UNIVERSITÄT BIELEFELD

Informationssicherheitsbeauftragter

Schutzbedarfsfeststellung für IT-Verfahren

Hinweise

Bitte füllen Sie für jedes IT-Verfahren einen eigenen Fragebogen aus. Für Fragen steht Ihnen der Informationssicherheitsbeauftragte Michael Sundermeyer (-3032) gerne zur Verfügung.

1. Organisationseinheit [Dezernat, Fakultät, Bereich]

2. Bezeichnung des IT-Verfahrens

Ein IT-Verfahren besteht aus zusammenhängenden Arbeitsabläufen (Prozessen), in denen Daten automatisiert verarbeitet werden.

Zu IT-Verfahren gehören:

- Zusammenhängende Arbeitsabläufe, die arbeitsorganisatorisch eine abgeschlossene Einheit bilden wie zum Beispiel eine Studierenden- oder Prüfungsverwaltung, eine Haushaltsmittelbewirtschaftung, ein Forschungsdatenportal oder ein Bewerbermanagement.
- IT-Verfahren haben einen längerfristigen Charakter, sie werden nicht kurzfristig betrieben.

Einzelne Dateien oder ein Computer mit installierter Software sind keine IT-Verfahren.

3. Datenverarbeitende Stelle & Verantwortliche/r [Abteilung/Bereich, Name, Durchwahl]

Unter dem Begriff Datenverarbeitung wird u.a. das Erfassen, Speichern, Lesen, Verändern, Übermitteln, Sperren und Löschen von Informationen bzw. Daten verstanden.

Als verantwortlich wird eine Person bezeichnet, die zentrale*r Ansprechpartner*in der datenverarbeitenden Stelle ist, das Verfahren im Hinblick auf die datenverarbeitenden Prozesse betreut und dazu Auskunft geben kann.

4. Bewertungsmatrix für den Schutzbedarf von IT-Verfahren

Beeinträchtigung (Kategorie)	Bedrohung	Folgen des Schadens		
1. Beeinträchtigung der Aufgabenerfüllung	Unbefugte Einsicht in Daten (Verlust von Vertraulichkeit) Manipulation der Daten (Verlust von Integrität) Verlust der Daten (Verlust von Verfügbarkeit)	Für alle Benutzer des Systems tolerierbar …führt maximal zum Ausfall einzelner Arbeitsabläufe (tolerierbare Ausfallzeit mehr als einen Arbeitstag).	Für einzelne Benutzer des Systems nicht tolerierbar …schränkt die Aufgabenerfüllung in einem Teilbereich ein (tolerierbare Ausfallzeit zwischen einer und 24 Stunden).	Für alle Benutzer des Systems nicht tolerierbar …gefährdet den Gesamtauftrag der Universität (tolerierbare Ausfallzeit weniger als eine Stunde).
2. Negative Innen- und/oder Außenwirkung	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	**Geringer** Ansehens- und Vertrauensverlust eines Teilbereichs der Universität	Ansehens- und Vertrauensverlust der Universität bei einer **eingeschränkten** Öffentlichkeit oder Hoher Ansehensverlust eines Teilbereichs der Universität	**Landesweiter** Ansehens und Vertrauensverlust der Universität in der **breiten** Öffentlichkeit
3. Finanzielle Auswirkungen	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	Finanzieller Schaden weniger als ca. 150.000€	Finanzieller Schaden weniger als ca. 3 Millionen €	Finanzieller Schaden mehr als ca. 3 Millionen €
4. Beeinträchtigung der persönlichen Unversehrtheit	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	...erscheint nicht möglich	...kann nicht absolut ausgeschlossen werden	Gravierende Auswirkungen sind möglich (Gefahr für Leib und Leben).
5. Verstoß gegen Gesetze, Vorschriften und/oder Verträge	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	...verstößt gegen Gesetze oder Vorschriften mit **geringen** Konsequenzen ...hat geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge.	...verstößt gegen Gesetze oder Vorschriften mit **erheblichen** Konsequenzen. ...hat Vertragsverletzungen mit hohen Konventionalstrafen und/oder erheblichen Haftungsschäden zur Folge.	...verstößt **fundamental** gegen Gesetze oder Vorschriften ...hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die UniBi ruinös sind.
Notwendiger Schutzbedarf:		**normal**	**hoch**	**sehr hoch**

5. Ergebnisse der Bewertungsmatrix

Bitte die Ergebnisse aus der Tabelle unter Punkt 4 übertragen

Beeinträchtigungen (Kategorien)	Bedrohung	Abschätzung des Schadens		
1. Beeinträchtigung der Aufgabenerfüllung	Unbefugte Einsicht in Daten			
	Manipulation der Daten			
	Verlust der Daten			
2. Negative Innen- und/oder Außenwirkung	Unbefugte Einsicht in Daten			
	Manipulation der Daten			
	Verlust der Daten			
3. Finanzielle Auswirkungen	Unbefugte Einsicht in Daten			
	Manipulation der Daten			
	Verlust der Daten			
4. Beeinträchtigung der persönlichen Unversehrtheit	Unbefugte Einsicht in Daten			
	Manipulation der Daten			
	Verlust der Daten			
5. Verstoß gegen Gesetze, Vorschriften oder Verträge	Unbefugte Einsicht in Daten			
	Manipulation der Daten			
	Verlust der Daten			
Notwendiger Schutzbedarf:		**normal**	**hoch**	**sehr hoch**

6. Schutzbedarf der Anwendung nach Grundwert

[wird durch den Informationssicherheitsbeauftragten ausgefüllt]

Grundwert	Schutzbedarf	Begründung
Vertraulichkeit		
Integrität		
Verfügbarkeit		

7. Anhang

Erläuterungen zu den Schadensszenarien

Im Folgenden sind für die fünf betrachteten Kategorien beispielhafte Fragestellungen aufgeführt. Diese Fragen sollen als Hilfsmittel für die Schutzbedarfsfeststellung dienen, vor allem im Bereich der Anwendungen.

7.1 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?

7.2 Schadensszenario "Negative Innen- und/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,
- Nichteinhaltung von Verschwiegenheitserklärungen,
- Schuldzuweisungen an die falschen Personen,
- Verhinderung der Aufgabenerfüllung einer Abteilung durch Fehler in anderen Bereichen,
- 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?

7.3 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 Strategiepapiere oder Umsatzzahlen,
- Ausfall eines Buchungssystems einer Reisegesellschaft,
- Ausfall eines E-Commerce-Servers,
- Zusammenbruch des Zahlungsverkehrs,
- 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?

7.4 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?

7.5 Schadensszenario "Verstoß gegen Gesetze, Vorschriften und/oder 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?