Dateisystem
Konsolidierung

Dateisystem- und Berechtigungsstrukturen zügig aufräumen

Der Leitfaden für die Dateisystem-Konsolidierung

econet

Vorwort

Datendiebstahl, Computerviren und Web-Attacken kosten ein deutsches Großunternehmen jährlich durchschnittlich 4,8 Millionen Euro. Allein 40 Prozent des Schadens entfallen auf Datenverluste, oft verursacht durch 'Taten krimineller Insider'.*

Um Unternehmens-Know-how und personenbezogene Daten schützen zu können, muss die Rechtesituation beim Zugriff auf Informationen klar sein. Vor allem in jahrelang gewachsenen Dateisystemen gibt es fehlerhafte Berechtigungen und entsprechend hohen Konsolidierungsbedarf. Hier spüren viele unserer Kunden auch den Druck von Regularien zur Risikobeherrschung, welche die Geschäftsleitung in Pflicht und Haftung nehmen.

Die in diesem Leitfaden beschriebene Methodik wird allen Betroffenen eine konkrete Hilfe sein, Dateisystem-und Berechtigungsstrukturen zügig und mit vertretbarem Aufwand aufzuräumen und fit zu machen für compliance-konformes Berechtigungsmanagement und effizientes Fileservice-Provisioning. Mit sicheren, einfachen und wirtschaftlichen Prozessen.

Ich wünsche Ihnen eine inspirierende und Gewinn bringende Nutzung unseres Leitfadens und freue mich auf Ihr Feedback.

Mit den besten Grüßen,
Ihr Gerhard Pölz
CEO econet

Compliance im Berechtigungsmanagement

Robert Kuhlig ist Gründer und Geschäftsführer des Munich Institute for IT Service Management und Lehrbeauftragter der LMU München. Er berät und schult Unternehmen in den Bereichen IT Security und IT Service Management.

Immer mehr Bestimmungen und Standards wie BDSG, GoBS, BSI GsHb, ISO 27002, GDPdU oder KonTraG fordern explizit die Risikobeherrschung beim Zugriff auf sensible Informationen. Feigenblattaktionen, wie vereinzelte Ist-Analysen der Rechte-verhältnisse in gewachsenen Dateisystemen, werden den Anforderungen nicht mehr gerecht.

Der Fileservice-Management-Spezialist econet hat eine Methodik entwickelt, um dauerhaft Transparenz in die Berechtigungssituation großer Dateisysteme zu bringen und um das Berechtigungs-management zu automatisieren. Denn nur regelbasierte und automatisierte Prozesse stellen diejenigen Kontrollmechanismen bereit, die von den Regularien für das Risikomanagement eingefordert werden.

* 2012 Cost of Cyber Crime Study · Ponemon Institute im Auftrag von Hewlett Packard, Oktober 2012

Gute Gründe für die Konsolidierung

Seit rund zwanzig Jahren gibt es Dateisysteme, wie wir sie heute kennen. Seither wachsen sie stetig mit dem Datenaufkommen und die Berechtigungssituation darin ändert sich mit jedem neuen Mitarbeiter und mit jeder neuen Projektablage. Es verwundert nicht, dass vielerorts die Floskel vom „gewachsenen Dateisystem“ ein Synonym für chaotische Zustände bei den Zugriffsrechten ist. Mancher Auszubildende hat nach seinem Gang durch das Unternehmen mehr Zugriffsrechte, als ein Abteilungsleiter. Eine Ursache dafür, dass missbräuchlicher Datenzugriff vor allem aus den eigenen Reihen zunimmt.

Vielen Unternehmen wird erst nach Datensicherheitspannen bewusst, wie sehr ihr sensibles Know-how oder ihre personenbezogenen Daten bedroht sind. Spätestens dann pochen Revision und Controlling auf die Umsetzung von Governance- und Compliance-Anforderungen bei der Zugriffsverwaltung.

Für eine Governance im Berechtigungsmanagement müssen die Fachbereiche mehr Verantwortung übernehmen. Sie kennen den eigenen Rechtebedarf besser als die IT. Dafür sind Workflows notwendig, die auch für Nicht-IT-Spezialisten einfach zu bedienen sind und gleichzeitig strenge Sicherheits-Level garantieren. Voraussetzung für solche Prozesse sind aufgeräumte und vereinfachte Berechtigungsstrukturen in Dateisystem und Active Directory.

