PASSION4IT

# PARTNERPROGRAMM BARTHHAAS
# THEMA DIGITALISIERUNG

RISIKOMANAGEMENT (CYBER SECURITY)

FLORIAN LAUMER – PASSION4IT

# AGENDA

Risikomanagement (Cyber Security)

01 Wer bin ich

02 Wer ist die PASSION4IT

03 Aktuelle Risikolage

04 Wie stehts um den Hopfen

05 Welche Risiken gibt es

06 NIS2

07 (NIS2) GAP-Analyse / Risikomanagement

08 Summary

# FLORIAN LAUMER

PASSION4IT


+49 151 11676 502

florian.laumer@passion4it.de

https://www.linkedin.com/in/florianlaumer/

www.passion4it.de

- ✓ 25 Jahre Leidenschaft für IT, Digitalisierung, digitale Transformation und Innovation
- ✓ Hands On Mentalität
- ✓ ITQ-Auditor (Informationssicherheit)
- ✓ LEAD Digital Transformation Analyst (LEADing Practice)
- ✓ Certified SAFe 6 Agilist
- ✓ ICO ISMS Security Officer according to ISO/IEC 27001:2022
- ✓ CISM Cyber Security Experte

SA SAFe 6

LEADing Practice · LEAD Digital Transformation Analyst · Global University Alliance

ICO-CERT International Certification Organization

Zertifizierter Auditor für IT-Sicherheit ITQ Institut für Technologiequalität

CISM Certified Information Security Manager. An ISACA® Certification

# 02

# WER IST DIE PASSION4IT

# ZAHLEN, DATEN, FAKTEN

**2019**
Gegründet

**8**
Digitale Bergführer

**70+**
Kunden D-A-CH

**3,8**
Millionen € Umsatz

**1%**
Vom Umsatz an den Umweltschutz

# ÜBERZEUGUNG. VERTRAUEN. STOLZ.

PASSION4IT

Diese Kunden vertrauen uns!

# 03

# AKTUELLE RISIKOLAGE

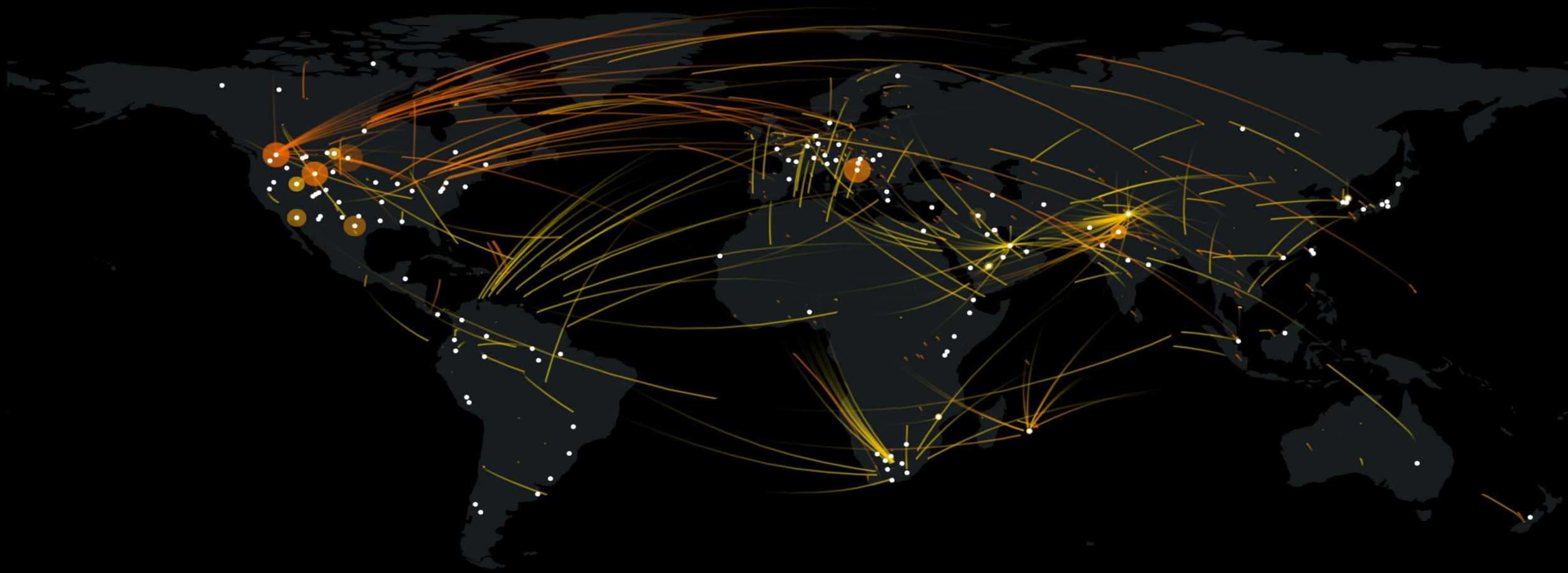
# NETSCOUT Omnis® Threat Horizon

Real-Time DDoS Attack Map

February 7, 2023

06:50:46 (UTC -1hr)

