THEMENBLATT **GeschGehG**

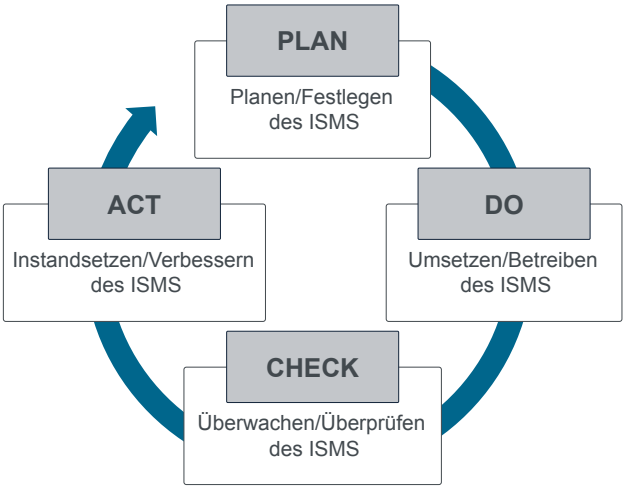
Gesetz zum Schutz von Geschäftsgeheimnissen – Auswirkungen auf die Informationstechnik

- ✓ Schaffung angemessener Geheimhaltungsmaßnahmen
- ✓ Verhinderung von Datenspionage und wirtschaftlichen Schäden
- ✓ Vermeidung von Imageverlusten und Schutz vor strafrechtlicher Verfolgung
- ✓ bewährtes Vorgehensmodell zur Herstellung von Informationssicherheit

Die Herausforderung

Mit dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) werden erneut Vorgaben der EU in deutsches Recht umgesetzt. Das neue Stammgesetz soll durch einen verbindlichen Rechtsrahmen die „Innovationsfähigkeit der deutschen Wirtschaft“ schützen. Aufgrund des weiten Wirkbereiches des Gesetzes finden sich auf den ersten Blick keine digitalen Aspekte wie in der DSGVO oder dem IT-Sicherheitsgesetz. Dennoch liegt die Vermutung nahe, dass sich aus dem Begriff „angemessene Geheimhaltungsmaßnahmen“ auch Auswirkungen für die Informationstechnik ergeben. Damit ist eine ganzheitliche Sicherheitsüberprüfung von IT-Systemen, die zur Verarbeitung und Speicherung schützenswerter Daten dienen, zwingend erforderlich.

Analog zu den Risikobewertungen beim Datenschutz und der Informationssicherheit kann auch für Geschäftsgeheimnisse ein Schutzbedarf ermittelt und definiert werden. Pauschal ist festzustellen: Je unternehmenskritischer der Datenbestand, desto höher der Schutzbedarf. Spezielles Wissen eines Unternehmens, dessen Offenlegung, ob nun fahrlässig durch eigene Mitarbeiter oder durch Spionage eines Wettbewerbers, unternehmenskritisch ist, verdient also eindeutig die Festschreibung eines hohen oder sehr hohen Schutzbedarfes. Außerdem sind laut Gesetz nur geschützte Daten tatsächlich auch Geschäftsgeheimnisse.



GeschGehG in der Praxis

In der Praxis der Informationssicherheit hat sich der Schutz solcher Daten anhand standardisierter Vorgehensmodelle und Kataloge bewährt. Auch eine Mitarbeitersensibilisierung und die Dokumentation der ergriffenen Maßnahmen zum Schutz von Geschäftsgeheimnissen sind dringend angeraten.

Hier bietet die jüngere Vergangenheit eine Reihe von Orientierungspunkten. Mit den ISO27xxx Normen und dem VDA-ISA-Standard liegen bereits praxiserprobte „Blaupausen“ für kritische Infrastrukturen (KRITIS) und die Automobilindustrie vor. Behandelt man Geschäftsgeheimnisse ebenso sorgfältig wie personenbezogene Daten, findet man weitere Orientierungspunkte in den technisch organisatorischen Maßnahmen des Bundesdatenschutzgesetzes – neu –.

