



IT-Compliance / IT-Sicherheit & Datenschutz im Unternehmen

Ausgangslage

Nicht nur stark wachsende Unternehmen passen ihre Strukturen regelmässig dem gestiegenen Bedarf an. Auch für jedes andere Unternehmen gibt es gute Gründe, die IT und alle davon abhängigen Prozesse bereits vor einem Ausfall auf den Prüfstand zu stellen.

Als Mindestforderung gilt es, die gesetzlichen Auflagen zu erfüllen. Darüber hinaus ändern sich jedoch Geschäftsprozesse und interne Firmenrichtlinien wie z.B. EDV-Regelungen, Dienstreisen, Dateiablagen etc. ständig. Dies führt zu immer neuen Lösungen und Erweiterungen, die – unfachmännisch durchgeführt – immer komplexer und anfälliger werden.

Es gilt also die Stabilität der Geschäftsprozesse als existenzielles Gut sicherzustellen. Unternehmen, die erst bei öffentlich gewordenen Datenpannen, Gesetzesverstößen und Sicherheitsvorfällen reagieren, gefährden mitunter Ihre gesamte Existenz und verspielen Vertrauen. Daher muss die IT-Organisation regelmässig den jeweils aktuellen Gegebenheiten angepasst werden, so dass das Unternehmen stets über effiziente und kostengünstige Strukturen verfügt, die letztlich Grundlage der Wettbewerbsfähigkeit sind.

Vorgehen

Zunächst werden die Organisation, die Abläufe und die (IT-)Infrastruktur auf Schwachstellen und Sicherheitsrisiken untersucht. Das Heranziehen externer Sichtweisen ist dabei sinnvoll, denn jede interne Ressource entwickelt im Laufe der Zeit eine gewisse „Betriebsblindheit“.

Dieser völlig normale Vorgang wird jedoch in jenem Moment problematisch, wenn wesentliche Lücken oder gesetzliche Auflagen übersehen werden.

Im zweiten Schritt werden die aufgedeckten Schwachstellen auf organisatorischer Ebene minimiert und ein unternehmensweiter Basis-Schutz hergestellt. Dies kostet keinen Cent Investition.

Zusammen mit evtl. weiteren technischen Maßnahmen erhält das Unternehmen ein Gesamtkonzept, das eine ständige Anpassung an Gesetzes- und Sicherheitslage ermöglicht. Diese neuen Strukturen sind in wenigen Tagen etabliert, halten jedoch ein „Unternehmerleben“ lang.

Im Einzelnen werden folgende Anforderungen im Unternehmen untersucht:

- **IT-Compliance** (E-Mail-Archivierung, elektronische Aktenhaltung etc. mit Blick u.a auf Handels- & Steuerrecht, Arbeitsrecht etc.)
- **IT-Sicherheit** (Risiken zu internen und externe Angriffen, Zugriffsregelungen etc.)
- **Datensicherheit** (Back-up & Recovery-Strategien, Umgebungs- und Media-Handling)
- **Datenschutz** (Überprüfung des Datenschutz-Konzeptes zur Einhaltung des BDSG)

1. Schritt: Analyse der Schwachstellen im Unternehmen (IT-Check)

Beratungsziel ist die Entwicklung von Handlungsfeldern und Lösungsansätzen durch die Offenlegung von Schwachstellen und Risiken in den Abläufen sowie in der IT-Infrastruktur.

Unabhängige und neutrale externe Analyse des Status quo

- IT-Compliance: Prüfung der Einhaltung von Archivierungspflichten und –Fristen aus Handels- & Steuerrecht, Arbeitsrecht etc., Umgang und Speicherung von geschäftlichen, steuerrelevanten und privaten E-Mails. Analyse der betrieblichen Übung sowie internen Regelungen.
- IT-Sicherheit: Risiko-Analyse zu Lücken in der Abwehr von externen und internen Angreifern. Überprüfung der Sicherheitsmaßnahmen von Betriebs- und Geschäftsgeheimnissen, der Vertraulichkeit, Integrität und Verfügbarkeit bei der Geschäftsleitung und in den Fachbereichen.
- Datensicherheit: Untersuchung der Backup / Recovery-Strategie, der durchgeführten Sicherungszyklen und der Ergebnisse. Prüfung der Umgebungsvariablen und Lagerung / Umgang mit Sicherungsmedien und Bestimmung der Haltbarkeit (und somit des Schutzniveaus)
- Datenschutz: Überprüfung des Datenschutz-Konzeptes zur Einhaltung des BDSG, insbesondere Verfahrensverzeichnis, Schulung und Verpflichtung des Personals, technisch-organisatorische Maßnahmen etc. (Vorgehen wie bei einer Außenprüfung durch die Aufsichtsbehörde)

Aufwand:

Zu sämtlichen genannten Standards wird eine Bestandsaufnahme durchgeführt, dessen Aufwand sich regelmässig zwischen 3-5 Tagen bewegt – abhängig von der Unternehmensgröße und der Komplexität der Geschäftsprozesse.

