

Gefährdungen geplant verhindern

Ingo Rauschenberg | ingo.rauschenberg@cms.hu-berlin.de
Roland Herbst | herbst@cms.hu-berlin.de

Meine Daten gehören mir ...

Vertraut man einer Einrichtung persönliche Daten an, wird mit Recht verlangt, dass diese treuhänderisch mit den ihr übergebenen Informationen im Zusammenhang mit Speicherung und Verarbeitung umgeht. An einer Hochschule sind beispielsweise folgende Prozesse davon betroffen:

- Bewerbung und Einreichung der Unterlagen zum Studium
- Eintragung von Prüfungsergebnissen
- Einsicht in Prüfungsergebnisse
- Bewerbung und Einreichung der Unterlagen als Mitarbeiter
- Erstellung von Zeugnissen
- Einsicht in Zeugnisse
- Zutritt zu Gebäuden und Räumen
- Erhebung personenbezogener Daten in Forschungsprojekten

Betrachtet man die Anzahl der IT-Systeme, die an einer Hochschule personenbezogene Daten verarbeiten, ist sofort ersichtlich, dass diese Liste um eine Vielzahl von Prozessen ergänzt werden könnte. Um zu verhindern, dass unberechtigte Dritte Einsicht in sensible Informationen erhalten, diese unbemerkt kopieren oder manipulieren können, werden von den IT-Verantwortlichen entsprechende Sicherheitsmaßnahmen, wie Firewalls, starke Authentifizierung, Verschlüsselung etc. ausgewählt und umgesetzt. Die häufig gestellte Frage nach dem Sinn dieser Maßnahmen ist schlüssig nur mittels eines Sicherheitskonzeptes zu beantworten. Im Sicherheitskonzept werden grundlegende Aspekte der Informationssicherheit betrachtet. Dabei geht es immer um den Zusammenhang zwischen einer eventuell vorhandenen Bedrohung, einer oder

Immer raffinierter werdende Angriffsmethoden erfordern die ständige Weiterentwicklung von Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Vor der Nutzung von IT-Systemen muss aus diesem Grund ein Sicherheitskonzept erstellt und umgesetzt werden. Welche Punkte dies beinhaltet und wie man zweckmäßig vorgehen sollte, wird nachfolgend vorgestellt.

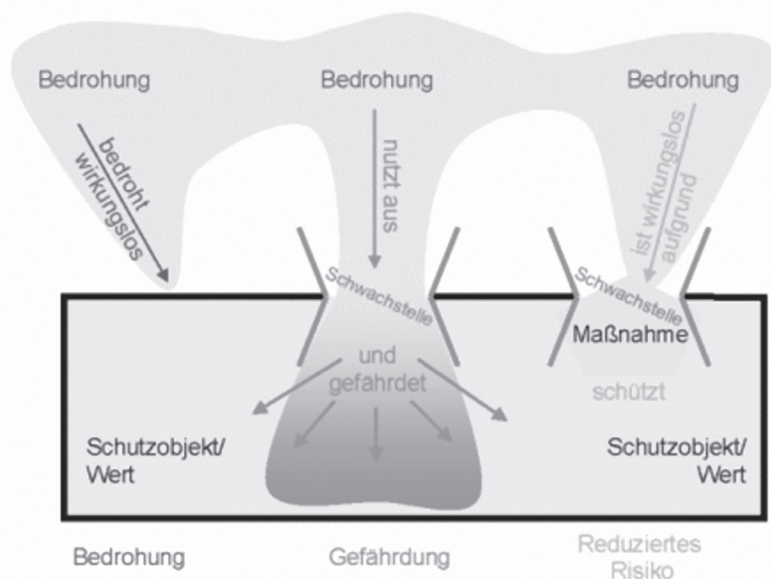


Abb. 1: Zusammenhang zwischen Bedrohung, Schwachstelle, Gefährdung und Maßnahme © [1]

mehrerer Schwachstellen und sich daraus ergebenden Gefährdungen. Am besten ist dies anhand einer Grafik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nachvollziehbar (Abb. 1).

