Daten-Audit mit VARONIS

17. April 2018

SEW EURODRIVE

ICS Stuttgart mbuf
16.&17. April 2018
mbufJK18
Kongress für Microsoft Business User

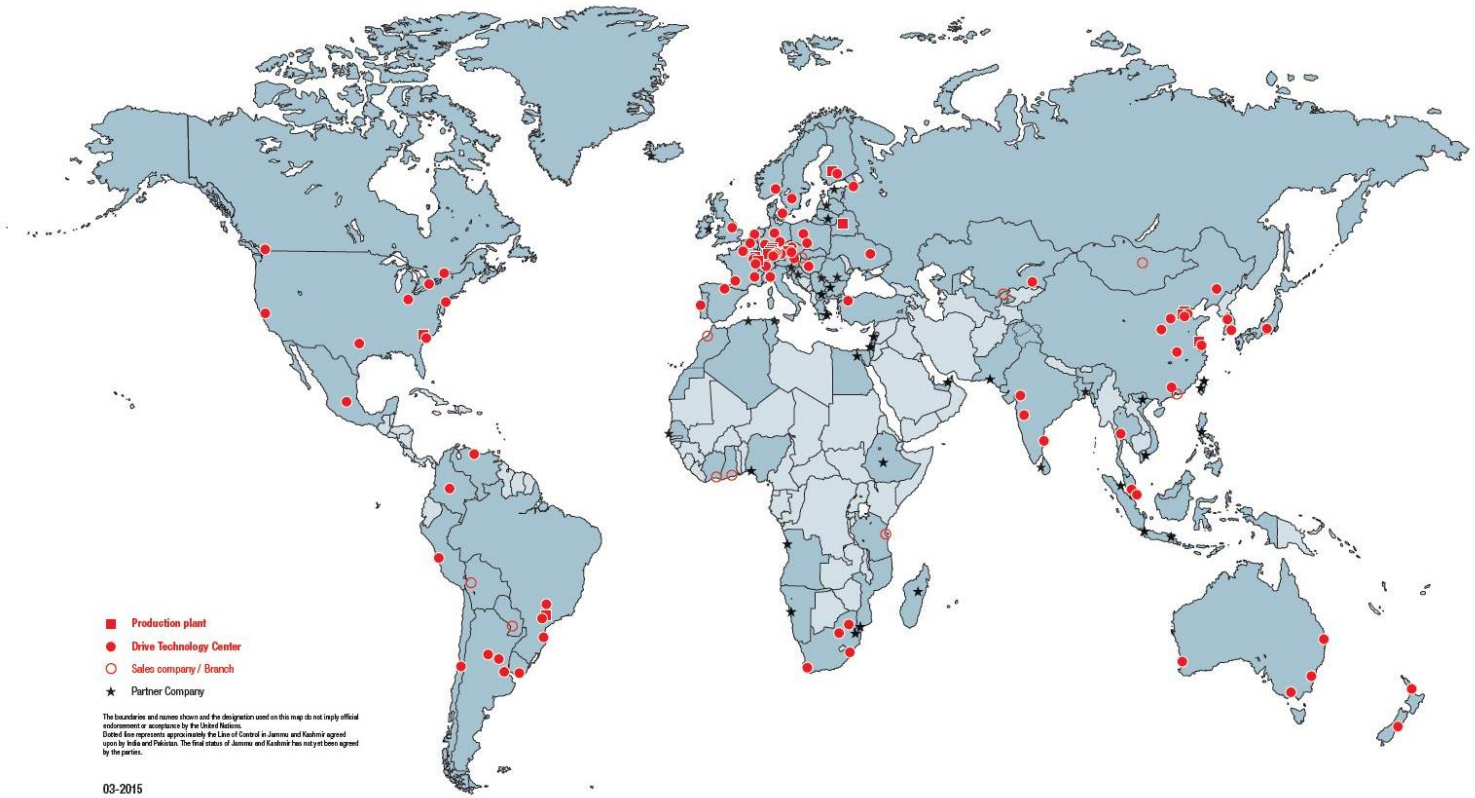
Bernhard F. Haungs
IT-Compliance & Information Security / ITC
Datenschutzbeauftragter

SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42
D-76646 Bruchsal

Tel. +49 7251 75-1606
Fax +49 7251 75-501606
Mobil +49 172 7261301
bernhard.haungs@sew-eurodrive.de
http://www.sew-eurodrive.de


SEW
EURODRIVE

International denken, national handeln



Über 17.000 Mitarbeiter	14 Fertigungswerke 82 Drive Technology Center	Standorte in 52 Ländern	3 Mrd. € Umsatz GJ 2016/2017	Seit über 85 Jahren

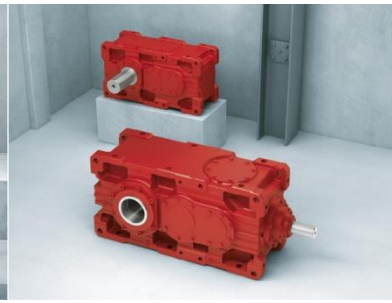
Komplettprogramm

Die Antriebstechnik von SEW-EURODRIVE steht für Produktvielfalt, Qualität, Zuverlässigkeit und Innovationskraft.

- Getriebemotoren und Frequenzumrichter
- Servo-Antriebssysteme
- Dezentrale Antriebssysteme
- Industriegetriebe
- Antriebsautomatisierungslösungen
- Systemkomponenten und Dienstleistungen







Unsere Branchenkompetenz

Ohne die Antriebstechnik von SEW-EURODRIVE würde auf der Welt vieles stillstehen. Mit Produktvielfalt und Kundennähe begegnen wir den Anforderungen der unterschiedlichsten Branchen und schaffen neue Standards im Markt.

– Transport und Logistik
– Automobilindustrie
– Nahrungsmittel- und Getränkeindustrie
– Bau- und Baustoffindustrie
– Chemie- und Pharmaindustrie
– Holzindustrie, u.v.a.m.



