Zentrum für
Risiko- & Krisenmanagement

Positionspapier:

„NIS 2 – die neue Cybersecurity Richtlinie“ der Europäischen Union

Autor: **Dipl.-Ing. Johannes GÖLLNER, MSc**

Globalisierung, Digitalisierung und Automatisierung sind die Treiber für eine **holistischen Betrachtung der Verletzbarkeit der Supply Chain und seiner Netzwerke** (Basic-, Supply- und Public Networks) **-in Beziehung zum CYBER-Raum und zu Cyber-Events.** Unter Berücksichtigung der Einbettung in transnationale und internationale Versorgungssysteme (Energie, Rohstoffe, Lebensmittel, medizinische Verbrauchsgüter, Informationen, etc.), die durch politische, rechtliche, ökonomische, zivile, technische, sowie Natur- und Umweltereignissen, „man-made“ und „non man-made“ zu Unterbrechungen und Engpässen in der Versorgung führen können, ist eine holistische Betrachtung die essentielle Grundlage zur Entwicklung von Strategien für Risikoreduktion und Resilienz-Design in der Supply Chain und ICT/CYBER Security. ICT/CYBER-Ereignis-/Bedrohungsbilder, die zu Unterbrechungen und Engpässen in der regionalen, nationalen, supranationalen und internationalen Versorgung bzw. Lieferkette beitragen können sind in Korrelation zu Supply Chain Unterbrechungen in das Risk Assessment mit einzubinden.

Die Entwicklung von **risikoreduzierenden Strategien und Resilienz Strategien** für **physische und digitale Supply und Value Chains und Verbindung mit deren Supply Chain Networks** *(Strategische [Kritische Infrastrukturen] Infrastrukturen)* bedürfen Innovationen bei qualitativen und quantitativen Konzepten, Modellen, Methoden und Werkszeugen im Bereich Risk Assessment sowie Modeling und Simulation, um den Grad der erforderlichen Resilienz der Supply und Value Chain auf staatlicher und unternehmerischer Ebene festzustellen, um zur Strategie- und Produkt-Entwicklung positiv und wertschöpfend beitragen zu können.

Das Erarbeiten eines umfassendes und ganzheitliches Cyber Security & Supply Chain Resilience (Security) Monitoring, -Rating und -Auditing Konzeptes, weil **Cyber Events** *(weltweit: **34%**; AT: **40%**; GE: **40%**; CH: **57%**)* und **Supply Chain Interruptions-Betriebsunterbrechungen** *(weltweit: **34%**; AT: **32%**; GE: **46%**; CH: **41%**)* zu den 10 weltweit größten Risiken gehören[1], wird Unternehmen, KMU und auch öffentliche Verwaltung ab 2024 und in den Folgejahren massiv herausfordern.

Die internationale Standardisierung, vertreten durch ISO (International Organisation for Standardization, Genf), hat bereits **2007** mit der Herausgabe von Supply Chain Security-Standards[2,3,4] reagiert und die Relevanz dokumentiert.

Bereits 2018 hat das National Cyber Security Centre, U.K. den thematischen Zusammenhang zwischen Supply Chain Security und Cyber Security dokumentiert und veröffentlicht (siehe u.a. Bild).

---

[1] siehe „Allianz Global Corporate & Specialty in Allianz Risk Barometer 2023: Die 10 größten Geschäftsrisiken 2023, weltweit”.

[2] ISO 28000 (Specification for security management systems for the supply chain), First edition: 2007-09-15; aktueller Stand: ISO 28000:2022; Revision in Vorbereitung.

[3] ISO 28001 (Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans Requirements and Guidance), First edition 2007-10-15;

[4] ISO 20858 (Ships and marine technology — Maritime port facility security assessments and security plan development), First edition 2007-10-15; aktueller Stand: ISO 20858:2012;

Der supranationalen Gesetzgeber (EU) reagierte darauf mit der EU NIS2-*Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022,* Publications Office (europa.eu)*)*, welche ab 18.10.2024 in Österreich und allen EU-Mitgliedschaften auch für spezifische KMU *(wesentliche und wichtige Einrichtungen)* gelten werden[5]. Betroffen sind alle Unternehmen und spezifische KMU, welche sogenannte wesentliche oder wichtige Einrichtungen sind und dem Kriterienkatalog dieser EU-Directive entsprechen. Das Wesentliche ist unter Anderen, daß zum Ersten Mal **Cyber Security mit Supply Chain Security, gemäß** Artikel 21[6] (2) d)[7] der NIS 2-Richtlinie verknüpft werden und welche bei der Auditierung nach ISO 27001 in Korrelation mit anderen Standards analysiert werden müssen.

II. NIS-2 Richtlinie:
NIS-2: Wesentliche und Wichtige Einrichtungen

Wesentliche Einrichtungen (Anhang I)	Wichtige Einrichtungen (Anhang II)
Energie (Elektrizität, Fernwärme/kälte, Öl, Gas, Wasserstoff)	Post- und Kurierdienste
Verkehr (NIS 1: Luft, Wasser, Schiene, Straße)	Forschung
Bankwesen	Chemie (Herstellung & Handel)
Finanzmarktaufsichtinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU Referenzlaboratorien, Forschung und Herstellung pharmazeutischer und medizinischer Produkte & Geräte)	Verarbeitendes & Herstellendes Gewerbe: (Medizinprodukte; Datenverarbeitungs - elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste, Suchmaschienen , Online-Marktplätze, Plattformen für Dienste sozialer Netzwerke
Abwasser	
Digitale Infrastruktur (IXP, DNS, TLD, Cloud Computing, Rechenzentren, Inhaltszustellnetzen, Vertrauensdiensteanbieter , und öffentliche elektronische Kommunikationsnetze)	Abfallbewirtschaftung *(Anmerkung GÖLLNER: „Kreislaufwirtschaft Circular Economy integriert JA/NEIN ?!)"*
IKT-Service Management	
Öffentliche Verwaltung	
Weltraum	

