soft5check
we identify vulnerabilities others don't

Handlungsempfehlung

Schwere Sicherheitslücken im Exchange-Server gefährden Ihren IT-Betrieb

Die Sicherheitslücken sind inzwischen publiziert; das BSI warnt vor den mit der Bedrohungsstufe 4 ‚Sehr hoch' eingestuften Sicherheitslücken seit dem 3. März.

Was ist zu tun?

Unseren Kunden empfehlen wir die folgenden 8 Schritte:

1. Informieren Sie die Unternehmensleitung über die Brisanz der Angriffe und die möglichen Folgen.

2. Überprüfen Sie den Update-Stand auf Ihren Systemen bzw. bringen Sie Ihre Systeme auf den jüngsten Stand. Dies ist Voraussetzung für alle weiteren Aktivitäten.

3. Setzen Sie zeitnah die beiden Prüfroutinen von Microsoft ein, um zu sehen, ob Sie angegriffen wurden. Bitte sorgen Sie dafür, dass Ihre Mitarbeiter die dazu notwendigen Zugriffs- und Ausführungsrechte erhalten.

4. **Trennen Sie bitte zeitnah Ihre Systeme vom Internet,** wenn die beiden Prüfroutinen zeigen, dass die Sicherheitslücken bei Ihnen ausgenutzt wurden, d.h. dass Sie erfolgreich angegriffen wurden. Sie müssen davon ausgehen, dass seit Januar Backdoors in Ihre Systeme eingebaut wurden, die seitdem beliebig ausgenutzt werden konnten und können, ohne dass Sie es bemerken.

5. Setzen Sie zeitlich parallel Exchange-Server völlig neu auf und spielen Sie das jüngste Backup ein. Schalten Sie diese(n) Server ans Internet und nehmen den üblichen Betrieb auf. Damit erreichen Sie eine kleinst-mögliche Downtime.

6. Kontrollieren Sie den Internetverkehr auf verdächtige Aktivitäten wie unberechtigte Kommunikation. Trennen Sie die IT-Systeme sofort vom Internet, wenn sich Verdachtsmomente ergeben.

7. Forensische Untersuchungen:
   - Untersuchen Sie forensisch die Exchange-Server auf weitere Angriffsspuren.
   - Untersuchen Sie alle IT-Systeme, die im Intranet mit den Exchange-Servern verbunden waren auf verdächtige Aktivitäten – insbesondere auf Backdoors.

8. Wir sind uns im Klaren darüber, dass durch das Abschalten erhebliche Kosten und ggf. Schadensersatzforderungen entstehen können – sind aber zu der Überzeugung gelangt, dass nur das Abschalten Manipulationen an Daten und Software (Sabotage) und Kopieren von Daten und Software (Spionage) verhindern kann. Informieren Sie Kunden, Partner und Mitarbeiter über diesen Schritt und erläutern ihn. Stellen Sie sich auf diesen Maßnahmen entsprechende Diskussionen ein und halten Sie Ihre Unternehmensleitung informiert. Die Angreifer sind nicht die immer noch kolportierten Schüler und Studenten, sondern Unternehmen mit 20 bis über 100 ausgewiesenen Fachleuten; von dieser Art Unternehmen gibt es weltweit mehr als 200.

Das (unverzichtbare!) Patchen beendet nicht den Angriff, wenn Backdoors eingebaut wurden.

Dass das chinesische Unternehmen Hafnium einer der Angreifer sein soll, halten wir für irrelevant. Dass die [1]Angriffe Programm-gesteuert (automatisiert) durchgeführt werden, steigert allerdings die Wahrscheinlichkeit zu den Opfern zu gehören.