RUHR-UNIVERSITÄT BOCHUM

RUB

NR. 1047 | 18. JUNI 2015

AMTLICHE BEKANNTMACHUNG

RAHMENKONZEPT ZUR INFORMATIONSSICHERHEIT RUHR-UNIVERSITÄT BOCHUM

vom 18.06.2015

RAHMENKONZEPT ZUR INFORMATIONSSICHERHEIT RUHR-UNIVERSITÄT BOCHUM

Version 1.0-0.0
Stand 19.05.2015
veröffentlicht am 18.06.2015

INHALTSVERZEICHNIS

1 EINLEITUNG

Die erfolgreiche Durchführung der Geschäftsprozesse der Ruhr-Universität Bochum in Forschung, Lehre und Verwaltung ist in hohem Maße von einer zuverlässig funktionierenden Informations- und Kommunikationstechnik (IT) abhängig. Daraus erwächst ein hoher Anspruch an die Verfügbarkeit, Vertraulichkeit und die Integrität der verarbeiteten Informationen, IT-Verfahren und IT-Systeme der Ruhr-Universität Bochum.

Um diesem Anspruch gerecht zu werden, hat das Rektorat der Ruhr-Universität Bochum einen Koordinierungsausschuss für Informationssicherheit eingesetzt. Der Koordinierungsausschuss hat eine *Leitlinie zur Informationssicherheit* sowie das vorliegende, die Leitlinie präzisierende *Rahmenkonzept zur Informationssicherheit* erarbeitet. Darin werden Leitsätze, Strategien und Maßnahmen (Regeln) zur Sicherung der Informationsverarbeitung beschrieben. Die definierten Maßnahmen berücksichtigen die besondere Situation des kooperativen und respektvollen Miteinanders in einem universitären Umfeld. Insbesondere dient das Konzept nicht dazu, arbeitsrechtliche Sanktionen zu begründen.

Den Verantwortlichen der Einrichtungen der Ruhr-Universität Bochum werden Empfehlungen an die Hand gegeben, die sie bei der für die Erreichung der Sicherheitsziele ihrer Einrichtung erforderlichen Risikoanalyse und der Auswahl der daraus resultierenden Maßnahmen unterstützen. Soweit sich aus diesem Konzept Arbeits- oder Handlungsanweisungen für Mitarbeiterinnen und Mitarbeiter der Ruhr-Universität Bochum ergeben, sind diese gesondert bekanntzugeben, zum Beispiel durch eine schriftliche oder mündliche Anweisung des jeweiligen Vorgesetzten.