Showing 186 DDoS events



Download Our Threat Report | DDoS Solutions

RECENT ATTACKS

ation ▲ 500 Mbps ▲ 47.7 kpps

Login or Sign Up for free now to access this feature

Login or Sign Up for free now to access this feature

Papua New Guinea | 83.4 Mbps ▲ 174 kpps

All Other Travel Arrangement and Reservation Services ▲ 16.2 Gbps | 1.43 Mpps

Inland Water Freight Transporta

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 February 7, 2023

# Heutzutage meldet sich bei Ihnen kein

# Nigerianischer Prinz ...

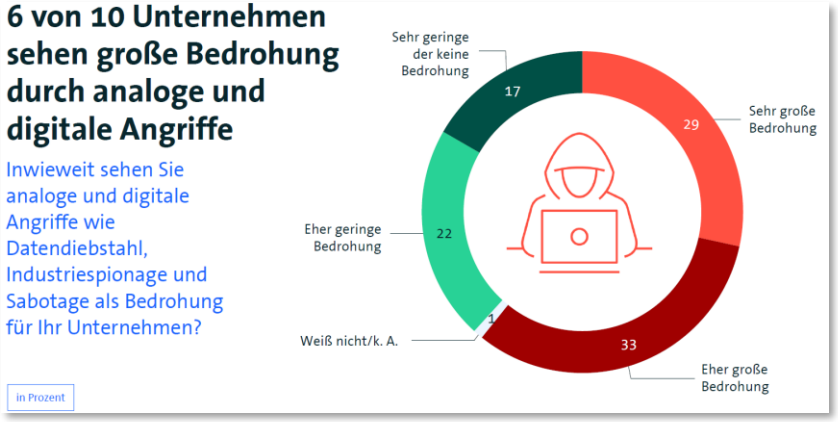
Heutzutage meldet sich bei Ihnen kein

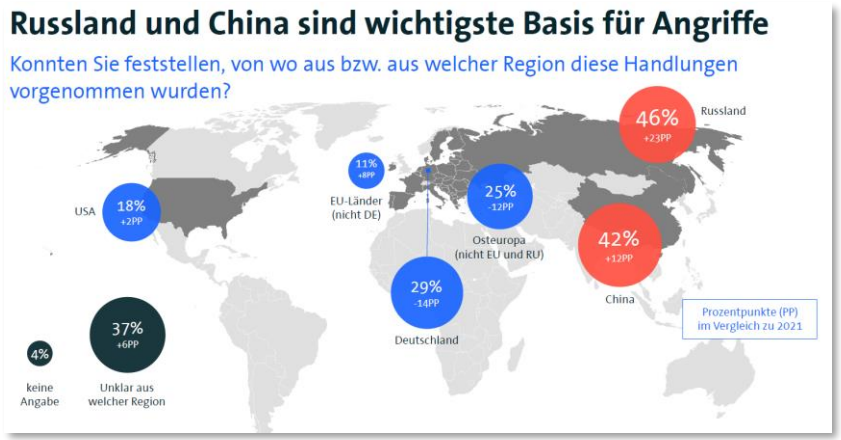
Nigerianischer Prinz ...

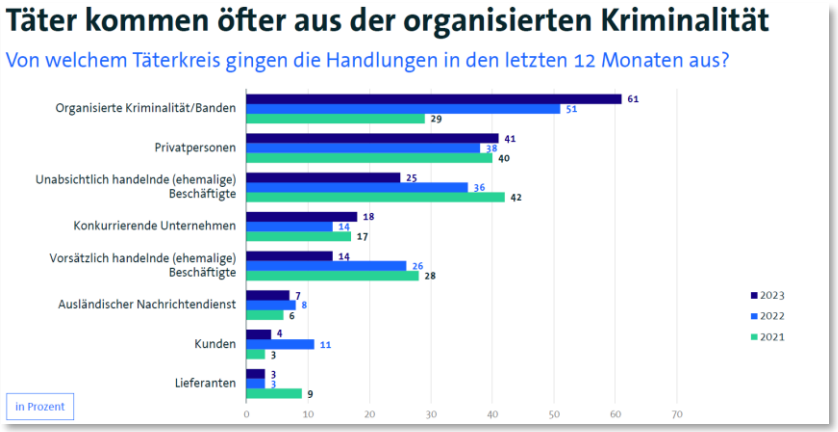
.... sondern ein Social Engineer!

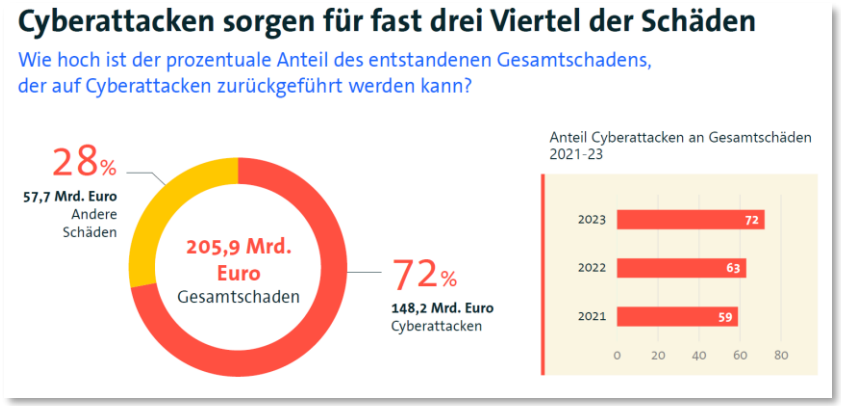

# DIE LAGE IM ÜBERBLICK

BITKOM Wirtschaftsschutz 2022




https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

# 82% der deutschen Unternehmen halten IT-Sicherheitsvorfälle geheim

## Mehrheit der Unternehmen verschweigt IT-Sicherheitsvorfälle

Redaktion / rh, 5.11.2023, 10:31 Uhr


**TÜV-Verband: 82 Prozent der deutschen Unternehmen, die in den vergangenen 12 Monaten IT-Sicherheitsvorfall zu verzeichnen hatten, hielten diesen geheim.**

Mehrheit der Unternehmen verschweigt IT-Sicherheitsvorfälle - silicon.de

# 04

# WIE STEHTS UM DEN HOPFEN

## Cyberangriff auf Duvel: Belgische Brauerei muss Produktion stoppen

Nach einem Cyberangriff auf die belgische Brauerei "Duvel" muss die Produktion gestoppt werden.

