mbuf

Arbeitsgruppe IT-Security

Vertraulichkeit und Integrität unstrukturierter Daten….

…und Tipps/Erfahrungen zu Einführung und rechtssicherem Betrieb von Überwachungssoftware in Deutschland.

Mannheim, 22./23.7.2019

Matthias Schmauch, Varonis Systems (Deutschland) GmbH

VARONIS

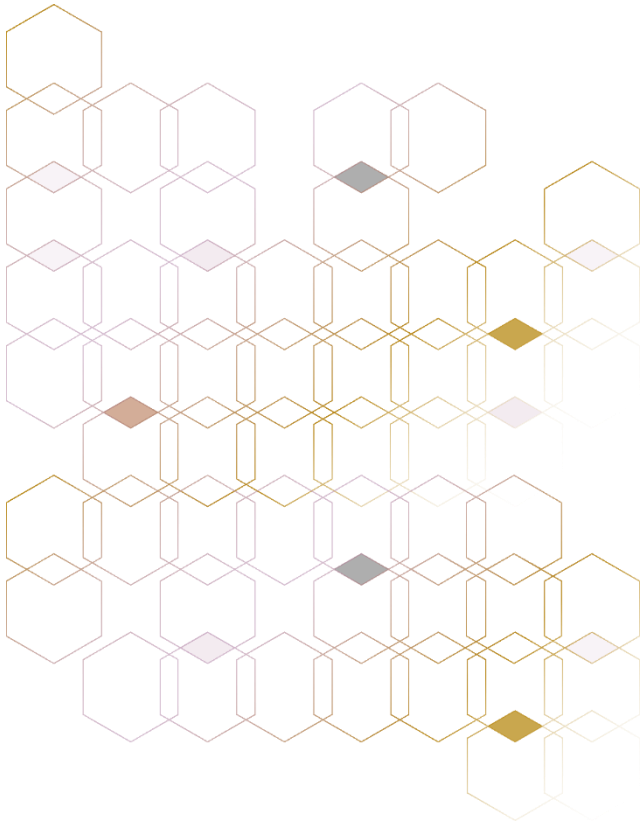
Agenda

- Wer ist Varonis und was können Sie mit unseren Lösungen machen?
- Erfahrungen aus Sicht eines Leidtragenden ☺:
  - Mythen & Sagen aus der Welt von BR & DSB
  - Does & Dont`s auf dem Weg zum rechtssicheren Betrieb

