

Cybersecurity Community

Das Sicherheitsnetzwerk für die Metropolregion Rhein-Neckar



Unsere Arbeitsgruppen

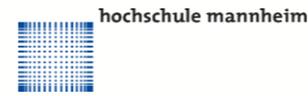
Cyberawareness



Notfall- und Krisenmanagement



Fachkräfte- und Kompetenzentwicklung



Technische Infrastruktur und Anforderungen



Compliance



Arbeitsgruppe

Cyber Awareness



AG Cyberawareness

Ziel

Durch die Förderung von Cyber Awareness können Unternehmen und Organisationen ihre Sicherheitslage erheblich verbessern und sich besser gegen die vielfältigen Bedrohungen der digitalen Welt wappnen. Awareness für Cyber Security ist entscheidend, um die Sicherheit in industriellen Umgebungen zu gewährleisten. Eine gezielte Sensibilisierung stärkt die Resilienz gegenüber Cyberangriffen und reduziert menschliche Fehler als Sicherheitsrisiko.

Wie

- ✓ Unterstützung bei der Etablierung einer sicherheitsbewussten Unternehmenskultur.
- ✓ Austausch bewährter Ansätze zur Förderung von Awareness.
- ✓ Zusammenarbeit zwischen IT und OT fördern.

Was

- ✓ Entwicklung von Bildungsformaten, Schulungen und Workshops
- ✓ Praktische Übungen: Tabletop- und Testlabor-Übungen
- ✓ Sensibilisierungstraining für Entscheider / Geschäftsführungsebene

Arbeitsgruppe

Fachkräfte- und Kompetenzentwicklung



AG Fachkräfte- und Kompetenzentwicklung

Ziel

Der Fachkräftemangel in der Cybersecurity bedroht die Sicherheit von IT- und OT-Infrastrukturen. Eine gezielte Fachkräfteentwicklung stärkt die Wettbewerbsfähigkeit und macht die Region attraktiver für Talente.

Wie

Konzeption, Sichtung, Einordnung sowie Entwicklung und Weiterentwicklung von Qualifizierungsangeboten

IT- vs. OT-Security / Sichere Software- und Systementwicklung / Security Management für KMU / Security vs. Safety / Security Awareness in Ingenieurstätigkeiten / IEC62443, Maschinenverordnung / CSMS (UN ECE 155&156; IEC 21434) / NIS-2 / CRA

Was

- ✓ Kostenlose, kurze Wissensveranstaltungen
- ✓ Online-Seminare (bis 1 Tag)
- ✓ Fachseminare
- ✓ Zertifikatskurse
- ✓ Studiengänge (berufsbegleitend, Master)
- ✓ Grundständige Studiengänge z.B. Cybersecurity Bachelor TH Mannheim

Arbeitsgruppe

Notfall- und Krisenmanagement



AG Notfall- und Krisenmanagement

Ziel

Unternehmen der Region durch praxisorientierte Strategien, standardisierte Prozesse und kontinuierlichen Wissensaustausch zu helfen, auf Cyberangriffe effizient zu reagieren und deren Auswirkungen zu minimieren.

Wie

Wir setzen uns für eine effektive Zusammenarbeit und Vorbereitung auf Cybervorfälle innerhalb des Clusters ein.

Was

- ✓ Erste Unterstützung zur Orientierung
- ✓ Erste Hilfe bei der Bewältigung des Vorfalls
- ✓ Unterstützung bei der Vermittlung von Spezialisten, um schnell und effizient die schnelle und effiziente Suche nach Ursachen, Wegen und Absichten, um Angriff zu klären, effektiv einzugreifen und Beweise zu sichern
- ✓ Plattform zu dem Austausch von Erfahrung und Informationen

Arbeitsgruppe

Technische Infrastruktur



AG Technische Infrastruktur

Ziel

Durch Kooperation, Wissensaustausch und die Entwicklung einheitlicher Sicherheitsstandards soll eine sichere und leistungsfähige digitale Infrastruktur gefördert werden, um Mitgliedsunternehmen des Clusters gemeinsam gegen Cyberbedrohungen zu wappnen.

Wie

- ✓ Förderung der Zusammenarbeit zwischen den Mitgliedsunternehmen, um Synergien im Bereich IT-Sicherheit zu nutzen.
- ✓ Gemeinsame Entwicklung und Etablierung von Best Practices zur Absicherung technischer Infrastrukturen.

Was

- ✓ Gemeinsame Überwachung und Reaktion auf Bedrohungen, um eine frühzeitige Erkennung und effektive Abwehr zu gewährleisten.
- ✓ Evaluation innovativer Sicherheitslösungen und neuer Technologien
- ✓ Unterstützung bei der Einhaltung regulatorischer Anforderungen (z. B. NIS-2, DSGVO).

Arbeitsgruppe

Compliance



AG Compliance

Ziel Bereitstellung eines Forums für Wissens- und Erfahrungsaustausch

Wie Organisation von Workshops zur Beleuchtung der Compliance-Anforderungen im Bereich Cybersecurity

Was

- ✓ Beratung
- ✓ Workshops und Informationsveranstaltungen
- ✓ Best-Practice-Sharing
- ✓ Zertifizierungsvorbereitung