

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



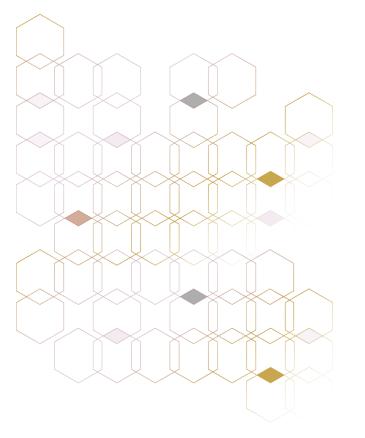


Arbeitsgruppe IT-Security

#### 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



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

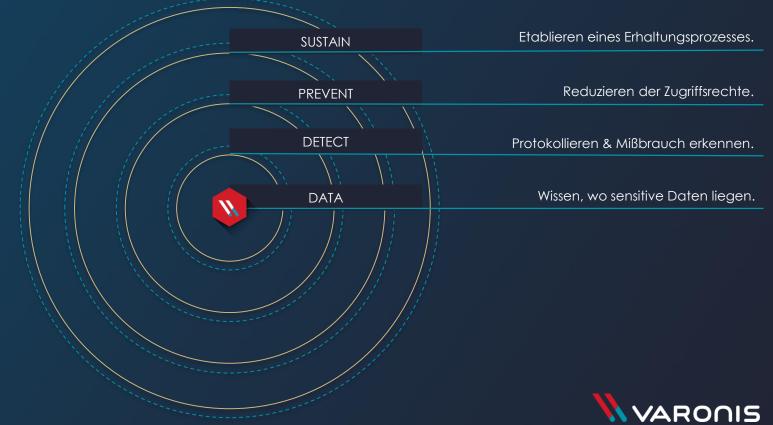
# 66

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.



#### 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 pr
  üfen?

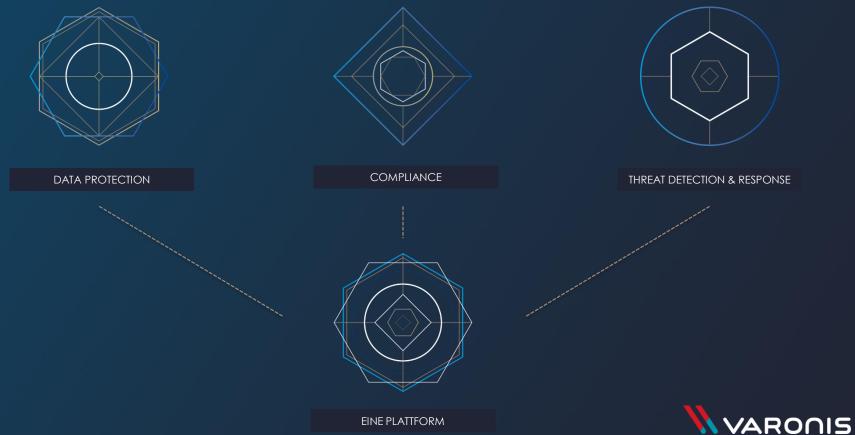
#### Kann ich einen Breach erkennen?