Zusammenfassung & Ausblick:

Im Nachfolgenden sind einige Herausforderungen angeführt, welche für NIS 2-betroffene[8] Unternehmen -und im besonderen KMU- relevant sind:

1. Entwicklung und Anwendung eines standardisierten, fakten- und auf einem mathematischen modell-basierten Cyber-Event und Bedrohungs-Monitoring sowie eines Risikoanalyse- und -bewertung-Modelles, sowie der notwendigen -teils permanenten- Dokumentation der Zusammenhänge und Wechselwirkungen, basierend auf den aktuell relevanten gesetzlichen Innovationen zwischen Cyber- und Supply Chain-Regelwerken.
2. Die Anforderungen und Strategische Ansätze: Status Quo und Innovationen für die Risikomodellierung & -monitoring in Bezug auf Zertifizierungen, Audits und Bonitätsprüfungen im Rahmen einer M&A-Due Diligence werden die Unternehmen (Einrichtungen) vor große Herausforderungen stellen, um Vertrauen bei bzw. in den betroffenen Unternehmen, Investoren und den nationalen zuständigen Aufsichtsbehörden zu begründen und um eine reduzierte Innovationsfreude -besonders bei KMU- oder Druck auf die digitale Transformation der KMU zu vermeiden.
3. Die Verfügbarkeit von qualitätsgesicherten modell-basierten Cyber-/Lieferketten Event und Bedrohungs-Monitoring-, Risikoanalyse- und Risikobewertungs-Werkzeugen sind fachlich nur eingeschränkt verfügbar.
4. Die Mitentwicklung von Leitfäden[9] und einheitlichen qualitätsgesicherten und getesteten Zertifizierungsstandards ist relevant, um die entstehenden Kosten *(wie z.B. infolge zusätzlicher Überwachung, zusätzlicher -womöglich permanenter- Berichterstattung von Vorfällen und*

[5] Bis zum 17.10.2024 erlassen und veröffentlichen die Mitgliedschaften die erforderlichen Vorschriften, um diese Richtlinie umzusetzen.

[6] Risikomanagementmaßnahmen im Bereich der Cybersicherheit

[7] Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern

[8] "Wesentliche und Wichtige Einrichtungen"

[9] Die RMA-Risk Management und Rating Association e.V., München, Deutschland, entwickelt im Rahmen ihres Arbeitskreises: Supply Chain Risiko Management einen Leitfaden für Supply Chain (Resilience/Security) Management in Korrelation zur NIS 2-Richtlinie, welcher voraussichtlich im 1. Quartal/2024 veröffentlicht wird, und Unternehmen kostenlos zur Verfügung stehen wird. Das Zentrum für Risiko- und Krisenmanagement leitet diesen Arbeitskreis.

Bedrohungen, supply chain security, zusätzlicher Vollzugskosten, einschließlich des zusätzlichen Rahmens für das Krisenmanagement, etc.) bei der Erfüllung der NIS 2-Richlinie Vorgaben reduzieren zu können.

5. Initiierung einer Aus-, Fort- und Weiterbildung-Kampagne zur Bewältigung des existierenden facheinschlägigen IT/Cyber-Fachkräftemangels bei österreichischen Unternehmen sowie der Ausbildung aktuell in Österreich nicht in der entsprechenden Anzahl verfügbaren NIS 2-Zertifizierungsexperten, um die nach ISO 27001, etc. in großer Anzahl zu erwartenden zu auditierenden Unternehmen fachlich und zeitnah bedienen zu können.

   Ein geeigneter Weg könnte hier auch in der Nutzung der mit dem Ingenieurgesetz (IngG 2017) geschaffenen Möglichkeit liegen, auf der Niveaustufe VI des NQR/EQR (Bachelorniveau) selbst geeignete Fachkräfte auszubilden und damit die Lücke an fehlenden Hochschulabsolvent:innen zu schließen.

6. Derzeit existiert noch kein verfügbares, inhaltlich qualitätsgesichertes Top-Management-Ausbildungskonzept für die die Zielgruppe: Top-Management (Geschäftsführer, Vorstände, Aufsichtsräte, Beiräte, etc.) im Sinne der Verantwortlichkeit des Top-Managements, gemäß NIS 2-Richtiinie.

Autor:

Dipl.-Ing. Johannes GÖLLNER, MSc leitet als Vorstandsvorsitzender des Zentrums für Risiko- & Krisenmanagement (ZRK), in Wien. Als Experte für Supply Chain Risiko & Network Analysis, der damit verbundenen Komplexität sowie Modeling und Simulation beschäftigt er sich seit 2003 -in Theorie und Praxis. Er ist seit 2013 RMA e.V.-Mitglied leitet er den RMA-Arbeitskreis: Supply Chain Risk Management, München, der Cyber Security Plattform Österreich und hat das ZRK-Competence Center for Supply Chain & Circular Economy von 2012 bis 2023 im Bereich der Forschung *(Rohstoff-Monitoring und Food Supply, etc.)* und Standardisierung geleitet. Er ist FH-Dozent/Lektor für Informations- und Wissensmanagement sowie Production Resources an Fachhochschulen. (www.zfrk.org)