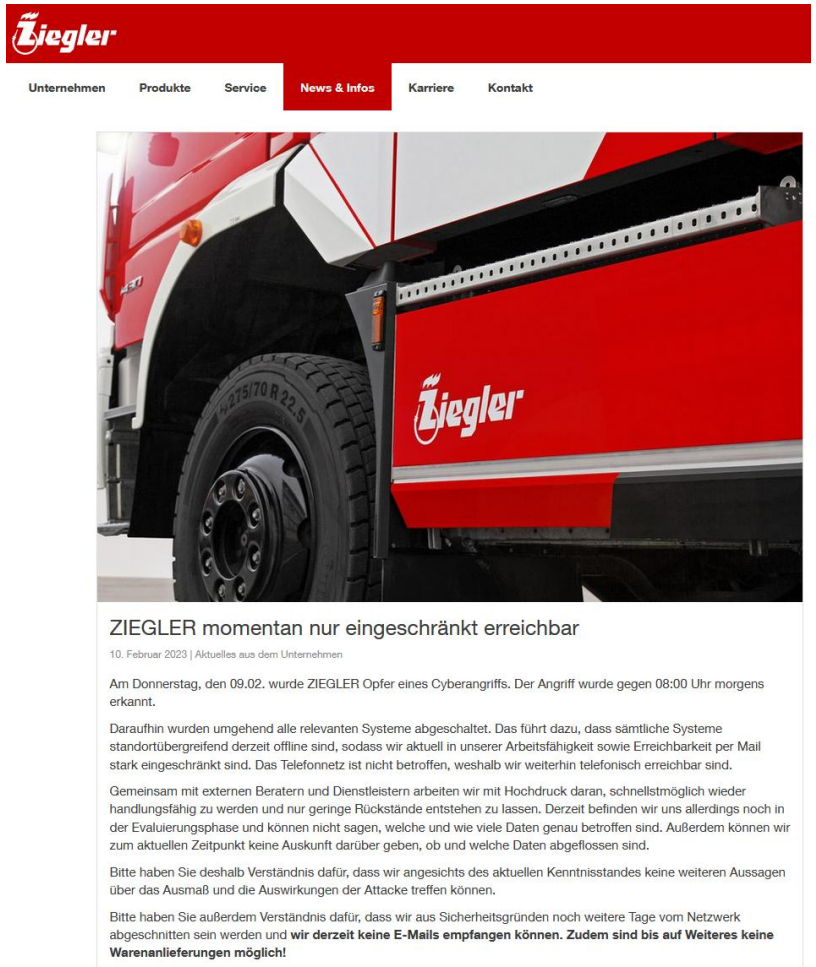
Was kostet ein Cyberangriff:

Wie finde ich die richtige, angemessene Umsetzung von Cybersecurity und schütze mein Unternehmen vor finanziellen Risiken?

Cyber Friday

Zufall?



Ziegler

Unternehmen | Produkte | Service | News & Infos | Karriere | Kontakt

ZIEGLER momentan nur eingeschränkt erreichbar

10. Februar 2023 | Aktuelles aus dem Unternehmen

Am Donnerstag, den 09.02. wurde ZIEGLER Opfer eines Cyberangriffs. Der Angriff wurde gegen 08:00 Uhr morgens erkannt.

Daraufhin wurden umgehend alle relevanten Systeme abgeschaltet. Das führt dazu, dass sämtliche Systeme standortübergreifend derzeit offline sind, sodass wir aktuell in unserer Arbeitsfähigkeit sowie Erreichbarkeit per Mail stark eingeschränkt sind. Das Telefonnetz ist nicht betroffen, weshalb wir weiterhin telefonisch erreichbar sind.

Gemeinsam mit externen Beratern und Dienstleistern arbeiten wir mit Hochdruck daran, schnellstmöglich wieder handlungsfähig zu werden und nur geringe Rückstände entstehen zu lassen. Derzeit befinden wir uns allerdings noch in der Evaluierungsphase und können nicht sagen, welche und wie viele Daten genau betroffen sind. Außerdem können wir zum aktuellen Zeitpunkt keine Auskunft darüber geben, ob und welche Daten abgeflossen sind.

Bitte haben Sie deshalb Verständnis dafür, dass wir angesichts des aktuellen Kenntnisstandes keine weiteren Aussagen über das Ausmaß und die Auswirkungen der Attacke treffen können.

Bitte haben Sie außerdem Verständnis dafür, dass wir aus Sicherheitsgründen noch weitere Tage vom Netzwerk abgeschnitten sein werden und **wir derzeit keine E-Mails empfangen können. Zudem sind bis auf Weiteres keine Warenanlieferungen möglich!**

400.000 Euro weg: Stadt Dülmen wird Opfer von Betrügern

Stand: 13.03.2025, 14:19 Uhr

Mit einer betrügerischen E-Mail haben Unbekannte bei der Stadt Dülmen Geld erbeutet, das für neue Feuerwehrautos gedacht war.

Von Markus Holtrichter

Der Fall ist der Stadt Dülmen extrem unangenehm. Er zeigt laut der Polizei im Kreis Coesfeld aber exemplarisch, dass nicht nur Leute privat von Betrugsversuchen per E-Mail bedroht sind. Und der Schaden ist beträchtlich: 400.000 Euro überwies die Verwaltung irrtümlich an die Täter.

Betrüger mit falscher Rechnung

Wie war das möglich? Die Stadt hatte zwei neue Fahrzeuge für die Feuerwehr in Auftrag gegeben. Davon wussten die Betrüger wohl, hatten offenbar auch den Hersteller ausspioniert. Mit diesen Daten erstellten sie dann eine täuschend echte Rechnung für die Stadtverwaltung. Mit Konto im Ausland.


GRAN TURISMO
RedBull
KUS
VELTINS
VELTINS
H&R
MOTUL
MOTUL
MOTUL

Den Schaden hatte der „Grello“

24h Nürburgring 2026

Ein anderes Fahrzeug verliert Betriebsmittel.

Der Grello gerät auf die Ölspur und scheidet nach dem Unfall aus.

