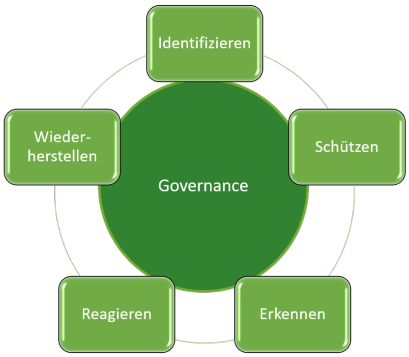
IT CONSULTING & ENGINEERING

EINFÜHRUNG UND OPTIMIERUNG VON IT-SECURITY FRAMEWORKS

NIST CYBERSECURITY FRAMEWORK, ISO/IEC 27001 UND ISAE3402 STANDARDS

In einer zunehmend digitalisierten Welt sind Informationssysteme und digitale Infrastrukturen zum Rückgrat moderner Unternehmen geworden. Mit dieser wachsenden Abhängigkeit von IT-Systemen steigt jedoch auch die Angriffsfläche für Cyberbedrohungen.

Um diesen vielfältigen Bedrohungen strukturiert und wirkungsvoll zu begegnen, haben sich in den letzten Jahrzehnten IT-Security-Frameworks und -Standards etabliert. Diese unterstützen die systematische Identifikation, Bewertung und Minimierung von IT-Sicherheitsrisiken. Frameworks wie das NIST Cybersecurity Framework (CSF) bieten einen ganzheitlichen Ansatz zur Etablierung der IT-Sicherheit im Unternehmen. Die konforme Umsetzung der IT-Sicherheit nach den Vorgaben der Standards ISO/IEC 27001 sowie ISAE 3402 kann durch Audits und Zertifizierungen nachgewiesen werden.



Die Umsetzung der IT-Sicherheitsvorgaben stärkt die Unternehmenssicherheit, senkt das Cyberangriffsrisiko und hilft, gesetzliche sowie normative Anforderungen nachzuweisen. Die entsprechenden Rahmenwerke decken dabei den gesamten Sicherheitszyklus ab – von Prävention und Erkennung über die Reaktion auf Vorfälle bis zur Systemwiederherstellung.

Basierend auf langjähriger Praxiserfahrung hat die In&Out AG ein Vorgehen zur Einführung und Optimierung von IT-Security Frameworks erstellt.

Definieren der gewünschten Frameworks und Standards

- Prüfen, welche IT-Security Standards umgesetzt werden sollen, wie z.B. ISO/IEC 27001 oder ISAE 3402
- Prüfen ob andere Standards bzw. Vorgaben eingehalten werden müssen, wie z.B. Regulatorien oder gesetzliche Vorgaben
- Basis für die Einführung des IT-Security Frameworks vereinbaren, z.B. auf Basis des NIST CSF

Bestehende Informationen prüfen

- Aufnahme der bereits bestehenden IT-Security Informationen und Dokumente
- Definieren, welche internen Abteilungen für die einzelnen IT-Security Bereiche zuständig sind, und festhalten der entsprechenden Zuständigkeiten

Gap- Analyse durchführen

- Prüfen der IT-Security Umsetzungen und vorhanden Dokumente sowie Evidenzen
- Abgleich mit den geforderten Kontrollpunkten und des gewünschten Reifegrads
- Erstellen eines Gap-Analyse Rapports
- Bei Bedarf können entsprechende interne Audits vorgenommen werden

Begleitung der Umsetzung der Massnahmen

- Definieren der Massnahmen zur Verbesserung der IT-Security, bei Bedarf kann die Umsetzung der Massnahmen begleitet werden
- Die Umsetzung kann anschliessend neu geprüft werden

Begleitung bei externen Audits

- Falls gewünscht kann das externe Audit für die gewünschte Zertifizierung begleitet werden

DAS VORGEHEN:

Der Leistungsumfang umfasst die Klärung der gewünschten IT-Security Standards und Frameworks die Gap-Analyse, die Definition der Massnahmen bis zur Begleitung des Audits.

IHR NUTZEN:

- Systematische Reduktion von Cyberrisiken
- Strukturierte Erkennung und Behebung von Schwachstellen
- Einheitlicher Schutz über alle Unternehmensbereiche
- Nachweis der Einhaltung gesetzlicher Vorgaben und Grundlage für Zertifizierungen (z.B. ISO 27001)
- Klare Verantwortlichkeiten und Prozesse und Sensibilisierung der Mitarbeitenden

KONTAKTIEREN SIE UNS:

Wir freuen uns über Ihre Kontaktaufnahme zur fachlichen Vertiefung der Thematik!

Silvio Pelli
Senior IT Consultant
silvio.pelli@inout.ch