rubrik | Zero Trust Data Security™

Secure your data.

Secure your business.

Frank Schwaak
Field-CTO EMEA @Rubrik, Inc.

Cyber Attacken in Deutschland

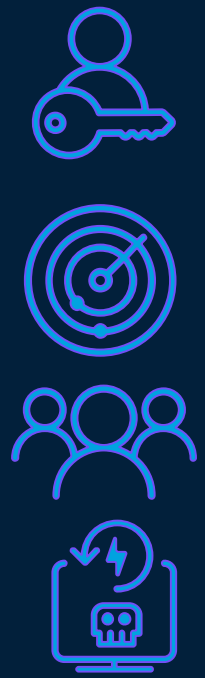
2022

Studien zu Cyberkriminalität und -gefahren

rubrik

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 Authetifizierung für alle Systeme und VPN Verbindungen aktiviert?
  - Sind die nötigen Monitoring Prozesse etabliert und funktionsfähig
  - Welche Systeme sind für kritische Geschäftsprozesse notwending?
  - 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.

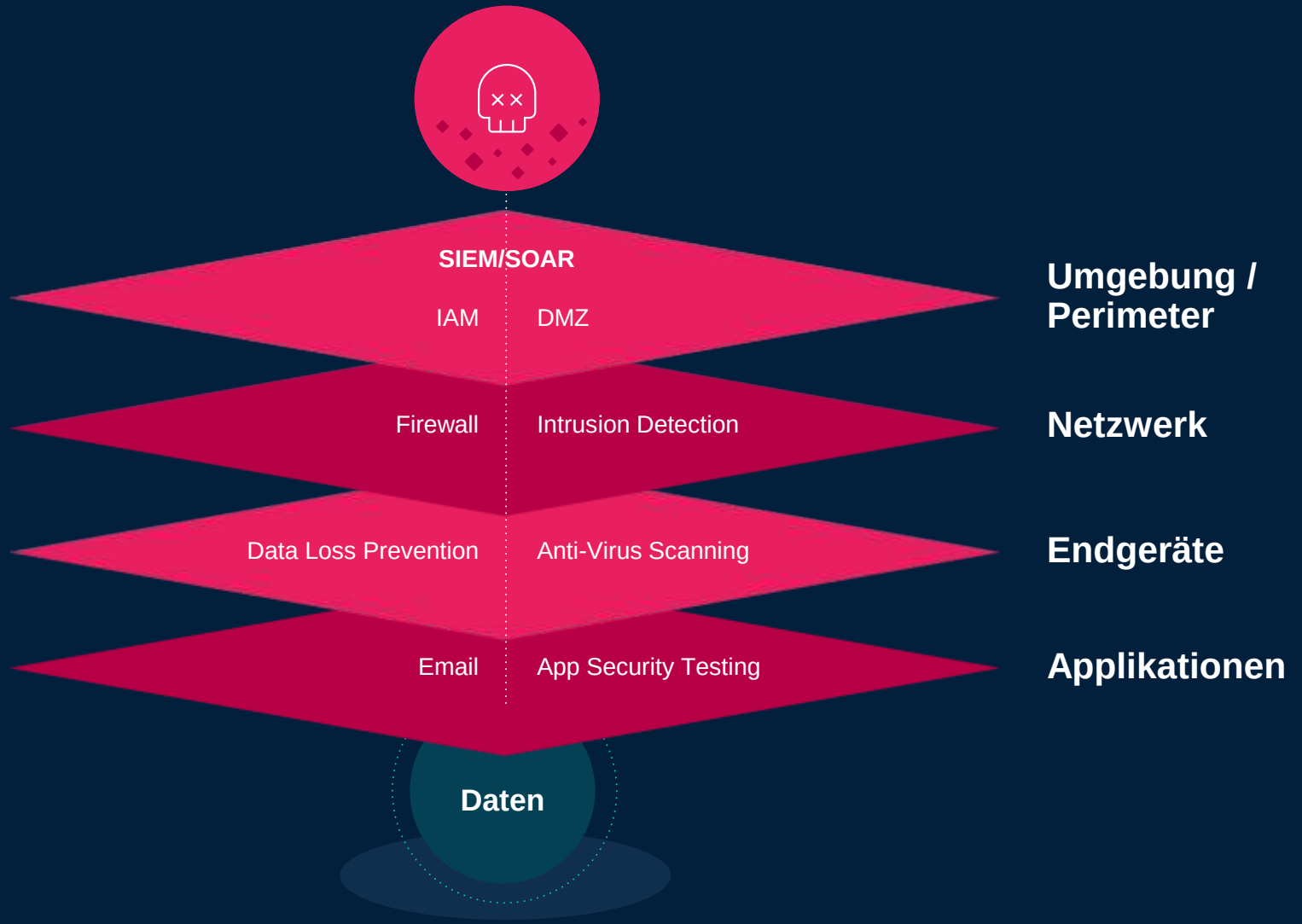
rubrik

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf?__blob=publicationFile&v=2

Die Anzahl der Cyber-Angriffe steigt kontinuierlich

Nur allein die Absicherung der Infrastruktur ist nicht ausreichend!



Warum zahlen Unternehmen das Lösegeld?

Verschlüsselung durch Ransomware

Option 1: Lösegeld bezahlen

Option 2: Versuch der Wiederherstellung

IT Ops

SecOps

Sind meine Daten wiederherstellbar?

Wurden sensible Daten abgegriffen?

Was ist das Ausmaß d. Angriffs

Können wir eine Reinfektion verhindern?

Können wir uns schnell erholen?

