

# Wie sicher ist ein Unternehmen?

Lukas Baumann · Gründer & CEO



**LocateRisk**  
MEASURE · COMPARE · OPTIMIZE IT SECURITY



# Angriffsziel deutsche Wirtschaft

Städtezeitung

Wie man nicht auf einen Cyberangriff reagiert

Spionage bei Adesso



Wegen Cyberattacke: Evotec verlässt MDax

5. Mai 2023 08:18



Der Pharma-Wirkstoffforscher Evotec aus Hamburg muss wegen nicht fristgerechter Veröffentlichung des testierten Geschäftsberichts den MDax verlassen.

SPIEGEL.net

Deutschlands größter Rüstungskonzern

### Cyberangriff auf Rheinmetall

Militärfahrzeuge, Munition – Rheinmetall gehört zu den Profiteuren des Ukrainekriegs. Nun ist das zivile Geschäft des Unternehmens Opfer von Hackern geworden. Nach SPIEGEL-Informationen laufen bereits Ermittlungen.



CSO DEUTSCHLAND

### DEUTSCHER STAHLPRODUZENT GEHACKT

## Cyberattacke auf Badische Stahlwerke

Das Netzwerk der Badischen Stahlwerke ist offenbar gehackt worden. Das Unternehmen hat die betroffenen Systeme abgeschaltet.

Von Julia Mutzbauer  
CSO | 24. APRIL 2023 16:20 UHR



Die Badischen Stahlwerke (BSW) sind von einem Cyberangriff betroffen.

heise online

### Cyberattacke auf KFC, Pizza Hut und Taco Bell

Während eines IT-Sicherheitsvorfalls bei Yum! Brands konnten Angreifer auf Interna zugreifen. Persönliche Kundendaten sollen aber nicht betroffen sein.

Lesezeit: 1 Min. In Pocket speichern



NDR

### Cyber-Attacke: "Ich hätte nicht gedacht, dass es so krass ist!"

Stand: 02.02.2023 05:00 Uhr

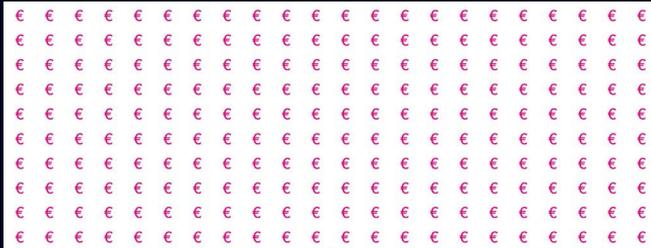
Das Handwerksunternehmen PLA aus Kaltenkirchen wird Opfer eines Hackerangriffs. Was folgt, ähnelt einer Geiselnahme - einer Daten-Geiselnahme: ein Erpressers Schreiben, Polizei-Forensiker, Gespräche mit dem Hacker, ein Rabattangebot und Existenzängste.



# Angriffsziel deutsche Wirtschaft

## Cyberangriffe

> 220 Milliarden Euro Schaden pro Jahr.



## Kriegsfolgen Ukraine-Krieg

Deutschland 2022 ~ 100 Milliarden Euro.



Quellen:

Studie des Digitalverbands Bitkom · Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro.

Deutsches Institut für Wirtschaftsforschung (DIW) · WirtschaftsWoche 20. Februar 2023

# Gefahr erkannt?

Forsa-Umfrage 2022 im Auftrag des GDV

Ich erwarte im Zuge des Ukraine-Krieges mehr Cyberangriffe ...

... auf deutsche Unternehmen.

**60%**

... auf mein Unternehmen.

**16%**

# Gesammelte Statistikdaten zur IT-Sicherheitslage von 3.609 Organisationen



- Datenbanksysteme gefunden
- Keine Datenbanksysteme gefunden

## 44%

schützen nicht alle Datenbanksysteme angemessen vor Cyberangriffen

Erleichtert Zugang zu weiteren Systemen und sensiblen Daten



- Teilweise ungeschützter E-Mail-Versand
- Geschützter E-Mail-Versand

## 53%

versenden E-Mails teilweise ungeschützt

Erleichtert Spam- und Phishing-Attacken durch Mail-Fälschung



- Unzulässige Transportverschlüsselungen
- Verwenden aktuelle Verfahren

## 90%

erlauben die Datenübertragung mit veralteter Transportverschlüsselung

Vereinfacht Datendiebstahl



- mind. 1 App mit kritischer ungepatchter Sicherheitslücke
- Alle Applikationen gepatcht

## 43%

haben mindestens eine Applikation mit kritischer ungepatchter Sicherheitslücke

Öffnet Tür und Tor für Angreifer



- Verwenden Tracking-Cookies ohne Nutzererlaubnis
- Verwenden keine Cookies ohne Nutzererlaubnis

