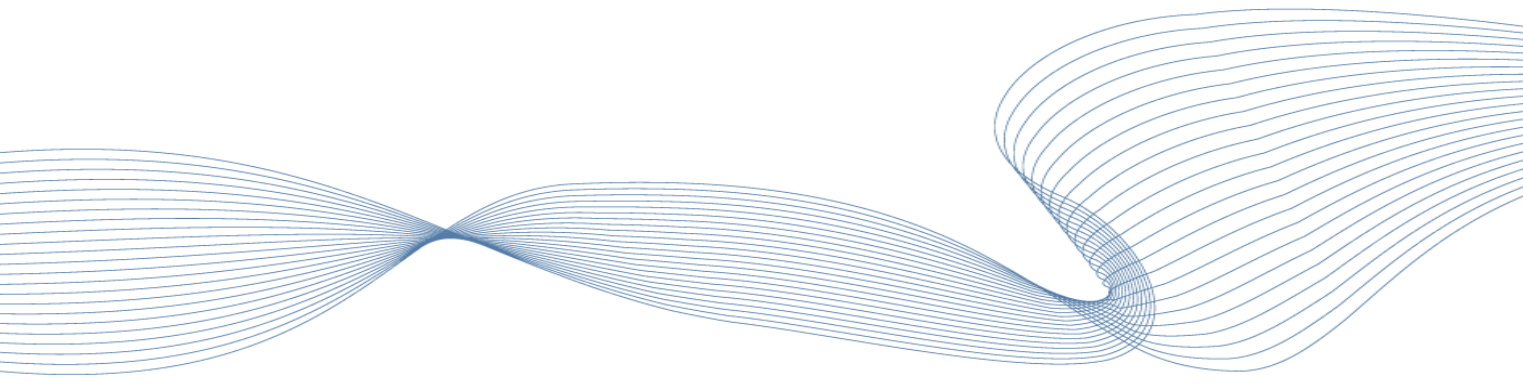
Digitalisierung in SAP-Umgebungen

Sensible Daten schützen, auch gegen sorglose Mitarbeiter

April 2016



PAC
A CXP GROUP COMPANY

Herausgegeben von

SECUDE GmbH

Rheinstrasse 97, 64295 Darmstadt

Pierre Audoin Consultants (PAC) GmbH

Holzstr. 26, 80469 München

Kontakt:

Joachim Hackmann (+49 [0]89 23 23 68 12, j.hackmann@pac-online.com)

INHALT

1. BEWUSSTSEIN FÜR DEN WERT DIGITALER DATEN SCHAFFEN

In Zeiten der Digitalisierung gewinnt das Thema Sicherheit und Datenschutz an Bedeutung. Das haben viele Unternehmen und auch Unternehmenslenker erkannt. Sie drängen daher ihre IT-Abteilungen dazu, die zunehmend digitalen Geschäftsmodelle entsprechend abzusichern. Während in den Medien und in der Öffentlichkeit vor allem über die Angriffe von außen durch versierte Hacker berichtet wird, ist den Security- und Datenschutzexperten schon lange klar, dass eine kaum minder große, aber schwerer zu kontrollierende Gefahr von innen droht.

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.

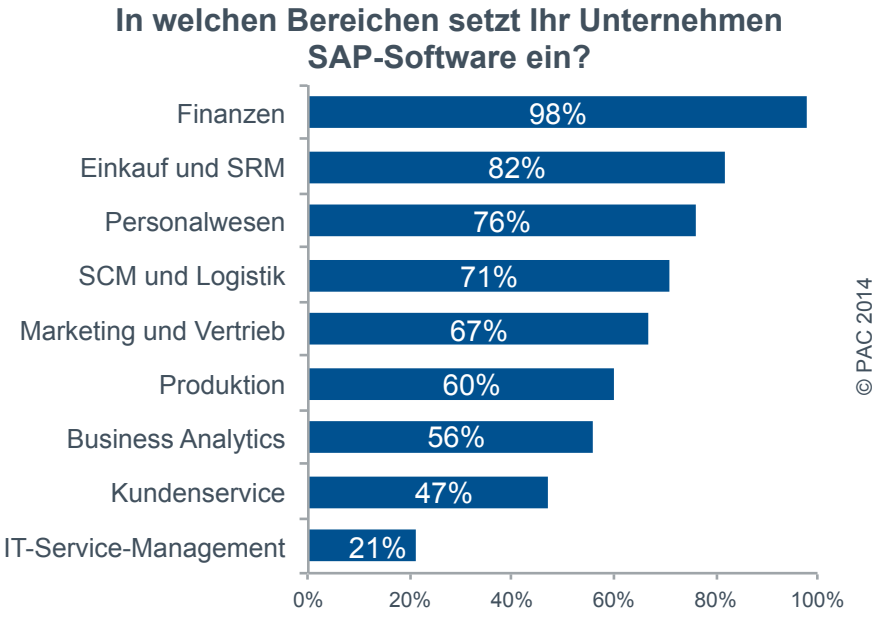
Derartige Unachtsamkeiten im Umgang mit unternehmenskritischen Daten wie etwa Materialstücklisten oder Konstruktionszeichnungen können wirtschaftliche Schäden anrichten, wenn die Daten über Umwege etwa in die Hände von Konkurrenten gelangen. Doch auch der Gesetzgeber versteht in Sachen Datenschutzverletzung 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 Datenabfluss sensibilisieren und auf Wege für einen sorgsamen 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.

