egerer

IT-Sicherheit

Risiken erkennen, bewerten und managen

Webinar der Reihe IT-Sicherheit 7. Staffel der BIHK | 25.11.2025

Martin Egerer | David Capriati

Vorstellung

Das sind wir

Martin Egerer
Gründer & Geschäftsführer
egerer Consulting GmbH

David Capriati
Managing Consultant Business Resilience
egerer Consulting GmbH

Mehr Infos unter
www.egerer-consulting.de

Agenda

Was uns heute erwartet

Inhalte des heutigen Webinars

01	Intro und Kontext	Zielsetzung des Webinars
02	Bedrohungslage	Aktuelle Trends | Informationsquellen für aktuelle Bedrohungslage
03	Risiken managen	Risikomanagement verstehen | Asset, Bedrohung, Schwachstelle | ISO/IEC 27005
04	Maßnahmen	Erste Schritte | Etablierung eines kontinuierlichen Verbesserungsprozesses (KVP)
05	Q&A	Abschluss mit Fragerunde

2 | Die Bedrohungslage

Die Schadenshöhe

Schadenshöhe durch Cyberangriffe in Deutschland pro Jahr:

202,4 Milliarden Euro*

entspricht ca. dem BIP Ungarns **

Vergleich mit Umsätzen 2024** in der Wirtschaft:

- Allianz SE: ca. 180 Mrd. €
- Schwarz Gruppe: ca. 175,4 Mrd. €
- BMW AG: ca. 142 Mrd. €
- Deutsche Telekom: ca. 115,8 Mrd. €
- E.ON SE: ca. 93 Mrd. €
- Siemens AG: ca. 78 Mrd. €

* Quelle: www.bitkom.org | Studie Wirtschaftsschutz 2025
** Quelle: www.wikipedia.org | div. Sub-Sites

2 | Bedrohungslage

Case Studys und BSI Lagebericht* zur IT-Sicherheit 2025

> *Die Bedrohung durch Cybercrime-as-a-Service, speziell Ransomware-as-a-Service, blieb im aktuellen Berichtszeitraum hoch. Ziele waren vermehrt mit Datenverschlüsselung und Datenexfiltration mit anschließender Erpressung konfrontiert.* ***Zu den Hauptbetroffenen zählen KMU.****

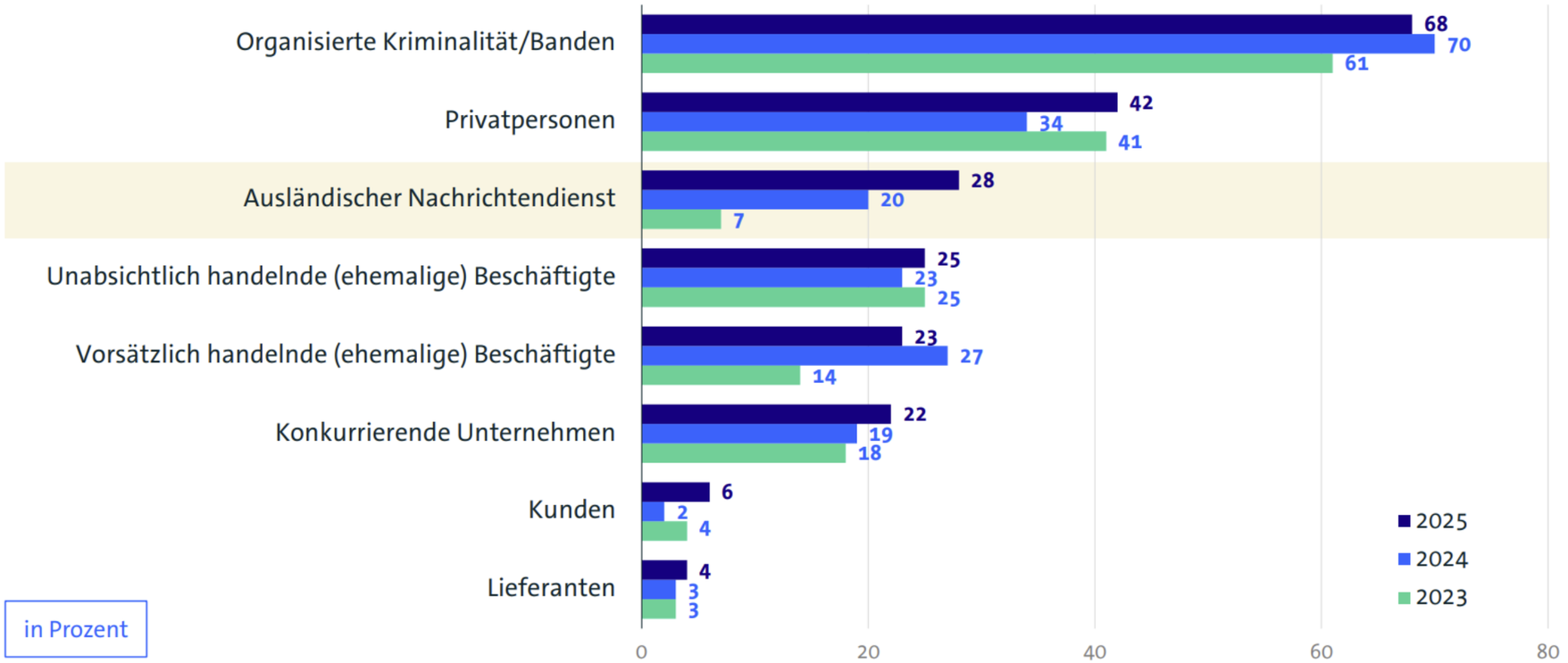
* Quelle: Bundesamt für Sicherheit in der Informationstechnik, Lagebericht zur IT-Sicherheit 2025, https://medien.bsi.bund.de/lagebericht/de/index.html

