Vorbereiten Einführung und Zertifizierung eines ISMS

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Hansjürg Wenger
Experte: Dr. René Bach (EFD, Informatiksteuerungen des Bundes ISB)
Industriepartner: SSE Engineering AG, Gümligen

Eine nachhaltige Sicherheit der unternehmerischen Informationen ist heute unerlässlich. Die Herausforderung liegt darin, die Informationen in Bezug auf Vertraulichkeit, Verfügbarkeit sowie Integrität zu schützen. Den verschiedenen Bedrohungen kann man mit Hilfe eines Information Security Management System (kurz ISMS, engl. für «Managementsystem für Informationssicherheit») nach ISO 27001 entgegenwirken.

Ausgangslage

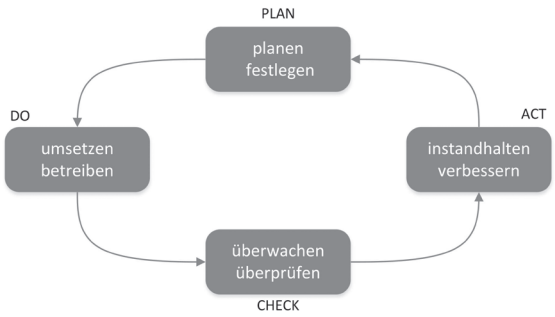
Die Firma SSE Engineering AG bearbeitet viele Aufträge der öffentlichen Hand. Um ausweisen zu können, dass das Security-Management von SSE Engineering AG korrekt und nach gängigen Normen und Standards durchgeführt wird, ist geplant ein ISMS nach ISO 27001 einzuführen und zu zertifizieren. Ist die Informationssicherheit in Bezug auf Vertraulichkeit, Verfügbarkeit sowie Integrität gefährdet, könnte dies für das Unternehmen zu schwerwiegende finanzielle Schäden oder einem Image Verlust führen.

Ziele

Durch den Aufbau und die Einführung eines ISMS macht SSE Engineering AG ein entscheidender Schritt in Richtung nachhaltige Sicherheit und generiert zahlreiche Vorteile: Erfüllung regulativer und vertraglicher Anforderungen für die Nachweisbarkeit der Informationssicherheit gegenüber Dritten, stärkeres Sicherheitsbewusstsein für Mitarbeiter, Führungskräfte und Leitung, Beitrag zur Sicherung der Geschäftskontinuität und damit des Erfolges, Reduzierung des Haftungsrisikos der verantwortlichen Führungskräfte und Kosteneinsparungen durch Vermeidung von Sicherheitsvorfällen.

ISMS nach ISO 27001

Ein ISMS ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Das primäre Ziel eines ISMS ist, die Risiken in Bezug auf die zu verarbeiteten Informationswerte zu kennen und zielgerichtet zu steuern. Ein solches Managementsystem lässt sich gut beherrschen und verbessern, wenn das richtige Vorgehen gewählt wird. Das PDCA-Modell und eine Standardisierung ermöglichen ein nachhaltiges, stabiles und effizientes ISMS zu betreiben. Die vier grundlegenden Aktivitäten des PDCA-Models sind: Plan, Do, Check und Act. Diese Aktivitäten bilden eine sich wiederholende Abfolge von Tätigkeiten und sind ein fester Bestandteil der ISO 27001. Dieser Ansatz stellt sicher, dass keine Entscheidungen getroffen werden, welche zu Fehlinvestitionen und Scheinlösungen führen.

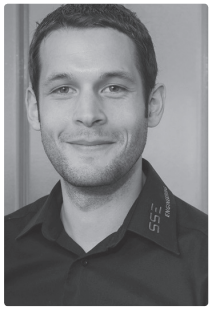


PDCA-Modell

Die ISO 27001 ist der weltweit angewendete Standard für die Zertifizierung eines ISMS. Die Norm spezifiziert Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Organisationen adaptiert werden sollen. Für die Realisation bietet die Normreihe der ISO 27001 umfangreiche Unterlagen. Die grundlegenden Ziele und Sicherheitsmassnahmen sind im Anhang A der ISO 27001 aufgeführt. Detaillierte Informationen mit Anwendungsregeln zur möglichen Umsetzung findet man in der ISO 27002. Insgesamt bietet die Norm 133 Massnahmen, welche bei einer Standardisierung zu berücksichtigen sind.

Ergebnis

Die in der Arbeit entstandenen Ergebnisse dienen als ideale Vorbereitung für die geplante Zertifizierung. Die ISO 27001 hat sich des Weiteren als sehr hilfreich und praktisch erwiesen, um das ISMS zu realisieren und die gesteckten Ziele zu erreichen. Im Verlauf der Arbeit sind 16 Dokumente im Bereich: Verfahren, Erklärungen, Richtlinien, Methoden, Pläne, Risikoeinschätzung und Risikobehandlung mit insgesamt 121 Seiten Inhalt entstanden.



Mathias Andreas Wenger