Richtlinie zur Risikoanalyse

2.1 Einleitung

Die RECPLAST GmbH hat ein Managementsystem für Informationssicherheit (ISMS) etabliert, das dem Regelwerk „IT-Grundschutz“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt. Zentraler Bestandteil eines ISMS ist ua die Durchführung einer Risikoanalyse. Die vorliegende Richtlinie beschreibt die Vorgaben zur Durchführung einer Risikoanalyse.

2.2 Geltungsbereich

Die vorliegende Richtlinie gilt für die Risikoanalyse innerhalb des Managementsystems für Informationssicherheit (ISMS) der RECPLAST GmbH gemäß IT-Grundschutz. Der Geltungsbereich ist damit der Geltungsbereich des ISMS, wie in der Strukturanalyse beschrieben. Die Richtlinie gilt für die zuständigen Mitarbeiter.

2.3 Ansprechpartner

Ihr Ansprechpartner zu allen Fragen dieser Richtlinie:
Informationssicherheitsbeauftragte (ISB).

3 Prozessbeschreibung

3.1 Verantwortlichkeiten

Verantwortlich für die Durchführung der Risikoanalyse ist der oben genannten Ansprechpartner. Verantwortlich für die Risikoeinschätzung und Auswahl der Risikobehandlungsoptionen ist der jeweilige Risikoeigentümer, ggf in Abstimmung mit den Fachabteilungen. Verantwortlich für die Übernahme der Restrisiken ist die Geschäftsführung.

3.2 Methodik

Es wird eine Risikoanalyse nach folgender Methodiken durchgeführt: BSI-Standard 200-3 für alle Bereiche in denen es um Verfügbarkeitsanforderungen und bei denen belastbare Werte für den Faktor Eintrittshäufigkeit gegeben sind. Damit gelten grundsätzlich die Vorgaben des BSI-Standards 200-3, die durch die Vorgaben der vorliegenden Richtlinie konkretisiert werden.

3.3 Anwendungsbereich

Eine Risikoanalyse ist für alle Zielobjekte erforderlich, die - einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder - mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder - in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

3.4 Dokumentation

Die Risikoanalyse wird jährlich sowie anlassbezogen überprüft und aktualisiert.

Die Risikoanalyse liegt dokumentiert vor.

3.5 Risikobewertung

Die Risikobewertung setzt sich aus Eintrittshäufigkeiten und Schadenshöhe zusammen, die für einzelne Schadensszenarien betrachtet werden. Um eine nachvollziehbare, reproduzierbare und plausible Risikobewertung durchführen zu können, werden die nachfolgenden Rahmenbedingungen definiert.

3.5.1 Eintrittshäufigkeiten

Zur Eintrittshäufigkeit werden die folgenden Kategorien definiert:

- selten: Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten

- mittel: Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein

- häufig: Ereignis tritt einmal im Jahr bis einmal pro Monat ein

- sehr häufig: Ereignis tritt mehrmals im Monat ein

Bei der Durchführung der Risikoanalyse ist für jeden einzelnen Sachverhalt darauf zu achten, dass die individuelle Einschätzung zur Eintrittshäufigkeit nachvollziehbar und reproduzierbar ist. Aus diesem Grund ist eine entsprechende Dokumentation erforderlich.

3.5.2 Schadenshöhe

Zur Schadenshöhe werden die folgenden Kategorien definiert:

- vernachlässigbar: Die Schadensauswirkungen sind gering und können vernachlässigt werden, hier: unter 5000 Euro

- begrenzt: Die Schadensauswirkungen sind begrenzt und überschaubar, hier: 5001 Euro bis 50000 Euro

- beträchtlich: Die Schadensauswirkungen können beträchtlich sein, hier: 50001 bis 500000 Euro

- existenzbedrohend: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen, hier: mehr als 501000 Euro

Bei der Durchführung der Risikoanalyse ist für jeden einzelnen Sachverhalt darauf zu achten, dass die individuelle Einschätzung zur Schadenshöhe nachvollziehbar und reproduzierbar ist. Aus diesem Grund ist eine entsprechende Dokumentation erforderlich.

3.5.3 Risikobewertung

Ausgehend von der Eintrittshäufigkeit und der Schadenshöhe wird für jeden Szenario anhand der nachfolgenden Matrix die Risikobewertung vorgenommen: Abbildung 1: Risikomatrix

Die Risikokategorien sind dazu wie folgt definiert:

- gering: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz

- mittel: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus

- hoch: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung

- sehr hoch: Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung

Es wird die folgende Risikoakzeptanz definiert:

- Risiken der Kategorie „gering“ werden grundsätzlich pauschal akzeptiert; für diese Risiken ist keine weitere Risikobehandlung erforderlich, gleichwohl werden diese Risiken in der jährlichen Aktualisierung überprüft

- Risiken der Kategorien „mittel“, „hoch“ und „sehr hoch“ werden in die Risikobehandlung überführt

3.6 Risikobehandlung

Zur Risikobehandlung sind grundsätzlich die folgenden Optionen möglich:

- Reduktion: Risiken werden reduziert durch die Umsetzung weiterer Maßnahmen; durch diese Maßnahmen kann sowohl die Eintrittshäufigkeit gesenkt oder die Auswirkungen reduziert werden

- Akzeptanz: Restrisiken können von der Geschäftsführung akzeptiert werden; hierzu ist es erforderlich, dass die Geschäftsführung fundiert, vollständig, transparent und verständlich über die Restrisiken samt Folgen informiert wird

- Transfer: Risiken können auch transferiert werden, etwa an eine Versicherung

- Vermeidung: Risiken können auch aus dem Geltungsbereich des Informationsverbundes ausgeschlossen werden.

Die RECPLAST GmbH favorisiert die Option „Reduktion“. Eine Akzeptanz von Risiken, die aus der Nichterfüllung von Basis-Anforderungen resultieren, ist nicht zulässig.

3.7 Umsetzungsplan

Maßnahmen, die im Rahmen der Risikobehandlung umgesetzt werden sollen, werden in einem Umsetzungsplan nachverfolgt. Der Umsetzungsplan enthält insbesondere die folgenden Informationen:

- Maßnahme

- zugeordnetes Risiko aus der Risikoanalyse

- Verantwortlichkeiten

- Fristen

- Status

Maßnahmen gehen in das IT-Grundschutz-konforme Sicherheitskonzept ein, können also insbesondere zur Aktualisierung von Strukturanalyse und IT-Grundschutz-Check führen.

4 Inkrafttreten

Die Richtlinie tritt zum 01-11-2019 in Kraft.

Freigegeben durch: Geschäftsführung Bonn, 26-10-2019, UNTERSCHRIFT GF