

Information Security Management System

S&T bietet seinen Kunden eine breite Palette an Beratungsdienstleistungen, die auf das Management von Risiken innerhalb der Informationssicherheit ausgelegt sind.

Die methodische Schaffung und Erhaltung eines unternehmensweiten, sicheren Umfeldes für Informationen, Transaktionen und die vereinbarte Verfügbarkeit der Kernprozesse wird mit der Implementierung eines Information Security Management Systems (ISMS) erreicht, welches sich in folgende Phasen gliedert:

- Sicherheits-Organisation mit definierten Verantwortlichkeiten
- Dokumentation und Prozesse für:
 - Risiko-Analyse für begegnete/unbegegnete Risiken
 - Richtlinien (Policies), Standards und Handlungsanweisungen
 - Umsetzung mittels Awareness-Training, Prozess-Redesign und Technologie
 - Audits und Reviews
 - Ergänzende Pläne für Business Continuity und Disaster Recovery

Das organisatorische Umfeld

Es wird nachdrücklich empfohlen, dass die erste Führungsebene des Unternehmens das Dokument beauftragt und für die Umsetzung verantwortlich zeichnet, weil dies den umfassenden Schutz von Informationen als strategisch wichtig einstuft.

Das Management ernennt den „Chief Information Security Officer“, der für die Errichtung und Erhaltung des spezifizierten, sicheren Umfeldes sorgt und alle Maßnahmen zur Umsetzung der Sicherheitsrichtlinie koordiniert.

Die Security Policy

In diesem Vorgehensmodell stellt die Formulierung einer unternehmensweiten Sicherheitsrichtlinie ein zentrales Element dar. Die Security Policy beschreibt alle sicherheitsrelevanten, strategischen Vorgaben und Standards, woraus Verantwortungen, Mitarbeiterverhalten, Prozesse und unterstützende Technologien klar und organisationsweit abgeleitet werden können, die durch strukturierte Audits auf ihre Wirksamkeit hin überprüft werden.

Die Security Policy ist somit die oberste Regelungs-Ebene, präzisiert durch Standards und konkrete Handlungsanleitungen.

Die Sicherheitsrichtlinie wird in folgender Struktur aufgebaut:

- Organisatorisches Umfeld
- Daten-Klassifikation
- Richtlinien für Benutzergruppen und Komponenten
- Flankierende Prozesse
- Weiterentwicklung und Erläuterung der Sicherheitsrichtlinie

Klassifizierungen

Ein Kernpunkt dieser Sicherheitsrichtlinie ist eine mehrdimensionale Klassifikation der Daten, aus denen differenzierte Schutzbedürfnisse und Maßnahmen abgeleitet und implementiert werden können.

Die geläufigsten Klassifizierungskategorien sind Daten-Vertraulichkeit, Datenwiederherstellung, Systemverfügbarkeit und das Management der vorgegebenen Behaltefristen von Dokumenten. Diese Klassifizierung und die Verknüpfung von Klassen mit adäquaten Schutzmaßnahmen in Hinblick auf Prozesse, Training und Technologien schafft ein sicheres Umfeld für Daten, Transaktionen und die Verfügbarkeit von Kern-Geschäftsprozessen.

Prozesse

Im Identity Management wird der Prozess für die Vergabe, Anpassung, Stilllegung und Auditierung von Zugriffsrechten pro Benutzergruppe beschrieben. Bei der Datenwiederherstellung ist sicherzustellen, dass bei Rücksicherungen von Daten keine Erweiterung von Zugriffsrechten erfolgen darf.

Ein weiterer wichtiger Prozess ist das sog. „Incident Management“, wo die Kommunikationslinien und Eskalationsstufen von Systemunterbrechungen festgelegt sind - von der Störungsmeldung des Benutzers, eines partiellen Systemausfalls bis hin zum Elementarereignis.

Business Continuity und Disaster Recovery Pläne

Im Analysefeld Business Continuity und Disaster Recovery geht es um den Aufbau von leistungsfähigen Notfall- und Krisenmanagement-Lösungen, die im Fall von anhaltenden Schadensereignissen wichtige Geschäftsprozesse aufrechterhalten oder so rasch wie möglich wieder herstellen.

Im ersten Schritt ermitteln die S&T Consultants gemeinsam mit dem Kunden die in seinem Unternehmen ablaufenden Geschäftsprozesse, analysieren und bewerten diese in Hinblick auf das Kerngeschäft des Unternehmens.

Die nächste Phase umfasst eine Identifizierung aller Arten von Ressourcen, die zum Ablauf der Kern-Geschäftsprozesse benötigt werden. In diesem Rahmen werden deren Wert innerhalb dieser



Prozesse sowie mögliche Gefahren und Schwachpunkte und die eventuellen Auswirkungen eines auftretenden Zwischenfalls auf das Geschäft festgestellt.

Die Ergebnisse einer Analyse der Geschäftsauswirkungen liefern wertvolle Informationen und bilden gleichzeitig die Grundlage eines Plans der Geschäftskontinuität sowie eines Plans zur priorisierten Behebung von Katastrophenfolgen für das Unternehmen.

Der von S&T angewandte risikobasierte Ansatz zur Informationssicherheit entspricht den geläufigen Information Security Standards und -verfahren.

Informationssicherheit – Bewusstsein und Schulung

Im Bereich der Unternehmenssicherheit ist der Mensch der kritischste Punkt. Mehr als 60 % der Verletzungen der Sicherheit werden durch menschliche Hand verursacht. Eine Steigerung des Sicherheitsbewusstseins und die Durchführung von Sicherheitsschulungen führen zu einer signifikanten Verringerung der auftretenden Sicherheitsvorfälle. Unser Schulungsportfolio richtet sich in zwei Phasen sowohl an Benutzer als auch Experten:

Zunächst entwickelt das S&T Information Security Consulting Team ein Bewusstseinsprogramm hinsichtlich der Informationssicherheit des Unternehmens und führt dieses vollständig ein. Webbasierte Lernprogramme unterstützen die effektive und interaktive Verbreitung der Inhalte. Zweitens werden für die Experten des Information Security Teams des Unternehmens Workshops mit sicherheitsrelevanten Themen abgehalten, um sie bezüglich führender Strategien und der zugehörigen Methoden auf dem Laufenden zu halten.

Vulnerabilitäts- u. Penetrationstest

Ein Penetrationstest ist eine aktive Bewertung der Sicherheitsmaßnahmen zum Schutz von Daten. Das gängigste Verfahren ist die aktive Analyse der Sicherheitsmaßnahmen in Bezug auf Design-Schwachstellen, technische Fehler und Anfälligkeiten.

Überprüfung der Informationssysteme

Überprüfungen von Information Security Systemen sind ein wesentlicher Teil von Wirtschaftsprüfungen. In vielen Ländern sind Finanzunternehmen und staatliche Unternehmen dazu verpflichtet, Überprüfungen der Informationssysteme durchzuführen und die Ergebnisse an die Behörden zu übermitteln.

S&Ts erfahrene, zertifizierte Prüfer für Informationssysteme (CISA; Certified Information Systems Auditors) und ISMS-Prüfer (ISO 27001) entwickeln vollständige Überprüfungsstrategien und -methoden für ihre Kunden und führen verschiedene Arten lückenloser Überprüfungen durch, um die Einhaltung festgelegter Richtlinien und Standards zu gewährleisten.