DER INFOR Anwenderverein

NIS-2 trifft ERP

Was der neue Cyber-Standard für Infor-Anwender wirklich bedeutet

Online-Vortrag · 45 Minuten + Q&A

SACHVERSTÄNDIGENBÜRO MÜLOT

Ihr Referent

Denis Zensen

- Studium der Rechtswissenschaften (2. Staatsexamen)
- Langjährige Tätigkeit als zugelassener Rechtsanwalt und Fachanwalt
- Zertifizierter Datenschutzbeauftragter (TÜV-Rheinland)
- Zertifizierter Datenschutzauditor

Fachgebiete

- Datenschutz
- Compliance
- Kommunikation
- KI

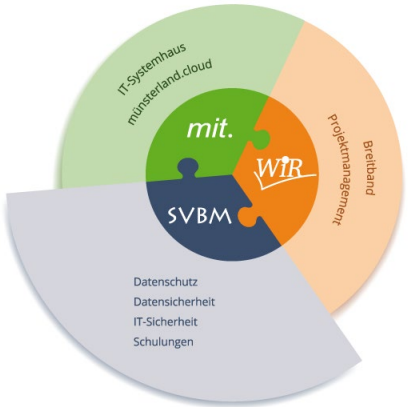
Spezialkompetenz(en)

- Verträge im Datenschutz
- Betroffenenrechte

Sachverständigenbüro Mülot GmbH

Wo kommen wir her?

- 1999 von Dirk-Michael Mülot als Einzelunternehmen gegründet
- 2018 Übergang in die Sachverständigenbüro Mülot GmbH mit Claus Wissing als Geschäftsführer
- Standorte in Greven und Langenberg



Was können wir?

- Über 20 Jahre Erfahrung in Datenschutz- und Datensicherheitsthemen nach DSGVO und kirchlichen Datenschutzgesetzen
- Starke Unternehmensgruppe für IT-Projektmanagement, Digitalisierung, Prozessautomatisierung, sichere Systemhauslösungen
- Insgesamt > 50 Beschäftigte mit Fachkompetenz (Ingenieure, Projektmanager, Rechtsanwälte, Planer, IT-Sicherheitsexperten, …)

25 Jahre Erfahrung und Lösungsorientierung

2024

- Ausweitung der innovativen Datenschutz-Dienste (Institut.com, VVT-Easy, DSMS-Dienste)
- Informationssicherheit (ISO 27001, Tisax, KRITIS, NIS2), Hinweisgeberschutz für verschiedenste Branchen
- Exzellente Dienstleistungen durch ausgebautes professionelles Datenschutz-Team
- Datenschutz- und Datensicherheitsthemen nach DSGVO und kirchlichen Datenschutzgesetzen

2018

- Übergang in die Sachverständigenbüro Mülot GmbH und weiterer Ausbau des Datenschutz-Teams
- Claus Wissing übernimmt die Geschäftsführung

1999-2018

- Stetige Erweiterung der Branchenberatung und Lehraufträge TÜV Rheinland sowie Fortbildungsakademie des Deutschen Caritasverbandes
- Tätigkeiten als „Freier Sachverständiger“ und Zertifizierung als Datenschutzbeauftragter und Datenschutzauditor
- Gegründet als Einzelunternehmen/Freiberufler durch Dirk-Michael Mülot

Über die Landesgrenzen hinaus tätig

Bisheriger Tätigkeitsradius:

EU-weit

- Für Unternehmen in Deutschland und deren Schwestergesellschaften

Europaweit/außerhalb der EU:

- Als Datenschutzvertretung nach Art. 27 DSGVO für Unternehmen außerhalb der EU, welche innerhalb der EU am Markt tätig sind
- In Zusammenarbeit mit Schwesterfirmen und Partner:innen wie der WiR Projects GmbH oder der datenschutzguide.ch GmbH in der Schweiz

International:

- Für international aufgestellte Mandant:innen, die z. B. Geschäftsbereiche oder Konzernmuttergesellschaften in den USA oder in anderen Drittländern haben

Typische Branchen unserer Kunden/Mandanten

Herstellende Industrie:

- Automobilindustrie (incl. Prototypenbau)
- Industrielle Fertigung, Maschinenbau
- Logistik, Reedereien, Distribution

Konsumgüter:

- Bekleidung und Mode
- Lebensmittel und Getränkeindustrie

Gesundheitswesen:

- Versicherungen, Kliniken, Arztpraxen
- Pflegeeinrichtungen

Finanzwesen:

- Versicherungen, Banken, Immobilienwesen

Soziale Organisationen:

- Kirchliche Träger: Bistümer, Kirchliche Gemeinden, Caritasverbände
- Sportverbände, Sportvereine

Bildungseinrichtungen:

- Große Träger der Erwachsenenbildung zur Sensibilisierung

Willkommen zum heutigen Stammtisch

Infos zur Durchführung

Regeln

- Die Mikrofone sind bitte ausgeschaltet, können aber von bei Bedarf eingeschaltet werden.
- Meldungen bitte über Handzeichen.
- Fragen – auch zur Technik – bitte in den Chat schreiben.

Unterlagen

- Foliensatz steht am Ende zur Verfügung.
- Feedback steht anschließend zur Verfügung.

