



PRESSEMITTEILUNG

NIS2 und SAP: Hinweise für Anwenderunternehmen

DSAG unterstützt die Umsetzung der NIS2-Richtlinie

Walldorf, 19.11.2024 – Die Deutschsprachige SAP-Anwendergruppe e. V. (DSAG) sieht in der Umsetzung der EU-Richtlinie zur Netz- und Informationssicherheit (NIS2) durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) eine bedeutende Chance, das Sicherheitsniveau in der deutschen und europäischen Unternehmenslandschaft zu erhöhen. Geplant ist das Inkrafttreten im März 2025. Dann gilt es, Maßnahmen zügig umzusetzen, um die Einhaltung der Anforderungen sicherzustellen. Die DSAG unterstützt Unternehmen bei der Umsetzung dieser Vorgaben, insbesondere im Hinblick auf die IT-Sicherheitsanforderungen im SAP-Umfeld. Hierzu hat der Verband z. B. ein [NIS2-Positionspapier](#) erstellt.

Die NIS2-Richtlinie erweitert den Geltungsbereich der Cybersicherheitsverpflichtungen erheblich: Neben den klassischen kritischen Infrastrukturen (KRITIS) betrifft sie künftig rund 6.000 Betreiber kritischer Anlagen und circa 24.000 „wichtige und besonders wichtige Einrichtungen“ in Deutschland. Dies schließt auch Unternehmen aus der Fertigung und Dienstleistung ein, die in kritischen Wertschöpfungsketten tätig sind. „Als DSAG begrüßen wir diesen Schritt und sehen in der Umsetzung durch das NIS2UmsuCG eine notwendige Reaktion auf das hohe Risiko durch Cyber-Angriffe und deren rasant zunehmende Zahl“, so Sebastian Westphal, DSAG-Technologievorstand.

NIS2-Umsetzung in SAP-Umgebungen

Wenngleich NIS2 kein spezifisches SAP-Thema ist, so ergibt sich für Anwenderunternehmen durch die neuen Regelungen eine Vielzahl an Handlungsfeldern. „Die DSAG setzt sich dafür ein, dass SAP seine Anwenderunternehmen mit spezifischen Sicherheitsrichtlinien und Maßnahmen zur Absicherung der IT-Infrastrukturen im Sinne der NIS2-Vorgaben unterstützt“, sagt Westphal. Dazu gehören aus DSAG-Sicht unter anderem:

PRESSEMITTEILUNG

- **Guidelines zur Sicherheitsoptimierung:** Unternehmen benötigen mehr denn je klare Richtlinien für IT-Sicherheit, die Entwicklungsstandards für SAP-Programme, Berechtigungsprüfungen sowie sichere Vergabe von Passwörtern und Benutzerrechten umfassen.
- **Absicherung der Integrationschnittstellen:** Sicherheitsmaßnahmen wie die Absicherung von RFC-Verbindungen und die Einführung eines lückenlosen Monitorings über das SAP Gateway sind essenziell.
- **Compliance und Governance für hybride SAP-Umgebungen:** Hybride Architekturen erfordern ein umfassendes Berechtigungsmanagement, um SOD-Konflikte (Segregation of Duties) zu verhindern und Compliance-Anforderungen zu erfüllen.

Verantwortung der Geschäftsleitung und neue Governance-Anforderungen

Neben technischen Sicherheitsmaßnahmen rückt die NIS2-Richtlinie auch die Verantwortung der Geschäftsleitung stärker in den Fokus. Führungskräfte sind zukünftig verpflichtet, sich in Sachen Cybersicherheit fortzubilden und Verantwortung für den Schutz von Netz- und Informationssystemen zu übernehmen. „Die Verantwortung der Geschäftsleitung ist ein entscheidender Aspekt. Cybersicherheit ist nicht nur eine technische, sondern auch eine Managementaufgabe“, kommentiert Westphal.

DSAG sieht SAP ebenfalls in der Verantwortung

Insgesamt ist aus DSAG-Sicht unabdingbar, dass SAP die Implementierung einheitlicher Sicherheitsstandards ermöglicht und ein stringentes Release-Management bietet – sowohl On-Premises als auch in der Cloud. „Sicherheit muss bei SAP als Standard gelten – für alle Lösungen. Das bedeutet, dass Systeme von vornherein so konfiguriert sein sollten, dass sie den Vorgaben von NIS2 und konkret denen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie Prüfungsempfehlungen externer Auditoren der Anwenderunternehmen entsprechen“, fasst Westphal zusammen. Im Rahmen der Betriebsmodelle SAP RISE und SAP GROW ist künftig zudem anstelle des heutigen isolierten SAP-zentrischen Betriebsmodells eine starke Integration mit den ITSM-Prozessen, dem Business



PRESSEMITTEILUNG

Continuity- und dem Notfallmanagement der Anwenderunternehmen sicherzustellen.

Handlungsbedarf und DSAG-Unterstützung

Fakt ist, dass SAP-Anwenderunternehmen aufgrund von NIS2 vor neuen Cybersicherheitsanforderungen stehen. Aus DSAG-Sicht ist das auch eine Chance für die Unternehmen, ihre Sicherheitsmaßnahmen zu optimieren. Unterstützen sollte SAP dabei mit einheitlichen Sicherheitsstandards und -richtlinien, sodass Systeme bereits voreingestellt den NIS2-Vorgaben entsprechen. Das gilt sowohl für hybride, als auch für Cloud-basierte Architekturen.

Das vollständige DSAG-Positionspapier zu NIS2-Positionspapier gibt es [hier](#).



PRESSEMITTEILUNG

Alle aktuellen DSAG-Positionen finden Sie im [DSAG-Pressezentrum](#).

Über die DSAG

Die Deutschsprachige SAP-Anwendergruppe e. V. (DSAG) ist einer der einflussreichsten Anwenderverbände der Welt. Über 4.000 Mitgliedsunternehmen und mehr als 70.000 Mitgliedspersonen bilden ein starkes Netzwerk, das sich vom Mittelstand bis zum DAX-Konzern und über alle wirtschaftlichen Branchen in Deutschland, Österreich und der Schweiz (DACH) erstreckt. Auf Basis dieser Reichweite gewinnt der Industrieverband fundierte Einblicke in die digitalen Herausforderungen im DACH-Markt. Die DSAG nutzt diesen Wissensvorsprung, um die Interessen der SAP-Anwender zu vertreten und ihren Mitgliedern den Weg in die Digitalisierung zu ebnen. Weitere Informationen finden Sie unter:

www.dsag.de, www.dsag.at, www.dsag-ev.ch

Ansprechpartner für die Presse

DSAG

Thomas Kircher, Julia Theis, Dana Walter
Deutschsprachige SAP® Anwendergruppe (DSAG) e. V.

Altrottstraße 34a

69190 Walldorf

Telefon: +49 151 25630665

E-Mail: presse@dsag.de

Internet: www.dsag.de