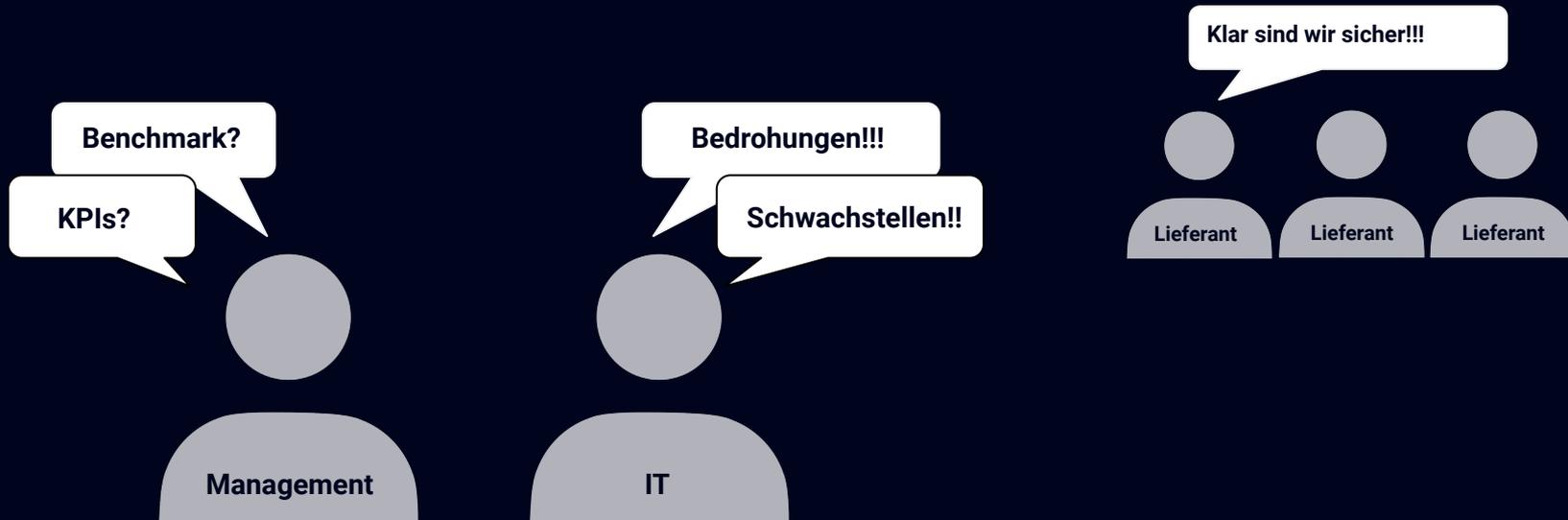
## 35%

verwenden Tracking-Cookies ohne Nutzererlaubnis

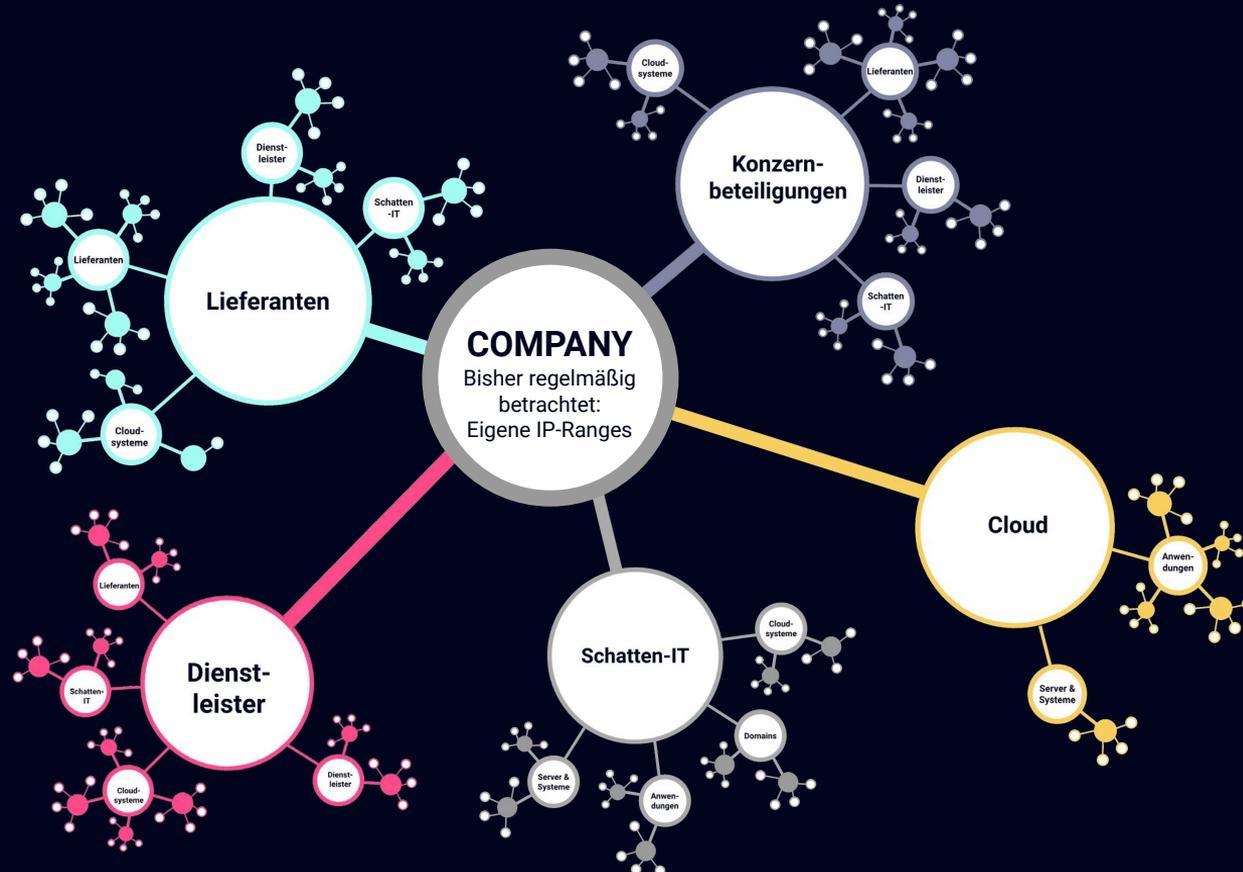
Abmahnungen und Bußgelder drohen

# Warum spricht niemand über dieses Problem?

Management und IT haben keine gemeinsame Basis für die Bewertung der unternehmensweiten IT-Sicherheitssituation



# Die IT-Angriffsfläche wird unüberschaubar



## Was wir so alles finden ...

