In 5 Schritten zum resilienten Cyber-Security Ökosystem

1 Ziele definieren

- Schutzziele identifizieren & bewerten
- Risiken evaluieren
- Ausgangssituation ergeben
- Geltungsbereich definieren
- Projektteam zusammenstellen
- Vorgehensweise festlegen

2 Maturität & Delta erheben

- Feststellung Ziele sowie Zeit- & Ressourceneinsatz
- Erhebung des Status Quo
- Soll-Ist-Vergleich: Status Quo zu avisiertem Zielbild
- Feststellung des Deltas Status Quo zu avisiertem Zielbild
- Festlegung des beabsichtigten Aufwandes

3 Lösungen & Fahrplan ableiten

- Lösungsentwicklung anhand der identifizierten Handlungsfelder
- Bewertung der Lösungen (Machbarkeit, Abwägen Aufwand/Nutzen)
- Fahrplan inkl. Zeit- und Ressourcenplan erstellen

4 Maßnahmen umsetzen & Prozesse verankern

- Durchführung von Pilotprojekten, um Akzeptanz und Wirksamkeit zu testen
- Während der Umsetzung regelmäßig überprüfen, ob die Maßnahmen greifen und verstanden werden
- Konsistente Botschaften senden (Kommunikation)
- Auf Beteiligung des Kernteams achten (inkl. Management)

5 Ergebnisse überwachen & optimieren

- Messung des Erfolgs
- Regelmäßige Kontrolle der Situation
- Befragung Mitarbeiter und Kernteam
- Sammlung von Verbesserungsoptionen

Dies ist ein komprimierter Auszug aus der publizierten Fassung des folgenden Werkes: S. Maier u. S. Aengenheyster, Geschäftsrisiko Cyber-Security: Leitfaden zur Etablierung eines resilienten Sicherheits-Ökosystems (essentials), Springer Gabler, 2020, vervielfältigt mit Genehmigung von Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020. Die komplette authentifizierte Version ist online verfügbar unter: http://dx.doi.org/10.1007/978-3-658-32046-1