Hinweis:
Das Web-Seminar wird **nicht** aufgezeichnet. Aufzeichnungen durch die Teilnehmenden sind **nicht** erlaubt!

Agenda

1. **Tag 9 ohne ERP – Aufwachen**
2. **Wer ist betroffen?**
3. **NIS-2 in Klartext (kurz!)**
4. **NIS-2 trifft Ihr ERP**
5. **5 typische Schwachstellen**
6. **Branchen-Cockpit**
7. **Was tun ab Montag?**

1 Tag 9 ohne ERP

Ein realer Fall

Maschinenbauer · 280 Mitarbeiter · Infor LN

Tag 1	Tag 2	Tag 3	Tag 9	Woche 6
Ransomware	**Stillstand**	**Restore?**	**System läuft**	**Bilanz**
Eintritt über kompromittierte Wartungs-VPN eines Dienstleisters.	ERP · MES · Dateisysteme verschlüsselt. Produktion steht.	Backup existiert. Reihenfolge wurde nie geprobt.	Grundsystem da. Aufträge wandern bereits ab.	Schaden 4,2 Mio. €. Ein Stammkunde verloren.

Live-Frage an Sie

Bitte ehrlich antworten

Wie viele Tage übersteht Ihr Unternehmen ohne funktionierendes ERP?

A	B	C	D
1 Tag	2 – 3 Tage	5+ Tage	Weiß ich nicht

⚠ **REALITÄT**

21 Tage Median bis zur vollen Wiederherstellung bei vergleichbaren Vorfällen

Quelle: BSI Lagebericht 2024 · Coveware Q4/2024

Die Bedrohungslage in Zahlen

BSI-Lagebericht 2025 · Berichtszeitraum Juli 2024 – Juni 2025

950

Ransomware-Angriffe

im Berichts-zeitraum vom BSI registriert

80 %

davon trafen KMU

kleine und mittlere Unternehmen

119

neue Schwachstellen

pro Tag bekannt – +24 % YoY

Quelle: BSI – Die Lage der IT-Sicherheit in Deutschland 2025 (medien.bsi.bund.de/lagebericht)

2 Wer ist betroffen?

Zwei Klassen — beide hochrelevant

Schwellen · Sektoren · Bußgelder im Direktvergleich

BESONDERS WICHTIG

Für Konzerne und KRITIS-nahe Häuser

≥ 250 Mitarbeiter

≥ 50 Mio. € Umsatz

11 Hoch-Kritikalitäts-Sektoren

10 Mio. € oder 2 % Konzernumsatz Bußgeld

BEISPIELE

Energie · Wasser · Gesundheit · Verkehr · Banken · IKT

WICHTIG

Für den klassischen Mittelstand

≥ 50 Mitarbeiter

≥ 10 Mio. € Umsatz

18 Sektoren

7 Mio. € oder 1,4 % Konzernumsatz Bußgeld

BEISPIELE

Maschinenbau · Fahrzeugbau · Chemie · Lebensmittel · Post · Forschung

Der 30-Sekunden-Selbsttest

Drei Fragen — wenn zweimal „Ja", sind Sie sehr wahrscheinlich dabei

1 Mein Unternehmen hat mehr als 50 Mitarbeiter ODER mehr als 10 Mio. € Umsatz.

2 Wir fertigen physische Produkte, betreiben kritische Lieferketten oder verarbeiten Lebensmittel / Chemie.

3 Wir liefern an mindestens einen Kunden, der selbst KRITIS oder „besonders wichtig" ist.

→ Zweimal „Ja" = Sie sind betroffen (direkt oder über die Lieferkette).

Auch „indirekt" Betroffene werden über NIS-2-Klauseln ihrer Großkunden mitgezogen.

Sie sind auch über die Lieferkette betroffen

Selbst wenn Sie nicht direkt unter NIS-2 fallen

1

GROSSKUNDEN

reichen die Pflichten weiter

OEMs und KRITIS-Betreiber müssen die Sicherheit ihrer Lieferanten nachweisen — und reichen NIS-2 1:1 in Lieferverträge ein.

2

TISAX / ISO 27001

werden zu Pflichtklauseln

Cyber-Anforderungen werden Bestandteil von Lieferantenverträgen, Rahmenvereinbarungen und Audits.

3

WETTBEWERBSFAKTOR

wer kann, gewinnt

Wer NIS-2 nachweislich erfüllt, qualifiziert sich für Großaufträge — wer nicht, verliert sie still und leise.

4

CYBER-VERSICHERUNG

verlangt Reifegrad

Cyber-Policen werden seit 2024 nur noch mit NIS-2-konformem Mindeststandard gezeichnet.

3 NIS-2 in Klartext (kurz!)

Drei Sätze zum Recht

Mehr brauchen Sie heute nicht — den Rest übersetzen wir gleich ins ERP

1

IN KRAFT.

Das NIS2-Umsetzungsgesetz (NIS2UmsuCG) gilt seit dem 6. Dezember 2025.

Registrierungsfrist beim BSI lief bis 6. März 2026.

2

PFLICHTEN AB TAG 1.

Risikomanagement · Meldepflicht 24h / 72h / 1 Monat · Schulung · Nachweise.

