topics.watch Wochenreport

Ausgabe im Überblick

Priorität	Anbieter	Kategorie	Ereignis
HOCH	**Microsoft**	Pricing	M365-Suites-Preiserhöhung ab 1. Juli 2026 — CHF-Dreijahres-Commitments vor 1. Juni abschließen
HOCH	**SAP**	Produkt	S/4HANA Compatibility Packs laufen zum 31. Mai 2026 ab — Migrationsstatus jetzt schriftlich bestätigen
MITTEL	**Adobe**	Produkt	Adobe Analytics: TLS-1.2-Cipher-Suite-Entfernung am 27. Mai 2026 abgeschlossen — Legacy-Clients prüfen
MITTEL	**Microsoft**	Security	Secure-Boot-Zertifikatsablauf am 26. Juni 2026 und Netlogon-RCE (CVSS 9,8) — Validierung und Patching vor Fristende
MITTEL	**SAP**	Security	SAP Patch Day 12. Mai 2026: CVSS-9,6-SQL-Injection in S/4HANA — Patches sofort einspielen
NIEDRIG	**Microsoft**	Partner Program	Microsoft Marketplace-Nutzungsbedingungen am 27. Mai 2026 automatisch aktualisiert — Procurement-Prüfung empfohlen
NIEDRIG	**SAP**	M&A	SAP schließt am 28. Mai 2026 Eurobond über 3,5 Mrd. EUR ab — M&A-Kurs signalisiert Bündelungsdruck

Dieser Report erfasst Vorgänge bei den beobachteten Anbietern mit unmittelbarer Bedeutung für die Beschaffung: (1) Meldungen, Bekanntmachungen und Berichte, die im genannten Recherchezeitraum öffentlich wurden; (2) frühere Vorgänge, deren Frist oder beschaffungsrelevanter Termin in diesen Zeitraum fällt; (3) laufende Vorgänge, deren Status sich verändert hat.

Meldungen

Adobe — Produkt

MITTEL — Adobe Analytics: TLS-1.2-Cipher-Suite-Entfernung am 27. Mai 2026 abgeschlossen — Legacy-Clients prüfen

Adobe entfernte am 27. Mai 2026 die Unterstützung für bestimmte TLS-1.2-Cipher-Suites von den Adobe Analytics-Datenerfassungsservern (**Adobe Experience League**). Für die meisten Implementierungen ist laut Adobe keine Maßnahme erforderlich.

Betroffen sind Organisationen, die Analysedaten über veraltete native Anwendungen mit überholten TLS-Bibliotheken oder über Legacy-Browser und -Betriebssysteme senden. Adobe begründet die Änderung mit der Angleichung an moderne Verschlüsselungsstandards.

IT-Teams mit Adobe-Analytics-Deployments sollten jetzt prüfen, ob proprietäre Datenerfassungs-Clients, On-Premise-Middleware oder ältere mobile Applikationen im Einsatz sind, die ausschließlich die am 27. Mai 2026 entfernten Cipher-Suites unterstützen. Für Standard-Web-Implementierungen und aktuelle Creative-Cloud-Clients besteht kein Handlungsbedarf.

Was wir beobachten

- Datenerfassungs-Clients auf TLS-Bibliotheksversion prüfen — insbesondere native Anwendungen und On-Premise-Middleware, die Daten an Adobe Analytics senden.
- Beim nächsten Adobe-Analytics-Verlängerungsgespräch den Support-Zeitplan für ältere SDK-Versionen erfragen, um weitere Cipher-Suite-Abschaffungen frühzeitig zu erkennen.

TW-26W22-32-003

Microsoft — Pricing

HOCH — M365-Suites-Preiserhöhung ab 1. Juli 2026 — CHF-Dreijahres-Commitments vor 1. Juni abschließen

Confidence: High - official vendor source.

Microsoft kündigte am 4. Dezember 2025 an, die Preise für Microsoft 365 Commercial Suites und ausgewählte Standalone-Komponenten — darunter Office 365 E3, Microsoft 365 E3/E5, Business, Frontline und Government-Äquivalente — zum 1. Juli 2026 weltweit anzuheben (**Microsoft Licensing**). Kunden, die vor dem 1. Juli 2026 verlängern, können laut offizieller FAQ den aktuellen Preis bis zur nächsten Vertragsverlängerung einfrieren (**Microsoft Licensing FAQ**).