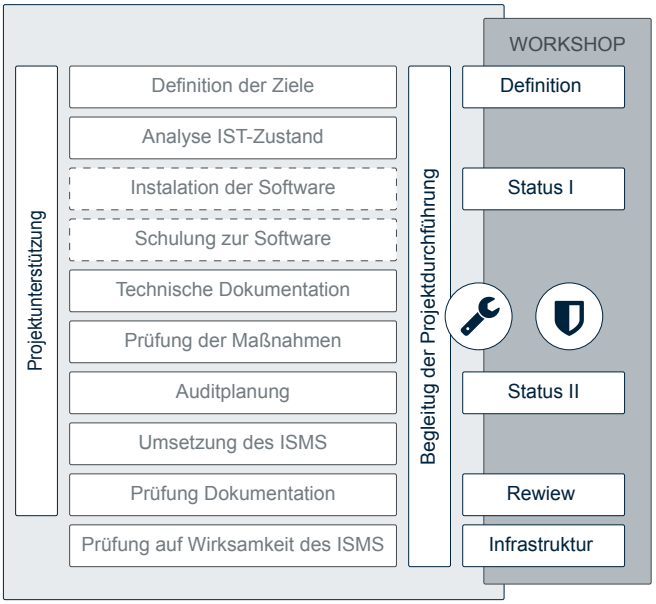
Resümierend kann festgestellt werden, dass das Gesetz zum Schutz von Geschäftsgeheimnissen nicht explizit auf den digitalen Umgang mit wichtigen Daten eingeht, aber durch die Gesamtverantwortung des Managements die Informationssicherheit zu einem elementaren Baustein der Rechtskonformität wird. Nur so kann letztendlich Compliance hergestellt werden.

THEMENBLATT **GeschGehG**

Gesetz zum Schutz von Geschäftsgeheimnissen – Auswirkungen auf die Informationstechnik

Unsere Unterstützung

Entsprechend Ihren Anforderungen sowie Zielstellungen unterstützt Sie procilon bei der Erstellung eines Informationssicherheitsmanagementsystems (ISMS) und damit zur Erreichung Ihres individuellen Sicherheitsniveaus.
Durch ein ISMS werden Regeln für die Einordnung von und den Umgang mit schützenswerten Daten und Objekten aufgestellt und umgesetzt. Das ISMS ist ein wichtiger Bestandteil des Managementsystems und zieht sich durch alle wichtigen Bereiche des Unternehmens. Zum ISMS gehören Verfahren zur regelmäßigen Überprüfung und Dokumentation organisatorischer, technischer sowie rechtlicher Änderungen.



Analyse

- komplette IT-Sicherheitsanalysen zur Erfüllung individueller Anforderung bzw. bekannter Standards, selbständig oder in Zusammenarbeit mit Ihren Mitarbeitern
- Erarbeitung von Empfehlungen und Durchführung von Schulungen zur Informationssicherheit

Beratung

- Beratung zur Einordnung der Themen und zum Vorgehen bei der Umsetzung des Vorhabens
- Beratung zu juristischen Themen
- Einführung Informationssicherheitsmanagementsystem

Umsetzung

- verschiedene standardisierte Workshops zur Vorbereitung, zum erreichten Stand und zur Prüfung der Umsetzung
- flexible und bedarfsgerechte Projektunterstützung in ver schiedenen Phasen der Umsetzung
- Bereitstellung von Mustern für die Dokumentation
- Einführung eines BSI-empfohlenen Informationssichereits managementsystems (ISMS)
- Einsatz eines externen Datenschutzbeauftragten

Ihre Vorteile

- zügiges Erreichen eines hohen IT-Sicherheitsniveaus
- Umsetzung Ihrer Zielstellung auf der Basis umfangreicher IT-Infrastrukturerfahrungen
- bedarfsgerechte und flexible Unterstützung
- Verwendung anerkannter Standards
- Herstellen der Compliance
- Erfüllen von Vorstandsvorgaben o. Auditor-Anforderungen
- umfangreiche elektronische Dokumentation
- Empfehlung individueller Lösungen

Zusätzliche Möglichkeiten

Mit i-doit ® steht ein bestens geeignetes ISMS-Tool zur Verfügung, welches IT-Prozesse optimal erfasst und dokumentiert. Zusätzlich eignet sich i-doit neben der Abbildung der IT-Infrastruktur durchaus auch für technisches-Security-Management (TSM). Weitere Synergien ergeben sich durch die Dokumentation von Verarbeitungsverzeichnissen, die laut EU-Datenschutzgrundverordnung geführt werden müssen.

T.I.S.P. TeleTrusT Information Security Professional

Kontakt

procilon GROUP
Leipziger Straße 110
04425 Taucha
+49 34298 48 78-31
anfrage@procilon.de
www.procilon.de

SecurITy made in Germany