20


Während die Ransomware-Gruppe "Stormous" angibt, den Angriff auf die belgische Brauerei begangen zu haben, wird schon diskutiert, welches Bier als kritische Infrastruktur gilt.
(Bild: Radiokafka/Shutterstock.com)

**07.03.2024, 15:35 Uhr  Lesezeit: 1 Min.**

RUGENBRÄU
INTERLAKEN

Versicherungen & Vorsorge › Angebote für Unternehmen › Ratgeber › So erlebte die Brauerei Rugenbräu den Cyberangriff

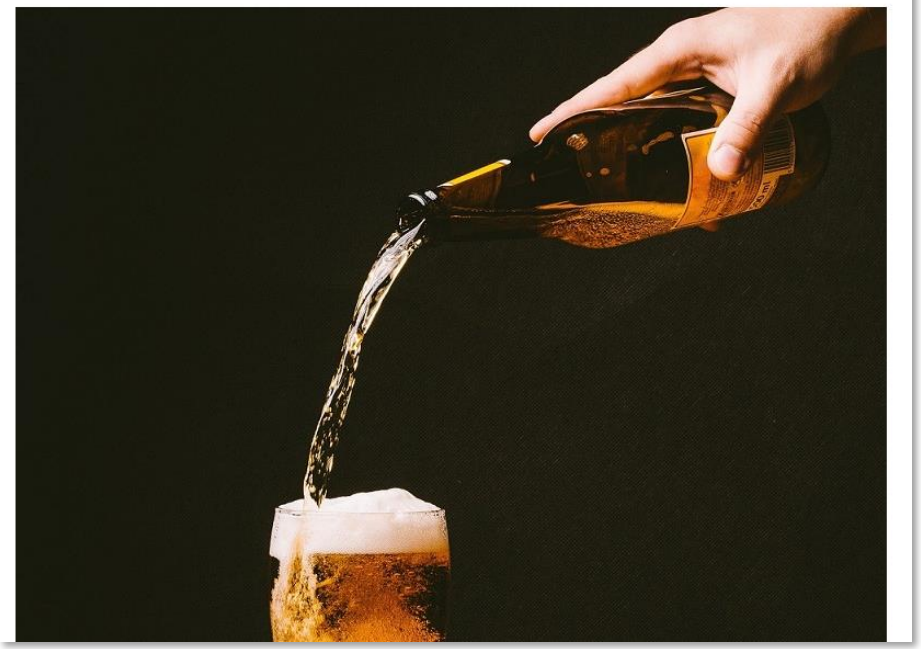
## So erlebte die Brauerei Rugenbräu den Cyberangriff

**Aus dem Alltag gerissen: Nach einem Hackerangriff auf ihren IT-Dienstleister geht nichts mehr. E-Mail-Server, Buchhaltung, Drucker und Zeiterfassung; das gesamte Netzwerk ist betroffen. Die Brauerei Rugenbräu AG aktiviert daraufhin Notfallmassnahmen.**

«In kurzer Zeit fühlte ich mich zurück in die 90er-Jahre versetzt». Damit beschreibt Remo Kobluk, CEO der Rugenbräu AG, den Hackerangriff auf einen vertraglich verbundenen IT-Dienstleister. Zusammen mit Christian Schneiter, dem Leiter Finanzen & Human Resources, steht Remo Kobluk vor lahmgelegten Computersystemen.  «An diesem Tag ging nur noch die Arbeit mit Stift und Papier», blickt Remo Kobluk zurück. Nicht einmal das Telefon funktioniert, denn auch dieses ist netzabhängig.

## Hacker hindern Hopfen: Spaniens zweitgrößte Brauerei lahmgelegt

16. November 2021 Kommentar hinterlassen



IT-SEC

# Cyberangriff legt Australiens größte Brauerei lahm

Lion warnt vor vorübergehenden Engpässen

12. Juni 2020, 15:57

In Australien hat ein Cyberangriff die größte Brauerei des Landes lahmgelegt – gerade, während die Wirtshäuser und Restaurants wieder aufmachen. Der Konzern Lion mit Marken wie XXXX Gold, Tooheys, Hahn oder Little Creatures teilte am Freitag mit, er sei Opfer einer Ransomware-Attacke.

# Russischen Brauereien droht Hopfen-Engpass

Russische Brauereien brauchen aktuell mehr vom dem Rohstoff. 98 Prozent des russischen Hopfens wird importiert.

08.04.22, 12:05

# Lieferkettenangriffe

Sydney, Melbourne, Brisbane

## Australische Häfen nach mutmaßlichem Hackerangriff weiter blockiert

Am Freitag hatte der Hafenbetreiber DP World "unbefugte Zugriffe" auf die Internetverbindung einiger Häfen Australiens gemeldet. Die Störung könne noch Tage dauern.

