Plan

ISMS – KURZE EINFÜHRUNG

Ein ISMS ist ein unabdingbares System, um die IT-Sicherheit in Ihrem Unternehmen zu garantieren. Neben dem automatischen Schwachstellen-Monitoring müssen viele Systeme manuell geprüft werden und die nötigen Verantwortlichen sowie Verfahren sollten beschrieben sein, damit diese nicht vergessen werden.

Bei einem ISMS handelt es sich nicht um ein IT-System (wie der Name suggeriert), sondern um eine Sammlung von Dokumenten, etwa Leitlinien, Richtlinien und Verfahren – teilweise mit engem Bezug zur Organisation, zu Stellenbeschreibungen sowie zu vertraglichen Dokumenten zwischen Arbeitgeber und Arbeitnehmern oder Lieferanten.

Prozesse und Verfahren bis hin zu den Notfallplänen sollten korrekt aufgesetzt werden, um Angriffe zu vermeiden oder im Falle eines erfolgreichen Angriffs angemessen reagieren zu können. Auch Cyber-Versicherungen fordern zumindest Teile eines ISMS ab, um den eventuellen Schaden überhaupt zu übernehmen.

Compliance-Normen geben die Richtung und Struktur für ein ISMS vor. Allerdings sind diese Standards entweder sehr konkret und kleinteilig formuliert – mit Umfängen von bis zu 5.000 Seiten (z. B. BSI IT-Grundschutz, ISO 27000) – oder sie sind mittelstandsgerecht kompakt gehalten, mit etwa 50 Seiten und flexiblen Kategorien (z. B. VdS 10000). Letztere fordern jedoch keine konkreten IT-Prozesse und Verfahren ein.

Völlig unabhängig davon, welcher Norm Sie folgen möchten: Eine ISMS-Dokumentenstruktur oder der Umfang selbst ist **nicht** vorgegeben. Ein ISMS muss lediglich alle Anforderungen abdecken und gleichzeitig praktikabel nutzbar sein. Der praktische Nutzen ist erfüllt, wenn das ISMS für alle Mitarbeitenden leicht und schnell lesbar sowie verständlich ist, konkret in der Anwendung bleibt und zudem einfach zu pflegen ist.

Der schnelle Weg zu einem ISMS führt über einen Satz konkreter, vorgefüllter Dokumenten-Templates, die jeweils leicht miteinander korrelierbar sind, inklusive Kategorien und der geforderten Maßnahmen aller relevanten Normen. Genau das ist der CAIRO ISMS-Baukasten.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim

Plan

AUFBAU EINES MINI-ISMS

Ein ISMS aufzubauen **kann** ein größeres, mehrmonatiges Projekt sein, **muss es aber nicht**.

Je nach Situation kann das ISMS zunächst mit Word und Excel erstellt werden. Bei größeren Unternehmen sollten hingegen professionelle Tools wie Intervalid eingesetzt werden, um das ISMS nach der initialen Erstellung und dem Rollout sicher zu pflegen und die operative Sicherheit kontinuierlich zu begleiten.

Die schnellste und beste Reihenfolge für die Erstellung eines Mini-ISMS ist:

- Aufbau eines **Asset-Registers** mit Assets und Asset-Typen – immer beginnend mit den Applikationen als Träger von Geschäftsprozessen
- Definition und Beschreibung von „Kritischen Systemen“ (Geschäftsprozesse, Daten) von den **Applikationen** zu den **IT-Infrastruktur-Assets inkl. Netzwerk**:
    - Benutzer
    - Abhängigkeiten und Schutzklassen-Definitionen
    - BCM-Maßnahmen
    - Backup & Restore & Recovery (am besten ein 3-2-1 Backup)
    - Risiko-Analyse
    - Schwachstellen pro System
- **Notfallpläne** für IT und Anwender

Dies ist in wenigen Tagen mit gemeinsamen Aktivitäten zu erreichen.

AUFBAU EINES ISMS

Ein umfangreiches ISMS, das auch dazu dient, IT-Audits erfolgreich zu gestalten, erfordert deutlich mehr Unterlagen als ein Mini-ISMS. Dessen Erstellung ist eher ein Unternehmens-Steuerungsprojekt als ein reines IT-Projekt:

- 1 Leitlinie
- 20-30 Richtlinien (mit Arbeitsrollen, OrgCharts)
- 20-30 Verfahren und Handlungsanweisungen (mit Tools, Arbeitsrollen)
- 10 Prozess-Pläne, die die Abhängigkeiten und Reihenfolge der Richtlinien und Verfahren beschreiben
- Zusatz-Dokumente wie Formulare und Checklisten

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim