S@PPORT

Entscheidungsgrundlagen für Auswahl, Installation und Betrieb von SAP*-Lösungen

AUSGABE 1-2_2022 | 9,50 EURO

ISSN 2190-118X

AUF DER DIGITALISIERUNGSREISE

OPTIMIERUNG VON SAP-SYSTEMEN UND -PROZESSEN

Im Jahr 2022 entscheidet sich, ob die Digitalisierung von Wirtschaft und Gesellschaft erfolgreich sein wird. Einerseits haben die Maßnahmen gegen die Corona-Pandemie die Digitalisierung vorangebracht – andererseits hat die Pandemie gezeigt, in welchem Maße Industrien oder auch die Gesundheitsbranche mit veralteten Technologien und ungenügenden Abläufen arbeiten. Jetzt heißt es, die Analysen zu sichten, zu beurteilen, in den Systemen aufzuräumen.

AB SEITE 13

4 196155 608508

TITEL Schwachstellen innerhalb von IT-Landschaften: SAP-Security verknüpft Netzwerk- und Applikationssicherheit Seite 13

SOLUTIONS Shortage Economy: Fünf Faktoren für ein robustes Lieferantennetzwerk Seite 30

BRANCHEN Logistik in der Automobilindustrie: Übersicht über die Entwicklung der IT-Prozesse und Jobanforderungen Seite 36

BRANCHEN Digitalisierung bei Daimler: Vertragsmanagement ist strategisches Element der Transformation Seite 39

*SAP ist ein eingetragenes Warenzeichen der SAP SE

Manipulation im Transportprotokoll

Höhere Sicherheit bei der Softwareverteilung

Bildquelle: Pixabay

Der IT-Hersteller Security Bridge hat eine Methode identifiziert, die es internen Angreifern ohne privilegierte Berechtigungen ermöglicht, unbemerkt in den Prozess der SAP-Softwareverteilung einzugreifen. Die Vulnerability wurde an SAP gemeldet, der entsprechende Patch ist bereits veröffentlicht, bestenfalls sogar schon im Kundensystem eingespielt.

Über die interne SAP Development Supply Chain können Kunden Einfluss auf die Ergänzung des SAP-Standards um gewünschte Funktionen und Eigenentwicklungen nehmen. Solche Codierungs- und Repository-Änderungen werden über die verschiedenen Staging-Systeme der jeweiligen SAP-Landschaft mittels SAP-Transportaufträgen bereitgestellt. Die Transportdateien werden benötigt, um Änderungen von der Entwicklung bis zur nächsten Staging-Ebene physisch bereitzustellen. Die Aufträge dürfen nach ihrem Export aus dem zentralen Transportverzeichnis – welches sich Entwicklungs-, Test- und Integrationsinstanzen in der Regel teilen – und ihrer Freigabe nicht mehr verändert werden.

Einschleusen von Schadcode in die SAP-Entwicklungsphase verhindern

Ende 2021 hatte Security Bridge mittels seiner SAP-Security-Plattform eine Methode entdeckt, die es internen Angreifern ohne privilegierte Berechtigungen ermöglicht, in diese SAP Software Supply Chain einzudringen. Unmittelbar nach dem Export eines Transportauftrags und vor dem Import in das nachfolgende Staging-System existierte ein Zeitfenster, während dessen jemand mit betrügerischer Absicht und ausreichenden Berechtigungen den Status des Transportauftrags von „freigegeben" auf „modifizierbar" ändern und dadurch Schadcode in die SAP-Entwicklungsphase hätte einschleusen können – sogar in Transportaufträge, die bereits in das Testsystem importiert wurden. Der Inhalt des Transportauftrags konnte kurz vor dem Import in die Produktion unbemerkt geändert werden, um die Codeausführung zu ermöglichen.

SAP-Sicherheitspatch

Ivan Mans, CTO von Security Bridge: „Solche Angriffe sind sehr effizient, insbesondere wenn sich die verschiedenen SAP-Staging-Systeme ein einziges Transportverzeichnis teilen. Ein Angriff auf die SAP Development Supply Chain ist dadurch sehr einfach möglich." SAP habe den Patch im Sicherheitshinweis „SNOTE 3097887– [CVE-2021-38178] Improper Authorization in SAP NetWeaver AS ABAP and ABAP Platform E" im Rahmen des SAP Security Patch Day am 12. Oktober 2021 mit einer Hot News Priority (CVSS 9.1) bereitgestellt. Dadurch könne laut Mans jetzt das Dateisystem vor Manipulation geschützt werden. Denn nur der Account erhalte Zugriff, auf dem auch die SAP NetWeaver- oder S/4HANA-Anwendung läuft (das sogenannte <SID>ADM). „SAP-Kunden sollten das Transportprotokoll vor dem Produktionsimport auf Manipulationen prüfen. Alle diejenigen, die den CVSS 9.1-Hinweis implementiert haben, sind auf der sicheren Seite", so Mans. *(cr)* @

Mehr zum Thema Cybersecurity ab Seite 13.