



Zero Trust  
Data Security™

**Secure your  
data.**



**Secure your  
business.**

**Frank Schwaak**

Field-CTO EMEA @Rubrik, Inc.



# Cyber Attacken in Deutschland

2022

Produktion in Pfaffenhofen steht still  
**Cyberangriff auf Hipp: Kriminelle legen IT-System des Unternehmens lahm**

06.10.2022 | Stand 06.10.2022, 11:51 Uhr

**Caritas Cyberattacke gegen Denso**

Hacker haben den Zulieferer Denso angegriffen. Sie drohen mit der Veröffentlichung von Geschäftsgeheimnissen.  
Montag, 14. März 2022, 13:12 Uhr

Saller-Bau bestätigt in Weimar Hackerangriff auf Teile des Unternehmens

25.08.2022, 10:15

**Hackerangriff auf Sixt – Beeinträchtigung für Kunden**

13. Oktober 2022 von Ralf Grimminger  
Angaben Ziel einer Cyberattacke geworden. Die -h läuft weiter – mit gewissen Einschränkungen.

**3 Wochen nach Cyberangriff hat der Baustoffrieser Knauf immer noch Probleme**

Von Philipp Anz, 21. Juli 2022 um 12:02

Produktion in Pfaffenhofen steht still  
**Cyberangriff auf Hipp: Kriminelle legen IT-System des Unternehmens lahm**

05.10.2022 | Stand 06.10.2022, 11:51 Uhr

Michael Kraus  
Redaktionsleiter

**Cyber-Angriff auf Wilken Software Group in Ulm**

Nach einem Ransomware-Angriff auf die Wilken Software Group hat das Ulmer Softwarehaus heute zur Sicherheit seine Systeme heruntergefahren und auch das Kundenportal abgeschaltet. Damit ist das Unternehmen

Dienste vorübergehend offline  
**Hackerangriff auf deutschen Energiedienstleister Ista**

AKTUALISIERT AM 10.08.2022 - 23:05

**Oiltankier**

**IT-Systeme von Bizerba we**

**Windtechnik AG attackiert**

Erstellt: 14.04.2022, 10:37 Uhr  
Von: Johannes Hub

**Warburg und Bielefeld betroffen**

**Hackerangriff auf Schultze & Braun**

Die Insolvenzrechtskanzlei Schultze & Braun ist Opfer einer Ransomware-Attacke geworden. Ausgeführt wurde der Angriff von einer Hackergruppe, die sich vergangene Woche zu Russlands Präsident Putin bekannte.

**Eilmeldung: Hackerangriff auf DVGW**

Kategorie: Verträge & Organisationen  
Themen: Gas | Wasser  
Autor: Kathrin Mundt

**Cyber-Angriff auf Unternehmen Ludwig F**

von Karsten Röhr

**Produktionsstillstand folgt auf Cyber-Angriff: Hacker legen Elobau zwei Wochen lahm**

leidet noch

# Studien zu Cyberkriminalität und -gefahren



**6 out of 10**  
weren't able to recover their data

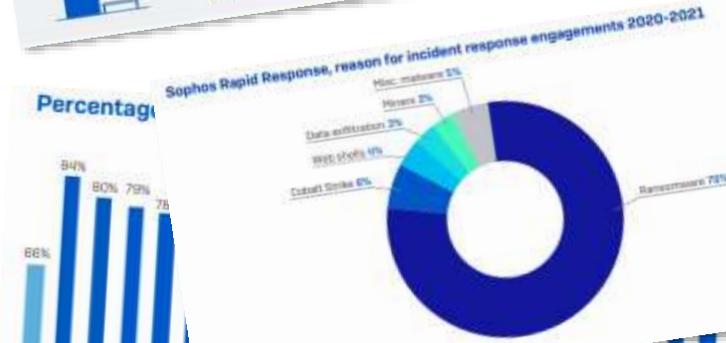
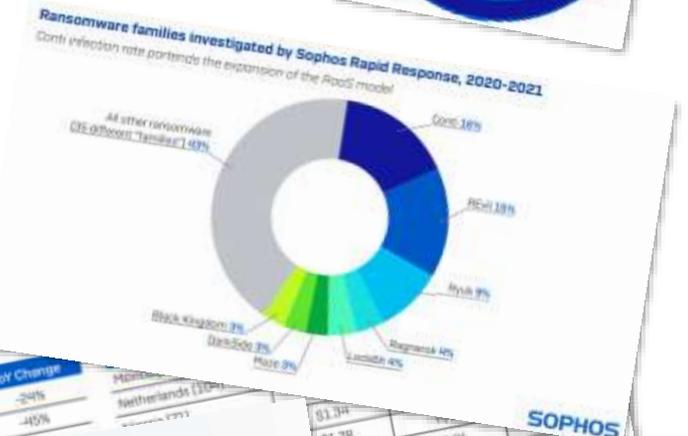
**90%**  
ransomware attack impacted their ability to operate