Die Parallele zur IT-Sicherheit

Ein externer Dienstleister wird kompromittiert.

Die Folgen treffen auch ein gut geschütztes Unternehmen.

Nicht jeder, der den Schaden erleidet, hat die Gefahr verursacht.

Wie sich Risiken entlang digitaler Abhängigkeiten ausbreiten

01

Fremder Vorfall

Dienstleister, Software oder Wartungszugang betroffen

02

Gefahr bleibt verborgen

Fehlende Transparenz oder zu späte Warnung

03

Folgeschaden

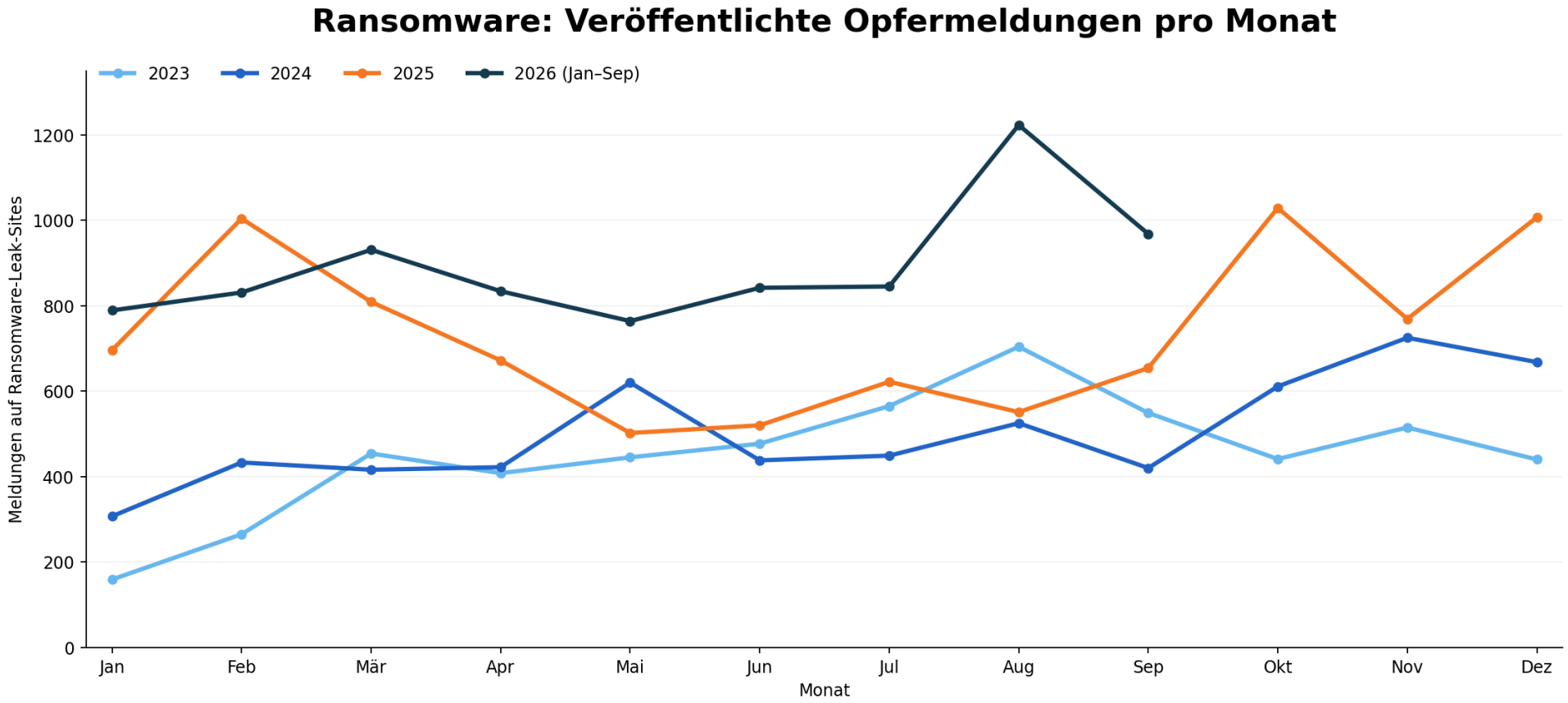
Kompromittierung, Ausfall oder Datenverlust

04

Betriebsunterbrechung

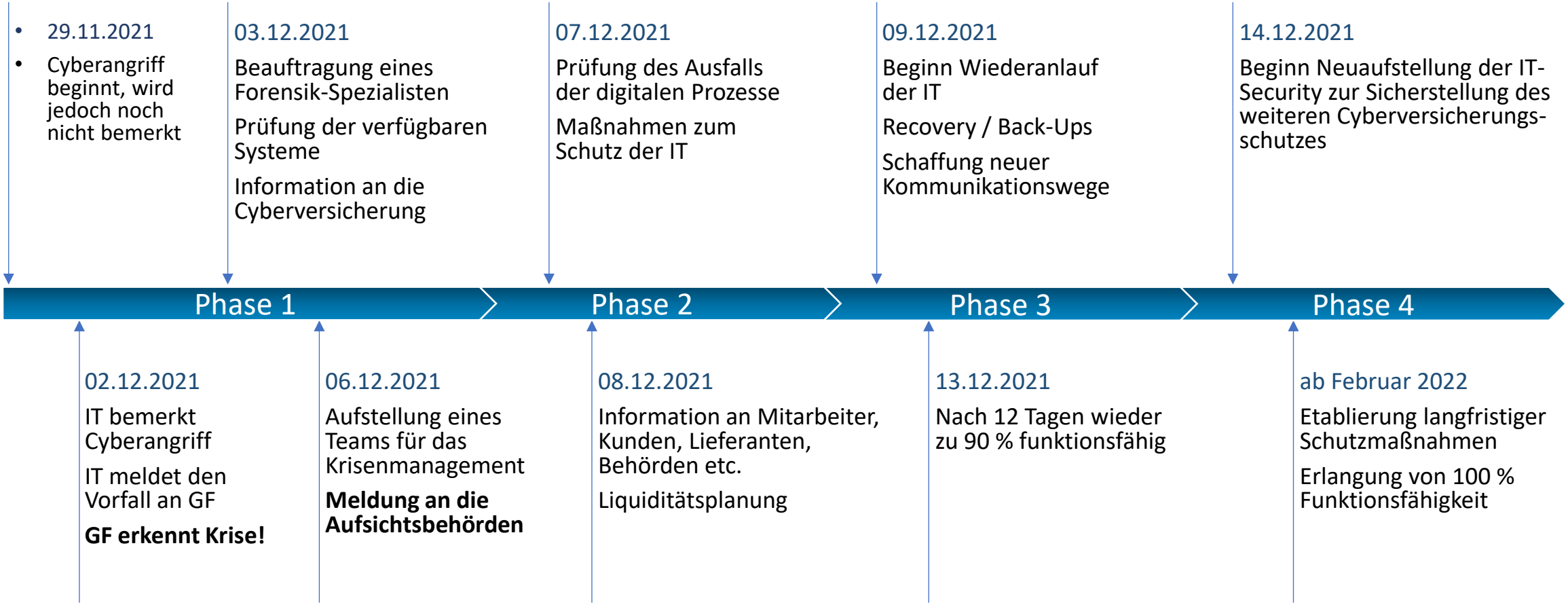
Produktion oder Dienstleistungen stehen still