Keine Übergangsfrist.

3

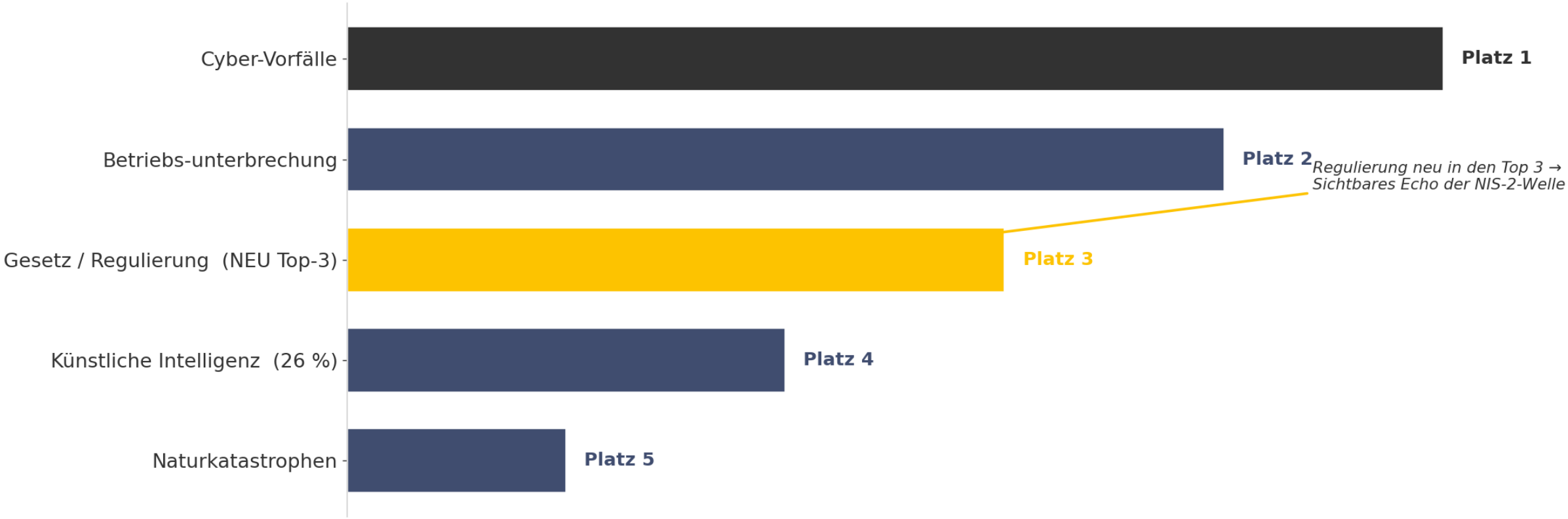
GESCHÄFTSFÜHRUNG HAFTET PERSÖNLICH.

Delegierbar ist die Aufgabe, nicht die Verantwortung.

Bußgeld bis 10 Mio. € oder 2 % weltweiter Konzernumsatz.

Top-Geschäftsrisiken in Deutschland 2026

Allianz Risk Barometer 2026 · 400 Befragte aus Deutschland



Quelle: Allianz Risk Barometer 2026, Deutschland-Ergebnis · commercial.allianz.com