2. DIE ANFORDERUNGEN AN DATENSICHERHEIT UND DATENSCHUTZ IN SAP-UMGEBUNGEN VERÄNDERN SICH

SAP bleibt auch in der digitalisierten Welt die zentrale Plattform für Geschäftsprozesse

Der zentrale Knotenpunkt für Unternehmensprozesse und -daten ist in sehr vielen Organisationen schon seit Jahren das hauseigene ERP-System von SAP. Einer Erhebung von PAC zufolge ist die Durchdringung von SAP in deutschen Unternehmen insbesondere in den Funktionsbereichen Finanzen, Einkauf/SRM und Personalwesen sehr hoch (siehe Abbildung 1). Die enge Bindung deutscher Anwender an SAP, was die internen Prozesse für Backoffice- und Support-Funktionen betrifft, wird auch in einer digitalen Unternehmenswelt Bestand haben. Daran ließ zumindest die Mehrheit von 57 Prozent der SAP-Verantwortlichen in einer weiteren Befragung[1] keinen Zweifel (befragt wurden Unternehmen mit mehr als 1.000 Mitarbeitern). Sie räumen der SAP-Software auch in einer digitalen Welt eine zentrale strategische Bedeutung ein, und zwar sowohl im Backend als auch im Frontend. Dabei zeigen sich allerdings enorme branchenspezifische Unterschiede. Ein starkes Signal für SAP als zentrale Plattform geht beispielsweise von der für den Standort Deutschland so wichtigen Gruppe der produzierenden Unternehmen aus. Hier rücken drei Viertel der Teilnehmer die SAP-Lösung an eine zentrale strategische Stelle in ihren künftigen Digitalisierungsvorhaben.



Anteile in Prozent der Unternehmen, n = 101

Abbildung 1: *In vielen deutschen Großunternehmen ist SAP als zentrales ERP-System gesetzt. Das gilt vor allem für den Bereich Buchhaltung.*

[1] „S/4HANA – Relevanz für SAP-Kunden, Erwartungen und Hindernisse, Trendstudie PAC, Oktober 2015

Enabling-Technologien schaffen Mehrwert – verursachen aber auch Risiken

Zu den wichtigen Enablement-Technologien der Digitalisierung zählen Analytics, Mobility und Cloud Computing. Sie füllen das Internet der Dinge und seine branchenspezifischen Ausprägungen (Industrie 4.0, Connected Car, Smart Energy u.a.) mit Leben, indem sie mobile Devices in Service- und Geschäftsprozesse einbinden, Daten sammeln und auswerten sowie spezielle Funktionen und Ressourcen aus der Cloud bereitstellen. Das schafft Schnelligkeit, Agilität und Flexibilität – allerdings häufig zulasten der Sicherheit, was wiederum einen sehr wunden Punkt im Bewusstsein deutscher Anwender trifft. Regelmäßig befragt PAC deutsche CxOs zu aktuellen Trendthemen, und dabei zeigt sich immer wieder ganz klar, dass Sicherheit das bestimmende Thema in deutschen Chefetagen ist. Unserer jüngsten Umfrage unter 400 C-Level-Managern in Deutschland zufolge (siehe Abbildung 2) hat die IT-Sicherheit die bei weitem größte Bedeutung, weit vor anderen Trendthemen wie Analytics und Cloud Computing. Die enorme Relevanz ist nachvollziehbar, beruhen heutzutage und künftig doch mehr und mehr Geschäftsmodelle auf IT-Infrastrukturen, Applikationen und Daten. Die Relevanz von IT-Security und Datenschutz wird in den kommenden Jahren noch steigen, je mehr IT-Intelligenz im Zuge der Digitalisierung in Produkte, Anlagen, Maschinen und Prozesse integriert wird.