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Management Service

ZERTIFIKAT

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
bescheinigt, dass das Unternehmen

SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42, 76646 Bruchsal, Deutschland
Ernst-Blickle-Str. 1, 76676 Graben-Neudorf, Deutschland
Christian-Pähr-Straße 10, 76646 Bruchsal, Deutschland

für den Geltungsbereich

Information Technology Services
- Entwicklung, Implementierung,
Betrieb und Support von IT-Services

ein Informationssicherheitsmanagementsystem
gemäß „Erklärung zur Anwendbarkeit" eingeführt hat und anwendet.
Durch ein Audit, Bericht-Nr. **70020679**,
wurde der Nachweis erbracht, dass die Forderungen der

ISO/IEC 27001:2013

erfüllt sind.
Dieses Zertifikat ist gültig vom **06.03.2018** bis **05.03.2021**.
Zertifikat-Registrier-Nr.: **12 310 24898 TMS**.
Version der Erklärung zur Anwendbarkeit: **1.4; 2017-12-28**.

Product Compliance Management
München, 07.03.2018

DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstraße 65 • 80339 München • Germany TÜV®

M591-41/10

Fragen der Geschäftsführung:

Wo sind eigentlich die Daten der SEW gespeichert?

Wer hat Zugriff auf die Daten?

und vor allem -

Wer erlaubt den Zugriff ?

Daten auf Papier

Elektronische Daten

PC/Notebook mobile Devices Externe Storage	Server / Storage SEW / RZ Bruchsal	SEW EURODRIVES	Extern
• Laufwerk C bei NB/PC (keine Empfehlung) • Kopierte/Synchr. Daten auf iPhone, USB-Sticks u.a. externe Geräte	• Nächste Seite	• Synchronisierte oder kopierte Daten aus Bruchsal • Eigener Fileserver • Eigene PC‘s	• Internet-Auftritt • Wallmedien -Katalog bei SRM • Zollabwickl.
Verantwortlich: Besitzer	**Verantwortlich:** IT und Fachbereich	**Verantwortlich:** Fachbereich und EURODRIVE	**Verantwortlich:** Fachbereich
Maßnahmen: SmartCard / Pin Verschlüsselung, Entsorgung, Corporate USB-Sticks	**Maßnahmen** varonis	**Maßnahmen**: Internationaler Security Level, VPN-Verbindungen	**Maßnahmen**: Security Checks

- Security Policy Anlage 3

Verantwortlich: Ersteller

Maßnahmen: Sensibilisierung, Audit

Daten auf Storage/Server im SEW/RZ Bruchsal

1. Strukturierte Daten	2. Unstrukturierte Daten		
Alle SAP-Systeme, DOXIS, Agile, CAD, Leitrechner usw.	**Exchange / Outlook**	**Fileserver**	**SharePoint/DriveNet**
• Zugriff ausschließlich über Anwendungen • Benutzerverwaltungssysteme • Berechtigungen (Rollen) werden vom Fachbereich via Workflow der IT vorgegeben – IT richtet ein. • Entscheidung obliegt dem Fachbereich, bei dem die Daten entstehen.	• Postfächer: – Zugriffserlaubnis ausschließlich bei Benutzer – Sehr restriktiv bei Anforderung an IT-Service Desk • Öffentliche Ordner - Jeder User legt diese selbst an - User vergibt die Rechte (an User oder an Verteiler)	• Einrichtung der Zugriffsrechte durch IT nach Vorgabe durch den Fachbereich (z. Bsp. : OG_GF/Gruppe/CF) • Fachbereich kann Unterordner kreieren mit „Vererbung“ der übergeordneten Rechte.	• Übergeordnete Struktur wird vorgegeben • Anforderer verteilt und verwaltet Zugriffsrechte
Maßnahmen: Konventionen User-ID‘s, Sicherheitskonzepte, physische Sicherheit uvm	**Maßnahmen:** dto zu strukturierte Daten	**Maßnahmen:** dto zu strukturierte Daten Einsatz „Varonis“. Verschlüsselung auf Fileserver-Ordner. Schlüsselverwaltung ausschließlich im Fachbereich. IT hat keine Möglichkeit des Zugriffs oder der Rekonstruktion	**Maßnahmen:** dto zu strukturierte Daten Einsatz „Varonis“

Produkte im SEW-Einsatz

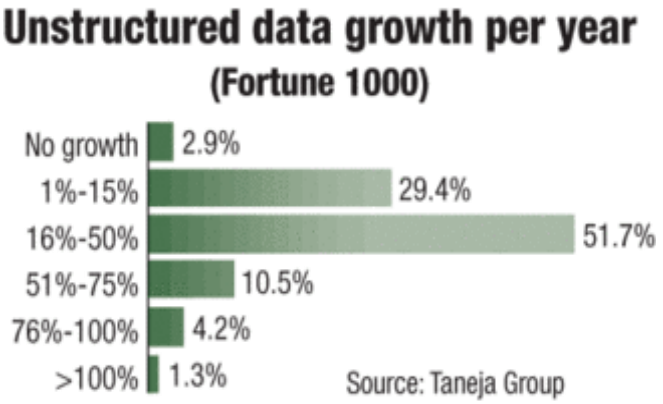
DATADVANTAGE für Filer (NetApp, Windows) seit 2011

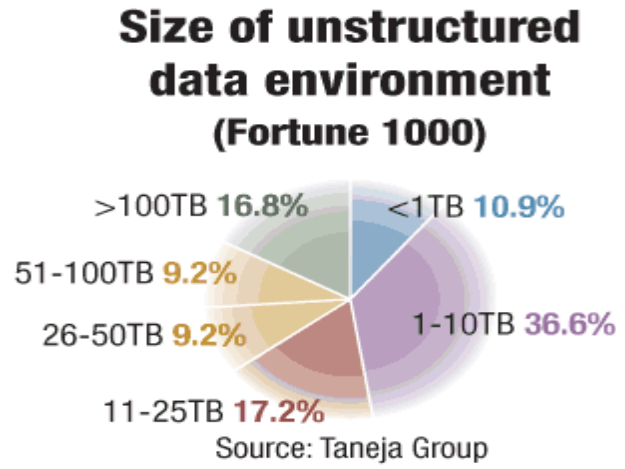
DATADVANTAGE für ActiveDirectory seit 2015

DATADVANTAGE für Sharepoint seit 2016

Probleme bei unstrukturierten Daten

- Mitarbeiter sind in der Regel überberechtigt
- Überprüfung und Einrichten von Benutzerberechtigungen ist sehr aufwändig
- Überprüfung von Datenzugriffen und deren Auswertung ist in der Regel nicht möglich
- Fachverantwortliche sind oft unbekannt
- Wachstum. Heute 1 TB mit 50 % pro Jahr = 57 TB in 10 Jahren !!