Lösegeld zahlen / auf schnelle Erholung hoffen


INCIDENT
SECURITY
IT

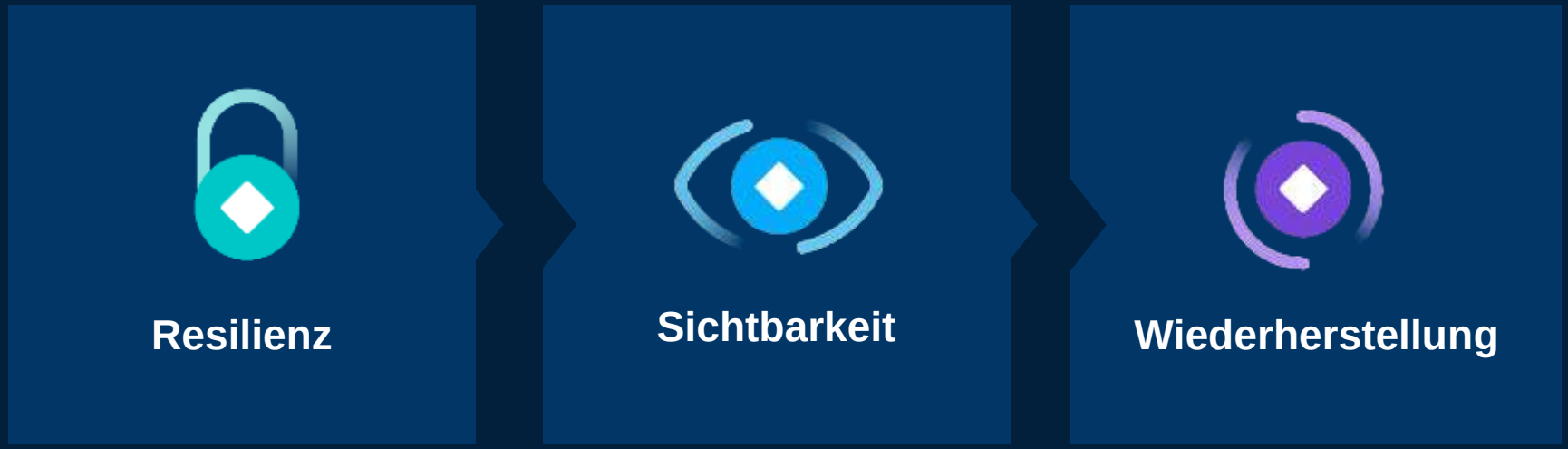
Die nächste Stufe der Cybersicherheit

Infrastructure Security und Data Security bilden gemeinsam Zero Trust Security

Infrastructure Security

Data Security

Es ist Zeit für einen neuen Ansatz