SVBM · NIS-2 trifft ERP

Die 10 Mindestmaßnahmen

§ 30 BSIG-neu · Heute zur Orientierung — gleich in der ERP-Übersetzung

1

Risikoanalyse

Sicherheitskonzept & Lagebild

2

Vorfallsbewältigung

Erkennen · Reagieren · Wiederherstellen

3

BCM & Backup

Geschäftsfortführung & Datensicherung

4

Lieferkette

Sicherheit bei Lieferanten & Dienstleistern

5

Entwicklung & Wartung

Sichere Software & Patch-Disziplin

6

Wirksamkeit

Messen, ob es funktioniert

7

Cyber-Hygiene

Schulung & Awareness

8

Kryptografie

Verschlüsselung & Schlüsselmanagement

9

IAM & Asset

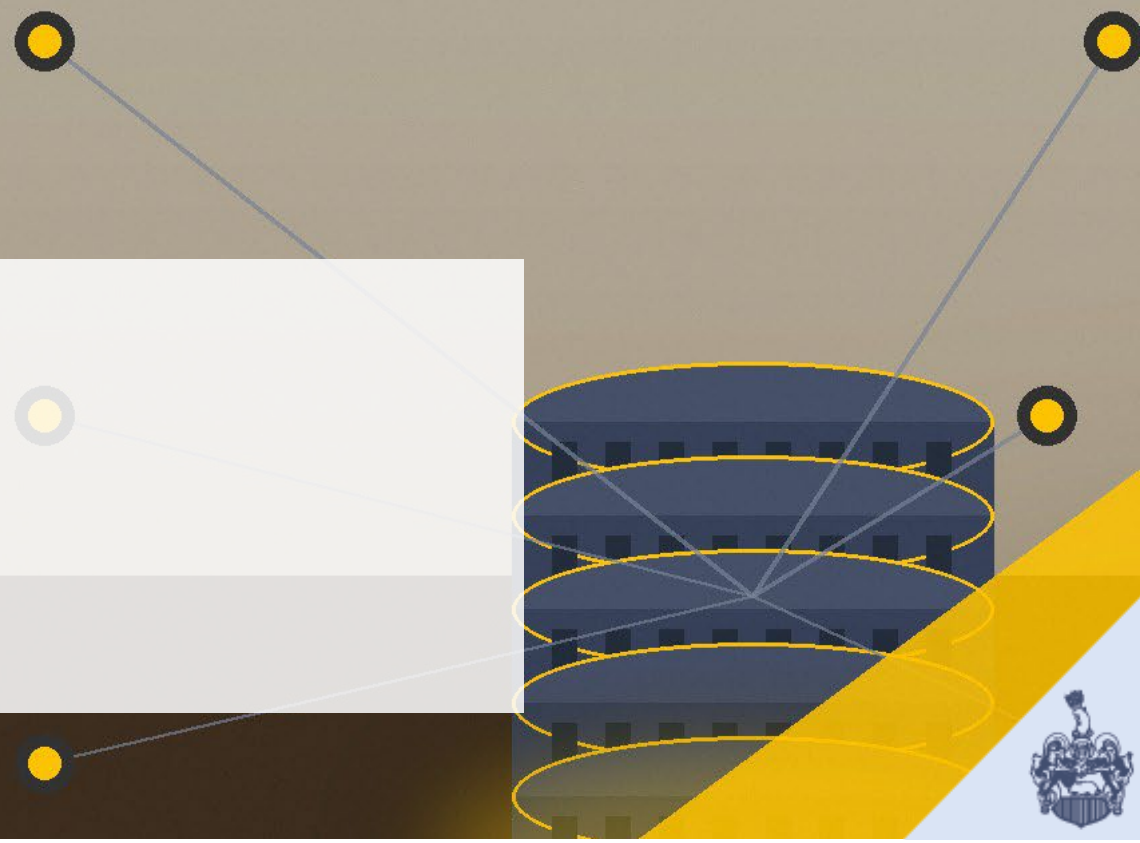
Identitäten · Rollen · Bestand

10

Authentisierung

MFA & gesicherte Kommunikation

4 NIS-2 trifft Ihr ERP



Infor-Universum & Verantwortung

Wo Sie selbst stehen — und wo Infor steht

PRODUKTFAMILIE

Wo Sie als Anwender stehen können

- **Infor LN**
  CloudSuite Industrial Enterprise · Maschinenbau
- **Infor M3**
  CloudSuite Fashion · F&B · Distribution · Chemicals
- **Infor LX / System21**
  IBM i · klassischer Mittelstand
- **Infor SyteLine / CSI**
  Mongoose-basiert · Auftragsfertigung
- **Infor OS**
  ION · IDM · Ming.le · Birst · IFS-SSO

INFOR VERANTWORTET

in der CloudSuite-Welt

- Infrastruktur · Compute · Storage · Netzwerk
- Plattform-Sicherheit · Patching der Basis
- Datenbank-Härtung & -Backup
- SOC 2 / ISO 27001-Zertifizierungen

SIE VERANTWORTEN

— auch in der Cloud!

- Identitäten · Rollen · Privileged Accounts
- Customizing · Mods · Eigenentwicklungen
- Daten · Stammdaten · Schnittstellen
- Vorfallsbewältigung · NIS-2-Nachweise

Die 10 Pflichten im ERP

Teil 1 von 2 · Wo Sie wahrscheinlich heute schon scheitern

1 **RISIKOANALYSE**
Ist das ERP als „Kronjuwel" beschrieben — oder nur als „Server unter vielen"?

2 **VORFALLSBEWÄLTIGUNG**
Wer entscheidet Sonntag 03:00 Uhr „Notbetrieb oder Stopp"?

3 **BCM & BACKUP**
Restore mit Stoppuhr geprobt? Wiederanlauf-Reihenfolge dokumentiert?

4 **LIEFERKETTE**
Wie viele permanente Berater-Admins haben Sie aktuell? Mit MFA?

5 **SICHERE ENTWICKLUNG**
LN-Sessions · M3-Mods · Mongoose — wann zuletzt sicherheitsreviewed?

Die 10 Pflichten im ERP

Teil 2 von 2 · Hier holen Sie die schnellsten Erfolge

6 **WIRKSAMKEIT**
Welche ERP-spezifischen KPIs misst Ihr CISO heute?

7 **CYBER-HYGIENE**
Wann hatten Power-User und Admins zuletzt eine ERP-Awareness-Schulung?

8 **KRYPTOGRAFIE**
ION-Verbindungen mit TLS 1.2+? Backups verschlüsselt?

9 **IAM / ASSET MGMT**
Rollenkonzept · SoD · Rezertifizierung · Joiner-Mover-Leaver — alles produktiv?