DACH-spezifisch: Laut Partner Center Mai 2026 wird Microsoft ab dem 1. Juni 2026 den CHF-Preis für die Microsoft 365 E3 Prepaid Three-Year-Commitment-SKU anpassen, um ihn rechnerisch mit dem Einjahres-Commitment-Äquivalent über drei Jahre gleichzusetzen (**Partner Center Mai 2026**). CSP-Partner, die in Schweizer Franken transagieren, sollten betroffene Dreijahresangebote vor dem 1. Juni 2026 abschließen; danach steigt dieser SKU-Preis (**cloudcockpit.com**).

Was wir beobachten

- Microsoft-365-Verlängerungen (E3/E5, Business, Frontline), die nach dem 1. Juli 2026 fällig werden, vor diesem Datum neu kalkulieren und gegebenenfalls vorzeitig erneuern, um den aktuellen Preis zu sichern
- CHF-Transaktionen für M365-E3-Dreijahres-Commitments vor dem 1. Juni 2026 abschließen, um die laufende Preisanpassung zu vermeiden

TW-26W22-32-002

Microsoft — Security

MITTEL — Secure-Boot-Zertifikatsablauf am 26. Juni 2026 und Netlogon-RCE (CVSS 9,8) — Validierung und Patching vor Fristende

Laut Fachpresse-Analysen zum Patch-Tuesday-Zyklus vom 12. Mai 2026 läuft am 26. Juni 2026 ein kritischer Secure-Boot-Zertifikatsablauf ab; Windows-Umgebungen müssen die Zertifikatsvalidierung vor dem 26. Juni 2026 abschließen, um Systemstartunterbrechungen zu vermeiden (**Help Net Security**, **Zecurit**).

Das offizielle MSRC-Update-Guide für Mai 2026 führt zudem CVE-2026-41089 auf — eine vorauthentifizierungsfreie Remote-Code-Execution-Schwachstelle im Windows-Netlogon-Dienst mit einem CVSS-Wert von 9,8, die alle als Domänencontroller betriebenen Windows-Server betrifft (**MSRC Mai 2026**, **Tenable**). Der Mai-2026-Patch für CVE-2026-41089 sollte vor dem nächsten regulären Wartungsfenster auf allen Domänencontrollern eingespielt sein.

Was wir beobachten

- Secure-Boot-Zertifikatsvalidierung in allen Windows-Umgebungen vor dem 26. Juni 2026 durchführen und Testergebnis intern dokumentieren
- Patch-Status für CVE-2026-41089 (Netlogon RCE, CVSS 9,8) auf allen Domänencontrollern vor dem nächsten regulären Wartungsfenster überprüfen

TW-26W22-32-005

Microsoft — Partner Program

NIEDRIG — Microsoft Marketplace-Nutzungsbedingungen am 27. Mai 2026 automatisch aktualisiert — Procurement-Prüfung empfohlen

Microsoft aktualisierte am 27. Mai 2026 die Nutzungsbedingungen des Microsoft Marketplace automatisch und ohne erforderliche Zustimmung der Partner; Signatur oder Bestätigung waren nicht notwendig (**Partner Center Mai 2026**). Die Aktualisierung dient laut Microsoft der Anpassung an aktuelle Geschäftspraktiken und regulatorische Anforderungen.

Procurement- und Legal-Teams sollten die am 27. Mai 2026 in Kraft getretenen aktualisierten Bedingungen auf Relevanz für bestehende Co-Sell-Vereinbarungen und laufende Marketplace-Transaktionen prüfen.

Was wir beobachten

- Aktualisierte Marketplace-Nutzungsbedingungen (wirksam 27. Mai 2026) auf Relevanz für bestehende Procurement- und Co-Sell-Vereinbarungen prüfen

TW-26W22-32-007

SAP — Produkt

HOCH — S/4HANA Compatibility Packs laufen zum 31. Mai 2026 ab — Migrationsstatus jetzt schriftlich bestätigen

Confidence: Medium - trade press reporting.

