Case Study: Deutsche Flugsicherung

Zugriff ganz nach Plan

Wer kann im zentralen Dateisystem eigentlich unsere Gehaltszettel und die Protokolle unserer Personalgespräche einsehen?

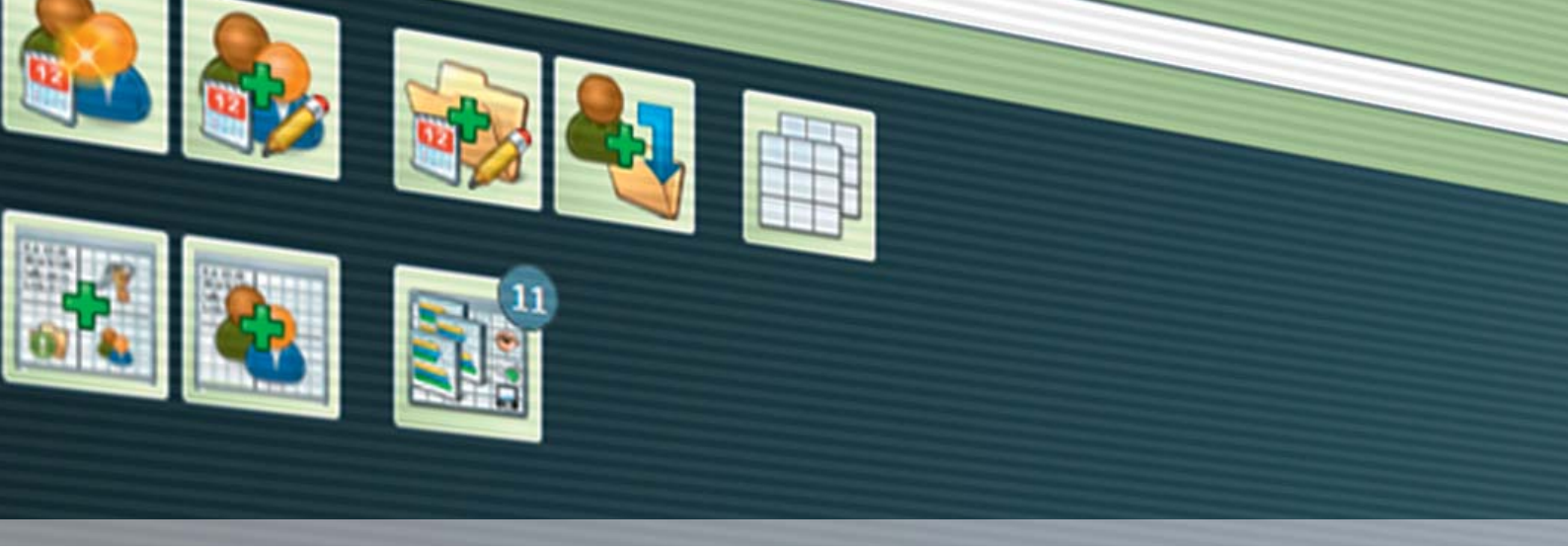
„Künftig soll sich der jeweilige Datenverantwortliche alle Zugriffsrechte auf Knopfdruck darstellen lassen und sie auch selbst bearbeiten können".

Die Frage der Mitarbeiter aus der Zweigniederlassung barg Sprengstoff: Wer kann im zentralen Dateisystem eigentlich unsere Gehaltszettel und die Protokolle unserer Personalgespräche einsehen? Die IT-Verantwortlichen der Deutschen Flugsicherung (DFS) in Langen bei Frankfurt mussten nach der genauen Antwort lange suchen. Zu tief im System verbarg sich der Wust von Regeln für den Datenzugriff, sagt Jörg Kundler. Er ist als Leiter der Business-IT oberster Herr über alle Computersysteme der DFS, die nicht unmittelbar den Flugbetrieb steuern. Also setzte sich die IT-Abteilung das Ziel, die Nutzerrechteverwaltung zu vereinfachen und zu dezentralisieren.

„Künftig soll sich der jeweilige Datenverantwortliche alle Zugriffsrechte auf Knopfdruck darstellen lassen und sie auch selbst bearbeiten können", erklärt Kundler. Die Software, die dies auch durchschnittlich begabten PC-Nutzern möglich machen soll, wird gerade nach und nach eingeführt: zunächst bei IT-affineren Gruppenleitern; diese sollen durch begeisterte Erzählungen auch skeptischeren Kollegen den Mund wässrig machen, so das Kalkül. Kundler selbst hat gerade die Zugriffsrechte-Hoheit für die rund 80 Mitarbeiter in seinem Bereich übernommen. Braucht ein neuer Kollege nun Lese- oder Schreibrechte, muss Kundler nur den Namen des Mitarbeiters mit der Maus über die betreffenden Verzeichnisse ziehen, bestätigen und eine kurze Begründung der Änderung eintippen – fertig. Nutzerrechte sind eine grundlegende Frage bei der Konzeption eines jeden Computernetzwerks: Wer darf welche Bereiche der Verzeichnisstruktur sehen, wer darf die dort gespeicherten Dateien lesen, wer sie verändern?

