TeleTrusT-interner Workshop

28.06.2023, Berlin

"Ausblick zur Lage der IT-Sicherheit"

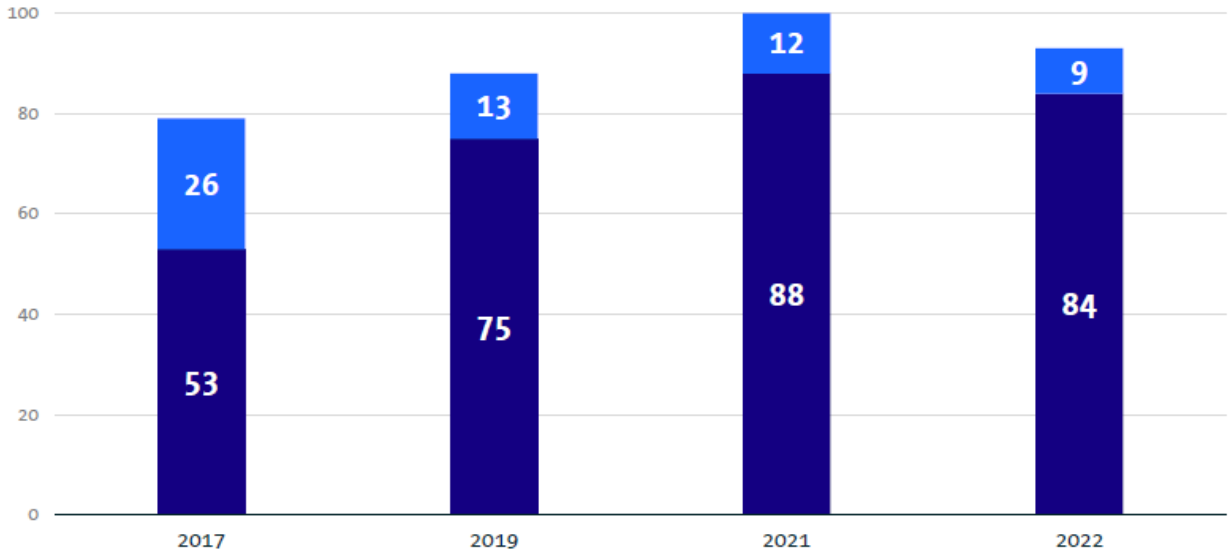
Ron Kneffel, Vorstandsvorsitzender CISO Alliance

Cybercrime-Bedrohungslage

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Deutsche Wirtschaft in der Breite von Angriffen betroffen

War Ihr Unternehmen innerhalb der letzten 12 Monate (2017 und 2019: innerhalb der letzten zwei Jahre) von Diebstahl, Industriespionage oder Sabotage betroffen?



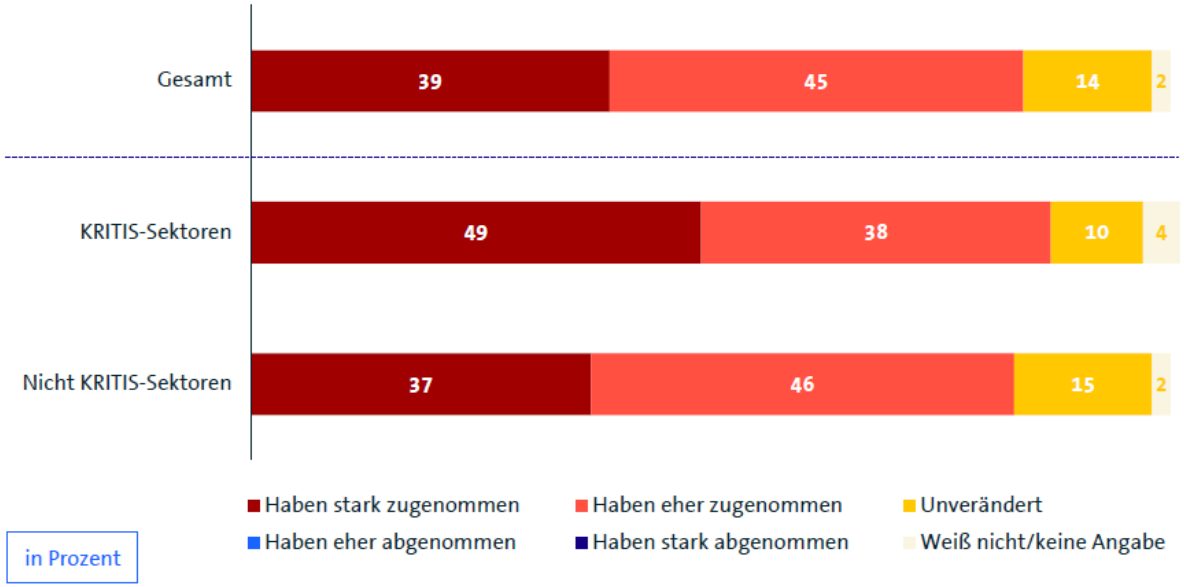
bitkom

2 Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

CISO ALLIANCE

Kritische Infrastruktur rückt in den Fokus von Cyberangriffen

Wie hat sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den vergangenen 12 Monaten entwickelt?