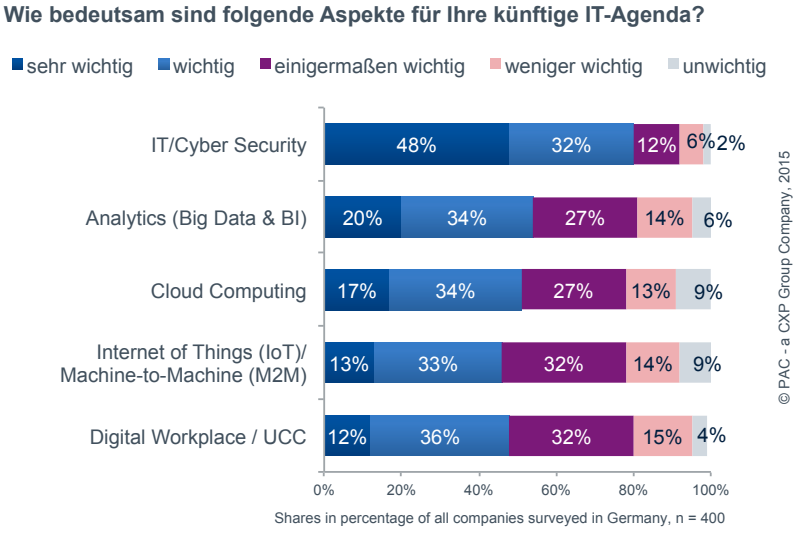


Abbildung 2: *Trendthemen wie Cloud und Analytics liegen in ihrer Bedeutung weit hinter IT-Sicherheit.*

SAPs Applikationssicherheit genügt höchsten Ansprüchen, aber...

Der Softwarekonzern SAP ist sich der Bedeutung seiner Software als wesentliches Element der Geschäftstätigkeit in sehr vielen Unternehmen durchaus bewusst und hat seinen Applikationen einen besonders sicheren Rahmen verpasst. Die IT-Sicherheit von SAP-Applikationen genügt höchsten Ansprüchen. Sie integrieren die modernsten Techniken, so dass Unternehmen, die ihre Business-Applikationen von SAP beziehen, in technischer Hinsicht grundsätzlich gut abgesichert sind.

... verhindert nicht die Gefährdung durch die eigenen Mitarbeiter

Vor diesem Hintergrund ist es verwunderlich, dass sich dennoch relativ viele Unternehmen um die Verbesserung ihrer Applikationssicherheit und Content Security sorgen. Mehr als jedes dritte Unternehmen hat aktuellen Handlungsbedarf bei der Applikationssicherheit, weitere 14 Prozent haben entsprechende Vorhaben in den kommenden zwei Jahren auf die Tagesordnung gesetzt. Ähnlich großer Bedarf besteht laut Erhebung bei der Content Security (siehe Abbildung 3).

Doch woher kommt die Sorge um die Sicherheit der eigenen Applikationen und Inhalte, wo die Daten doch in einer sehr sicheren Umgebung abgelegt werden? Die Antwort auf diese Frage weist in zwei Richtungen: Zum einen haben prominente Sicherheitsvorfälle wie etwa die viel beachteten Hackerattacken auf den deutschen Bundestag und auf Sony sowie die intensiv geführte Diskussion um die NSA-Schnüffelei dazu geführt, dass das Thema Schutz der unternehmensinternen Daten ganz oben auf die Agenda auch im Top-Management vieler Unternehmen gerückt wurde. IT-Sicherheit ist zum Thema auf Vorstandsebene geworden.

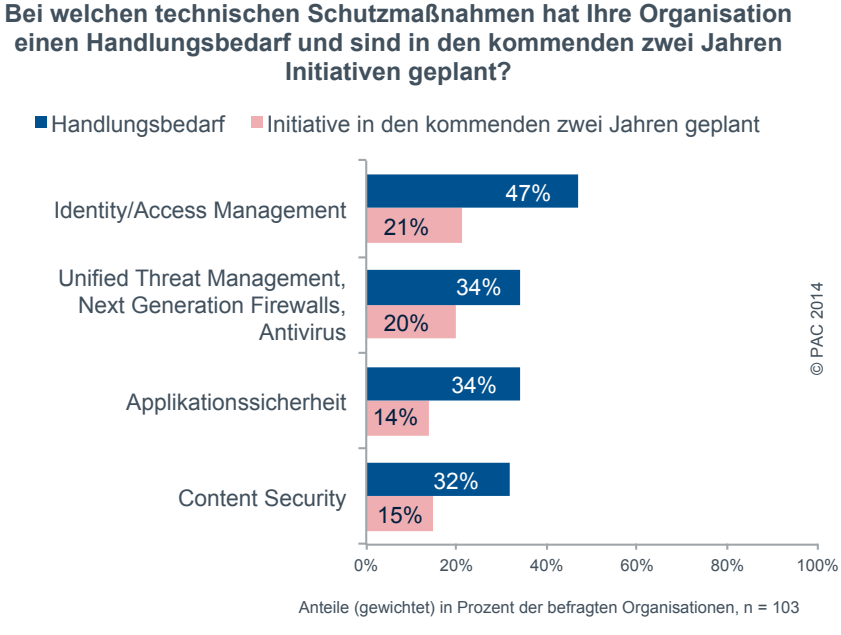


Abbildung 3: *Security-Initiativen in deutschen Unternehmen sind vielfältig und erstrecken sich auch auf Applikations- und Content-Sicherheit.*