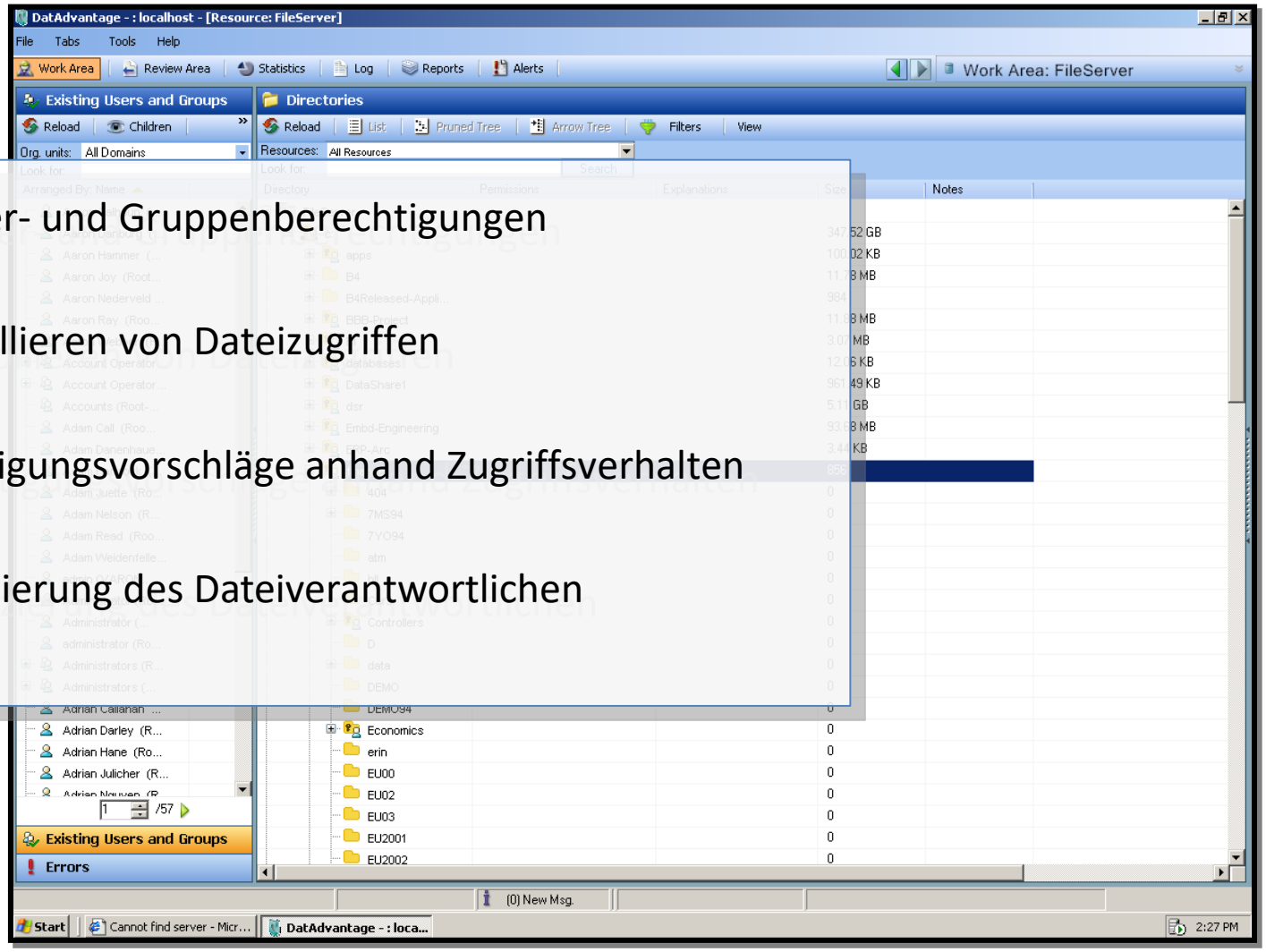




Varonis - DatAdvantage

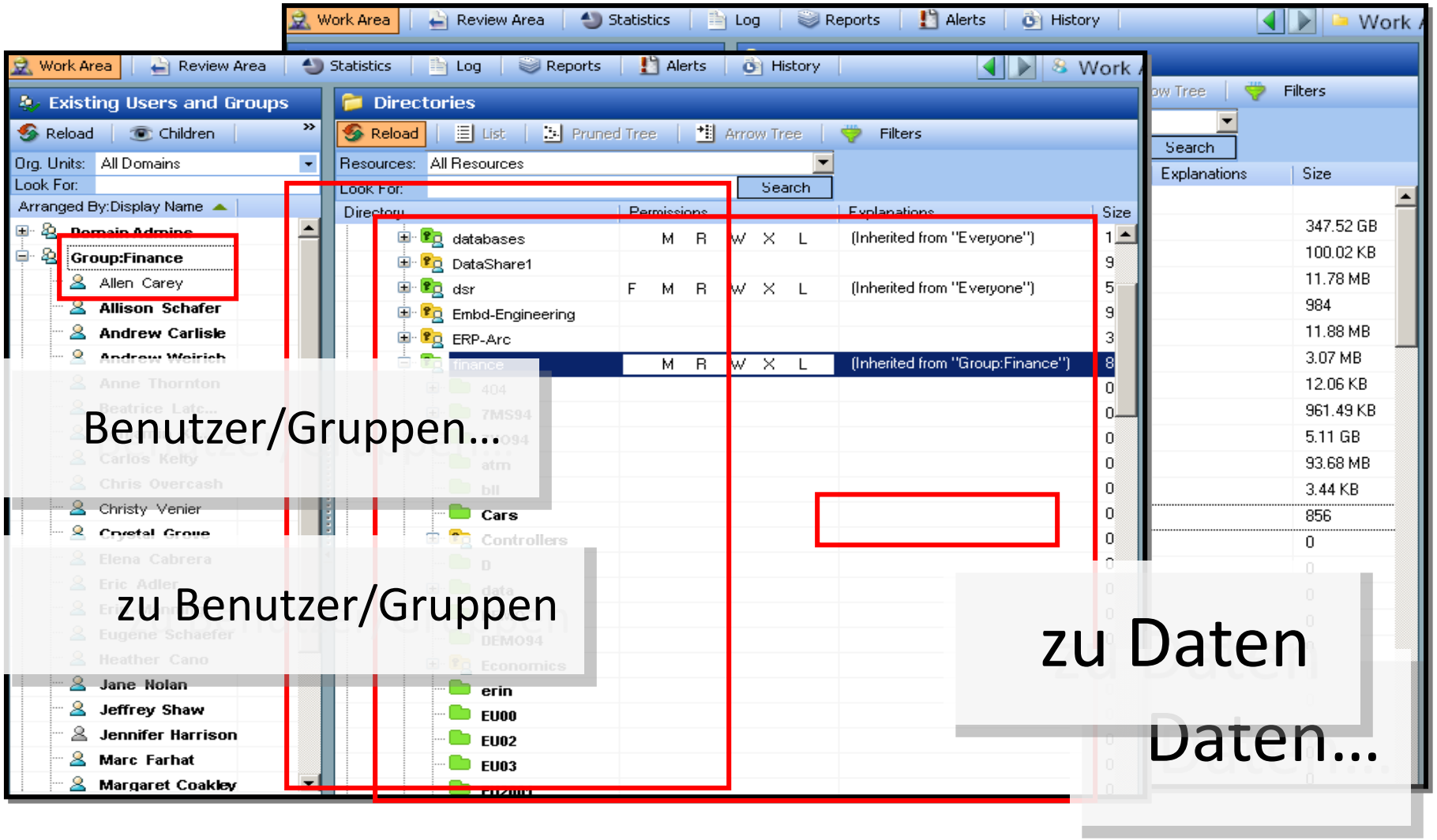
- ✓ Der Zugang und die Nutzung von Daten wird verwaltet
- ✓ Schutz von personenbezogenen und geschäftskritischen Daten
- ✓ Analyse und Überwachung der Zugriffe auf alle Daten von allen Usern
- ✓ Der Zugriff wird protokolliert, nicht die Inhalte
- ✓ Ordner von der Überwachung ausschließen

