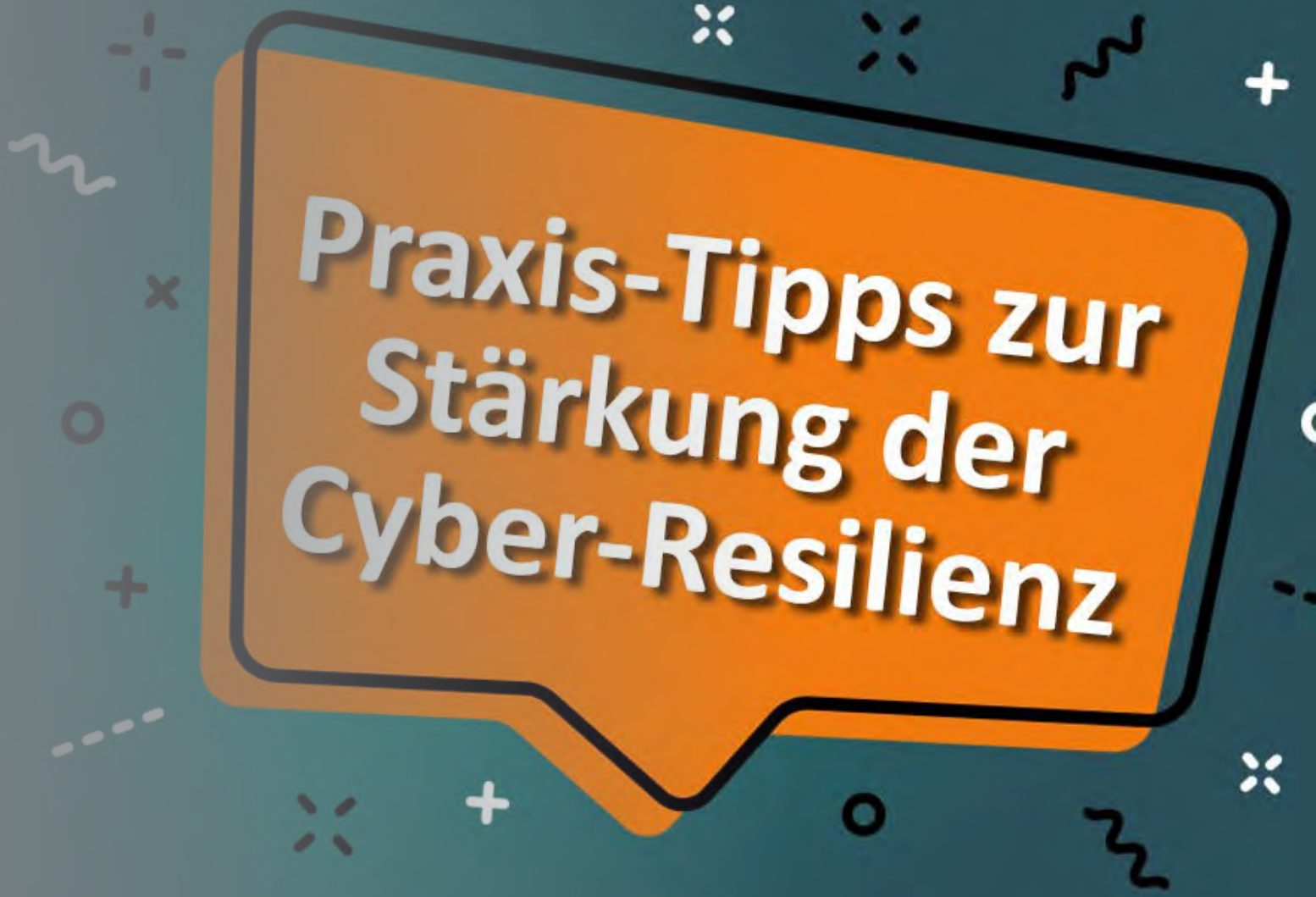
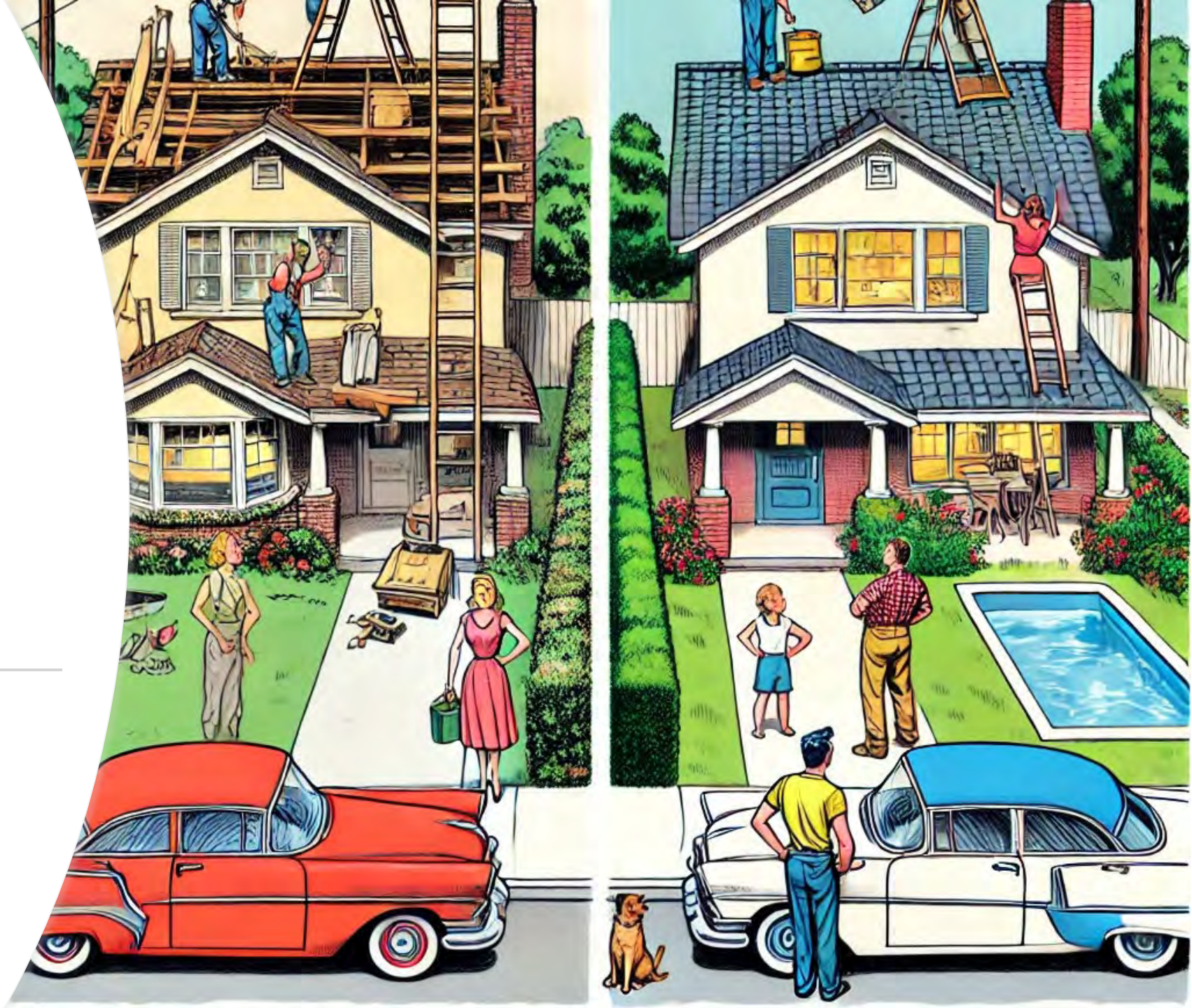
LUNCH + LEARN: Stärkung der Cyber-Resilienz in der Praxis

