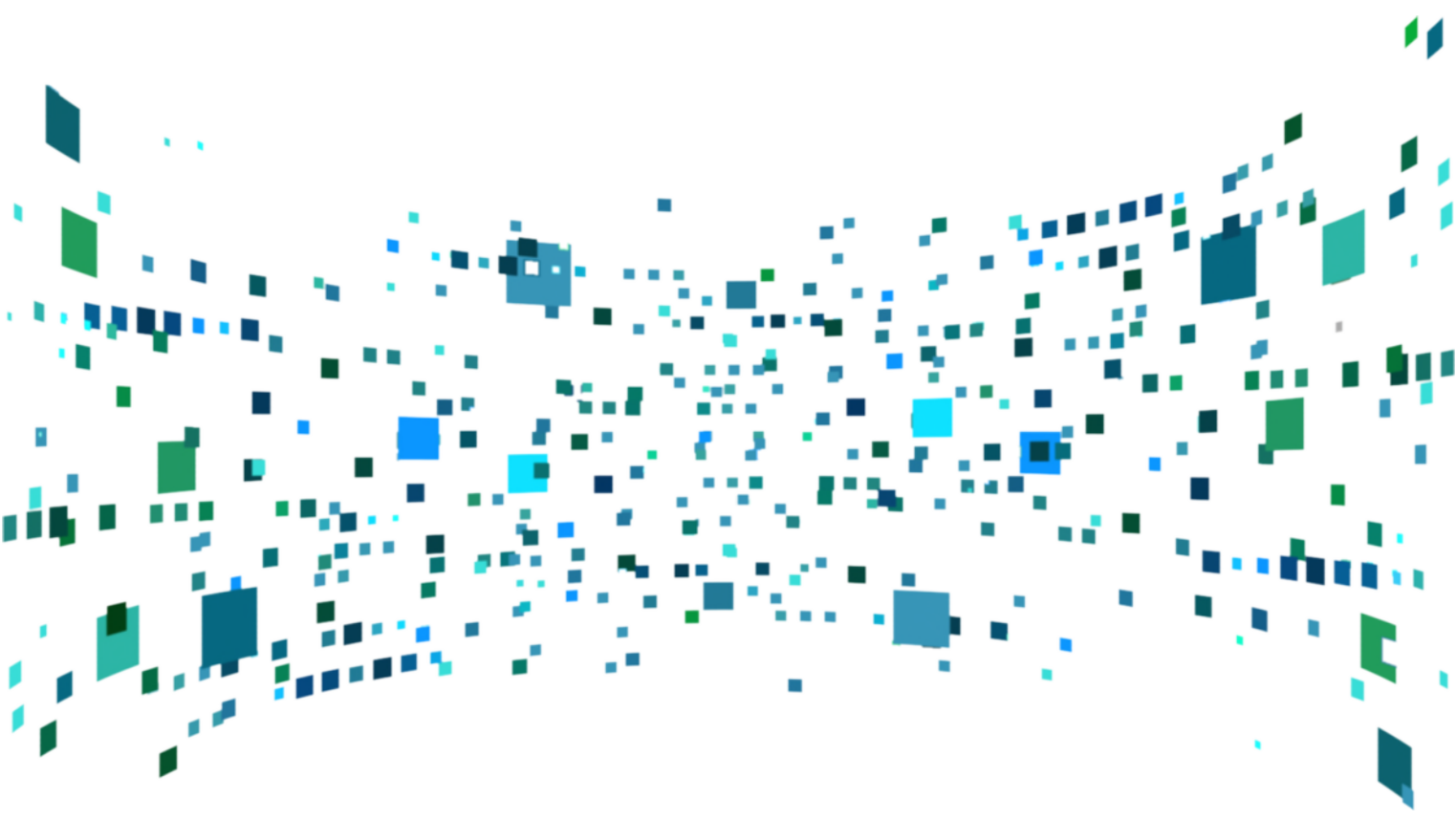


Umgang mit unternehmenskritischen Daten: Transparenz ergänzt IT Security

PAC Research Highlight

Von Joachim Hackmann, Principal Consultant

Dezember 2015

A CXP GROUP COMPANY

0IT-Sicherheit: Gefährdung durch die eigenen Mitarbeiter

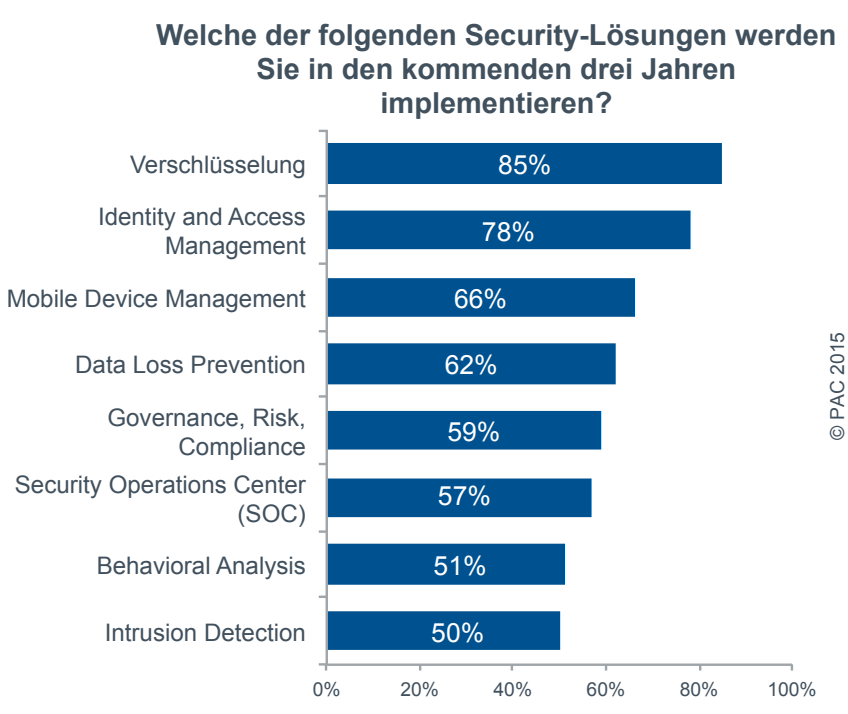
Schon seit geraumer Zeit ist der Schutz unternehmensinterner Daten ganz oben auf die Agenda vieler Unternehmen gerückt. Obwohl das Thema schon seit Anbeginn der professionellen IT-Nutzung diskutiert wird, haben unternehmensweite IT-Security-Initiativen in den vergangenen Jahren an Schubkraft gewonnen. Bedeutende Auslöser dieser neuen Aufmerksamkeit waren unter anderem der Verkauf von CDs mit Kundenlisten schweizerischer Banken an deutsche Steuerfahnder, die viel beachteten Hackerattacken auf den deutschen Bundestag (oder auf Sony) sowie die intensiv geführte Diskussion um die NSA-Schnüffelei. All diese prominenten Vorfälle haben unter anderem dazu geführt, die Sensibilität für IT-Sicherheit zu schärfen und entsprechende Gegenmaßnahmen einzuleiten.

