"DAS IT-NETZWERK MEINES UNTERNEHMENS IST SICHER." GANZ SICHER?

Ein realistischer Blick auf IT-Sicherheit in KMU
XPoint Anwendertagung 2025

Andre Gastreich.

Über mich

Beruf

Geschäftsführer dng IT GmbH & Co. KG
Datenschutzbeauftragter (IHK)
Informationssicherheitsbeauftragter (IHK)
IT-Notfallmanager (IHK)

Privat

45 Jahre
Verheiratet
Vater von 4 Kindern

dng IT . Wenden

www.dng.de

Gründung: 2001

17 Mitarbeiter:innen

Spezialisten für RZ-Lösungen und IT-Security

Die Ortsbestimmung.

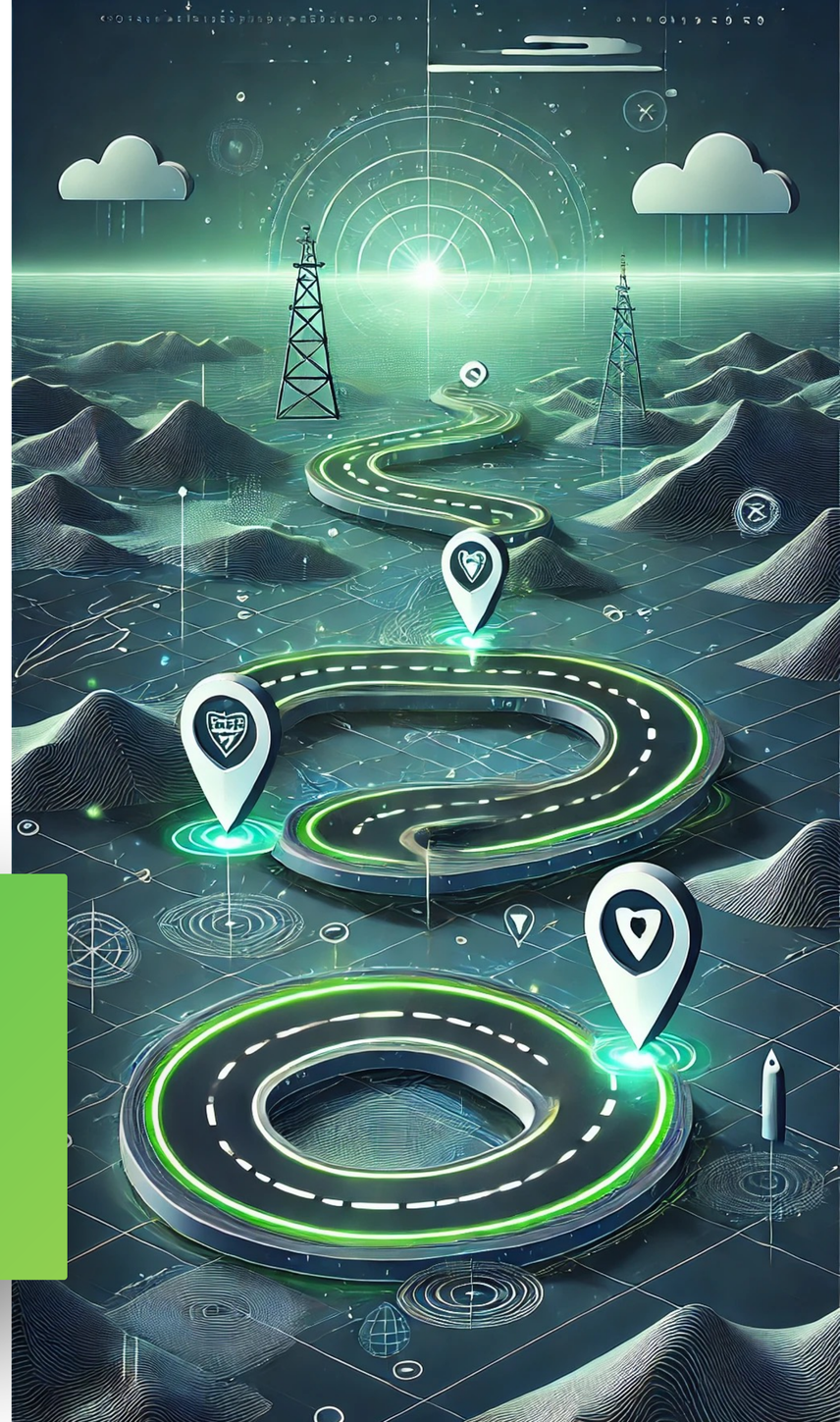
Wo befinden Sie sich auf der Route?

A Gut vorbereitet
Wir haben eine sichere Route und kennen die Abkürzungen.

B Teils, teils
Wir sind unterwegs, aber die Straße ist holprig.

C Wir sind noch am Start
Wir wissen, dass IT-Sicherheit wichtig ist, aber haben wenig umgesetzt.

> Wie schätzen Sie Ihre aktuelle IT-Sicherheit ein?