6 Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

bitkom

CISO ALLIANCE

Cybercrime-Bedrohungslage

Was erwartet uns in den kommenden Monaten?

1. Smart devices als Hacking-Ziel
2. Phishing und Social Engineering
3. Crime as-a-Service
4. Mehrere Bedrohungsvektoren bei Angriffen
5. Attacken auf Cloud Security
6. Risiken mit Third-Party-Zugängen
7. Mangel an IT-Personal-Ressourcen
8. Cyber Attacken durch nation state actors

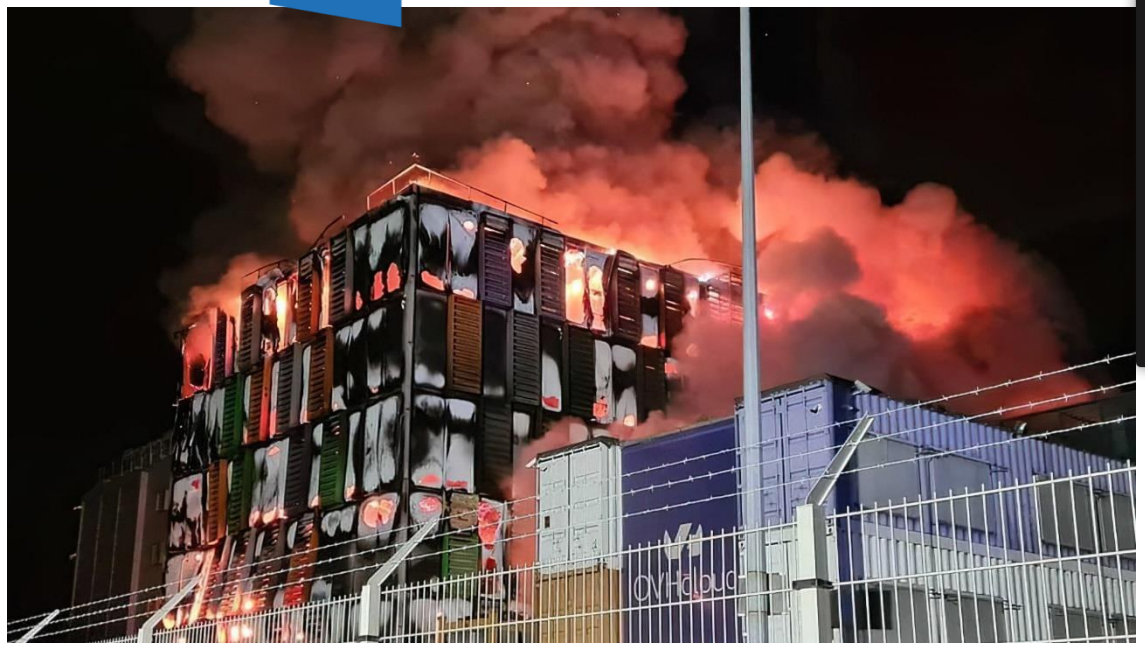
Cybercrime-Bedrohungslage

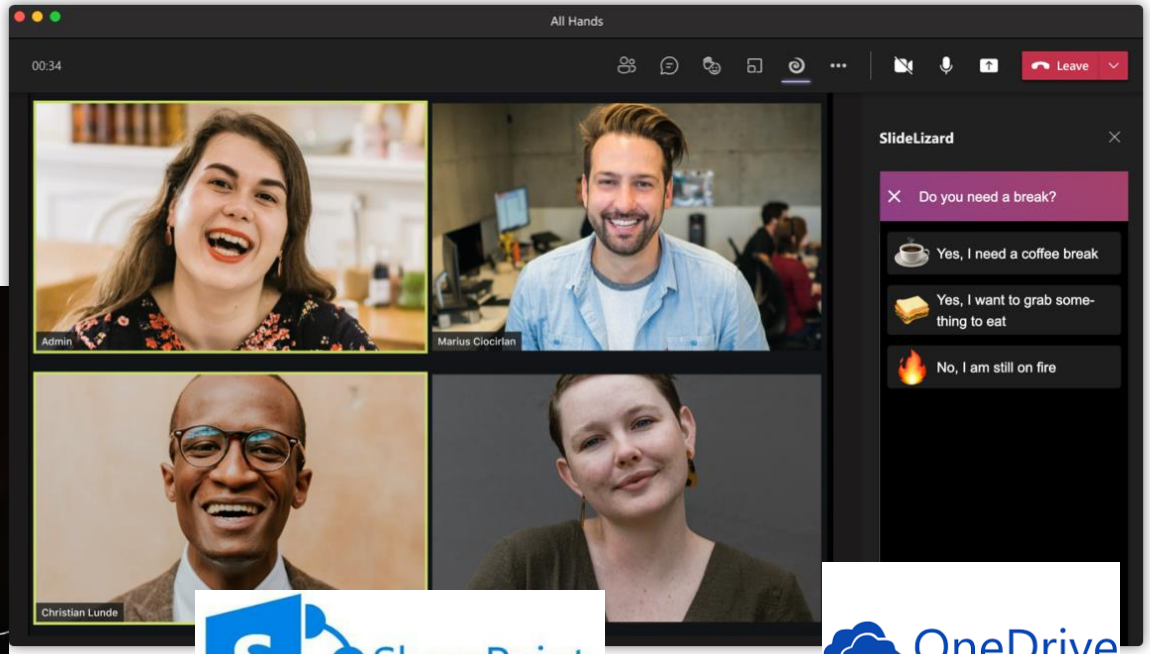
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Ausfälle bei Auslagerungen sind problematisch