Neben den Anforderungen an Governance, Risikomanagement und Compliance gibt es noch weitere Beweggründe für eine Konsolidierung:

- Organisatorische Umstrukturierungen, die eine Anpassung der Ablage- und Rechtestruktur notwendig machen, ob intern oder im Zuge von Mergers & Acquisitions
- Technische Umstrukturierungen wie die Neukonzipierung der Active Directory-Struktur
- Outsourcing-Strategien, bei denen Ablagen und Berechtigungen strukturiert übergeben werden müssen.

Zurückhaltung bei der Umsetzung

Hauptgrund für die Zurückhaltung bei solchen Konsolidierungsprojekten ist immer wieder der immense Aufwand, den die Verantwortlichen erwarten, und das nicht zu Unrecht. Bei Dateisystemen mit Hunderttausenden Ordnern konnte man alleine für das Feststellen der effektiven Berechtigungen mit manueller Arbeit im Bereich von mehreren Mannjahren rechnen. Hier gibt es mittlerweile jedoch zuverlässige Tool-Unterstützung, die einen - für solche Massenoperationen nötigen - hohen Grad an Automatisierung bieten.

Für alle Organisationen, die mit der FDA zu tun haben fordert die **FDA-Vorschrift 21 CFR Part 11** u. a. die „Beschränkung des Systemzugriffs für berechtigte Personen“ **(§ 11.10d)** sowie „die Durchführung von Rechte- und Rollenüberprüfungen um zu gewährleisten, dass nur berechtigte Personen das System benutzen“ **(§ 11.10g)**. **Bundesdatenschutzgesetz (BDSG) § 9** bzw. **Anlage zu § 9 Satz 1** […] Dabei sind insbesondere Maßnahmen zu treffen, die […] verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle), […] zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle) **BSI Grundschutzhandbuch BSI Standard 100-2** - **M 2.220** Richtlinien für die Zugriffs bzw. Zugangskontrolle **M 2.30** Regelung für die Einrichtung von Benutzern / Benutzergruppen **M 2.31** Dokumentation der zugelassenen Benutzer und Rechteprofile **M 2.370** Administration der Berechtigungen unter Windows Server 2003 **M 2.8** Vergabe von Zugriffsrechten **M 4.149** Datei- und Freigabeberechtigungen unter Windows **M 4.135** Restriktive Vergabe von Zugriffsrechten auf Systemdateien **M 4.247** Restriktive Berechtigungsvergabe unter Windows Client-Betriebssystemen. Aus dem **Deutschen Aktiengesetz AktG §91 (2), § 93 (1)** und dem **GmbHG §43 (1)-(2)** gehen Haftungsrisiken für das Unternehmen und die Mitglieder der Unternehmensführung hervor. **ISO 27002** "Information Technology – Code of practice for information security management" – insbesondere **Tz. A.11 Access Control**: **3.2** Access Restrictions: Zugriffe auf IT-Systeme (Applikationen) und (deren) Daten sind restriktiv und sicher wie möglich zu implementieren. **3.31** Segregation of Duties within Applications: Sicherstellung, dass die Gewaltentrennung innerhalb von IT-Systemen (Applikationen) gewährleistet ist. **3.42** Management and Monitoring of User Accounts: Es sind Mechanismen etabliert, welche die Veränderung von User-Accounts und User-Profilen lückenlos überwacht, um Risiken unbefugter und unangemessener Zugriffe auf IT-Systeme (Applikationen) und (deren) Daten auszuschließen. **GoBS - Tz. 5 Datensicherheit**: Ziel der Datensicherungsmaßnahmen ist es, die Risiken für die gesicherten Programme/Datenbestände hinsichtlich Unauffindbarkeit, Vernichtung und Diebstahl zu vermeiden. **Abgabenordnung (AO) § 147 Abs. 2,** Pflichten zur Aufbewahrung von rechnungslegungsrelevanten Daten. **PCI-DSS, Anforderung 7**: **7.1.1** Einschränkung der Zugriffsrechte auf Benutzer-ID auf niedrigste Stufe, die zur Erfüllung der Prozessabwicklung notwendig ist. **7.2.2** Zuteilung der Benutzerrechte an Einzelanwender auf Basis der Jobklassifizierung und Funktion. **Cobit DS 5.3** Benutzerprofil-Management: Sicherstellung, dass Benutzerzugriffsrechte auf Systeme und Daten konform mit festgelegten und dokumentierten Geschäftsanforderungen sind, und diese Anforderungen den Benutzerprofilen zugeordnet sind. **DS 5.4** Benutzerkontenverwaltung: Rechte und Vorgaben für den Zugriff auf Unternehmenssysteme und -informationen sollen für alle Benutzertypen festgehalten werden. Regelmäßige Überprüfungen aller Benutzerkonten und entsprechender Benutzer-

Datendiebstahl durch eigene Mitarbeiter ist bei fast der Hälfte aller konkreten Spionagehandlungen für den Informationsabfluss verantwortlich.