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

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

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

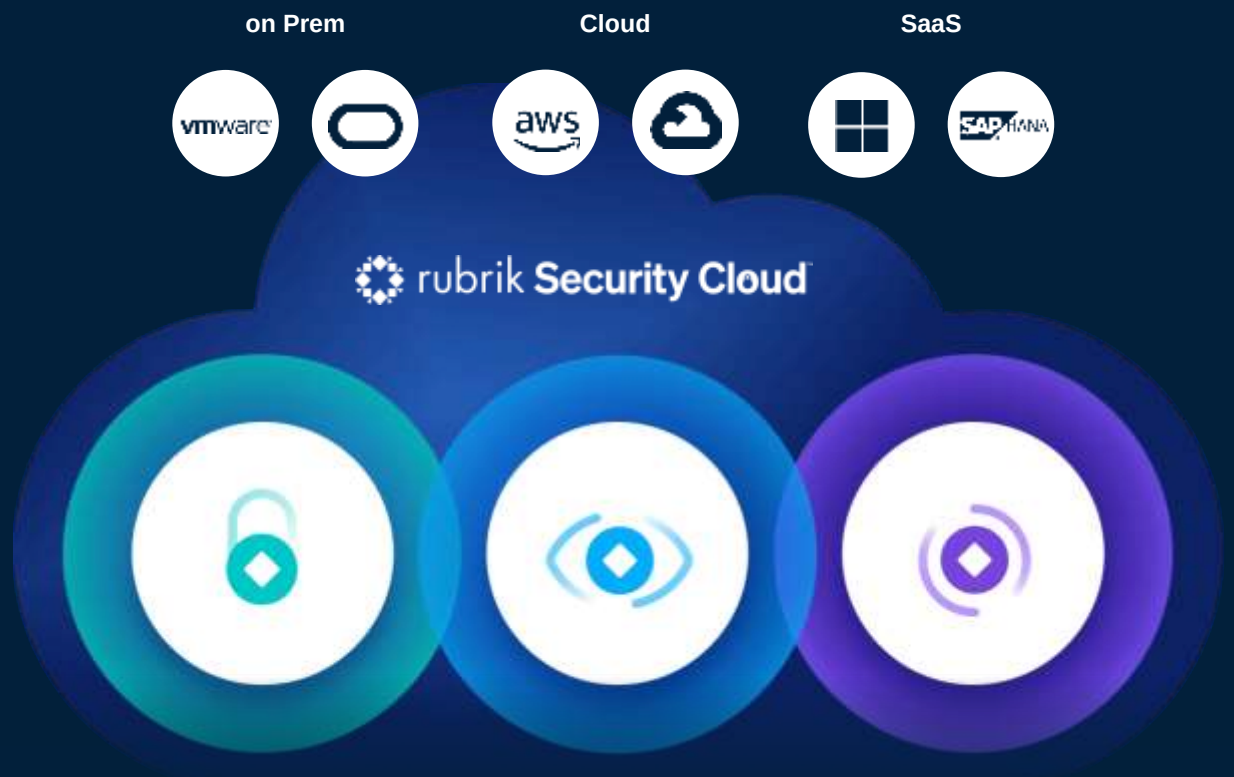
Wie kann ich die Wiederherstellung meiner wichtigsten Anwendungen automatisieren?