Varonis- Basisfunktionalitäten

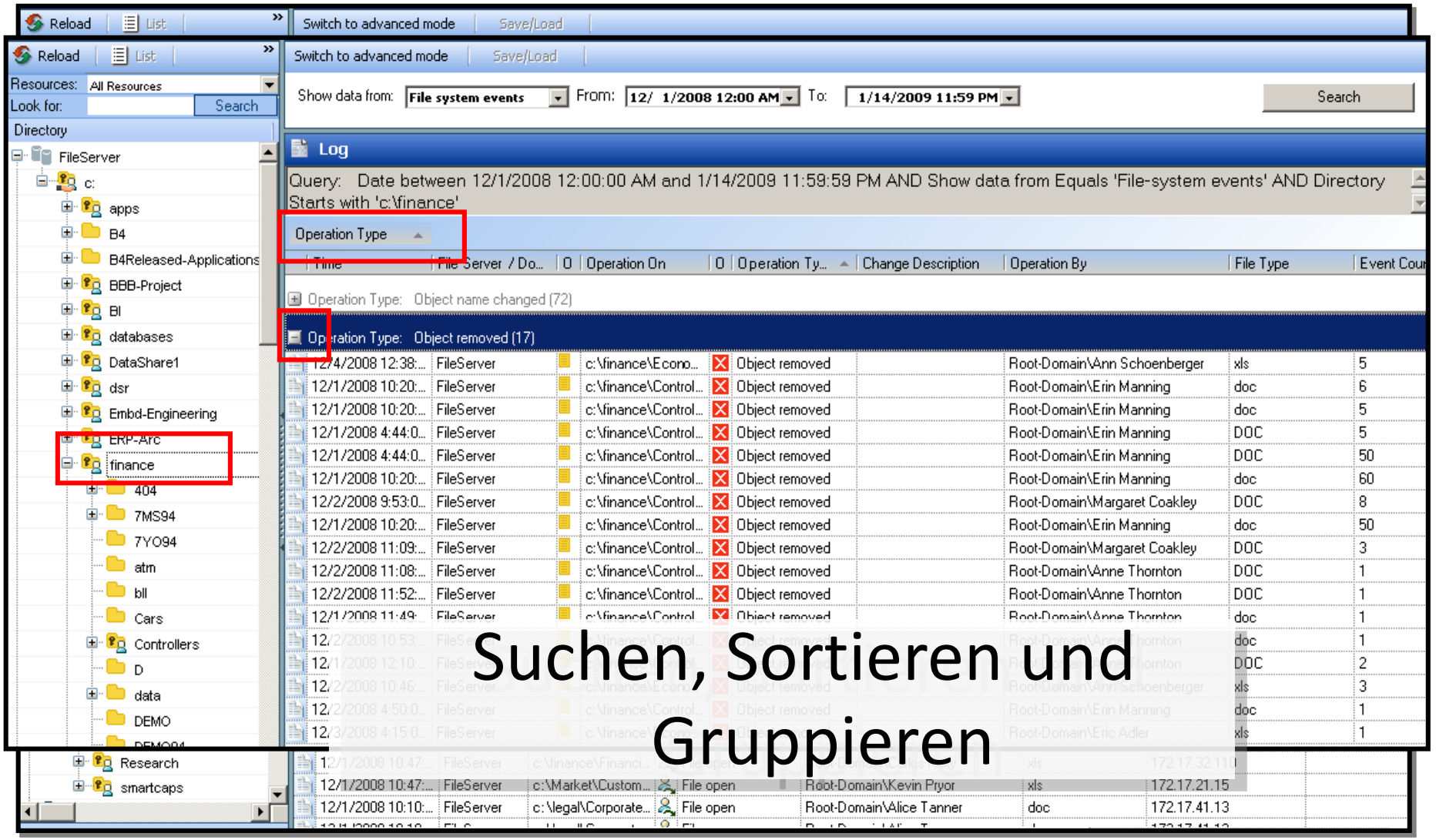


- Benutzer- und Gruppenberechtigungen
- Protokollieren von Dateizugriffen
- Berechtigungsvorschläge anhand Zugriffsverhalten
- Identifizierung des Dateiverantwortlichen