2 GRUNDSÄTZE

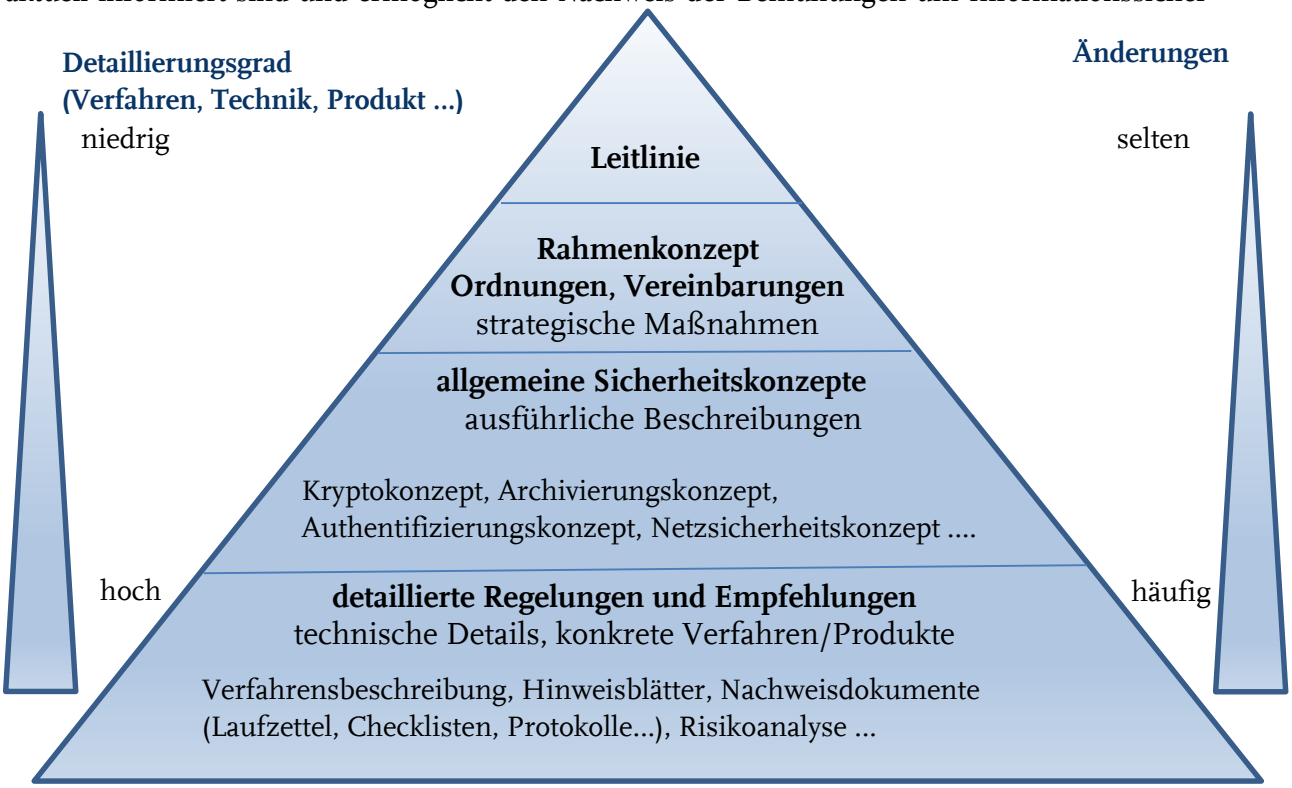
In der Leitlinie zur Informationssicherheit (☞[1] Leitlinie zur Informationssicherheit, Amtliche Bekanntmachung Nr. 872, 05/2011) der Ruhr-Universität Bochum hat das Rektorat die Prinzipien zur Ausgestaltung der Informationssicherheit an der Ruhr-Universität Bochum festgelegt.

Aufbauend auf diesen Prinzipien beschreiben die nachfolgenden Kapitel des vorliegenden Rahmenkonzepts Strategien und Maßnahmen, die der Sicherung der Informationsverarbeitung an der Ruhr-Universität Bochum dienen. Sie orientieren sich an den Anforderungen der international anerkannten Standards DIN ISO/IEC 27001/27002.[2] Jedes der Kapitel beginnt mit einer Motivation und einer allgemeinen Risikobetrachtung, aus der sich die Zielsetzungen der beschriebenen Maßnahmen ableiten. Die Wirksamkeit und Angemessenheit der Strategien und Maßnahmen wird in regelmäßigen Abständen überprüft, um das Informationssicherheitsniveau auch dauerhaft zu etablieren und zu verbessern.

Das Rahmenkonzept gilt für alle Einrichtungen der Ruhr-Universität. Bei der Umsetzung der Maßnahmen werden die Einrichtungen durch zentrale Angebote unterstützt.

2.1 Management der Dokumentation (Dokumentenlenkung)

Die Maßnahmen zur Informationssicherheit an der Ruhr-Universität Bochum werden angemessen, funktional und transparent dokumentiert. Dies gewährleistet, dass Mitglieder und Angehörige der Ruhr-Universität Bochum über Maßnahmen, Abläufe und Verfahren nachvollziehbar und aktuell informiert sind und ermöglicht den Nachweis der Bemühungen um Informationssicher-



[1] Zugriff zu den mit ☞ gekennzeichneten weiterführenden Informationen und Dokumenten sind über das separate Dokumentenverzeichnis in der jeweils aktuellen Fassung möglich (siehe auch Abschnitt 2.1).