Laut Fachpresse-Berichten verlängerte SAP die Nutzungsrechte für Compatibility Packs für On-Premises-S/4HANA-Kunden einmalig vom 31. Dezember 2025 auf Ende Mai 2026 (**ERP.today**). SAP hat diesen Stichtag als endgültig kommuniziert und eine weitere Verlängerung ausgeschlossen.

Ausblick zum 2026-05-28: Am 31. Mai 2026 enden die Nutzungsrechte für Compatibility Packs ohne weiteren Aufschub. Kunden, die bis zum 31. Mai 2026 keine Ablösefunktionen in SAP-Cloud-Lösungen aktiviert haben, verlieren den Zugang zu klassischen SAP-ERP-Funktionen innerhalb von S/4HANA.

Beschaffungsseitig besteht unmittelbarer Handlungsbedarf: Betriebsteams müssen offene Compatibility-Pack-Abhängigkeiten identifizieren und entweder auf native S/4HANA-Cloud-Prozesse migrieren oder gemeinsam mit dem SAP-Account-Team vor dem 31. Mai 2026 eine individuelle Ausnahmeregelung schriftlich beantragen. Fehlt die Migration zum Stichtag, drohen operative Unterbrechungen in Buchhaltungs-, Beschaffungs- und Logistikprozessen.

Was wir beobachten

- Bis Ende Mai 2026 offene Compatibility-Pack-Abhängigkeiten im eigenen S/4HANA-Mandanten vollständig inventarisieren und Migrationsstatus mit dem SAP-Account-Team schriftlich bestätigen.
- Falls die Migration nicht rechtzeitig abschließbar ist, vor dem 31. Mai 2026 beim SAP-Account-Manager eine individuelle Ausnahmevereinbarung schriftlich beantragen.

TW-26W22-32-001

SAP — Security

MITTEL — SAP Patch Day 12. Mai 2026: CVSS-9,6-SQL-Injection in S/4HANA — Patches sofort einspielen

SAP veröffentlichte am 12. Mai 2026 auf dem monatlichen Patch Day 15 neue Sicherheitshinweise, darunter zwei HotNews-Hinweise mit CVSS-Wert 9,6 und einen High-Priority-Hinweis mit CVSS 8,2 (**SAP Security Support**).

Den Kopf des Release vom 12. Mai 2026 bildet SAP Security Note 3724838 (CVE-2026-34260): eine SQL-Injection-Schwachstelle in SAP S/4HANA Enterprise Search for ABAP, die authentifizierten Angreifern mit niedrigen Rechten den Zugriff auf vertrauliche Datenbankdaten ermöglicht; SAP gibt keinen Workaround an —

die Behebung erfordert das Einspielen des Korrektur-Pakets (**Layer Seven Security**).

Ein zweiter HotNews-Hinweis (Note 3733064, CVE-2026-34263, CVSS 9,6) betrifft SAP Commerce Cloud: eine fehlende Authentifizierungsprüfung erlaubt nicht authentifizierten Angreifern das Hochladen bösartiger Konfigurationsdateien und die anschließende serverseitige Code-Ausführung (**Onapsis**). Zusätzlich adressierte Note 3747787 einen Supply-Chain-Angriff auf SAP-npm-Pakete (CAP-Modell), der laut SAP am 29. und 30. April 2026 aktiv war; betroffene Entwicklungssysteme könnten Cloud-Zugangsdaten und CI/CD-Secrets exponiert haben.

Was wir beobachten

- SAP Security Note 3724838 (S/4HANA Enterprise Search) sofort einspielen — kein Workaround verfügbar; Priorität auf Produktionssystemen mit breitem Benutzerzugang.
- Commerce-Cloud-Patch für Note 3733064 auf Release 2205.49 / 2211.51 / 2211-jdk21.10 heben und Redeploy abschließen.
- Falls SAP-CAP- oder MTA-Build-Tool-Pakete genutzt werden: Prüfen, ob im Zeitfenster 29.–30. April 2026 kompromittierte npm-Pakete geladen wurden, und Zugangsdaten sowie CI/CD-Secrets rotieren.

