



Business Continuity Management: Bedrohungen durch Cyberangriffe

Nicolai Czink

Bedrohung durch Cyberangriffe

Cyberangriffe mit dem Einsatz von Ransomware

ist eine der größten Bedrohungen
und es gibt **keinen 100% Schutz** davor!

Ziel von Cyberangriffen: Erpressung

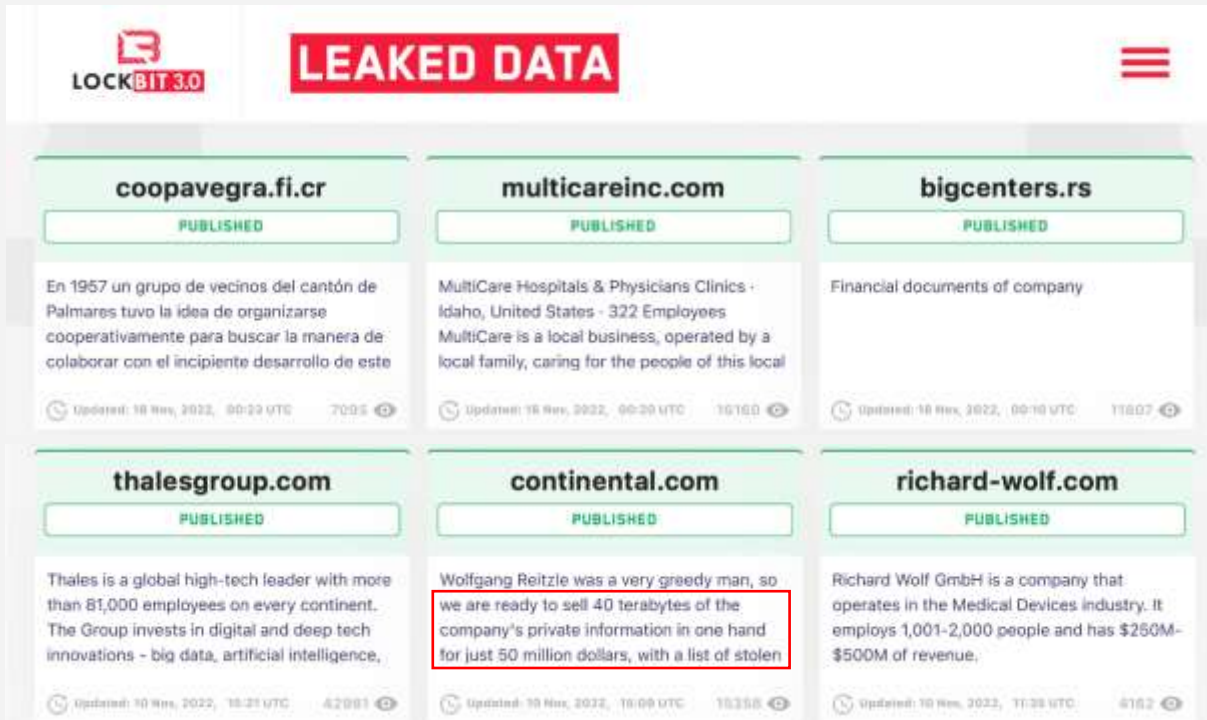
Oft durch **Triple Extortion** – einen Cocktail, den man nicht an der Bar genießt...

1. **Verschlüsseln/Sperren/Verhindern** – durch Lösegeld erhält man wieder Kontrolle
2. **Veröffentlichung von Daten** – Lösegeld, sonst werden Daten leaked
3. **Erpressung über die Kunden** – Lösegeld, sonst werden Kunden angegriffen

Die massive Störung der Geschäftsprozesse ist das Ziel!