[2] DIN ISO/IEC 27001:2015: IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen/ DIN ISO/IEC 27002:2014: IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management

heit gegenüber Dritten. Das vorliegende strategisch ausgerichtete Rahmenkonzept wird durch nachgelagerte Konzepte und Dokumente ergänzt. Durch den hierarchischen Aufbau der Dokumentation (Abbildung 1 Dokumentenhierarchie) werden die unterschiedlichen fachlichen Voraussetzungen und Aufgabengebiete der Beteiligten (Hochschulleitung, Benutzer, Administrator, Sicherheitsexperte) berücksichtigt. Im ☞ Dokumentenverzeichnis sind sämtliche Dokumente mit Kennzeichnung des Werdegangs (Dokumentenlenkung) aufgelistet. Es ist im Intranet über die Webseite der Stabsstelle für Informationssicherheit zugreifbar (☞ itsb.rub.de).

2.2 Organisationsstruktur der Informationssicherheit

1. An der Ruhr-Universität Bochum ist eine mehrstufige Organisationsstruktur für Informationssicherheit, bestehend aus einer Stabsstelle des Rektorates (geleitet von der oder dem zentralen Beauftragten für Informationssicherheit), dem Koordinierungsausschuss und den dezentralen Beauftragten für Informationssicherheit etabliert. Allen Einrichtungen wird empfohlen, eine/n dezentralen Beauftragten für Informationssicherheit zu benennen. Andernfalls nimmt die Leitung der Einrichtung diese Funktion wahr. Die Benennung muss schriftlich und im Einvernehmen erfolgen und bei Änderung der Zuweisung wieder entzogen werden. Die gültigen Zuständigkeiten sind der Stabsstelle für Informationssicherheit anzuzeigen. (☞ Leitlinie zur Informationssicherheit)
2. Die dezentralen Beauftragten für Informationssicherheit sind frühzeitig schon in der Planungsphase bei der Einführung oder Änderung von IT-gestützten Geschäftsprozessen in ihrer Einrichtung zu beteiligen. Die/Der zentrale Beauftragte für Informationssicherheit ist bei der Einführung oder Änderung von IT-gestützten Geschäftsprozessen mit einrichtungsübergreifender Wirkung sowie bei sonstigen Verfahren auf Verlangen zu beteiligen. (☞ Leitlinie zur Informationssicherheit)

2.3 Berechtigte Nutzer

1. Die Nutzung der IT-Infrastruktur der Ruhr-Universität Bochum ist nur Mitgliedern und Angehörigen erlaubt. Soweit und solange es im Interesse der Ruhr-Universität Bochum begründet ist, kann Dritten die Mitnutzung der IT-Infrastruktur gestattet werden. Art und Umfang sollen schriftlich festgehalten werden (☞ Nutzungserlaubnis für Dritte).
2. Die Nutzung der IT-Infrastruktur der Ruhr-Universität Bochum ist grundsätzlich den Zwecken von Forschung, Lehre und Studium sowie der Aus- und Weiterbildung und der Erfüllung sonstiger Aufgaben der Verwaltung der Ruhr-Universität Bochum vorbehalten. Eine private Mitnutzung der einem Mitglied oder einem/einer Angehörigen der RUB zur Verfügung gestellten Ressourcen ist zulässig, es sei denn, dienstliche Vorgänge, Ressourcen oder Normen werden erheblich beeinträchtigt. (☞ Datendiensteordnung)