Berechtigungen – Bidirektionale Sicht

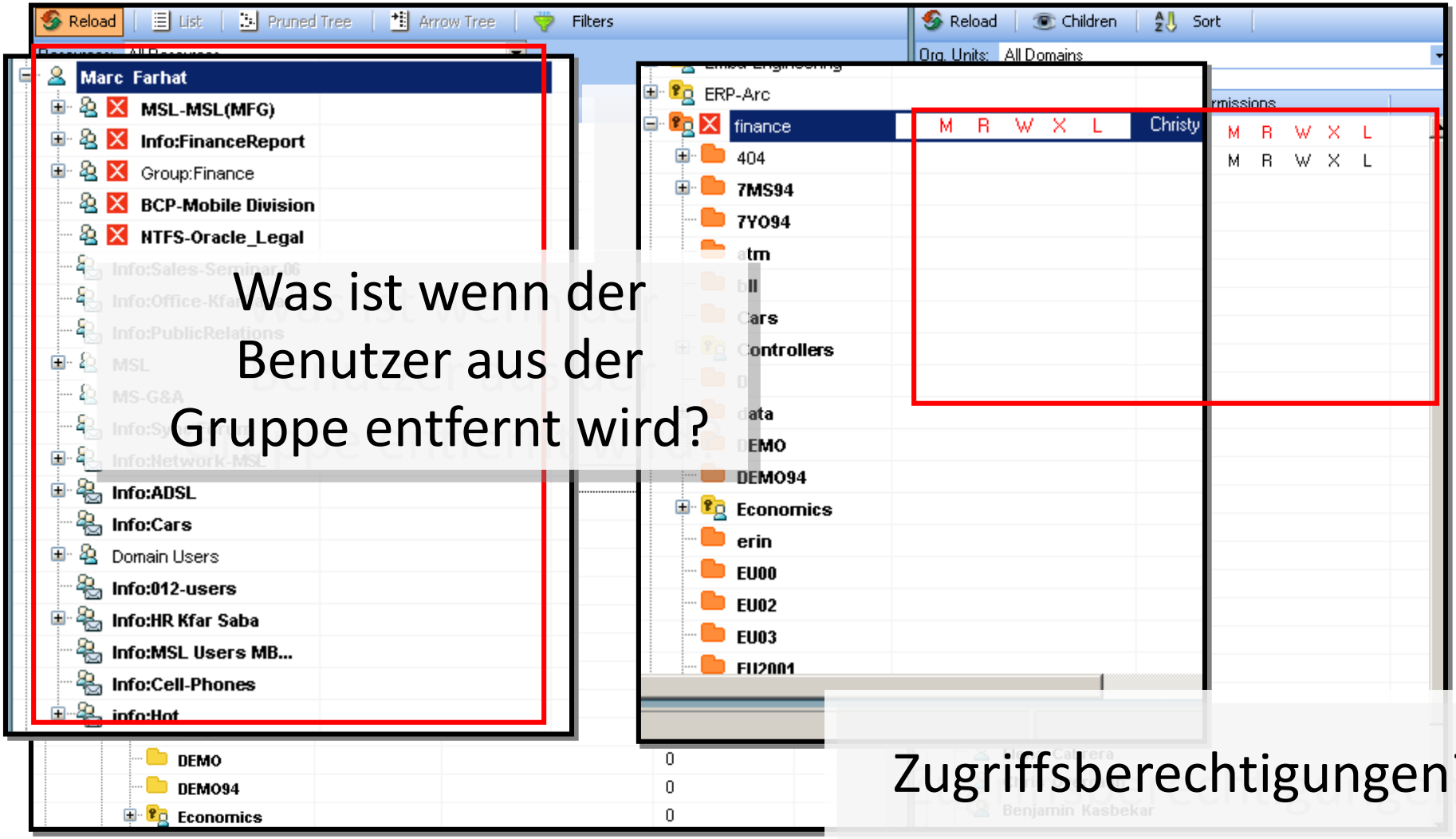


Operationen auf Dateien

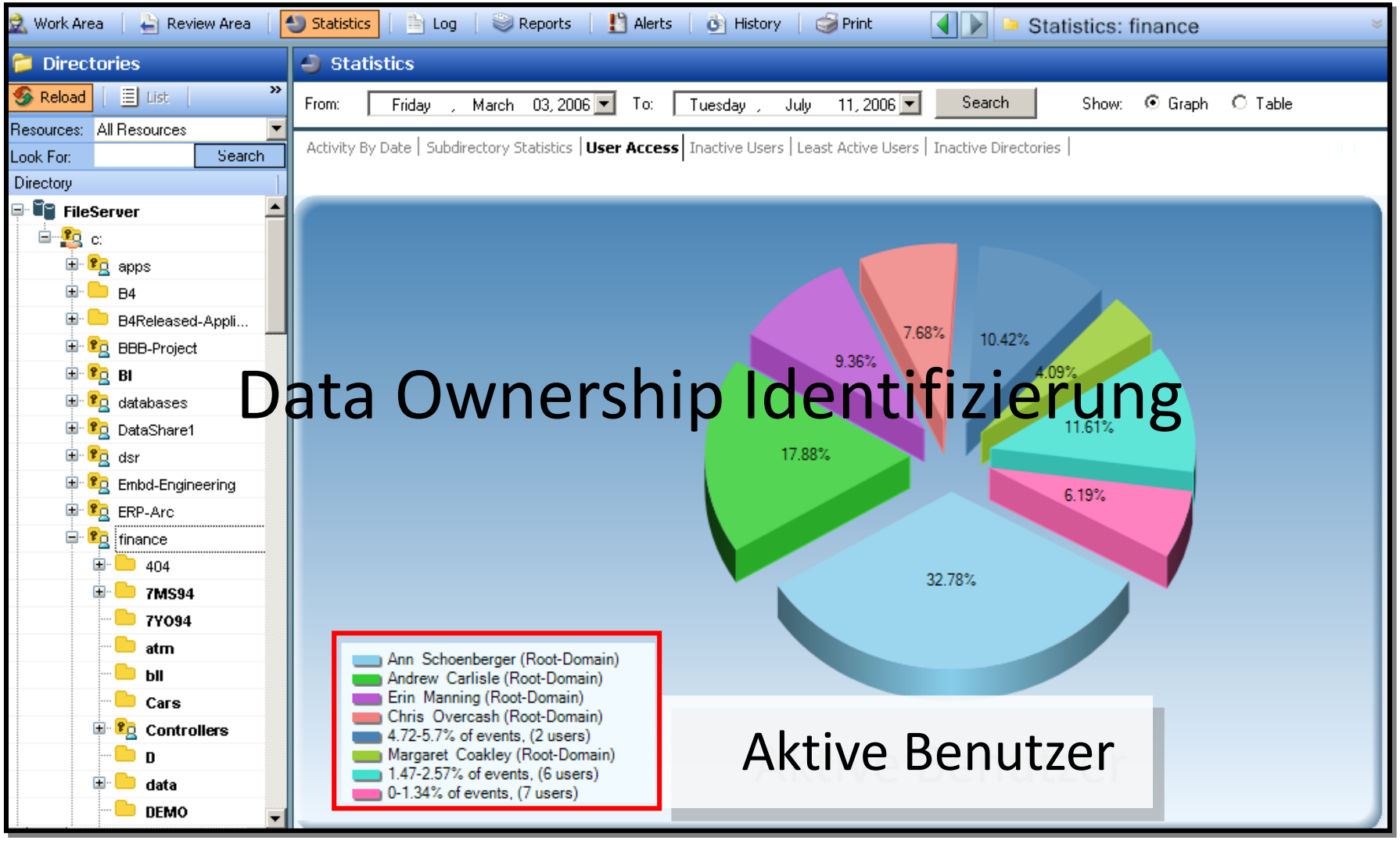


Suchen, Sortieren und Gruppieren

Berechtigungs-Vorschläge



“Data Ownership” Identifizierung



Aktion Rückspiegelung mit Varonis 2014 Wiederholung 2018

Auswertung der kompletten Fileserver nach 18 HAL-Bereiche:

Welche Ordner sind für „jedermann“ (everyone) zugänglich

Auf welche Ordner hat wer Zugriff (Usergruppen / einzelne User)

Welche Ordner wurden gar nicht mehr gelesen (seit Installation varonis)

…….anschließend umfangreiche Bereinigungsmaßnahmen !!

Aktion Rückspiegelung mit Varonis 2014

Mi 06.08.2014 16:22

Haungs, Bernhard

AW: Berechigungen auf Fileserver-Ordnern bei EM

An Herrling, Cornelia; Hagemann, Björn

Cc Schaaf, Andreas

open_EM_CAD-Cluster.xls
0 Bytes

CAD-Data_EM.pdf
0 Bytes

EM_publicstore.pdf
0 Bytes

Sehr geehrte Frau Herrling, sehr geehrter Herr Dr. Hagemann,

anbei die Auswertungen zu Ihrem Bereich.