...damit der Leidensdruck hoch genug ist, um zu zahlen

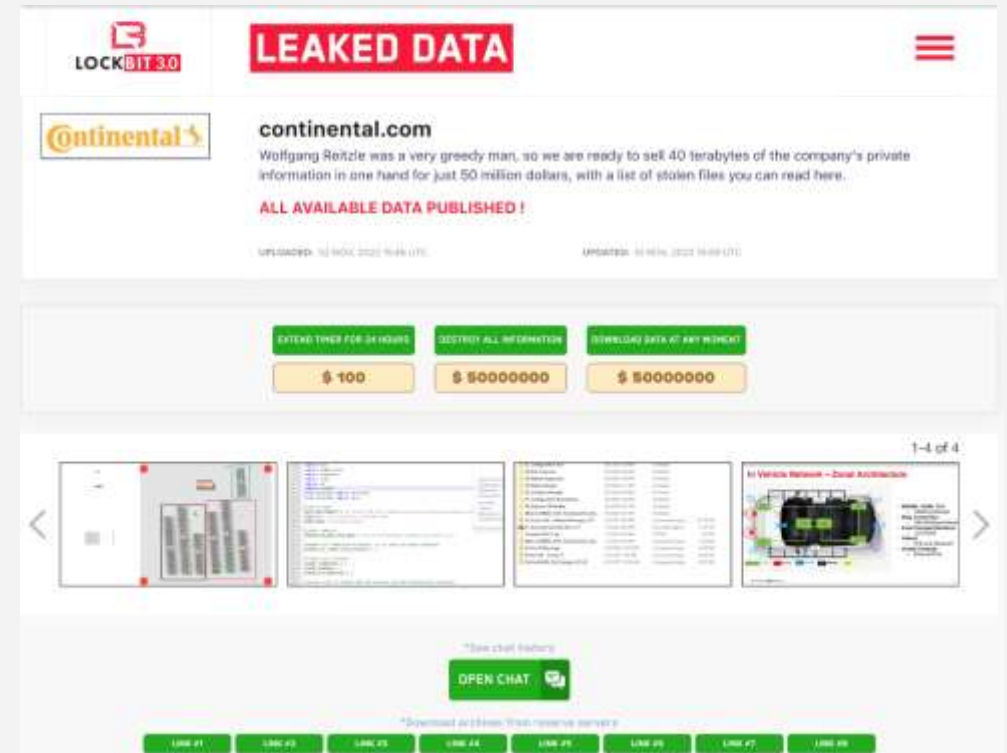
Ransomware as a Service



LOCKBIT 3.0 **LEAKED DATA**

coopavegra.fi.cr	multicareinc.com	bigcenters.rs
PUBLISHED	PUBLISHED	PUBLISHED
En 1957 un grupo de vecinos del cantón de Palmares tuvo la idea de organizarse cooperativamente para buscar la manera de colaborar con el incipiente desarrollo de este	MultiCare Hospitals & Physicians Clinics - Idaho, United States - 322 Employees MultiCare is a local business, operated by a local family, caring for the people of this local	Financial documents of company
Updated: 18 Nov, 2022, 00:23 UTC 7005	Updated: 18 Nov, 2022, 00:20 UTC 16160	Updated: 18 Nov, 2022, 00:10 UTC 11607

thalesgroup.com	continental.com	richard-wolf.com
PUBLISHED	PUBLISHED	PUBLISHED
Thales is a global high-tech leader with more than 81,000 employees on every continent. The Group invests in digital and deep tech innovations - big data, artificial intelligence,	Wolfgang Reitzle was a very greedy man, so we are ready to sell 40 terabytes of the company's private information in one hand for just 50 million dollars, with a list of stolen	Richard Wolf GmbH is a company that operates in the Medical Devices industry. It employs 1,001-2,000 people and has \$250M-\$500M of revenue.
Updated: 18 Nov, 2022, 18:21 UTC 42081	Updated: 18 Nov, 2022, 16:09 UTC 16358	Updated: 18 Nov, 2022, 11:33 UTC 6162



LOCKBIT 3.0 **LEAKED DATA**

continental.com

Wolfgang Reitzle was a very greedy man, so we are ready to sell 40 terabytes of the company's private information in one hand for just 50 million dollars, with a list of stolen files you can read here.

ALL AVAILABLE DATA PUBLISHED !