Ladestation in kommunaler IT. Niemand wusste, woher sie kommt, wem sie gehört, wo sie steht.

Ü-Kamera, die aus Werkshalle eines Sportwagenherstellers Prototypen-Bilder ins Netz streamt.

Webshop02.unternehmen.de mit Fehlermeldung, die Passwort für Mail-Server beinhaltet.

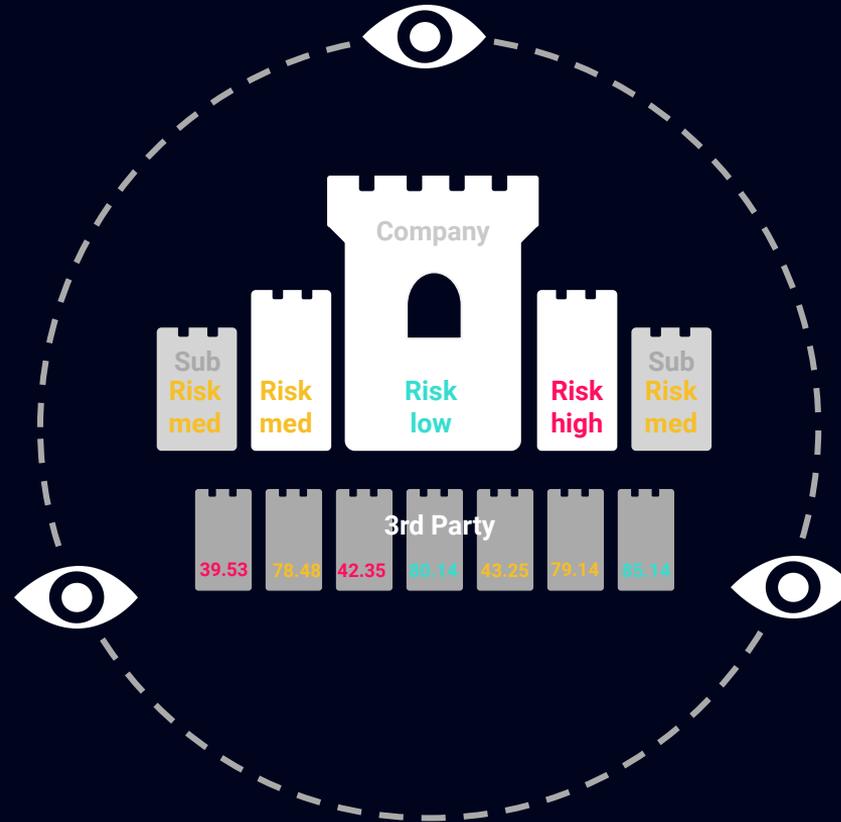
GIT-Verzeichnisse mit Passwörtern für alles Mögliche.

System-Backups für jeden zum Download.