**MANUFACTURING, UTILITIES**  
highest average ransom payment (\$2M)

**Top Data Types Targeted for Double Extortion**

**68%**  
who paid once were hit again in less than a month for a higher ransom

**88%**  
hit by ransomware say they have sufficient cybersecurity budget



**35%**  
reported C-level resignations following the attack

**61%**  
encrypted data restored after paying the ransom

**3x**  
increase in proportion that paid ransoms of US\$ 1M or more



**ONE MONTH**  
average time to recover from an attack

**27%** PHI  
**34%** PII  
**54%** SENSITIVE CUSTOMER DATA  
**90%** ...

Age Cost to Organization to Rectify

Country	2021	2020	YoY Change
Average (3,702)	\$1.40	\$1.85	-24%
Australia (200)	\$1.01	\$1.84	-45%

**86%**  
ransomware attack caused loss of business/revenue

**\$812,360**  
average ransom payment (excluding outliers)

**54%**  
who paid still reported system issues or corrupted data after decryption

**4%**  
that paid the ransom got ALL their data back

**80%**  
of those who paid were victims of a second attack

**65%**  
attacks resulted in data encryption

**33%**  
forced to temporarily suspend business

**66%**  
hit by ransomware in the last year

**\$1.4M**  
average cost to remediate an attack

**37%**  
forced to lay off employees

**46%**  
paid the ransom

# Präventive Grundlagen zur Vorbereitung



- **Prüf-Interview**

- Sind auf extern erreichbaren Systemen die aktuellsten Patches aufgespielt?
- Welche Netzbereiche werden von uns genutzt? Werden diese zentral verwaltet?
- Welche Systeme müssen zwingend von außen erreichbar sein?
- Wird grundsätzlich VPN für die Verbindung zu internen Systemen verwendet?
- Ist Multifaktor Authentifizierung für alle Systeme und VPN Verbindungen aktiviert?
- Sind die nötigen Monitoring Prozesse etabliert und funktionsfähig
- Welche Systeme sind für kritische Geschäftsprozesse notwendig?
- Sind wir auf einen Vorfall vorbereitet?
- Sind alle kurzfristigen Eskalationsmechanismen festgelegt und bekannt?
- Gibt es ein Backup-Konzept?
- Sind Backups im Normalfall nicht über das Netzwerk erreichbar?



