Cybersecurity 4.0:

Strategische und fallbezogene Cybersecurity für Industrie 4.0 in kleinen und mittleren Unternehmen

Industrie 4.0 hat zweifellos die Digitalisierung in der Produktionslandschaft vorangetrieben. Vernachlässigt wird jedoch häufig der exponenzielle Anstieg der Cyberrisiken, der durch die zunehmende Vernetzung von Produktionssystemen infolge dieser Digitalisierung entsteht. Insbesondere kleine und mittlere Unternehmen (KMU), die im Durchschnitt über weniger Ressourcen zur Sicherung ihrer Cyberresilienz verfügen als große Unternehmen, sind dabei gefährdet. Das Projekt Cybersecurity 4.0 richtet sich an KMU im Fertigungsbereich sowie an Anbieter von Cybersicherheitstechnologien für KMU. Ziel ist die Bereitstellung maßgeschneiderter Lösungen zur Stärkung der Cyberresilienz in KMU. Das Projekt läuft seit fast zwei Jahren und wird von den deutschen Kooperationspartnern *FIR an der RWTH Aachen* und *IDA FH Aachen* sowie den belgischen Organisationen *Sirris* und *Howest* durchgeführt. >

Cybersecurity 4.0:

Strategic and Case-Specific Cybersecurity for Industry 4.0 in Small and Medium-Sized Enterprises

Industry 4.0 has undoubtedly driven the digital transformation of the manufacturing sector. However, the surge in cyber risks associated with the increased connectivity of production systems resulting from this digital transformation is frequently overlooked. Small and medium-sized enterprises (SMEs), in particular, are vulnerable, as they have fewer resources to invest in cybersecurity compared to larger corporations. The Cybersecurity 4.0 project is aimed at SMEs within the manufacturing sector, as well as providers of cybersecurity technologies for SMEs. The goal is to develop tailored solutions that bolster cyber resilience for SMEs. The project has been underway for almost two years, with German partners *FIR an der RWTH Aachen* and *IDA FH Aachen* collaborating with Belgian organizations *Sirris* and *Howest*. >

Im Rahmen des Forschungsprojekts Cybersecurity 4.0 entstehen ein KMU-orientiertes Cybersicherheits-Framework, Werkzeuge, Richtlinien und eine Lernumgebung speziell für Industrie 4.0. Dies ermöglicht KMU, umsetzbare Sicherheitsmaßnahmen für ihre vernetzten Produktionssysteme und Industrie-4.0-Anwendungen anzugehen. Das Projektkonsortium konzentriert sich auf die verwundbarsten und bisher am wenigsten adressierten Bereiche der Cybersicherheit für Industrie 4.0: OT (Operation-Technology), Lieferkette und Datenaustausch.

Die Ziele des Projekts sind wie folgt definiert:

- Entwicklung eines Industrie-4.0-Cybersecurity-Maturity-Modells für KMU.
- Erstellung eines webbasierten Tools für Self-Assessment und Planung eines sichereren Cybersecurity-Reifegrads.
- Entwicklung eines Demonstrators als Proof of Concept zur Simulation von Angriffs- und Verteidigungsszenarien an einer realen Automatisierungsanlage.
- Bereitstellung von Guidelines und Erhöhung der Cybersecurity-Awareness durch Gamification-Tools.

Cybersecurity-4.0-Reifegradmodell

Das Cybersecurity-Reifegradmodell basiert auf der Analyse empirischer Erkenntnisse aus früheren Phasen des Projekts sowie der IEC 62443[1] und Frameworks wie dem *NIST Cybersecurity Framework*[2] sowie dem ICS-Security-Kompendium des BSI[3]. Dieses Cybersecurity-Reifegradmodell unterstützt

[1] s. International Electrotechnical Commission 2009

[2] s. US National Institute of Standards and Technology 2014

[3] s. Bundesamt für Sicherheit in der Informationstechnik 2013

The Cybersecurity 4.0 research project aims to develop a cybersecurity framework tailored for SMEs, complete with tools, guidelines, and a specialized learning environment for Industry 4.0. This framework will empower SMEs to implement practical security measures for their interconnected production systems and Industry 4.0 applications. The project consortium is concentrating on the most vulnerable and often overlooked aspects of cybersecurity for Industry 4.0: Operation Technology (OT), supply chains, and data exchange.