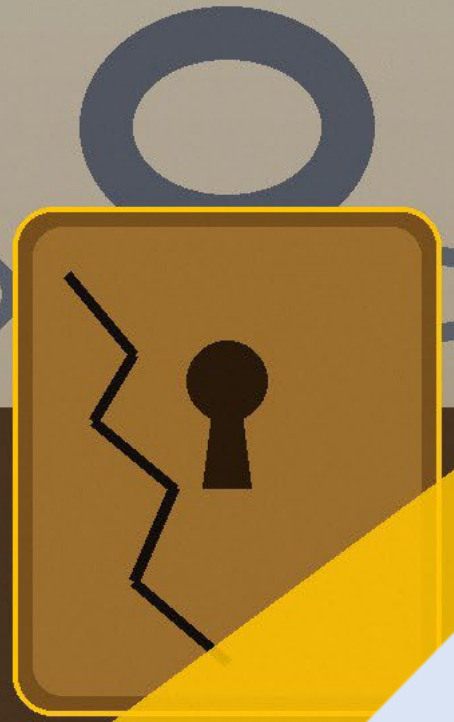
10 **AUTHENTISIERUNG**
MFA für ALLE ERP-Zugänge — auch Service-Konten und Partner?

Die Selbst-einschätzungs-Lücke

Wahrnehmung vs. Realität bei kleinen und mittleren Unternehmen

Quelle: BSI-Lagebericht 2025 · Erfüllungsgrad gemessen am BSI-CyberRisikoCheck (Basisanforderungen)

5 Die 5 typischen Schwachstellen



Schwachstelle 1: Der ewige Admin

Story · Warum jetzt Pflicht · Lösung

STORY

Was wir typischerweise sehen

Externer LN-Berater hat seit 2014 produktiven Admin-Account im ERP. Niemand kennt das Passwort, MFA gibt es nicht.

WARUM PFLICHT

Welche NIS-2-Maßnahme greift

Lieferkettensicherheit + sichere Authentisierung. Ein kompromittierter Berater-Account kompromittiert das ganze ERP.

LÖSUNG

Was Sie konkret tun

Just-in-Time-Zugänge über PAM. MFA-Pflicht für alle Externen. Vierteljährliche Rezertifizierung. Vier-Augen-Freigabe.

Schwachstelle 2: Wir customizen seit 2008

Story · Warum jetzt Pflicht · Lösung

STORY

Was wir typischerweise sehen

M3-Anwender mit 250+ aktiven H5-Mods. Niemand kennt mehr alle sicherheitsrelevanten. Updates seit drei Jahren ausgesetzt.

WARUM PFLICHT

Welche NIS-2-Maßnahme greift

Sichere Entwicklung und Cyber-Hygiene. Unpatched ERP ist heute ein dokumentierter NIS-2-Verstoß.

LÖSUNG

Was Sie konkret tun

Mod-Inventur mit Risiko-Scoring. CloudSuite-Standard zuerst, Mods nur wenn unverzichtbar. Patch-Strategie mit Wartungsfenstern.

Schwachstelle 3: Backup haben wir doch

Story · Warum jetzt Pflicht · Lösung

STORY

Was wir typischerweise sehen

Lebensmittelhersteller, LX auf IBM i. Backup-Job läuft täglich, Logs prüft niemand. Beim Krisentest funktioniert der Restore, aber niemand kennt die Reihenfolge.

WARUM PFLICHT

Welche NIS-2-Maßnahme greift

BCM und Backup. Es zählt der nachgewiesene Wiederanlauf, nicht das Vorhandensein von Bändern.