Was verbirgt sich hinter dem Begriff der Informationssicherheit?[2]:

„Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken.“

Informationssicherheit ist dabei immer als Prozess zu verstehen, da sich IT-Systeme in ständigem Wandel befinden. Es kann z. B. vorkommen, dass ein heute noch als sicher betrachtetes System schon morgen durch das Auftreten eines sogenannten Zero-Day-Exploits – einer Schwachstelle, die ausgenutzt wird, bevor sie öffentlich bekannt wurde – so unsicher wird, dass die gesamte Sicherheit des Systems in Frage zu stellen ist. Wenn ein Anwender eine Sicherheitslücke in einem Programm oder einem IT-System erkennt, so wendet er sich im Allgemeinen an den Hersteller der entsprechenden Software oder an das entsprechende Open-Source-Projekt, um auf das bestehende Problem hinzuweisen. Der Hersteller programmiert dann einen sogenannten Patch, um diese Lücke zu schließen und stellt diesen zeitnah zur Verfügung. Wird der Hersteller nicht informiert bzw. ignoriert dieser die erhaltenen Hinweise auf die Sicherheitslücke, was leider keine Seltenheit ist, erlangt das Opfer erst nach einem erfolgreichen Angriff Kenntnis von der Existenz der Sicherheitslücke.

Dieser Fall zeigt, dass Informationssicherheit generell als Prozess verstanden werden muss. Allgemein gibt es hierfür das PDCA-Modell (Abb. 2). Der Prozess gliedert sich in:

1. Planung
2. Durchführung
3. Kontrolle
4. Agieren

Dies ist als geschlossener Kreislauf zu verstehen, denn als Ergebnis des Agierens wird wieder ein neuer Planungsvorgang angestoßen. IT-Sicherheit unter-

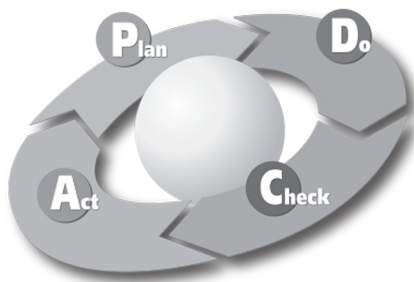


Abb. 2: Das PDCA-Modell stammt ursprünglich aus dem Qualitätsmanagement [3]

scheidet sich demnach nicht wesentlich vom allgemeinen Prozess der Software-Entwicklung.

BSI-Standards und Software-Tools

Das BSI stellt neben den im Kasten 1 beschriebenen Lage- und Jahresberichten eine Reihe von Hilfsmitteln zur Unterstützung bei der Erstellung und Umsetzung von Sicherheitskonzepten auf seiner Website zur Verfügung. Im Einzelnen sind das u. a.:

1. BSI-Standard 100-1 Managementsysteme für die Informationssicherheit [4]
2. BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise [5]
3. BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz [6]
4. BSI-Standard 100-4 Notfallmanagement [7]

Das BSI gibt in regelmäßigen Abständen (quartalsweise) Publikationen zur allgemeinen Lage der Informationssicherheit in Deutschland heraus. Darin werden die wichtigsten Bedrohungen für die Informationssicherheit behandelt. Es werden Informationen zu den Themen

- Angriffe und Ereignisse,
- Bedrohungen und Gefahren sowie
- Trends und Statistik

gegeben und erklärt. IT-Verantwortliche können diese interpretieren und Reaktionen darauf vorbereiten. Zusammengefasst für die Quartale 2/2010 und 3/2010 waren dies z. B. folgende [8]:

Angriffe und Ereignisse

- Angriff über Werbebanner
- Webserver Apache Tomcat als Sicherheitslücke
- DHL-Packstation weiter im Visier von Kriminellen
- PDF-Dateien bleiben beliebtes Angriffswerkzeug
- Stuxnet – ein Warnsignal für die IT-Sicherheit
- Trojaner Zeus stiehlt mobile TANs
- Voice over IP verstärkt im Visier von Angreifern
- Experiment beeinträchtigt Stabilität des globalen Internets

Bedrohungen und Gefahren

- der TwitterNET Builder: mit einem Mausklick zur Schadsoftware
- DLL-Schadsoftware arbeitet mit falschem Zertifikat
- Schadsoftware wird immer einzigartiger
- kritische Schwachstellen in Adobes PDF- und Flash-Programmen
- neuer Trojaner „Carberp“ späht Zugangsdaten aus
- Wie sicher sind Telefonate über GSM-Handys?

