

Cyber-Security Awareness & Kultur

Lead: FH Salzburg

Herausforderungen:

- Faktor Mensch als wichtigstes Einfallstor für Angriffe
- Fehlendes Bewusstsein der Mitarbeiter*innen
- Fehlendes Bewusstsein der Führungskräfte
- Technische Maßnahmen alleine sind NICHT ausreichend

Use Case Ziel:

- ✓ Schaffung einer angemessenen, sicherheitsorientierten Unternehmenskultur im KMU mit informierten, sensibilisierten und verantwortungsvollen agierenden Mitarbeiter*innen. (Security-First-Kultur)

Ihre Benefits:

- ✓ Erhöhte Sicherheit durch Fokus auf das wichtigste Einfallstor für Angriffe
- ✓ Konkrete Tools, um eine Security-First Kultur aufzubauen
- ✓ Sensibilisierte Mitarbeiter*innen & Führungskräfte

Verbessern Sie mit uns Ihre Cyberscurity&Resilienz

Kontaktieren Sie uns:



Cybersecurity Awareness & Kultur

CySeReS-KMU Use Case Beschreibung

Lead: FH Salzburg

Use Case bezogene Problemstellung bei KMU

Bis zu 95% aller Cybersecurity Vorfälle sind auf den Faktor Mensch zurückzuführen. Menschliches Verhalten und menschliche Interaktionen sind eine Schwachstelle, die von Angreifern gezielt ausgenutzt wird. Durch technische Maßnahmen alleine kann Resilienz in der Cyber Sicherheit nicht erreicht werden, da der Faktor Mensch selbst die beste IT-Sicherheitstechnologie konterkarieren kann. Ein angemessenes Verhalten und Bewusstsein der Mitarbeiter*innen sowie eine adäquate, gelebte Kultur im Unternehmen sind weitere, unabdingbare Voraussetzungen dafür.

Die Unternehmenskultur und die Einhaltung von Richtlinien spielen eine wichtige Rolle. Eine Kultur, die Sicherheit priorisiert und Compliance fördert, kann das Risiko von Sicherheitsvorfällen verringern, während ein Mangel an Sicherheitsbewusstsein zu erhöhten Risiken führen kann.

Use Case Zielsetzung CySeReS-KMU

Der Use Case verfolgt zwei Zielsetzungen:

- Es wird prototypisch eine für KMU geeignete Unternehmenskultur (bzw. an Bausteinen, die in die Kultur integriert werden sollen) erarbeitet, die den Anforderungen an ein in Bezug auf Cyber-Resilienz gut aufgestelltes KMU entspricht. Die erforderlichen Rahmenbedingungen sowie ein Konzept, wie der Sollzustand erreicht werden kann, werden in diesem Use Case erarbeitet.
- Es werden Konzepte, Tools und Methoden vorgestellt, wie KMU gezielt Mitarbeiter*innen auf das Thema Cybersecurity schulen und sensibilisieren können. Hier wird einerseits auf Best-Practices zurückgegriffen, bei Bedarf wird jedoch gemeinsam mit Expert*innen aus Wirtschaft und Forschung auch Neues entwickelt.

Beschreibung Use Case Output

Zum Abschluss wird folgender Output erwartet:

- Beschreibung (Bild) einer angemessenen Unternehmenskultur bzw. der relevanten Bausteine, um cyber-resilient zu werden
- Werkzeugkasten mit erprobten Tools, um die Awareness bei den Mitarbeiter*innen zu stärken

Benefits für Unternehmen / Teilnehmer:innen

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

- Erhöhte Sicherheit durch Fokus auf das wichtigste Einfallstor für Angriffe
- Konkrete Tools, um eine Security-First Kultur aufzubauen
- Sensibilisierte Mitarbeiter*innen & Führungskräfte

Kontakt für weitere Informationen



Alexander Zeisler, B.A., M.A alexander.zeisler@fh-salzburg.ac.at

Projektleiter: Mag. Michael Herburger, BA MA PHD michael.herburger@fh-steyr.at

Projektkoordinatorin: Carina Hochstrasser, BA MA carina.hochstrasser@fh-steyr.at