Monatliche Angriffszahlen 2023-2026



Quelle: Ransomnews Ransomtracker / RansomLook (CC BY 4.0), Abruf 29.10.2026. 2026 nur Jan–Sep.
Täterangaben; keine unabhängig bestätigten Vorfälle. Historische Erfassung kann unvollständig sein.

Wie läuft ein Angriff ab?



Ein Cyberangriff verursacht weit mehr als reine IT-Kosten.

Beispiel – Cyberangriff auf die Südwestfalen-IT

01

IT-Wiederherstellung

Systeme, Daten, Infrastruktur

02

Betriebsunterbrechung

Notbetrieb, Rückstände, Mehrarbeit

03

Folgen für Dritte

Kunden, Partner und Lieferketten

72 Mitgliedskommunen | über 100 NRW-Kommunen unterschiedlich betroffen

Die IT-Rechnung bildet nur einen Teil der wirtschaftlichen Folgen ab.

Quelle: Landtag NRW, Drucksache 18/7439

Drei Zahlen – drei verschiedene Bedeutungen

2,8 Mio. €

Zusatzaufwendungen der SIT

bis 30.09.2024

4,2 Mio. €

Jahresfehlbetrag der SIT

Geschäftsjahr 2023

550.500 €

Zusätzliche Zahlungen

Kreis Soest, 2024

Nicht addieren: Aufwand, Jahresergebnis und Finanzierung überschneiden sich.

Quellen: SIT-Jahresbilanz; HSK- und Soester Beteiligungsberichte

„Cybersicherheit ist jetzt Chefsache!“

Vor dem Vorfall: „Brauchen wir das wirklich?“

Nach dem Vorfall: „Wo muss ich unterschreiben? Auch auf Seite 37? Mache ich!“

"Cybersecurity ist jetzt Chefsache." –

Die Geschäftsführung. Zwei Tage nach dem Ransomware-Angriff, wenn Panikbudget plötzlich Innovationsmotor wird:

- Alles wird unterschrieben.
- Budget? Egal.
- Security-Awareness für alle – sogar fürs Bistro-Team.
- Zero Trust? Nehme ich.
- Backup? Doppelt. Und mit Aromatherapie.

„Aber hey – wenigstens ist jetzt endlich Geld da!“- Vielleicht? – Hoffentlich!

Was haben Luftschiff fliegen und Informationssicherheit gemeinsam?

Die Planung macht mehr als 95 % des Erfolges aus!

Offensichtlich läuft´s gut



Offensichtlich läuft´s gar nicht gut



Anscheinend alle Gefahren zu erkennen…



Und plötzlich werden versteckte Risiken auch sichtbar…



Was ist ein wirkliches Risiko?



Bugatti Veyron

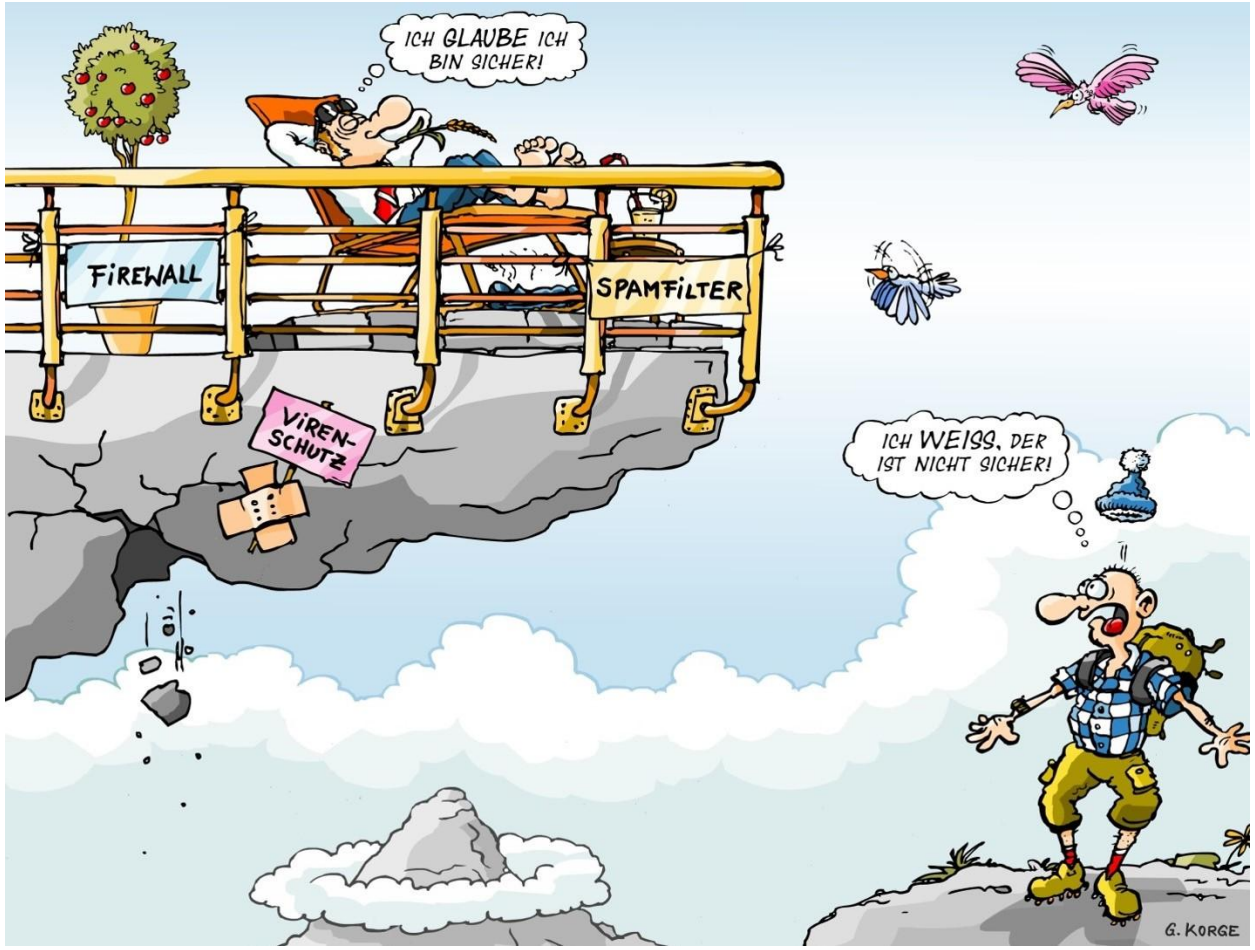
Bewertung von Bugatti:
Kein Handlungsbedarf!
Nach 12 min. ist der Tank sowieso leer!

