



Digitalisierung in SAP-Umgebungen:

Sensible Daten schützen, auch gegen sorglose Mitarbeiter

Die IT-Sicherheit spielt in deutschen Unternehmen eine zentrale Rolle. Die Bereitschaft zu Investitionen ist vorhanden, und anders als in früheren Jahren wird die IT-Sicherheit nicht ausschließlich als lästige Pflichtaufgabe wahrgenommen, sondern als bedeutsamer Schutz von kritischen und wichtigen Unternehmenswerten. Aufgrund der medialen Berichterstattung rücken vielerorts Maßnahmen zur Abwehr externer Angreifer ins Zentrum des Interesses, obwohl vor allem den CIOs und den Sicherheitsverantwortlichen durchaus bewusst ist, dass die größte Gefahr für die Datensicherheit von den eigenen Mitarbeitern oder Partnern mit Zugang zu sensiblen Unternehmensdaten ausgeht.



Abbildung 4: Viele Unternehmen erachten Mitarbeiter als Sicherheitsrisiko. Das ist kein Misstrauensvotum. Oft bereitet der unachtsame Umgang mit Daten Sorge.

Dabei müssen Verfehlungen beim Datenschutz und bei der IT-Security durch eigene Mitarbeiter oder durch Partnerfirmen gar nicht immer vorsätzlich geschehen. Eine Personalakte hat den Schutz der gesicherten IT-Umgebung eines Unternehmens verlassen, sobald sie der wohlmeinende Kollege auf seinen USB-Stick geladen hat, um sie abends nach Feierabend zu Hause noch zu bearbeiten. Derartige Unachtsamkeiten im Umgang mit unternehmenskritischen Daten wie etwa Materialstücklisten oder Konstruktionszeichnungen können wirtschaftliche Schäden anrichten, wenn die Daten über Umwege etwa in die Hände von Konkurrenten gelangen.



Doch auch der Gesetzgeber versteht in Sachen Datenschutzverletzung keinen Spaß. Unternehmen wie auch den Verantwortlichen drohen rechtliche Konsequenzen, wenn mit dem Datenschutz und der Gefahrenabwehr fahrlässig umgegangen wird. Da in der Mehrzahl der großen deutschen Unternehmen Lösungen von SAP als zentrale Business-Applikationen im Einsatz sind, konzentriert sich dieses Whitepaper auf IT-Sicherheit und Datenschutz sowie GRC-Aspekte (Governance, Risk, Compliance) in SAP-Umgebungen. PAC möchte mit diesem Report für die Gefahren durch den unkontrollierten Datenabflusssensibilisieren und auf Wege für einen sorgsameren Umgang mit unternehmenskritischen Daten hinweisen. Vor allem erscheint es uns wichtig, dass Unternehmen ihre herkömmlichen Wege der Gefahrenabwehr und des Datenschutzes kritisch durchleuchten und neue Lösungen in Betracht ziehen, die dem Schutz der Datenquelle eine größere Beachtung schenken.

Fünf Handlungsfelder für mehr Sicherheit in zentralen ERP-Installationen:

- Informieren Sie Ihre Mitarbeiter über datenschutzrelevante Aspekte im Umgang mit kritischen Daten. Dabei sollten keine gesetzlichen und juristischen Argumente im Vordergrund stehen, sondern reale Szenarien aus dem jeweiligen Arbeitsumfeld.
- Analysieren Sie Ihre vorhandene Security-Installation und ERP-Umgebung auf Schwachpunkte hinsichtlich der Möglichkeit, kritische Daten und Dokumente zu downloaden und lokal zu speichern.
- Machen Sie Bestandsaufnahme der digitalen Inhalte. Welche Art von Dokumenten, aber auch welche strukturierten Daten werden besonders häufig bearbeitet und heruntergeladen? Wie geschäftsrelevant und sensibel sind die Inhalte?
- Installieren Sie besondere Schutzmechanismen für besonders kritische Daten. Achten Sie darauf, dass die anwenderfreundliche Nutzung erhalten bleibt. Datenschutz und Security dürfen die Abläufe nicht komplizierter machen, sonst werden Schutzmechanismen von Mitarbeitern unterlaufen.
- Sorgen Sie für Transparenz bei der Bearbeitung und Speicherung kritischer Daten und Dokumente. Veränderungen sollten auch aus Compliance-Gründen dokumentiert werden.

Lesen Sie weiter und erfahren Sie mehr warum es wichtig ist, dem Schutz auf inhaltlicher Ebene mehr Beachtung zu schenken, indem etwa Dokumente und Daten je nach ihrer unternehmenskritischen Bedeutung klassifiziert und geschützt werden: [Link zum Whitepaper](#)



Herausgegeben von **SECUDE GmbH & Pierre Audoin Consultants (PAC) GmbH**

Autor:



Joachim Hackmann
Principal Consultant –
Software & Related
Services
j.hackmann@pac-online.com

Kontakt:



Susanne Grebe
Sales Coordinator
PAC GmbH

s.grebe@pac-online.com

Über PAC – a CXP Group Company:

PAC liefert fokussierte und objektive Antworten auf die Wachstumsherausforderungen der Akteure im Markt für Informations- und Kommunikationstechnologie (ITK) – von der Strategie bis zur Umsetzung.

Wir unterstützen ITK-Anbieter mit quantitativen und qualitativen Marktanalysen sowie strategischer und operativer Beratung. CIOs und Finanzinvestoren beraten wir bei der Bewertung von ITK-Anbietern und -Lösungen und begleiten sie bei ihren Investitionsentscheidungen. Öffentliche Organisationen und Verbände bauen auf unsere Analysen und Empfehlungen als Grundlage für die Gestaltung ihrer ITK-Politik.

PAC wurde 1976 gegründet und gehört seit Juni 2014 zur CXP-Gruppe, dem führenden europäischen Marktanalyse- und Beratungsunternehmen für Software- und IT-Services.

Weitere Informationen unter www.pac-online.com

Besuchen Sie auch den PAC Blog! Kurzanalysen und Kommentare zu aktuellen ITK-Trends und Entwicklungen von PAC-Analysten und -Beratern: www.pac-online.com/blog

Über SECUDE

SECUDE ist ein innovativer, weltweit tätiger Anbieter von IT-Datenschutzlösungen für SAP-Kunden. Das Unternehmen wurde 1996 als Joint Venture von der SAP AG und Europas größter anwendungsorientierter Forschungseinrichtung, dem Fraunhofer Institut gegründet, um SAP-relevante Sicherheitssoftware zu entwickeln. SECUDE ermöglicht heute SAP-Kunden, ihre unternehmenskritischen SAP-Datenexporte vor Verlust und Diebstahl zu schützen sowie die Auflagen branchenspezifischer Compliance-Richtlinien zu erfüllen. Sensible Datenexporte aus SAP werden mit SECUDE Softwarelösungen durch intelligente Kontext-Analysen identifiziert, klassifiziert, verschlüsselt und mit Berechtigungen versehen. Damit wird ein vertraulicher Austausch geschäftskritischer SAP-Exporte, sowohl im eigenen Unternehmen als auch mit externen Geschäftspartnern, über die Cloud oder auf mobilen Endgeräten sichergestellt. Mit Niederlassungen in Europa, Nordamerika und Asien steht SECUDE für weltumspannende IT-Sicherheit. Weitere Informationen unter www.secude.de