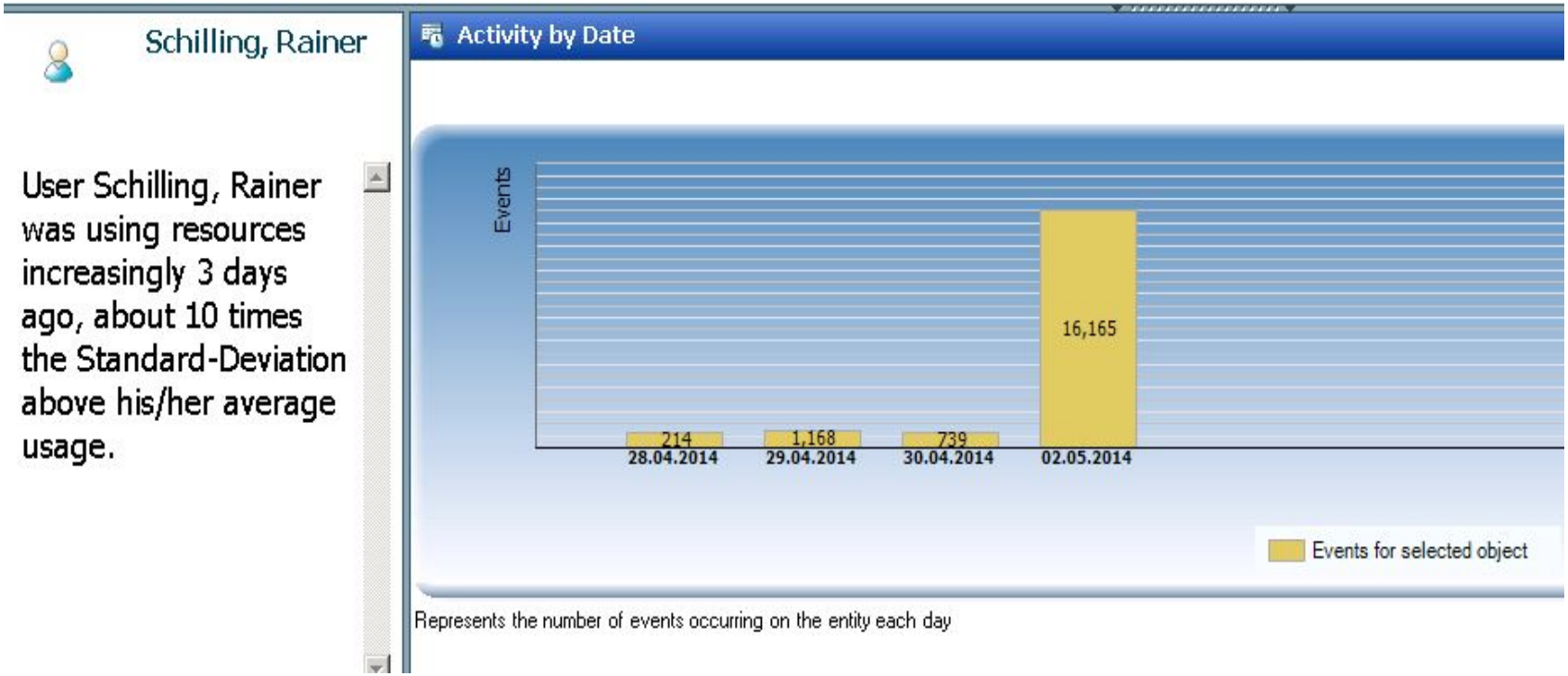
Die Excel-Datei sind die für „jedermann“ offenen Ordner vom Pfad CAD-DATA. Insgesamt 41 Ordner mit allen Unterordnern sind komplett offen!!

Das .pdf CAD-Data_EM zeigt die gesetzten Rechte auf diesem Verzeichnis. Zu beachten ist die Spalte „Current Permission“. „RXL“ steht für Leserecht und „MRWXL“ für Schreib-/Leserecht und bei „L“ sieht der User zwar Ordner und Unterordner, kann aber keine Dateien öffnen. Teilweise sind die User deaktiviert (siehe letzte Spalte).

In der .pdf-Datei zu publicstore haben alle genannten User Schreib/Leserecht.

Falls Sie Änderungen in den Berechtigungen wünschen, dann wenden Sie sich bitte an den ITServiceDesk.

„Anomalieerkennung Fileserver“

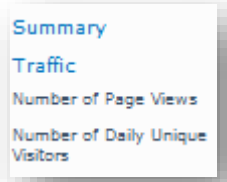


Varonis für SharePoint

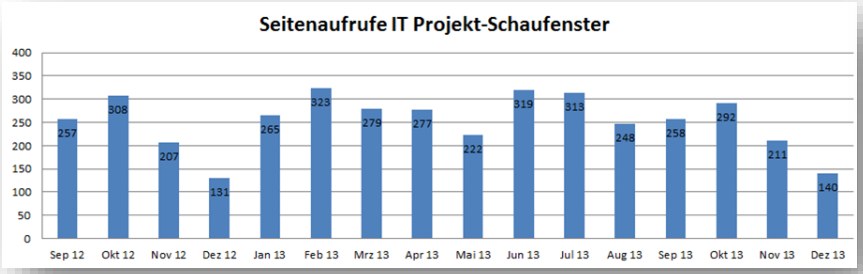
Aktuelle Probleme / Einschränkungen

- Mitarbeiter oft über oder doppelt berechtigt
  - AD / Verteilergruppen + Direkte Rechte Vergabe
- Überprüfung von Benutzerberechtigungen ist sehr aufwendig
  - Vererbung / Gruppen und Berechtigungsstufen sind komplex aufgebaut
- Überprüfung von Datenzugriffen und deren Auswertung ist in der aktuellen SharePoint Version nicht mehr möglich
- Fachverantwortliche / Dateneigner sind oft unbekannt
  - Site-Owner / Beantrager nicht gleichzeitig der aktuelle Ansprechpartner (oftmals aufgrund von Umstrukturierungen)
- Die häufigsten Fragen im Bezug auf DriveShare bei ITSD sind Berechtigungsfragen!

Benutzeranforderungen



- Auswertungen über Seiten / Dokumentzugriffe
  - Sekretariate
  - Schulungsdokumente
  - Welche User können auf welche Inhalte zugreifen?
  - Element / Seiten Zugriffs-Übersichten



	Page URL (under http://optimus:3333/OkeToys)	Number of Page Views
1	/_layouts/dynamicimageprovider.aspx	144
2	/dashboards/burndown.aspx	139
3	/_layouts/tswa/ui/pages/workitems/workitemedit.aspx	136
4	http://portal.geveo.com:3333/oketoys/dashboards/burndown.aspx	77
5	http://portal.geveo.com:3333/oketoys/_layouts/dynamicimageprovider.aspx	42
6	/shared documents/forms/allitems.aspx	34
7	http://portal.geveo.com:3333/oketoys/_layouts/tswa/ui/pages/workitems/workitemedit.aspx	29
8	/_layouts/tswa/ui/pages/workitems/queryresultnw.aspx	18
9	/_layouts/listfeed.aspx	16
10	/_layouts/inplview.aspx	11