Die speziellen Reifen von Michelin halten einen 400-km/h-Run angeblich nur 20 min. lang aus.

Was ist die aktuelle Situation?

Die meisten Unternehmensprozesse werden heute überwiegend IT-gestützt durchgeführt (Zahlungswesen, Lagerhaltung, Kontrollfunktionen, Produktionsprozesse, Zulieferermanagement usw.).

Durch einen Cyberangriff können zusätzlich viele Prozesse betroffen sein, die bei einer **Betriebsunterbrechung nicht sofort sichtbar** werden, aber kritisch sein können (Lieferkettenprozesse, Abhängigkeiten mit Kunden usw.).



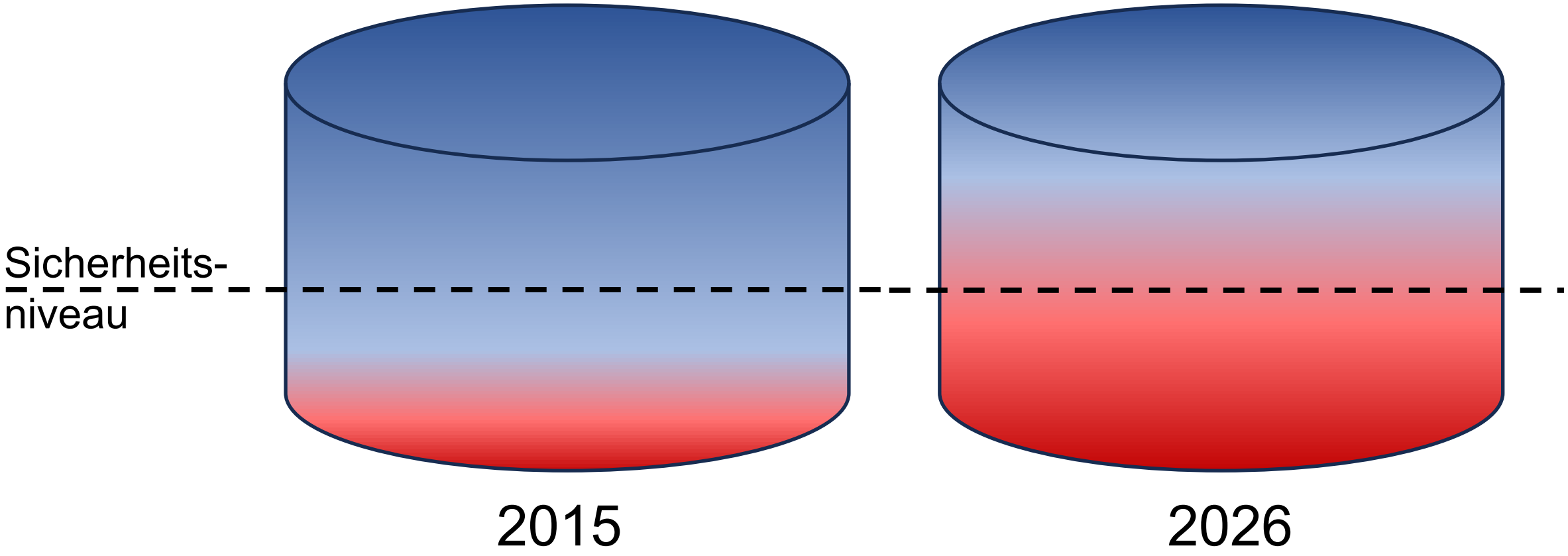
Betrachtungsweise

Wie sieht es denn dann mit der Informationssicherheit aus?