Microsoft Teams

Exchange





SharePoint

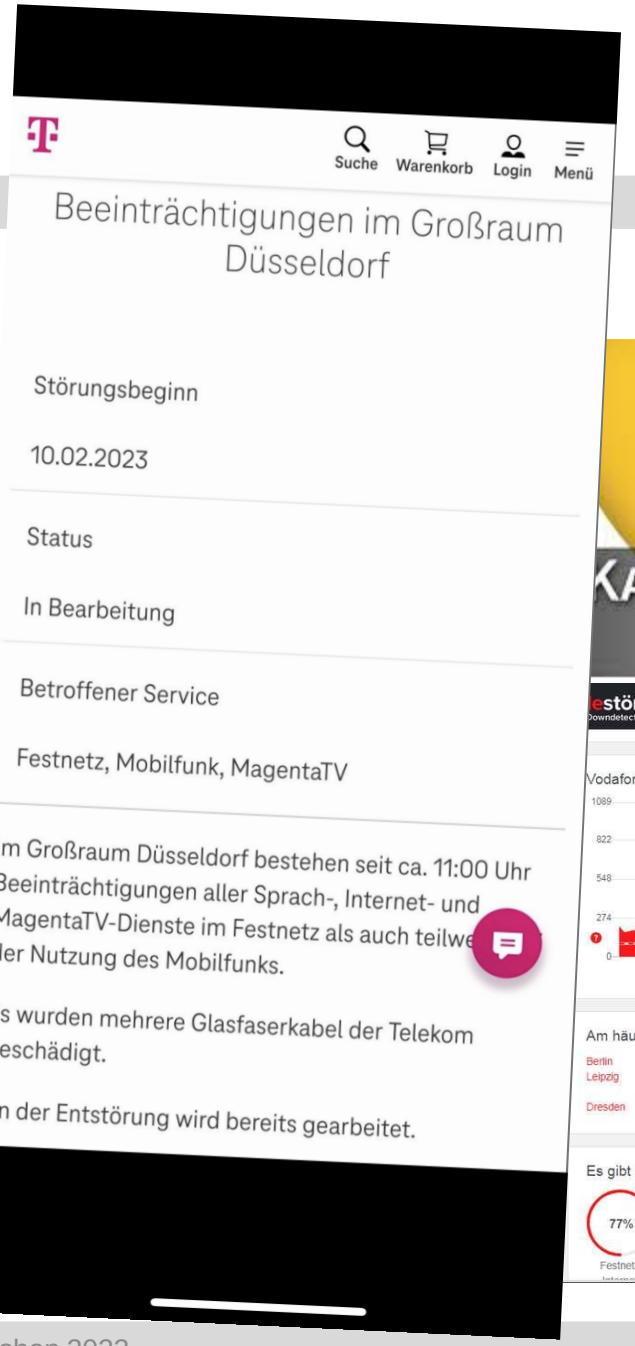
OneDrive

CISO ALLIANCE

Cybercrime-Bedrohungslage

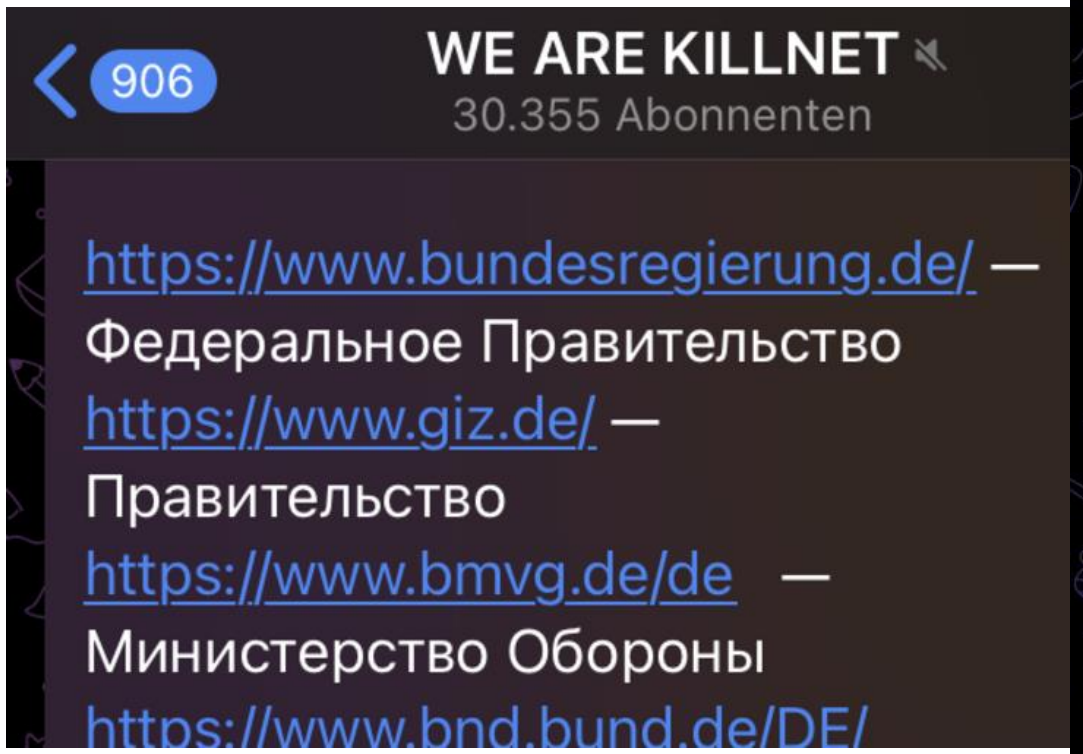
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