Aktualisiert am 12. November 2023, 12:05 Uhr / Quelle: ZEIT ONLINE, AFP, mmh / 9 Kommentare

Artikel hören



*Laut DP World kam es in den Hafenstädten Sydney, Melbourne, Brisbane und Fremantle zu Störungen im Betrieb. © James Ross/AAP/dpa*

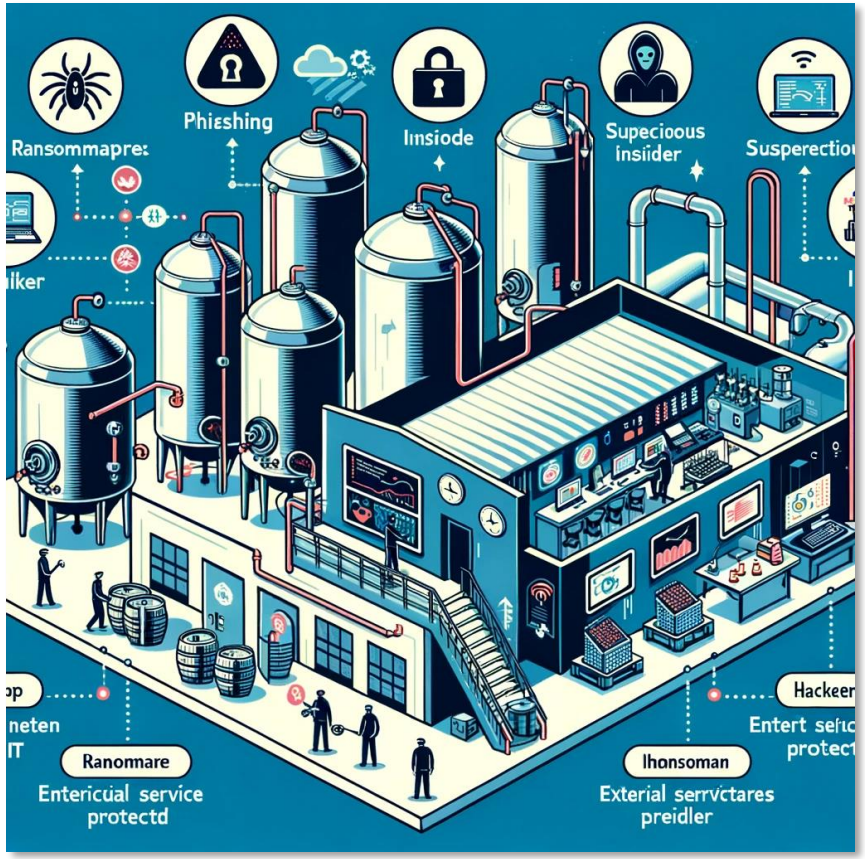
# 05

# WELCHE RISIKEN GIBT ES?

# IT RISIKEN

Informationstechnologie

- **Phishing & Social Engineering**: Mitarbeiter könnten auf gefälschte E-Mails oder Nachrichten hereinfallen
- **Ransomware**: Cyberkriminelle können IT-Systeme verschlüsseln
- **Schwachstellen in Software**: Veraltete oder unsichere Software



# OT RISIKEN

Operative Technologie

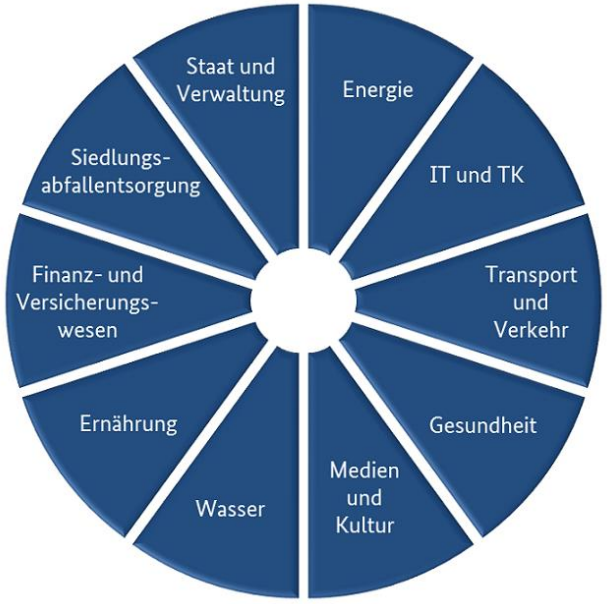
- **Sabotage & Manipulation:** Produktionsanlagen könnten manipuliert oder absichtlich gestört werden
- **Veraltete Technologie:** Viele OT-Systeme basieren auf älteren Betriebssystemen
- **Netzwerksegmentierung:** Wenn OT-Systeme nicht richtig vom Unternehmensnetzwerk isoliert sind
- **IoT-Sicherheitslücken:** Vernetzte Geräte in der Produktion (IoT)
- **Externe Dienstleister:** Fremdfirmen, die Zugang zu OT-Systemen


# 06

## NIS2

# NIS-2

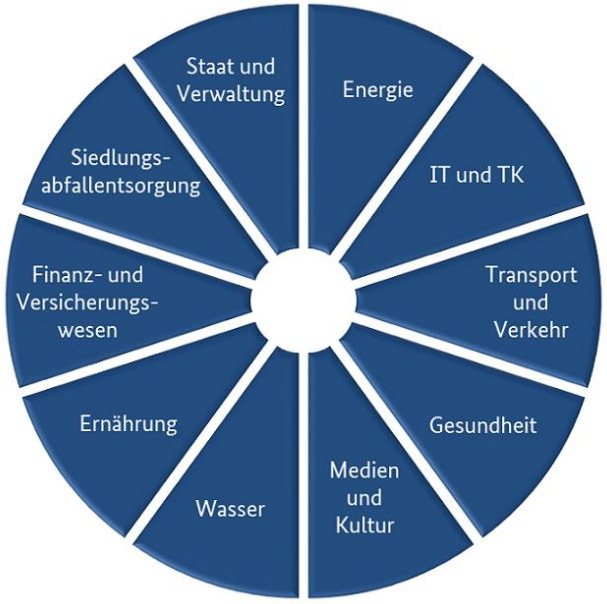
Network Information Security - 2




**Die EU NIS2-Richtlinie (Netz- und Informationssicherheit) der EU zielt darauf ab, die Cybersicherheit und Widerstandsfähigkeit kritischer Infrastrukturen zu stärken, indem sie strengere Anforderungen an Risikomanagement und Meldepflichten für Cybervorfälle einführt.**

# NIS-2

Network Information Security - 2




- Im Bereich Lebensmittel- und Getränkeherstellung müssen die Hersteller einen gewissen Schwellenwert überschreiten: **Dieser liegt etwa bei 350 Mio Liter Getränke**.
- Die Meldepflicht liegt dabei bei den Versorgern selbst
- Zudem müssen die betroffenen Betriebe Prozesse zur IT-Sicherheit, zum Risikomanagement und zur Angriffserkennung implementieren.