The project's objectives are as follows:

- Develop an Industry 4.0 Cybersecurity Maturity Model specifically for SMEs
- Create of a web-based tool that enables self-assessment and planning to enhance cybersecurity maturity
- Develop a demonstrator to serve as a proof-of-concept, simulating attack and defense scenarios on a real automation system
- Provide guidelines and increase cybersecurity awareness through the use of gamification tools

Cybersecurity 4.0 Maturity Model

The cybersecurity maturity model is based on the analysis of empirical findings from the project's earlier phases, alongside established standards such as IEC 62443[1], the NIST Cybersecurity Framework[2], and the ICS Security Compendium from the German Federal Office for Information Security[3].

[1] see International Electrotechnical Commission 2009

[2] see US National Institute of Standards and Technology 2014

[3] see Bundesamt für Sicherheit in der Informationstechnik 2013

Jetzt an der Umfrage zur „Cyberresilienz mit dem Cybersecurity-4.0-Reifegradmodell" teilnehmen!

Basierend auf dem Reifegradmodell wurde ein Fragebogen entwickelt, den Unternehmen ausfüllen können, um Feedback zu ihrem Cybersicherheitsstatus sowie Empfehlungen zur Verbesserung zu erhalten.

Wenn Sie das Reifegradmodell testen möchten und mehr über Ihren Cybersicherheitsstatus erfahren wollen, folgen Sie diesem Link:

> su.vc/ijjgnyvl

Der Bericht wird Ihnen automatisch per E-Mail zugesandt.
Wir freuen uns über Ihre Teilnahme und bedanken uns im Voraus!

Unternehmen dabei, ihren aktuellen Reifegrad zu bestimmen, erreichbare Zielzustände festzulegen und sie durch den Prozess der Erreichung dieser Ziele zu führen.

Das Modell besteht aus vier Sicherheitsstufen: unzureichend (Stufe 0), grundlegend (Stufe 1), zuversichtlich (Stufe 2) und widerstandsfähig (Stufe 3). Jede Stufe baut auf der vorherigen auf, was gleichzeitig bedeutet, dass die Erfüllung jeder Stufe eine Voraussetzung für das Erreichen der nächsten ist.

Stufe 0 – Insufficient: Auf dieser Stufe hat ein Unternehmen die Anforderungen von Stufe 1 entweder nicht oder nur teilweise implementiert. Es zeigt einen Mangel an angemessenen Cybersicherheitsmaßnahmen, was das Unternehmen anfällig für aktuelle Bedrohungen macht.

Stufe 1 – Baseline: Das Unternehmen hat grundlegende Sicherheitsmaßnahmen integriert und Maßnahmen eingeleitet, um sich gegen Cyberangriffe zu schützen; dennoch bleibt ein beachtliches Risiko bestehen.

Stufe 2 – Confident: Auf Stufe 2 hat das Unternehmen ein spürbares Maß an Sicherheit in seinen Cybersicherheits-

This model is designed to help companies assess their current cybersecurity maturity level, set realistic target goals, and navigate the path to achieving these goals.

The model comprises four security levels: Inadequate (Level 0), Basic (Level 1), Confident (Level 2), and Resilient (Level 3). Each level builds on the previous one, requiring companies to meet the criteria of one level before progressing to the next.

Level 0 – Insufficient: At this level, a company has either not implemented the requirements of Level 1 or has done so only partially. This indicates a lack of adequate cybersecurity measures, leaving the company vulnerable to current threats.