2.4 Verantwortlichkeit

1. Die Leitung der Ruhr-Universität Bochum trägt die Gesamtverantwortung für die Informationssicherheit an der Ruhr-Universität Bochum. Sie hat sicherzustellen, dass die Einrichtungen der Ruhr-Universität Bochum in der Lage sind, eine angemessene Informationssicherheit an ihrer Einrichtung umzusetzen. Die Leitung jeder Einrichtung trägt in diesem Rahmen die Verantwortung für die Informationssicherheit an ihrer Einrichtung.
2. Die Leitung jeder Einrichtung hat sicherzustellen, dass der Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit (☞ Klassifikation von Informationen) der zum Einsatz kommenden IT-Anwendungen und IT-Komponenten sowie der dabei verarbeiteten Informationen korrekt festgestellt wird und angemessene Sicherheitsmaßnahmen implementiert werden. Die Aufgaben für die Umsetzung der Sicherheitsmaßnahmen sind klar zuzuweisen. Es wird empfohlen, schon frühzeitig bei der Erstellung von System- und Projekt-

Anforderungen (Pflichtenheft) Maßnahmen zur Informationssicherheit (insbesondere IT-Compliance-Anforderungen) zu berücksichtigen.

3. Alle Anwenderinnen und Anwender sind verpflichtet, die geltenden Regeln zur Informationssicherheit anzuwenden.

2.5 Grundsätze für den Einsatz von IT-Systemen und IT-Verfahren

1. IT-Systeme dienen dazu, die Effizienz und Qualität der Arbeits- und Geschäftsprozesse zu erhöhen. Vor- und Nachteile des Betriebs eines IT-Systems sind im Einzelfall unter Beachtung von Nutzen und möglichen Gefährdungen, insbesondere der IT-Infrastruktur, abzuwägen.
2. Elektronische Verfahren, die Geschäftsprozesse in Forschung, Lehre und Verwaltung unterstützen (IT-Verfahren), sollen angemessen dokumentiert werden. Bestandteile der Dokumentation können eine Beschreibung des IT-Verfahrens, ein Umsetzungs-, Betriebs- und Sicherheitskonzept sein. (☞ Hinweise zur Verfahrensdokumentation)

2.6 Datenschutz und IT-Compliance

1. Die Übereinstimmung von Regeln und Handeln, insbesondere die Einhaltung der Sicherheitsanforderungen, die sich aus diesem Rahmenkonzept sowie den Ordnungen und Dienstvereinbarungen der Ruhr-Universität Bochum zum IT-Einsatz ergeben, ist regelmäßig und in angemessenem Umfang zu überprüfen. (☞ Handlungsempfehlung zur Umsetzungsprüfung)

   Eine Prüfung muss insbesondere durchgeführt werden:

   a. bei Einführung neuer Prozesse und IT-Anwendungen,
   b. bei organisatorischen und infrastrukturellen Veränderungen,
   c. nach Sicherheitsvorfällen,
   d. bei veränderter Bedrohungslage.

2. Auskünfte und Übermittlungen von personenbezogenen Daten an Dritte (z.B. an Strafverfolgungsbehörden) sind nur in wenigen Ausnahmefällen gestattet. Hierbei sind geregelte Verfahren der Ruhr-Universität Bochum zur Behandlung von Auskunftsersuchen Dritter (z.B. zur Netzwerknutzung) einzuhalten. Dabei sind die rechtlichen Anforderungen, insbesondere des Datenschutzgesetzes NRW zu beachten. Das Vorgehen ist mit der/dem behördlichen Datenschutzbeauftragten, dem Justiziariat und/oder mit dem/der Beauftragten für Informationssicherheit abzustimmen. (☞ Merkblatt zur Übermittlung von Daten an Dritte)

2.7 Risikomanagement und Umgang mit IT-Sicherheitsvorfällen

1. An der Ruhr-Universität Bochum wird ein Risikomanagement etabliert, das dazu dient, mögliche Schäden für die Informationssicherheit frühzeitig zu identifizieren, zu bewerten, angemessene Gegenmaßnahmen zu benennen, akzeptierte Restrisiken zu kommunizieren und zu überwachen. Dazu gehört auch, dass Vorfälle, die die Informationssicherheit betreffen offen kommuniziert werden. (☞ Methoden zur Risikoeinschätzung und –behandlung)
2. Vorfälle, die die IT-Sicherheit der Ruhr-Universität Bochum beeinträchtigen, sind der oder dem zuständigen dezentralen Beauftragten für Informationssicherheit anzuzeigen. Alle Mitarbeiterinnen und Mitarbeiter einer Einrichtung sind über diese Meldepflicht zu unterrichten. Alle anderen Nutzer, die nicht Mitarbeiterinnen und Mitarbeiter der Ruhr-Universität sind (z.B. Studierende), sind aufgefordert, derartige Vorfälle zu melden. (☞ Sicherheitsrelevante Vorfälle)

