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

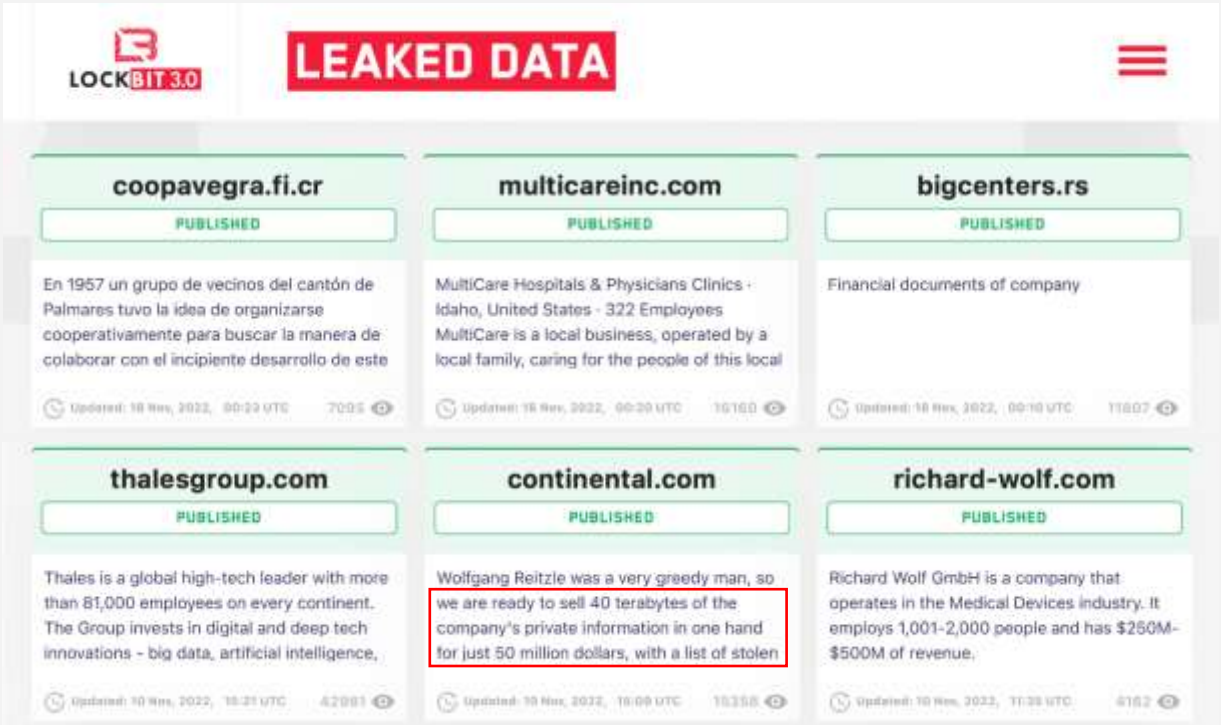
Oft durch **Triple Extortion** – einen Cocktail, den man nicht an der Bar genießt…

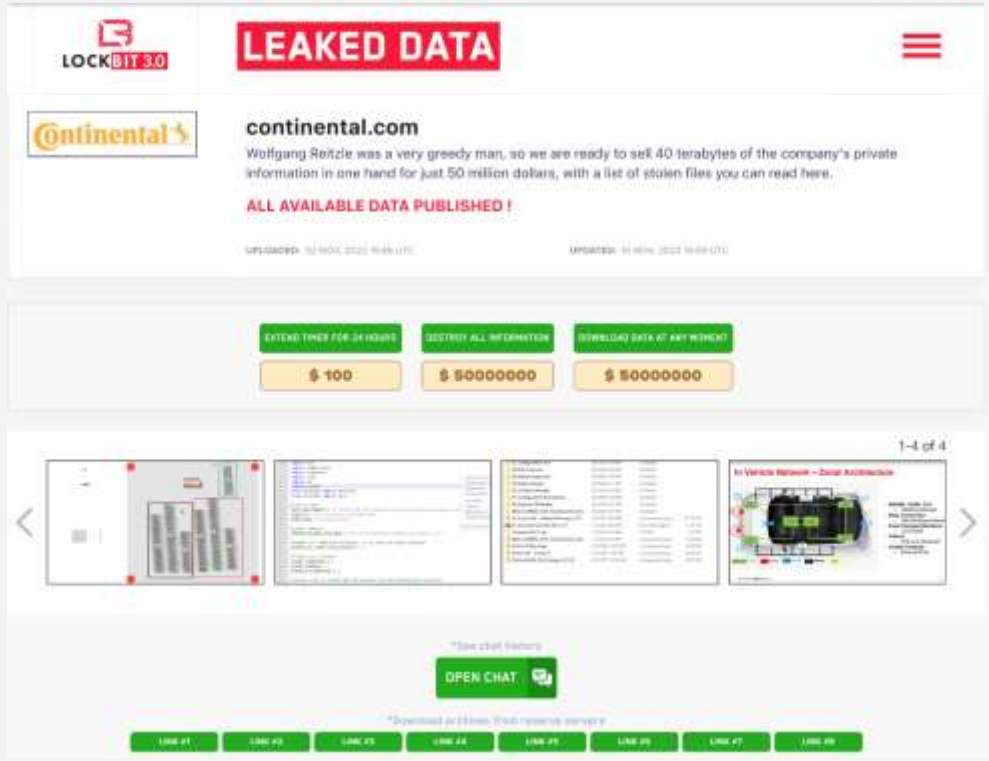
1. **Verschlüsseln/Sperren/Verhindern** – durch Lösegeld erhält man wieder Kontrolle
2. **Veröffentlichung von Daten** – Lösegeld, sonst werden Daten geleaked
3. **Erpressung über die Kunden** – Lösegeld, sonst werden Kunden angegriffen

Die massive Störung der Geschäftsprozesse ist das Ziel!