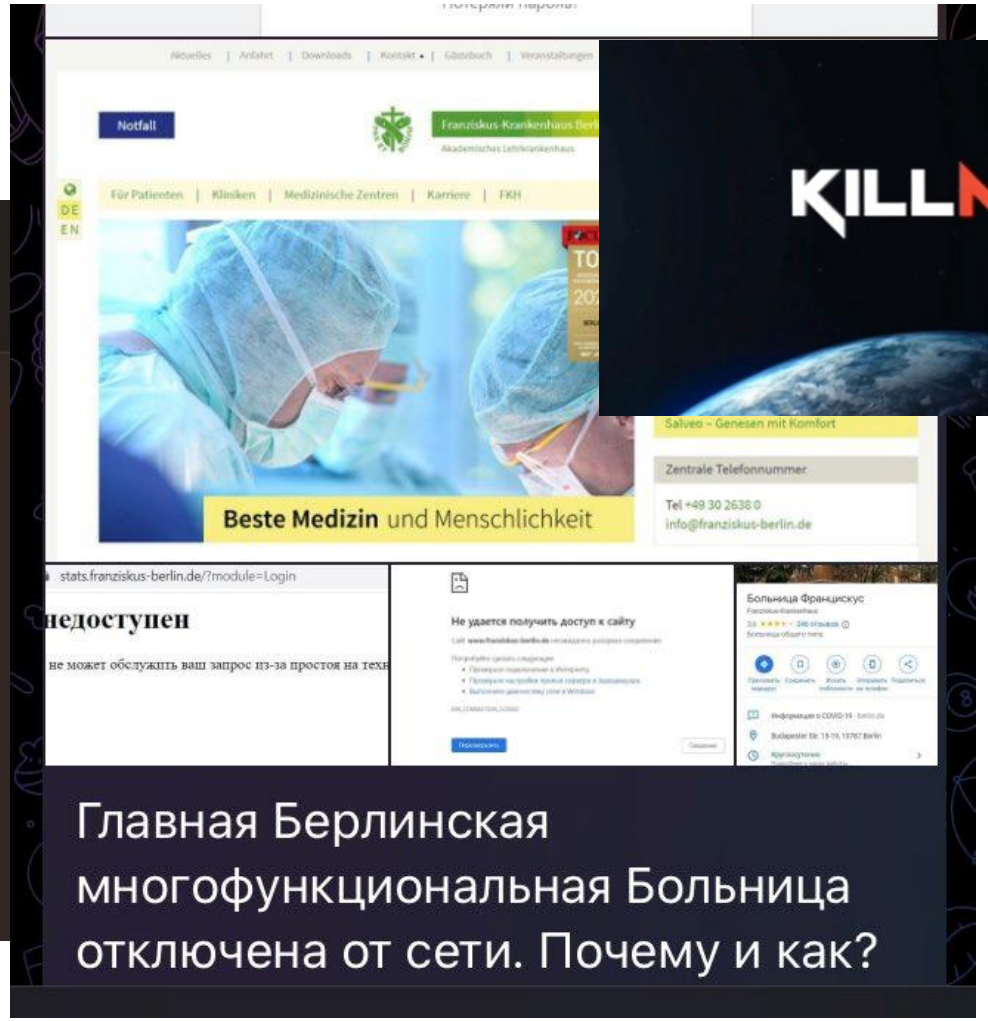
Störung der Internetanbindung führt zu erheblichen Arbeitsbeeinträchtigungen



