NIS-2: was Sie jetzt tun können, um gut vorbereitet zu sein

- [ ] **Ist Ihr Unternehmen von der NIS-2-Richtlinie betroffen?**
Überprüfen Sie, ob Ihr Unternehmen einem der betroffenen Wirtschaftssektoren zugerechnet werden könnte und beachten Sie dabei eventuelle Unklarheiten bei der Klassifizierung. Berücksichtigen Sie außerdem die Schwellenwerte für die Unternehmensgröße: grundsätzlich sind nur mittlere und große Unternehmen betroffen. Es gibt jedoch Ausnahmen!

- [ ] **Erhalten Sie einen Überblick über die NIS-2-Anforderungen und mögliche Sanktionen**
Prüfen Sie eingehend die Mindeststandards gemäß den EU-Richtlinien für NIS-2 und gewährleisten Sie deren Einhaltung. Es ist wichtig, dass die Geschäftsführung über die beiden Sanktionstypen von NIS-2 informiert wird:
1. hohe und vordefinierte Bußgelder
2. Haftung von Geschäftsführern sowie C-Level-Führungskräften im Unternehmen.

- [ ] **Identifizieren Sie kritische Infrastrukturen und bewerten Sie deren Sicherheitsniveau**
Ihre kritischen Geschäftsprozesse und sensible Daten müssen besonders geschützt werden. Haben Sie auch Notfall- und Wiederherstellungspläne nach Angriffen auf Ihre Infrastruktur parat?
Führen Sie zudem eine Lückenanalyse durch, um Schwachstellen der IT-Sicherheit zu identifizieren.

- [ ] **Planen und budgetieren Sie notwendige Ausgaben**
Berücksichtigen Sie nicht nur die Ausgaben für die Einhaltung der NIS-2-Richtlinien, sondern planen Sie auch Mittel für proaktive Investitionen in digitale Abwehrmaßnahmen ein.

- [ ] **Bewerten Sie Ihre Lieferketten-Sicherheit**
Stellen Sie sicher, dass Ihre Lieferanten die NIS-2-Richtlinie ebenfalls einhalten und geeignete Maßnahmen treffen, um sich vor Cyberkriminellen zur schützen.

- [ ] **Reduzieren Sie Risiken und entwickeln Sie Pläne für den Umgang mit Sicherheitsvorfällen**
Risikomanagement ist ein zentraler Bestandteil eines ISMS und steht daher auch im Fokus der NIS-2-Richtlinie. Durch effektives Risikomanagement können potenzielle Gefahren frühzeitig erkannt, bewertet und behandelt werden, um Cyberbedrohungen für Ihr Unternehmen wirksam zu bekämpfen.

- [ ] **Definieren Sie klare Verantwortlichkeiten und führen Sie Schulungen für Mitarbeitende durch**
Legen Sie klare Rollen und Verantwortlichkeiten für Cybersicherheit, Informationssicherheit und Business Continuity-Management fest. Sensibilisieren Sie darüber hinaus Ihre Mitarbeitenden und schulen Sie diese für Verhaltensweisen im Umgang mit Cyberbedrohungen und Phishing-Attacken.

UNSER TIPP!
Implementieren Sie klare Reporting-Strukturen, um alle Beteiligten über Fortschritte und Herausforderungen zu informieren und Transparenz zu fördern.

SIE BENÖTIGEN UNTERSTÜTZUNG?
Wir begleiten Sie auf dem Weg NIS-2-konform zu werden.

MELDEN SIE SICH BEI UNS!

Die TechniData IT-Service GmbH ist ein Full-Service-Anbieter von hochwertigen IT-Dienstleistungen für mittlere und große Unternehmen sowie öffentliche Auftraggeber vorwiegend aus Süddeutschland. Das Portfolio umfasst IT-Services und -Support, Cloud Services, Management von IT-Infrastrukturen sowie IT-Consulting. TechniData IT-Service ist Teil der TechniData IT-Gruppe

TechniData IT-Service GmbH ■ Planckstraße 1 ■ 88677 Markdorf ■ info@technidata-its.de ■ www.technidata-its.de