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

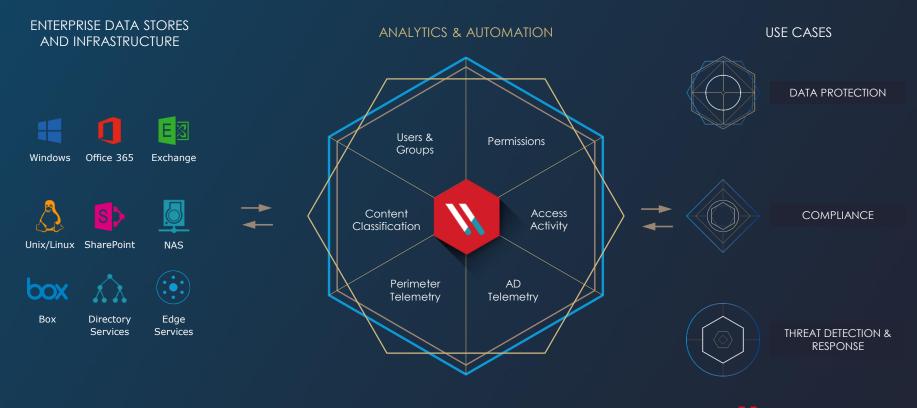


#### DREI ANWENDUNGSBEREICHE



EINE PLATTFORM

#### Varonis Data Security Platform





#### Einheitlicher Audittrail.

Operation By: corp.local/Andrew 4/10/2017 7:15:00 AM	corp.local/Andrew Carli, corpts02	b Travel 2005 xls	C:\share'finance'Financial Reports'surplus	File deleted	Access Denied		172 17 30 161
			C:share/finance/Financial Reports/Traveling	File deleted	Access Denied	24	172 17 30 161
4/10/2017 8:21:00 AM	corp.local/Andrew Carli. corpfs02				Access Denied	*3	172 17 30 161
4/10/2017 9:20:00 AM	corp.local/Andrew Carli. corpfs02		C:\share\finance\Financial Reports\Traveling	S. File opened			1/2 1/ 30 101
4/10/2017 9:22:00 AM	corp.local/Andrew Carli. exchang	e Grorporates_200	Mailbox Store/AndrewCarlisle@corp.local		Message received from corp local Kim Heins		
4/10/2017 9:22:00 AM	corp.local/Andrew Carli. exchang	e 🧐 Re Travel 2005	Mailbox Store/AndrewCarlisle@corp.local		Message received from corp local Daniel Yen		
4/10/2017 9:22:00 AM	corp.local/Andrew Carli, exchang		Mailbox Store/AndrewCarlisle@corp.local	Message sent	Message sent to corp local Andrew Carlisle		
	corp.local/Andrew Carli_ exchang		Mailbox Store/AndrewCarlisle@corp.local		Message sent to corp local Andrew Cartisle		
4/10/2017 9:22:00 AM	corp.local/Andrew Carli. exchang		Mailbox Store/AndrewCarlisle@corp.local	😡 Message sent	Message sent to corp local Andrew Cartisle		
4/10/2017 9:22:00 AM			Mailbox Store/AndrewCarlisle@corp.local	Message received	Message received from corp.local/Aaron Nederveld		
4/10/2017 9:22:00 AM	corp.local/Andrew Carli. exchang		Mailbox Store Andrew Carlisle@corp.local	S Message received	Message received from corp local/Aaron Nederveld		
4/10/2017 9:22:00 AM	corp.local/Andrew Carli. exchang		Mailbox Store/AndrewCarlisle@corp.local	Message received	Message received from corp local Ann Schoenberger		
4/10/2017 9:22:00 AM	corp.local/Andrew Carli_ exchang		Mailbox Store Andrew Carlisle@corp.locaf.inbox	& Message opened			
4/10/2017 9:22:00 AM	corp.local/Andrew Carli_ exchang	e 😡 string legal letter.	Mailbox Store/AndrewCarlisle@corp.local	Message received	Message received from corp local Alan Jumper	22	172 17 30 161
	corp.local/Andrew Carli. exchang	e 😡 Flash RoadMap.	Mailbox Store Andrew Carlislee Corporation	& File opened		101	172 17 30 167
4/10/2017 9:22:00 AM	corp.local/Andrew Carli_ corpfs02		C:\share\financelhinancial Reports so pros	File deleted	Access Denied	5	172 17 30 161
4/10/2017 9:23:00 AM	corp.local/Andrew Carli_ corpfs02		Cishare'financelFinancial Reports'surplus	File deleted			1 72 27 93 157
4/10/2017 9:25:00 AM	corp.local Andrew Calic. corp.	Travel 2005 xls	C:\share\finance\Financial Reports\surplus	2 File recent	1		1002 Mil
4/10/2017 9:43:00 AM	corp.local/Andrew Carli_ corpfs02		Carbon France France Bearing and S				In the second
4102017 04500 AM	Com In al Satery Cati and Ca						A DESCRIPTION OF THE OWNER.
The second a feature							Contraction of the

## 66

Wir nutzen Varonis um **pharmaspezifische Compliance-Anforderungen** abzudecken. Pharmaunternehmen, 2200 User

"

### Nutzung sensitiver Daten monitoren.



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

"

#### Least Privilege – Empfehlung.

L No. of users with removal recommendations

663 Results

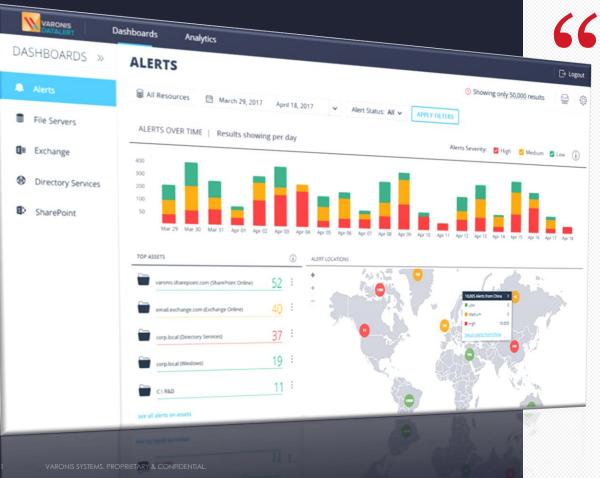
Grouped by: User

lser i	SAM Account Name	Group Name				
Administrator	1	2	Email	Department   Manager		
Nancy Coram		2	1	0		
	1	4	1	0		
Jim Sheldon	1	7	1	0		
Brendan Delan	1	3	4			
> Deanne Hackn 1			1	0		
		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			
	MichaelFederle	corp.local\Info_FinanceReport	MichaelFederle@corp.local	Finance		
		corp.local/linfo_FinanceReport	MichaelFederle@corp.local			
Varonis syst <u>ems, f</u>	PROPRIETARY & CONFIDENTI	coubypocau (public) (240-Ceuelia) AL				

" Varonis zeigt den Data Ownern die Berechtigungen, die ohne das Risiko einer Betriebsunterbrechung 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."



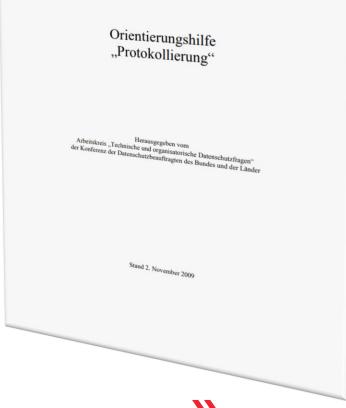
#### Transparenz, Transparenz, Transparenz

- 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 f
  ür Berechtigten



- 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)
IDWP\$330	Alle Unternehmen >50 Mitarbeiter
UGMP, FDA, MHRA	Pharma / Chemie
oder die Angst seinen Marktvorsprung zu verlieren	Marktführer, Innovatoren



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

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



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

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



- 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)