Updated: 18 Nov, 2022, 16:09 UTC

[EXTEND TIME FOR 24 HOURS](#) [DESTROY ALL INFORMATION](#) [DOWNLOAD DATA AT ANY MOMENT](#)

[\\$ 100](#) [\\$ 50000000](#) [\\$ 50000000](#)

1-4 of 4

[LINK #1](#) [LINK #2](#) [LINK #3](#) [LINK #4](#) [LINK #5](#) [LINK #6](#) [LINK #7](#) [LINK #8](#)

Quelle: Lockbit BLOG (öffentliche Website im Dark Web)

17:30 Uhr am Karfreitag 2022

„Ich hab grad die Nummer von eurem Support nicht bei der Hand...

...wir wurden gehackt! HILFE!“

Direkte Challenges bei der Behebung

Kommunikation - Womit?

Login - Wie?

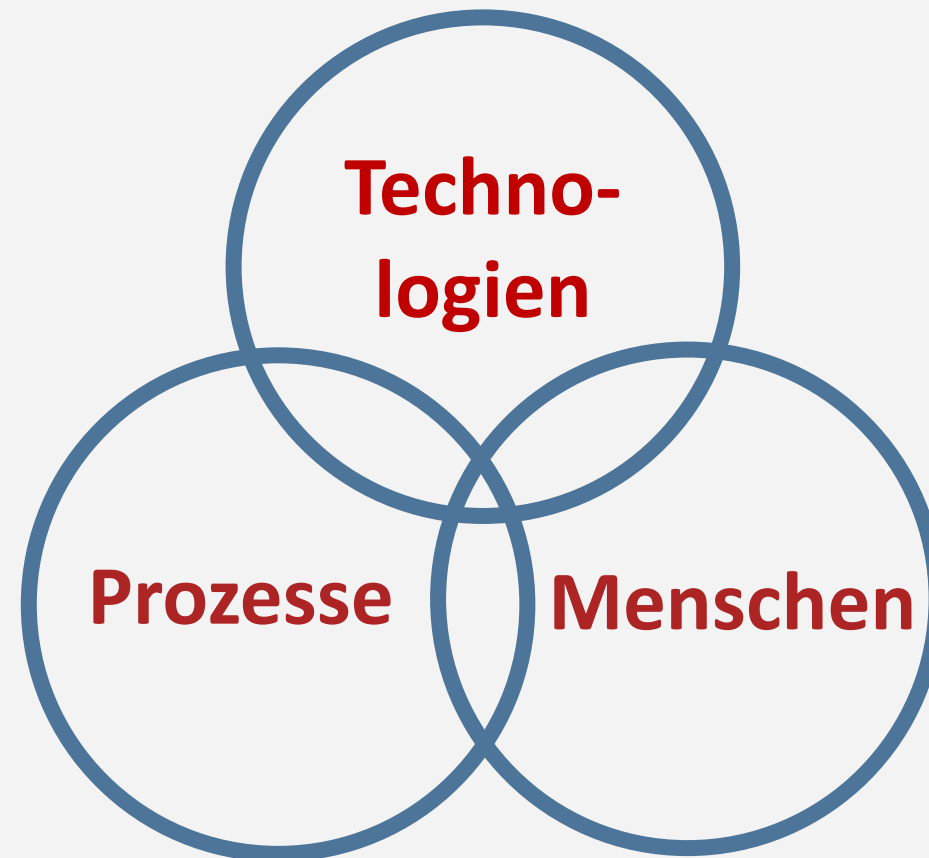
Notfallplan - Wo?

Rücksichern – Wohin?

Wie schütze ich nun mein Unternehmen?

Nur ein aktives **Business Continuity Management**
bietet umfassende Prävention und rasche Reaktion bei
Ransomware-Angriffen!