3. Für die Meldung schwerwiegender Vorfälle, insbesondere rechtswidriger Nutzungen von IT-Systemen der Ruhr-Universität Bochum, sind definierte Meldeverfahren einzuhalten, die auch anonyme Meldungen vorsehen. (☞ Meldewege)

2.8 Abwehr von Gefährdungen

Bei Gefährdung der Informationssicherheit, die von den Beauftragten für Informationssicherheit, der/dem behördlichen Datenschutzbeauftragten, der Leitung einer betroffenen Einrichtung oder dem zentralen IT-Dienstleister der Ruhr-Universität Bochum festgestellt wird, veranlassen diese nach Risikoabwägung unverzüglich die notwendigen und angemessenen Maßnahmen. Bei erheblichen Gefährdungen kann dies insbesondere die Sperrung von Zugängen für die Nutzung eines IT-Verfahrens oder die Isolierung der gefährdenden oder gefährdeten IT-Systeme und Netze sein. Die Maßnahmen zur Gefahrenabwehr werden durch den zentralen IT-Dienstleister oder durch die Betreiber/innen der IT einer Einrichtung umgesetzt. Die Betroffenen sind der Gefährdung und der Maßnahme entsprechend zu informieren. (☞ Handlungsempfehlung zur Abwehr von Gefährdungen)

3 ORGANISATORISCHE UND PERSONELLE MAßNAHMEN

3.1 Motivation, Begriffe und Erläuterungen

Die Verbesserung der Informationssicherheit an der Ruhr-Universität Bochum lässt sich nicht allein durch den Einsatz technischer Maßnahmen erreichen. Informationssicherheitsmaßnahmen sind auch durch planvolle Abläufe auf organisatorischer oder personeller Ebene zu treffen. Mitarbeiterinnen und Mitarbeiter müssen die für ihren Arbeitsplatz gültigen internen Regelungen, einschlägigen Gesetze und Vorschriften kennen und einhalten. Durch Schulungen und Sensibilisierungsmaßnahmen sind das Problembewusstsein für die Belange der Informationssicherheit zu stärken und die erforderlichen Kenntnisse zu vermitteln. Die innovativsten Zugangskontrollen und Sicherheitsmaßnahmen für IT-Systeme und Netzwerk bleiben wirkungslos, wenn Benutzerinnen und Benutzer achtlos mit Zugangstoken und sensiblen Informationen umgehen und ihnen die damit verbundenen Risiken nicht bewusst sind.

3.2 Allgemeine Risikobetrachtung

IT-gestützte Geschäftsprozesse und die damit verarbeiteten Informationen sind einer Reihe von **Bedrohungen** ausgesetzt:

- Personalausfall,
- unzulässige Nutzung von Diensten,
- unbefugter Zugang zu Systemen,
- achtloser oder fahrlässiger Umgang mit Informationen und Systemen,
- bewusste Verletzung von Regelungen und Vorschriften.

Durch organisatorische **Schwachstellen** werden diese Bedrohungen begünstigt:

- unzureichende Information des Personals über geltende Regelungen,
- mangelnde Aus- und Fortbildung,
- unklare Aufgabenzuweisung,
- mangelnde Zeit und Überlastung des Personals,
- fehlende Vertretungsregelungen,
- mangelhafte Rechte- und Betriebsmittelverwaltung,
- fehlende, ungeeignete oder inkompatible Betriebsmittel.