Studie „Industriespionage 2012“ von Corporate Trust, Unternehmensberatung im High-Level-Security-Bereich

Um sicherzustellen, dass Mitarbeiter nur so viele Zugriffsrechte besitzen, wie sie für ihre Arbeit benötigen, müssen die Fachabteilungen die Verantwortung dafür künftig selbst übernehmen können. Dafür braucht es neben business-tauglicher Prozesse bei der Rechtevergabe ein sauber aufgeräumtes Dateisystem mit klaren Rechtestrukturen.

Vorab Mitarbeiter in den Fachabteilungen einbinden

Gibt es im Zuge der Berechtigungs-Konsolidierung auch Änderungen an der Ablagestruktur, stößt dies bei der Mitarbeiterschaft nicht immer auf Begeisterung. Die Reaktionen sind sehr abhängig vom herrschenden Betriebsklima und der Kultur im Umgang miteinander. Neben der viel beschworenen Einbeziehung des Managements, die für Projekte solcher Reichweite notwendig ist, bedarf es einer klaren Kommunikation über die Notwendigkeit und die Vorteile solcher Changes. Sonst könnten sich die Mitarbeiter schnell bevormundet fühlen.

Dass es auch etwas zu gewinnen gibt, spüren die Mitarbeiter nach der Migration, wenn sie beispielsweise innerhalb kürzester Zeit ihre beantragten Berechtigungen auf eine Projektablage erteilt bekommen, auf die sie früher tagelang warten mussten. Oder wenn sie via Service-Portal selbst Projektablagen einrichten dürfen und Kollegen darauf Rechte vergeben können.

Die richtige Vorgehensweise

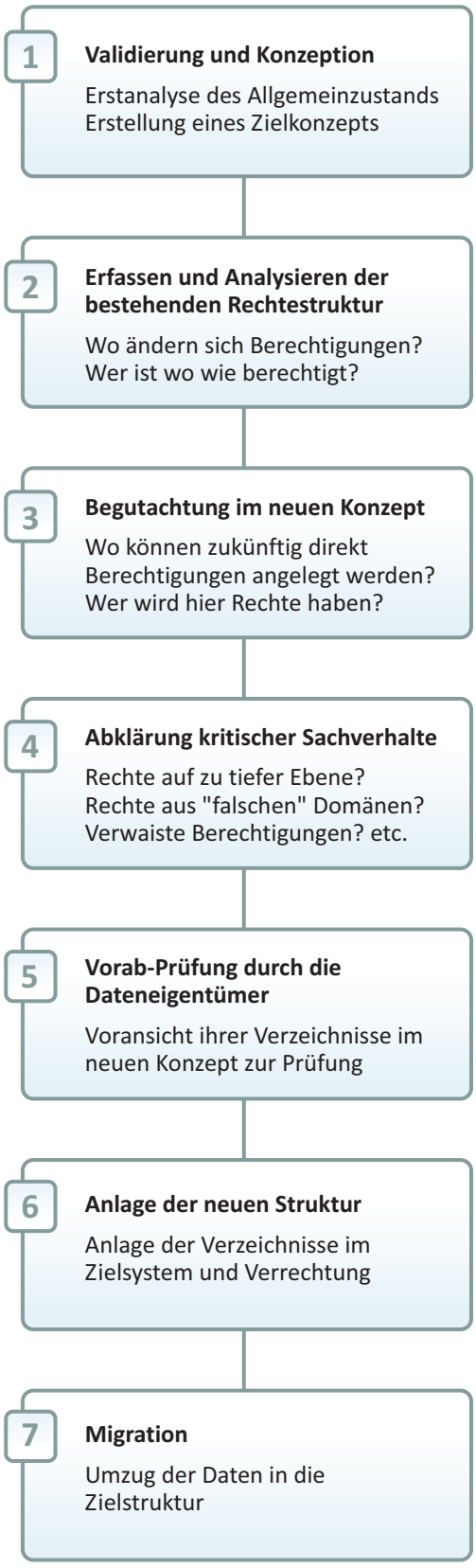
Vor der Entwicklung eines Zielkonzepts steht die **Erstanalyse des Allgemeinzustandes**. Das ist vergleichbar mit dem ersten Blick in den Keller, zur Einschätzung der Situation vor dem großen Aufräumen.