Cybercrime-Bedrohungslage

Hacktivisten bedrohen EU und vor allem NATO-Länder

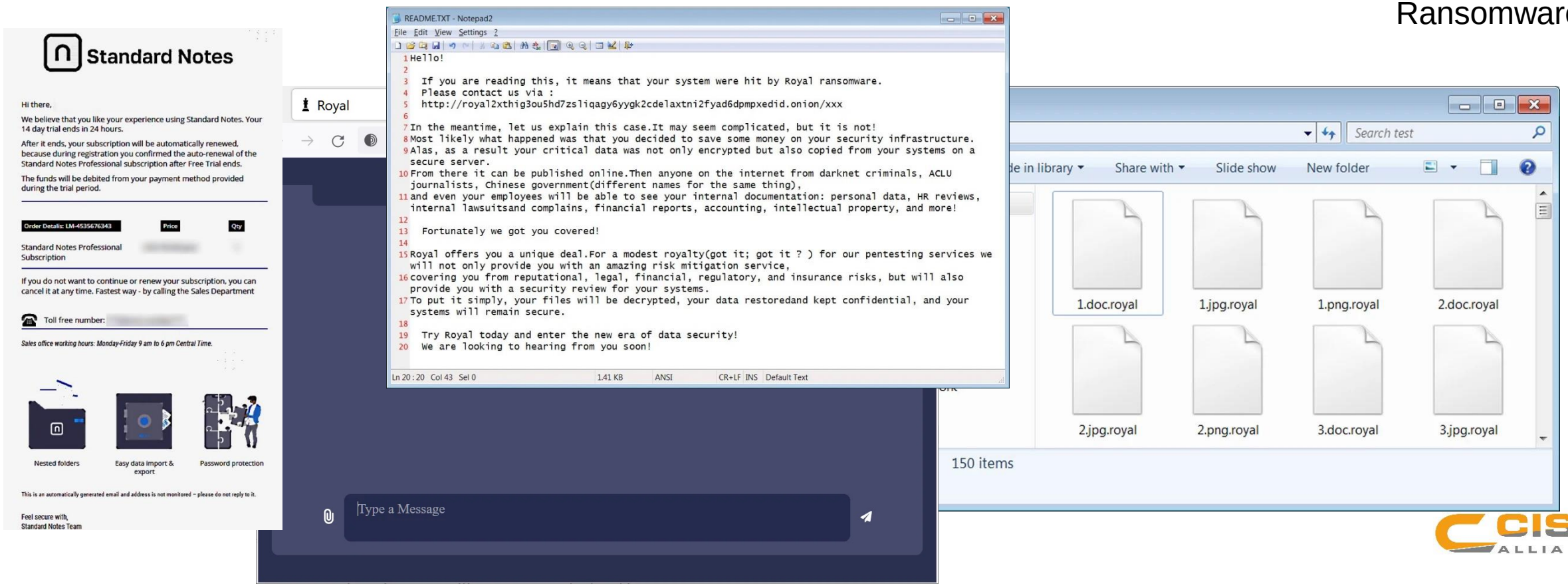




Cybercrime-Bedrohungslage

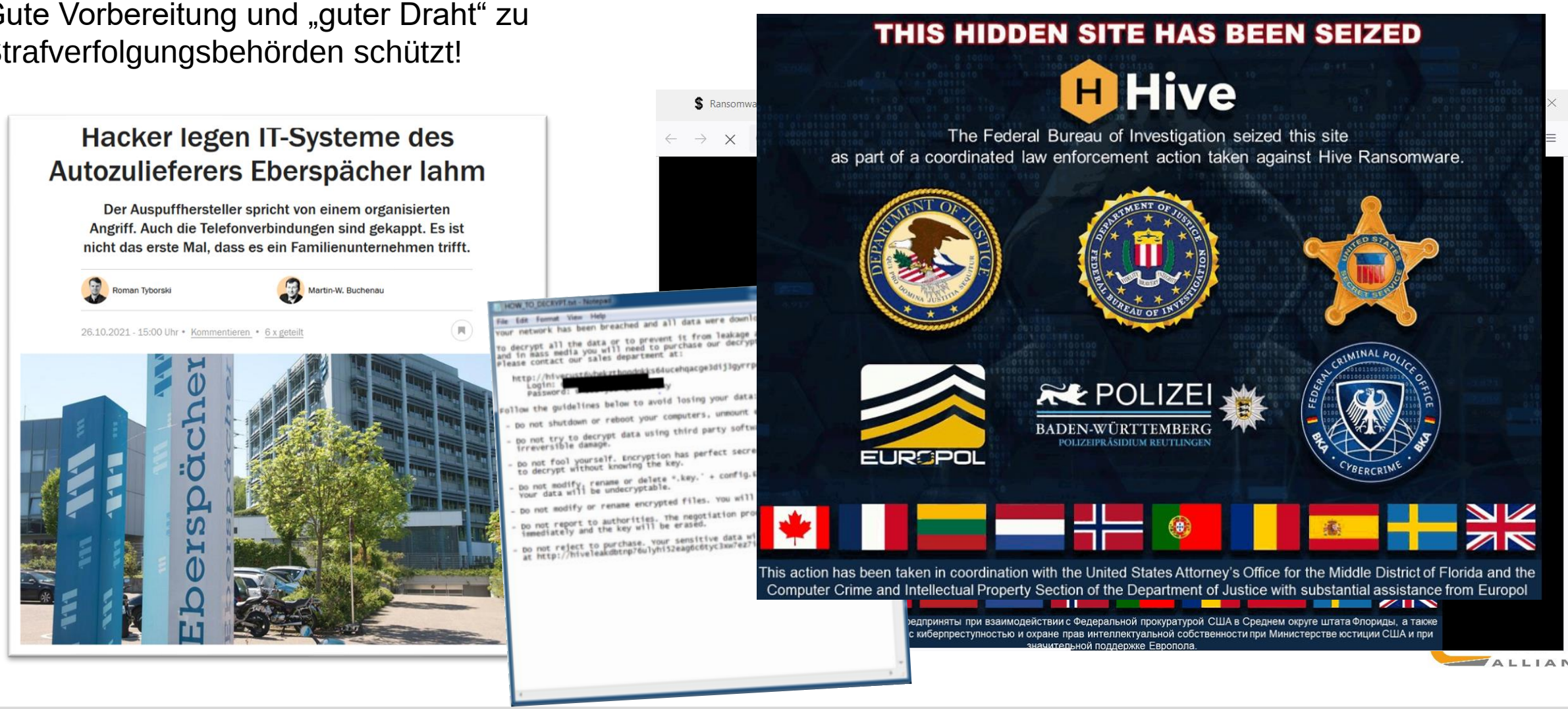
Die organisierte Kriminalität entdeckt Cybercrime und steigt vermehr in Ransomwarebanden ein

