Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Version 1.0

Leitfaden zur Schutzbedarfsanalyse

vom 14.10.2024

1 Einleitung

Dieser Leitfaden richtet sich an Unternehmen und Behörden die das Sicherheitsverfahren der Bundesverwaltung umsetzen möchten. Der blaue Text ist insbesondere relevant für Verwaltungseinheiten der Bundesverwaltung und andere Organisationen, welche dem Informationssicherheitsgesetz oder der Informationssicherheitsverordnung unterstellt sind.

Gemäss Art. 16 Absatz 1 ISG müssen verpflichtete Behörden für den Einsatz von Informatikmitteln ein Sicherheitsverfahren festlegen, das gemäss Art. 16 Absatz 2 Buchstabe a ISG eine Beurteilung des Schutzbedarfs mit umfasst. Dieser Leitfaden beschreibt ein Verfahren, mit dem der Schutzbedarf eines (möglicherweise aggregierten) Informatikschutzobjektes vor dessen Inbetriebnahme ermittelt werden kann. Das Verfahren wird summarisch als Schutzbedarfsanalyse bezeichnet.

Die zu verantwortende IT-Infrastruktur muss dazu vorgängig in eine Menge von Informatikschutzobjekten aufgeteilt werden. Dabei kann und wird sich ein Informatikschutzobjekt aus verschiedenen Informatikmitteln, wie z. B. Hard- und Softwarekomponenten, sowie darin gespeicherte, verarbeitete und übertragene Daten, zusammensetzen, die alle einem gemeinsamen und definierten Zweck dienen und deshalb auch logisch zusammengehören (z. B. Fachanwendung zur Abwicklung eines bestimmten Geschäftsprozesses). Informatikschutzobjekte, die ihre Dienstleistungen weiteren Informatikschutzobjekten zur Verfügung stellen, gelten als Plattforme und stellen selbst Informatikschutzobjekte dar. Beispiele sind eIAM, virtualisierte Serverinfrastrukturen und Software as a Service (SaaS) Angebote.

Ein Informatikschutzobjekt besteht dabei in der Regel nicht nur aus den Informationen, weil es nicht zweckdienlich wäre, für jede Art Dokument eine eigene Schutzbedarfsanalyse zu erstellen.

Grundsätzlich muss im Sicherheitsverfahren der Bundesverwaltung für jedes Informatikschutzobjekt der Schutzbedarf ermittelt und ausgewiesen werden. Für die Beurteilung des Schutzbedarfs werden nur die möglichen Auswirkungen im Falle einer Kompromittierung berücksichtigt. Welche Bedrohung zu dieser Kompromittierung führen kann, wird dabei nicht berücksichtigt.[1] Die Schutzbedarfsanalyse beurteilt damit, ob ein Risiko besteht, welches reduziert werden muss.

[1] So ist es z. B. für einen Datenverlust unerheblich, ob dieser auf fehlende Sicherungskopien, einen Hacker-Angriff oder einen böswilligen Mitarbeitenden zurückzuführen ist (in allen Fällen sind die Daten verloren).

Der Schutzbedarf von Informationen wird als erhöht oder nicht erhöht ausgewiesen, wobei dieser Ausweis pro Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Datenschutz) erfolgt. Zusätzlich zum Schutzbedarf werden auch die Sicherheitsstufen nach Art. 17 ISG ausgewiesen. Damit soll die darauffolgende Auswahl von sinnvollerweise einzusetzenden Massnahmen bei erhöhtem Schutzbedarf vereinfacht werden.

2 Verfahren zur Ermittlung des Schutzbedarfs

Mit dem im Folgenden beschriebenen Verfahren[2] kann Schutzbedarf und Sicherheitsstufe eines Informatikschutzobjektes ermittelt und damit auch festgestellt werden, ob der Schutzbedarf erhöht ist oder eben nicht. Das Verfahren umfasst zwei Schritte. In Schritt 1 wird das Informatikschutzobjekte beschrieben und ein Informationsverzeichnis erstellt. In Schritt 2 werden die möglichen Auswirkungen bei einer Verletzung der Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit und Datenschutz[3]) beurteilt.

Schritt 1

Das Informatikschutzobjekt und seine technische Ausgestaltung müssen möglichst detailliert beschrieben werden. Die folgenden Angaben sind dazu empfohlen, wobei die Angaben jederzeit (auch später) vervollständigt werden können:

a) Gegenstand und Ziele des Informatikschutzobjektes unter Nennung der betroffenen Geschäftsprozesse und Identifikatoren[4];

b) Beteiligte Leistungsbezüger und Leistungserbringer (soweit bekannt), sowie Personen mit konkreten Rollenangabe (z.B. ISBO, Schutzobjektverantwortliche, Projektleiter, …);

c) Technische Ausgestaltung (inkl. Entwicklungsumgebung und allfällig benutzte Plattformdienstleistungen) mit möglichst genauen, insbesondere auch die Netzwerksituation betreffenden Architekturskizzen;

d) Zugriffsberechtigungen (für Personen, -gruppen, Rollen und Prozesse);

e) Allenfalls vorhandene geografische Rahmenbedingungen (z.B. in welchen Ländern Informationen gespeichert werden und von wo aus zugegriffen wird).