Betrachtungsweise



Betrachtungsweise



Ein Automobil

1999

ABS
Wegfahrsperre
Tempomat
Radio
Front- und Seiten-Airbags
Klimaanlage
H4 Licht
Zentralverriegelung



2026

Verkehrszeichen-Assistent
Totwinkel-Assistent
Tempomat mit Abstandsregelung
Parkassistent
Touch-Bedienung
Beheizte Frontscheibe
Digitales Radio
Keyless Go
LED-Licht
Lenkradheizung
Klimaautomatik
Elektrische Kofferraumklappen
Sitzheizung / Sitzlüftung



Ausgangssituation des Unternehmers

1999

Kopierer
Netzwerkverkabelung
manuelle Schließanlage
autarke Telefonanlage
separate Mobiltelefone
Manuelle Bankgeschäfte
Windows 98 und NT
Stempelkarten



2026

LAN und WLAN
Mobile Device Management
Windows 11 und Server 2021
Virtualisierung
Cloud Computing
Verschlüsselung
Social Media
Archivierung
Datenschutz
Digitale Steuerprüfung
Microsoft M365
Cyber Risiko (Ransomware, Trojaner, etc.)
Tablet Computer
Künstliche Intelligenz



Eintrittswahrscheinlichkeit vs. Konsequenz

Feuerversicherung

Anschnallpflicht im PKW (seit 1.1.1976)

- 48 Jahre x 220 Arbeitstage = 10.560 potentielle nutzenfreie Anschnallmanöver bei Unfallfreiheit

Wasserstopp an Wasch- und Spülmaschine

Wo investieren wir wie selbstverständlich?



Wo investieren wir wie selbstverständlich?





Ausfallsituation IT vs. IoT (Internet of Things)

IT-Ausfall (klassische IT-Systeme):

- Bürokommunikation (E-Mail, Telefonie) unterbrochen
- Datenzugriff (ERP, CRM, Fileserver) nicht möglich
- Verwaltungstätigkeiten gestört
- Wiederanlauf möglich durch Backups und IT-Notfallpläne

IoT-Ausfall (vernetzte Geräte und Systeme):

- Produktionsanlagen, Maschinen, Logistiksysteme fallen aus
- Automatisierte Prozesse stehen still
- Physische Schäden an Anlagen/Produkten möglich
- Wiederanlauf oft komplex: Reparatur oder Austausch nötig

Finanzielle Auswirkungen bei IT- und IoT-Ausfällen

IT-Ausfall:

- Produktivitätsverlust (E-Mail, ERP, CRM)
- Hohe Wiederherstellungskosten
- Risiko von Bußgeldern (z.B. DSGVO)
- Reputationsschäden

IoT-Ausfall:

- Produktionsstillstand → direkte Umsatzverluste
- Anlagenschäden und hohe Reparaturkosten
- Vertragsstrafen durch Lieferverzögerungen
- Ersatzinvestitionen bei defekten IoT-Geräten

Finanzielle Auswirkungen bei IT- und IoT-Ausfällen

Kernaussage:

- IT-Ausfall: Verwaltung und Daten betroffen
- IoT-Ausfall: Umsatz und Produktion massiv betroffen

Was heute selbstverständlich sein sollte…

Was machen wir mit IT – Wie schützen wir unsere „Diamanten“ vor Verlust/Zerstörung?

- Einsatz von Multifaktor-Authentifizierung
- Einsatz einer mehrstufigen Firewall
- Einsatz eines Intrusion-Detection-System
- Durchführung von regelmäßigen und ramsomwaregeschützte Backups und deren Funktionsprüfung
- Kennen wir die finanziellen Risiken eines Ausfalls?
- Ein Notfallplan!



„Dafür haben wir doch den IT-Dienstleister!“

IT-Dienstleister:

Übernimmt die Verantwortung für vereinbarte Leistungen

Schafft die fachliche Entscheidungsgrundlage.

- Identifiziert Risiken,
- zeigt mögliche Auswirkungen auf,
- empfiehlt Maßnahmen und
- unterstützt bei der Umsetzung.

„Dafür haben wir doch den IT-Dienstleister!“

Die Geschäftsleitung:

- trägt die unternehmerische Verantwortung
- entscheidet auf der Grundlage der Informationen des IT-Dienstleisters über Prioritäten, Ressourcen und den Umgang mit verbleibenden Risiken.

Diese Entscheidungen können jedoch nicht vollständig an einen IT-Dienstleister übertragen werden.

„Dafür haben wir doch den IT-Dienstleister!“

Unser Rat an die Geschäftsleitung:

- Lassen Sie sich regelmäßig über wesentliche IT- und Datenschutzrisiken sowie offene Maßnahmen informieren.
- Stellen Sie sicher, dass Verantwortlichkeiten klar geregelt und ISB bzw. DSB entsprechend qualifiziert sind.
- Treffen und dokumentieren Sie die notwendigen Entscheidungen zu Prioritäten, Ressourcen und verbleibenden Risiken.

Neben den finanziellen Auswirkungen:

Ein Cyberangriff kann für ein Unternehmen auch schwerwiegende rechtliche Konsequenzen haben.

- Geldstrafe, das Unternehmen gegen Datenschutzgesetze verstößt.
- Haftung gegenüber Personen, wenn durch den Angriff personenbezogene Daten veröffentlicht werden.
- Schadenersatzforderungen, wenn Kunden oder Mitarbeiter durch den Angriff Schaden erleiden.
- Imageschaden für das Unternehmen, wenn Kunden das Unternehmen als unsicher oder unzuverlässig einschätzen.

Die NIS2 – Regelungen beinhalten auch die persönliche Haftung eines Geschäftsführers bei fahrlässiger Handlung – „Tun durch Unterlassen.“