Trends und Statistik

- starkes Wachstum gestohlener Zugangsdaten
- Schadsoftware-Trends
- Zugangsdaten weiterhin heiß begehrt
- bösartige Datenströme vor allem aus Russland, Brasilien und Taiwan

Kasten 1: BSI-Publikationen zur allgemeinen Lage der Informationssicherheit in Deutschland

Im BSI Standard 100-1 werden Systeme für das Management der Informationssicherheit – Information Security Management Systems (ISMS) – beschrieben. Im Einzelnen geht es hier um eine Einführung in die Informationssicherheit, die Betrachtung des ISMS als Prozess und notwendige Management-Prinzipien. Es folgen Abschnitte über die Einbindung der Mitarbeiter in den Sicherheitsprozess, die Beschreibung des Sicherheitsprozesses und das eigentliche Sicherheitskonzept. Konsequenterweise gelangt man am Schluss zum IT-Grundschutz.

Der BSI Standard 100-2 thematisiert die Vorgehensweise für den IT-Grundschutz. Nach einer Einleitung werden für das Informationsmanagement mit IT-Grundschutz die einzelnen Schritte des Informationsmanagement-Prozesses beschrieben. Hier geht es um die Initiierung des Sicherheitsprozesses (A), die Erstellung und Umsetzung einer Sicherheitskonzeption nach IT-Grundschutz (P, D) und die Aufrechterhaltung und kontinuierliche Verbesserung (C, A) der Informationssicherheit (Abb. 3).

Auf Basis der nach BSI-Standard 100-2 gewonnenen Erkenntnisse ist im Anschluss eine Risikoanalyse durchzuführen. Dazu werden eine Gefährdungsübersicht erstellt und eventuell zusätzliche Gefährdungen ermittelt. Anschließend erfolgen eine Bewertung dieser und die Ermittlung der daraus resultierenden Risiken. Die dazu erforderlichen Schritte und die anschließende Rückführung in den Sicherheitsprozess werden im BSI-Standard 100-3 behandelt.

BSI-Standard 100-4 beschäftigt sich schließlich mit der Konzeption und Umsetzung eines Notfallmanagements. Auch hier erfolgt eine Prozessdefinition, die sich in die Phasen Konzeption (P), Umsetzung (D), Tests und Übungen (C), Aufrechterhaltung und kontinuierliche Verbesserung (A) aufgliedert.

Ergänzend zu den BSI-Standards wird vom BSI eine kostenpflichtige Software-Umgebung (GSTOOL) angeboten, mit der es möglich ist, den Informationssicherheits-Prozess in Form einer Datenbank mit Report-Funktionen umzusetzen und zu begleiten. Adressiert werden hier „erfahrene Anwender der IT-Grundschutz-kataloge“ [9]. Das Tool kann 30 Tage kos-



Abb. 3: Phasen des Sicherheitsprozesses [12]

tenfrei getestet werden. Eine Alternative zu dieser Software ist „verinice“ [10], eine Open-Source-Umsetzung der Inhalte der IT-Grundschutz-Kataloge.

Um diese Prozesse für den IT-Verbund der Humboldt-Universität vollständig umzusetzen, ist ein hoher organisatorischer, zeitlicher und personeller Aufwand notwendig. Dieser kann mit den aktuell vorhandenen Ressourcen nicht umfassend geleistet werden. In Abstimmung mit dem Behördlichen Datenschutzbeauftragten (behDSB) der Universität (siehe Artikel in diesem Heft) hat die Abteilung „DV in der Verwaltung“ des CMS der Humboldt-Universität eine alternative organisatorische Herangehensweise bezüglich des Prozesses der Erstellung und Umsetzung von IT-Sicherheitskonzepten etabliert. Dabei orientiert sich die Abteilung inhaltlich an den Grundschutz-Katalogen des BSI.

Dem Herangehen wurde das Berliner Datenschutzgesetz (BlnDSG) [11] zugrunde gelegt. Das Gesetz geht in § 5 (siehe Kasten 2) auf technische und organisatorische Maßnahmen ein, die bei der automatischen Verarbeitung personenbezogener Daten getroffen werden müssen, um die in Absatz 2 dieses Paragraphen beschriebenen Forderungen zu erfüllen. Zu diesen Forderungen gehören neben den eingangs erwähnten Faktoren Vertraulichkeit, Integrität und Verfügbarkeit der Daten zusätzlich deren Revisionsfähigkeit, Authentizität sowie die Transparenz der Datenverarbeitung.

