Sicherheit von SAP-Systemen – kontinuierliche Inventarisierung von Sicherheitslücken erforderlich

Der Zugriff auf unternehmenskritische Daten und Anwendungen ermöglicht Betrug, verhindert Compliance und bedroht den Erfolg eines Unternehmens. Ganz real ist dabei die Gefahr für SAP-Systeme. Laut einer Studie des Ponemon-Instituts vom Februar 2016 räumen zwei von drei befragten Unternehmen ein, dass ihre SAP-Plattform innerhalb der letzten zwei Jahre mindestens einmal angegriffen wurde. Dabei entstand laut der Studienteilnehmer ein durchschnittlicher Gesamtschaden von 4,5 Millionen USD.

ILaut der unabhängigen Organisation BIZEC ist der Einsatz nicht aktualisierter, nicht gepatchter Software der größte aller Risikofaktoren gefolgt von der Verwendung von Standard-Usern mit Default-Passwörtern. Daneben spielen noch ungesicherte Gateways, gefährliche SAP-Web-Applikationen und unzureichend geschützte Administrationsdienste eine Rolle.

Durch die Komplexität individueller SAP-Implementierungen und Fehlkonfigurationen entstehen Schwachstellen, die unter anderem Betrug und Sabotage durch externe Angreifer und eigene Mitarbeiter ermöglichen. Diese kapern sich beispielsweise Profile mit sehr umfassenden Berechtigungen, können damit neue Kreditoren fingieren und sich regelmäßig kleinere unauffällige Beträge überweisen und dabei unerkannt bleiben. Viel gefährlicher ist der Zugriff auf sensible Daten bzw. Interna. Der schlimmste Fall ist die Sabotage des SAP-Systems, das Verändern oder Löschen von Informationen, was unter Umständen die Existenz eines Unternehmens bedroht.

Allein durch die zügige Implementierung neuer SAP-Patches können laut Expertenschätzung bis zu 80 % aller Angriffe verhindert werden. Ein fehlender Überblick über die Gefahrenlage, mangelndes Sicherheitsbewusstsein sowie unklare Zuständigkeiten charakterisieren jedoch die aktuelle SAP-Ungewissheit in vielen Unternehmen. Es fehlen oftmals Ressourcen, Technologien, Personal und Zeit. Viele Verantwortliche erliegen dem Trugschluss, ein System wie SAP sei mit seiner hohen Komplexität vor Angriffen geschützt. Ebenfalls sind sich wenige bewusst, dass das SAP-System kein internes Netzwerk ist, sondern in vielen weiteren Anwendungen integriert ist und so eine weitreichende Sicherheitspolitik verlangt. Schlecht verteilte oder im schlimmsten Fall keine eindeutigen Zuständigkeiten für die SAP-Sicherheit vervollständigen dieses Bild. Diese soeben beschriebene Ungewissheit können sich gerade Unternehmen mit ihren Compliance-Verpflichtungen nicht leisten.

Eine SAP-Sicherheit muss auf neue Grundlagen gestellt werden. Um dieses Problem zu lösen, sehen viele Experten die Nachfrage nach einer automatisierten, kontinuierlichen Inventarisierung aller Sicherheitslücken in den SAP-Implementierungen und verlangen Lösungen zu Abwehr von Angriffen. Das ist umso wichtiger, weil SAP-Anwendungen häufig unternehmenskritische Anwendungen und Daten verwalten, die ein lukratives Ziel für alle Angreifer sind. Denn alle digitalen Angriffsmöglichkeiten, die auch in der klassischen IT möglich sind, werden auch auf SAP-Systeme übertragen und angewendet.