- Wie tief in der Hierarchie liegen Ordner, bei denen sich Rechte ändern?
- Wie hoch ist der Anteil solcher Ordner?
- Ist die Ablagestruktur an sich noch praktikabel?
- Ist ein generelles Aufräumen notwendig oder reicht eine einfache Umstrukturierung schon aus?

Wer sich hier nicht sicher ist, kann über externe Beratung von der Erfahrung Anderer profitieren.

Empfehlungen für die Zielstruktur:

- Weniger komplex, Beschränkung auf zwei bis vier verwaltbare Hierarchie-Ebenen, tiefer liegende Ordner erben die Rechte.
- Beschränkung auf wenige Rechtetypen; „Read“ und „Change“ sind für den normalen User in der Regel ausreichend
- Bei der Änderung der Verzeichnisstruktur, diese besser generisch anlegen oder themen- und projektbezogen ausrichten; organisatorische Gegebenheiten ändern sich erfahrungsgemäß schneller.
- Gliederung der Projekt-Ablagen in eine sinnvolle Struktur, damit dem End-User der schnelle Zugriff garantiert ist.
- Gliederung möglichst unabhängig vom physikalischen Speicherort



In der Konzeptphase sind auch rein technische Einschränkungen zu beachten, beispielsweise die begrenzte Anzahl an Gruppenmitgliedschaften, die im Active Directory möglich sind. Hier kann bei rund 1.000 schon Schluss sein.

Steht das Konzept folgt die **genaue Erfassung des Status Quo**. Schrittweise müssen nun alle Berechtigungsinformationen aus Dateisystemen und Active Directory ausgelesen werden. Eine automatisierte Lösung kann das weitgehend selbstständig übernehmen, ebenso wie die Berechnung der effektiven Rechte und der Punkte im Dateisystem, an denen sich Berechtigungen ändern.

Probleme im Vorfeld der Migration ausräumen

Um schon im Vorfeld zu erkennen, wo bei einer Migration mit Problemen zu rechnen ist, sollten geeignete Migrations-Lösungen in der Lage sein, eine **Darstellung in der neuen Struktur** berechnen zu können. Der Fileservice Migration Manager von econet weist beispielsweise auf wichtige Aspekte hin wie:

- Wo liegen Berechtigungen auf tieferer Ebene, als im neuen Konzept für eine Verwaltung vorgesehen sind?
- Wo kollidieren alte Ordnernamen mit dem neuen Namenskonzept (Umlaute, Leerzeichen, Sonderzeichen etc.)
- Wo gibt es Berechtigungen aus Domänen, die nicht mehr berechtigt sein sollen?
- Wo existieren verwaiste Berechtigungen?
- Wo gibt es Spezialrechte, die nicht im neuen Konzept vorgesehen sind?
- Gibt es noch verschachtelte Gruppenstrukturen, die aufgelöst werden müssen?

Hier hält eine Tool-Unterstützung nicht nur den Aufwand in engen Grenzen sondern sie identifiziert auch Schwachstellen und hilft bei der **Klärung der kritischen Sachverhalte**, bevor sie sich zu den gefürchteten negativen Auswirkungen einer Migration auswachsen können.

Als nächstes folgt die **Überprüfung durch die Dateneigentümer**. Die Zeiten in denen sie endlose Excel-Listen mit kryptischen Account- und Gruppennamen für einen Rechteabgleich vorgesetzt bekamen, sollten vorbei sein. Heutzutage lassen sich ihre Folder-Strukturen als „business-verständliche“ Darstellungen im Dateibaum präsentieren, zusammen mit passenden Gruppenberechtigungen und Namen der Berechtigten.

Auch muss die Kommunikation zwischen Dateneignern und Migrationsbeauftragten nicht mehr via E-Mail und Telefon laufen, sondern lässt sich gut über Workflows in einem Service-Portal abwickeln.

Sachverhalte, die eine Klärung des Dateneigners erfordern, müssen für ihn ersichtlich sein. Beispielsweise Ordner, die eine direkte Rechteverwaltung benötigen, aber in einer tieferen Ebene liegen würden, als im neuen Konzept veranschlagt. In solchen Fällen sind die Eigner in der Regel verpflichtet, in einer bestimmten Zeitspanne die Ordner in höhere Ebenen umzuziehen und so Zug um Zug konform zu werden.

Automatisierungspotenzial nutzen

Sind alle Sachverhalte geklärt und der Dateneigner gibt via Serviceportal sein Einverständnis, kann die **Anlage der neuen Struktur im Zielsystem** und die entsprechende Verrechtung der Verzeichnisse erfolgen. Auch das kann ein modernes Migrations-Tool. Es nutzt dazu die Informationen aus den vorangegangenen Prozessen. Dann kann der eigentliche **Umzug der Daten** von der alten in die neue Struktur erfolgen.

