

Unstrukturierte Daten wachsen exponentiell. Unternehmen aller Größenordnungen sehen sich einer zunehmenden Datenflut ausgesetzt, die verfügbar gehalten werden muss. In einem typischen Fortune 1000-Unternehmen wachsen unstrukturierte Daten jährlich mit ca. 30% (vgl. Gartner). Ein Großteil der Daten können als unternehmenskritisch eingeschätzt werden, da sie entweder personenbezogenen Inhalt haben oder als vertrauliche Daten gelten. Dieses rasante Wachstum führt dazu, dass sicherheitsrelevante Fragen immer schwerer beantwortet werden können:

- Wer hat welche Berechtigungen?
- Wer hat auf welche Daten tatsächlich zugegriffen?
- Wer sollte auf welche Daten zugreifen können?
- Wer ist der „Data Owner“?

Der erhebliche Kostendruck in der Administration und die dadurch reduzierten Mittel zur Überprüfung der Berechtigungen führen zu einem Aufweichen der Sicherheitsregeln. Dies bedeutet: Unternehmen setzen Berechtigungen in vielen Fällen so, dass unternehmenskritische Daten im Zugriff zu vieler Mitarbeiter sind. Dies stellt nicht nur ein finanzielles wie auch ein Sicherheitsrisiko dar sondern auch einen rechtlichen Verstoß. So gibt es mehrere rechtliche Regularien, die eindeutig vorgeben, wie Berechtigungen auf personenbezogene als auch auf unternehmenskritische Daten zu regeln sind. Der folgende Text zeigt auf, welche regulatorischen Maßgaben existieren und wie adäquat auf diese Herausforderung reagiert werden kann.

Varonis DatAdvantage

Varonis DatAdvantage ist eine Lösung zur Optimierung von Daten- und Berechtigungsmanagement auf Windows und Unix File Servern, NAS-Devices, Exchange und Microsoft Share Point. Über standardisierte Workflows und eine zentrale administrative Oberfläche bietet Varonis die optimale Voraussetzung, um Daten zu analysieren, zu reporten und Filesysteme zentral unter Kontrolle zu halten und so rechtlichen Regularien zu entsprechen.

DatAdvantage Features

Feature 1: Bidirektionale Sicht

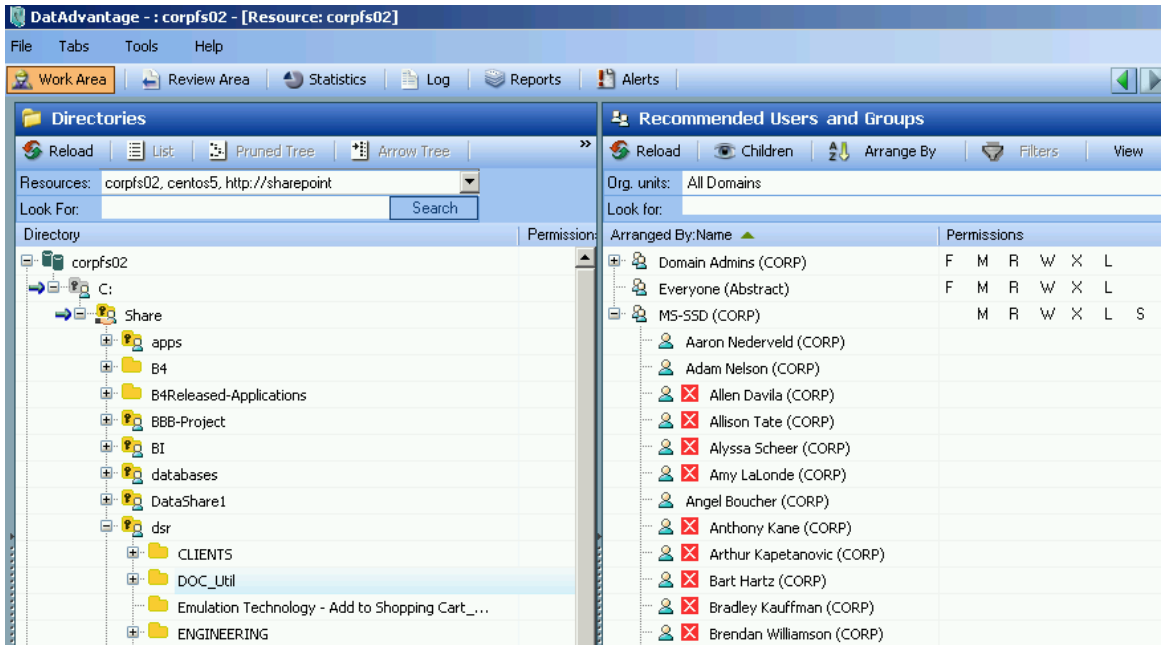
Diese Funktion ermöglicht einem Administrator, ohne Aufwand eine zentrale Übersicht über die gesamten Filesystemberechtigungsstrukturen zu erhalten. Dies wird von Varonis DatAdvantage durch das Auslesen/Scannen der Benutzer und Gruppen aus dem Active Directory, der ACLs und der Ordnerstruktur möglich. Die Kombination ermöglicht eine zentrale und visuelle Wiedergabe. Es ist zu ersehen, wer an welchem Ordner welche Rechte hat und warum. Ungeachtet von Verschachtelung oder von direkten Berechtigungen. Dies liefert die Grundlage, um Berechtigungskonzepte zu prüfen, zu überarbeiten, aufzuräumen oder auch Filesysteme zu migrieren. Desweiteren kann direkt aus der zentralen administrativen Oberfläche eine Berechtigungsänderung/-säuberung durchgeführt werden. Alle Berichte sind auch per Report darstellbar. Die Reports können per Mail in verschiedensten Formaten versendet werden. Durch diese Funktionalität können Fragen beantwortet werden wie z.B.:

- An welchen Ordnern haben globale Gruppen (z.B. Jeder) Zugriffsrechte?
- An welchen Ordner hat ein gewisser User Zugriffsrechte?
- Welche Personen und Gruppen haben auf einen Ordner Zugriffsrechte?

DatAdvantage Features

Feature 2: Berechtigungsvorschläge

Mit der Berechtigungsvorschläge-Funktion bietet Varonis DatAdvantage einen einzigartigen Prozess zum Aufzeigen und Eliminieren von Überberechtigungen. So kann sicher gestellt werden, dass Mitarbeiter nur die Berechtigungen an Daten haben, die Sie auch wirklich zum täglichen Arbeiten benötigen. Überberechtigungen können vielfältige Gründe haben, so z.B. Abteilungswechsel oder Mitarbeit in Projekten. Varonis erkennt Berechtigungen, die Benutzer zu Unrecht führen und macht konkrete Vorschläge, diese zu beseitigen. Darüber hinaus können in diesen Prozess Data-Owner (Fachverantwortliche) involviert werden.



Feature 3: Audit Trail

Mit dem Audit-Trail bietet Varonis DatAdvantage eine 100%ige Nachvollziehbarkeit zur Frage der Datenverwendung in Unternehmen. Varonis loggt die Filesystem- Events (CIFS, NFS). Konkret kann nachvollzogen werden, ob eine Datei geöffnet, erstellt, gelöscht, umbenannt, verschoben oder verändert wurde. Diese Events werden in einer zentralen Datenbank abgelegt und können durchsucht, sortiert und gruppiert werden. Events werden nicht nur für Benutzer, sondern auch für lokale Administratoren erstellt. Die Filesystem-Events werden über Standardschnittstellen geloggt- ohne das Aktivieren der Microsoft Auditing-Funktion.