Zum anderen entsteht die Sorge der befragten IT-Leiter nicht zuletzt aus der Erkenntnis, dass die eigenen Mitarbeiter ein besonderes und nur schwer zu beherrschendes Sicherheitsrisiko darstellen können. Dabei muss nicht einmal Vorsätzlichkeit im Spiel sein – oftmals ist Nachlässigkeit die Ursache für Informationslecks. Interne Daten werden kopiert, lokal abgelegt, zur Einsichtnahme per E-Mail an externe Partner verschickt und landen schließlich über Umwegen auf einem öffentlichen Cloud-Ordner.

Wie unterbindet man den sorglosen Umgang mit kritischen Daten?

Der sorglose Umgang mit Daten und Datenträgern kann zu einem gefährlichen Informationsleck anwachsen. Verlorene USB-Sticks oder auch entwendete Laptops können sich zu einem enormen Fiasko für Unternehmen entwickeln. Zum finanziellen Schaden und Vertrauensbruch gegenüber Kunden und Geschäftspartnern gesellen sich oft eine nachhaltig beschädigte Reputation sowie rechtliche Konsequenzen. Um einem solchen Szenario vorzubeugen, ergreifen Unternehmen oft drastische Maßnahmen. So hat etwa eine IT-Leiterin aus einem deutschen mittelständischen Unternehmen der Stahlverarbeitungsbranche jegliche Speicherung von Unternehmensdaten auf lokalen Datenträgern unterbunden. Im Gespräch mit PAC verriet sie, das Verbot gelte für alle mobilen IT-Geräte der Mitarbeiter. Der Download von Daten auf ein Smartphone sei technisch unmöglich, und das Ablegen von Informationen auf Notebooks per unternehmensweit geltender Richtlinie strikt untersagt.

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

Auch ein SAP-System birgt potenzielle Risiken in der Nutzung

Um die internen Sicherheitsvorkehrungen auszuhebeln, müssen nicht einmal mobile Endgeräte zum Einsatz kommen. SAP bietet beispielsweise an, im ERP-System gespeicherte Daten und Geschäftsinformationen über eine Download-API lokal zu speichern. Diese integrierte Download-Option eröffnet Nutzern die Möglichkeit, die Daten auch außerhalb des sicheren SAP-Kosmos weiterverarbeiten zu können. Für viele Anwendungen, Projekte und Vorhaben wird das sinnvoll und wünschenswert sein, doch SAPs Download-API kann IT-Security-Maßnahmen unterlaufen: Haben kritische Daten durch den Download einmal den sicheren Raum einer geschlossenen SAP-Umgebung verlassen, sind sie den bestehenden Sicherheitskonzepten quasi unwiederbringlich entzogen. PAC empfiehlt daher dringend, das Bewusstsein der Mitarbeiter dafür zu schärfen, dass Daten nur in geschäftlich zwingend erforderlichen Fällen lokal oder in SAP-fremden Umgebungen gespeichert werden dürfen.

3. UMGANG MIT UNTERNEHMENSKRITISCHEN DATEN: TRANSPARENZ ERGÄNZT IT-SECURITY

Deutsche Unternehmen planen umfangreiche Maßnahmen für mehr IT-Sicherheit

Ganz entscheidend für ein ganzheitliches Sicherheitskonzept ist neben einer intensiven Mitarbeiterschulung aber auch, dass die Unternehmen die technischen Möglichkeiten für IT-Security und Datenschutz ausschöpfen. Die jüngste PAC-Anwenderumfrage unter 400 deutschen CxOs[2] belegt das Bemühen der Unternehmen, mit technischen Lösungen Abhilfe zu schaffen (siehe Abbildung 5). Ganz oben auf der Prioritätenliste steht die Verschlüsselung, die in der Regel auf den sicheren E-Mail-Verkehr abzielt. Starke beziehungsweise lange Schlüssel verhindern dabei, dass Hacker mit Brute-Force-Angriffen zum Erfolg kommen, indem sie sämtliche Kombinationen systematisch und automatisiert durchprobieren. Doch vollkommene Sicherheit kann auch die Verschlüsselung nicht bieten. Wenn etwa Mitarbeiter sorglos mit dem Private Key umgehen oder schwache Passwörter verwenden, verliert sie ihre Wirkung.

