HORN & COMPANY

Cyber-Attacken! Bedrohungen und deren Berücksichtigung in Sanierungsgutachten

Zunehmende Gefahren für Unternehmen aller Branchen

Düsseldorf, November 2022

Cyber-Attacken – eine zunehmende Gefahr für Unternehmen aller Branchen

Ausgewählte Kennzahlen zu Cyber-Attacken in Deutschland

46% der **mittelgroßen/großen Unternehmen** wurden in **2021** mindestens ein Mal Opfer einer Cyber-Attacke

Im Jahr 2020 dauerte es durchschnittlich **207 Tage**, um **Cybersicherheitsverletzungen** in Unternehmen **zu erkennen**

Cyber-Attacken verursachen Schäden in **Milliardenhöhe** – die **Tendenz** ist weiter **steigend**

Die **Anzahl erfasster Cyberstraftaten** steigt weiter an – im Jahr 2021 um über **12%**. Die **Aufklärungsquote** liegt knapp **unter 30%**

85% der Cybersicherheits-verletzungen werden **durch menschliches Versagen** verursacht

87% der Unternehmen schätzen das **Risiko**, Opfer eines Ransomware-Angriffes zu werden, als **hoch oder sehr hoch** ein

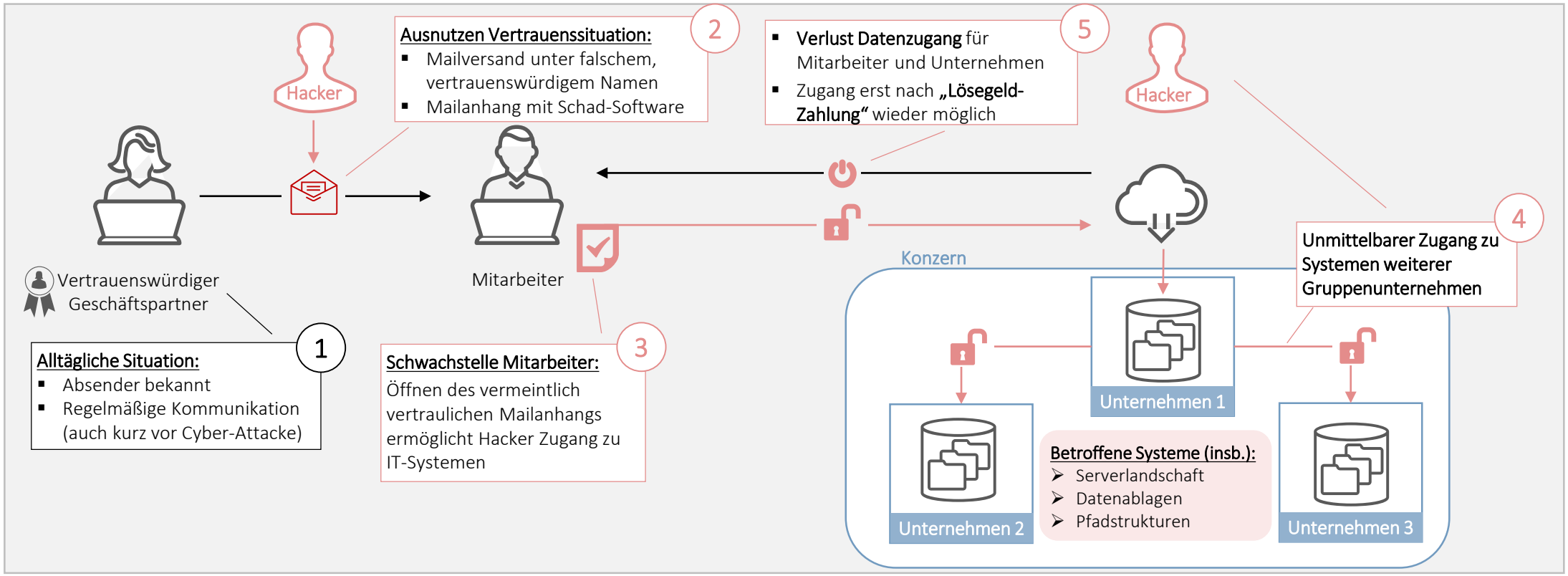
Umfang & Qualität der angebotenen **Tools und Dienstleistungen** für Cyber-Attacken **nehmen stark zu**. Zudem **sinken Eintrittsbarrieren**

Bedrohungen durch Ransomware sind 2021 **deutlich angestiegen** – diese Attacken haben das **höchste Schadenspotenzial**

Quelle: BKA, Statista

Aus unserer Praxis: Mandant wurde Opfer einer Cyber-Attacke mit Millionenschaden

Vorgehen & Angriffspunkte (schematische Darstellung)



Aus unserer Praxis: Mandant wurde Opfer einer Cyber-Attacke mit Millionenschaden

Wesentliche Erkenntnisse

Beobachtete Ungewissheiten bei Cyber-Attacke

- Welche **Systeme und Daten** (Kunden, Unternehmen, etc.) sind betroffen?
- Sind **leistungswirtschaftliche Prozesse** (Verkauf, Produktion) betroffen?
- Kann der **Zahlungsverkehr** weiterhin abgewickelt werden?
- **Wer ist der Hacker**? Mit wem ist zu verhandeln?
- Sind die **Aussage der Hacker** zur „Wieder-Bereitstellung“ **glaubhaft**?
- Wie hoch ist die **Höhe des Lösegeldes**? **Wie wird es bezahlt werden**?
- Sind die (noch) aufrufbaren **Dokumente und Dateien echt**?

