Anhang

Erläuterungen zu den Schadensszenarien

Im Folgenden sind für die in Kapitel 4.3.1 definierten Schadensszenarien beispielhafte Fragestellungen aufgeführt. Diese Fragen sollen als Hilfsmittel für die Schutzbedarfsfeststellung dienen, vor allem im Bereich der Anwendungen. Anhand der individuellen Anforderungen sollten die Fragen angepasst und ergänzt werden.

Schadensszenario "Verstoß gegen Gesetze/Vorschriften/Verträge"

Sowohl aus dem Verlust der Vertraulichkeit als auch der Integrität und ebenso der Verfügbarkeit können derlei Verstöße resultieren. Die Schwere des Schadens ist dabei oftmals abhängig davon, welche rechtlichen Konsequenzen daraus für die Institution entstehen können.

Beispiele für relevante Gesetze sind (in Deutschland):

Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, Bundesdatenschutzgesetz und Datenschutzgesetze der Länder, Sozialgesetzbuch, Handelsgesetzbuch, Personalvertretungsgesetz, Betriebsverfassungsgesetz, Urheberrechtsgesetz, Patentgesetz, Informations- und Kommunikationsdienstegesetz (IuKDG), Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG).

Beispiele für relevante Vorschriften sind:

Verwaltungsvorschriften, Verordnungen und Dienstvorschriften.

Beispiele für Verträge:

Dienstleistungsverträge im Bereich Datenverarbeitung, Verträge zur Wahrung von Betriebsgeheimnissen.

Fragen:

Verlust der Vertraulichkeit

- Erfordern gesetzliche Auflagen die Vertraulichkeit der Daten?
- Ist im Falle einer Veröffentlichung von Informationen mit Strafverfolgung oder Regressforderungen zu rechnen?
- Sind Verträge einzuhalten, die die Wahrung der Vertraulichkeit bestimmter Informationen beinhalten?

Verlust der Integrität

- Erfordern gesetzliche Auflagen die Integrität der Daten?
- In welchem Maße wird durch einen Verlust der Integrität gegen Gesetze bzw. Vorschriften verstoßen?

Verlust der Verfügbarkeit

- Sind bei Ausfall der Anwendung Verstöße gegen Vorschriften oder sogar Gesetze die Folge?
- Schreiben Gesetze die dauernde Verfügbarkeit bestimmter Informationen vor?
- Gibt es Termine, die bei Einsatz der Anwendung zwingend einzuhalten sind?
- Gibt es vertragliche Bindungen für bestimmte einzuhaltende Termine?

Schadensszenario "Beeinträchtigung des informationellen Selbstbestimmungsrechts"

Bei der Implementation und dem Betrieb von IT-Systemen und Anwendungen besteht die Gefahr einer Verletzung des informationellen Selbstbestimmungsrechts bis hin zu einem Missbrauch personenbezogener Daten.

Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts sind:

- Unzulässige Erhebung personenbezogener Daten ohne Rechtsgrundlage oder Einwilligung,
- unbefugte Kenntnisnahme bei der Datenverarbeitung bzw. der Übermittlung von personenbezogenen Daten,
- unbefugte Weitergabe personenbezogener Daten,
- Nutzung von personenbezogenen Daten zu einem anderen als dem bei der Erhebung zulässigen Zweck und
- Verfälschung von personenbezogenen Daten in IT-Systemen oder bei der Übertragung.

Die folgenden Fragen können zur Abschätzung möglicher Folgen und Schäden herangezogen werden:

Fragen:

Verlust der Vertraulichkeit

- Welche Schäden können für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht vertraulich behandelt werden?
- Werden personenbezogene Daten für unzulässige Zwecke verarbeitet?
- Ist es im Zuge einer zulässigen Verarbeitung personenbezogener Daten möglich, aus diesen Daten z. B. auf den Gesundheitszustand oder die wirtschaftliche Situation einer Person zu schließen?
- Welche Schäden können durch den Missbrauch der gespeicherten personenbezogenen Daten entstehen?