23.09.2024 ICN GmbH + Co. KG



DIGITALE WOCHE DORTMUND

Entscheiden, was einem wichtig ist…



… und es bestmöglich schützen!

Andere interessieren sich für Ihre Prioritäten!

Praxis-Tipps zur Stärkung der Cyber-Resilienz

Michael Brinkmann

- **Alter:** 41 Jahre
- **Position:** Operations Manager
- **Erfahrung:** Technikaffiner Manager mit 15 Jahren Erfahrung in der IT-Betreuung und Entwicklung von KMUs bis hin zu Enterprise-Kunden.
- Spezialisiert auf adressatgerechte Kommunikation und Compliance.

ICN
...mit Sicherheit IT!

Agenda

- **Praxis Tipp 1:** Kommen Sie ins Handeln
- **Definition:** Cyber-Resilienz – Was steckt dahinter?
- **Praxis Tipp 2:** Bestandsaufnahme und Risikoermittlung
- **Praxis Tipp 3:** Orientierung am BSI-Grundschutz
- **Praxis Tipp 4:** Maßnahmen umsetzen – 10 Quick Wins für mehr Sicherheit
- **Praxis Tipp 5:** Kontinuierliche Prüfung und Nachverfolgung
- **Tool-Vorstellung:** SecurNotix
- **Zusammenfassung:** Die wichtigsten Punkte im Überblick

Praxis Tipp 1:
Kommen Sie ins Handeln

Praxis Tipp 1: Kommen Sie ins Handeln

- Identifizieren Sie Ihre Kronjuwelen - „Was ist das Wertvollste in Ihrem Unternehmen?
- Diese Frage ist der Ausgangspunkt jeder Cyber-Resilienz-Strategie.
- **Beispiele:**
  - Sensible Kundendaten?
  - Ihre innovativen Entwicklungsprozesse? (Rezepte, Kalkulationen, usw.)
  - Oder vielleicht Ihre gesamte IT-Infrastruktur?

- Der erste Schritt zur Stärkung Ihrer Cyber-Resilienz ist die genaue Identifikation dessen, was für Ihr Unternehmen besonders schützenswert ist.
- Schaffen Sie somit Transparenz und Klarheit – die Bedeutung dieses Wertes wird drastisch zunehmen!

Definition:

Cyber-Resilienz – Was steckt dahinter?

Definition: Was bedeutet Cyber-Resilienz?

- Cyber-Resilienz beschreibt die Fähigkeit eines Unternehmens, auf Cyberangriffe vorbereitet zu sein, diese abzuwehren, sich schnell davon zu erholen und aus diesen Angriffen zu lernen.

- Es geht nicht nur um den reinen Schutz vor Angriffen, sondern auch um die Fähigkeit, den Betrieb nach einem Angriff schnellstmöglich wieder aufzunehmen.

- In einer immer stärker digitalisierten Welt ist Cyber-Resilienz eine der zentralen Herausforderungen für Unternehmen.

Praxis Tipp 2:
Bestandsaufnahme und Risikoermittlung

Praxis Tipp 2: IST-Aufnahme und Risiko

- Bevor Sie Sicherheitsmaßnahmen umsetzen können, sollten Sie eine möglichst gründliche Bestandsaufnahme Ihrer IT-Landschaft und der bestehenden Risiken durchführen.

- Fragen Sie sich: Welche Systeme habe ich im Einsatz? Welche Daten verarbeite ich? Wo liegen mögliche Schwachstellen?

- Eine sorgfältige Risikoermittlung ist unerlässlich, um angemessene Schutzmaßnahmen zu implementieren.