# NIS-2

## Network Information Security - 2

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Sicherheit in der Entwicklung, Beschaffung und Wartung
- Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- Schulungen Cybersicherheit und Cyberhygiene
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation

# 07

# (NIS2) GAP-ANALYSE / RISIKOMANAGEMENT

# NIS2 GAP ANALYSE

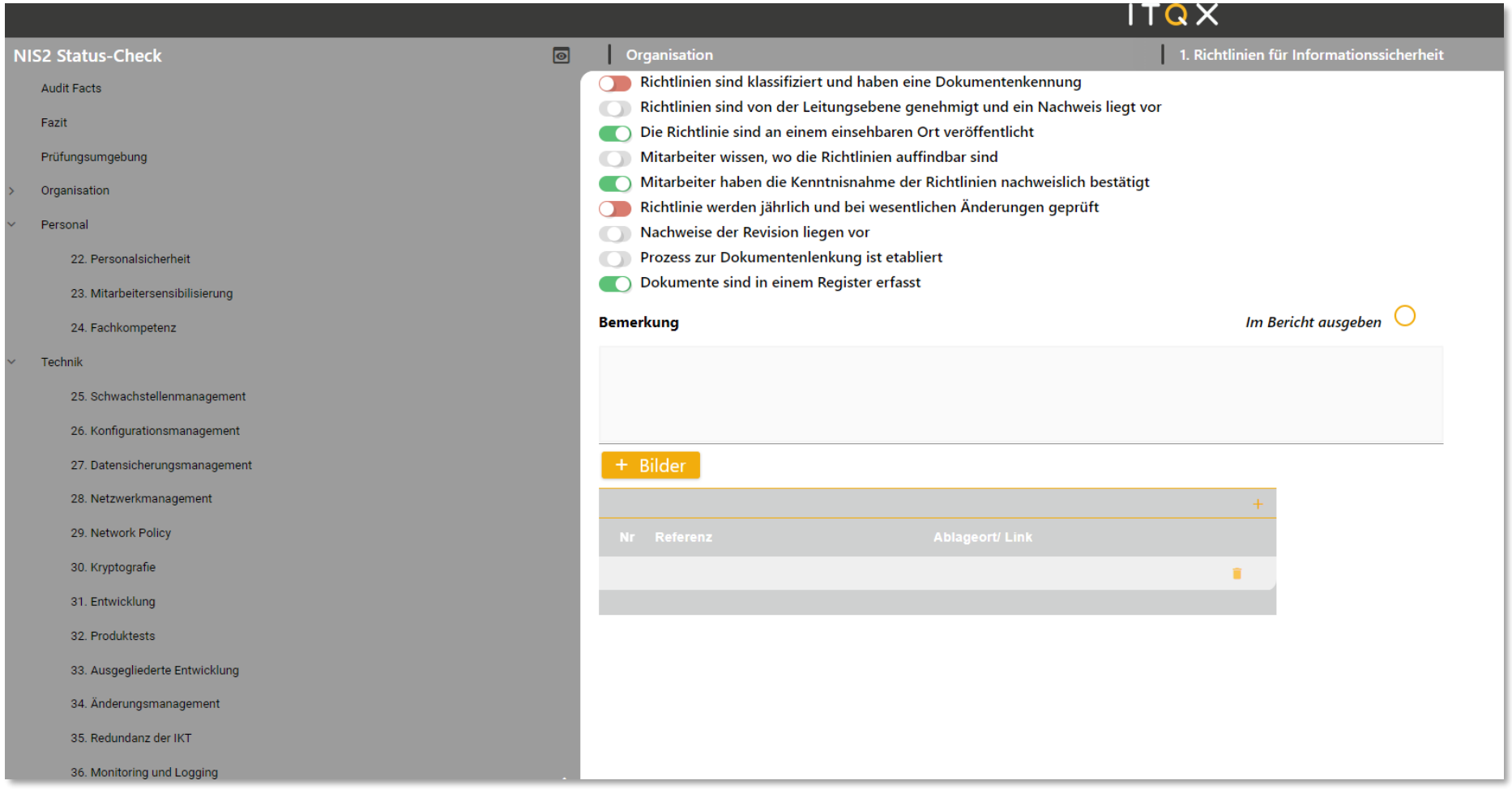
PASSION4IT

Der Ideale Einstieg in die IT-Sicherheit basierend auf dem BSI-IT Grundschutz und der ISO-270001