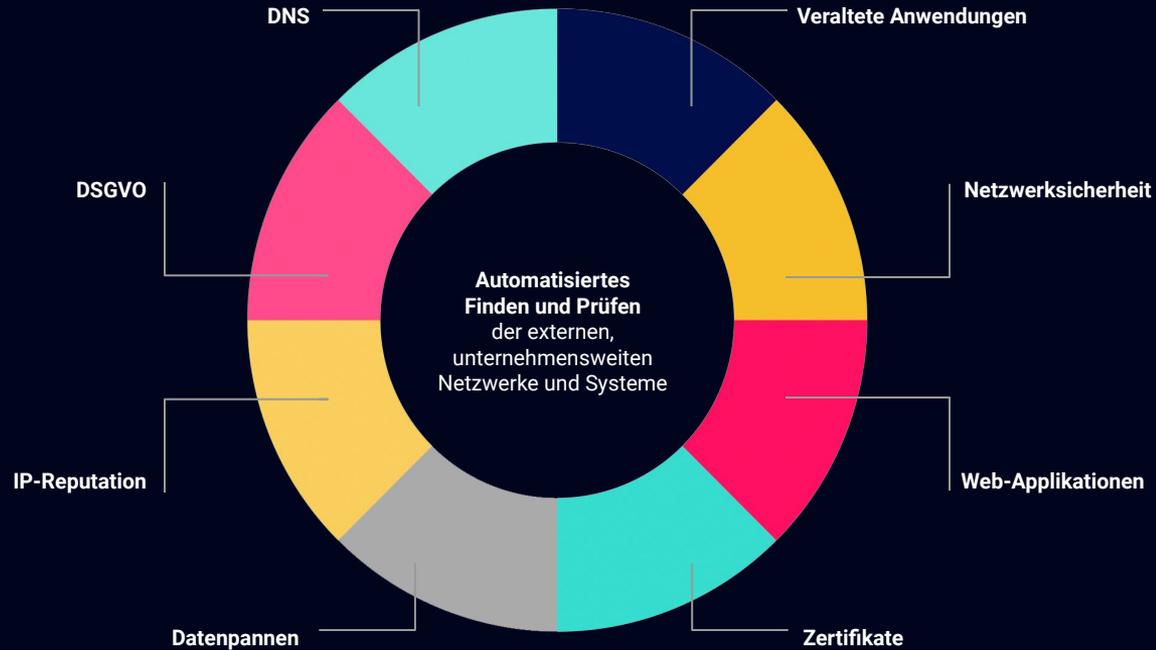
Payment-Verwaltungssystem eines Onlineshops war internetweit einseh- und manipulierbar.



# Automatisierte SaaS-Lösung für mehr Cybersicherheit



# Was genau wird geprüft?



# Ergebnis: Auditierte IT-Sicherheit als Nachweis gegenüber Dritten + Geschäftspartner-Risikomanagement



+



## Vorteile fürs eigene Unternehmen



### Präventiv statt Reaktiv / Cyber-Hygiene

Angriffsfläche kontinuierlich  
und effizient minimieren.



### Zeitersparnis

Automatische Asset-Erkennung +  
Funktionen, die den Sicherungsprozess  
beschleunigen.



### NIS2, DORA & TISAX ready

Messung der Effektivität von  
Informationssicherheit +  
Lieferkette automatisiert auditieren.

## Fundierte Datenbasis

**> 4 Mio**  
Server gemessen



**> 14 Mio**  
Handlungsempfehlungen

**> 50.000**  
Unternehmen verglichen

# Referenzen



+ 13 weitere Städte  
 + 5 Landkreise  
 + 10 Versorgungsunternehmen  
 + mehr als 500 andere



Erwähnt in FAZ, Manager Magazin, Stern, Süddeutsche Zeitung, Zeit, Heise, FFH...

## Auszeichnungen & Nominierungen

1. Preis beim Insurathon der Sparkassenversicherung
3. Preis im Accelerator-Programm für Cybersecurity-Startups "SpeedUpSecure"



Nominiert von der internationalen Expertenorganisation DEKRA

# NIS2 Ready

Unterstützt bei der Umsetzung der NIS2-Mindestanforderungen hinsichtlich:

- Analyse und Bewertung von IT-Sicherheitsrisiken
- Gewährleistung von Sicherheit bei Beschaffung
- Gewährleistung von Kontrollen der Sicherheitsanforderungen von Lieferanten in der Lieferkette

Derzeit ist keine Umsetzungsfrist vorgesehen. Heißt: auch für wichtige Einrichtungen gilt die Umsetzung des Gesetzes sofort nach Inkrafttreten, voraussichtlich zum 17. Oktober 2024.

# Wie ist Ihr Sicherheitsstatus?

Gewinnen Sie einen Einblick  
anhand Ihrer echten Daten!

[LB@LocateRisk.com](mailto:LB@LocateRisk.com)  
06151 6290246

