Extrem kritische Exchange-Sicherheitslücke

Weltweiter Angriff auf Microsofts E-Mail-Plattform “Exchange Server”

"Sofortiges Handeln notwendig", forderte das Bundesamt für Sicherheit in der Informationstechnik (BSI). Gleich über mehrere Sicherheitslücken griffen Hacker Exchange-Server an.

Was war eigentlich passiert?

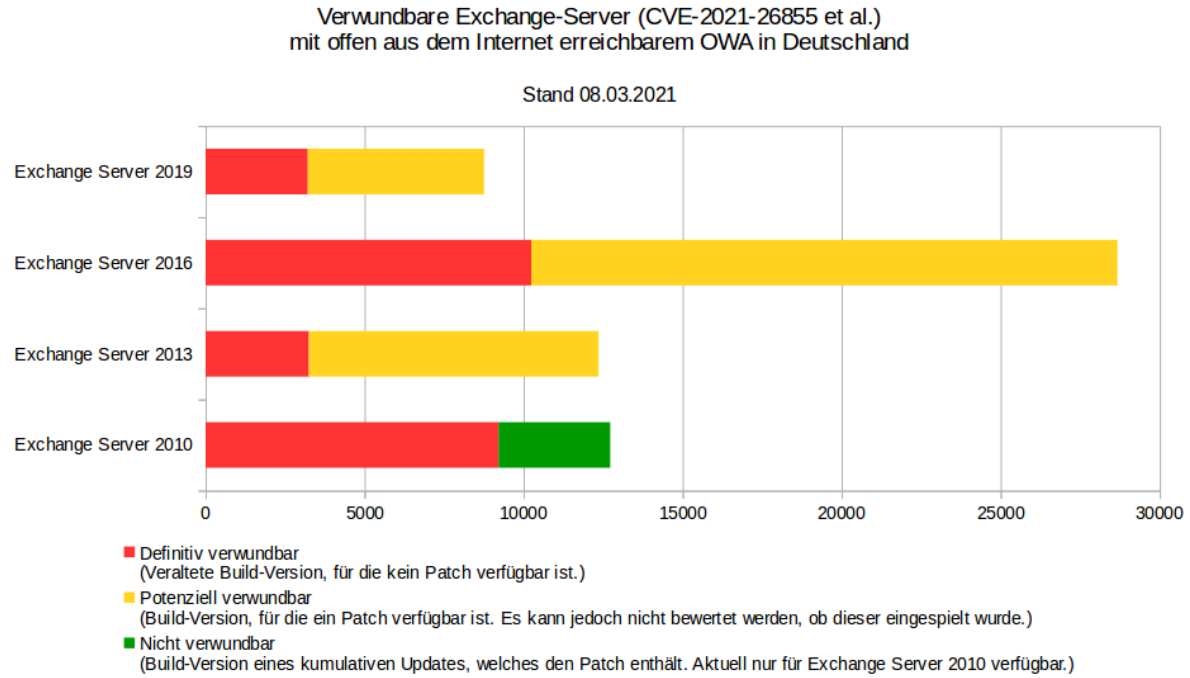
In der Nacht vom 2. auf den 3. März informierte Microsoft darüber, dass auf der E-Mail-Plattform “Exchange Server” Sicherheitslücken entdeckt wurden, die flächendeckend von Hackern zur Datenspionage ausgenutzt wurden.
Microsoft stellte daraufhin außerplanmäßige Updates (sogenannte Patches), umfangreiche Informationen sowie weitere Tools zur Verfügung, um nicht nur die Sicherheitslücken zu schließen, sondern auch, um feststellen zu können, ob Hackern bereits ein erfolgreiches Eindringen in das System gelungen ist.
Eine Woche später stellte Microsoft weitere Patches zur Schließung der Sicherheitslücken zur Verfügung.

Das BSI sprach hierzu die höchste IT-Bedrohungslage der Kategorie 4/rot aus und informierte umfassend zu den Ereignissen.
Nach Einschätzung der Experten sei die IT-Bedrohungslage extrem kritisch. Durch den Ausfall vieler Dienst könne der Regelbetrieb nicht aufrechterhalten werden.*

Wie später bekannt wurde, waren die Sicherheitslücken schon länger bekannt, eine davon seit mindestens Anfang Januar. Damit blieb den Angreifern viel Zeit, diese Lücken zu analysieren und auszunutzen.

Deutsche Unternehmen waren und sind durch die Angriffe besonders gefährdet, da sie im internationalen Vergleich vielfach wichtige Dienste eher lokal als in der Cloud (Bereitstellung von IT-Services über das Internet), betreiben.

Die folgende Grafik (Stand: 8.3.2021) veranschaulicht die Größenordnung der betroffenen Systeme:



Quelle: CERT-Bund

Welche Auswirkungen waren zu verspüren?

Sofern es Angreifern gelungen ist, in die Systeme einzudringen, können nicht nur Daten abgeleitet oder verschlüsselt, sondern die gesamte interne und externe Kommunikation zum Stillstand gebracht werden, da E-Mail-Dienste teilweise eingeschränkt oder gar temporär abgeschaltet werden mussten.

Unternehmen und auch Behörden waren somit von der Außenwelt abgeschnitten, ihre Existenz könnte gar gefährdet werden, da Kommunikation zu den überlebenswichtigen Aspekten gehört.

Welche Maßnahmen sind zu ergreifen?

Als wichtigste Maßnahme sind alle erforderlichen Patches zu installieren.
Alle Systeme sind zu untersuchen, ob sie ggfs. kompromittiert worden sind.

Sofern Ihr System kompromittiert wurde, besteht nach DSGVO eine unverzügliche Meldepflicht an die Landesbeauftragte für den Datenschutz Niedersachsen.

Die aktuellen Informationen und Veröffentlichungen rund um das Thema intensiv weiterverfolgen.

Einen IT-Security-Experten zur Unterstützung hinzuziehen.

Ausblick - wie geht es weiter?

Trotz aller empfohlenen Maßnahmen des BSI und Microsoft kann keine Entwarnung ausgesprochen werden. Die Systeme müssen durch die verantwortlichen IT-Administratoren und Dienstleister weiterhin intensiv beobachtet werden.

Microsoft selbst hält sich zu den Auswirkungen und Vorfällen noch recht bedeckt. Es ist davon auszugehen, dass in Kürze eine Stellungnahme erfolgt.

Sollten Sie Unterstützung benötigen, wenden Sie sich gerne bei Interesse an die cit:

Michael Rode – Senior Consultant
+49 531 180 59 500 m.rode@cit-net.de

Informationen zur i-unit group finden Sie hier:
www.i-unit-group.de

Quelle 1 TLP:White
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf;jsessionid=058EEEE80FA5A2E9591457788DDBAECA.internet472?__blob=publicationFile&v=10