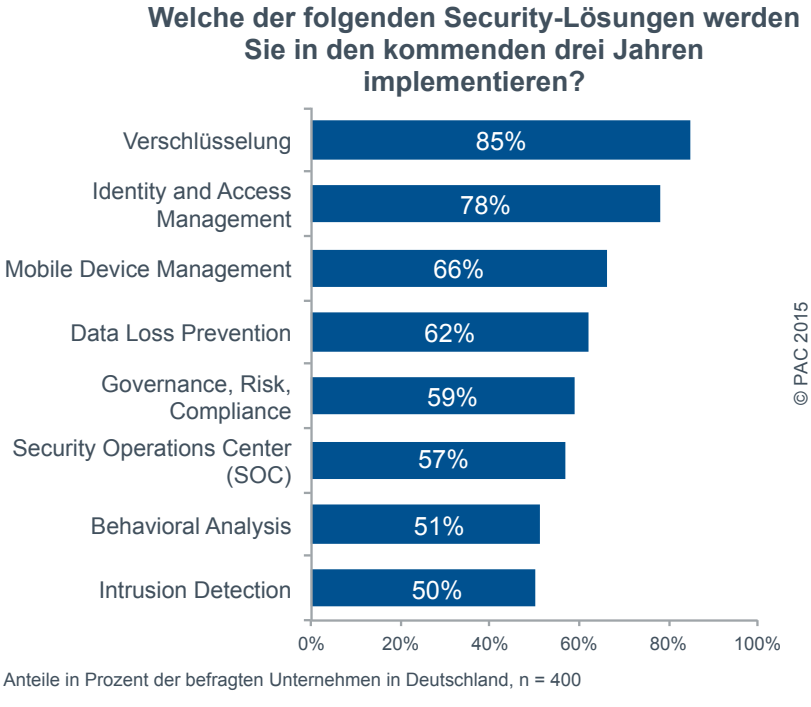


Abbildung 5: *Technische Lösungen wie Verschlüsselung und IAM beherrschen die Initiativen für mehr Sicherheit in Unternehmen.*

Folgerichtig verlassen sich die Unternehmen nicht allein auf Verschlüsselung, sondern nehmen weitere Sicherungsmechanismen in Angriff. Das Identity and Access Management (IAM) zielt beispielsweise darauf ab, den Zugang zu bestimmten IT-Ressourcen und Applikationen auf definierte Personengruppen zu beschränken, meistens basierend auf den Angaben im unternehmensweiten Verzeichnisdienst (etwa Active Directory). Mobile Device Management (MDM) spielt seit dem Einzug von mobilen Endgeräten – insbesondere von Smartphones – in die Unternehmens-IT eine bedeutende Rolle, da es neben der Inventarisierung und Softwareverteilung auch dem Schutz der Daten dient. Data Loss Prevention schließlich will den unkontrollierten Abfluss von unternehmenskritischen Daten verhindern. Insgesamt sind deutsche Unternehmen mit einer Kombination derartiger Schutzmaßnahmen unter dem Gesichtspunkt der IT-

[2] CxO 3000 – Investment Priorities 2015 – Germany, PAC, Oktober 2015

Sicherheit sehr gut aufgestellt, vorausgesetzt natürlich, die beschriebenen Projekte werden, wie in der Umfrage angekündigt, auch tatsächlich umgesetzt.

Wo bleibt die Transparenz? Wie steht es um die Dokumentation?

Im Zuge eines GRC-Managements (Governance, Risk, Compliance) stehen Unternehmen darüber hinaus in der Pflicht zur Dokumentation. Gesetze und Richtlinien ändern sich stetig und verlangen unter anderem auch Transparenz im Umgang mit Daten. Im Sinne einer unternehmensweiten GRC-Strategie müssen CIOs und Security-Verantwortliche auch zu diesem Thema ihren Beitrag liefern und daher den Umgang mit Daten nicht nur schützen, sondern auch dokumentieren. Die Geschäftsmodelle etwa von Versicherungen, Finanzdienstleistern und Telekommunikationsanbietern basieren mittlerweile auf IT-Lösungen, so dass auch weite Teile der Unternehmenswerte in digitaler Form gespeichert werden. Im Zuge der Digitalisierung werden weitere Branchen eine ähnliche Entwicklung nehmen und mehr und mehr unternehmenskritische Daten sowohl in internen als auch externen IT-Umgebungen speichern.