2 | Bedrohungslage

egerer

Die Täter

Von welchem Täterkreis gingen die Handlungen in den letzten 12 Monaten aus?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=868) | Mehrfachnennungen möglich |
Quelle: Bitkom Research 2025

2 | Bedrohungslage

Aktuelle Trends

Phishing

- **Betrügerische Nachrichten** mit dem Ziel, **Zugangsdaten** zu erbeuten und **Schadsoftware** zu installieren
- **94 %** aller Schadsoftware wird via E-Mails übertragen
- **2024:** Phishing-Angriffe haben bei 22 % der Unternehmen in den letzten 12 Monaten einen Schaden verursacht

2 | Bedrohungslage

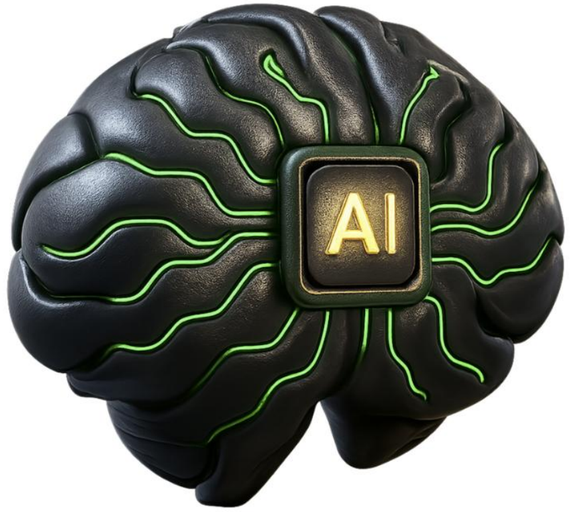
Aktuelle Trends

Ransomware

- **Verschlüsselung** Ihrer Daten durch Schadsoftware und Erpressung von Lösegeld
- **Größte Cyberbedrohung** für Unternehmen laut BSI
- **2024:** Ransomware hat bei 34 % der Unternehmen in den letzten 12 Monaten einen Schaden verursacht

2 | Bedrohungslage

Aktuelle Trends



AI

- **Perfektionierung von Social Engineering:** KI generiert fehlerfreie, täuschend echte „Spear Phishing“-Mails und ermöglicht Angriffe in jeder Sprache
- **Deepfakes und Voice Cloning:** Einsatz von künstlichen Stimmen (z. B. CEO Fraud) und Video-Fakes zur Überlistung von Authentifizierungen
- **Automatisierung und Skalierung:** Senkung der Einstiegshürde für Kriminelle, denn KI schreibt Schadcode und findet Sicherheitslücken automatisiert und schneller als der Mensch

2 | Bedrohungslage

Aktuelle Trends

Supply Chain Attack

- **Gezielte Angriffe** auf Supply Chain des eigentlichen Ziels
- **Infiltrieren** des Lieferanten, um Zugang zu den Systemen des Ziels zu bekommen
- Kollateralschaden wird in Kauf genommen

