Schutz vor Cyber-Schwachstellen in KMU-Lieferketten

Lead: FH Oberösterreich, Campus Steyr

Herausforderungen:

- Verhandlungsmacht und Transparenz in KMU-Lieferketten gering
- Hohe Komplexität aufgrund vieler Lieferanten
- Verbindungen zu Lieferanten & Kunden als potenzielle Gefahrenquelle

Use Case Ziel:

- Framework zur Identifikation und Maßnahmenableitung für cyber-kritische KMU-Unternehmenspartnern

Ihre Benefits:

- Vorgehensweise anhand von internationalen Standards
- Begleitung bei der Einführung des Frameworks
- Compliance zu (zukünftigen) Regulativen (zB NIS2, Cyber Resilience Act, EU Maschinenverordnung)

Verbessern Sie mit uns Ihre Cybersecurity.

Kontaktieren Sie uns: michael.herburger@fh-steyr.at

CySeReS KMU
Interreg Bayern-Österreich
Kofinanziert von der Europäischen Union

CySeReS KMU Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

Schutz vor Cyber-Schwachstellen in KMU-Lieferketten

CySeReS-KMU Use Case Beschreibung

Lead: FH Oberösterreich

Use Case bezogene Problemstellung bei KMU

Vor welchen Problemen stehen die KMU bei dem Use Case?

KMU arbeiten mit unterschiedlichen Lieferanten, Dienstleistern und Partnern zusammen, um ihre Produkte oder Dienstleistungen zu entwickeln und zu vertreiben. Diese Vernetzung schafft Angriffsflächen für Cyberkriminelle, die Schwachstellen in den Systemen und Prozesse der Partner ausnutzen können, um auf das Netzwerk des KMU zuzugreifen. In vielen Fällen ist unklar, welche potenziellen Verbindungen ausgenutzt werden könnten und welche Unternehmenspartner aus Sicht der Cybersecurity besonders kritisch sind. Außerdem stellt das Etablieren von Cybersecurity-Maßnahmen in der Lieferkette häufig eine Herausforderung aufgrund der fehlenden Verhandlungsmacht gegenüber Großunternehmen dar.

Use Case Zielsetzung CySeReS-KMU

Was soll mit dem Use Case erreicht werden?

Im Use Case „Schutz vor Cyber-Schwachstellen in KMU-Lieferketten“ soll ein Framework entwickelt und getestet werden, mithilfe dessen es für KMU möglich ist, kritische Unternehmenspartner innerhalb ihrer Lieferkette zu identifizieren und anschließend passende und risikoorientierte Maßnahmen ableiten zu können, die regelmäßig aktualisiert werden. Dabei soll sich an bisherigen, existierenden Frameworks für Supply Chain Security angelehnt werden (zB NCSC Framework, ENISA Best Practice Guide, etc.)

Beschreibung Use Case Output

Welche konkreten Outputs werden im Use Case erwartet? (zB Dokumente)

- Good-Practice Guide mit Schritt für Schritt Anleitung zur Bewältigung von Cyber-Schwachstellen in Lieferketten

CySeReS KMU Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

Schutz vor Cyber-Schwachstellen in KMU-Lieferketten

Benefits für Unternehmen / Teilnehmer:innen

Was können Teilnehmer:innen / Unternehmen aus dem Workshop mitnehmen?

- Die Teilnehmer:innen erhalten einen direkten Einblick in den aktuellen Stand der Forschung sowie in international anerkannte Frameworks, die durch Expert:innen weiter erläutert und verglichen werden
- Die Teilnehmer:innen, die in einem KMU tätig sind, können die Problemstellungen und Barrieren für Cybersecurity außerhalb des eigenen Unternehmens gezielt mit anderen Unternehmen sowie dem Projektkonsortium aus Expert:innen diskutieren.
- Auf Basis der Erkenntnisse des Workshops wird ein spezifischer Framework für Cybersecurity in Lieferketten entwickelt, wodurch die Wahrscheinlichkeit zur Anwendbarkeit bei den teilnehmenden Unternehmen steigt.
- Die Teilnehmer:innen erhalten Einblicke, wie andere Unternehmen (KMU oder GU) mit dem Thema Cybersecurity in Lieferketten derzeit umgehen und erhalten praxisorientierte und anwendbare Ansätze.

Kontakt für weitere Informationen

Projektleiter: Mag. Michael Herburger, BA MA PHD michael.herburger@fh-steyr.at
Projektkoordinatorin: Carina Hochstrasser, BA MA carina.hochstrasser@fh-steyr.at

FH OÖ Oberösterreich · Logistikum · Universität Passau · Technische Hochschule Deggendorf · THD · universität innsbruck · FH Salzburg