Mannheim, 22./23.7.2019

Matthias Schmauch, Varonis Systems (Deutschland) GmbH

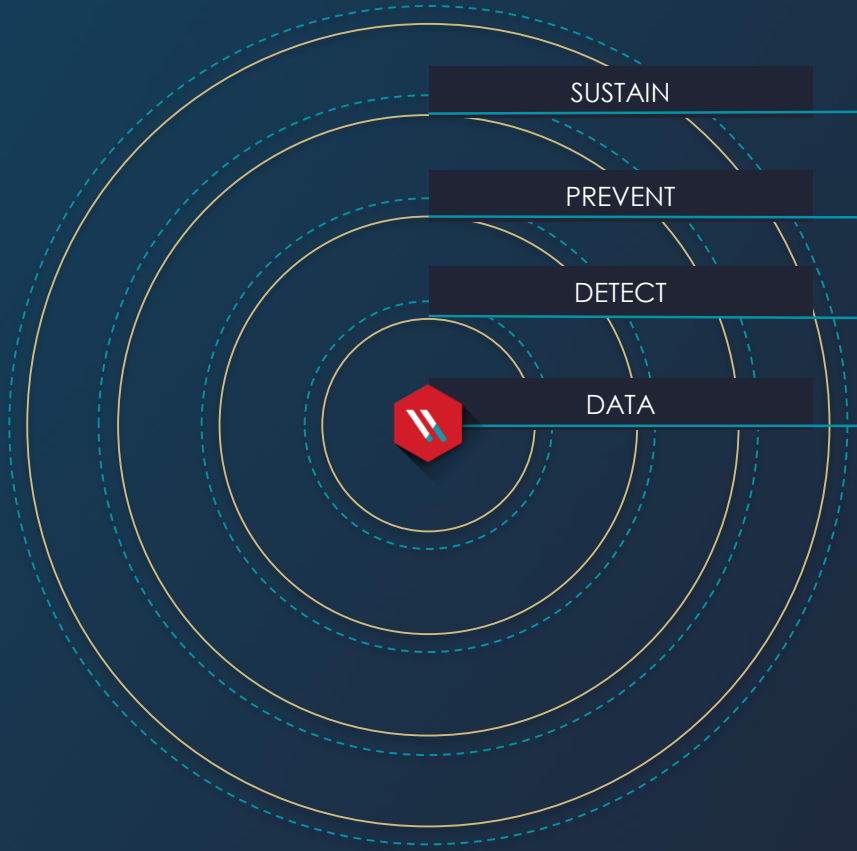
VARONIS



Regain Control of Access to Your Unstructured Data Repositories On-Premises and in the Cloud | April 2017

> **Unstrukturierte Datenspeicher** sind in den Unternehmen **chronisch zu wenig verwaltet** und zu großzügig geöffnet worden. Die fortschreitende Einführung von **Cloud-Speichern und Kollaborationsplattformen** in den letzten Jahren hat es **noch komplizierter gemacht**, der Situation Herr zu werden.
>
> Gartner®

Vertraulichkeit & Integrität beginnen bei den Daten.



Etablieren eines Erhaltungsprozesses.

Reduzieren der Zugriffsrechte.

Protokollieren & Mißbrauch erkennen.

Wissen, wo sensitive Daten liegen.

Fragen, die Varonis beantwortet.

Sind meine Daten betroffen?

- Sind meine Daten exponiert?
- Wer kann zugreifen?
- Wer hat zugegriffen?
- Zu wem gehören Sie?

Bin ich compliant?

- Wo liegen “regulierte” Daten?
- Kann ich Sie löschen?
- Kann ich die Compliance prüfen?

Kann ich einen Breach erkennen?

- Mißbraucht jemand Daten?
- Von welchen Geräten/Orten?
- Kann ich adhoc Analysen machen?

DREI ANWENDUNGSBEREICHE

DATA PROTECTION

COMPLIANCE

THREAT DETECTION & RESPONSE

EINE PLATTFORM

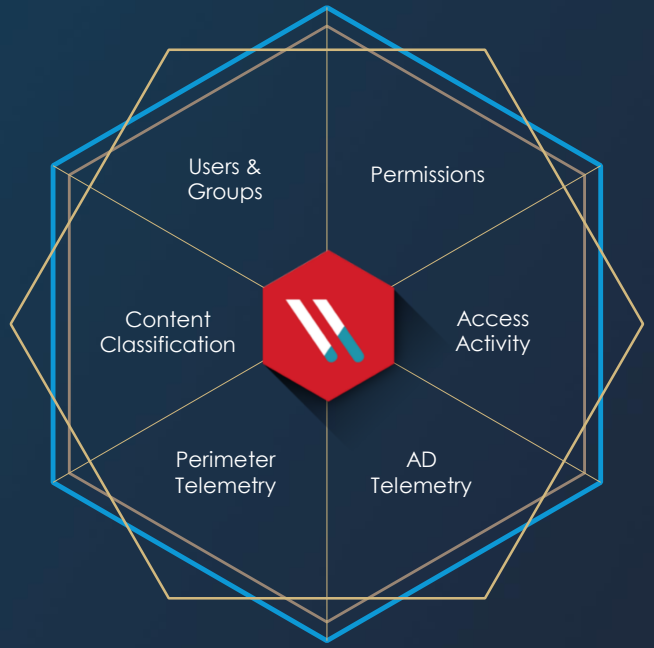
VARONIS

Varonis Data Security Platform

ENTERPRISE DATA STORES AND INFRASTRUCTURE

Windows
Office 365
Exchange
Unix/Linux
SharePoint
NAS
Box
Directory Services
Edge Services