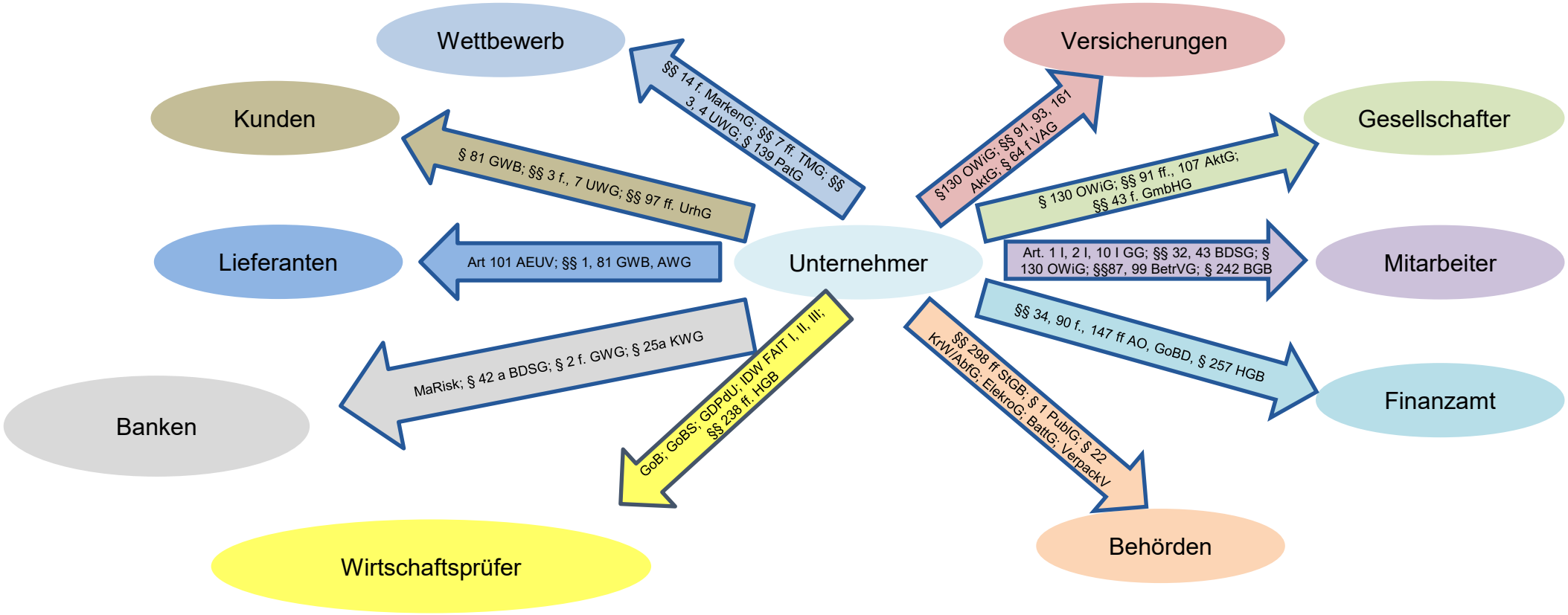
Ausgangssituation des Unternehmers und wie kann ich mich angemessen schützen?

Kontrollverlust?

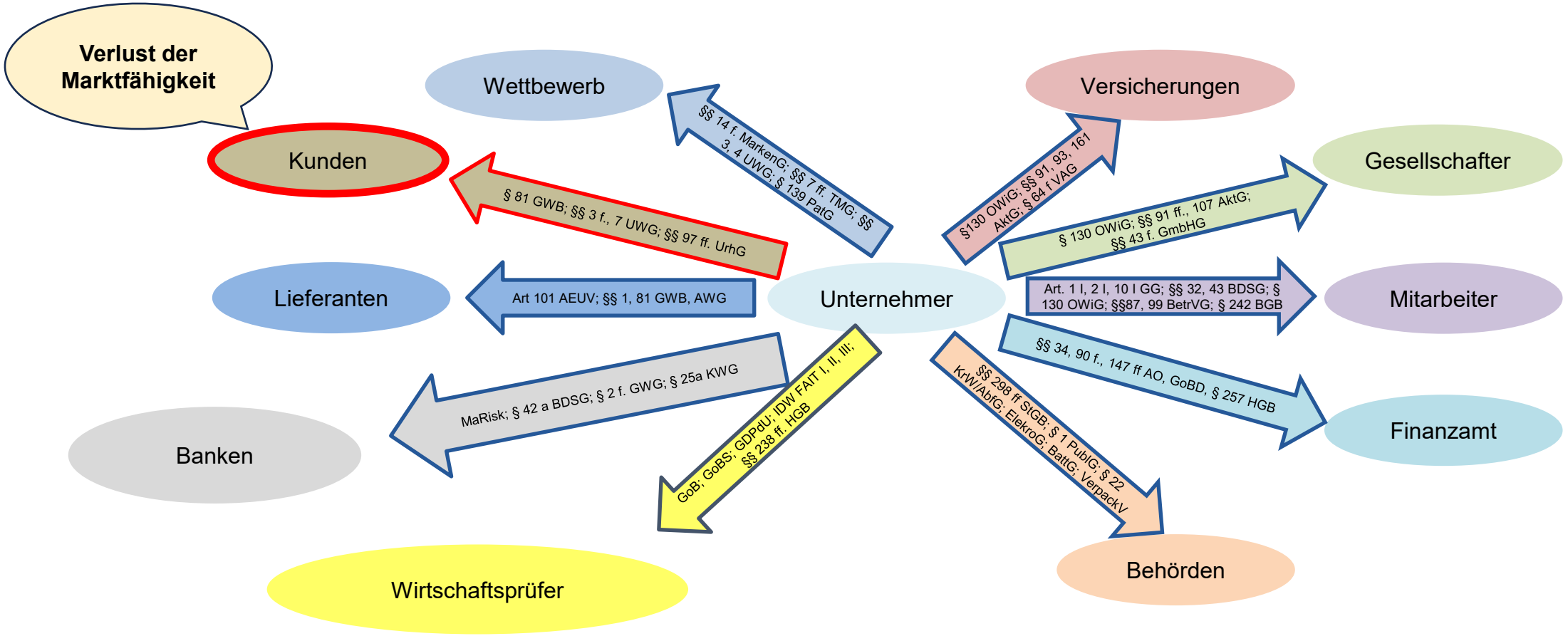
- **Ist das Unternehmen den Anforderungen gewachsen?**
- **Kenne ich meine Ausfallkosten?**
- **Bekomme ich die Kosten in den Griff?**
  - **Inflation, Energiekrise, Zulieferengpässe, Facharbeitermangel…**

Ersetze Glauben durch Wissen und Vertrauen durch Überprüfbarkeit!

