

# INVENTORY

SECURING DIGITAL PRODUCTIVITY



# GEFAHRENBETRACHTUNG FÜR KLEINE UND MITTLERE UNTERNEHMEN

„Die IT-Sicherheitslage in Deutschland ist insgesamt angespannt bis kritisch“

Bundesamt für Sicherheit in der Informationstechnik



# ANGEGRIFFENE UNTERNEHMEN 2022 (EIN AUSZUG):

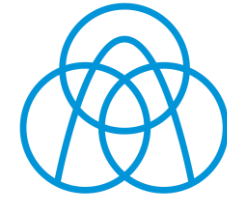
Unternehmen aller Größen sowie aller Branchen





# ANGEGRIFFENE UNTERNEHMEN 2023 (EIN AUSZUG):

Unternehmen aller Größen sowie aller Branchen



thyssenkrupp





# ANGEGRIFFENE UNTERNEHMEN 2023 (EIN AUSZUG):

Unternehmen aller Größen sowie aller Branchen



thyssenkrupp




**WEITERE FOLGEN**





# AKTUELLES BEISPIEL: DEUTSCHE LEASING


## Hackerangriff am 03.06.2023

 IT Finanzmagazin

### Schwerwiegender Cyberangriff auf Deutsche Leasing · IT Finanzmagazin

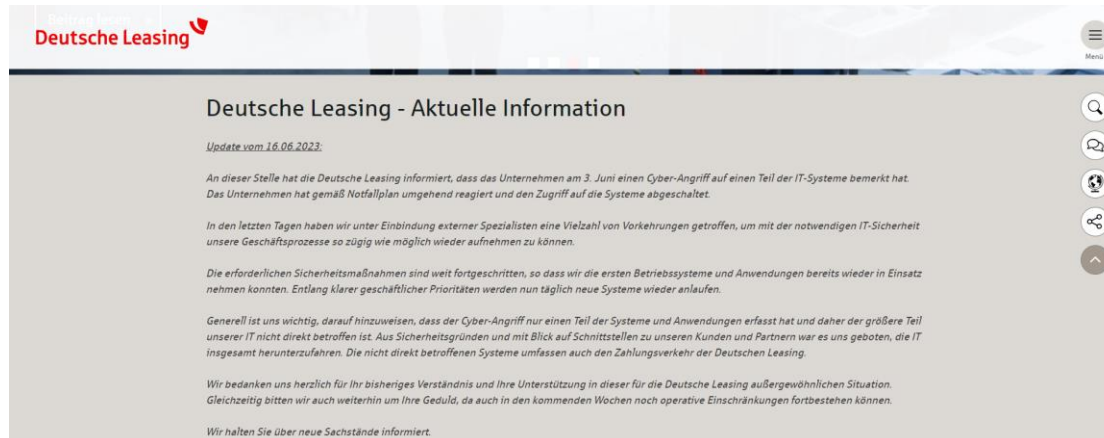
Die Deutsche Leasing ist seit mehr als 48 Stunden praktisch offline. Aus Sicherheitsgründen wurden die meisten IT-Systeme heruntergefahren.  
vor 20 Stunden



 Heise

### Cyber-Angriff: IT der Deutsche Leasing seit Samstag offline

Bei Deutsche Leasing, einer großen Leasinggesellschaft zahlreicher Sparkassen, kam es am Samstag zu einem Cyber-Angriff.  
vor 23 Stunden



**Deutsche Leasing**

#### Deutsche Leasing - Aktuelle Information

Update vom 16.06.2023.

An dieser Stelle hat die Deutsche Leasing informiert, dass das Unternehmen am 3. Juni einen Cyber-Angriff auf einen Teil der IT-Systeme bemerkt hat. Das Unternehmen hat gemäß Notfallplan umgehend reagiert und den Zugriff auf die Systeme abgeschaltet.

In den letzten Tagen haben wir unter Einbindung externer Spezialisten eine Vielzahl von Vorkehrungen getroffen, um mit der notwendigen IT-Sicherheit unsere Geschäftsprozesse so zügig wie möglich wieder aufnehmen zu können.

Die erforderlichen Sicherheitsmaßnahmen sind weit fortgeschritten, so dass wir die ersten Betriebssysteme und Anwendungen bereits wieder in Einsatz nehmen konnten. Entlang klarer geschäftlicher Prioritäten werden nun täglich neue Systeme wieder anlaufen.

Generell ist uns wichtig, darauf hinzuweisen, dass der Cyber-Angriff nur einen Teil der Systeme und Anwendungen erfasst hat und daher der größere Teil unserer IT nicht direkt betroffen ist. Aus Sicherheitsgründen und mit Blick auf Schnittstellen zu unseren Kunden und Partnern war es uns geboten, die IT insgesamt herunterzufahren. Die nicht direkt betroffenen Systeme umfassen auch den Zahlungsverkehr der Deutschen Leasing.