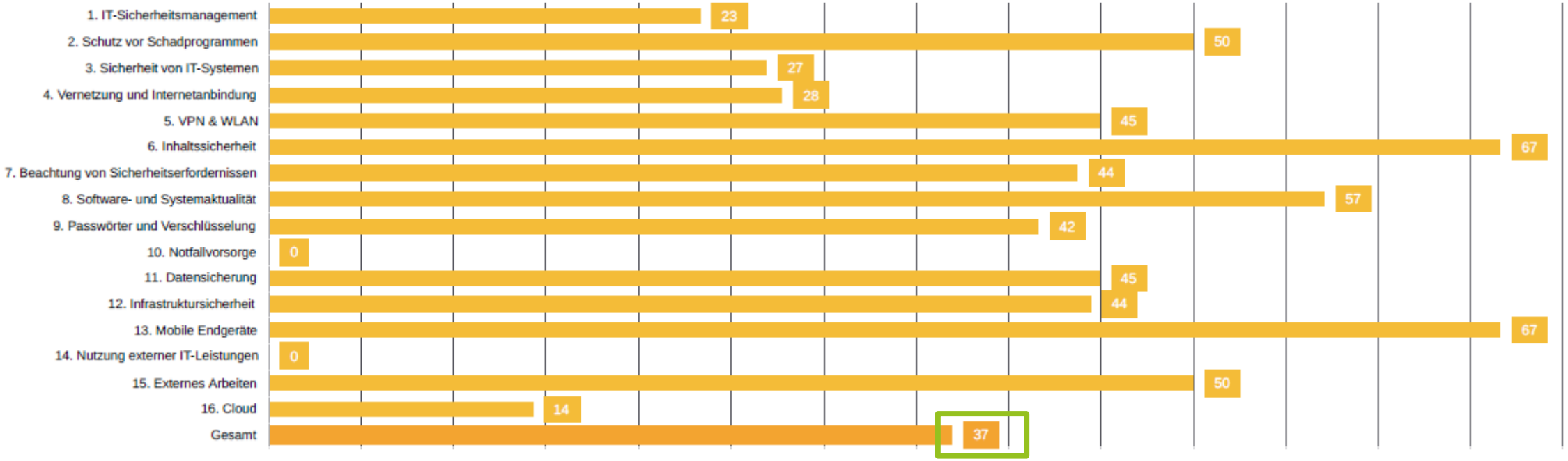
- 260 Fragen aus 32 Prüfgruppen
- Prüfung der technischen, menschlichen und organisatorischen Schutzmaßnahmen
- Ausführlicher Bericht mit Abschlusspräsentation
- konkrete und Maßnahmenempfehlungen
- Gemeinsame Priorisierung der Maßnahmen
- Vergleichender Benchmark aus über 1550 durchgeführten Audits

# NIS-2 GAP ANALYSE

Professionelle Portallösung (SaaS) für PASSION4IT und Kunden

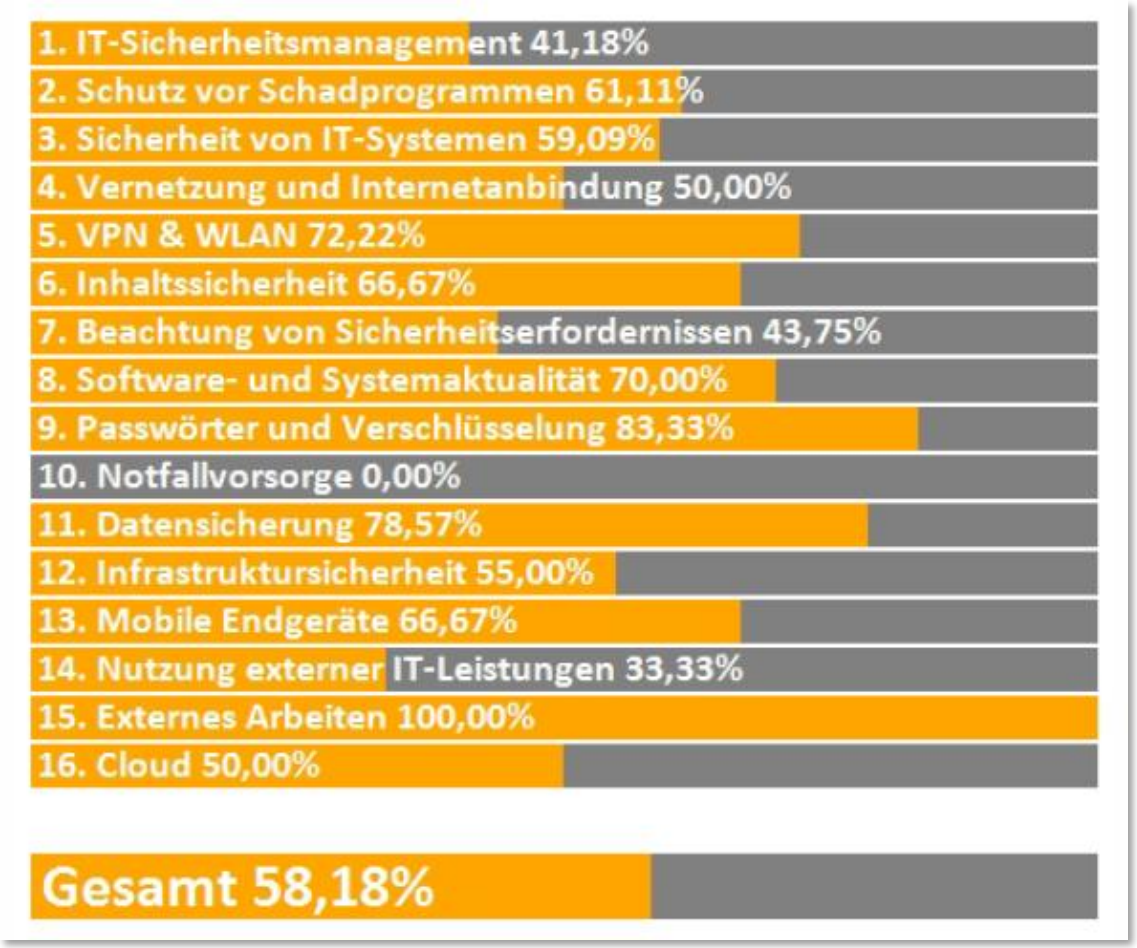


# ERFÜLLUNGSGRAD NACH PRÜFGRUPPEN




# NIS2 GAP ANALYSE

Benchmark Ergebnisse und Maßnahmenempfehlungen




Probleme mit **hohem Risikograd** sind rot gekennzeichnet.
Probleme mit **mittlerem Risikograd** orange.
Probleme ohne Farbkodierung weisen einen **niedrigeren Risikograd** auf.