Umso wichtiger erscheint es, dem Zugang zu Dokumenten und Daten mehr Transparenz zu verschaffen. Maßnahmen, die etwa darstellen, welche Daten wann angesehen, bearbeitet, verändert und exportiert wurden, können die Sicherheit von SAP-Umgebungen erheblich verbessern und bereits vorhandene Security-Mechanismen sinnvoll ergänzen. Die Klassifizierung von Dokumenten je nach Kritikalität schafft darüber hinaus mehr Verlässlichkeit und Sicherheit, weil sich beispielsweise Reports gezielter erstellen und Alarmfunktionen genauer einstellen lassen, wenn etwa besonders sensible Dateien geöffnet werden. Vor allem eine Alert-Funktion beim Zugriff auf kritische Daten kann dabei auch eine wichtige Funktion für Mitarbeiter sein, die damit beispielsweise nicht zuletzt dafür sensibilisiert werden, mit den von ihnen verarbeiteten Daten verantwortungsvoll umzugehen.

Anwenderbeispiel: Datensicherheit im Handel

Der Fall eines Handelsunternehmens zeigt anschaulich, wie weit oft Selbsteinschätzung und externe Bewertung in puncto Datenschutz auseinanderdriften. Im Zuge seiner Analyse wollte der externe Datenschutzbeauftragte wissen, wie die Kundendaten geschützt sind. „Die liegen bei uns alle im SAP-System“, lautete die Antwort des Handelsunternehmens. Damit gab sich der Datenschutzbeauftragte nicht zufrieden. Er hakte nach, wie die Daten gesichert werden, wenn sie das SAP-System verlassen. „Wir schützen den Zugang mit SAPs Rollen- und Berechtigungskonzept“, hieß es daraufhin.

Aber auch das – so musste es das Handelsunternehmen lernen – ist im Sinne eines umfassenden Datenschutzes nicht ausreichend, denn das SAP-Rollen- und Berechtigungskonzept beschränkt zwar den Zugang zu Systemen und kann Benutzern auch Rechte für den Download nehmen. Das gilt dann aber für den Download aller Daten, was zu massiven Behinderungen bei der Arbeit führen kann und daher sehr selten angewendet wird. Es gibt also keine Möglichkeit, Downloads für unkritische Daten freizugeben und für sensible Daten zu beschränken.

Das Handelsunternehmen hat bei einer Assekuranz um Versicherung angefragt. Die zu versichernde Summe errechnete sich aus dem Kundenstamm von 220.000 aktiven Kunden, die mit je 50 Euro veranschlagt wurden.

4. VOLKER KYRA, VP SALES EMEA DER SECUDE GROUP: GEFAHR FÜR SAP-SECURITY DROHT OFT VON INNEN

Volker Kyra, Vice President Sales EMEA, Spezialist für SAP-Security, betont im Interview mit PAC: SAP-Installationen sind – eine fachgerechte Implementierung vorausgesetzt – sehr sicher, solange Dokumente die Umgebung nicht verlassen. Doch die Unternehmen sollten sich auch über die Grenzen der SAP-Sicherheit im Klaren sein.

PAC: Das Bewusstsein in den Unternehmen für Themen wie IT-Sicherheit und Datenschutz hat sich seit geraumer Zeit verbessert. Worauf führen Sie das zurück?

Volker Kyra ist seit dem 01.10.2015 Vice President Sales EMEA bei der SECUDE Group. Er war zuvor für Ciber Inc. und Hewlett-Packard in ähnlichen Rollen tätig. Volker Kyra berichtet in seiner neuen Funktion an den CEO der SECUDE Group. Mit mehr als 30 Jahren Berufserfahrung bringt er Kenntnisse aus der IT-Branche in verschiedenen Vertriebs- und Marketingpositionen für Hardware, Software sowie Systemintegration unter anderem im SAP-Umfeld sowie für Consulting Services mit. Er ist staatlich geprüfter Techniker mit Schwerpunkt Informationselektronik.

Kyra: Sicher hat die Diskussion um die Digitalisierung die Themen Datenschutz und IT-Sicherheit noch einmal befeuert, weil den Unternehmen klar wird, dass wesentliche Firmenwerte künftig ausschließlich in digitaler Form vorliegen werden. Auch Big Data und Analytics haben für eine Initialzündung gesorgt, denn mit der Möglichkeit, große Datenmengen auszuwerten, haben die Unternehmen erkannt, wie wertvoll digitale Daten sein können. Außerdem sind die Datenschutzrichtlinien in den vergangenen Jahren strenger und die Strafen bei Verstößen deutlich höher geworden. Auch das hat sicher zu der Entwicklung beigetragen.

PAC: SAP gilt aber allgemein als sehr sicheres System.

Kyra: Das stimmt, die Daten sind sicher – solange sie das SAP-System nicht verlassen. Der Abfluss der Daten muss auch gar nicht immer absichtlich geschehen. Viel häufiger tritt der Fall ein, dass dies unbewusst geschieht. Das SAP-Rollen- und Berechtigungskonzept definiert die Befugnisse der Mitarbeiter auf Basis des unternehmensweiten Verzeichnisdienstes. Ein Mitarbeiter aus der HR-Abteilung darf die Personalakten einsehen, bearbeiten und herunterladen, um sie weiterzuverarbeiten oder in ein anderes System zu laden. Das SAP-Konzept verhindert nicht den Download von gesamten Tabellen oder Personalakten.