Der unbekannte Hacker oder der beschlagene Wirtschaftsspion eignen sich sehr gut, die Bedrohungsszenarien für IT-Infrastrukturen und geschäftskritische Daten zu veranschaulichen. Ohne Zweifel sind Angriffe und Attacken von außen gefährlich. Noch häufiger und oft auch bedeutsamer sind die Bedrohungen der IT-Sicherheit durch die eigenen Mitarbeiter. Das belegt beispielsweise eine Umfrage von PAC zum Status quo der Cyber Security in Deutschland (siehe Grafik[1]). Demnach räumen 45 Prozent der befragten CIOs und IT-Security-Leiter ein, dass von eigenen Mitarbeitern eine relevante, bisweilen sogar sehr große Bedrohung ausgeht.

Dabei unterstellen die CIOs und Security-Verantwortlichen gar nicht zwingend bewusste Sicherheitsverstöße durch eigene Mitarbeiter. Oft ist es der sorglose Umgang mit Daten und Datenträgern, der zu einem gefährlichen Informationsleck wird. Eine IT-Verantwortliche aus einem deutschen mittelständischen Fertigungsunternehmen aus der Stahlverarbeitung schilderte beispielsweise in einem PAC-Expertengespräch zum Thema Security, dass man genau aus diesem Grunde jegliche Speicherung von Unternehmensdaten auf lokale Datenträger unterbunden habe. Das gelte insbesondere für alle mobilen IT-Geräte der Mitarbeiter. Der Download von Daten auf ein Smartphone sei technisch nicht mehr möglich, und das Ablegen von Informationen auf Notebooks per unternehmensweit geltender Richtlinie strikt untersagt.