Auch wenn beim Thema „Datensicherheit" viele vor allem an Bedrohungen von außen denken: In rund der Hälfte aller Fälle, bei denen Firmen auf elektronischem Wege Schaden zugefügt wurde, waren eigene Mitarbeiter die Täter, ergab die „e-Crime-Studie 2010" der Wirtschaftsprüfungsgesellschaft KPMG. Ganz oben auf der Hitliste: Datendiebstahl.

Dies Problem wird verschärft, weil viele Mitarbeiter nicht mehr nur vom eigenen Schreibtisch aus auf Daten zugreifen können, sondern durch Zugänge im Home-Office oder über Smartphones an Daten gelangen. Zugriffsrechte möglichst restriktiv zu handhaben ist deshalb für die Informationssicherheit unabdingbar. Viel steht auf dem Spiel: Scheidende Mitarbeiter könnten Kundendatenbanken oder andere Geschäftsgeheimnisse auf einen USB-Stick ziehen – ihr neuer Arbeitgeber freut sich womöglich. Dreiste Angestellte könnten Dienstanweisungen umschreiben, Untergebene mit Rachegelüsten Geschäftszahlen manipulieren. Schließlich drohen auch noch rechtliche Folgen, wenn durch laxe Rechtevergabe gesetzliche Bestimmungen, etwa hinsichtlich des Datenschutzes oder Bankgeheimnisses, verletzt werden. „So viel wie nötig, so wenig wie möglich", postuliert deshalb auch das Bundesamt für Sicherheit in der Informationstechnik als Maxime in Sachen Zugriffsrechte.



„Das Tool ist so intuitiv – ich denke, den meisten Datenverantwortlichen kann man innerhalb von zehn Minuten zeigen, wie es geht."

Deshalb muss bei jeder Berechtigungsänderung ein Workflow von Beantragung, Genehmigung und Umsetzung eingehalten werden. Die Folgen: Wartezeit für die Nutzer und, bei deutschlandweit 6.000 Mitarbeiterinnen und Mitarbeitern, viel lästige Routinearbeit für die Admins. Hinzu kommen prinzipielle Schwachstellen. Da niemand sich über zu viele Privilegien beklagt, wird etwa bei einer Versetzung leicht vergessen, die Zugriffsrechte wieder zu entziehen. „Der Extremfall sind Praktikanten, die von Abteilung zu Abteilung wandern und am Ende überall Zugriff haben", sagt Schanz. Zudem fühle sich für manche Verzeichnisse niemand verantwortlich – etwa bei abgeschlossenen Projekten. Mitte 2011 machten sich Alexander Schanz und Kollegen auf die Suche nach einer Software, welche die genannten Probleme löst.

Infrage kamen nur deutsche Anbieter: „Es gibt auch US-Produkte, aber die haben einen anderen Hintergrund", erklärt Schanz. „Da geht es dann auch um Überwachung von Mitarbeiter-Aktivitäten, was mit deutschem Arbeitnehmerschutz kaum vereinbar ist." Inländische Hersteller solcher Berechtigungsmanagement- oder Provisioning-Lösungen sind etwa Beta Systems, Econet, Parks Informatik und Tesis Sysware. Die DFS entschied sich nach einigen Produktpräsentationen Ende 2011 für das Tool von Protected Networks. Listenpreis: 35 Euro pro verwaltetem Nutzer plus rund 500 Euro pro Fileserver. Die Angebote der Wettbewerber fallen ähnlich aus. Hinzu kommen jährlich 20 Prozent des Anschaffungspreises für Updates und umfassenden Support. Außerdem die Kosten für die Einführung, deren genaue Höhe die Deutsche Flugsicherung nicht kommuniziert.

Bislang sind rund 15 Mann-Tage angefallen. „Nun befindet sich das Projekt in der vielleicht spannendsten Phase", sagt Arne Vodegel, Kundenbetreuer bei Protected Networks. „Mit der neuen Transparenz in Sachen Berechtigung muss erst mal umgegangen werden." Denn oft passen Kunden im Nachgang bestimmte Strukturen und Abläufe an. Schanz ist sehr zufrieden mit der neuen Lösung. „Das Tool ist so intuitiv – ich denke, den meisten Datenverantwortlichen kann man innerhalb von zehn Minuten zeigen, wie es geht." Praktikanten könne man nun von vornherein zeitlich befristete Rechte erteilen. Und um technische Details wie Gruppenmitgliedschaften und Leserechte für übergeordnete Verzeichnisse kümmere sich das Programm selbsttätig im Hintergrund. „Die meisten Probleme mit der Bedienung haben eigentlich wir IT-Admins, weil wir an das Thema Berechtigungen mit einer zu komplexen Denke herangehen."

Aber die Software macht nicht nur die Administratoren glücklich, die neue Freiräume für anspruchsvollere Aufgaben gewinnen. Auch die interne Revision sei begeistert, berichtet Schanz – sorgt das Programm doch für eindeutige Verantwortlichkeiten und dokumentiert nebenbei automatisch, wer wann warum Zugriff auf welche Daten hatte. Und schließlich könne das Tool sogar helfen, Strukturen zu optimieren, weil etwa die Arbeitsweisen verschiedener Standorte leicht miteinander verglichen werden können.

Quelle: Bundesagentur für Arbeit - www.faktor-a.arbeitsagentur.de