PAC: Dennoch erlaubt das SAP-Konzept, sehr enge Grenzen bei den Systemzugängen zu definieren.

Kyra: SAP-Installationen sind oft lebende Systeme, in denen die Berechtigungsregeln wachsen und daher schwer kontrollierbar sind. Ich möchte das anhand eines Beispiels erläutern: Wenn ein Mitarbeiter seinen Job im Rechnungswesen antritt, weist man ihm die entsprechenden Zugriffsrechte im SAP-System zu. Wechselt er innerhalb des Unternehmens in den Einkauf, bekommt er weitere SAP-Rechte. Wird er dann noch zeitweilig in der HR-Abteilung eingesetzt, kommen nochmals Zugangsrechte hinzu. In der Praxis werden Rechte schnell hinzugefügt, aber selten weggenommen.

> ***Sobald das Unternehmen und das Management Kenntnis von Lücken hat, muss es handeln – nicht nur vor dem Hintergrund, dass der Abfluss der Daten verhindert wird, sondern auch, um sich rechtlich abzusichern.***

Oder nehmen Sie einen anderen häufigen Fall: Ein Mitarbeiter verlässt das Unternehmen und wird durch einen neuen Kollegen ersetzt. Der Einfachheit halber werden die Rollen und Berechtigungen des ausgeschiedenen Mitarbeiters quasi als Blaupause dem neuen Kollegen übertragen. Die Beispiele zeigen: Das Bewusstsein für die Themen Sicherheit und Datenschutz ist insgesamt zwar gestiegen. Im konkreten Einzelfall, in der Praxis und auf Mitarbeiterebene gibt es aber noch viel zu tun.

PAC: Gegen den ungewollten Datenabfluss setzen Unternehmen häufig schon Tools für Endpoint Data Protection ein. Reicht das nicht?

Kyra: Data Loss Prevention-Lösungen arbeiten meistens kontextbasierend, das heißt sie scannen Dokumente auf Schlüsselbegriffe und verhindern den Datenabfluss, wenn verdächtige Inhalte erkannt wurden. Die in SAP-Systemen gespeicherten Informationen liegen jedoch fast immer in strukturierter Form vor, so dass die Kontexterkennung hier nicht zuverlässig greift.

Der Datenschutz funktioniert hier nur, wenn auf Dokumentenebene klassifiziert wird und der Zugang, die Bearbeitung und vor allem der Download je Dokument und Anwender geregelt wird. Damit lässt sich auch der Herausforderung begegnen, dass das Bewusstsein der Mitarbeiter im Lauf der Zeit schwindet. Appelle zum sorgsamen Umgang mit kritischen Daten verlieren irgendwann immer ihre Wirkung.

Wenn dem Mitarbeiter jedoch klar und deutlich signalisiert wird, dass das Dokument, das er gerade zum Download ausgewählt hat, als unternehmenskritisch klassifiziert wurde, dann geht er ganz anders mit den ihm anvertrauten Daten um. Wer dann trotzdem Daten kompromittiert, handelt vorsätzlich.

PAC: Am Ergebnis, dass die Daten verändert oder entwendet wurden, ändert sich in dem Fall unter dem Strich aber nichts?

Kyra: Man muss die Themen Sicherheit und Datenschutz umfassend angehen. Unsere Lösungen setzen auf ein fünfstufiges Konzept, indem wir erstens auditieren, also den Zugriff auf sensible SAP-Datenexporte nachverfolgen und analysieren, um die Kontrolle und Compliance zu verbessern. Zweitens klassifizieren wir, um sensible SAP-Datenexporte sofort als solche zu identifizieren, und um den angemessenen Umgang mit ihnen zu gewährleisten. Als Drittes haben wir Alarmfunktionen implementiert. Mit Warnungen weisen wir Nutzer darauf hin, wenn sie sensible Daten herunterladen. Damit lassen sich Risiken senken und Compliance-Vorgaben durchsetzen. Viertens lassen sich Downloads blockieren. Mit Hilfe der einzigen SAP-nativen DLP-Lösung können wir so den Verlust von Daten aus SAP-Anwendungen verhindern. Da der Download für einige Anwendungsszenarien aber durchaus erwünscht ist, bieten wir fünftens die Möglichkeit an, sämtliche Daten, die die SAP-Umgebung verlassen, zu schützen und zu verschlüsseln. Über Microsofts Rights Management kontrollieren wir den Zugriff auf sensible Daten, die aus SAP heruntergeladen werden.