Mögliche **Auswirkungen** können sein:

- Verlust, Ausspähen, Diebstahl oder Manipulation von Informationen,
- Störungen der Verfügbarkeit und Integrität unterstützender IT-Infrastruktur,
- Verletzung von gesetzlichen oder vertraglichen Vorgaben.

Als **Schäden** können für die Ruhr-Universität Bochum entstehen:

- Verlust von Arbeits- und Forschungsergebnissen,
- Haftungsrisiken durch Verletzung geltenden Rechts (z.B. Urheberrecht, Datenschutzrecht),
- Vertrauensverlust in den sachgerechten Umgang mit Informationen sowohl im Innen- wie im Außenverhältnis,
- finanzielle Aufwendungen für die Behebung von Schäden.

3.3 Verantwortlichkeiten

Die Organisationsverantwortung trägt das Rektorat der Ruhr-Universität Bochum.

Aufgabe der Leitung jeder Einrichtung der Ruhr-Universität Bochum ist es, unter Beachtung dieses Rahmenkonzeptes zur Informationssicherheit angemessene organisatorische und personelle Maßnahmen für ihre Einrichtung zu veranlassen.

3.4 Maßnahmen

3.4.1 Maßnahmen für das Personal der Ruhr-Universität Bochum

Informationssicherheit erfordert geregelte Verfahren im Personalmanagement einer Hochschule von der Einstellung in den Dienst (oder Funktionszuweisung) über Funktionsänderungen bis hin zum Ausscheiden aus dem Dienst.

Die in diesem Abschnitt beschriebenen Maßnahmen für Mitarbeiterinnen und Mitarbeiter in einem Dienst- oder Beschäftigungsverhältnis gelten auch für Personen, die über ein anderes Rechtsverhältnis entsprechende Funktionen für die Ruhr-Universität Bochum wahrnehmen.

1. Bei Einstellung oder Funktionszuweisung sind Mitarbeiterinnen und Mitarbeiter auf die Einhaltung einschlägiger Gesetze und Vorschriften (z.B. Datenschutz, Urheberrecht, Vertraulichkeitsgebot) sowie auf die Einhaltung interner Regelungen zur Informationssicherheit für ihren Arbeitsplatz zu verpflichten. Dies muss schriftlich erfolgen mit Aushändigung erforderlicher Informationen zu den Gesetzen und Regelungen. Auf neue oder geänderte Regelungen und Gesetze ist geeignet hinzuweisen. (☞ Gesetze und Regelungen)
2. Die Auswahl von Administratorinnen oder Administratoren sowie von Beauftragten zur Informationssicherheit muss aufgrund der besonderen Anforderungen an die Zuverlässigkeit und Vertrauenswürdigkeit dieser Personen sorgfältig erfolgen. Sie müssen über die erforderliche Fachkunde verfügen. Die Aufgabenzuweisung und deren Änderungen müssen schriftlich erfolgen.
3. Mitarbeiterinnen und Mitarbeiter müssen über die nötigen Kenntnisse für den sicheren Umgang mit den IT-Systemen ihres Arbeitsumfeldes verfügen. Regelmäßige und anlassbezogene Schulungen werden angeboten. (☞ Schulungskonzept zur Informationssicherheit)
4. Zur Aufrechterhaltung IT-gestützter Geschäftsprozesse sind angemessene Vertretungsregelungen festzulegen. Eine Übernahme im Vertretungsfall setzt voraus, dass die notwendigen Tätigkeiten ausreichend dokumentiert sind.
5. Mitarbeiterinnen und Mitarbeiter müssen mit den für die Ausführung der zugewiesenen Tätigkeit erforderlichen Rechten (Zutritt zu Räumen, Zugang zu Systemen, Zugriff auf Informationen) und Betriebsmitteln (Systeme, Lizenzen) ausgestattet werden. Bei Beendigung des Dienstverhältnisses oder Funktionswechsel ist darauf zu achten, dass die erteilten Berechtigungen und Betriebsmittel entzogen oder entsprechend angepasst werden. Rechtevergabe und der Rechteentzug sind schriftlich zu dokumentieren. (☞ Handlungsempfehlung zur Verwaltung von Berechtigungen)

3.4.2 Verwaltung der Betriebsmittel

Die Verwaltung von Betriebsmitteln (IT-Systeme, Software, Lizenzen etc.) muss vom Erwerb über die Wartung bis zur Entsorgung sorgfältig erfolgen.