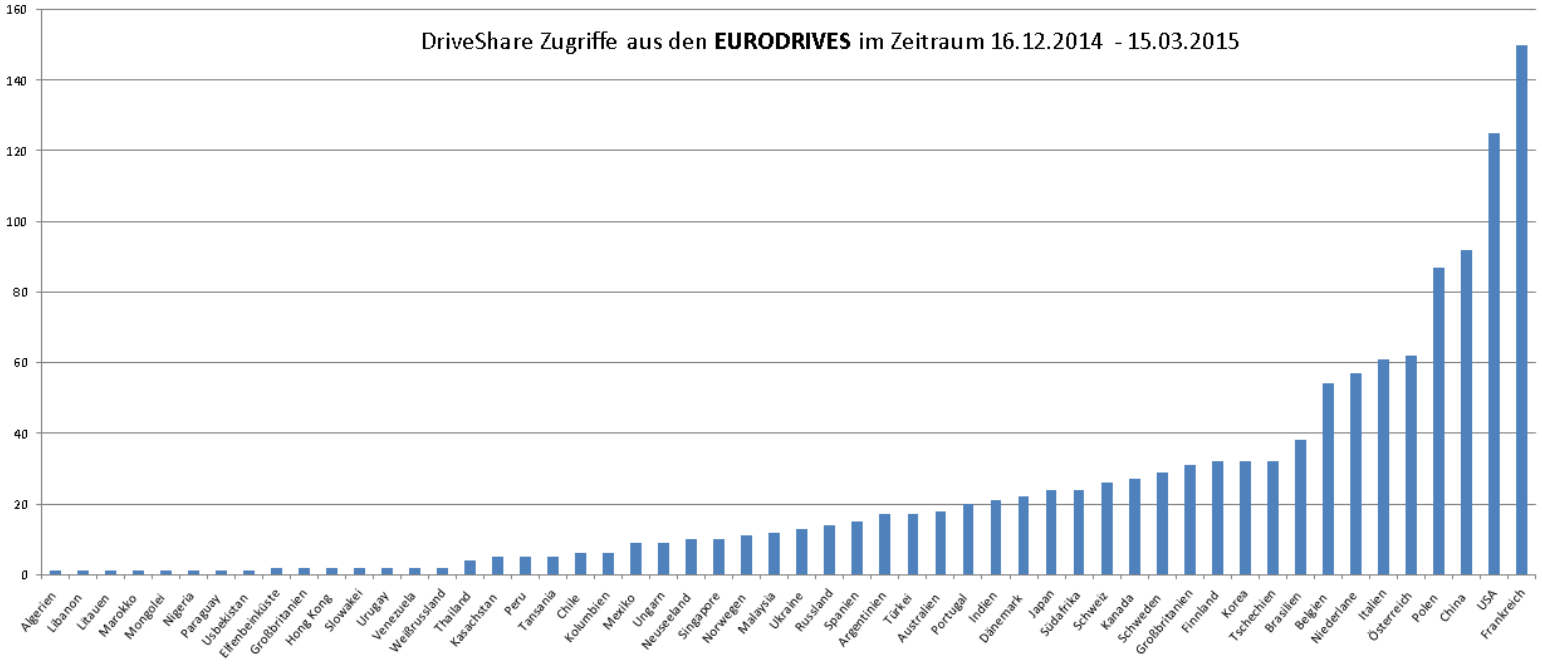
Zugriffe / Historie / Lifecycle

- Userberechtigungen werden bei Austritt / Deaktivierung des AD Users nicht auf den SharePoint Sites entfernt
- Wer und wie viele User sind tatsächlich noch aktiv?
- Auf welchen Seiten sind welche Nutzer berechtigt?
- Auswertungen für späteren Abgleich der AD Gruppe „SharePoint Enterprise User“ relevant (CAL Anzahl abgleichen)

- Wie lange wurde eine bestimmte Site nicht mehr verwendet?
  - PowerShell Auswertungen nicht eindeutig nutzbar
  - Verschiebung / Löschung der Sites nach Zeitraum X nur schwer bestimmbar

Bisherige Auswertungsmethoden

- **MAP** - Microsoft Assessment and Planning (MAP) Toolkit User und Anzahl der Zugriffe auf DriveShare



EURODRIVES		1254
Deutschland		2767
Insgesamt		**4021**

Bisherige Auswertungen

PowerShell:

```
PS C:\Users\ossadm> $s = Get-SPSite https://driveshared/teamsites/Daniel
PS C:\Users\ossadm> $s.LastContentModifiedDate

Dienstag, 27. Oktober 2015 14:35:50
```

- Get-SPUser
- LastModifiedDate für einzelne Sites
- …

Unter **SharePoint 2010**:

- Analytics Reports

	Page URL (under http://optimus:3333/OkeToys)	Number of Page Views
1	/_layouts/dynamicimageprovider.aspx	144
2	/dashboards/burndown.aspx	139
3	/_layouts/tswa/ui/pages/workitems/workitemedit.aspx	136
4	http://portal.geveo.com:3333/oketoys/dashboards/burndown.aspx	77
5	http://portal.geveo.com:3333/oketoys/_layouts/dynamicimageprovider.aspx	42
6	/shared documents/forms/allitems.aspx	34
7	http://portal.geveo.com:3333/oketoys/_layouts/tswa/ui/pages/workitems/workitemedit.aspx	29
8	/_layouts/tswa/ui/pages/workitems/queryresultnw.aspx	18
9	/_layouts/listfeed.aspx	16
10	/_layouts/inplview.aspx	11

Zusammenfassend: Nutzung von Varonis DA bei SEW

- Bereinigung der Zugriffsgenehmigungen
- Erkennung von Konfigurationsfehlern
- Finden von verlorenen, verschobenen oder gelöschten Daten
- Aufdecken von anormalem Zugriffsverhalten (Alerting)
- Überprüfung von Berechtigungs- oder Gruppen-Änderungen
- Logging von Administratoraktivitäten
- Zurückspiegeln der Dateizugriffe an den Dateneigner
- Identifizierung von selten genutzten Daten
- Automatisiertes Reporting bei zu definierenden Vorfällen

Vielen Dank für Ihre Aufmerksamkeit

SEW EURODRIVE

VARONIS

ICS Stuttgart mbuf
16.&17. April 2018
mbufJK18
Kongress für Microsoft Business User