Es muss ein Informationsverzeichnis erstellt werden, das alle Informationen enthält, die entweder vom Informatikschutzobjekte erzeugt, gespeichert, verarbeitet und/oder übertragen oder für die Bereitstellung des Informatikschutzobjektes benötigt werden. Die Informationen sind in sinnvoller Weise zu gruppieren. Die folgenden Angaben müssen für jede Informationsgruppe gemacht und dokumentiert werden:

a) Beschreibung der Informationsgruppe;

b) Allenfalls vorhandene und/oder erforderliche Klassifizierungen gemäss Art. 18, 19 und 20 ISV[5];

c) Angabe, ob eine Informationsgruppe auch Personendaten enthält, bzw. um welche

---

[2] Das Verfahren ist vom Rapid Risk Assessment vom Mozilla inspiriert (https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment).

[3] https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html

[4] Z. B. Projektname, Projekt Nr. / ID, usw.

[5] Bei «intern», «vertraulich» oder «geheim» klassifizierten Informationen sollte auch die Gruppe der Berechtigten mitangegeben werden. Das ist wichtig für die Erkennung von Risiken und später für die Auswahl von geeigneten Massnahmen.

Personendaten es sich handelt.

Schritt 2

Für jede Informationsgruppe aus dem in Schritt 1 erstellten Informationsverzeichnis muss geklärt werden, welche Auswirkungen eine Kompromittierung des Informatikschutzobjektes hätte. Dazu müssen mindestens die folgenden vier Fragen beantwortet werden:

a) Was würde passieren, wenn die Informationen offengelegt oder von Nachrichtendiensten oder ähnlichen Organisationen abgehört wird[6]? (Verletzung der Vertraulichkeit)

b) Was würde passieren, wenn die Informationen längere Zeit nicht zur Verfügung stehen? (Verletzung der Verfügbarkeit)

c) Was würde passieren, wenn die Informationen unautorisiert verändert werden? (Verletzung der Integrität)

d) Was würde passieren, wenn nicht lückenlos klar ist, durch wen Informationen nach deren Ersteingabe verändert wurden? (Verletzung der Nachvollziehbarkeit)

Für die Einstufung muss nun geprüft werden ob

a) diese Auswirkungen eine Beeinträchtigung der Informationssicherheit oder ein finanzielles Schadenspotential anhand der Kriterien aus Art. 28 ISV zur Folge haben könnte;

b) Gesetze und Verordnungen (z.B. Heilmittelgesetz, Firmengeheimnisse etc.) einen erhöhten Schutzbedarf rechtfertigen oder verlangen;

c) der oder die Datenschutzbeauftragte zum Schluss kommt, dass ein erhöhtes Risiko der Verletzung von Grundrechten der betroffenen Personen nach Art. 22 Absatz 1 DSG besteht[7];

d) die Auswirkungen für die Organisation nicht akzeptierbar sind[8].

3 Ergebnisse der Schutzbedarfsanalyse

Das in Kapitel 2 skizzierte Verfahren liefert eine Zusammenstellung von Informationsgruppen und möglichen Auswirkungen, die für das Schutzobjekt relevant sind, wobei die möglichen Auswirkungen nach Schutzzielen (d.h. Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit, sowie Datenschutz) ausgewiesen und bewertet sind.

Die Sicherheitsstufe (eines Informatikschutzobjektes) gemäss Art. 17 ISG wird anhand der folgenden Kriterien beurteilt:

a) Die Sicherheitsstufe «Grundschutz» gilt, sofern das Informatikschutzobjekt nicht höher eingestuft werden muss;

b) die Sicherheitsstufe «hoher Schutz» gilt, wenn an mindestens einer Stelle erhebliche Auswirkungen nach Art 28 Abs 1 ISV ausgewiesen sind oder «vertraulich» klassifizierte Informationen bearbeitet werden;

a) die Sicherheitsstufe «sehr hoher Schutz» gilt dann, wenn an mindestens einer Stelle

---

[6] Für klassifizierte Informationen kann die Frage mit Hilfe des Klassifizierungskataloges beantwortet werden.

[7] In der Bundesverwaltung wird für die Beurteilung mithilfe des Hilfsmittels zur Risikovorprüfung des Bundesamts für Justiz vorgenommen

[8] Dazu sollte die Organisation eine Business Impact Analyse durchführen und für ihre Geschäftsprozesse relevante Kriterien festlegen.

schwerwiegende Auswirkungen nach Art 28 Abs 2 ISV ausgewiesen sind oder «geheim» klassifizierte Informationen bearbeitet werden.