2 | Bedrohungslage

Informiert bleiben: Quellen für aktuelle Bedrohungen

Bundesamt
für Sicherheit in der
Informationstechnik

Immer aktuell: [BSI Cyber-Sicherheitslage]

bitkom

Digitalverband bitkom

[Bitkom Dataverse | Sicherheit & Datenschutz]

3 | Risiken managen

Warum das Managen von Risiken sinnvoll ist

Option A

Option B

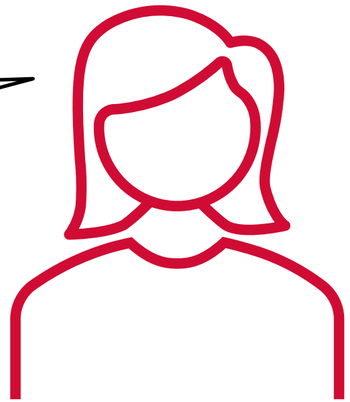
Für welche Option würden Sie sich entscheiden?
Reagieren oder Vorbeugen?

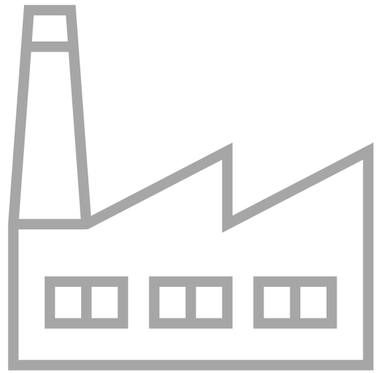
3 | Risiken managen

Unsere Storyline

Ich wähle Option B, ich möchte Vorbeugen.

Ich bin mir meiner Verantwortung bewusst.





Sabine Beispiel

Geschäftsführerin eines produzierenden Betriebs (3D-Print Solution GmbH)

300 Mitarbeiter, 3D-Druck im B2C-Bereich

3 | Risiken managen

Begriff des IT-Risikomanagements

Was ist IT-Risikomanagement?
IT-Risikomanagement ist ein **systematischer Prozess** zur Identifikation, Bewertung und Behandlung von Risiken, die die Informationssicherheit einer Organisation gefährden können. Es geht darum, potentielle Bedrohungen frühzeitig zu erkennen und Schutzmaßnahmen zu implementieren.

Was ist das Ziel?
Das **Ziel ist nicht das vollständige Eliminieren aller Risiken**, das wäre unrealistisch und unwirtschaftlich. Vielmehr wird eine ausgewogene Balance zwischen Sicherheit, Funktionalität und Kosten angestrebt.

Was ist der Effekt?
Ein effektives Risikomanagement ermöglicht es Unternehmen, **kritische Werte und Geschäftsprozesse zu schützen** und die drei Schutzziele **Vertraulichkeit, Verfügbarkeit** und **Integrität** zu stützen.

3 | Risiken managen

Risikomanagement verstehen – wichtige Begriffe

Das Asset (Wert)

- Primäres Asset (Informationen, Geschäftsprozesse), z. B. Prozess Produktionssteuerung, Kundendaten
- Sekundäres Asset (unterstützende Werte, auf diesen werden die primären Assets verarbeitet, z. B. Server, Datenbanken)

3 | Risiken managen

Risikomanagement verstehen – wichtige Begriffe

Das Asset

- Primäres Asset (Informationen, Geschäftsprozesse), z. B. Prozess Produktionssteuerung, Kundendaten
- Sekundäres Asset (unterstützende Werte, auf diesen werden die primären Assets verarbeitet, z. B. Server, Datenbanken)

Bedrohung

- Mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder eine Organisation führen kann
- Oft unabhängig vom Unternehmen existent
- z. B. Gefährdungskatalog des BSI als Quelle

3 | Risiken managen

Risikomanagement verstehen – wichtige Begriffe

Schwachstelle

- Von einer Bedrohung ausnutzbare Schwäche eines Wertes (asset) oder einer Maßnahme
- Beispiel technische Schwachstelle: ungepatchtes Betriebssystem
- Beispiel organisatorische Schwachstelle: einfache Passwörter

Das Asset

- Primäres Asset (Informationen, Geschäftsprozesse), z. B. Prozess Produktionssteuerung, Kundendaten
- Sekundäres Asset (unterstützende Werte, auf diesen werden die primären Assets verarbeitet, z. B. Server, Datenbanken)

Bedrohung

- Mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder eine Organisation führen kann
- Oft unabhängig vom Unternehmen existent
- z. B. Gefährdungskatalog des BSI als Quelle