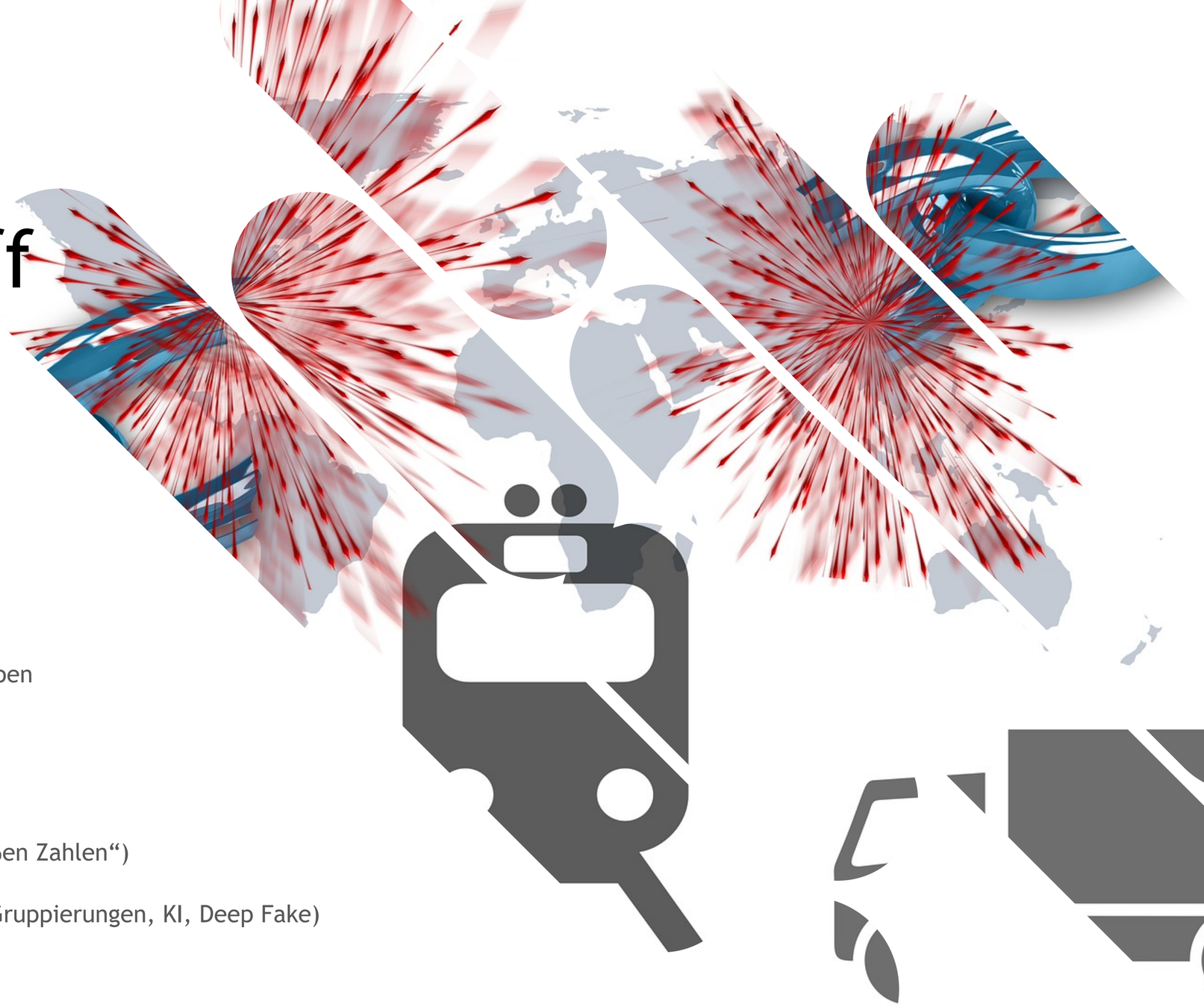
WER ist betroffen?

Ein Blick auf die aktuelle Bedrohungslage

Jährliche Schäden in Höhe von 267 Milliarden Euro
8 von 10 Unternehmen Opfer von Datendiebstahl und Sabotage

Gezielter Angriff vs. Phishing

„Das betrifft uns doch nicht“



Gezielter Angriff

Staatliche Akteure oder Hackergruppen
Ziel: Industriespionage, Sabotage

Phishing

Massenangriffe („Die Macht der großen Zahlen“)
Über 90% aller Angriffe per eMail
Professionalisierung der Angreifer (Gruppierungen, KI, Deep Fake)
Ziel: Erpressung, Geld erbeuten

"DAS IT-NETZWERK MEINES UNTERNEHMENS IST SICHER."

"DAS IT-NETZWERK MEINES UNTERNEHMENS IST SICHER." GANZ SICHER?

Was ist der nächste Schritt?

Achtung, Ohrwurm!

„Ich hab ‘ne Zwiebel in der IT, ich bin sicher“

EDR

Firewall

Patch-Management

Technische Maßnahmen

Backup

MFA

Awareness-Schulungen

Risikoanalyse

Phishing-Simulationen

Organisatorische Maßnahmen

Richtlinien

Notfallpläne

Alles in die Cloud?

Cyber-Versicherung

Absicherung - kein Ersatz für IT-Sicherheit

Abdeckung

Schutz bei finanziellen Schäden
Kostenübernahme für Forensik und Wiederherstellung
Selten Erstattung von Lösegeld

Grenzen

Keine Deckung ohne „Stand der Technik“
Indirekte Schäden sind nicht abgedeckt

Sinnvoll?

Finanzielle Absicherung im Worst Case
IT-Sicherheit bleibt Eigenverantwortung

Checkliste

- Bestandsaufnahme und Risikoanalyse
- MFA für alle kritischen Konten aktivieren
- Phishing-Trainings für die Mitarbeiter
- Patch-Management sicherstellen
- Schwachstellenscans regelmäßig durchführen
- Backup-Strategie entwerfen und umsetzen
- Restore-Tests durchführen
- Security-Monitoring und Protokollierung aktivieren
- Notfallplan erstellen

VIELEN DANK

Jetzt starten statt warten

www.dng.de