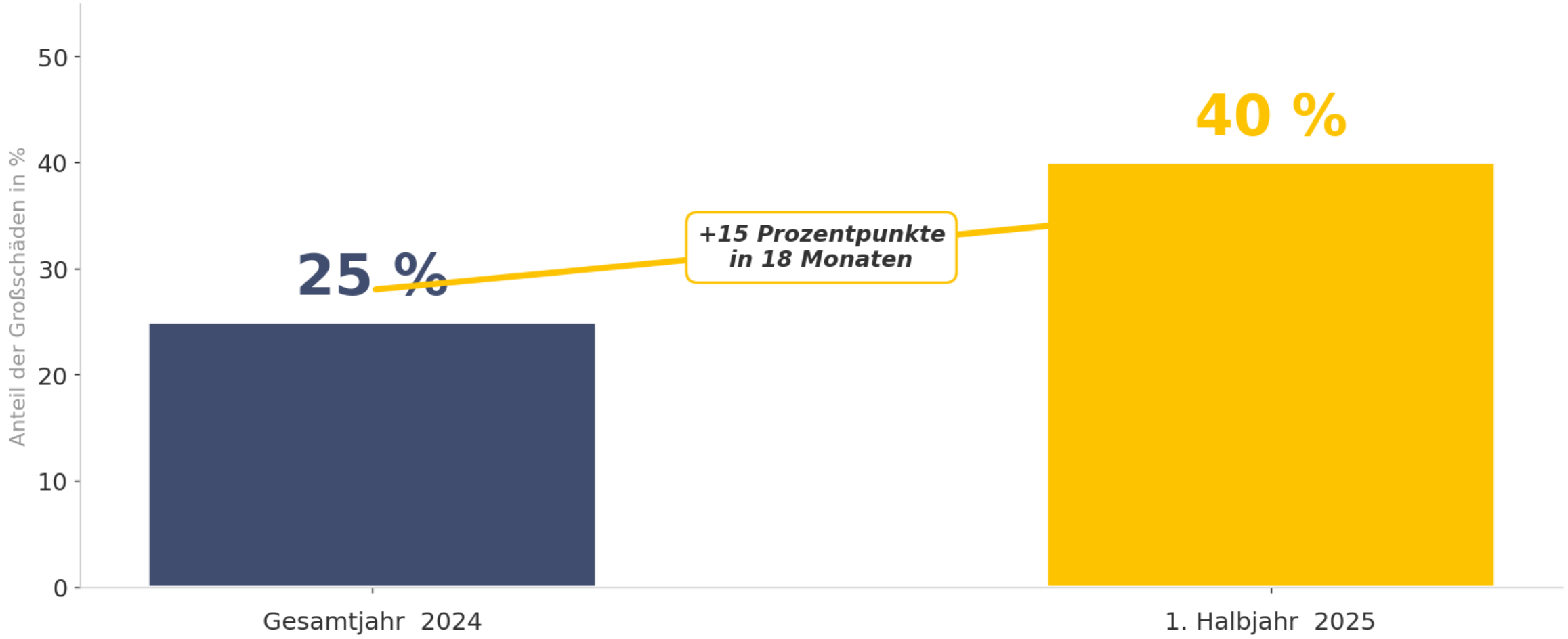
LÖSUNG

Was Sie konkret tun

Restore-Drill mit Stoppuhr mindestens zweimal pro Jahr. Wiederanlauf-Reihenfolge dokumentieren und üben. Immutable Backup-Ziele mit Object Lock.

Doppel-Erpressung wird zur Norm

Anteil großer Cyber-Schäden (>1 Mio. €) mit Datendiebstahl



„Backup haben wir doch" reicht nicht mehr – die Daten sind ohnehin bereits abgeflossen.

Quelle: Allianz Cyber Risk Trends 2025 · Allianz Commercial · H1-2025-Schadensdaten

Schwachstelle 4: Die Schnittstellen kennt nur Hr. Müller

Story · Warum jetzt Pflicht · Lösung

STORY

Was wir typischerweise sehen

Anlagenbauer mit 47 ION-Schnittstellen zu MES, CRM, BI, EDI. Authentifizierung mit Service-Accounts und statischen Passwörtern. Wissen bei einer Person.

WARUM PFLICHT

Welche NIS-2-Maßnahme greift

Gesicherte Kommunikation und Asset Management. Bus-Faktor 1 ist ein klassischer Audit-Befund.

LÖSUNG

Was Sie konkret tun

Schnittstellen-Inventur. Rotation der Service-Tokens. Wechsel auf zertifikatsbasierte Authentifizierung. SIEM-Anbindung. Wissens-Doubling.

Schwachstelle 5: Wer ruft das BSI an?

Story · Warum jetzt Pflicht · Lösung

STORY

Was wir typischerweise sehen

Freitag 17:30 Uhr: massenhaft fehlgeschlagene Logins gegen Infor OS. Niemand weiß, ob das schon ein erheblicher Vorfall ist. Wer entscheidet? Wer meldet binnen 24 Stunden?

WARUM PFLICHT

Welche NIS-2-Maßnahme greift

Vorfallsbewältigung und Meldepflicht. 24 Stunden vergehen über das Wochenende sehr schnell.

LÖSUNG

Was Sie konkret tun

Vorfalls-Playbook mit klaren Eskalationsstufen. 24/7-Erreichbarkeit intern oder MSP. Vorlagen für die BSI-Frühwarnung. Regelmäßige Tabletop-Übungen.

6 Branchen-Cockpit

Sechs Branchen, sechs Bedrohungsbilder

Wo Ihre Branche steht — kompakt

Maschinenbau

Infor LN · CSI

⚠ TOP-RISIKO

Fernwartung & Engineering-Zugänge

Lebensmittel

Infor M3 F&B

⚠ TOP-RISIKO

OT-/IT-Kollision · 24/7-Patching

Chemie

Infor M3 / LN

⚠ TOP-RISIKO

Rezeptur-Abfluss · alte Steuer-OS

Mode

Infor M3 Fashion

⚠ TOP-RISIKO

Filialen · Saison-Patches

Auto · Diskret

Infor LN · LX · CSI

⚠ TOP-RISIKO

EDI-Service-Accounts · IBM-i

Distribution

Infor M3 / LX · WMS

⚠ TOP-RISIKO

Preisstamm · Aushilfen · Portale

Vertiefung: Maschinen- & Anlagenbau

Wo NIS-2 Ihre Service- und Engineering-Welt trifft

SETUP

Was Sie typischerweise haben

- Infor LN, oft On-Premise oder Single-Tenant
- Tiefe CAD-/PLM-/MES-Integration
- Hoher Customizing-Anteil (LN-Sessions, DAL)

KRONJUWELEN

Was Ihr ERP wirklich schützt

- ETO-Projekte & Auftragsabwicklung
- Stücklisten & Konfigurationen
- Service-Verträge mit installierter Basis
- Exportkontrolle & Embargo-Prüfung

QUICK WINS

Was Sie in 90 Tagen tun

1. Engineering-VLAN vom ERP-Netz trennen
2. MFA + JIT-Zugänge für Service-Partner
3. Fernwartungs-Konzept mit 4-Augen-Prinzip
4. LN-Customizing-Inventur & Risiko-Scoring
5. Exportkontroll-Workflow als KPI