Vorbereitung ist alles



Gewappnet sein gegen Cyberangriffe

Alles dreht sich um Business Continuity



Gewappnet sein gegen Cyberangriffe

Alles dreht sich um Business Continuity



Gewappnet sein gegen Cyberangriffe

Alles dreht sich um Business Continuity



- BCM Assessments durchführen
- Vulnerability / Risk Assessments durchführen

Gewappnet sein gegen Cyberangriffe

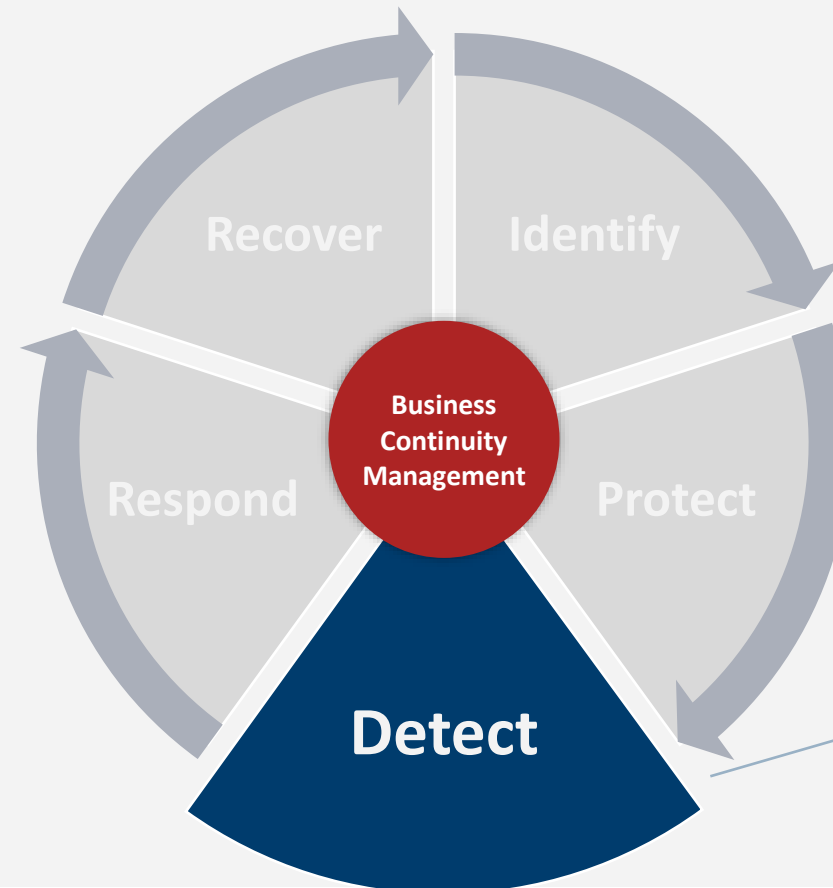
Alles dreht sich um Business Continuity



- Einfallstore technisch schließen
- Regelmäßige Backups sicherstellen
- Mitarbeiter trainieren
- Notfallplan erstellen

