ist nicht zu 100% zuverlässig, aber bietet einen guten Anhaltspunkt welche Maßnahmen notwendig sind. Das Skript können Sie hier herunterladen: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Wie schützt man den Server vor diesen Angriff?

- Ist ein On-Premise Exchange-Server im Unternehmen im Einsatz, ist es wichtig die aktuellste Version einzuspielen, sprich das neueste Kumulative Update (CU) zu installieren. Microsoft hat eine Support-Richtlinie, welche immer nur die beiden neuesten CU-Versionen unterstützt, daher wird der notwendige Patch nur für diese Versionen ausgeliefert.
- Wenn im Unternehmen die Webmail-Funktion von Exchange Server (Outlook Web Access – OWA) nicht genutzt wird, dann sofort deaktivieren. Dadurch können Angreifer die Sicherheitslücke nicht ausnutzen. Lassen Sie die Funktion deaktiviert, außer es arbeitet jemand im Unternehmen damit.
- Mit Sophos kann eine solche Attacke ebenfalls abgewehrt werden. Der Serverschutz erkennt das verdächtige Verhalten und stoppt den Zugriff auf den Exchange Server. Auch eine massenhafte Dateiverschlüsselung erkennt die Endpoint Protection und stoppt die Schadsoftware umgehend.

Kategorien

- Cybersicherheit
- DSGVO Entscheidung
- DSGVO Strafen
- easyGDPR
- Expertentipps
- FAQ
- News