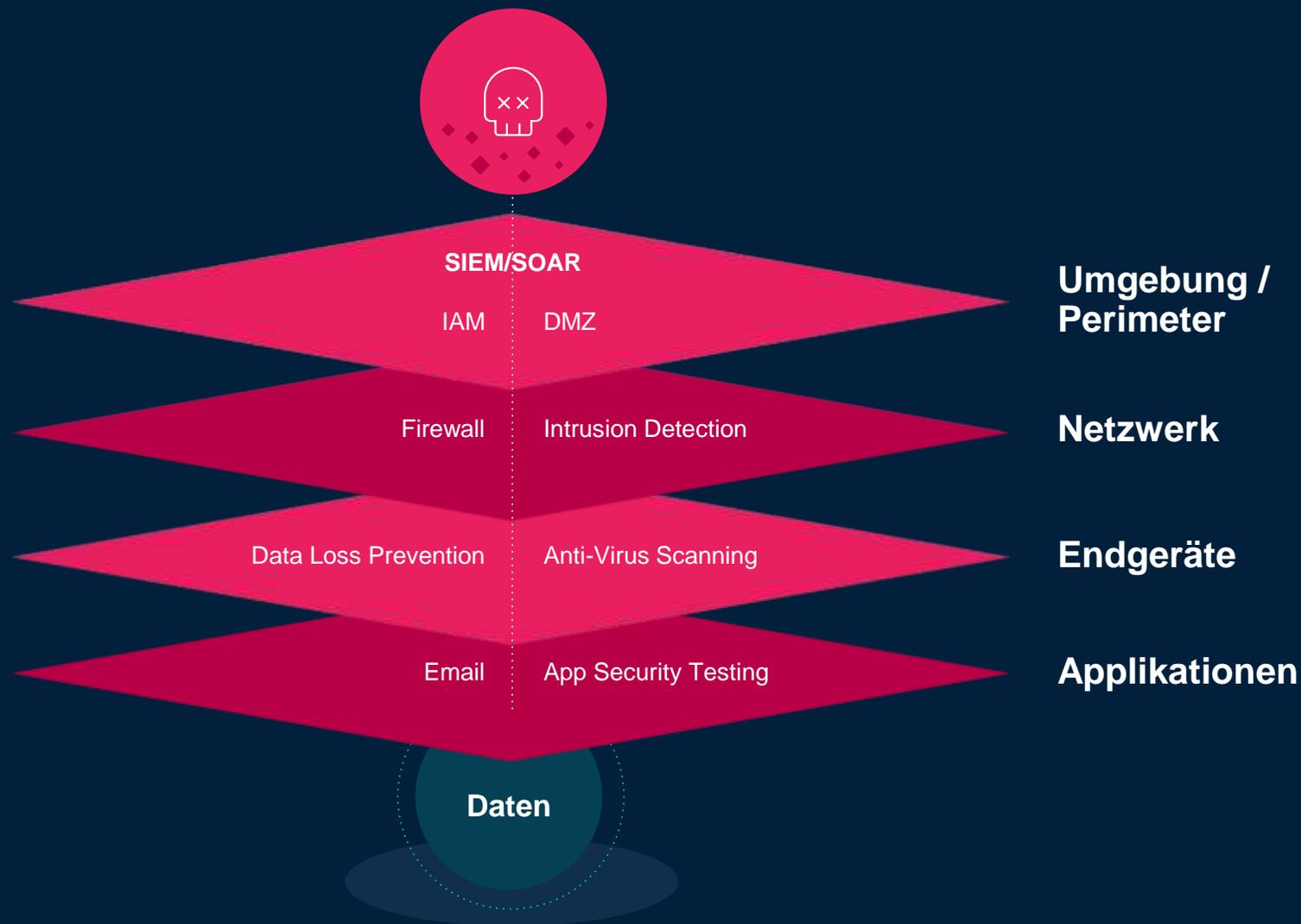
*Es ist inzwischen bei Schadprogramm-Infektionen üblich, dass Angreifende mit zuvor erlangten Administrationsrechten gezielt nach allen Backups suchen und diese, ebenso wie Produktivsysteme, verschlüsseln.*





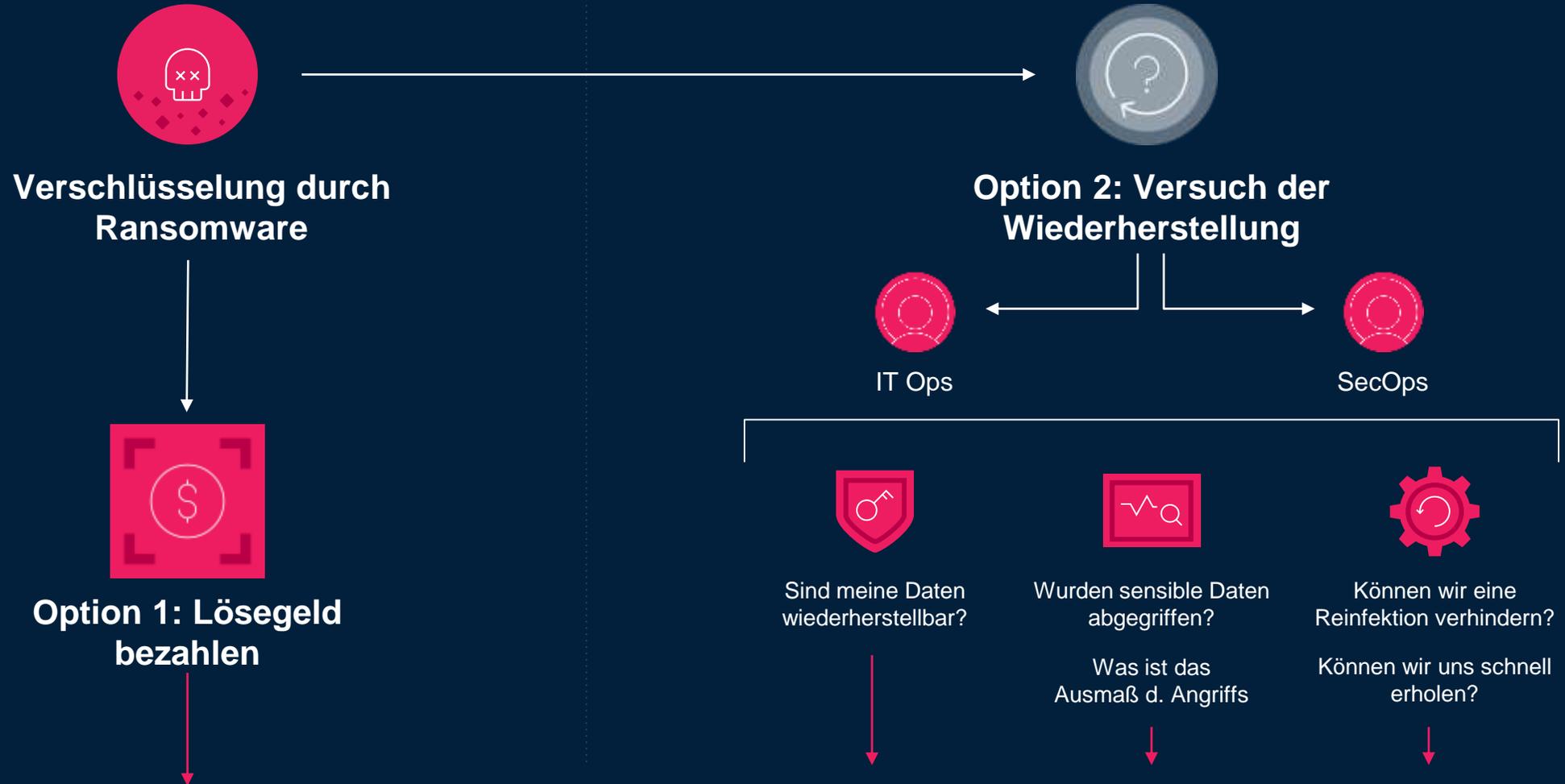
# Die Anzahl der Cyber-Angriffe steigt kontinuierlich

