

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.

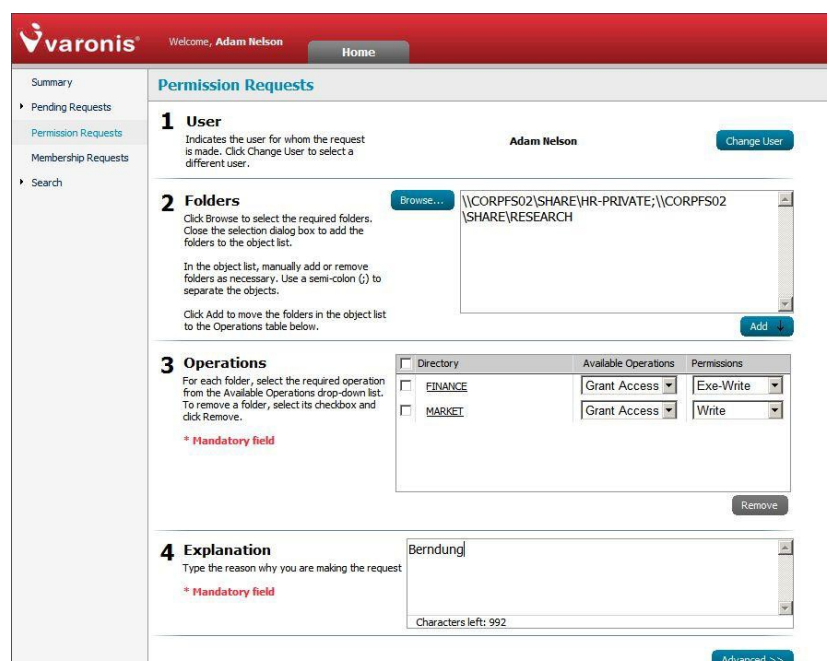
Varonis DataPrivilege

Varonis DataPrivilege ermöglicht es, die Verantwortung für das Management der Datenzugriffsberechtigung vom IT-Bereich auf die Business Owners ohne Änderungen der Infrastruktur oder Unterbrechungen im Firmengeschäft zu übertragen. DataPrivilege bringt Dateninhaber und Datenbenutzer in einem Forum zur Kommunikation, Autorisierung und Aktivierung von Berechtigungen zusammen. Varonis DataPrivilege erlaubt es, ein geschlossenes Umfeld zur Datenzugriffsberechtigung zu schaffen und dabei die Verantwortlichkeit zu verbessern und Risiken zu verringern.

DataPrivilege Features

Webbasierte Berechtigungsanfrage

Mit Varonis DataPrivilege implementieren Sie einen webbasierten Prozess zur Berechtigungsvergabe auf bestehende Ordnerstrukturen: Ein Mitarbeiter erfragt über eine Website Berechtigungen an einem Ordner bzw. mehreren Ordnern. Die Website, über welche die Anfrage gestellt wird, kann in vorhandene Systeme eingebunden werden (z.B. Intranet). Sobald der Mitarbeiter die Anfrage bestätigt, wird diese dokumentiert und aufgezeichnet. Desweiteren wird eine Mail generiert, die an den vorher definierten Business Owner versandt wird. In dem Prozess können mehrere Business Owner definiert werden. Der Mitarbeiter kann zu jedem Zeitpunkt den Bearbeitungsstand über das Webinterface abfragen.



The screenshot shows the 'Permission Requests' form in the Varonis DataPrivilege web interface. The form is titled 'Permission Requests' and is divided into four main sections:

- 1 User:** Indicates the user for whom the request is made. The user is 'Adam Nelson'. There is a 'Change User' button.
- 2 Folders:** Click Browse to select the required folders. Close the selection dialog box to add the folders to the object list. In the object list, manually add or remove folders as necessary. Use a semi-colon (;) to separate the objects. Click Add to move the folders in the object list to the Operations table below. The object list contains: \\CORPFS02\SHARE\HR-PRIVATE; \\CORPFS02\SHARE\RESEARCH.
- 3 Operations:** For each folder, select the required operation from the Available Operations drop-down list. To remove a folder, select its checkbox and click Remove. The table below shows the selected operations for the folders:

Directory	Available Operations	Permissions
<input type="checkbox"/> FINANCE	Grant Access	Exe-Write
<input type="checkbox"/> MARKET	Grant Access	Write
- 4 Explanation:** Type the reason why you are making the request. The explanation is 'Berndung'. There is a 'Characters left: 992' indicator.

DataPrivilege Features

Webbasierte Gruppenmitgliedschaftsanfrage

Mit Varonis DataPrivilege implementieren Sie einen webbasierten Prozess zur Mitgliedschaftsanfrage auf bestehende Gruppen: Ein Mitarbeiter erfragt über eine Website Gruppenmitgliedschaften an bzw. mehreren Gruppen. Die Website, über welche die Anfrage gestellt wird, kann in vorhandene Systeme eingebunden werden (z.B. Intranet). Sobald der Mitarbeiter die Anfrage bestätigt, wird diese dokumentiert und aufgezzeichnet. Desweiteren wird eine Mail generiert, die an den vorher definierten Business Owner versandt wird. In dem Prozess können mehrere Business Owner definiert werden. Der Mitarbeiter kann zu jedem Zeitpunkt den Bearbeitungsstand über das Webinterface abfragen.