Wir bedanken uns herzlich für Ihr bisheriges Verständnis und Ihre Unterstützung in dieser für die Deutsche Leasing außergewöhnlichen Situation. Gleichzeitig bitten wir auch weiterhin um Ihre Geduld, da auch in den kommenden Wochen noch operative Einschränkungen fortbestehen können.

Wir halten Sie über neue Sachstände informiert.



# PRAXISBEISPIEL



- Mittelständisches Unternehmen
- Verschlüsselt, Kontakt zum Hacker via Chat
- Forderung: 180.000€ via Banküberweisung
- Lösegeldsumme soll auf ein russisches Konto überwiesen werden

**= Macht & Demütigung**



# 66 %

Wahrscheinlichkeit betroffen zu sein





# 90 %

Nicht in der Lage nach dem Angriff weiterzuarbeiten



# 30 Tage

Durchschnittliche Ausfallzeit nach einem Angriff



# 252.000 €

Durchschnittlich gezahlte Lösegeldsumme



# 46 %

Bezahlt das geforderte Lösegeld



< 1 %

Aufklärungsquote



# Die Frage ist nicht **ob** sondern **wann**

Präventive Maßnahmen entscheiden, ob und wie schnell  
das Unternehmen wieder geschäftsfähig ist



# GESCHÄFTSFÜHRERHAFTUNG



# ALLGEMEINE BETRACHTUNG



- Rechtsform GmbH zum **Schutz** des Privatvermögens des Geschäftsführers
- **Latente Bedrohung** der persönlichen Haftung (gesellschaftsrechtlich / steuerrechtlich)
- **Schuldhaftes** Verhalten
- **Verletzung** der Pflichten
- Geschäftsführer muss im Interesse des Unternehmens handeln und **Gefahr abwenden**
- **Überwachung** der Finanzen, Datenschutz, Compliance, etc.





# CYBERSICHERHEIT ALS PFLICHT

NIS-2-Richtlinie (EU Vorgabe, 73 seitiges Dokument)

Dienstag, 6. Juni 2023    Newsletter   Podcasts   Club   ePaper   Archiv   Shop   Jobs   Inside    Login   Abo

**4 Wochen für 1€**  
29,99€  
Zum Angebot

**Handelsblatt**

MEINE NEWS | HOME   POLITIK   UNTERNEHMEN   TECHNOLOGIE   FINANZEN   MOBILITÄT   KARRIERE   ARTS & STYLE   MEINUNG   VIDEO   SERVICE

Börsenkurse ▾   Märkte ▾   Anlagestrategie ▾   Musterdepots   Banken + Versicherungen ▾   Geldpolitik   Immobilien ▾   Vorsorge ▾   Steuern + Recht ▾   Tools ▾

**EU-REGULIERUNG**

## Cybersicherheit als Pflicht

Ein Gesetzentwurf sieht vor, dass Manager haften, wenn sie Cyberrisiken nicht prüfen. Das kann Führungskräfte abschrecken – und war auf EU-Ebene nicht vorgesehen.

Eren Basar

29.05.2023 - 10:29 Uhr • [Kommentieren](#) • [6 x geteilt](#)



- **Ausweitung** von Pflichten
- **Anhebung** Bußgeldhöhe  
Mindestens 10 Mio. EUR / 2 % des weltweiten Jahresumsatzes
- **Verschärfung** der Haftung von Leitungsorganen
- Geschäftsführer müssen das Cyber-Risikomanagement **persönlich überwachen**
- **Übertragung** auf Dritte wird untersagt
- Geschäftsführung haftet persönlich für **Regressansprüche** und **Bußgeldforderungen**
- **Verzicht** wird ausgeschlossen



# KONSEQUENZEN



- Vollständiger/Teilweiser **Verlust** von Daten
- In Folge:
  - **Aufbewahrungspflichten** können nicht eingehalten werden können
  - **Geschäftsbetrieb** nicht weitergeführt werden kann
  - Tritt eine **Schädigung Dritter** ein
- Keine angemessenen **Vorkehrungsmaßnahmen**
- **Bei Insolvenz:** Hätte dieser Schaden abgewendet werden können?

# CYBERSECURITY VERSICHERUNG



- **Hohe Voraussetzungen** für Aufnahme
- Teilweise **ISO27001** als Voraussetzung
- **Deckung** nicht immer gewährleistet  
*Beispiel: Fehlverhalten Kunden/Partner*
- Teilweise **unbezahlbar** für KMU



# DATENSICHERUNG

DIE „LEBENSVERSICHERUNG“



**Wer sichert seine Daten?**

**Wie häufig wird gesichert?**

# WIE SICHERE ICH MEINE DATEN?



- In **regelmäßigen Abständen** (am besten täglich)
- Für einen Zeitraum von **mindestens 6 Monaten**
- **Tägliche Überprüfung**
- **Intervention** bei Störfällen
- **Physisch Trennung** zum Netzwerk / den Systemen
- **Außerhalb** der Geschäftsräume
- Regelmäßige **Wiederherstellungstests**





# DREI SÄULEN DER IT-SICHERHEIT



# IT-SICHERHEIT

## PRÄVENTION

- Hohe Sicherheitsstandards
- Mitarbeiter-sensibilisierung
- Frühzeitiges Erkennen und Melden

## DATEN-SICHERUNG

- Zuverlässige Datensicherung
- Tägliche Überwachung
- Integritätsprüfung
- Physische Trennung

## NOTFALL-PLAN

- Sofortmaßnahmen
- Kommunikation
- Wiederanlaufplan



WER IST EIGENTLICH...

