Checkliste: 7 Fragen, die jeder Geschäftsleiter sich stellen muss

1. Was bedeutet es für die wirtschaftliche Situation meines Unternehmens konkret, wenn die gesamte IT für vier Wochen ausfällt?

Je näher sie der Antwort „Es steht komplett still“ kommen, desto höher der Handlungsbedarf.

2. Erbringt mein Unternehmen oder einer meiner Kunden Leistungen in einer der folgenden Branchen?

- Energie
- Verkehr/Transport
- Finanzwesen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Raumfahrt
- Post- und Kurierdienste
- Abfallwirtschaft
- Chemische Industrie
- Lebensmittelproduktion
- Maschinenbau

Dann könnte es, abhängig von weiteren Parametern, möglich sein, dass ihr Unternehmen von der neuen NIS-2-Richtlinie betroffen ist.

3. Verfügen wir bereits über ein strukturiertes Informationssicherheitsmanagementsystem (ISMS)?

Wenn ja, erfüllen sie bereits eine der zentralen Anforderungen der NIS-2-Richtlinie. Es gibt jedoch weitere, wie zum Beispiel das Training des Managements, die Registrierung beim BSI oder die Etablierung von Meldeprozessen.

4. Haben wir ein aktuelles Risikomanagement, dass alle kritischen Geschäftsprozesse abdeckt und uns eine Priorisierung von Maßnahmen zur Erhöhung der Sicherheit erlaubt?

Die Identifikation der Risiken und der systematische Umgang damit sind wichtige Bausteine der IT Sicherheit.

5. Ist die Geschäftsleitung aktiv in das Thema Cybersicherheit eingebunden und ausreichend informiert?

Genau das ist ein zentraler Punkt der neuen Anforderungen. Das Thema ist nicht mehr delegierbar. Eine kompetente Beratung kann den Aufwand für die Geschäftsleitung jedoch spürbar verringern.

6. Wie gut sind unsere Mitarbeiter für Informationssicherheit sensibilisiert und geschult? (Phishing, Passwortsicherheit, Umgang mit sensiblen Daten etc.)

Die meisten Angriffe laufen nicht auf der technischen Ebene ab, sondern nutzen kleine menschliche Schwächen aus. Das richtige Training kann diese Lücke sehr viel kleiner machen.

7. Haben wir unsere kritischen Systeme, Daten und Dienstleistungen vollständig identifiziert und priorisiert?

Man kann nur schützen, was man kennt. Ein präzises Asset Management ist die Basis und Voraussetzung fast aller Maßnahmen der IT Sicherheit.

Jetzt Kennenlerngespräch vereinbaren