SAP-Systeme sind ein beliebtes Ziel für Cyberkriminelle[1]

Der Grad der Vernetzung nimmt nicht nur in unserer Gesellschaft, sondern auch in der Wirtschaft stark zu. Die Digitalisierung hat nahezu alle Bereiche unseres Lebens erreicht. Unsere Wohnungen werden mit Alexa & Co. stetig smarter. In der Geschäftswelt ist es die vierte industrielle Revolution „Industrie 4.0“, welche die Vernetzung von Maschinen, Geräten und Sensoren anstrebt – Der Mensch verliert immer mehr den Einfluss und wird unbewusst zur Zielscheibe für Cyberkriminelle.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ermittelt, dass im Jahr 2019 etwa 114 Millionen neue Schadprogrammvarianten im Umlauf waren. In Summe sind es mehr als 800 Millionen Schadprogrammvarianten. Täglich gibt es bis zu 110.000 Bot Infektionen in deutschen Systemen. Allein ein einzelnes Unternehmen erlitt 2019 durch einen Ransomware-Angriff einen Schaden in höhe von 40 Millionen Euro. Die Geschwindigkeit der Angriffe erreichte dabei in den Peaks eine Angriffsbandbreite von über 390 Gbit/s über die Cloud. Zum Vergleich lag der Wert 2018 noch unter 100 Gbit/s.[2]

Diese Statistiken machen deutlich, dass ein Investment in die Sicherheit der Systeme zwingend erforderlich ist und eine Vernachlässigung an Fahrlässigkeit grenzt.

SAP-Systeme zählen zu den „beliebten“ Systemen für Datenklau und Prozessmanipulationen. Die Möglichkeiten ein SAP-System anzugreifen sind vielfältig und einfach. Angefangen bei der Ausnutzung & Manipulation von Standartfunktionen und Funktionsbausteinen bis hin zu Schwachstellen und Hintertüren im SAP Gateway sowie Java-Portalen.

Im Internet finden sich zahlreiche Anleitungen, die es selbst ungeübten Angreifern ermöglichen einen Zugriff auf SAP-Systeme zu erlangen.

Um ein System ausreichend schützen zu können sind viele Punkte zu beachten und stringent umzusetzen. Dazu gehören zum Beispiel ausgeprägte Sicherheits- und Berechtigungs-konzepte, sowie eine strikte Entwicklerrichtlinie.

Weiterhin ist eine verschlüsselte Kommunikation via SNC Client Encryption® (Secure Network Communications) unabdingbar, um vor unbefugten Personen geschützt zu werden, die

[1] Quelle: it-daily.net
[2] Quelle: bsi.bund.de

vorhaben, Informationen wie Anmeldedaten oder Geschäftsdaten zu erhalten oder zu manipulieren. [3]

Auch ein regelmäßiges Patchen der SAP-Systeme ist erforderlich, um ein Mindestmaß an Sicherheit gewährleisten zu können, da diese Sicherheitslücken natürlich zum Veröffentlichungszeitpunkt auch potenziellen Angreifern bekannt gemacht werden.

Darüber hinaus hilft eine großzügige Protokollierung und entsprechende nachgelagerte Kontrolle, um individuelle Schwachstellen in der Sicherheit zu identifizieren und Methoden zur Mitigation zu entwerfen.

Produkte wie SAP-Governance, Risk & Compliance (GRC)® können hilfreiche Werkzeuge sein, um Bereiche der Berechtigungsverwaltung und Protokollierung von kritischen Tätigkeiten im SAP Umfeld zu managen.[4]

Die hier aufgezählten Aspekte sind nur ein Teil einer großen Bandbreite an Maßnahmen, die die Sicherheit ihrer SAP-Systeme erhöhen können.

Wir als Beratungshaus legen sehr großen Wert darauf, dass unsere Mitarbeiter zum Thema Security kontinuierlich weitergebildet werden, um stets am Puls der Zeit zu agieren, damit unseren Kunden die bestmöglichsten Lösungen angeboten werden können.

Möchten Sie sich unverbindlich über Security-Maßnahmen rundum SAP-Systeme informieren?

So kontaktieren Sie uns einfach:

matrix Systems & Consulting GmbH
Industriestraße 50B
D-69190 Walldorf

Tel. +49 (0) 6226 / 84 11 85
E-Mail: info@matrix-sc.de

[3] Quelle: SAP.com
[4] Quelle: SAP.com