TerraXaler und NIS-2

Wie hilft der terraXaler konkret bei der Erfüllung der Anforderungen von NIS-2 an den Betrieb von IT-Infrastrukturen in Unternehmen, Körperschaften, Einrichtungen und Verbänden.

Die NIS-2-Richtlinie (Network and Information Systems Direktive) der Europäischen Union stellt erweiterte Anforderungen an die Cybersicherheit und den Schutz kritischer Infrastrukturen. Die Richtlinie baut auf der ursprünglichen NIS-Richtlinie auf und zielt darauf ab, ein höheres Maß an Cyberresilienz in der EU zu erreichen. Nachfolgend sind hier die wichtigsten Anforderungen der NIS-2 an den Betrieb von IT-Infrastrukturen in Unternehmen, Körperschaften, Einrichtungen und Verbänden aufgelistet:

1. Risikomanagement und Sicherheitsmaßnahmen

- **Risikobewertung**: Regelmäßige Bewertung der Risiken für die Netz- und Informationssys teme.
- Sicherheitsmaßnahmen: Implementierung von technischen und organisatorischen Maßnah men zur Risikominderung, einschließlich:
  - **Netzwerksicherheit**: Schutz der Netzwerke vor Angriffen.
  - **Zugriffskontrollen**: Sicherstellen, dass nur autorisierte Personen Zugang zu den Systemen haben.
  - **Datenintegrität**: Schutz der Daten vor unbefugter Veränderung oder Verlust.
  - **Verschlüsselung**: Verschlüsselung von Daten, um ihre Vertraulichkeit zu gewährleisten.
  - **Notfallpläne**: Erstellen von Notfallplänen und Durchführung regelmäßiger Übungen.

2. Vorfallmanagement

- **Meldepflicht**: Verpflichtung zur Meldung von sicherheitsrelevanten Vorfällen an die zustän digen Behörden (z.B. nationale Cybersicherheitsbehörden) innerhalb von 24 Stunden nach Erkennung.
- Reaktionsfähigkeiten: Implementierung von Prozessen zur schnellen Reaktion auf Sicher heitsvorfälle, einschließlich:
  - **Erkennung**: Fähigkeit zur Erkennung von Sicherheitsvorfällen.
  - **Reaktion**: Maßnahmen zur Eindämmung und Behebung der Vorfälle.
  - **Berichterstattung**: Dokumentation und Berichterstattung über Vorfälle und ergriffene Maßnahmen.

3. Sicherheitskultur und Ausbildung

- **Sensibilisierung**: Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter bezüglich Cyberrisiken und Sicherheitsmaßnahmen.
- **Verantwortlichkeiten**: Klare Zuweisung von Verantwortlichkeiten für die Cybersicherheit innerhalb der Organisation.

4. Kooperation und Informationsaustausch

- **Zusammenarbeit**: Verpflichtung zur Zusammenarbeit mit anderen Unternehmen und staatlichen Stellen im Bereich Cybersicherheit.
- **Informationsaustausch**: Aktiver Austausch von Informationen über Bedrohungen und Sicherheitsvorfälle mit anderen Betroffenen und relevanten Akteuren.

5. Governance und Audit

- **Sicherheitsstrategie**: Entwicklung und Implementierung einer umfassenden Cybersicherheitsstrategie.
- **Audit und Kontrolle**: Regelmäßige Überprüfung und Audits der Sicherheitsmaßnahmen und protokolle.
- **Berichtswesen**: Regelmäßige Berichterstattung über den Status der Cybersicherheit an die Geschäftsleitung und gegebenenfalls an externe Aufsichtsbehörden.

6. Compliance und Sanktionen

- **Einhaltung der Vorschriften**: Sicherstellung, dass alle Anforderungen der NIS-2-Richtlinie erfüllt werden.
- **Strafen**: Klare Definition von Sanktionen und Bußgeldern bei Nichteinhaltung der Vorschriften.

Diese Anforderungen sollen sicherstellen, dass Unternehmen und Organisationen in der EU besser auf Cyberbedrohungen vorbereitet sind und ihre Netz- und Informationssysteme wirksam schützen können. Es ist wichtig, dass alle betroffenen Akteure die NIS-2-Richtlinie sorgfältig umsetzen, um die Cybersicherheit auf einem hohen Niveau zu gewährleisten.

Wie hilft hier der terraXaler?

Der terraXaler löst die 3 von 5 der geforderten techn. und organisatorischen **Sicherheitsmaßnahmen**, nämlich

- ☑ **Netzwerksicherheit**: Schutz der Netzwerke vor Angriffen.
- ☑ **Zugriffskontrollen**: Sicherstellen, dass nur autorisierte Personen Zugang zu den Systemen haben.
- ☑ **Datenintegrität**: Schutz der Daten vor unbefugter Veränderung oder Verlust.

Im **Vorfallmanagement** verschafft TerraXaler die **Reaktion**sfähigkeit, sehr schnell wieder arbeitsfähig zu sein und trotzdem die verschlüsselten Daten vorzuhalten, was im Bereich Kooperation und Informationsaustausch sowohl mit Versicherungen als auch mit staatlichen Stellen im Bereich der Cybersicherheit dazu beiträgt, trotz eigener Arbeitsfähigkeit die verschlüsselten Daten und Informationen für Forensik und Cyberabwehr bereitstellen zu können.