Level 1 – Baseline: The company has put in place basic security measures and taken initial steps to protect itself against cyberattacks. However, significant risks persist.

Level 2 – Confident: At Level 2, the company has established a tangible degree of confidence in its cybersecurity measures. By implementing additional security measures,

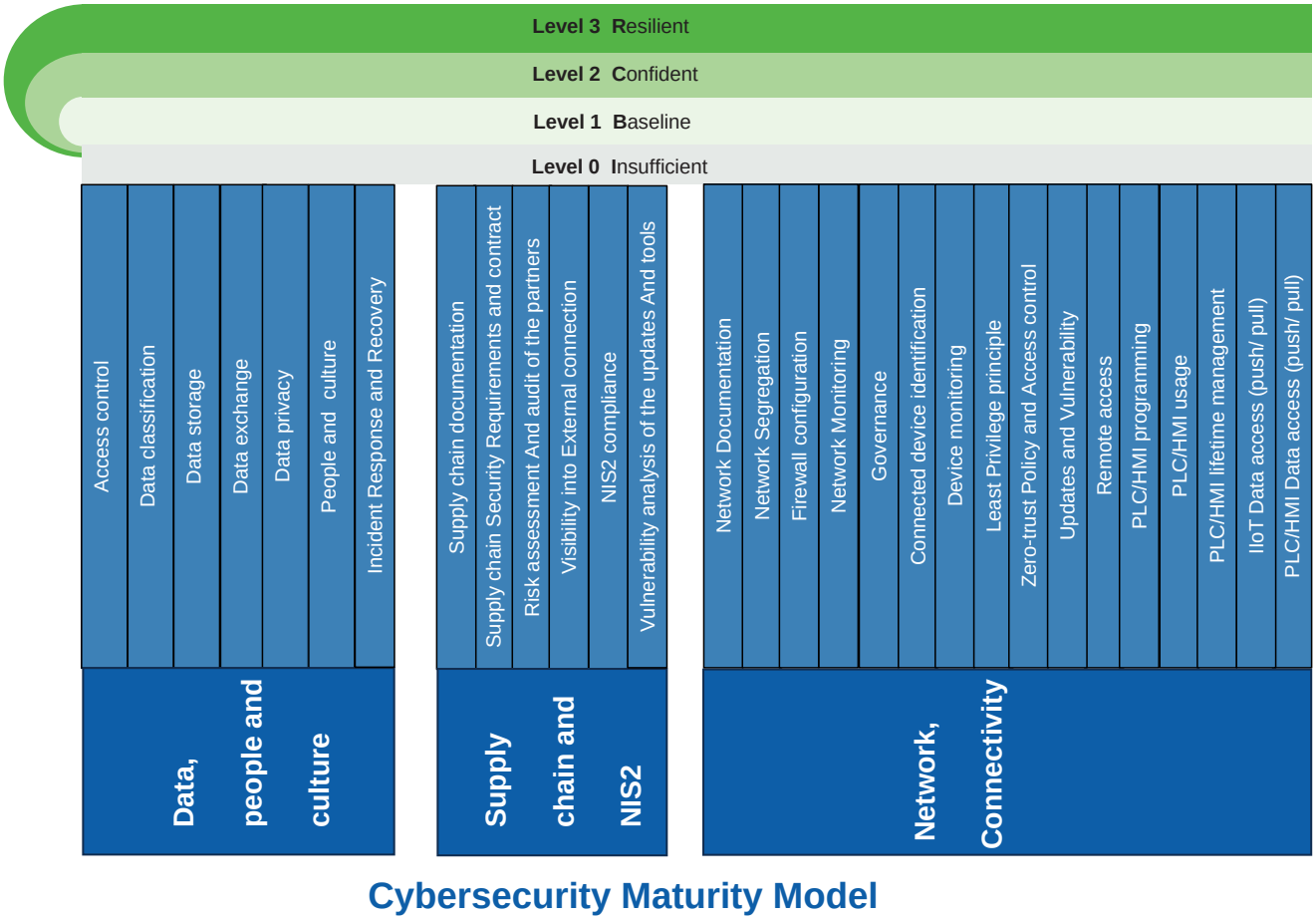

Figure 1: Cybersecurity Maturity Model

maßnahmen erlangt. Initiativen zur Stärkung der Sicherheitsposition wurden eingeleitet, was zu einem verbesserten Schutz vor bekannten Bedrohungen führt.