ANALYTICS & AUTOMATION



USE CASES

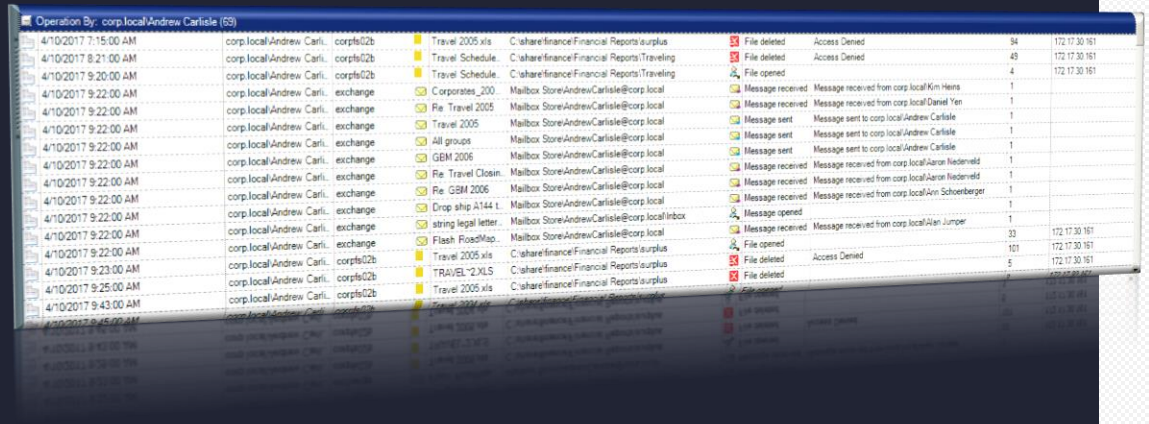
DATA PROTECTION

COMPLIANCE

THREAT DETECTION & RESPONSE

VARONIS

Einheitlicher Audittrail.

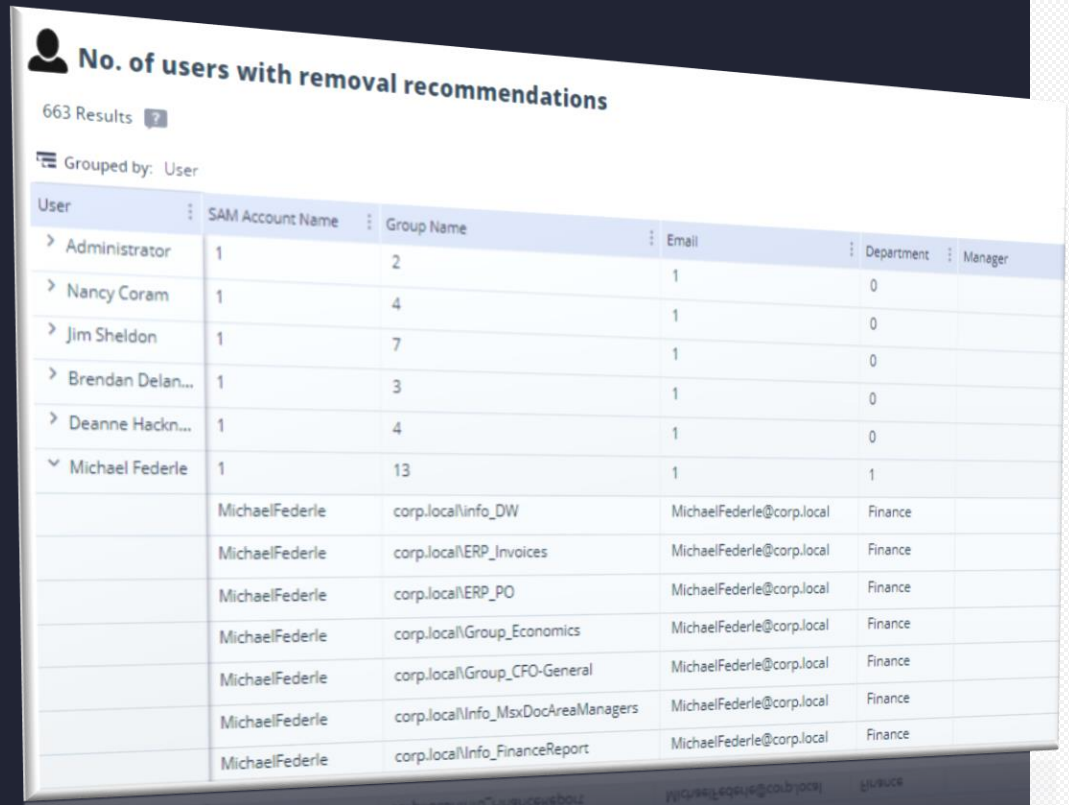


> Wir nutzen Varonis um **pharma-spezifische Compliance-Anforderungen** abzudecken.
>
> Pharmaunternehmen, 2200 User

Nutzung sensitiver Daten monitoren.

