



## Security managed by obscurity

Wenn jetzt all diese neuen Information-Management-Technologien, Plattformen und Lösungen kommen, mit denen man Dokumente und Mails

besser finden, in Portalen und Cockpits jederzeit top-aktuelle Daten aus allen Systemen anschauen und mit denen jeder Mitarbeiter auf Knopfdruck mit anderen einen eigenen kleinen Arbeitsraum zum Austausch von Daten einrichten kann (auch mit externen Mitarbeitern), drängt sich natürlich die Frage auf, wie es um die Datensicherheit bestellt ist. «Kein Problem, machen Sie sich da mal keine Sorgen. Alles ist selbstverständlich Security-trimmed!» sagt der nette Herr von Microsoft. «Aha», antworten Sie, ohne richtig zu verstehen, was «Security-trimmed» eigentlich bedeutet.

Plötzlich beschleicht Sie das Gefühl, dass es einige Dinge gibt, die Sie schon immer über Ihre Firma wissen wollten, aber bisher nie zu fragen wagten. Zum Beispiel, wer eigentlich die Übersicht über die Zugriffsberechtigungen auf den File Shares des Unternehmens hat? Oder, wer den Überblick über Ihre File Shares hat? Das ist für jemanden, der zum Beispiel

eine Enterprise-Search-Lösung einführen möchte, die für alle File Shares allen Benutzern einen Volltext-Index zur Verfügung stellen wird, eine durchaus gescheite und in einem grösseren Umfeld nicht unbedingt leicht zu beantwortende Frage.

Eine kurze Zwischenbemerkung: Security-trimmed bedeutet, dass die anzuzeigenden Elemente zum Beispiel eines Suchresultats vor der Anzeige mit den Berechtigungen des Suchenden verglichen werden und dieser nur das zu sehen bekommt, worauf er Zugriff hat. Das ist eine Grundvoraussetzung für eine Enterprise-Search-Lösung. Doch es wird damit nicht verhindert, dass zum Beispiel der Inhalt eines File Shares, von dem bisher ausser der Geschäftsleitung niemand wusste, in den Suchresultaten eines normalen Mitarbeiters erscheint, wenn es versäumt wurde, den Zugriff zu regeln. Nur weil jemand etwas bisher nicht gesehen hat, heisst das ja noch lange nicht, dass er keine Leseberechtigung darauf hat. «Security managed by obscurity» nennt das ein Kollege von mir, der bei einem grossen Schweizer Finanzunternehmen in der IT ganz oben sitzt und dies und das befürchtet, wenn erst einmal unternehmensweit gesucht werden

kann. So richtig im Dunkeln tappen Sie dann, wenn Ihre Benutzer anfangen, über die neuen Collaboration-Werkzeuge Ad-hoc-Workspaces zu eröffnen, die gerade so in Mode kommen, und ihre Kollegen aus anderen Firmen einladen, an Dokumenten mitzuarbeiten, auf welche diese sonst gar keinen Zugriff hätten. Direkt über das Internet und ohne dass jemand etwas davon weiss. Klar: Man kann ja die Dokumente auch per Mail verschicken, dann sind sie ebenfalls extern zugänglich. Allerdings besteht schon ein Unterschied, ob ich einmal jemandem ein Dokument maile oder ob er auch ein halbes Jahr nach abgeschlossener Zusammenarbeit noch Zugriff auf die Hälfte meines Datenbestands hat, nur weil ich vergessen habe, meinen Workspace wieder zu schliessen. Da waren die Chat-Tools noch heilig.

Vielleicht sollte man sich doch überlegen, schon bald eine Digital-Rights-Management-Lösung anzuschauen, um nicht in naher Zukunft gar nicht mehr wissen zu wollen, was man sich heute nicht zu fragen traut.

PATRICK PÜNTENER IST MITGLIED DER GESCHÄFTSLEITUNG DER ITSYSTEMS AG, PATRICK.PÜNTENER@ITSYSTEMS.CH