Ständig entstehen neue Cybercrime-Aktoren wie UAC-0098, die Bloody Ransomware Gang oder Royal Ransomware



Cybercrime-Bedrohungslage

Gute Vorbereitung und „guter Draht“ zu Strafverfolgungsbehörden schützt!



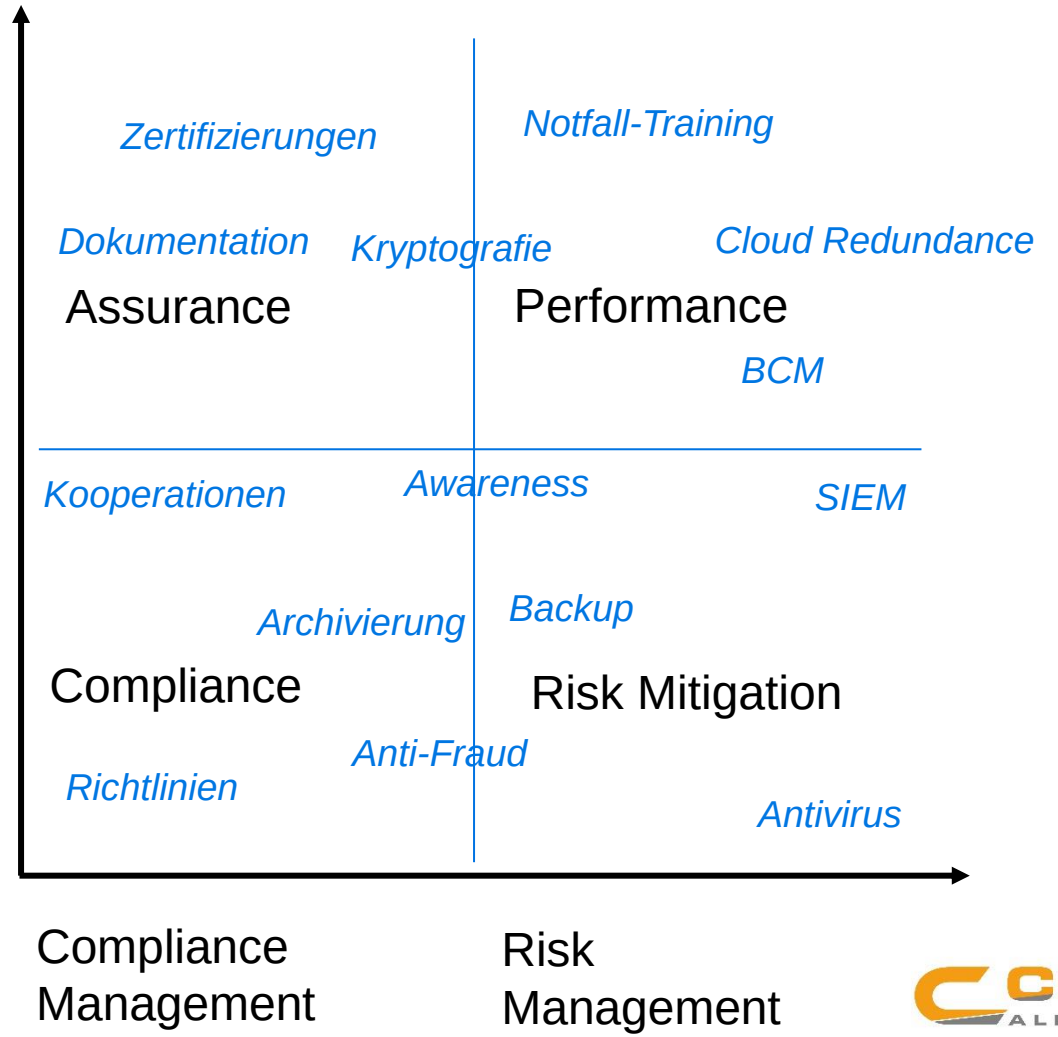
Projektintention

Evolution der IT-Sicherheitsstrategie

In den Themen Compliance und Risk clustern wir die notwendigen Maßnahmen in „ökonomisch sinnvoll“ und „strategisch notwendig“.

Ziel ist es, mit der Sicht aufs Ganze das Sicherheits-Niveau des Informations-Verbundes derart zu heben, dass externe Anforderungen und interner Schutzbedarf ganzheitlich befriedigend bedient werden.