1. Aspekte der Informationssicherheit sind Bestandteil der Beschaffungsrichtlinien der Ruhr-Universität Bochum. (☞ Beschaffungsrichtlinien der Ruhr-Universität Bochum) Um sicherheitsrelevante Anforderungen zu erfüllen, wird empfohlen, die zentralen Angebote zur Beschaffung von IT-Systemen zu berücksichtigen.
2. Bei Aufstellung und Betrieb der IT-Systeme sind die geltenden Dienstvereinbarungen zu berücksichtigen. (☞ Dienstvereinbarungen zur Aufstellung von IT-Systemen)
3. Für jedes in der Netzinfrastruktur der Ruhr-Universität Bochum betriebene IT-System müssen Personen benannt werden, die für den sicheren und ordnungsgemäßen Betrieb zuständig sind. Ist niemand benannt, so ist die Leitung der zuständigen Einrichtung verantwortlich.

4. Die Nutzung universitätseigener IT-Systeme außerhalb der Einrichtung darf nur mit Erlaubnis der jeweiligen Einrichtung erfolgen und ist z.B. über einen Leihschein zu dokumentieren.
5. Eine sichere Entsorgung von IT-Systemen und Informationsträgern ist zu gewährleisten. Zentrale Entsorgungsmöglichkeiten werden bereitgestellt. (☞ Handlungsempfehlung zur Entsorgung und Wartung)
6. Wartungen und Reparaturen an IT-Systemen sollen von eingewiesenem Fachpersonal durchgeführt werden. Werden IT-Systeme gewartet oder repariert, so hat die Leitung der Einrichtung für die Sicherheit schutzwürdiger Daten zu sorgen. (☞ Handlungsempfehlung zur Entsorgung und Wartung)
7. Für die auf IT-Systemen installierte Software müssen entsprechende Nutzungsberechtigungen (z.B. Lizenzen) vorliegen.
8. Geeignete Maßnahmen zum Schutz von Informationen und zum physischen Schutz von IT-Systemen sind zu treffen (z.B. Diebstahlschutz, sichere Verwahrung mobiler Systeme, sichere Serverräume, Datenverschlüsselung).

3.4.3 Benutzerverwaltung

Der Zugang zur Netzinfrastruktur, zu IT-Systemen und IT-Diensten der Ruhr-Universität Bochum muss auf Berechtigte eingeschränkt werden. Eine sorgfältige aufgabenbezogene Benutzerverwaltung und Datenstrukturierung ist die Grundlage für den angemessenen Schutz von Systembereichen und Dateibereichen von Benutzerinnen und Benutzern. Insbesondere muss der Umfang der Zugriffsberechtigung auf Informationen dem Aufgabengebiet von Benutzerinnen oder Benutzer entsprechen. Für Kennungen mit weitreichenden Rechten ist eine besondere Sorgfaltspflicht geboten.

1. Der Zugang zur Netzinfrastruktur, zu IT-Systemen und IT-Diensten der Ruhr-Universität Bochum muss durch ein angemessenes Verfahren geschützt werden. Dazu bietet die Ruhr-Universität Bochum ein zentrales Authentifizierungssystem (Identity-Managementsystem) an. In Abwägung der Gefährdungslage ist eine Zweifaktor-Authentifizierung anzuwenden; hierzu können z.B. die von der Ruhr-Universität Bochum zentral angebotenen Verfahren eingesetzt werden.
2. Mitglieder und Angehörige der Ruhr-Universität Bochum sowie von der Hochschulleitung autorisierte Dritte erhalten eine Benutzerkennung beim zentralen IT-Dienstleister der Ruhr-Universität Bochum. Diese wird im zentralen Identity-Managementsystem der Ruhr-Universität Bochum verwaltet.
3. Sämtliche Benutzerkennungen, die an der Ruhr-Universität Bochum vergeben werden, sollen grundsätzlich personengebunden und zeitlich beschränkt sein. Für die Einrichtung, Änderung, regelmäßige Überprüfung und den Entzug der Benutzerberechtigungen ist ein geregeltes und dokumentiertes Verfahren einzuhalten, das dem Stand der Technik entspricht.