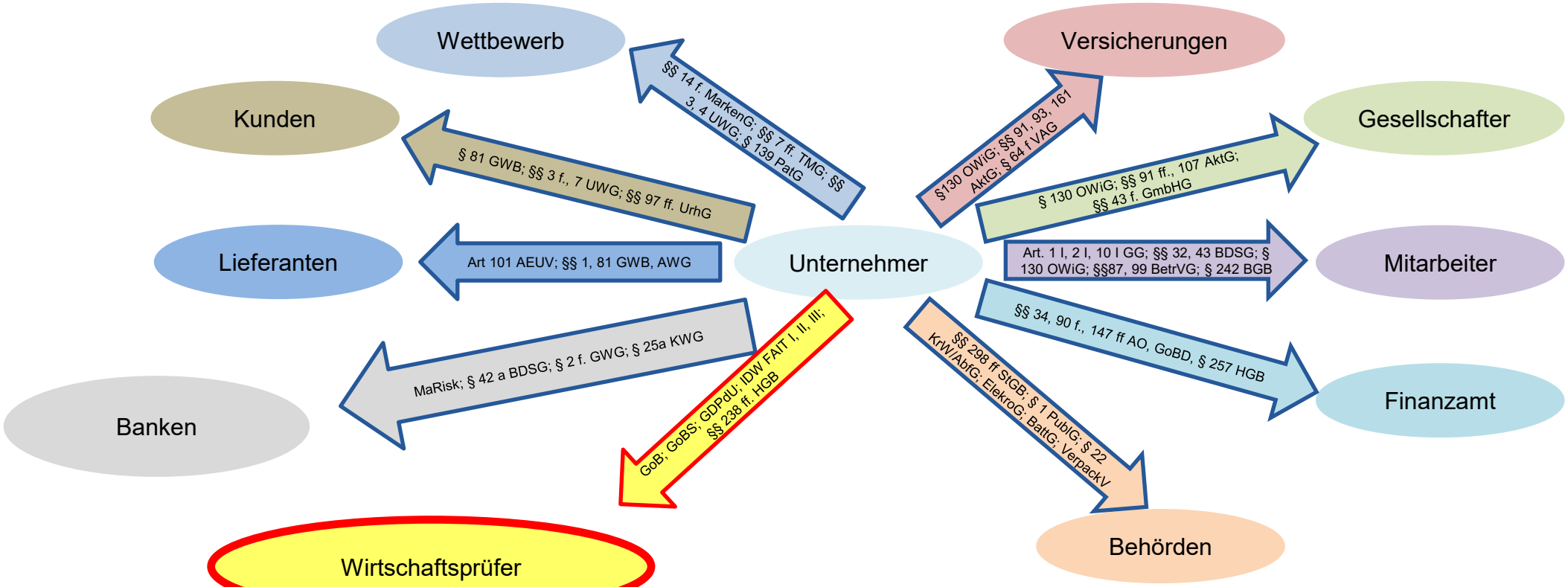
Was beeinflusst den Unternehmer?



Was beeinflusst den Unternehmer?



Was beeinflusst den Unternehmer?



Und es wird mehr:

Seit: 2025

DORA
seit 17.01.2025
Finanzsektor: ICT-Risiken, Vorfälle, Tests, Dienstleister

CRA
seit 11.09.2026
Meldung aktiv ausgenutzter Schwachstellen und schwerer Vorfälle

2026

KI-VO
02.02.2025 / 02.08.2025
KI-Kompetenz, Verbote, GPAI-Governance

CRA
ab 11.12.2027
Pflichten für Produkte mit digitalen Elementen: Secure-by-design, CE, Schwachstellenmanagement

NIS2 / BSIG n.F.
seit 06.12.2025
Registrierung, Risikomanagement, Meldepflichten, GL-Verantwortung

KI-VO
2027 / 2028
Hochrisiko-KI: Risikomanagement, Dokumentation, Aufsicht, Konformität

2027 / 2028

KI-VO
seit 02.08.2026
Transparenzpflichten, Kennzeichnung, nationale/EU-Durchsetzung

Data Act / Lieferkette
seit 2025 wirksam
Datenzugang, Cloud-Wechsel, Verträge und Nachweisfähigkeit prüfen

Kernaussage für Geschäftsleitungen:

Regulatorik wird praktisch: Unternehmen müssen Scope, Verantwortlichkeiten, Risikomaßnahmen, Meldewege und Nachweise beherrschbar machen – nicht nur Richtlinien ablegen.

Weitere aktuelle Meldungen: (Quelle: crn.de)

„NIS2 ist Hürde für Cyberversicherungen“

„Versicherer lehnen bereits heute jedes zweite größere Unternehmen ab, das sich gegen Hackerangriffe versichern will.

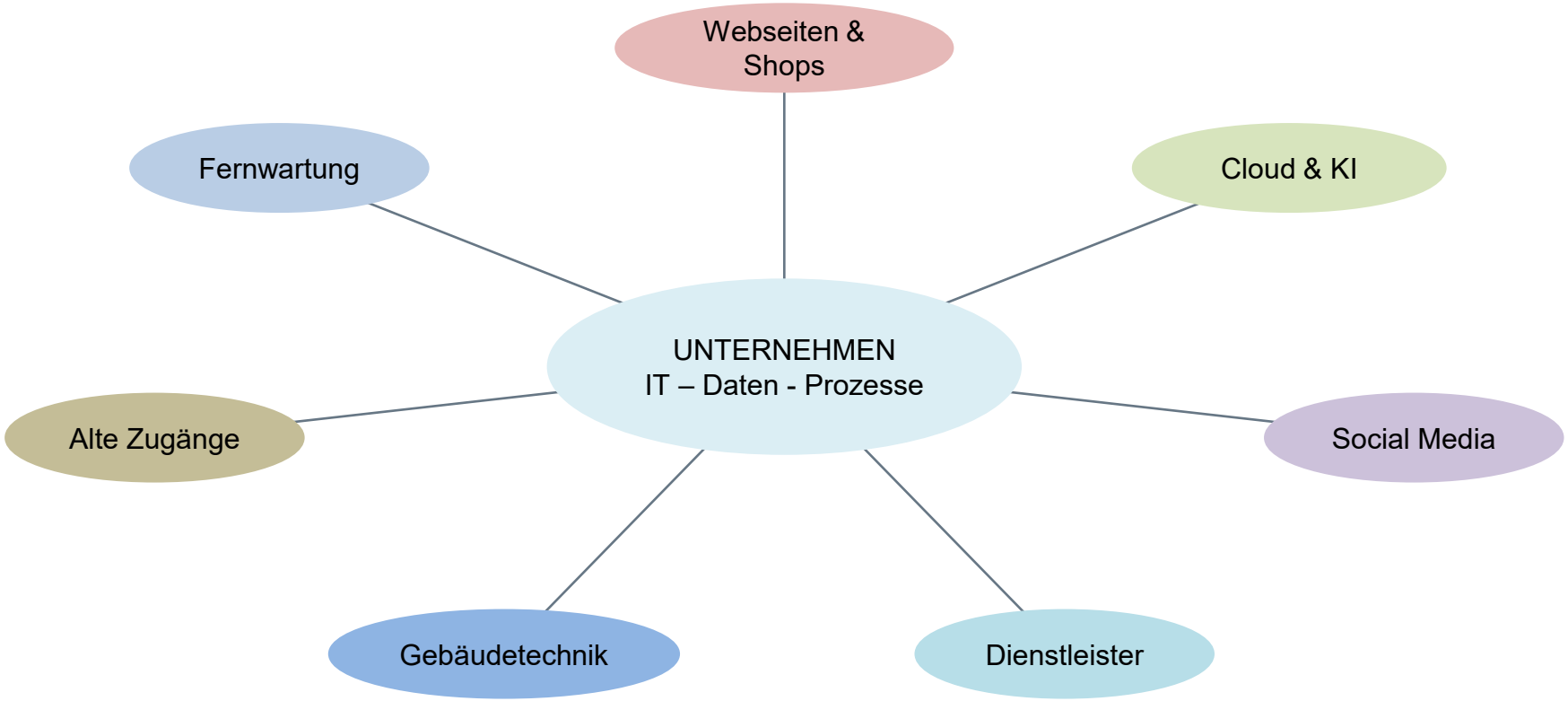
Grund: Unzureichende IT-Sicherheit.

