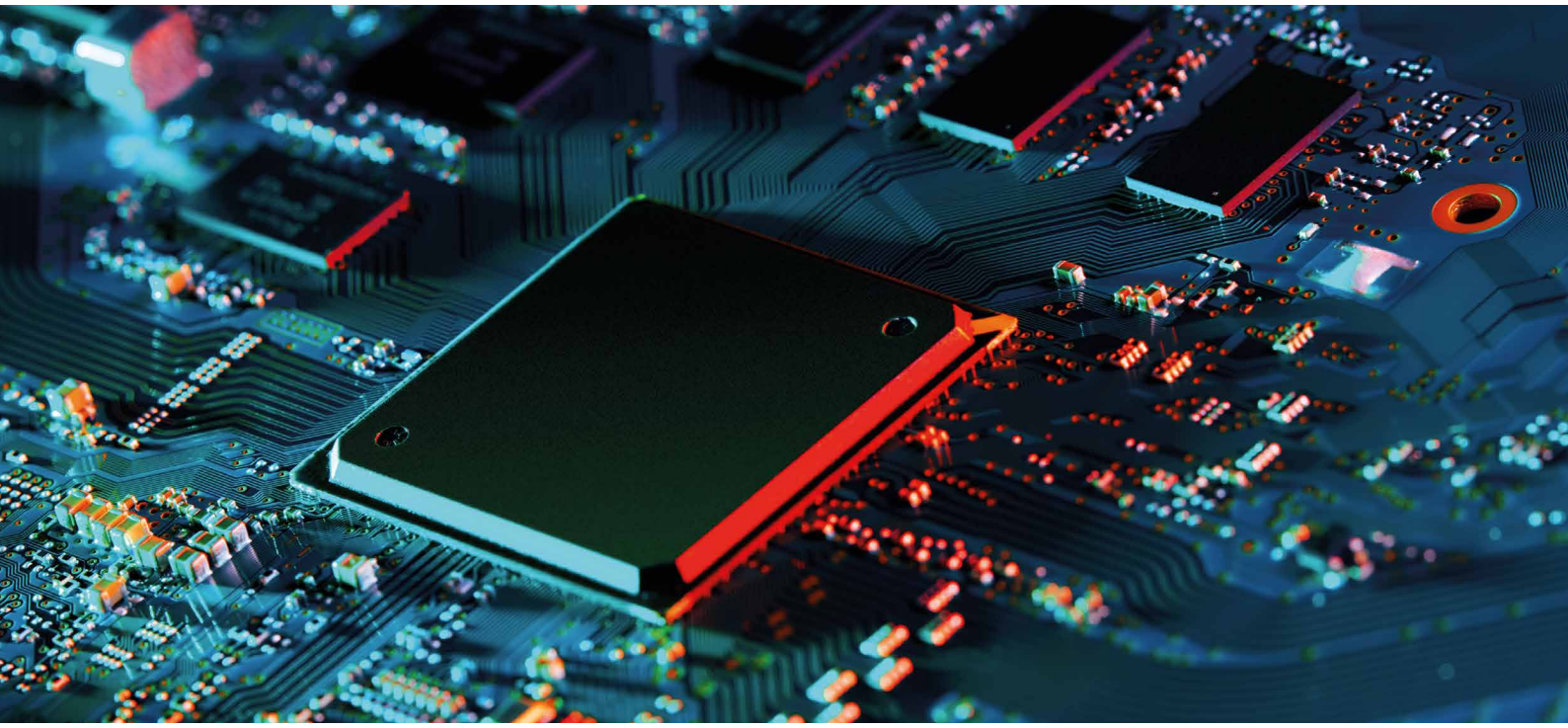
Cyber-Security



Cyber-Security als Wettbewerbsfaktor in der digitalen Transformation

Der Schutz Ihrer Systeme, Netzwerke und Programme gegen Angriffe von außen wird mit zunehmender Vernetzung und Digitalisierung zu einem zentralen Handlungsfeld in der digitalen Transformation. Cyber-Security ist dabei längst nicht nur eine Frage der Technik, sondern des Zusammenspiels zwischen Mitarbeitern, Prozessen und Technologie, welches eine effektive Verteidigung Ihrer Systeme sicherstellt. Unser Quick-Check hilft Ihnen, Ihre Bedrohungslage einzuschätzen und effiziente Abwehrmaßnahmen abzuleiten.