In Absatz 3 dieses Paragraphen wird darüber hinaus gefordert, dass vor dem Einsatz einer automatischen Verarbeitung der Daten die technischen und organisatorischen Maßnahmen auf Grundlage einer Risikoanalyse und eines Sicherheitskonzeptes zu ermitteln sind. Weiterhin

Berliner Datenschutzgesetz

§ 5

Technische und organisatorische Maßnahmen

(1) Die Ausführungen der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Die Art und Weise der Maßnahmen hat für den angestrebten Schutzzweck angemessen zu sein und richtet sich nach dem jeweiligen Stand der Technik.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
 2. personenbezogene Daten während der Verarbeitung unversehr, vollständig und aktuell bleiben (Integrität),
 3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
 4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
 5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- und
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzeptes zu ermitteln. Dazu gehört bei Verfahren, mit denen Daten verarbeitet werden, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder die zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden, eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung.

Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 2 oder eine Modifizierung der automatisierten Datenverarbeitung verhindert werden können, darf ein Verfahren nicht eingesetzt werden.

(4) Werden personenbezogene Daten nicht automatisiert verarbeitet, so findet Absatz 2 Nr. 1 bis 4 entsprechende Anwendung.

(5) Die automatisierte Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

Kasten 2: Paragraph 5 des Berliner Datenschutzgesetzes

ist diese Ermittlung in regelmäßigen Abständen zu wiederholen, was auch hier den schon beschrie-

benen Kreislauf des Planens (P), Durchführens (D), Kontrollierens (C) und Agierens (A) erkennen lässt.

Bei der Herangehensweise des CMS werden die in §5 Absatz 3 geforderten Komponenten Risikoanalyse und Sicherheitskonzept, die vor der Inbetriebnahme eines datenverarbeitenden Systems vorliegen müssen, in einem Dokument zusammengefasst. Es werden neben der Risikoanalyse die Punkte beschrieben, die nötig sind, um die in Absatz 2 formulierten Anforderungen zu erfüllen.

Eine Vorabkontrolle des Sicherheitskonzeptes durch den behDSB, wie sie in Absatz 3 gefordert wird, ist nur in besonderen Fällen notwendig. Ein Beispiel ist die automatisierte Verarbeitung von Personaldaten. In den Fällen, bei denen die Kontrolle vor der Inbetriebnahme nicht vorgeschrieben ist, ist die zeitnahe Beteiligung des behDSB ebenfalls angeraten. Dadurch kann direkt auf kritische Rückmeldungen zu Fehlern oder Missständen bezüglich technischer oder organisatorischer Maßnahmen eingegangen werden und der Kreis im Prozess-Modell schließt sich wieder.

Weiterhin müssen im Falle der Mitbestimmung des Personalrates diesem das Sicherheitskonzept und die Stellungnahme des behDSB vorliegen.

Daneben kann eine rechtzeitige Beteiligung des behDSB, wie in seinem Artikel zum Thema „Datenschutz als Kommunikationsauftrag“ in diesem Journal beschrieben, auch bei der Projektplanung hilfreich sein. Hier kann die Einführung von Systemen, die aus datenschutzrechtlicher Sicht nicht tragbar sind, rechtzeitig verhindert und gemeinsam mit dem behSDB nach alternativen Lösungen gesucht werden.

Sicherheitskonzept

Wie bereits erwähnt, geht der CMS bei der Erstellung von Sicherheitskonzepten einen Kompromiss ein, der lediglich die Risikoanalyse und einen Teil der Anforderungen an ein Sicherheitskonzept nach den BSI-Grundschutz-Katalogen beinhaltet.

Um die Erstellung weiter zu vereinfachen, werden neue Sicherheitskonzepte in Anlehnung an bereits bestehende und durch den behDSB abgenommene Sicherheitskonzepte erstellt. Nachfolgend wird das von der Abteilung „DV in der Verwal-

tung“ des CMS verwendete Muster näher beschrieben. Die inhaltliche Gliederung entspricht den folgenden Abschnitten:

Abschnitt 1: Ziel, Motivation, Kurzbeschreibung

Dieser Abschnitt beinhaltet eine kurze, prägnante Beschreibung des IT-Systems, für welches das Sicherheitskonzept erstellt werden soll. Es ist davon auszugehen, dass das Sicherheitskonzept von außenstehenden Personen gelesen wird. Die Leser des Sicherheitskonzeptes sollen nach dieser Einführung grob verstehen können, welche Funktionen das IT-System besitzt und weshalb es betrieben werden soll.