| Kennung | Maßnahmenempfehlung | Prüfpunkt |
|---|---|---|
| A02 | Erstellen eines Sicherheitskonzeptes | 1.2 |
| A03 | Übersicht der gesetzlichen Anforderungen | 1.3 |
| A04 | Ernennen eines IT-Sicherheitsbeauftragten | 1.4 |
| A07 | Durchführen einer Schutzbedarfsanalyse | 1.7 |
| A10 | Stellvertretungsregelungen definieren | 1.10 |
| A11 | Passworthinterlegung regeln | 1.11 |
| A14 | Bereitstellen von verschließbaren Behältnissen | 1.14 |
| A17 | Erstellen einer Richtlinie zum Informationsaustausch | 1.17 |
| A18 | Jährliche Revision des Sicherheitsstatus | 1.18 |
| B04 | Dedizierter Virenschutz für E-Mail Server | 2.4 |
| B07 | Handlungsanweisung zur Verhaltensweise bei Virenbefall | 2.7 |
| B08 | Routineaufgabe zur regelmäßigen Überprüfung der Virenschutzprogramme | 2.8 |
| C10 | Systemdokumentationen erstellen oder aktualisieren | 3.10 |
| D07 | Netzwerk-Topologieplan erstellen | 4.7 |
| D08 | Erstellen einer Sicherheitsrichtlinie für Router und Switches | 4.8 |
| E06 | Erstellen einer WLAN-Sicherheitsrichtlinie | 5.6 |
| F03 | Erstellung einer E-Mail-Richtlinie | 6.3 |

# SCHADENSKLASSE

PASSION4IT

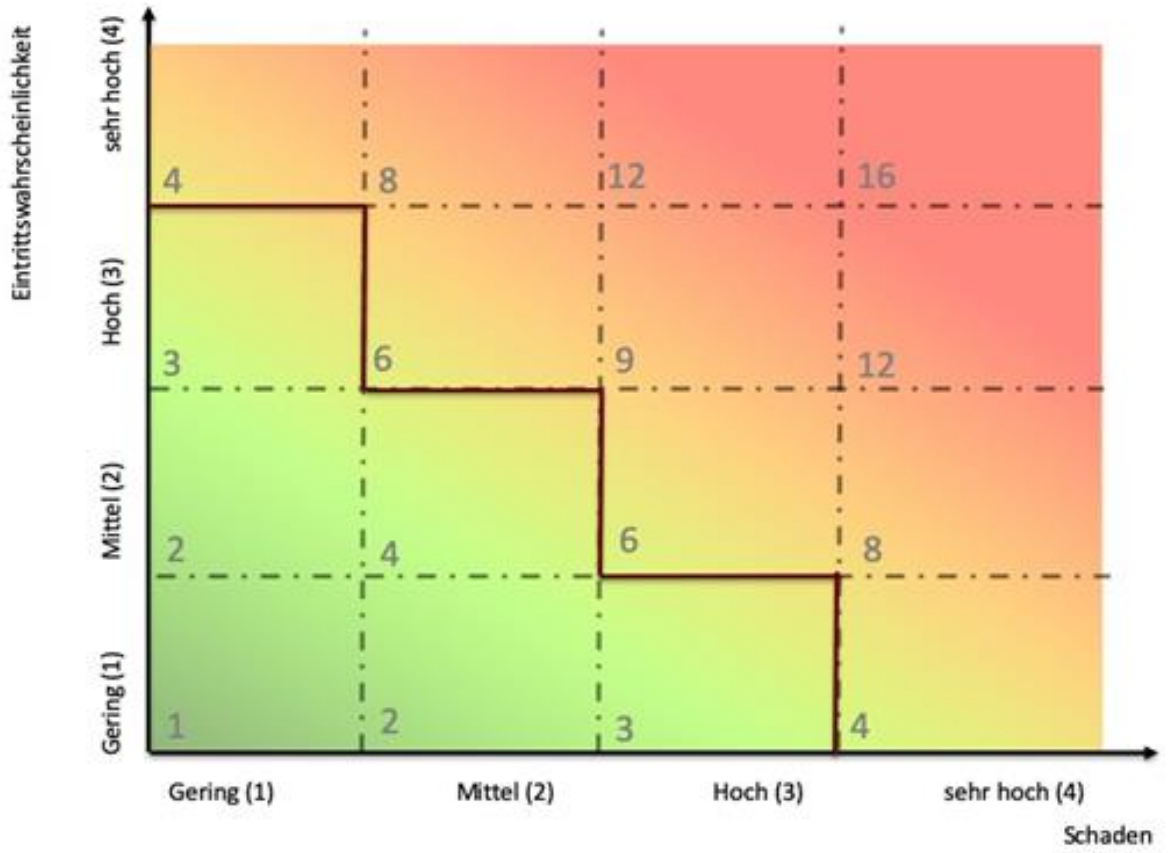
| Schadensklasse | Wert | Finanzieller Schaden | Ausfall Kernprozesse | Reputationsschaden | Auswirkungen auf natürliche Personen |
|---|---|---|---|---|---|
| **gering** | **1** | < 5.000 € | Minimale Verzögerungen in den nachfolgenden Prozessen (bis zu 2 Stunden) | Vorfall ist nur internen Mitarbeitern bekannt. Keine medialen Auswirkungen | Nachteile (wirtschaftlich, gesellschaftlich) im geringen Umfang für die Person |
| **mittel** | **2** | Zwischen 5.000 € und 20.000 € | Führt zu einer Verzögerung von ca. einen Tag bei den nachfolgenden internen Prozessen | Regionale mediale Auswirkungen | Finanzieller Schaden (nicht existenzgefährdend) |
| **hoch** | **3** | Zwischen 20.000 € und 50.000 € | Führt zu einer Verzögerung von mehr als einen Tag bei den nachfolgenden internen Prozessen | Vorfall hat nationale Mediale Auswirkungen, negatives Images auch bei Stellenausschreibungen | Identitätsdiebstahl, Diskriminierung |
| **sehr hoch** | **4** | > 50.000 € | Führt zu einer Verzögerung bei den geplanten Lieferzeiten; Kundentermine können nicht eingehalten werden | Vorfall hat internationale mediale Auswirkungen, Verlust von Kunden | Lebensgefahr, Existenzgefährdend |