Verlust der Integrität

- Welche Schäden würden für den Betroffenen entstehen, wenn seine personenbezogenen Daten unabsichtlich verfälscht oder absichtlich manipuliert würden?
- Wann würde der Verlust der Integrität personenbezogener Daten frühestens auffallen?

Verlust der Verfügbarkeit

- Können bei Ausfall der Anwendung oder bei einer Störung einer Datenübertragung personenbezogene Daten verloren gehen oder verfälscht werden, so dass der Betroffene in seiner gesellschaftlichen Stellung beeinträchtigt wird oder gar persönliche oder wirtschaftliche Nachteile zu befürchten hat?

Schadensszenario "Beeinträchtigung der persönlichen Unversehrtheit"

Die Fehlfunktion von IT-Systemen oder Anwendungen kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiele für solche Anwendungen und IT-Systeme sind:

- medizinische Überwachungsrechner,
- medizinische Diagnosesysteme,
- Flugkontrollrechner und
- Verkehrsleitsysteme.

Fragen:

Verlust der Vertraulichkeit

- Kann durch das Bekanntwerden von Daten eine Person physisch oder psychisch geschädigt werden?

Verlust der Integrität

- Können Menschen durch manipulierte Programmabläufe oder Daten gesundheitlich gefährdet werden?

Verlust der Verfügbarkeit

- Bedroht der Ausfall der Anwendung oder des IT-Systems unmittelbar die persönliche Unversehrtheit von Personen?

Schadensszenario "Beeinträchtigung der Aufgabenerfüllung"

Gerade der Verlust der Verfügbarkeit einer Anwendung oder der Integrität der Daten kann die Aufgabenerfüllung in einer Institution erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele hierfür sind:

- Fristversäumnisse durch verzögerte Bearbeitung von Verwaltungsvorgängen,
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
- fehlerhafte Produktion aufgrund falscher Steuerungsdaten und
- unzureichende Qualitätssicherung durch Ausfall eines Testsystems.

Fragen:

Verlust der Vertraulichkeit

- Gibt es Daten, deren Vertraulichkeit die Grundlage für die Aufgabenerfüllung ist (z. B. Strafverfolgungsinformationen, Ermittlungsergebnisse)?

Verlust der Integrität

- Können Datenveränderungen die Aufgabenerfüllung in der Art einschränken, dass die Institution handlungsunfähig wird?
- Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Daten wahrgenommen werden? Wann werden unerlaubte Datenveränderungen frühestens erkannt?
- Können verfälschte Daten in der betrachteten Anwendung zu Fehlern in anderen Anwendungen führen?
- Welche Folgen entstehen, wenn Daten fälschlicherweise einer Person zugeordnet werden, die in Wirklichkeit diese Daten nicht erzeugt hat?

Verlust der Verfügbarkeit

- Kann durch den Ausfall der Anwendung die Aufgabenerfüllung der Institution so stark beeinträchtigt werden, dass die Wartezeiten für die Betroffenen nicht mehr tolerabel sind?
- Sind von dem Ausfall dieser Anwendung andere Anwendungen betroffen?
- Ist es für die Institution bedeutsam, dass der Zugriff auf Anwendungen nebst Programmen und Daten ständig gewährleistet ist?

Schadensszenario "Negative Innen- oder Außenwirkung"

Durch den Verlust einer der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit in einer Anwendung können verschiedenartige negative Innen- oder Außenwirkungen entstehen, zum Beispiel:

- Ansehensverlust einer Institution,
- Vertrauensverlust gegenüber einer Institution,
- Demoralisierung der Mitarbeiter,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Institutionen,
- verlorenes Vertrauen in die Arbeitsqualität einer Institution und
- Einbuße der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Innen- oder Außenwirkung.

Die Ursachen für solche Schäden können vielfältiger Natur sein:

- Handlungsunfähigkeit einer Institution durch IT-Ausfall,
- fehlerhafte Veröffentlichungen durch manipulierte Daten,
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
- Nichteinhaltung von Verschwiegenheitserklärungen,
- Schuldzuweisungen an die falschen Personen,
- Verhinderung der Aufgabenerfüllung einer Abteilung durch Fehler in anderen Bereichen,
- Weitergabe von Fahndungsdaten an interessierte Dritte und
- Zuspielen vertraulicher Informationen an die Presse.