Durch die Kurzbeschreibung wird der Forderung der Transparenz des BlnDSG Rechnung getragen.

Abschnitt 2: Verantwortlichkeiten

Die Verantwortlichkeiten beschreiben, welche Stelle, Einrichtung oder Abteilung für den Einsatz und den Betrieb des IT-Systems verantwortlich ist. Hierbei kann eine Unterscheidung zwischen technischer und inhaltlicher Verantwortlichkeit erfolgen, da der technische Betreiber eines Systems, typischerweise der CMS, sich von dem inhaltlich nutzenden und somit verantwortlichen Betreiber, zum Beispiel der Personalabteilung, unterscheiden kann.

Mit der Beschreibung der Verantwortlichkeiten für das IT-System wird der Forderung des BlnDSG nachgekommen, klarzustellen, wer für die Verarbeitung der personenbezogenen Daten verantwortlich ist.

Abschnitt 3: Gefährdungen

Bei der Erläuterung der Gefährdungen sollten explizit die Anwendungskomponenten des IT-Systems aufgezählt werden, bei denen eine besondere Gefährdung in Bezug auf personenbezogene Daten besteht. Weiterhin ist zu erklären, warum gerade diese Bereiche besonders gefährdet sind. Der Bezug der Gefährdung der personenbezogenen Daten zu den einzelnen Punkten des §5 Absatz 2 muss hier hergestellt werden.

Die Beschreibung von Gefährdungen ist Teil der Risikoanalyse.

Abschnitt 4: Beteiligte IT-Komponenten / Angriffe / Verteidigungskonzept

Allgemein sind für den Betrieb eines IT-Systems mehrere interagierende IT-Komponenten nötig. Alle Komponenten sollten hier dargestellt und deren Bedeutung für das System hervorgehoben werden.

Da nicht nur das IT-System selbst, sondern auch von diesem verwendete oder benötigte IT-Komponenten gefährdet sind, sollten in diesem Abschnitt besonders die möglichen Schwachstellen der Komponenten aufgezeigt werden. Dabei können mögliche Angriffsszenarien mit ihren Gegenmaßnahmen geschildert werden. Bei dieser Betrachtung ist ebenfalls eine Einschätzung zu geben, was ein erfolgreicher Angriff für das IT-System bedeutet.

Die Beschreibung der Komponenten, Angriffe, Folgen und des Verteidigungskonzeptes sind Teil der Risikoanalyse und sollten alle erdenklichen Fälle abdecken. Anhand dieser Analyse kann entschieden werden, ob ein Einsatz des IT-Systems trotz der aufgeführten Risiken denkbar ist.

Für den Teil der beteiligten IT-Komponenten, die nur von dem IT-System genutzt werden, jedoch nicht integrale Bestandteile sind, existieren gesonderte Sicherheitskonzepte. Daher ist es ausreichend, die Komponenten und deren Gefährdungen kurz zu beschreiben und für detailliertere Informationen auf die entsprechenden Sicherheitskonzepte zu verweisen. Als Beispiel nutzt AGNES die zentralen Datenbankserver der Verwaltung. Diese werden jedoch nicht ausschließlich von AGNES genutzt und in einem separaten Sicherheitskonzept behandelt.

Diese Verweise erübrigen die Aktualisierung aller Sicherheitskonzepte, wenn das Sicherheitskonzept eines IT-Systems geändert wird, das von vielen anderen IT-Systemen genutzt wird.

Abschnitt 5: Zugriffsrechte

Hier werden alle Arten von Zugriffsrechten aufgezählt. Dies beinhaltet neben den Zugriffen auf das IT-System auch Zugriffe (softwareseitig und phy-

sisch) auf die beteiligten Komponenten. Durch diese Beschreibung wird klar, welche Personen in welcher Weise Zugriff auf die personenbezogenen Daten haben und diese gegebenenfalls ändern können.

Die Erklärung der Zugriffsrechte trägt der Forderung nach der Vertraulichkeit aus dem BlnDSG Rechnung.