# EINTRITTSWAHRSCHEINLICHKEIT

PASSION4IT

| Eintritts-wahrscheinlichkeit | Wert | Schätzung für die Zukunft | Blick in die Vergangenheit |
|---|---|---|---|
| **gering** | **1** | Vorfall tritt frühestens in 6 Jahren oder später ein | Vorfall bisher noch nie eingetreten bzw. vor über 6 Jahren eingetreten |
| **mittel** | **2** | Vorfall tritt in den nächsten 4-6 Jahren ein | Vorfall ist in den letzten 4-6 Jahren eingetreten |
| **hoch** | **3** | Vorfall tritt in den nächsten 1-3 Jahren ein | Vorfall ist in den letzten 1-3 Jahren eingetreten |
| **sehr hoch** | **4** | Vorfall tritt im nächsten Jahr ein | Vorfall ist im letzten Jahr eingetreten |

# RISIKOAKZEPTANZNIVEAU



# RISIKOKLASSIFIZIERUNG / BEHEBUNG

PASSION4IT

| Risikoeigner | Risiko Szenario (Beschreibung eines möglichen Vorfalls) | Beschreibung des Schadens ("...führt zu") | Ursache / Grund für das Eintreten des Szenarios (= Schwachstelle) | Schadens-klasse | Eintritts-wahrschein-lichkeit | Risiko | | Geplante Zusatzmaßnahmen | Schadens-klasse (neu) | Eintritts-wahrscheinlich-keit (neu) | Risiko | Status Zusatzmaßnahme | Verantwortlich für Zusatzmaßnahme | Datum der Umsetzung |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Insider-Bedrohungen | Führt zu Datenverlust, finanziellen Verlusten und Rufschädigung des Unternehmens. | Unzureichende Überwachung und mangelnde Sicherheitskontrollen für interne Benutzer. | gering | gering | | | Implementierung strenger Zugriffskontrollen, regelmäßige Überprüfung von Benutzeraktivitäten und Einführung von Whistleblower-Programmen. | mittel | mittel | | | | |
| | Schwachstellen in Software und Hardware | Führt zu unbefugtem Zugriff auf sensible Daten, möglichen Datenverlusten und Sicherheitsverletzungen. | Unzureichende Sicherheitsüberprüfungen und Tests bei der Entwicklung von Software und Hardware. | mittel | mittel | | | Durchführung regelmäßiger Sicherheitsbewertungen und Penetrationstests sowie schnelle Behebung von entdeckten Schwachstellen. | mittel | mittel | | | | |
| | Ransomware-Angriffe | Führt zu Datenverlust, Betriebsunterbrechungen und finanziellen Verlusten. | Unzureichende Sicherheitsmaßnahmen wie fehlende Datensicherungen und unzureichender Schutz vor Schadsoftware. | sehr hoch | hoch | | | Implementierung regelmäßiger Backups, Schulung der Mitarbeiter und Einsatz von Anti-Malware-Software. | mittel | mittel | | | | |
| | Distributed Denial of Service (DDoS) | Führt zu Dienstunterbrechungen und möglichen finanziellen Verlusten durch Ausfallzeiten. | Fehlende Schutzmechanismen gegen DDoS-Angriffe. | hoch | mittel | | | Einsatz von DDoS-Schutzdiensten und Lastverteilungsmechanismen, um Angriffe abzufangen und zu mitigieren. | mittel | mittel | | | | |
| | Man-in-the-Middle-Angriffe | Führt zu unbefugtem Zugriff auf vertrauliche Informationen und möglichen finanziellen Verlusten. | Verwendung unsicherer Kommunikationsprotokolle oder fehlende Verschlüsselung. | mittel | mittel | | | Implementierung sicherer Kommunikationsprotokolle und Verschlüsselung von Datenübertragungen. | mittel | mittel | | | | |
| | Schwache Authentifizierungsmechanismen | Führt zu unbefugtem Zugriff auf Systeme und Daten. | Verwendung schwacher Passwörter und fehlende zusätzliche Authentifizierungsmaßnahmen. | hoch | gering | | | Einführung von Zwei-Faktor-Authentifizierung und Schulung der Benutzer zur Erstellung sicherer Passwörter. | mittel | mittel | | | | |

# 08

# SUMMARY

Cyber Security und Risikomanagement ist keine einmalige Aufgabe, sondern muss als Prozess verstanden werden, indem kontinuierlich an der Verbesserung, Aufrechterhaltung und Kontrolle der Sicherheitsmaßnahmen gearbeitet wird.


PASSION4IT