SYNTAX

SAP Security Checkliste

7 Schritte zum Schutz der sensibelsten Daten Ihres Unternehmens

Ihre SAP-Systeme beinhalten die sensibelsten Daten Ihres Unternehmens und sind damit ein ideales Ziel für Angriffe.

Sobald die Angreifer Ihre Schwachstellen ausnutzen, müssen Sie nicht nur mit Betriebsunterbrechungen rechnen, sondern auch mit Unzufriedenheit Ihrer Kunden, was wiederum dem Ruf Ihres Unternehmens ernsthaft schaden würde.

Wie können Sie also sicherstellen, dass Ihre SAP-Daten wirklich sicher sind?

Diese 7 Punkte helfen Ihnen, die Sicherheit ihrer SAP-Systeme zu erhöhen

1 **Folgen Sie den Sicherheitshinweisen, die am SAP Security Patch Day veröffentlicht werden.** SAP Security Notes werden von SAP an jedem zweiten Dienstag im Monat veröffentlicht und enthalten wichtige Updates für gemeldete Sicherheitslücken in der SAP Netweaver Technologie und der SAP Business Suite. Die Implementierung dieser Sicherheitspatches schützt das SAP-System vor unberechtigtem Zugriff.

2 **Entwerfen Sie Ihren eigenen SAP Patch Management Wartungsplan.** Seien Sie proaktiv und implementieren Sie Ihre Patches rechtzeitig. Wie oft setzen Sie Ihre Sicherheits-Patches um? Haben Sie ein eigenes Teammitglied, das für die Bewertung der Implementierungsprioritäten zuständig ist? Sind die Patches so geplant, dass während des Implementierungsprozesses möglichst geringe Ausfallzeiten in der Produktion entstehen?

3 **Setzen Sie in der Liste der Sicherheitsschwachstellen die richtigen Prioritäten.**
Nicht jede in den SAP-Sicherheitshinweisen aufgeführte Schwachstelle ist für Ihre SAP-Umgebung relevant. Je nach Konfiguration kann die empfohlene Patch-Implementierung eine niedrigere Priorität haben als andere, kritischere Schwachstellen, wie beispielsweise Schwachstellen, die die Ausführung von Remote-Code ermöglichen oder den unberechtigten Zugriff auf sensible Daten erlauben. Ein kurzer Blick auf den CVSS Score ist ein erster guter Anhaltspunkt, aber ein erfahrener Security-Dienstleister kann Ihnen einen detaillierteren, automatisierten Bericht erstellen.

4 **Planen Sie Penetrationstests für SAP-Systeme.**
Zusätzlich zu einer sorgfältigen Patch-Verwaltung können Sie Ihre Verteidigung mit speziellen Testmodulen für SAP-Anwendungen auf Windows- oder Linux-Rechnern verstärken. Unternehmen können entweder umfassende Penetrationstests durchführen, bei denen sich jemand wie ein Hacker ohne Kenntnis der SAP-Umgebung verhält, oder mit SAP Focus Run Tests an SAP-Basisdokumenten durchführen.

5 **Befolgen Sie die Best Practices für das SAP Security Access Management.**
Jedes SAP-Konto sollte personalisiert sein, mit einem klaren Zweck erstellt werden und dem Benutzer genau die Rechte gewähren, die er benötigt. Jede Aktion, die im System durchgeführt wird, sollte einem bestimmten Benutzer zugeordnet werden können. Viel zu oft verwenden Unternehmen zu viele generische SAP-Konten, die als vorübergehende Schnellzugriffslösungen bei Systemmigrationen gedacht waren.

6 **Verwenden Sie Verhaltensanalysen, um Änderungen im Benutzerverhalten zu erkennen.**
Was passiert, wenn ein nicht autorisierter Mitarbeiter versucht, auf eine SAP-Anwendung zuzugreifen? Verwenden Sie Tools zur Protokollanalyse wie SAP Enterprise Threat Detection, Elasticsearch oder Splunk, um beunruhigende Anmeldemuster zu erkennen und automatische Benachrichtigungen zu erhalten.

7 **Halten Sie die Branchenvorschriften wie GDPR, PCI DSS und SOX ein.**
Dies gilt für alle Unternehmen, unabhängig davon, ob sie in einer SAP-Umgebung arbeiten oder nicht. Bei Audits, bei denen geprüft wird, ob das Unternehmen z. B. die PCI DSS-Vorschriften oder die ISAE3402-Anforderungen einhält, wird die Kontrollinstitution nach dem Status Ihrer Schwachstellen- und Patch-Managementprozesse fragen.

Erfahren Sie mehr
syntax.com/de-de/cyber-security