Diese Aufwandschätzung der IST-Analyse beinhaltet alle Arbeiten, um zu einem abschließenden Ergebnis zu kommen, inklusive detailliertem Bericht und Erörterung vor Ort. Somit erfolgt diese Analyse als eigenständiges Modul.

Ergebnis:

Der Einhaltungsgrad der gesetzlichen und anderen Auflagen wird analysiert und grafisch dargestellt. Zusätzlich werden die gegenwärtigen Sicherheitsmaßnahmen mit anerkannten Sicherheits-Standards sowie den Ergebnissen anderer untersuchter Unternehmen in der gleichen Klasse (anonym) verglichen.

Abweichungen (positiv wie negativ) werden gesondert beleuchtet, Handlungsfelder priorisiert und individuelle Lösungswege ausgearbeitet.

Sämtliche Ergebnisse werden in einen strukturierten Bericht schriftlich dokumentiert, vor Ort präsentiert und mit der Geschäftsleitung erörtert. In der Diskussion werden weitere Schritte und Vorgehensweisen beratend begleitet.

2. Schritt: Risikominimierung und Schwachstellenbeseitigung

Beratungsziel ist die Beseitigung der entdeckten Schwachstellen aus Modul 1 durch Umsetzung der im Bericht empfohlenen Maßnahmen sowie eine Strategie der kontinuierlichen Anpassung zur Aufrechterhaltung des neuen, hohen Compliance- und Sicherheitsniveaus im Unternehmen.

Zielgerichtete und wirtschaftlich sinnvolle Umsetzung von gesetzlichen Auflagen und Sicherheitsmaßnahmen mit Elementen aus anerkannten Sicherheits-Standards

Ermittlung der gegenwärtigen Standards im Unternehmen zu

- IT-Compliance: Beratung beim Umgang mit elektronischen Dokumenten, insbesondere E-Mail zur Einhaltung der Archivierungspflichten und – Fristen aus Handels- & Steuerrecht. Beratung bei der Einhaltung von Löschrufen aus dem Datenschutzrecht, zu Zugriffsregelungen und Speicherung durch das Personal und zu den Anforderungen der Arbeitnehmervertretung (sofern vorhanden).
- IT-Sicherheit: Minimieren der Risiken und Stärken der Gefahrenabwehr bei internen und externen Angriffsszenarien individuell für das Unternehmen. Erstellen und Einführen von individuellen Sicherheitsrichtlinien, Schulung des Personals und Verpflichten auf die (neuen) Sicherheitsstandards. Beratung bei der Sicherung von Betriebs- und Geschäftsgeheimnissen etc.
- Datensicherheit: Beratung bei der Anpassung der Backup / Recovery-Strategie an die aktuellen Anforderungen, an den Stand der Technologie und beim Lagerung / Umgang mit Sicherungsmedien.
- Datenschutz: Beratung bei der Herangehensweise und Umsetzung eines Datenschutz-Konzeptes. Bei Bestellopflicht Berechnung der Wirtschaftlichkeit, ob ein interner Datenschutzbeauftragter oder ein externer DSB bestellt werden sollte. Beratung bei der Optimierung von Geschäftsprozessen und Dokumentation.

Aufwand:

Der Aufwand ist abhängig von Art und Anzahl der in Modul 1 identifizierten Schwachstellen und der sich daraus ergebenden Handlungsfelder.

Ergebnis: Ein modernes Unternehmen

Hoher Einhaltunggrad von gesetzlichen Auflagen, Beseitigung / Minimierung von Schwachstellen und Risiken, Schulung und Unterweisung des Personals zur Einhaltung direkt in den Abläufen, Vorbereitung zur Bestellung eines Datenschutzbeauftragten.

Fragen zu diesem Thema beantworten wir Ihnen gerne!

RKW Rheinland-Pfalz – 06131- 8937771 oder info@rkw-rlp.de

www.rkw-rlp.de