Stufe 3 – Resilient: Das Unternehmen hat ein erhöhtes Maß an Widerstandsfähigkeit gegen Cyberangriffe erreicht. Es ist gründlich darauf vorbereitet, sich gegen eine breite Palette von Cyberbedrohungen zu verteidigen und mit wirksamen Gegenmaßnahmen zu reagieren.

Neben diesen vier Sicherheitsstufen wurden Sicherheitsdomänen identifiziert, die verschiedene cybersicherheitsrelevante Bereiche darstellen. Jede Domäne gehört zu einer bestimmten Sicherheitsstufe. Die Gesamtsicherheitsstufe des Unternehmens wird durch die erreichte Stufe in jeder Domäne bestimmt. Innerhalb jeder Domäne gibt es mehrere Sicherheitskategorien, die jeweils spezifische Anforderungen haben. Diese Struktur bietet Unternehmen einen umfassenden Überblick über ihren Sicherheitsstatus in verschiedenen Bereichen sowie eine detaillierte Sicht auf spezifische Sicherheitsaspekte. Für jede Stufe und jede Kategorie existieren spezifische Sicherheitsanforderungen, die erfüllt sein müssen, um die entsprechende Stufe innerhalb dieser Kategorie zu erreichen. Mit zunehmendem Reifegrad werden die Anforderungen anspruchsvoller, was zusätzliche Ressourcen für die Implementierung erfordert und die Sicherheit des Unternehmens erhöht.

Fabian Seidel

the company has enhanced its protection against known threats.

Level 3 – Resilient: The company has achieved robust resilience against cyberattacks. It is fully equipped to fend off a wide range of cyber threats and respond with effective countermeasures.

In addition to these four security levels, various security domains have been identified. Each domain represents a key area relevant to cybersecurity and belongs to a specific security level. The overall security level of the company is determined by the level achieved in each domain. Within each domain, there are multiple security categories, each with its own set of specific requirements. This structure provides companies with both a comprehensive overview of their security status across different areas and a detailed view of specific security aspects. Specific security requirements must be met at each level and within each category in order to achieve the corresponding level within that category. As the maturity level increases, the requirements become more stringent, demanding additional resources for implementation and bolstering the company's security.

Fabian Seidel

Project Title: CyberSecurity 4.0

Funding/Promoters: *Federal Ministry for Economic Affairs and Climate Action (BMWK);*
Arbeitsgemeinschaft industrieller Forschungsvereinigungen "Otto von Guericke" e. V. (AiF)

Funding no.: 328 EN

Website: cybersecurity-40.fir.de

The Cornet project 328 EN of the Research Association *FIR e. V. an der RWTH Aachen*, Campus-Boulevard 55, 52074 Aachen, is funded via the *AiF* within the framework of the Cornet program for the promotion of international projects of pre-competitive joint research for the benefit of small and medium-sized enterprises by the *Federal Ministry for Economic Affairs and Climate Action* (BMWK) on the basis of a resolution of the *German Bundestag*.

Fabian Seidel, M. A.
Project Manager
Research Unit Information Management
FIR e. V. an der RWTH Aachen
Phone: +49 241 47705-505
Email: Fabian.Seidel@fir.rwth-aachen.de

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag
ptj projektträger jülich

Open Access: Dieser Artikel wird unter der Creative-Commons-Lizenz „Share Alike 4.0 International – Weitergabe unter gleichen Bedingungen 4.0 International" (CC BY-SA 4.0) veröffentlicht.