Nachhaltiger Aufbau eines ISMS

Sicherheit ist ein zentrales Thema in unserer vernetzten Welt. Immer mehr Informationen werden digital gespeichert und ausgetauscht. Die letzten Jahre haben darüber hinaus gezeigt, dass auch die Bedrohungslage durch Cyber-Angriffe stetig zunimmt. Deshalb ist es entscheidend, dass Unternehmen und Organisationen ein effektives Informationssicherheitsmanagement (ISMS) etablieren. Ein ISMS ist ein ganzheitlich gelebter Ansatz zur sicheren Verwaltung und Verarbeitung von Informationen und Daten in einem Unternehmen. Es umfasst Richtlinien, Verfahren, Prozesse und Technologien, die dazu beitragen, mindestens die drei primären Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

Die nachhaltige Investition in ein ISMS ist für Unternehmen und Organisationen meiner Meinung nach aus verschiedenen Gründen wichtig, darunter die folgenden.

- **Schutz vor Cyberangriffen**
  Ein ISMS hilft Unternehmen, ihre Informationen vor Cyberangriffen zu schützen. Es ermöglicht eine bessere Überwachung, Erkennung von Angriffen und Reaktion auf Bedrohungen, was das Risiko von erfolgreichen Cyberangriffen verringert.
- **Compliance**
  Viele Rechtsräume und Branchen haben spezifische Anforderungen für den Schutz von Informationen und Daten. Ein ISMS hilft Unternehmen, diese Anforderungen systematisch zu er fassen, zu bewerten und Compliance-Regeln einzuhalten. Also Beispiel sei hier die Regulierung von kritischen Infrastrukturen durch die EU NIS Directive und das deutsche IT-Sicherheitsgesetz genannt.
- **Vertrauen und Reputation**
  Kunden und Partner haben verstärkt hohe Anforderungen für Datenschutz und Informationssicherheit. Unternehmen, die in ein ISMS investieren, können das Vertrauen und die Reputation ihrer Kunden und Partner stärken. Als ein Nachweis der Umsetzung werden häufig Zertifikate wie ISO 27001, ISO 27001 auf Basis von BSI-IT Grundschutz, ISO 22301 oder spezifische Audits wie TISAX, SWIFT, PCI DSS oder eine KRITIS Nachweisprüfung angesehen.
- **Kosteneffizienz**
  Ein ISMS kann dazu beitragen, die Kosten für Datenschutz- und Informationssicherheitsmaßnahmen zu senken in dem es hilft die zur Verfügung stehenden Mittel auf die wirklich wichtigen Aspekte zu fokussieren. Durch eine bessere Kontrolle und Überwachung können Unternehmen ihre Ausgaben für Sicherheitsvorfälle und Compliance-Verstöße reduzieren.
- **Digitale Souveränität**
  Bei allen Investitionen, also auch beim Aufbau und Betrieb eines ISMS, sollten Unternehmen und Organisationen auf die Nachhaltigkeit der Mittelverwendung achten. Unter anderem bedeutet dies, dass die eingesetzten Komponenten robust und zukunftsfähig sind. Außerdem muss der Aspekt der digitalen Souveränität bedacht werden. Es sollte also die Möglichkeit bestehen die eingesetzten Komponenten nicht nur zu nutzen, sondern auch zu betrieblichen Zwecken anzupassen und weiterzuentwickeln. Bei herstellerspezifischen Komponenten gilt es den „Lock-In-Effekt" weitestgehend zu vermeiden.

Aus über 25-jähriger Beratungs- und Zertifizierungspraxis von Informationssicherheitsmanagementsystemen kann ich berichten, dass die allermeisten Unternehmen und Organisationen die genannten Aspekte „auf der Agenda" haben, bei der Umsetzung aber sicher noch einen nicht so kurzen Weg vor sich haben. Dieses Heft soll einen Beitrag dazu leisten die Themen erstens nochmal kompakt vorzustellen und zweitens zur Umsetzung anzuregen.

Wilhelm Dolle[1]

1 Wilhelm Dolle leitet als Partner der KPMG AG Wirtschaftsprüfungsgesellschaft den Bereich Cyber Security und ist Geschäftsführer der KPMG CERT GmbH. Er verfügt über mehr als 25 Jahre Berufserfahrung und ist Experte sowohl für technische als auch organisatorische Aspekte der Informationssicherheit. Darüber hinaus ist Wilhelm Dolle intensiv mit regulatorischen Anforderungen an die Informationssicherheit und das IT-Risikomanagement befasst. E-Mail: WDolle@kpmg.com