Vertiefung: Lebensmittel & Getränke

Wenn das ERP 24/7 läuft und ein Rückruf droht

SETUP

Was Sie typischerweise haben

- Infor M3 F&B, produktiv 24/7
- Wiegezellen, Etikettendrucker, Linien
- Catchweight, Chargen, MHD, Allergene
- EDI an LEH und Großhandel

KRONJUWELEN

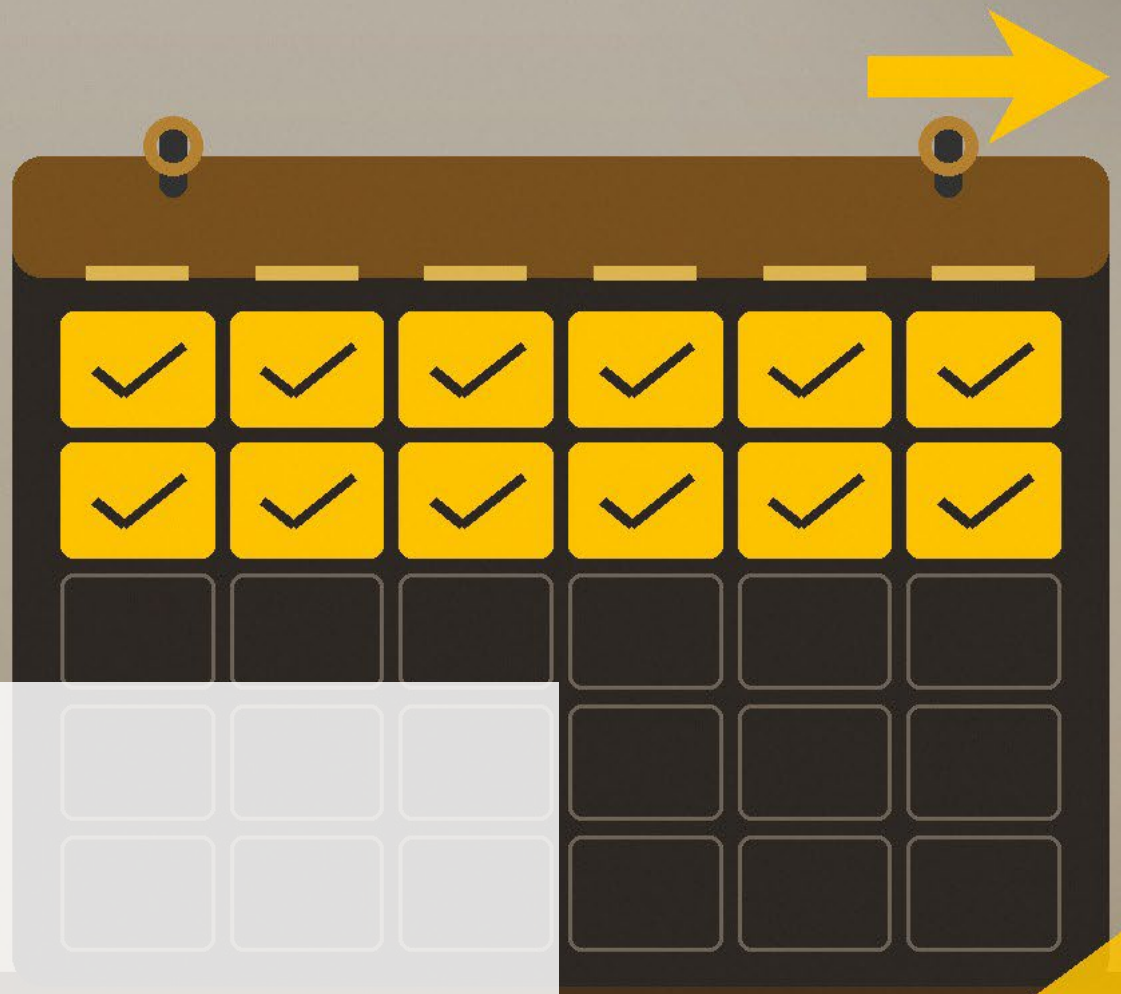
Was Ihr ERP wirklich schützt

- Rückverfolgbarkeit (Forward/Backward)
- Rezepturen & Spezifikationen
- HACCP-relevante Datenflüsse
- JIT-Lieferung an LEH

QUICK WINS

Was Sie in 90 Tagen tun

1. OT-/IT-Segmentierung mit Übergängen
2. Rolling Maintenance Windows definieren
3. Chargen-Integrität: Hash-Prüfungen
4. EDI: Zertifikate statt statischer Passwörter



7 Was tun ab Montag?

Die 90-Tage-Roadmap

Zu kurz für Ausreden, zu lang für Aktionismus

1

Woche 1

KLARHEIT

NIS-2-Verantwortlichen benennen, BSI-Registrierung prüfen.

2

Woche 2-3

BESTANDSAUFNAHME

ERP-Assets, Schnittstellen, Zugänge, Mods, Backup-Status.

3

Woche 4-5

QUICK WINS

MFA für Admins + Service-Partner. Default-Passwörter ändern.

4

Woche 6-8

PROZESSE

ERP-Vorfalls-Playbook, Tabletop-Übung mit GF, Lieferantenklauseln.