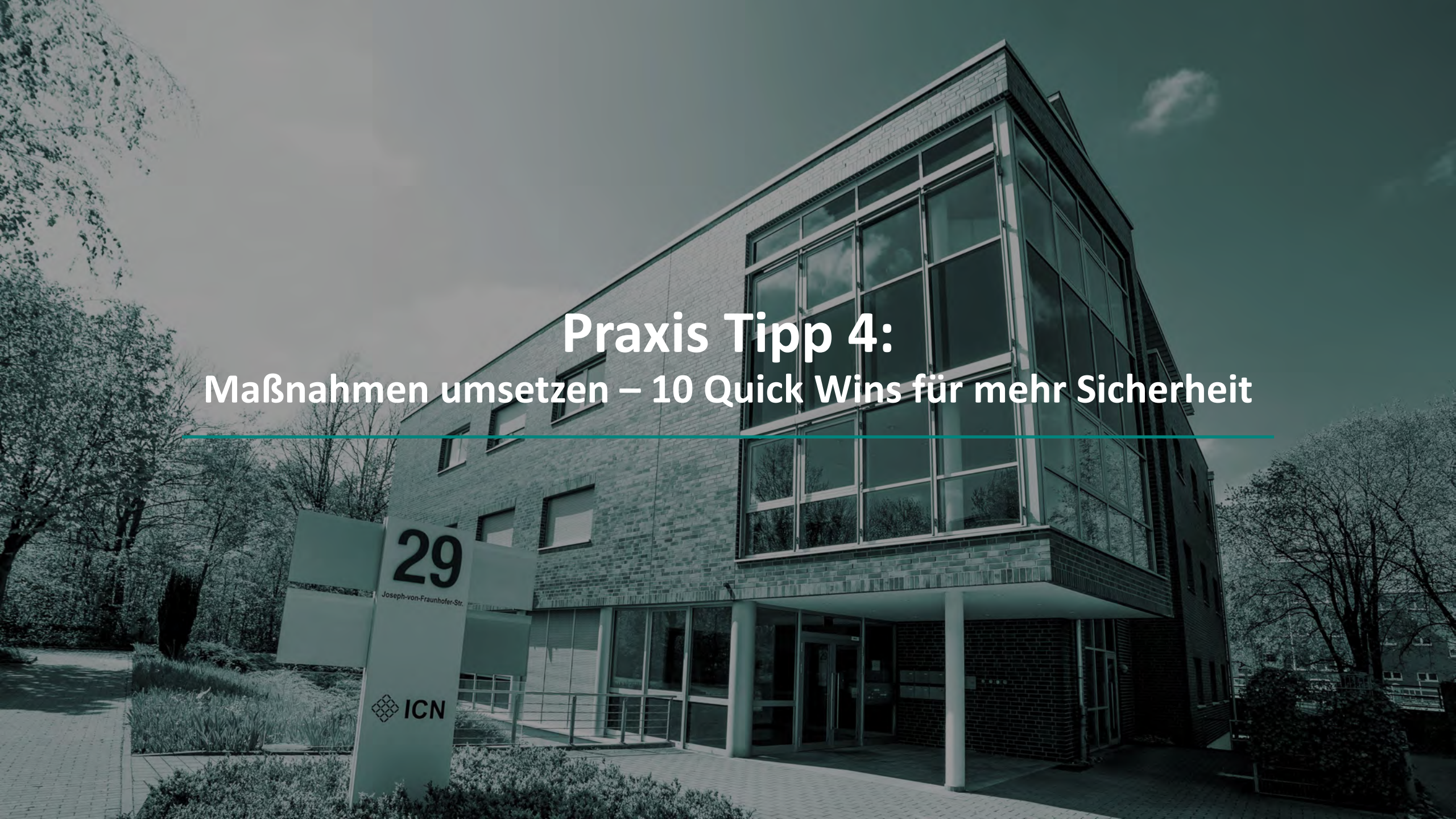
Praxis Tipp 3:
Orientierung am BSI-Grundschutz

Praxis Tipp 3: Orientierung am BSI (WIBA)

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit dem IT-Grundschutz einen umfassenden Rahmen, an dem Sie sich orientieren können.

- Neben den konkreten Handlungsempfehlungen ist das BSI auch die offizielle Meldestelle für Sicherheitsvorfälle – hier sind Sie also gut aufgehoben, wenn es um die Umsetzung von Schutzmaßnahmen geht.

- Besonders empfehlenswert ist der Katalog des BSI zum Weg in die Basisabsicherung (WIBA), der Ihnen hilft, erste wichtige Schritte zu gehen und dabei grundlegende Maßnahmen systematisch umzusetzen.



Praxis Tipp 4:

Maßnahmen umsetzen – 10 Quick Wins für mehr Sicherheit

Praxis Tipp 4: Maßnahmen – 10 Quick Wins

1. Multifaktor-Authentifizierung (MFA) einführen

- Durch die Einführung der Multifaktor-Authentifizierung erhöhen Sie die Sicherheit von Benutzerkonten sofort. Selbst wenn Passwörter kompromittiert werden, bietet die zweite Authentifizierungsstufe einen effektiven Schutz.

2. Regelmäßige Datensicherungen (Backups) einrichten und extern lagern

- Richten Sie automatisierte, regelmäßige Backups Ihrer wichtigen Daten ein.
- Lagern Sie diese Backups außerhalb des Unternehmens, damit sie im Falle eines Cyberangriffs oder einer Systemstörung sicher sind.