Auf Management-Ebene versuchen wir, das Bewusstsein dafür zu schaffen, dass der Datenabfluss sowohl für das Unternehmen als auch für das Management unter Compliance-Gesichtspunkten schwierig werden kann.

PAC: Wer sind Ihre Zielgruppen?

Kyra: Unsere Ansprechpartner sind oft Datenschutzbeauftragte, die interne Revision, Compliance-Manager sowie die Fachbereiche, aber auch die Enterprise-IT beziehungsweise deren IT-Security-Experten. Bei letzteren fehlt aber oft das Bewusstsein für die Risiken, die entstehen, wenn Daten das SAP-System verlassen. Die IT-Security-Abteilungen sind oft auf die Abwehr äußerer Gefahren ausgerichtet. Wir konzentrieren uns vor allem auf die Risiken, die aus dem Inneren des Unternehmens drohen.

Auf Management-Ebene versuchen wir daher, das Bewusstsein zu schaffen, dass der Datenabfluss sowohl für das Unternehmen als auch für das Management unter Compliance-Gesichtspunkten schwierig werden kann. Bei fahrlässigen Datenschutzverfehlungen drohen hohe Strafen, sowohl für das Unternehmen als auch für das Management.

5. FAZIT: INHALTSBEZOGENE SICHERHEIT GEWINNT AN BEDEUTUNG

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.

Insgesamt zeigen diverse PAC-Erhebungen, dass die Unternehmen durchaus sinnvolle Pläne für die Sicherung ihrer IT-Umgebungen verfolgen. Allerdings werden die Maßnahmen oft aus IT-Security-Sicht angestoßen und konzentrieren sich daher auf Zugangskontrolle zu IT-Installationen und Applikationen sowie auf das Verhindern von Datenabfluss, indem Download-Möglichkeiten eingeschränkt werden und das lokale Speichern technisch unterbunden wird.

Wichtig wäre es, dem Schutz auf inhaltlicher Ebene mehr Beachtung zu schenken, indem etwa Dokumente und Daten je nach ihrer unternehmenskritischen Bedeutung klassifiziert und geschützt werden. Vor allem ließe sich mit einem solchen Vorgehen sowohl die Kontrolle als auch die Transparenz der Zugriffe verbessern, weil klar ersichtlich wird, wer welche Daten wann bearbeitet oder heruntergeladen hat. Je digitaler die Geschäftsmodelle in den kommenden Jahren werden, desto bedeutsamer wird der Schutz geschäftskritischer Inhalte, und desto wichtiger wird der transparente Umgang mit sensiblen Daten.

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 Bestandsaufnahmen 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.

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. Seit 2011 ist SECUDE Value Added Reseller (VAR) im PartnerEdge™-Programm von SAP sowie SAP-Vertriebspartner in Deutschland und in der Schweiz. SECUDE genießt heute das Vertrauen zahlreicher Fortune-500- und DAX-Unternehmen. Mit Niederlassungen in Europa, Nordamerika und Asien steht SECUDE für weltumspannende IT-Sicherheit.

Weitere Informationen unter www.secude.de.

ÜBER PAC

Pierre Audoin Consultants (PAC) wurde 1976 gegründet und gehört seit Juni 2014 zur CXP Group, dem führenden unabhängigen europäischen Marktanalyse- und Beratungsunternehmen für die Software- und IT-Dienstleistungsindustrie sowie für Themen rund um die digitale Transformation.

Wir bieten unseren Kunden umfassende Support-Services in der Bewertung, Auswahl und Optimierung ihrer Softwarelösungen sowie bei der Bewertung und Auswahl von IT-Dienstleistern und begleiten sie bei der Optimierung ihrer Sourcing- und Investitionsstrategien. Die CXP Group begleitet IKT-Entscheidungsträger bei ihrer digitalen Transformation.

Schließlich steht die CXP Group Software- und IT-Dienstleistungsanbietern mit quantitativen und qualitativen Analysen sowie strategischer und operativer Beratung bei der Optimierung ihres Go-to-Market-Ansatzes zur Seite. Auch öffentliche Einrichtungen vertrauen bei der Entwicklung ihrer IT-Richtlinien auf unsere Studien.

Mit 40 Jahren Markterfahrung, 17 Niederlassungen in weltweit 8 Ländern und 140 Mitarbeitern unterstützt die CXP Group jährlich mehr als 1.500 IKT-Entscheidungsträger und die operativen Unternehmensbereiche sowohl großer als auch mittelständischer Unternehmen und deren Provider. Die CXP Group besteht aus drei Gesellschaften: Le CXP, BARC (Business Application Research Center) und Pierre Audoin Consultants (PAC).

Weitere Informationen unter www.pac-online.com.