Abschnitt 6: Protokollierung, Beweissicherung

In diesem Bereich wird erläutert, auf welche Art der Zugriff und die Änderung von personenbezogenen Daten erfolgt und welche personenbezogenen Daten bei dieser Protokollierung zusätzlich anfallen. Somit betrifft die Protokollierung nicht nur das IT-System selbst, sondern auch die beteiligten IT-Komponenten. Sofern bei der Protokollierung personenbezogene Daten anfallen, z. B. IP-Adressen im Log eines Webservers, ist hier zu erklären, was mit den Protokolldaten geschieht. So sind Protokolldaten in bestimmten definierten Fristen zu löschen. Weiterhin müssen alle Auswertungen beschrieben werden, die auf Basis dieser Daten erstellt werden.

Die Beschreibung der Protokollierung und der Beweissicherung berücksichtigt die Forderung nach Verarbeitungstransparenz, Integrität und Authentizität der personenbezogenen Daten nach BlnDSG.

Abschnitt 7: Notfallvorsorge

In dem Bereich der Notfallvorsorge wird dokumentiert, was unternommen wird, um die im BlnDSG geforderte Verfügbarkeit der Daten zu gewährleisten. Werden z. B. bestimmte IT-Komponenten für das IT-System redundant vorgehalten, ist dies hier zu erklären. Weiterhin sind in diesem Bereich die Planungen für den Fall zu erläutern, dass bestimmte Notfallsituationen eintreten. Auch wenn es für eine dieser Situationen keine Lösung gibt, z. B. das Abbrennen des Serverraums, wird dies hier beschrieben.

Abschnitt 8: Datensicherung

Die Datensicherung trägt der Forderung des BlnDSG nach Verfügbarkeit der

Daten Rechnung. Es werden also die Maßnahmen beschrieben, die für die Sicherung personenbezogener Daten unter- nommen werden. Gibt es verschiedene Maßnahmen, so muss dokumentiert werden, für welche Fälle die jeweilige Sicherungsmaßnahme vorgesehen ist.

Abschnitt 9: Anhänge

In den Anhängen zum Sicherheitskonzept ist der Datenkatalog (Dateibeschriftung nach §19 Absatz 2 BlnDSG) aufzuführen. Weiterhin kann auf verschiedene Aspekte eingegangen werden, die nicht direkt für die Beurteilung des Sicherheitskonzeptes aus Sicht des Datenschutzes nötig sind. So können ein Betriebskonzept, eine detaillierte Beschreibung des IT-Systems mit Screenshots oder weiterführende Informationen zum Rollen- und Rechtekonzept aufgeführt werden.

Fazit

Das hier vorgestellte Verfahren zur Erstellung von Sicherheitskonzepten stellt einen weiteren Schritt in Richtung umfassender Sicherheitsrichtlinien für den Geltungsbereich der Humboldt-Universität dar. Eine kommende Aufgabe wird die Erstellung eines Sicherheitskonzeptes für virtualisierte Umgebungen sein, da sich dieses Thema gegenwärtig als Trend der zukünftigen IT-Entwicklung erweist.

Literatur / Abbildungen

- [1] © BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Zusammenhang zwischen Bedrohung, Schwachstelle, Gefährdung und Maßnahme*. https://www.bsi.bund.de/SharedDocs/Bilder/DE/BSI/Themen/Internet_Sicherheit/Begriff-Gefahrung_gif.gif?__blob=normal&v=2
- [2] *Informationssicherheit*. <http://de.wikipedia.org/wiki/Informationssicherheit>
- [3] CC BY KARN G. BULSUK: *Das PDCA-Modell stammt ursprünglich aus dem Qualitätsmanagement*. <http://blog.bulsuk.com>
- [4] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-1*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001.pdf?__blob=publicationFile
- [5] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-2*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf?__blob=publicationFile
- [6] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-3*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003.pdf?__blob=publicationFile
- [7] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-4*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004.pdf?__blob=publicationFile
- [8] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Lagebericht IT-Sicherheit 2009*. https://www.bsi.bund.de/cln_183/DE/Publikationen/Lageberichte/lageberichte_node.html
- [9] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *GSTOOL – Download*. https://www.bsi.bund.de/cln_156/DE/Themen/weitereThemen/GSTOOL/Download/download_node.html
- [10] VERINICE: *verinice-Downloads*. <http://www.verinice.org/download/>
- [11] *Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG)*. <http://www.datenschutz-berlin.de/attachments/346/BlnDSG2008.pdf>
- [12] © BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Phasen des Sicherheitsprozesses*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf?__blob=publicationFile
Seite 13