Fragen:

Verlust der Vertraulichkeit

- Welche Konsequenzen ergeben sich für die Institution durch die unerlaubte Veröffentlichung der für die Anwendung gespeicherten schutzbedürftigen Daten?
- Kann der Vertraulichkeitsverlust der gespeicherten Daten zu einer Schwächung der Wettbewerbsposition führen?
- Entstehen bei Veröffentlichung von vertraulichen gespeicherten Daten Zweifel an der amtlichen Verschwiegenheit?
- Können Veröffentlichungen von Daten zur politischen oder gesellschaftlichen Verunsicherung führen?
- Können Mitarbeiter durch die unzulässige Veröffentlichungen von Daten das Vertrauen in ihre Institution verlieren?

Verlust der Integrität

- Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Daten ergeben?
- Wird die Verfälschung von Daten öffentlich bekannt?
- Entstehen bei einer Veröffentlichung von verfälschten Daten Ansehensverluste?
- Können Veröffentlichungen von verfälschten Daten zur politischen oder gesellschaftlichen Verunsicherung führen?

- Können verfälschte Daten zu einer verminderten Produktqualität und damit zu einem Ansehensverlust führen?

Verlust der Verfügbarkeit

- Schränkt der Ausfall der Anwendung die Informationsdienstleistungen für Externe ein?
- Verhindert der Ausfall von Anwendungen die Erreichung von Geschäftszielen?
- Ab wann wird der Ausfall der Anwendung extern bemerkt?

Schadensszenario "Finanzielle Auswirkungen"

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall von Anwendungen entstehen. Beispiele dafür sind:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Manipulation von finanzwirksamen Daten in einem Abrechnungssystem,
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
- unerlaubte Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen,
- Ausfall eines Buchungssystems einer Reisegesellschaft,
- Ausfall eines E-Commerce-Servers,
- Zusammenbruch des Zahlungsverkehrs einer Bank,
- Diebstahl oder Zerstörung von Hardware.

Die Höhe des Gesamtschadens setzt sich zusammen aus den direkt und indirekt entstehenden Kosten, etwa durch Sachschäden, Schadenersatzleistungen und Kosten für zusätzlichen Aufwand (z. B. Wiederherstellung).

Fragen:

Verlust der Vertraulichkeit

- Kann die Veröffentlichung vertraulicher Informationen Regressforderungen nach sich ziehen?
- Gibt es in der Anwendung Daten, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?
- Werden mit der Anwendung Forschungsdaten gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie unerlaubt kopiert und weitergegeben werden?
- Können durch vorzeitige Veröffentlichung von schutzbedürftigen Daten finanzielle Schäden entstehen?

Verlust der Integrität

- Können durch Datenmanipulationen finanzwirksame Daten so verändert werden, dass finanzielle Schäden entstehen?
- Kann die Veröffentlichung falscher Informationen Regressforderungen nach sich ziehen?
- Können durch verfälschte Bestelldaten finanzielle Schäden entstehen (z. B. bei Just-in-Time Produktion)?
- Können verfälschte Daten zu falschen Geschäftsentscheidungen führen?

Verlust der Verfügbarkeit

- Wird durch den Ausfall der Anwendung die Produktion, die Lagerhaltung oder der Vertrieb beeinträchtigt?
- Ergeben sich durch den Ausfall der Anwendung finanzielle Verluste aufgrund von verzögerten Zahlungen bzw. Zinsverlusten?
- Wie hoch sind die Reparatur- oder Wiederherstellungskosten bei Ausfall, Defekt, Zerstörung oder Diebstahl des IT-Systems?
- Kann es durch Ausfall der Anwendung zu mangelnder Zahlungsfähigkeit oder zu Konventionalstrafen kommen?
- Wie viele wichtige Kunden wären durch den Ausfall der Anwendung betroffen?