The screenshot shows the 'Membership Requests' page in the Varonis DataPrivilege web interface. The user is Adam Nelson. The page is divided into four main sections:

- 1 User:** Indicates the user for whom the request is made. The user is Adam Nelson. There is a 'Change User' button.
- 2 Groups:** Click Browse to select the required groups. The selection dialog box shows 'CORP(Group_Finance)'. There is an 'Add' button.
- 3 Operations:** A table with columns 'Display Name' and 'Available Operation'. The table contains one row: 'Group_Finance (CORP)' with the available operation 'Grant membership'. There is a 'Remove' button.
- 4 Explanation:** Type the reason why you are making the request. The explanation is 'Grund'. There is a 'Characters left: 995' indicator and an 'Advanced >>' button.

"With Varonis® DatAdvantage® and DataPrivilege® we have automated the process of identifying folder ownership, managing folder permission requests, tracking changes and we have been able to identify orphaned groups within the Active Directory — 1800 to date."

Elroy Overdijk Ziggo

Webbasierte Berechtigungs- und Gruppenmitgliedschaftserteilung

Sobald ein Benutzer eine Berechtigungs- oder Gruppenmitgliedschaftsanfrage gestellt hat, erhält der Verantwortliche auf der Fachseite eine Benachrichtigung per Mail, dass er diese Anfrage frei geben kann oder muss. Über das Webinterface sieht er die Anfrage und kann diese entsprechend bearbeiten. So ist es ihm möglich, diese Anfrage zu verwerfen, ihr zuzustimmen oder auch nur zeitlich eingeschränkt zu entsprechen. Alle Aktionen werden dokumentiert und lassen sich im Nachgang nachvollziehen.

The screenshot shows the 'Request Details' page in the Varonis DataPrivilege web interface. The request is pending. The details are as follows:

- Request ID:** 35
- Request Operation Type:** Grant Access
- Requested For:** Entity Name: Adam Nelson, Logon Name: AdamNelson, Domain Name: CORP, Department: Engineering
- Permissions For Directory:** Path: \\CORPFS02\SHARE\FINANCE, Requested: Exe-Write, Membership to: Exe-Write - Group_Finance
- Expiration Date:** Never (selected), On: May 31, 2011, After: days
- Authorizers:** Erin Manning, Dir. Owner
- Request Reason:** need for Job
- Authorization Explanation:** Grund
- Authorization:** Approve (selected), Decline

DatPrivilege Features

Entitlement Review

Das regelmäßige Überprüfen von gewährten Berechtigungen ist extrem wichtig, da nur so Überberechtigungen auf Dauer verhindert werden können. Berechtigungen müssen an geänderte Strukturen fortlaufend angepasst werden. Hierzu gibt es den Prozess des Entitlement Reviews. Hier wird dem Data Owner in einem festgesetzten Intervall (z.B. einmal im Quartal) eine Mail gesendet mit der Bitte über das Webinterface Berechtigungen zu überprüfen und gegebenenfalls diese zu entziehen. Über den Workflow kann gesteuert werden was passieren soll wenn der Data Owner seiner Aufgabe nicht nachkommt. Eine Möglichkeit wäre eine Erinnerung zu schreiben oder den Vorgang an eine andere Person weiterzuleiten.

Entitlement Review Details -- Webpage Dialog

Request ID: 7706
Request Type: Entitlement Review

Folder Name: CONTROLLERS
Full Name: \\CORPFS02\SHARE\FINANCE\CONTROLLERS

Review only objects that have changed since your last review ?
 Review only actionable objects

View: Users' effective permissions

Status	User	Group	Permission	Decision And Explanation
	Anne Thornton (CORP)	NTFS-Contro... (CORP)	Exec-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Erin Manning (CORP)	NTFS-Contro... (CORP)	Exec-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Margaret Coakley (CORP)	NTFS-Contro... (CORP)	Exec-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Maria Hirasaki (CORP)	NTFS-Contro... (CORP)	Exec-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Michael Federle (CORP)	NTFS-Contro... (CORP)	Exec-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Nathan Sonneborn (CORP)	NTFS-Contro... (CORP)	Exec-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove

Total 6 Records
No. Of Rows: 7

Reason: Grund

Authorizers:

Name	Role
Erin Manning	Dir. Owner

Total 1 Record
No. Of Rows: 3

I confirm that I have reviewed the objects listed above, along with their content.
Type the word 'Verify'. Verify

Data last synchronized with environment: May 14, 2011 11:32:35 AM

Sign Cancel

Unterstützte Plattformen

- Windows Server
- NetApp (NTFS)
- EMC (NTFS)
- BlueArc (NTFS)

Ihr Partner für IT Security und IT Automation

Deutschland / Österreich:
IBV Informatik GmbH
Junkersstrasse 5
DE-82178 Puchheim

Tel: +49 89/800 70 98 290
Fax: +49 89/800 70 98 299

Schweiz:
IBV Informatik AG
Schönenwerdstrasse 7
CH - 8902 Urdorf

Tel. +41 44/745 92 92
Fax +41 44/ 745 92 93