TW-26W22-32-004

SAP — M&A

NIEDRIG — SAP schließt am 28. Mai 2026 Eurobond über 3,5 Mrd. EUR ab — M&A-Kurs signalisiert Bündelungsdruck

SAP SE schloss am 28. Mai 2026 eine Eurobond-Transaktion über insgesamt 3,5 Mrd. EUR in vier Tranchen mit Laufzeiten von zwei, drei, fünf und sieben Jahren ab (**SAP Investor Relations**). Die Nettoerlöse dienen laut SAP allgemeinen Unternehmenszwecken einschließlich der (Re-)Finanzierung zuletzt angekündigter Akquisitionen — konkret der im Mai 2026 abgeschlossenen Übernahme von Reltio sowie der angekündigten Übernahmen von Dremio und Prior Labs (Ankündigung Mai 2026, Abschluss ausstehend). SAP ist mit A1-stabil (Moody's) und A+/stabil (S&P Global) geratet.

Ausblick zum 2026-05-28: Der Abschluss der Dremio- und Prior-Labs-Übernahmen steht noch aus. SAP finanziert seinen M&A-Kurs über die Kapitalmärkte, ohne die operative Ertragsstärke zu beanspruchen. Angesichts eines Cloud-Umsatzwachstums von 27 % im Q1 2026 (gemeldet am 23. April 2026) und eines laufenden Cloud-Backlogs von 21,93 Mrd. EUR bleibt die Vendor-Stabilität auf kurze Sicht unkritisch. Käufer sollten beobachten, ob der Akquisitionshunger sich in Bündelungsdruck oder Lizenzmodell-Verschiebungen — insbesondere rund um SAP Business Data Cloud und die Sapphire-Plattform-Ankündigungen vom 12. Mai 2026 — niederschlägt.

Was wir beobachten

- Verfolgen, ob die integrierten Reltio- und Dremio-Funktionen in neue Pflichtbündel oder überarbeitete Preismodelle für SAP Business Data Cloud-Abonnements einfließen.
- Bei anstehenden SAP-Verlängerungen die Roadmap-Kommunikation zu Dremio- und Prior-Labs-Integration schriftlich bestätigen lassen, um spätere Lizenz-Scope-Änderungen nachweisbar zu machen.

TW-26W22-32-006

Dieser Briefing-Bericht zitiert 14 öffentliche Quellen, alle inline verlinkt.

Über diesen Dienst — topics.watch wird von KI-Agenten unter menschlicher redaktioneller Aufsicht erstellt. Der Dienst erfasst öffentlich verfügbare Informationen über benannte juristische Personen — Anbieter, Konzernmütter, Aufsichtsbehörden, Vertragspartner. Öffentliche Quellen können natürliche Personen benennen (Führungskräfte, Amtsträger, Verfahrensbeteiligte, Journalisten, Analysten), soweit sie Teil eines Anbietereereignisses sind; wir verwenden diese Information ausschließlich zur Erklärung des Ereignisses und legen keine Profile oder Dossiers zu Personen an und erheben keine nicht-öffentlichen personenbezogenen Daten. Empfänger sind für die eigene Verwendung dieses Materials nach geltendem Datenschutzrecht selbst verantwortlich. KI-Ergebnisse können Fehler enthalten — wir gewährleisten weder Richtigkeit noch Vollständigkeit oder Aktualität, und Empfänger müssen kritische Punkte vor einer Handlung unabhängig prüfen. Nichts in diesem Bericht stellt eine Rechts-, Finanz- oder Anlageberatung dar. Kontakt: briefing@topics.watch

Wie dieser Briefing-Bericht entsteht — Recherche, Erstellung und Faktenprüfung erfolgen durch KI-Agenten unter menschlicher redaktioneller Aufsicht. Mehrere Prüfdurchgänge verringern Fehler, schließen sie aber nicht aus. Sollte etwas unstimmig wirken, antworten Sie bitte — wir korrigieren in der nächsten Ausgabe.