3 | Risiken managen

Risikomanagement verstehen – wichtige Begriffe

Risiko

- Negative Auswirkung von Ungewissheit auf Ziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)
- Ausgedrückt durch Wahrscheinlichkeit des Eintretens eines bestimmten Schadensereignisses und Auswirkung bzw. zu erwartende Folgen bei Eintritt dieses Ereignisses

Schwachstelle

- Von einer Bedrohung ausnutzbare Schwäche eines Wertes (asset) oder einer Maßnahme
- Beispiel technische Schwachstelle: ungepatchtes Betriebssystem
- Beispiel organisatorische Schwachstelle: einfache Passwörter

Das Asset

- Primäres Asset (Informationen, Geschäftsprozesse), z. B. Prozess Produktionssteuerung, Kundendaten
- Sekundäres Asset (unterstützende Werte, auf diesen werden die primären Assets verarbeitet, z. B. Server, Datenbanken)

Bedrohung

- Mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder eine Organisation führen kann
- Oft unabhängig vom Unternehmen existent
- z. B. Gefährdungskatalog des BSI als Quelle

3 | Risiken managen

egerer

Der Risikomanagement-Prozess nach ISO 27005

Risiko = Bedrohung + Schwachstelle

Wirken auf Asset, bedrohen ein Schutzziel

Wahrschein-lichkeit x Auswirkung?

=

Risikolevel

Vergleich mit Akzeptanz-kriterien und Priori-sierung

Risikoakzeptanzkriterien

- Niedrige Risiken werden immer akzeptiert.
- Mittlere Risiken können von der Leitung akzeptiert werden.
- Hohe Risiken müssen innerhalb von drei Monaten, sehr hohe Risiken innerhalb von einem Monat behandelt werden.

Risikobehandlungsplan:

- Risiko beibehalten
- Risiko modifizieren
- Risiko teilen
- Risiko vermeiden

Identifikation → **Analyse** → **Bewertung** → **Option wählen** → **Maßnahmen festlegen** → **Plan erstellen** → **Zustimmung einholen**