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

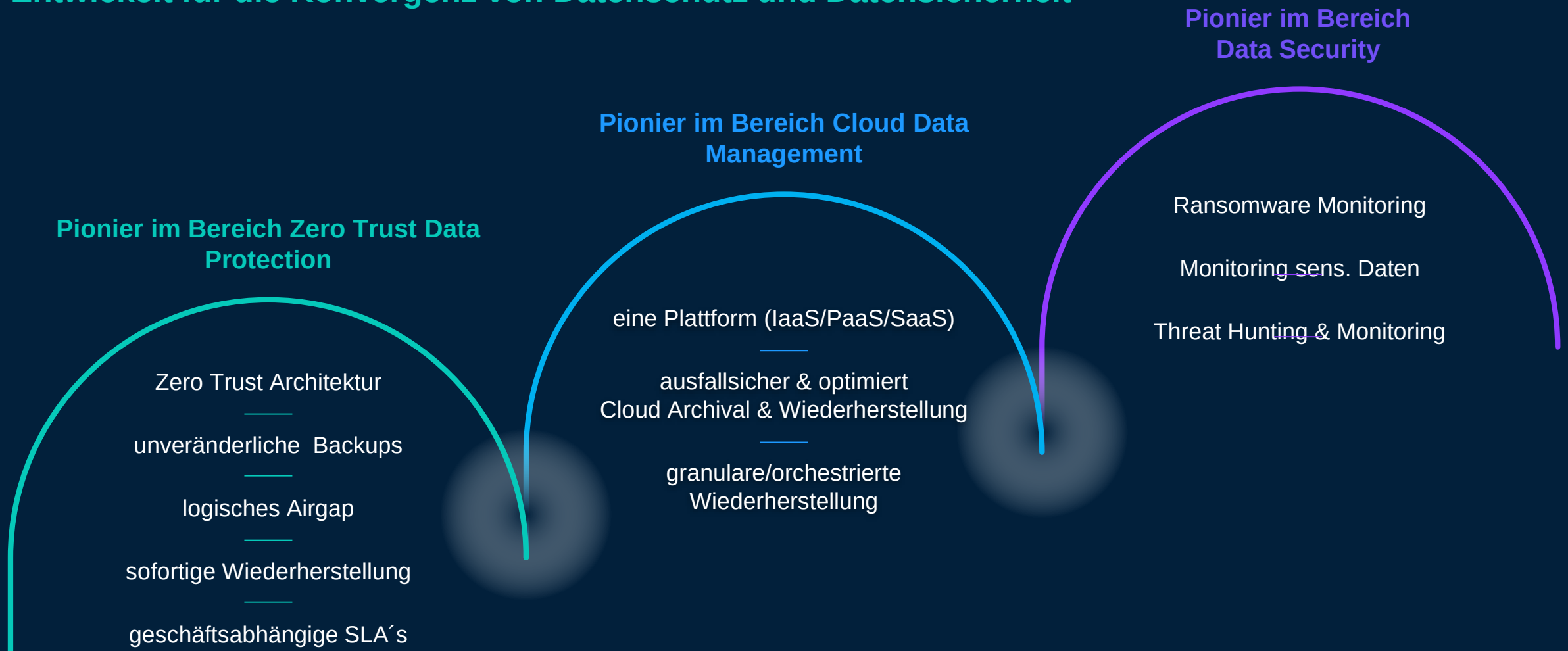
Fortlaufende Überwachung Ihrer Daten auf Ransomware
Gefährdung sensibler Daten beheben
Indikatoren für eine Gefährdung erkennen

NIST Security Standards

Preparation | Detection and Analysis | Containment Eradication and Recovery

Rubrik’s Evolution

Entwickelt für die Konvergenz von Datenschutz und Datensicherheit



2014

Heute

Wir halten was wir versprechen

rubrik

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
- Konsequent, vertraulich, kundenspezifische & schnelle Wiederherstellung
- Wir bleiben so lange Sie uns brauchen.

rubrik

The News…!

rubrik

PRODUCTS SOLUTIONS PARTNERS CASE STUDIES RESOURCES SUPPORT Get started

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

rubrik

PRODUCTS SOLUTI

Company ▶ Newsroom ▶ Press Releases

MAY 25, 2022 | PRESS RELEASE

Rubrik Appoints Former Cer Intelligence Agency (CIA) C Information Security Officer (CISO) Michael Mestrovich Company's CISO

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

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

Get

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
linkedin.com/in/frankschwaak/
@FrankSchwaak