5

Woche 9-10

TECHNIK

Restore-Drill mit Stoppuhr, Patch-Strategie, SIEM-Anbindung.

6

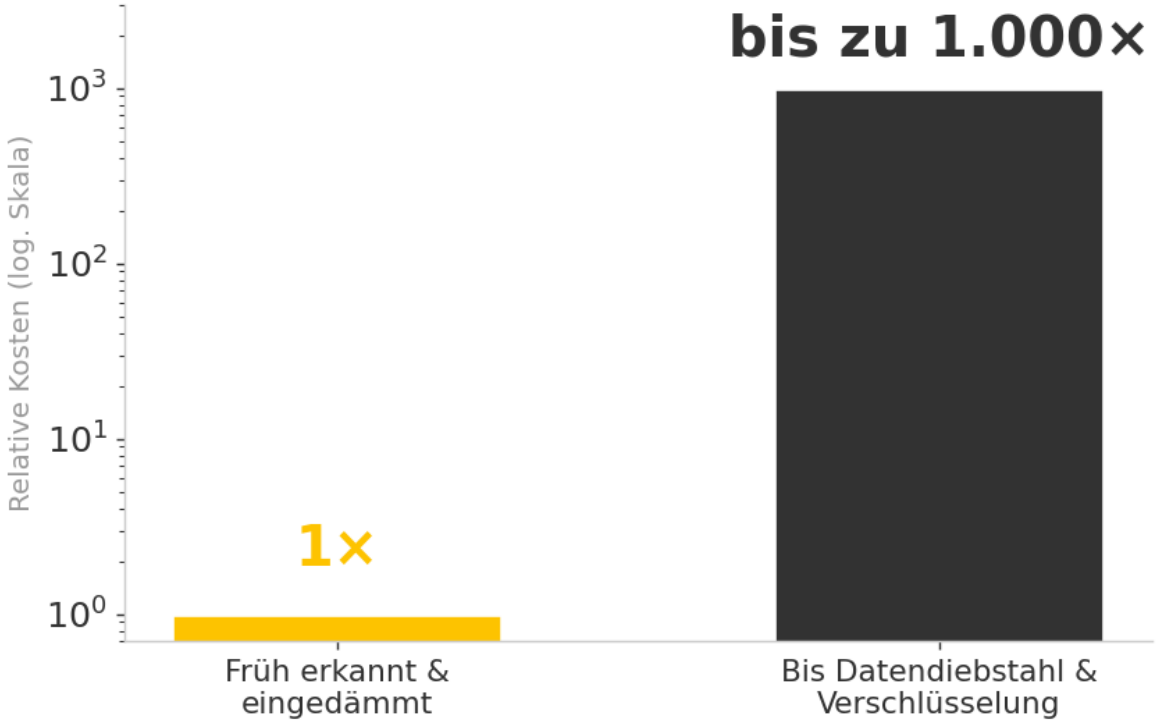
Woche 11-12

WIRKSAMKEIT

GF-Report mit KPIs. Nächste 90-Tage-Welle planen.

Was Früherkennung wirklich wert ist

Wirkung verbesserter Detection- und Response-Fähigkeiten



-50 %
Höhe der großen Cyber-Schäden

-30 %
Häufigkeit der großen Cyber-Schäden

in der ersten Jahreshälfte 2025, zurückgeführt von Allianz Commercial auf bessere Erkennung und Reaktion.

Quelle: Allianz Cyber Risk Trends 2025 - Allianz Commercial - Michael Daum, Global Head of Cyber Claims

Die 5 Fragen für diese Woche

Foto-Folie zum Mitnehmen — ein Gespräch pro Frage

1 AN DIE GESCHÄFTSFÜHRUNG

Wer ist bei uns formal für NIS-2 zuständig — und seit wann?

2 AN DIE IT-LEITUNG

Wann haben wir zuletzt einen ERP-Restore geprobt — und wie lange hat er gedauert?

3 AN DIE INFOR-ACCOUNT-MANAGER

Welche NIS-2-relevanten Informationen und Templates stellt Infor uns bereit?

4 AN DIE SERVICE-PARTNER

Welche Berater-Accounts in unserem System sind aktiv — und welche davon haben MFA?

5 AN DIE SICH SELBST

Wenn morgen ein Vorfall passiert: Wer ruft binnen 24 h das BSI an, mit welcher Vorlage?

Drei Sätze für unterwegs

Wenn Sie nur drei Sätze mitnehmen — diese hier

> **NIS-2 ist kein IT-Projekt.**
>
> Es ist ein Geschäftsführungs-Thema — und das ERP ist der Beweis dafür.

> **Vier von fünf Schwachstellen sind organisatorisch.**
>
> Disziplin schlägt Budget.

> **90 Tage reichen für 80 % Risikoreduktion.**
>
> Den Rest baut man iterativ — Quartal für Quartal.

Noch Fragen?

SACHVERSTÄNDIGENBÜRO MÜLOT GMBH

Datenschutz | Datensicherheit | Forensische Informatik

Risikomanagement | ISO27001

Grüner Weg 80
48268 Greven

Tel.: 02571/5402 0
info@svb-muelot.de

www.svb-muelot.de