sichtbare Zeichen
gegen unsichtbare Bedrohungen

MGID

+++ Aktuelle Information zu den MS Exchange Schwachstellen +++

Seit dieser Woche kommt man als Unternehmer oder IT-Leiter an einer Nachricht nicht vorbei: Den tausenden kompromittierten MS Exchange-Servern. Die Mitarbeiter der MGID GmbH beraten seit 10 Jahren zu den Themen Datenschutz und Informationssicherheit. Daher geben wir Ihnen folgend eine erste Handreichung, was im Zuge der aktuellen Ausnutzung von Schwachstellen von MS-Exchange Servern nachhaltige Schäden verhindern kann.

Ist mein Unternehmen betroffen?
Sie sind betroffen, wenn Sie einen Exchange Server mit einem von diesem im Internet erreichbaren Port 443 (z.B. Outlook Web Client OWA, ActiveSync) betreiben / betreiben lassen.

Handeln Sie jetzt!
Die zugrundeliegenden Schwachstellen werden seit Wochen automatisiert im großen Stil ausgenutzt. Das BSI ist der Ansicht, dass alle anfälligen Server auch angegriffen wurden. Sollten Sie keine regelmäßigen Sicherungen der Daten erstellen, muss dies unverzüglich geschehen! Speichern Sie diese Daten **offline** auf einem **getrennten Datenträger**!

Führen Sie eine Systemsicherung durch!
Sichern Sie den Server für eine spätere Untersuchung komplett. Läuft dieser in einer virtuellen Maschine, sichern Sie einen Snapshot und kopieren Sie diesen auf einen externen Datenträger. Bei einem physischen Server sichern Sie idealerweise den RAM-Speicher und die angeschlossenen Festplatten bitweise auf externe Datenträger.

Richten Sie das System neu ein!
Installieren Sie offline ein Backup, das idealerweise vor dem 5. Januar 2021, mindestens aber vor dem 26. Februar 2021 erstellt wurde. Patchen Sie das System mit den von Microsoft zur Verfügung gestellten Updates offline. Übertragen Sie die notwendigen gesicherten Daten zurück in das System. Prüfen Sie seit Jahresbeginn neu eingerichtete Nutzer auf Validität.
Ändern Sie die Zugangsdaten für **ALLE** Exchange-Konten!

Zählen Sie auf unsere Hilfe und gehen Sie auf Nummer sicher!
Auch wenn auf den ersten Blick und vielleicht nach Info Ihres IT-Dienstleisters nichts darauf hinweist: Gehen Sie von einer Kompromittierung Ihres Systems aus! Angreifer verwischen ihre Spuren gekonnt. Gerade diesmal ist öffentlich bekannt, welche Spuren hauptsächlich auf den erfolgten Angriff hinweisen können und von den meisten Anwendern untersucht werden sollten.

Die forensische Analyse der MGID ermöglicht das Finden von Spuren, die einen erweiterten Angriff auf Ihre Netzwerkstruktur oder einen möglichen Datenabfluss belegen. Sollten keine derartigen Spuren feststellbar sein, ist ein Angriff zwar noch immer nicht zu 100% auszuschließen, die Notwendigkeit drastischer Maßnahmen wie z.B. der Neueinrichtung der Domäne und Meldungen an die Aufsichtsbehörde und Betroffene nach Art. 33 und Art. 34 DSGVO sind aber damit nicht mehr begründet. Zur Planung notwendiger weiterer Maßnahmen bieten wir Ihnen eine forensische Untersuchung der von Ihnen gesicherten Systeme an. Die forensische Untersuchung wird in Form einer Erstanalyse mit schriftlichem Gutachten zu einem Pauschalpreis von 3500 € pro System/VM bei eigener Übermittlung der Daten angeboten.

Die MGID hat bis zum 31.03.2021 eine 24/7-Rufbereitschaft eingerichtet. Sie erreichen uns unter **0341-96273559**.

Aufgrund der starken Nachfrage werden die Analysen in der Reihenfolge des Eingangs des Auftrags und der Daten bearbeitet.
Das Angebot gilt bis zum 31.03.2021.