…damit der Leidensdruck hoch genug ist, um zu zahlen

Ransomware as a Service





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?

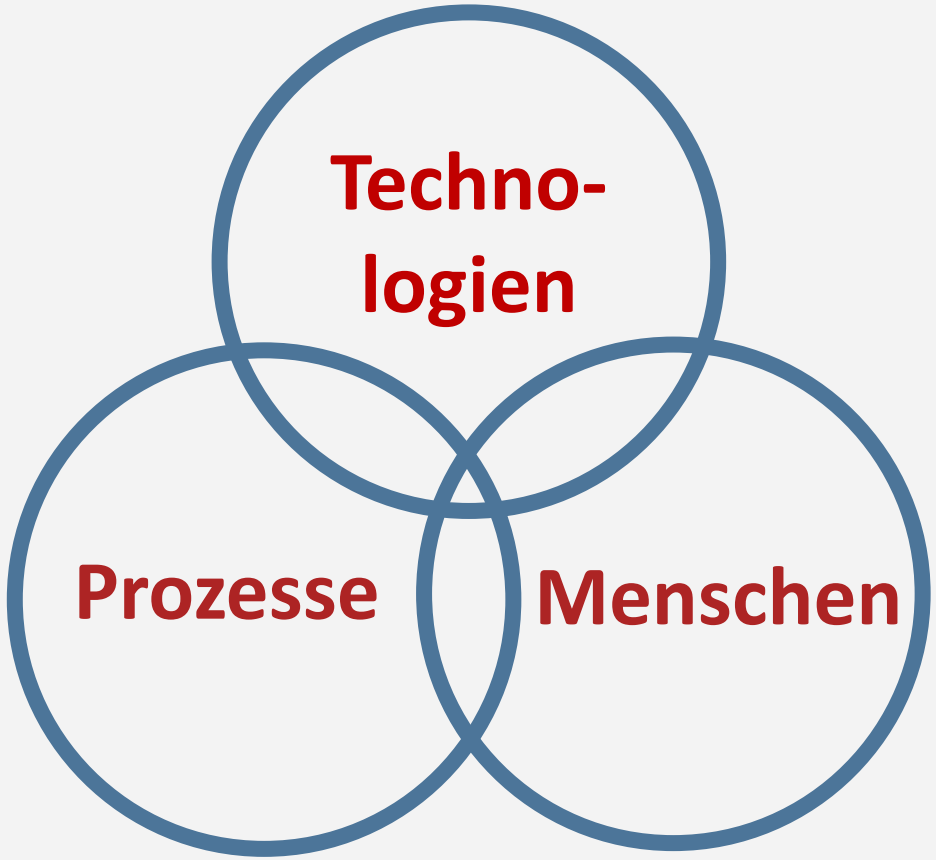
Notfallplan - Wo?

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

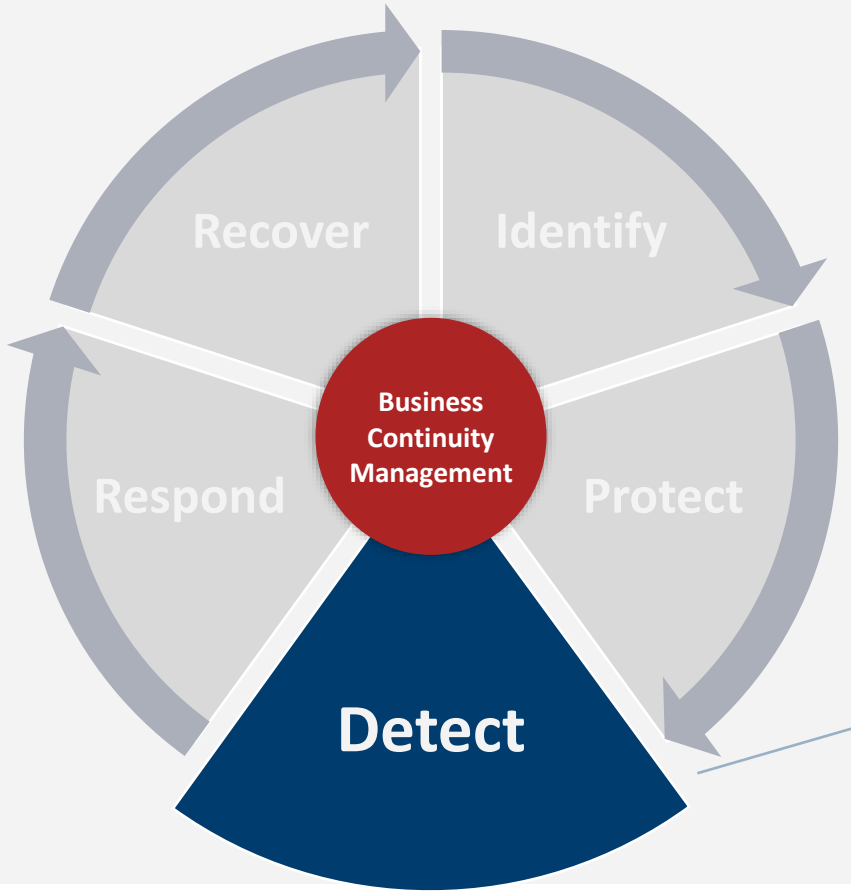
Gewappnet sein gegen Cyberangriffe

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

Üben
Üben
Üben

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

m*IT*verantwortung

Bacher Systems EDV GmbH
Wienerbergstr. 11/B9
1100 Wien
info@bacher.at
Tel: +43 1 60 126-0
www.bacher.at