Wir unterstützen Sie bei der

- Aufnahme Ihrer Bedrohungslandschaft
- Analyse und Bewertung der zu schützenden Assets im Fahmen einer Risikoanalyse
- Bestimmung des aktuellen Stands Ihrer Cyber-Security
- Definition und Detaillierung von Maßnahmen und Einordnung in eine Umsetzungsroadmap

Ansprechpartner
Max-Ferdinand Stroh, M.Sc
✉ Max-Ferdinand.Stroh@fir-aachen.gmbh

Mit dem Cyber-Security-Quick-Check bewerten wir die Bedrohungslage Ihres Unternehmens und identifizieren potenzielle Schwachstellen. Dabei berücksichtigen wir Ihre unternehmensindividuellen Digitalisierungsziele und Assets, etwa die Anbindung des Shopfloors, neue Geschäftsmodelle oder Automatisierung. So schaffen Sie die Grundlage für eine systematische Bewältigung der Herausforderungen Ihrer digitalen Transformation.

Gemeinsam mit Ihren Mitarbeiter*innen nehmen wir Ihre Kernprozesse auf und analysieren diese hinsichtlich möglicher Schwachstellen. Untersucht werden die Ressourcen-, die System-, die Vernetzungs- und die Anwendungsebene Ihres Unternehmens, die Unternehmensstrategie, das Geschäftsmodell, Produkte & Services sowie Geschäftsprozesse. Anhand verschiedener Prüfkategorien auf Basis bekannter Standards und Rahmenwerke analysieren wir Ihre Prozesse und Gegebenheiten wie den Strategieprozess, das Netzwerkmanagement, den Umgang mit Fernzugriffen, personelle Aspekte sowie die Planung von Audits und Revisionen.

1 Vorbereitung

- Sichtung aller bereitgestellten Unterlagen
- Vorbesprechung und Konzeption der Workshopinhalte

2 Durchführung

- Workshops zur Aufnahme der ausgewählten Kernprozesse
- Interviews mit Fach- und Führungskräften der IT und weiterer Fachbereiche

3 Nachbereitung

- Identifikation von Handlungsfeldern und Maßnahmen
- Abschlusspräsentation und Diskussion der Maßnahmenroadmap

Ergebnisse

Sie erhalten eine Maßnahmenroadmap für die Abwehr der größten Bedrohungen und die Beseitigung von Schwachstellen Ihrer schützenswerten Assets. Die Workshop-Ergebnisse aus der Betrachtung Ihrer Assets und Prozesse stellen wir Ihnen in einer ausführlichen Dokumentation zur Verfügung.

Ihr Nutzen

- Transparenz über die Bedrohungslandschaft Ihres Unternehmens
- Kenntnis der potenziellen Schwachstellen Ihrer schützenswerten Assets
- Zusammenbringen von IT- und Fachabteilungen zur Förderung des engeren Austauschs im interdisziplinären Thema
- Roadmap mit detaillierten Maßnahmen zur systematischen Bearbeitung der identifizierten Handlungsfelder

Unsere Leistung

- Sichtung aller bereitgestellten Unterlagen
- Konzeption und Vorbereitung der Workshopmodule zur Bestimmung der Bedrohungslage und schützenswerten Assets
- Durchführung eines zweitägigen Workshops mit Moderation durch zwei Expert*innen des FIR
- Bereitstellung einer Maßnahmenroadmap mit konkreten Handlungsempfehlungen
- Vollständig aufbereitete Dokumentation der Workshop-Ergebnisse sowie der abgeleiteten Handlungsfelder
- Abschlusspräsentation mit Vorstellung der Ergebnisse

Hinweis: Die Workshoptage werden üblicherweise mit Beteiligung von drei Fachabteilungen und einer IT-Einheit geplant.

FIR Aachen GmbH
Campus-Boulevard 55
52074 Aachen
fir-aachen.gmbh