DIN SPEC 27076 – IT-Sicherheitsberatung für KMU

Viele KMU würden gerne mehr für ihre IT-Sicherheit unternehmen, wissen aber oftmals nicht wie. Bereits existierende Standardwerke zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS), wie das IT-Grundschutz-Kompendium des BSI oder die Norm ISO/IEC 27001, sind insbesondere für Unternehmen mit weniger als 50 Beschäftigen eine grosse Herausforderung beziehungsweise bedeuten einen riesigen Aufwand zur Umsetzung.

Um auch KMU zu unterstützen, wurde ein Konsortium zur Erarbeitung einer DIN SPEC gegründet. Insgesamt waren fast 20 Partner beteiligt. Das Ergebnis ist die DIN SPEC 27076 «IT-Sicherheitsberatung für kleine und Kleinstunternehmen» und der darauf basierende CyberRisikoCheck. Durch diesen können KMU bei IT-Dienstleistern eine standardisierte Beratung erhalten, die speziell auf ihre Bedürfnisse angepasst ist. In der DIN SPEC wurden auch die Handlungsempfehlungen standardisiert. Dadurch wissen sowohl Auftraggeber als auch Auftragnehmer, welche Leistung zu erwarten beziehungsweise zu erbringen ist.

Beim CyberRisikoCheck befragt ein IT-Dienstleister ein Unternehmen in einem ein- bis zweistündigen Interview zur IT-Sicherheit im Unternehmen. Darin werden 27 Anforderungen aus sechs Themenbereichen daraufhin überprüft, ob das Unternehmen sie erfüllt. Für die Antworten werden Punkte vergeben. Als Ergebnis erhält das Unternehmen einen Bericht, der unter anderem die Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält. Die Handlungsempfehlungen sind nach Dringlichkeit gegliedert. Gleichzeitig sensibilisiert der IT-Dienstleister das Unternehmen zu gängigen Gefahren. Wichtig zu beachten ist, dass der CyberRiskoCheck keine IT-Sicherheitszertifizierung ist. Er ermöglicht einem Unternehmen jedoch eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus und zeigt auf, welche konkreten Massnahmen ein Unternehmen umsetzen beziehungsweise bei einem autorisierten IT-Dienstleister beauftragen sollte.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Schauen wir etwas genauer in den Check hinein

Das Kapitel 4 definiert die Ziele (Ermittlung des IST-Zustandes, Unterbreitung von Handlungsempfehlungen, Sensibilisierung) und Grundsätze (Objektiv, nach bestem Wissen und Gewissen, keine Täuschung von Dritten, Unterschrift zur Bestätigung) sowie die Angemessenheit der Informationssicherheit.

Im Kapitel 5 werden die Anforderungen an die durchführenden IT-Dienstleister definiert. Der Berater muss über mindestens ein Jahr Erfahrung in der Durchführung von IT-Sicherheitsberatungen/Audits, mindestens drei Referenzprojekte bei KMU und das methodische Wissen verfügen.

Das Kapitel 6 beschreibt ausführlich die Durchführung der IT-Sicherheitsberatung. Diese erfolgt in vier Schritten:

1. Erstinformation des zu beratenden Unternehmens
2. Durchführung des Gespräches zur Erhebung des IST-Zustandes
3. Auswertung der Erhebungsdaten und Erstellung des Ergebnisberichts
4. Präsentation des Ergebnisberichts und Hinweis auf umzusetzende Handlungsempfehlungen

Die Erstinformation enthält die folgenden Aspekte: Ablauf, zeitlicher und personeller Aufwand, die am Prozess notwendigen

Bild: Pixabay

Um auch KMU zu unterstützen, wurde ein Konsortium zur Erarbeitung einer DIN SPEC gegründet.

Personen (insbesondere die Geschäftsleitung), die groben Themenbereiche sowie die Kosten.

Das Erstgespräch muss mindestens drei Stunden dauern. Es darf sowohl als Präsenztermin oder Online durchgeführt werden. Die Norm verlangt, dass die gesamte Geschäftsführung, falls vorhanden die für die IT- und Informationssicherheit zuständige Person und falls externe Dienstleister involviert sich auch diese, daran teilnehmen. Das Unternehmen muss bei diesem Gespräch die folgenden Dokumente, falls vorhanden, zur Verfügung stellen:

- Backup-Konzepte;
- Sicherheitsrichtlinien;
- Vertraulichkeitserklärungen;
- Betriebsanweisungen für die IT;
- Notfallpläne;
- Rollenkonzepte;
- Zugriffs- und Zutrittsrechte;
- Übersicht über die hauptsächlich genutzte Hard- und Software.

Risiko-Status errechnen

Im Gespräch gilt es festzustellen, ob die Anforderungen erfüllt sind oder nicht. Das Gespräch darf keine beratenden Anteile besitzen. Im Gespräch darf der Dienstleister dem befragten Unternehmen gegenüber nicht zu erkennen geben, ob eine Anforderung erfüllt wurde oder nicht. Dies könnte sehr schnell zu einem Beratungsgespräch führen.

Bei der Auswertung wird ein Risiko-Status errechnet. Jede der Top-Anforderungen erhält bei Erfüllung 3 Punkte, ansonsten bei Nicht-Erfüllung –3 Punkte. Jede der regulären Anforderungen erhält bei Erfüllung 1 Punkt, sonst 0 Punkte. Anforderungen müssen entweder als «erfüllt» oder «nicht erfüllt» bewertet werden. Eine Bewertung dazwischen, wie zum Beispiel «in Teilen erfüllt», darf nicht vorgenommen werden. Auch wenn rein rechnerisch ein negatives Total herauskommen könnte, ist der tiefste Wert 0.

Im Standard sind auch die Anforderungen an den Bericht haargenau beschrieben. Der Bericht sollte eine Länge von maximal zwei DIN-A4-Seiten umfassen. Der Inhalt der beiden Seiten ist in der Norm festgehalten. Auf der ersten Seite wird unter anderem das Ergebnis ausgewiesen. Die zweite Seite muss zunächst die zu priorisierenden Top-Handlungsempfehlungen und dann die weiteren ermittelten Handlungsempfehlungen in Listenform darstellen. Auch der Abschlusssatz ist definiert, inkl. der Zusicherung, dass der vorliegende Bericht nach bestem Wissen und Gewissen erstellt wurde. Danach folgt der Anhang des Berichts. Format, Schriftgrösse und Inhalt sind ebenfalls durch die Norm vorgegeben. Diese Vorgaben helfen, Berichte miteinander zu vergleichen.

Den Abschluss macht die Präsentation der Ergebnisse und Handlungsempfehlungen. Sie enthält eine detaillierte Erläuterung des Ergebnisses, Erklärung der priorisierten und weiteren Handlungsempfehlungen, die gängigsten Gefahren sowie das Aufzeigen von Möglichkeiten zur weiteren Förderung der IT- und Informationssicherheit.

Zusammenfassend ist die DIN SPEC 27076 eine geeignete Möglichkeit für KMU, schnell eine Übersicht über die Informationssicherheit zu bekommen. Der Bericht zeigt auf, was gut gelöst wurde und wo noch Schwächen bestehen. In der Folge können diese durch das Unternehmen in Angriff und geschlossen werden.

Die DIN SPEC 27076 kann kostenlos unter www.beuth.de/de/technische-regel/din-spec-27076/365252629 heruntergeladen werden. Vorgängig ist eine Registrierung notwendig.