Erkenntnisse aus der Praxis

- **Ca. 2 Wochen für Verhandlungen / Zugang zu Daten**
- **Ca 5-6 Monate: Wiederherstellung betroffener Systeme**
- **Lösegeld: Millionen-Betrag;** Bezahlung in Kryptowährung im Darknet
- **Einbindung BKA:** Verhandlungen und Bezahlung im Darknet (**Achtung!: Geldwäsche, Terrorismusfinanzierung**)

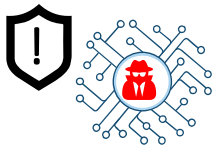
Bewertung der Risiken durch Cyber-Attacken mittels „3-Punkte-Check“

Prüfbereiche und Zielsetzungen

I. Allgemeines Sicherheitsmanagement

- **Commitment der Geschäftsführung**
- Klare **strategische/konzeptionelle Vorgaben** definieren
- **Durchsetzbarkeit von Sicherheits-maßnahmen** sicherstellen
- **Fehlinvestitionen vermeiden**
- Zielgerichtetes **Ressourcenmanagement** betreiben
- …

II. Personelle & organisatorische Aspekte



- Gefährdungen durch die **Schwachstelle „Mensch“** abwehren: Malware, Drive-By-Downloads, Ransomware, Botnetze (DDoS-Angriffe), USB-/IoT-Geräte etc.
- Alle Mitarbeiter für das Thema „Cyber-Sicherheit“ sensibilisieren
- **Zutritts-, Zugangs- und Zugriffsrechte** konsequent und restriktiv verwalten
- **IT-Sicherheitskonzept** für angemessenes Sicherheitsniveau erarbeiten
- **IT-Notfallplan** nach Risikoanalyse erstellen und kommunizieren
- …

III. Technische Aspekte

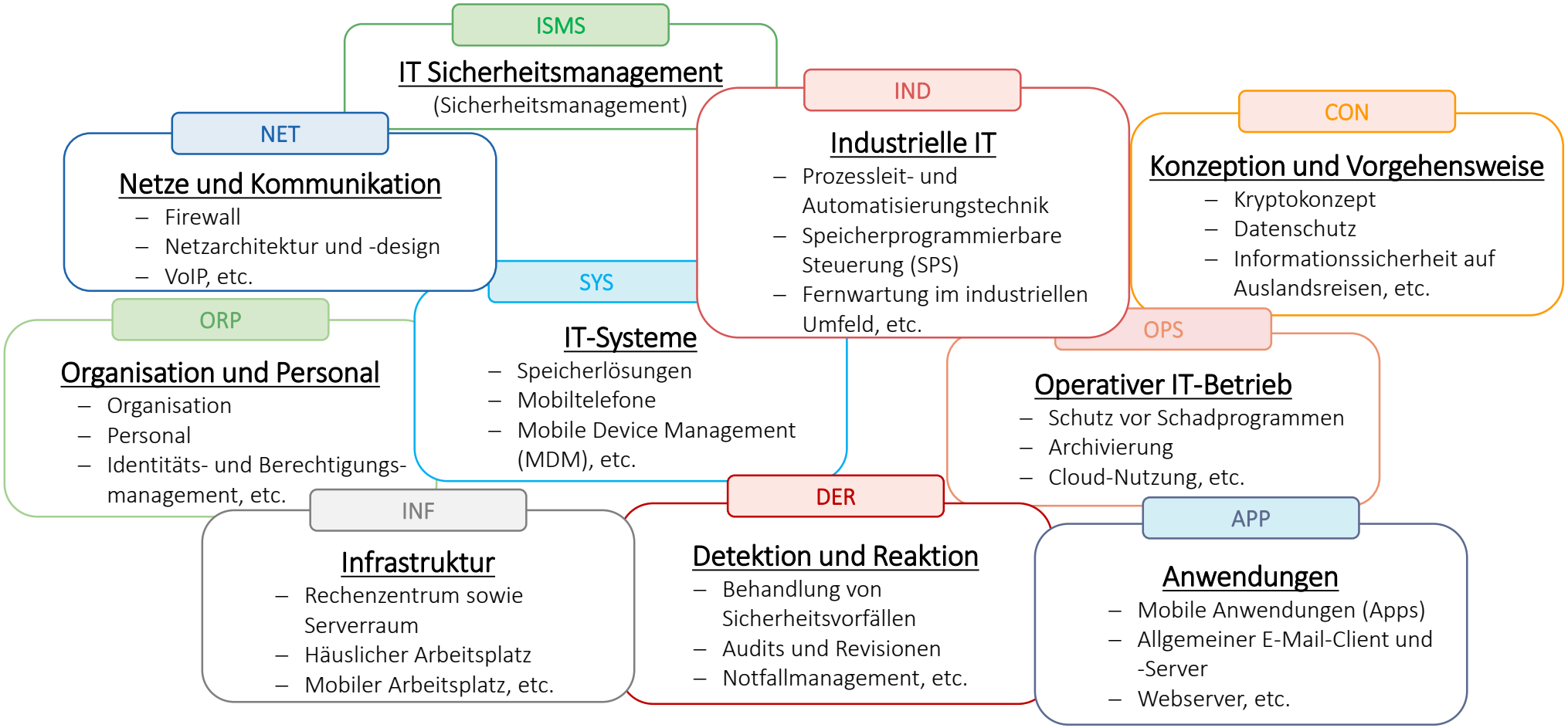
Daten und Netzwerke in allen digitalen Bereichen und Prozessen schützen:

- Zugelassene Hardware/Software einsetzen
- Datensicherungskonzept erstellen und leben
- Alle Schnittstellen mit Verbindung in den IT-Verbund schützen
- …

Risiko-Assessment mittels Checklisten-Logik

Im Fokus: IT-Grundschutzbausteine und Schutzbedarfe

Übersicht



Assessment Cyber-Security entlang der relevanten Grundschutzbausteine und der jeweiligen Schutzbedarfe (B – Basis -> S – Standard -> H – Hoch)

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Ansätze zur Berücksichtigung von Cyber-Attacken in Sanierungsgutachten

Zentrale Fragestellungen und Berücksichtigung in der Sanierungsplanung

Zentrale Fragestellungen

1. Wird die Gesamtverantwortung für die Informationssicherheit vom Top-Management übernommen („Chefsache“)?
2. Wird die Belegschaft für „Cyber-Risiken“ sensibilisiert und entsprechend geschult?
3. Existiert ein dokumentiertes IT-Sicherheits-konzept mit angemessenem/ausreichendem Sicherheitsniveau?
4. Existiert ein IT-Notfallplan, basierend auf einer vorherigen Risikoanalyse?
5. Werden alle Bereiche und Schnittstellen der IT-Landschaft ausreichend geschützt?
6. Liegen ISO/IEC 2700x-Zertifizierungen vor?
7. Welche Risiken werden durch Versicherungen abgedeckt?

Berücksichtigung in Sanierungsgutachten

1. <u>Risikoquantifizierung von Schadensereignissen durch:</u>
   a. Identifizierung potenzieller Bedrohungen
   b. Prognose jeweiliger Eintrittswahrscheinlichkeiten:
      Ansatz zur Klassifizierung: selten, mittel, häufig, sehr häufig -> *Gewichtung möglicher Bedrohungen*
   c. Schätzung des Schadenspotenzials bei tatsächlichem Eintritt
      - Ansatz zur Klassifizierung: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend
      - Fokus: Bedrohungen mit materiellen Schadenshöhen
2. <u>Plausibilisierungsmöglichkeiten (zentrale Fragestellungen):</u>
   a. Korrespondiert die vorgenommene Risikoquantifizierung mit den Investitionen in Cyber-Sicherheit und benötigten Kapazitäten (Technologie, Personal)?
   b. Stimmt die Risikoquantifizierung mit der vom Unternehmen angegebenen Risikoaversion bzgl. Cyber-Security überein?

Ihre Ansprechpartner für Finanzierungs- und Restrukturierungsbegleitungen

Horn & Company Top-Management Beratung

Dr. Michael Lukarsch
Managing Partner

Johannes Dachlauer
Manager

Erfahrung	▪ Roland Berger (Partner) ▪ AVI Packaging (CEO) ▪ HOYER Logistics (CRO/CFO) ▪ Droege & Comp. (Associate Partner)	▪ UniCredit (Restrukturierungsspezialist) ▪ PricewaterhouseCoopers ▪ Helaba
Schwerpunkte	▪ Strategic turnaround programs, restructuring and refinancing ▪ Overhead optimization ▪ End-2-End process optimization	▪ Restructuring ▪ German Restructuring Opinions ▪ Financial Structuring ▪ Liquidity Projections
Kontakt	✉ michael.lukarsch@horn-company.de +49 162 27 26 004	✉ johannes.dachlauer@horn-company.de +49 162 27 26 079

HORN & COMPANY

Internationale Top-Management-Beratung

DÜSSELDORF | BERLIN | FRANKFURT | HAMBURG | KÖLN | MÜNCHEN | NEW YORK | SINGAPUR | WIEN