Risikobeurteilung | **Risikobehandlung**

Risikomanagement-Prozess

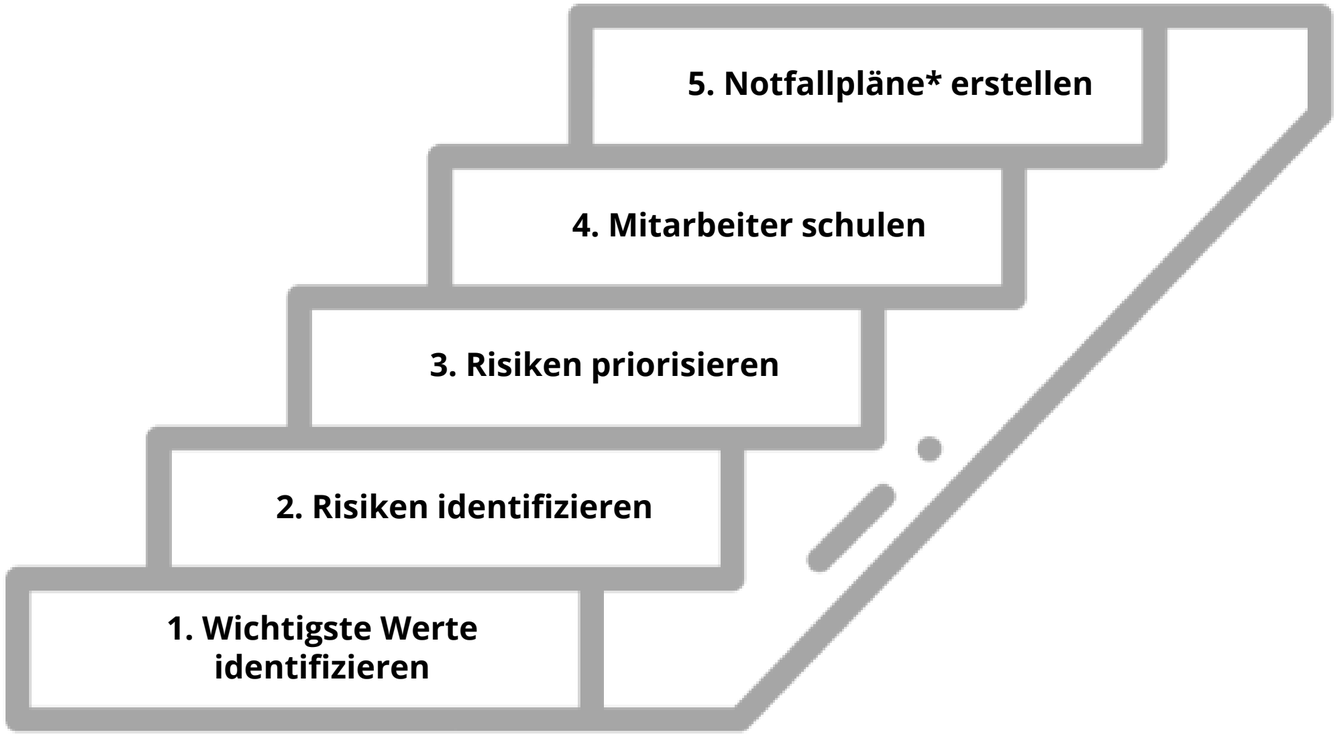
Risikomatrix

Eintrittswahrscheinlichkeit				
sehr hoch	M	H	SH	SH
hoch	N	M	H	SH
mittel	N	M	M	H
niedrig	N	N	N	M
Schadenshöhe	niedrig	mittel	hoch	sehr hoch

4 | Maßnahmen

Erste Schritte

„Das erschlägt mich. Ich weiß nicht, wo ich anfangen soll!“



* Muster: Notfallplan der IHK München und Oberbayern

4 | Maßnahmen

Kontinuierliche Verbesserung | der PDCA-Zyklus

Informationssicherheit ist kein Zustand, sondern ein Prozess.

Plan

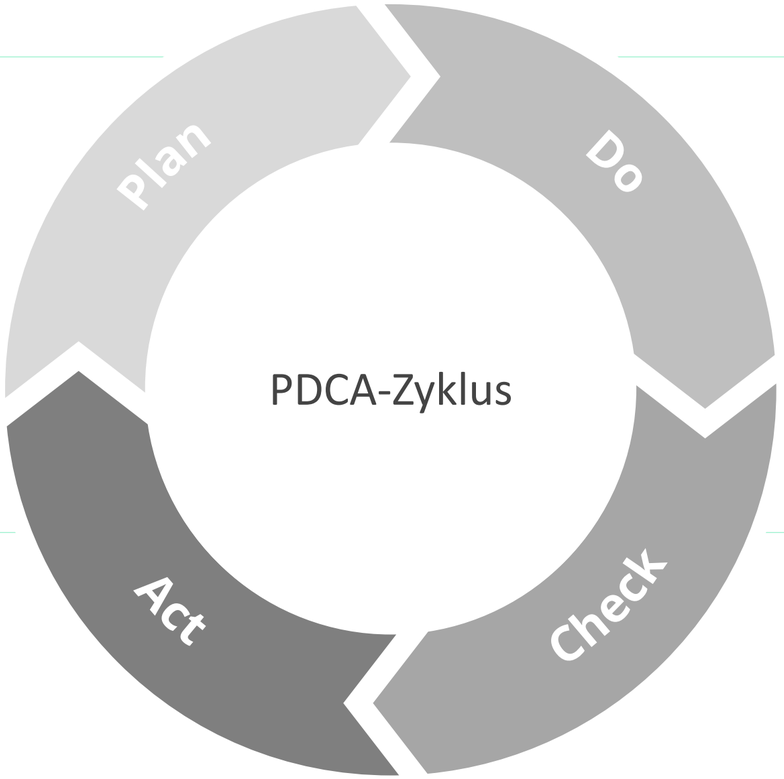
Was möchte ich tun? Wie möchte ich es tun?

- Kontext der Organisation verstehen
- Rollen und Verantwortlichkeiten festlegen
- Planung von Maßnahmen
- u.v.m.

Do

Die eigentliche Phase der Umsetzung:

- Ressourcen vorhalten
- Maßnahmen umsetzen



Act

“Nacharbeit”

- Behebung der in Check gefundenen Schwachstellen

Check

Überwachung der umgesetzten Maßnahmen

- Messung der Wirksamkeit
- Internes Audit
- Managementbewertung

Wenn es komplex ist,

schaffen wir Klarheit und Struktur

Martin Egerer
Gründer & Geschäftsführer
egerer Consulting GmbH

David Capriati
Managing Consultant Business Resilience
egerer Consulting GmbH

Mehr Informationen:

egerer Consulting - Risikomanagement

inkl. Whitepaper

5 | Fragerunde und Abschluss

Q & A

Ihre Fragen sind herzlich willkommen!