Gewappnet sein gegen Cyberangriffe

Alles dreht sich um Business Continuity

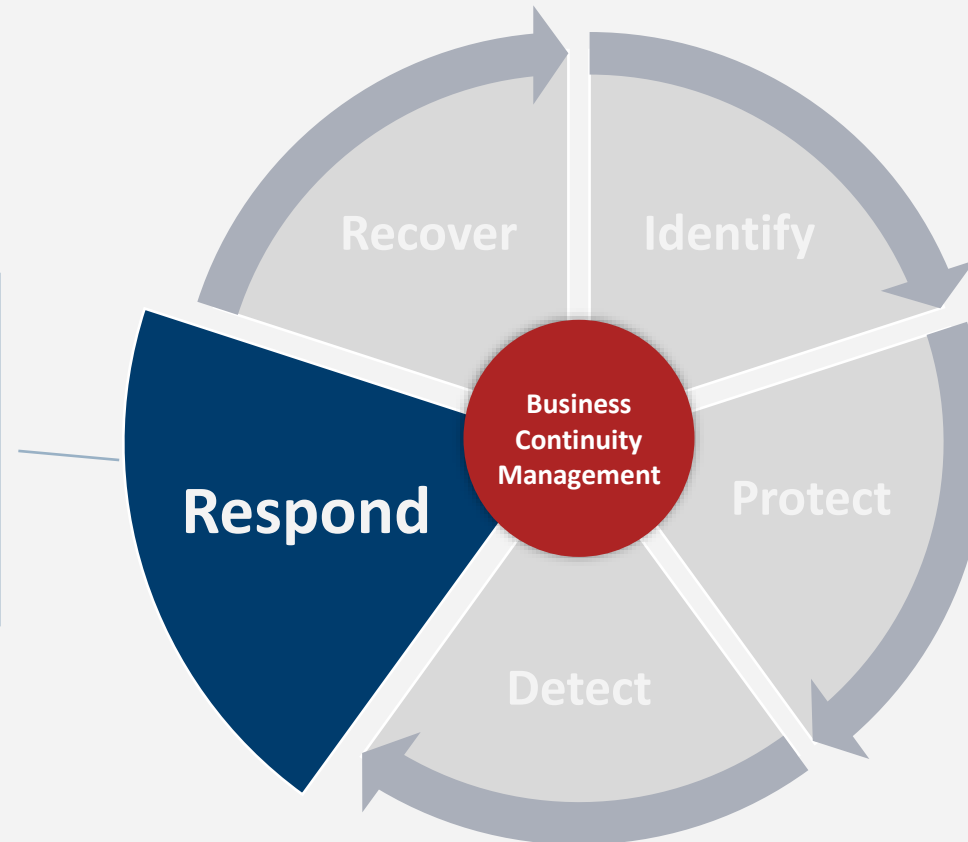


- Anomalien erkennen (SOC / EDR & MDR)
- Backups scannen

Gewappnet sein gegen Cyberangriffe

Alles dreht sich um Business Continuity

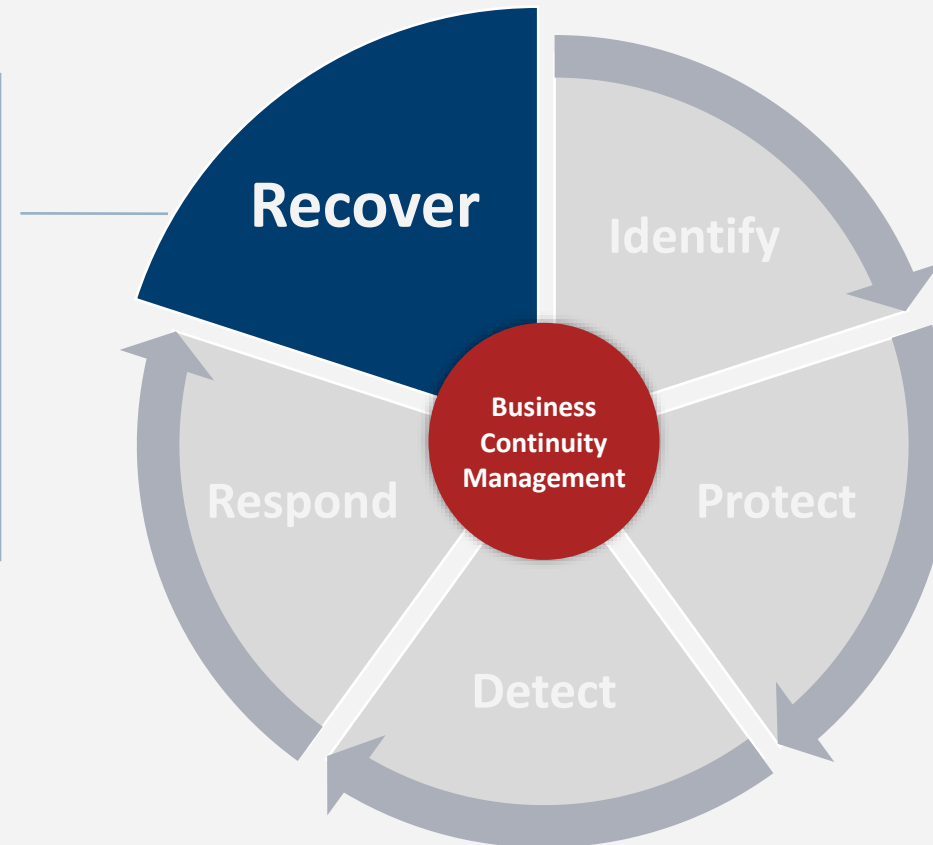
- Incident Response starten (Isolieren, Analysieren)
- D/R First Response starten