[1] *Cyber Security – Investitionspläne, Chancen und Herausforderungen in deutschen Unternehmen, PAC in Kooperation mit Arkoon und Netasq, Atos SE, Trend Micro Deutschland GmbH und T-Systems International GmbH, Juni 2014*

Deutsche Unternehmen planen umfangreiche Maßnahmen für mehr IT-Sicherheit



Anteile in Prozent der befragten Unternehmen in Deutschland, n = 400

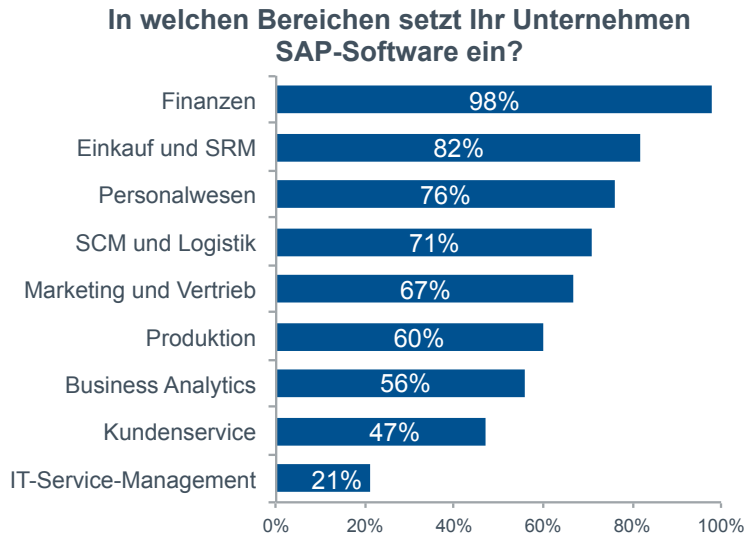
Auch die jüngste PAC-Anwenderumfrage unter 400 deutschen CxOs belegt das Bemühen der Unternehmen, mit technischen Lösungen Abhilfe zu schaffen (siehe Grafik[2]). Ganz oben auf der Prioritätenliste steht die Verschlüsselung, die in der Regel auf den sicheren E-Mail-Verkehr abzielt. Starke bzw. lange Schlüssel 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.

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

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

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 Industrien eine ähnliche Entwicklung nehmen und mehr und mehr unternehmenskritische Daten sowohl in internen als auch externen IT-Umgebungen speichern.



Anteile in Prozent der Unternehmen, n = 101

Viele der genannten Security-Initiativen verhindern und begrenzen Zugriffe, haben aber Defizite darin, beispielsweise Downloads auf Dokumenten- und Benutzerebene transparent darzustellen. Insbesondere in deutschen Unternehmen wird ein erheblicher Teil der geschäftskritischen Daten in SAP-Systemen gespeichert und verarbeitet. Eine PAC-Umfrage unter mehr als 100 SAP-Verantwortlichen zeigt, dass SAP-Anwendungen in sämtlichen unternehmenskritischen Prozessen deutscher Unternehmen eine tragende Rolle spielen (siehe Grafik[3]).

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 Transparenz 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.

[3] SAP goes Cloud: Pläne, Strategien und Investitionspläne deutscher Unternehmen, PAC in Kooperation mit All for One Steeb AG, Fujitsu Technology Solutions GmbH, InEssence Reply, itelligence AG, SAP Deutschland SE & Co. KG, Steria Mummert Consulting GmbH, Swisscom Enterprise Customers, November 2014

Fazit: IT-Security verlangt nach Transparenz

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 in der Sicherung ihrer IT-Umgebungen verfolgen. Allerdings werden die Maßnahmen oft aus IT-Sicht angestoßen und konzentrieren sich daher auf Zugangskontrolle zu IT-Installationen und Applikationen. Wichtig wäre es, dem Schutz auf Inhaltsebene mehr Beachtung zu schenken, indem etwa 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 über Zugriffe verbessern, weil klar ersichtlich wird, welche Daten wann bearbeitet oder heruntergeladen wurden. Je digitaler die Geschäftsmodelle in den kommenden Jahren werden, desto bedeutsamer wird der Schutz digitaler Inhalte und der transparente Umgang mit ihnen.

Über CXP Group

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.

PACs News: www.pac-online.com/blog

Folgen Sie uns auf Twitter: @PAC_DE

Kontakt

Joachim Hackmann

Principal Consultant
Software & related Services

M: +49 (0)160 97 77 96 29
E: j.hackmann@pac-online.com