**INVENTORY** 



- IT-Dienstleistungsunternehmen
- Sitz: Darmstadt-Griesheim
- Einsatz: Regional- / Bundesweit
- Kunden: Kleine und mittelständische Unternehmen
- Fokus: IT-Sicherheit
- Leistungen & Kosten: Transparent und skalierbar
- Baukastensystem

**„Externe IT-Abteilung“**

# DAS INVENTORY BAUKASTENSYSTEM



## RUFBEREIT-SCHAFT

- Servicezeiten: Montag bis Freitag 06:00-19:00 Uhr
- Servicezeiten: Montag bis Sonntag 00:00-24:00 Uhr
- Erbringung: Remote
- Abrechnung: Regulärer Stunden-Verrechnungssatz (15 Minuten Takt)
- Kein Zuschlag



## REAKTIONS-ZEIT

- Zugesicherte Reaktionszeit in den vereinbarten Servicezeiten
- Reaktionszeit: 12 Stunden
- Reaktionszeit: 6 Stunden
- Reaktionszeit: 4 Stunden
- Reaktionszeit: 2 Stunden
- Reaktionszeit: 1 Stunde



## CLIENT MANAGEMENT

- Einspielen von Betriebssystem Updates
- Ressourcen Monitoring
- Antiviren Schutz
- Überwachung der Aktualität des Virenschutzes & der Betriebssystem Updates
- Security Operations Center (SOC)
- Software Deployment



## SERVER MANAGEMENT

- Einspielen von Betriebssystem Updates
- Ressourcen Monitoring
- Antiviren Schutz
- Überwachung der Aktualität des Virenschutzes & der Betriebssystem Updates
- Security Operations Center (SOC)



## BACKUP MANAGEMENT

- Überwachung der Datensicherung an Werktagen (Mo-Fr)
- Intervention bei Störfällen



## INKLUSIV KONTINGENT

- Vorzugspreis von 110€/Stunde bei verbindlicher Abnahme
- Regulärer Stundensatz: 132€/Stunde



## ON-SITE DAYS

- Regelmäßige Erbringung von ganzen Tagen vor Ort

## BASIS PAKET

IT-Hotline / Ticketsystem

Servicezeiten: Montag bis Freitag 08:00-17:00 Uhr

Reaktionszeit: Next Business Day

Erbringung: Remote

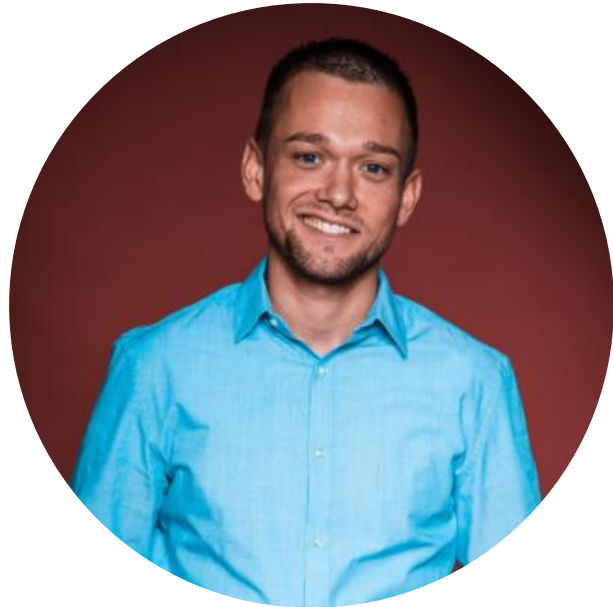


# KOSTENLOSER QUICK GUIDE

## Verhalten im Falle eines Cyberangriffs



E-Mail an [contact@inventory.de](mailto:contact@inventory.de)  
Betreff: Quick Guide



# MAURICE TELTSCHER

FOUNDER & CEO

**INVENTORY** 

INVENTORY GmbH  
Pfungstädter Str. 1  
64347 Griesheim

Phone: +49 6155 - 7043971  
Mobile: +49 151 - 22333903

Mail: [Maurice.Teltscher@inventory.de](mailto:Maurice.Teltscher@inventory.de)  
Web: [www.INVENTORY.de](http://www.INVENTORY.de)