Gewappnet sein gegen Cyberangriffe

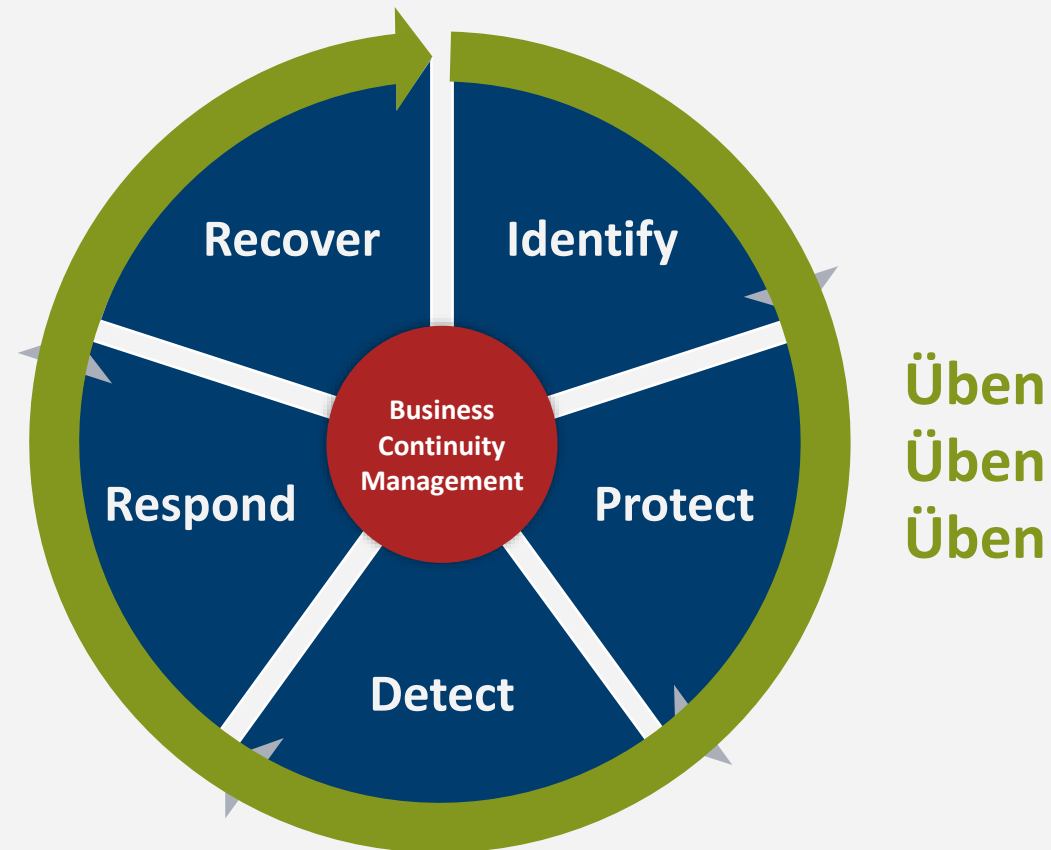
Alles dreht sich um Business Continuity

- D/R Plan und Mechanismen nutzen
- Systeme und Daten wiederherstellen
- Clean-Up durchführen
- Root Cause Analyse



Gewappnet sein gegen Cyberangriffe

Alles dreht sich um Business Continuity



Key Take Aways

-  **Krisenmanagement und Business Continuity Management sind essentiell**
Technik schützt, im Falle des Falles muss aber die Rettungskette reibungslos funktionieren
-  **Cloud Services können Lebensretter sein**
Kommunikation (Mail, Chat, Telcos) und Management (Endpoint/Perimeter)
schneller Zugriff auf Daten/Logs, für Produktionsrestart und Forensic
-  **Unzerstörbare WORM Backups - Die kritischen Daten bleiben erhalten**

Handeln Sie **JETZT**...

...denn Angreifer halten sich nicht an Budget-Zyklen!



Heute: Tauschen Sie sich hier mit anderen Teilnehmern und mit uns aus

Morgen: Besprechen Sie mit Ihrem Team die derzeitigen Maßnahmen

Nächste Woche: Setzen Sie eine Taskforce zur Analyse ein

In einem Monat: Schließen Sie die ersten Gaps und üben Sie



Nicolai Czink

Strategie und Transformation

n.czink@bacher.at

+43 664 601 26 256



...wir leben
mITverantwortung

Bacher Systems EDV GmbH

Wienerbergstr. 11/B9

1100 Wien

info@bacher.at

Tel: +43 1 60 126-0

www.bacher.at