> Wir kauften Varonis, **um personenbezogene Daten auf unseren Fileservern zu finden und zu monitoren** wegen der DSGVO.
>
> Automotive Retailer, 1000 User

Least Privilege – Empfehlung.



No. of users with removal recommendations

663 Results

Grouped by: User

User	SAM Account Name	Group Name	Email	Department	Manager
Administrator	1	2	1	0	
Nancy Coram	1	4	1	0	
Jim Sheldon	1	7	1	0	
Brendan Delan...	1	3	1	0	
Deanne Hackn...	1	4	1	0	
Michael Federle	1	13	1	1	
	MichaelFederle	corp.local\Info_DW	MichaelFederle@corp.local	Finance	
	MichaelFederle	corp.local\ERP_Invoices	MichaelFederle@corp.local	Finance	
	MichaelFederle	corp.local\ERP_PO	MichaelFederle@corp.local	Finance	
	MichaelFederle	corp.local\Group_Economics	MichaelFederle@corp.local	Finance	
	MichaelFederle	corp.local\Group_CFO-General	MichaelFederle@corp.local	Finance	
	MichaelFederle	corp.local\Info_MsxDocAreaManagers	MichaelFederle@corp.local	Finance	
	MichaelFederle	corp.local\Info_FinanceReport	MichaelFederle@corp.local	Finance	

“Varonis zeigt den Data Ownern die Berechtigungen, die **ohne das Risiko einer Betriebs-unterbrechung** entfernt werden könnten.”

Produzierendes Unternehmen, 1000 User

Datenzentrierte Anomalieerkennung.

“

Varonis **erhöht unsere Sicherheit** und hilf uns **Compliance Anforderungen unserer Kunden** einzuhalten.

Automobilzulieferer, 750 User

”

Mythen & Sagen aus der Welt von BR / DSB

„Das darf man in Deutschland doch gar nicht.“

„Das verbietet die DSGVO“.

„Was sagt denn der Betriebsrat dazu?“

„Das darf man doch nur anonymisiert.“

Transparenz, Transparenz, Transparenz

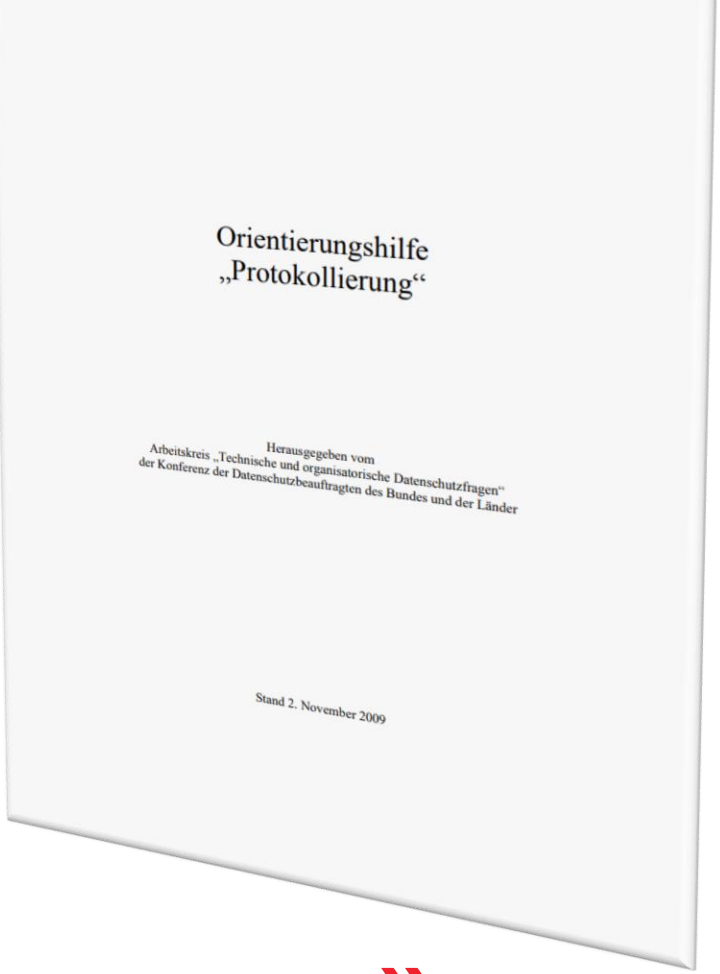
- **Geschäftsführung** einbeziehen (Risikothema)
  Aktivitäten ohne Mandat/Awareness scheitern oft am Rückhalt