Wir möchten darstellen können, dass wir die Resilienz des Unternehmens sowohl gegenüber Aufsichtsorganen als auch der Marktsituation sichergestellt haben.

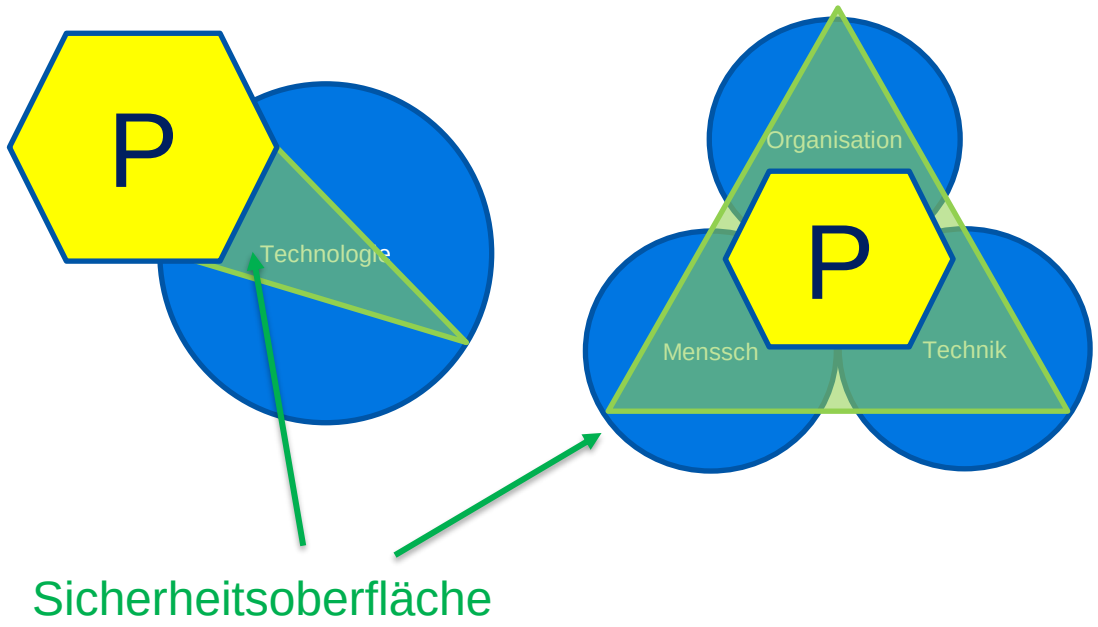


Projektintention

Wohin müssen wir:

Next Steps… für mehr Choices!

- Ausgeglichener Maßnahmenaufbau der Faktoren Technik – Mensch – Organisation

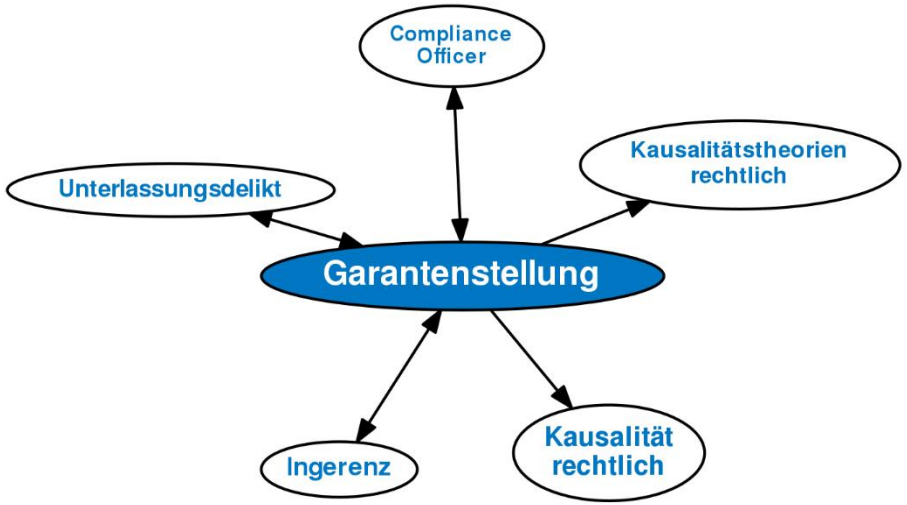


Was wir bereits tun

Die Auslagerung von IT-Services ist heute aus Usability- und Kostengründen alternativlos.
Dadurch ist **Supply Chain** aber nicht nur Liefern, sondern auch Versorgen und Bereitstellen.