Das Informatikschutzobjekt und dessen Schutzbedarf wird als «Asset» inventarisiert.

Die Schutzbedarfsanalyse ist durch die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten der Verwaltungseinheit (ISBO) zu prüfen. Zur Prüfung gehört unter anderem auch die Kontrolle, ob die ausgewiesenen möglichen Auswirkungen plausibel sind und die Bewertung nachvollziehbar und gut begründet ist. Dazu sind ggf. weitere relevante Stellen mit einzubeziehen. Sofern auch Personendaten betroffen sind, sollte die Datenschutzberaterin oder der Datenschutzberater involviert sein. Im Rahmen von Projekten und Geschäftsprozessen ist es sinnvoll, dass die Schutzbedarfsanalyse von den Auftraggebern und Geschäftsprozessverantwortlichen genehmigt wird.

4 Weitere Schritte im Sicherheitsverfahren

Die Schutzbedarfsanalyse beurteilt, ob ein Risiko bestehen könnte, das reduziert werden muss. Bei nicht erhöhtem Schutzbedarf ergeben sich für die Organisation keine ausserordentlichen Risiken, welche eine erweiterte Risikoanalyse notwendig machen würden. Die minimalen Anforderungen an die IT-Sicherheit werden über Basisanforderungen (dem IT-Grundschutz (Si001)) abgedeckt. Diese müssen für jedes Informatikschutzobjekt umgesetzt werden.

Von besonderem Interesse sind die Auswirkungen, die für die Organisation erheblich oder schwerwiegend sind und zu einem erhöhten Schutzbedarf führen. Diese müssen mit geeigneten technischen und organisatorischen Massnahmen auf ein akzeptierbares Mass reduziert werden. Dabei sind zusätzlich die Weisungen für den erhöhten Schutzbedarf (P042) gemäss einem ISDS-Konzept umzusetzen. Das Zusammenspiel der Schutzbedarfsanalyse, dem IT-Grundschutz und dem Prozess bei erhöhtem Schutzbedarf ist in Abbildung 1 schematisch dargestellt.

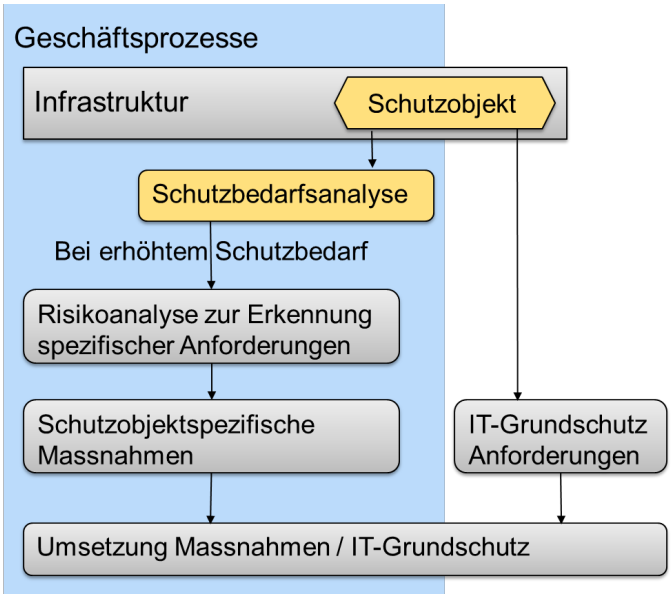

Abbildung 1: Schutzbedarfsanalyse als Teil des Sicherheitsverfahrens

Müssen vertraulich oder geheim klassifizierte Informationen an externe Betriebe übergeben werden oder sollen externe Betriebe an der Entwicklung, der Verwaltung, dem Betrieb, der Wartung oder der Überprüfung eines Informatikschutzobjektes mit Sicherheitsstufe «hoher

Schutz» oder «sehr hoher Schutz» beteiligt sein, muss ein Betriebssicherheitsverfahren gemäss VBSV eingeleitet werden.

Wenn Personendaten mit dem Informatikschutzobjekt bearbeitet werden, müssen möglicherweise auch ein Verzeichnis der Bearbeitungstätigkeiten nach Art. 12 DSG sowie ein Bearbeitungsreglement nach Art. 6 DSV (bei Bundesorganen) respektive Art. 5 DSV (bei privaten Personen) erstellt werden.

Eine Schutzbedarfsanalyse ist ein Artefakt in Projekten aber auch ein Teil der Dokumentation für jedes Informatikschutzobjekt. Ein Projekt kann mehrere Informatikschutzobjekte beinhalten, so dass es nicht zwingend nur eine (Informatikschutzobjekt-) Schutzbedarfsanalyse pro Projekt gibt. Die Schutzbedarfsanalyse muss bei Projekten früh in einer ersten Version abgeschlossen sein. Sie soll danach aber für die Dokumentation weitergeführt werden und muss zu jedem Zeitpunkt aktuell sein.