Mit der gesetzlichen Verschärfung ab kommenden Herbst (NIS2) könnten die Hürden noch höher werden.“

Budget bestimmen:

KMUs benötigen ein Budget, das ihrem Risikoprofil entspricht – also ihre jeweiligen Bedürfnisse, wichtige Geschäftsinformationen sowie eventuell vorhandene, sensible Daten berücksichtigt. „Jedes Unternehmen sollte für sich selbst abwägen, wie viel es bereit ist zu investieren, um mögliche Betriebsunterbrechungen zu verhindern.“ – aber wie?

Und die Angriffsfläche ist größer als die eigene IT!



Und es geht noch weiter:

Regulierung	Fokus
AI Act (KI-VO)	Regulierung von KI-Systemen nach Risiko-Stufen (z. B. geringes, hohes, unannehmbares Risiko). Rechtsrahmen für einen sicheren und vertrauenswürdigen KI-Einsatz in Europa.
Data Act	Ermöglichung eines fairen Zugangs zu und einer fairen Nutzung von Daten in Europa. Verpflichtung für Unternehmen zur Datenbereitstellung in bestimmten Fällen..

Und es geht noch weiter:

Regulierung	Fokus
AI Act (KI-VO)	Regulierung von KI-Systemen nach Risiko-Stufen (z. B. geringes, hohes, unannehmbares Risiko). Rechtsrahmen für einen sicheren und vertrauenswürdigen KI-Einsatz in Europa.
Data Act	Ermöglichung eines fairen Zugangs zu und einer fairen Nutzung von Daten in Europa. Verpflichtung für Unternehmen zur Datenbereitstellung in bestimmten Fällen..

Fazit:

Unternehmen sind künftig nicht nur für die **Reaktion** auf Sicherheitsvorfälle verantwortlich, sondern auch für deren **Vermeidung** durch vorausschauende Planung, rechtliche Konformität und technische Robustheit.

Informationssicherheit ist damit nicht länger nur ein IT-Thema

– sondern ein strategischer Bestandteil moderner Unternehmensführung.

Wie komme ich dahin?

Wo stehe ich in der Informationssicherheit?

Standortbestimmung:

- Erster Schritt in die Informationssicherheit
- Basis für ISMS und Cybersecurity-Versicherung
- Gründliche Risikoanalyse und -bewertung mit 124 Prüfpunkten
- Ist eine NIS2-Betroffenheit gegeben?
- Habe ich die Einführung künstlicher Intelligenz (KI) unter Kontrolle?

Aufnahmen vor Ort - Ergebnis



Ausfallkosten - Beispielrechnung

- Mittelständisches Unternehmen mit 35 Mitarbeitern
- Ausfallzeit min. 1 Tag mit Produktionsstillstand

• 35 x 8 h x € 42,00 Lohnverrechnungssatz =	€ 11.760,00
• + externer EDV-Dienstleister ca.	€ 2.500,00
• Zwischensumme	€ 14.260,00
• + Umsatzausfall	€ 15.000,00

€ 29.260,00

Ausfallkosten - Beispielrechnung

- 118 PCs + 35 Notebooks = 153 Geräte
- Ausfallzeit min. 1 Tag, d. h. 153 Arbeitsplätze ohne Beschäftigung + weitere ca. 50 Mitarbeiter wegen Produktionsstillstand
- 200 x 8 h x € 42,00 Lohnverrechnungssatz = € 67.200,00
- + externer EDV-Dienstleister ca. € 2.500,00
- Zwischensumme € 69.700,00
- + Umsatzausfall € 174.000,00

€ 243.700,00

Daraus folgt:

Handlungsempfehlung:

- Umfangreicher Ergebnis- und Managementbericht (ca. 90 Seiten) mit Management Summary
- Empfehlungen für technische und organisatorische Maßnahmen
- Kosten-Nutzen-Analyse
  - Was kostet mich ein Ausfall?
  - Was ist eine angemessene Investition?

Fazit:

Der Standort ist jetzt klar.

Ein Kostengefühl stellt sich wieder ein.

Ein Investitionsbudget kann erstellt werden.

Die Kontrolle wurde zurückerlangt.

Bewusste Entscheidungen sind möglich.

Ersetze Glauben durch Wissen und Vertrauen durch Überprüfbarkeit!

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Gern!