Damit aus einem so aufgeräumten Dateisystem mit korrespondierenden Berechtigungsgruppen im Active Directory und mit übersichtlichen Hierarchie-Ebenen und Zugriffstypen nicht in absehbarer Zeit wieder ein sogenanntes „gewachsenes Dateisystem“ wird, empfiehlt sich ein regelkonformes Berechtigungs-Management mit Genehmigungs-Workflows, so wie es der Identity & Service Manager von econet großen Unternehmen und IT-Service-Anbietern ermöglicht.

Damit wäre dann der Kreislauf von der Anforderung von Berechtigungen bis zur ihrer Validierung geschlossen und die geforderte Transparenz und Kontrolle auf dem Gebiet der Zugriffsrechte auf Informationen ist gewährleistet.

Tool-Unterstützung bei der Konsolidierung

Der Fileservice Migration Manager von econet

econet begleitet seit Jahren große Unternehmen bei komplexen Konsolidierungsprojekten mit fundiertem Beratungswissen und der Erarbeitung individueller Dateisystem- und Berechtigungskonzepte.

Das eigens für diese Projekte entwickelte Tooling - der Fileservice Migration Manager - steht nun allen Unternehmen zur Verfügung, die unter dem Druck von Revision und Regularien klare Verhältnisse in ihre Daten- und Zugriffsverwaltung bringen müssen.

Mit dem für solche Massenoperationen nötigen hohen Grad an Automatisierung und mit abgesicherten Workflows unterstützt der Fileservice Migration Manager die verschiedenen Schritte bis zur Migration der Daten.

Der Fileservice Migration Manager ist ein zentrales Teilstück im methodischen Ansatz von econet. In überschaubaren Schritten reicht er von der Berechtigungsanalyse über die Dateisystemkonsolidierung bis zum sicheren und effizienten Fileservice Management mit Genehmigungs-Workflows.

Mit einer sauberen Methodik und dem Einsatz von geeignetem Tooling lassen sich gewachsene Dateisysteme samt Berechtigungen konsolidieren und auf Dauer transparent halten.

1 Rechte- & Risiko-Analyse

Erfassen aller Berechtigungen im Dateisystem: Wer darf was?

Erfassen der Dateisystemstruktur: Wo ändern sich Berechtigungen?

-> Reports

- Berechtigungen und Strukturen
- Risiken und deren Bewertung

Zuverlässige Datenbasis für die anstehende Konsolidierung ->

econet Reporting Studio

2 Konsolidierung

Erarbeitung eines Dateisystem-konzepts mit nur wenigen verwalteten Ebenen

Tool-unterstützte Anpassung von Folder-Struktur und Berechtigungen

-> Berechtigungen, die erhalten bleiben sollen, bleiben erhalten

-> Rechteinformationen im Dateisystem korrespondieren mit denen im Active Directory

Vorraussetzung für die automatisierte Verwaltung ->

econet Migration Manager

3 Fileservice Management

Import von Rechteinformationen und Metadaten (z. B. Kostenstelle, Verantwortliche etc.) in cMatrix

Prozess-orientiertes Management von Fileservices mit sicherer Steuerung der Berechtigungen

-> Prozesse bei der Rechtevergabe sind klar definiert und durchgängig automatisiert z. B. kontrollierte Self-Services

-> Prozesse bei der Versorgung mit Dateiablagen sind einheitlich und effizient

-> Sicheres Deprovisioning

-> Regelverstöße bei der Rechte-vergabe werden erkannt

-> Alle Prozesse sind dokumentiert

econet Fileservice Management

econet

Microsoft Partner
Gold Independant Software Vendor (ISV)
Cloud Essentials Partner

econet GmbH
Landaubogen 1
81373 München
Tel. +49 89 514 510
info@econet.de
www.econet.de

econet steht seit Jahren Organisationen bei der Konsolidierung ihrer Dateisysteme zur Seite. Dax-Unternehmen wie der Siemens AG ebenso wie dem gehobenen Mittelstand oder großen Behörden wie der Stadt Köln. Sei es im Rahmen von Umorganisationen, im Zuge von Migrationen oder auf Verlangen der Revision mit dem Ziel einer sauberen Access Governance. Schwerpunkte dabei sind Analysen von Benutzerrechten und Zugriffsrisiken in Dateisystemen, Erstellen von Berechtigungskonzepten, Einführung von Antrags- und Genehmigungsverfahren und effizientes Fileservice Provisioning.
Mehr erfahren Sie unter www.econet.de