

Newsletter Nr. 3

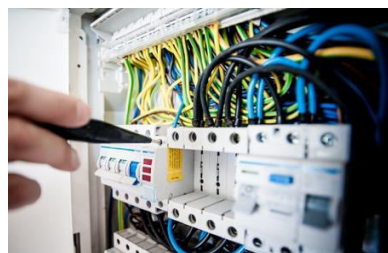
CSEC TOR - SCHUTZ UNSERER INDUSTRIELLEN KMUs

CSEC TOR (Cyber Security Training on Operational Technologies Resilience) ist ein innovatives, vom Erasmus+ Programm der Europäischen Union finanziertes Projekt, das sich mit einem Thema beschäftigt, das sowohl von Branchenexperten als auch von politischen Entscheidungsträgern oft übersehen wird: der Cybersicherheit von Betriebstechnologien (OT).

Pläne, Projekte, Schulungs- oder Sensibilisierungsmaßnahmen usw., die sich auf die IT-Sicherheit von Netzen konzentrieren, oder besser gesagt, auf die Verhinderung von Cyberangriffen, Datendiebstahl oder -missbrauch bei der Nutzung des Internets zu Arbeits- oder Unterhaltungszwecken.

In einer zunehmend vernetzten und digitalisierten Welt können jedoch auch betriebliche Technologien Gegenstand von Cyberangriffen sein, die kritische Infrastrukturen gefährden und den Produktionsbetrieb unterbrechen können.

Das CSEC TOR-Projekt geht diese wichtige Herausforderung mit einer Reihe von Maßnahmen und Instrumenten an, die wir im Folgenden kurz beschreiben



ANGRIFFE AUF OT- UND IT- SYSTEME

KonBriefing (Cyber-Angriffe weltweit 2022 | [KonBriefing.com](https://www.konbriefing.com)) führt eine jährliche Umfrage zu Cyber-Angriffen durch, die alle Branchen in allen Ländern der Welt betroffen haben, von den USA über China bis Europa.

Schon ein Blick auf die Umfrage zeigt, wie wichtig die Cybersicherheit von OT-Systemen ist



DIE ZIELE DES PROJEKTS

Das Projekt CSecTOR befasst sich mit der digitalen Transformation, indem es die digitale Bereitschaft, Widerstandsfähigkeit und Kapazität der europäischen KMUs entwickelt und ihnen hilft, industrielle Cybersicherheit auf einfache, verständliche und zugängliche Weise zu erreichen.

Die wichtigsten erwarteten Ergebnisse sind:

1. Die Entwicklung einer **OT-Cybersicherheitsmethodik** zur Unterstützung industrieller KMU bei der Sicherung ihrer industriellen Anlagen und Abläufe
2. Entwicklung des **OT-Cybersecurity-Trainingskurses** zur Unterstützung von Unternehmen

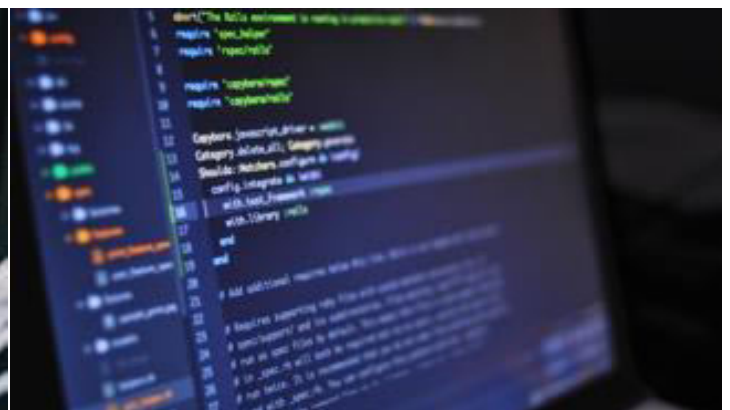
das derzeitige Niveau der betrieblichen Cybersicherheit und mögliche Lücken in den Sicherheitsmaßnahmen zu bewerten, den Mitarbeitern Schulungen zur Verbesserung ihrer Fähigkeiten im Bereich der betrieblichen Cybersicherheit anzubieten usw.

3. Entwurf und Programmierung der **OT-Cybersecurity e-training** Plattform

4. **Verbreitung** und Verwertung

Das Hauptziel des Projekts besteht darin, Organisationen dabei zu helfen, die Widerstandsfähigkeit ihrer betrieblichen Technologiesysteme zu erhalten, damit diese auch angesichts potenzieller Cyber-Bedrohungen weiterhin ordnungsgemäß funktionieren können.

OT-Sicherheit konzentriert sich auf den Schutz von Netzwerken und Computersystemen, die in betrieblichen Umgebungen eingesetzt werden



FÜR WEITERE INFORMATIONEN

<https://csector.eu/project/>

FOLLOW US!



CsectorerasmusplusProjekt



csector

DIE PARTNER DES PROJEKTS

FH JOANNEUM
University of Applied Sciences

FH Joanneum - University of Applied Sciences, ist eine der führenden Fachhochschulen Österreichs



Tournis Symvouleftiky EE ist ein griechisches Beratungsunternehmen in den Bereichen Business Resilience, Governance, Risk & Compliance Management, Incident & Crisis Management, Business Continuity Management, Informationssicherheit und Datenschutzmanagement.



PCX Computers & Information Systems Ltd ist ein zypriotisches KMU, das über große Erfahrung bei der Anwendung innovativer Technologielösungen im Bildungswesen verfügt.



ASSET ist eine Agentur der Handelskammer der Basilicata



Die Lettische Industrie- und Handelskammer (LCCI) ist der größte Unternehmerverband in Lettland, der 6000 Mitglieder - Kleinst-, Klein-, Mittel- und Großunternehmen - vereint.

Blieben Sie mit uns in Kontakt: Im nächsten Newsletter werden wir Sie über den Methodikrahmen informieren!