Wir überprüfen alle Service Level Agreements wie folgt:

1. Erhalt der Betriebsbereitschaft der Prozesse
2. Unterstützung bei Aufrechterhaltung der Sicherheit
3. Zusicherung einer angemessenen Entstörgeschwindigkeit
4. Versorgung mit notwendigen Komponenten
5. Zukunftssicherheit für die Investition
6. Plansicherheit für die Kosten



Springer Gabler

Quelle: https://wirtschaftslexikon.gabler.de/definition/garantenstellung-32061

Dienstleistungen und Services können wir auslagern – nicht aber die Verantwortlichkeit.
-> Primärgarantenstellung

Geplante Maßnahmen

Effiziente Sicherheit entsteht durch Gleichgewicht in Prävention – Detektion und Reaktion

Aufgrund des Fortschrittes starker **präventiver Fähigkeiten muss** eine verstärkte Priorisierung der Handlungsfelder erfolgen:

Detektion von Bedrohungen: Aufbau eines SIEM, Verbesserung der Sensorik im Netzwerk

Reaktion auf Gefährdungen: Aufbau eines SIRT (Security Incident Response Teams) und MDR (managed detection & response)

Im Bereich Prävention muss kurzfristig vor allem die Supply-Chain-Sicherheit betont werden.
Dies soll dem starken Hang zu Auslagerungen besser gerecht werden und der Frage nach dem „Wann“ schneller entgegenwirken

Geplante Maßnahmen

Die Zusammenführung von BCM und ITSCM

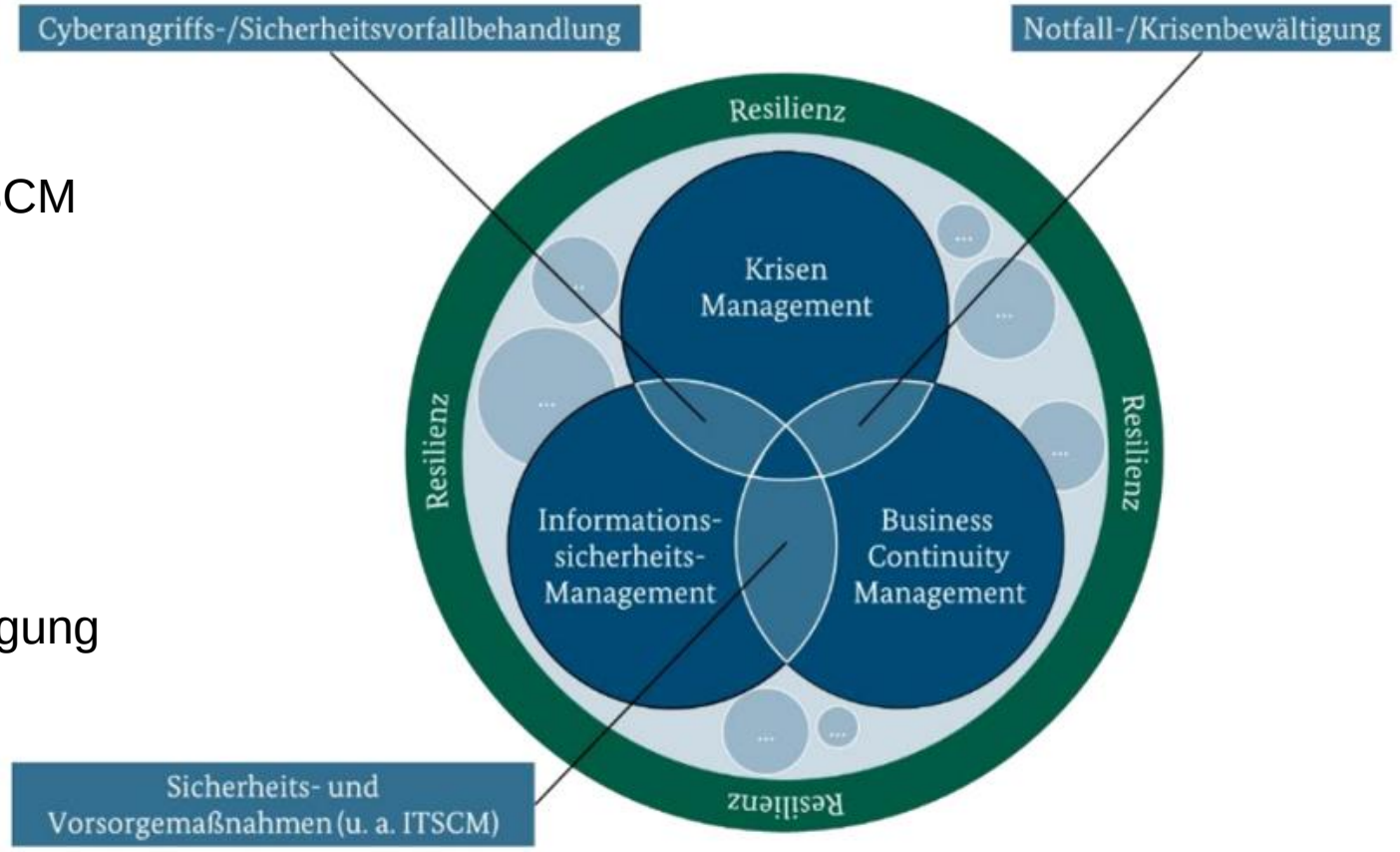
in Zuarbeit des Krisenstabes soll die

Fähigkeit zu mehr Resilienz

im Verbund fördern

Kernaufgabe ist nach wie vor die Ertüchtigung

der Vorfallreaktionsfähigkeit



Projekt IT-Security - Report PLA 01/2023

TeleTrusT-interner Workshop

28.06.2023, Berlin

Danke für Ihre Aufmerksamkeit!