Praxis Tipp 4: Maßnahmen – 10 Quick Wins

3. Verschlüsselung sensibler Daten

- Stellen Sie sicher, dass alle sensiblen Daten, insbesondere Kundeninformationen und finanzielle Daten, sowohl im Ruhezustand als auch bei der Übertragung verschlüsselt werden.

4. Antiviren- und Antimalware-Software installieren und regelmäßig aktualisieren

- Verwenden Sie zuverlässige Antiviren- und Antimalware-Software auf allen Clients und Servern und sorgen Sie dafür, dass diese regelmäßig aktualisiert wird, um neue Bedrohungen abzuwehren.

5. Sicherheitsupdates und Patches zeitnah einspielen

- Stellen Sie sicher, dass alle Betriebssysteme, Anwendungen und Geräte regelmäßig auf dem neuesten Stand sind, indem Sie Sicherheitsupdates und Patches zeitnah einspielen. Veraltete Software ist eine häufige und absolut vermeidbare Angriffsfläche.

Praxis Tipp 4: Maßnahmen – 10 Quick Wins

6. Netzwerksegmentierung

- Durch die Segmentierung Ihres Netzwerks in verschiedene Bereiche (z.B. Trennung von internen und externen Netzwerken) können Sie die Auswirkungen eines Angriffs eingrenzen. So wird es für Angreifer schwerer, sich frei im Netzwerk zu bewegen.

7. Sicherheitsrichtlinien für Passwörter

- Implementieren Sie strikte Richtlinien für Passwörter, die Mindestanforderungen an Komplexität und Länge beinhalten. Setzen Sie zudem regelmäßige Passwortwechsel durch, um die Wahrscheinlichkeit von Angriffen zu minimieren.

Praxis Tipp 4: Maßnahmen – 10 Quick Wins

8. E-Mail-Filterung und Schutz vor Phishing

- Richten Sie fortschrittliche E-Mail-Filter ein, um Phishing-Mails und schädliche Anhänge automatisch zu blockieren. Schulungen für Mitarbeiter zur Erkennung von Phishing-Versuchen sind ebenfalls entscheidend.

9. Zugriffsrechte beschränken (Prinzip der geringsten Privilegien)

- Gewähren Sie Mitarbeitern und externen Dienstleistern nur den minimal notwendigen Zugriff auf Systeme und Daten. Dadurch wird das Risiko verringert, dass ein Angriff großen Schaden anrichten kann.

Praxis Tipp 4: Maßnahmen – 10 Quick Wins

10 . Schulung und Sensibilisierung der Mitarbeiter

- Organisieren Sie regelmäßige Schulungen und Sensibilisierungskampagnen für Ihre Mitarbeiter, um das Bewusstsein für Cyber-Sicherheitsrisiken zu erhöhen.
- Gut informierte Mitarbeiter sind oft die erste Verteidigungslinie gegen Angriffe wie Phishing. Mitarbeiter ohne diese Wahrnehmungsfähigkeit sind im Gegenzug eine Achillesferse.

Praxis Tipp 5:
Kontinuierliche Prüfung und Nachverfolgung

Praxis Tipp 5: Kontinuierliche Prüfung

- Cyber-Resilienz ist kein Einmal-Projekt, sondern ein fortlaufender Prozess.