- **Datenschutzbeauftragten** einbeziehen
  Datenschutzfolgeabschätzung hilft „UseCases“ für den Betriebsrat zu beschreiben

- **Betriebsrat** einbeziehen
  Prüfung/Erweiterung vorhandener BVs oder Neuabschluss kann die Zeitachse erheblich beeinflussen

Orientierungshilfe „Protokollierung“

- Konferenz der DSB der Länder und des Bundes aus dem Jahr 2009
- „Aufrechterhaltung von Datenschutz/Datensicherheit“ vs. Zielkonflikt „automatisierte Verhaltens- und Leistungskontrolle“



Die Protokolldaten (gem. OH Prot.)

- „Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten so transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.“
- Vollständigkeit (Wer, Wann, Was, Wo?)
- Datensparsamkeit
- Revisionssicherheit
- Zugriff nur für Berechtigten

Datenschutzfolgeabschätzung

- Ziele und Zwecke
- Beschreibung der Lösung
- Bewertung
- Ergebnis der Bewertung

- Risikomanagements des Unternehmens und seiner Kunden
- Branchenstandard wie z.B. TISAX, SOX, GxP, ISO27001, Kritis, etc.
- Stand der Technik in Sachen Cybersecurity / DLP, etc.

Zweckbeispiele

Normen, Richtlinien, Gesetze	
BSI / IT Sicherheitsgesetz	Kritische Infrastrukturen
DSGVO / EU GDPR	Alle Unternehmen >250 Mitarbeiter
Aktiengesetz / SOX	Börsennotiert / US-Börsennotierung
BAFIN	Banken / Versicherung
PCI DSS	E-Payment Provider
ISO 27001 / TISAX	Freiwillig (z.B. Automotive, WPs)
IDWPS330	Alle Unternehmen >50 Mitarbeiter
UGMP, FDA, MHRA	Pharma / Chemie
...oder die Angst seinen Marktvorsprung zu verlieren	Marktführer, Innovatoren

Datenschutzfolgeabschätzung

- Ziele und Zwecke
- Beschreibung der Lösung
- Bewertung
- Ergebnis der Bewertung

- Benennung der Software-Lösung
- Vertrag und Zusammenarbeit (Auftragsdatenverarbeitung, auch für den Supportfall)

Datenschutzfolgeabschätzung

- Ziele und Zwecke
- Beschreibung der Lösung
- Bewertung
- Ergebnis der Bewertung

- Verarbeitung personenbezogener Daten
- Rechtsgrundlagen
- **Interessenabwägung**
- Maßnahmen zur Minimierung des Risikos
- Unzulässige Verwendungen
- Aufbewahrungsfristen

Datenschutzfolgeabschätzung

- Ziele und Zwecke
- Beschreibung der Lösung
- Bewertung
- Ergebnis der Bewertung

Leistungsbewertung?
Ja, Nein, Jain?

Betriebsaspekte beim Protokollieren

- Erzeugung (Was ist die Notwendigkeit?)
- Übertragung (verschlüsselt und vollständig)
- Speicherung (Kontrollzeitpunkte, Zugriffsmöglichkeiten, Speicherort)
- Auswertung (Auswerteszenarien definieren: anlassbezogen oder regelmäßig, 4-Augen, Mitbestimmung der Mitarbeitervertretung)
- Löschung (Aufbewahrungdauer festgelegen, Lösch- und Aufbewahrungsfristen beachten, 1 Jahr)

Vertraulichkeit und Integrität für unstrukturierte Daten.

- Matthias Schmauch, Sales DACH Central
- NSDQ: **VRNS** | 6.000 Kunden
- www.varonis.com