Nur allein die Absicherung der Infrastruktur ist nicht ausreichend!





# Warum zahlen Unternehmen das Lösegeld?



**Lösegeld zahlen / auf schnelle Erholung hoffen**



INCIDENT

SECURITY

IT

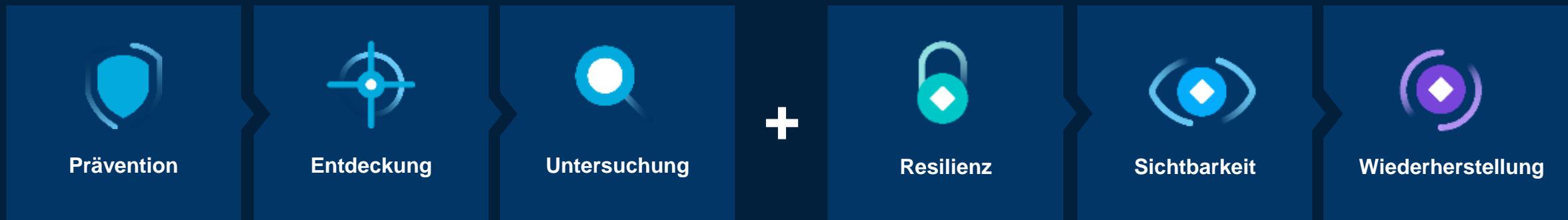


# Die nächste Stufe der Cybersicherheit

Infrastructure Security und Data Security bilden gemeinsam Zero Trust Security

Infrastructure Security

Data Security





# Es ist Zeit für einen neuen Ansatz



**Resilienz**

**Was wäre, wenn Sie Ihre Backupdaten gegen Cyberangriffe schützen könnten?**



**Sichtbarkeit**

**Was wäre, wenn Sie Risiken überwachen und Bedrohungen schnell untersuchen könnten?**



**Wiederherstellung**

**Was wäre, wenn Sie genau die Daten, die Sie benötigen, sofort wiederherstellen könnten?**



# Datenresilienz

Haben wir einen  
Wiederherstellungsplan falls alles  
kompromittiert ist?

Können meine  
Aufbewahrungsregeln  
verändert werden?

Können meine Admin-Accounts  
kompromittiert werden?



Können meine Backups  
von böswilligen Akteuren gefunden  
werden?

Können meine Backups  
von Angreifern eingesehen  
werden?

Können meine Backupdaten verändert  
werden?



# Datensichtbarkeit



Wann wurde ein mit Malware infiziertes System zum ersten mal gesichert?

Gab es irgendwelche ungewöhnlichen Löschungen oder Änderungen an meinen Daten?

Waren sensible Daten bei einem Angriff betroffen?



# Datenwiederherstellung

Wie kann ich die Wiederherstellung meiner wichtigsten Anwendungen automatisieren?



Wie kann ich Daten wiederherstellen ohne das System zu reinfizieren?