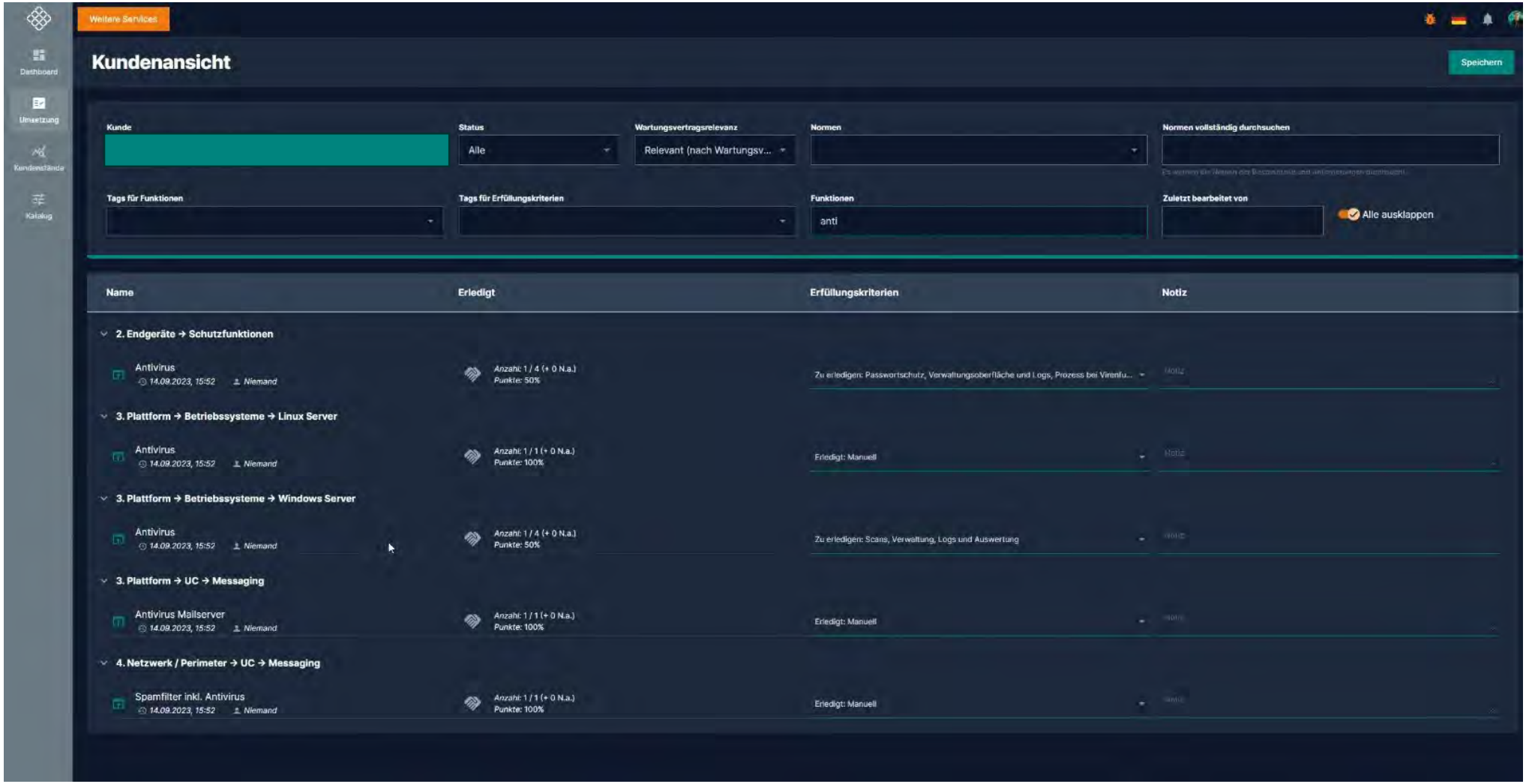
- Regelmäßige Überprüfungen Ihrer Sicherheitsmaßnahmen und deren Aktualisierung sind unerlässlich, um neue Bedrohungen abzuwehren.

- Dabei kann Ihnen das Tool SecurNotix helfen

Bleiben Sie dran!

Tool-Vorstellung:
SecurNotix

SecurNotix – Strukturiertes Vorgehen



Zusammenfassung:
Die wichtigsten Punkte im Überblick

Die wichtigsten Punkte auf einen Blick

- Cyber-Resilienz beginnt mit dem Erkennen Ihrer **Kronjuwelen** – den schützenswertesten Aspekten Ihres Unternehmens.
- **Bestandsaufnahme** und **Risikoermittlung** sind der Schlüssel, um passende Maßnahmen zu ergreifen.

- Der BSI-Grundschutz (**WIBA-Katalog**) bietet eine verlässliche Orientierung.

- Stellen Sie sicher, dass Sie die Basisthemen (**Quick Wins,** wie Multifaktor-Authentifizierung, Verschlüsselung und regelmäßige Backups) im Griff haben.

- **Bleiben Sie dran!** – Cyber-Resilienz ist ein kontinuierlicher Prozess. Tools wie **SecurNotix** helfen Ihnen dabei, Ihre Maßnahmen systematisch umzusetzen und fortlaufend zu prüfen.

Danke für ihre Aufmerksamkeit