Wie kann ich gezielt das wiederherstellen was benötigt wird?



# Einführung Rubrik Security Cloud

Sichern Sie Ihre Daten, wo auch immer sie gespeichert sind, on Prem, Cloud und SaaS



Cyber-proof mit Hilfe von  
 Air Gap,  
 immutable Filesystem,  
 Access Control,  
 redundante backups



Operative  
 Wiederherstellung von  
 Anwendungen, Dateien  
 oder Benutzern unter  
 Vermeidung einer erneuten  
 Malware-Infektion

Fortlaufende Überwachung Ihrer Daten auf Ransomware  
 Gefährdung sensibler Daten beheben  
 Indikatoren für eine Gefährdung erkennen

NIST Security Standards

Preparation

Detection and Analysis

Containment Eradication  
 and Recovery



# Rubrik's Evolution

Entwickelt für die Konvergenz von Datenschutz und Datensicherheit

## Pionier im Bereich Zero Trust Data Protection

- Zero Trust Architektur
- unveränderliche Backups
- logisches Airgap
- sofortige Wiederherstellung
- geschäftsabhängige SLA's

## Pionier im Bereich Cloud Data Management

- eine Plattform (IaaS/PaaS/SaaS)
- ausfallsicher & optimiert  
Cloud Archival & Wiederherstellung
- granulare/orchestrierte  
Wiederherstellung

## Pionier im Bereich Data Security

- Ransomware Monitoring
- Monitoring sens. Daten
- Threat Hunting & Monitoring



Wir halten was wir versprechen



\*Terms and conditions apply.

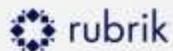


# Rubrik Ransomware Response Team (RRT)

- Globales 24x7x365 Team für alle Rubrik Kunden
- Die meisten Angriffe finden an Wochenenden oder über Feiertage statt
- 300+ L2/L3 level FTEs
- Über 100 Ransomware Recoveries durchgeführt
- Incident Management Team wird bei Meldung eines Angriffs zugewiesen
- Konsequenz, vertraulich, kundenspezifische & schnelle Wiederherstellung
- Wir bleiben so lange Sie uns brauchen.



# The News...!



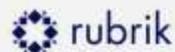
Company ▶ Newsroom ▶ Press Releases

AUG 31, 2022 | PRESS RELEASE

## Rubrik Surpasses \$400 Million in Subscription ARR and Launches Rubrik Zero Labs, Data Threat Research Unit to Help Combat Global Cyber Events



Former Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to Further Rubrik's Mission to Secure the World's Data.



Company ▶ Newsroom ▶ Press Releases

MAY 25, 2022 | PRESS RELEASE

## Rubrik Appoints Former Central Intelligence Agency (CIA) Chief Information Security Officer (CISO) Michael Mestrovich as Company's CISO

Rubrik Strengthens Cybersecurity and Policy Expertise; Continues Building its Distinguished Leadership Team to Tackle the Ransomware Challenge



rubrik

Zero Trust  
Data Security

Our momentum is a reflection of our relentless drive to help our customers **secure their data**





# SAVE THE DATA – RANSOMWARE SIMULTATION

ESSEN  
MONTAG, 14.  
14:00 UHR -

## Save Work

Tauchen Sie  
besonderen  
Ransomware  
mit unseren  
gemeinsame

Jetzt



## Worum es geht:

"Save the Data" ist Strategiespiel und Tabletop-Action pur. Machen Sie mit! Sie erleben die ganz realen Konsequenzen eines Cyber-Angriffs.

Von der CIO-Sicht bis zur Teilnahme an Vorstandssitzungen, am Ende haben alle Player ein neues und umfassendes Verständnis davon, was im Ransomware-Fall in einer Organisation wirklich passiert.

Wir freuen uns, wenn Sie im Anschluss noch bleiben, für Drinks und Snacks ist gesorgt. (auf freiwilliger Basis).



# SAVE THE DATA – RANSOMWARE SIMULTATION



Essen: 1



München



## Ihre Gastgeber

**Frank Schwaak**  
Field CTO EMEA  
Rubrik



---

**Michael Pietsch**  
Regional VP and General Manager  
Germany  
Rubrik

**Thomas Schuchmann,**  
Regional VP Sales Engineering Central &  
Northern Europe

<https://www.rubrik.com/company/events/save-the-data/emea>



# Vielen Dank.



 [frank.schwaak@rubrik.com](mailto:frank.schwaak@rubrik.com)  
 [linkedin.com/in/frankschwaak/](https://www.linkedin.com/in/frankschwaak/)  
 @FrankSchwaak