Weitere Details regelt das ☞ RUB Authentifizierungskonzept.

4 ZENTRALE IT-DIENSTE

4.1 Motivation, Begriffe und Erläuterungen

Die Ruhr-Universität Bochum stellt zentrale IT-Grunddienste und zusätzlich erweiterte zentrale IT-Dienste bereit. IT-Grunddienste sind für den Geschäftsbetrieb der Ruhr-Universität Bochum als Ganzes unerlässlich. Bei allen zentralen IT-Diensten finden die Verfügbarkeit und die weiteren Aspekte von Datenschutz und Informationssicherheit in besonderem Maße Berücksichtigung.

Die zentralen IT-Dienste sollen zudem die Organisationseinheiten von fachfremden Dienstleistungen entlasten, die Beachtung definierter und einheitlicher Geschäftsprozesse begünstigen und universitätsweit ein bedarfsgerechtes Ressourcenmanagement ermöglichen. Als weitere Vorteile lassen sich die Mehrfachspeicherung und damit Inkonsistenz von Datenbeständen weitestgehend vermeiden, personelle und materielle Ressourcen wirtschaftlich einsetzen und Schnittstellen zu erforderlichen Folgeanwendungen zentral bereitstellen. Zudem können hochschulweite Geschäftsprozesse und zugehörige zentrale IT-Dienste einfacher aufeinander abgestimmt werden.

Vor- und Nachteile der Verwendung eines zentralen IT-Dienstes sind im Einzelfall unter den Aspekten Sicherheit, Wirtschaftlichkeit und Nutzungskomfort abzuwägen.

4.2 Allgemeine Risikobetrachtung

Analog mit der Verbreitung und Nutzung steigt auch das Gefährdungspotential eines IT-Dienstes, so dass zentrale Dienste besonderen Sicherheitsbetrachtungen unterzogen werden müssen. Die Art der **Bedrohungen** und **Schwachstellen** sind zunächst für alle Dienste (zentrale und dezentrale) vergleichbar. Das Risiko der Beeinträchtigung eines zentralen Dienstes steigt allerdings durch die signifikant größere Zahl der Nutzerschaft und der verarbeiteten Daten. Mit der Menge der von dem Dienst verarbeiteten Daten wächst in der Regel auch das „Interesse“ an diesen Daten.

Beispielsweise erhöhen Single-Sign-On-Funktionalitäten, die über eine einzige Authentifizierung mehrere Dienste verfügbar machen, das Risiko des unberechtigten Zugriffs auf geschützte Daten und somit die **Auswirkungen** möglicher **Schäden**. Andererseits lassen sich die Anforderungen von Datenschutz und Datensicherheit bei einem zentralen Dienst effizienter umsetzen. Eine professionelle Betreuung eines zentralen IT-Dienstes ist in der Regel eher zu gewährleisten, als dies bei lokal bereitgestellten IT-Diensten häufig möglich ist.

4.3 Verantwortlichkeiten

Für zentrale IT-Dienste ist die Leitung der Einrichtung zuständig, die sie bereitstellt. Die datenschutzrechtliche Verantwortung der Nutzer (Anwender und Einrichtungen) ist hiervon unbenommen. Die Anbieter der zentralen Dienste haben eine Mitwirkungspflicht bei der Umsetzung der datenschutzrechtlichen Anforderungen.

4.4 Maßnahmen

Die nachfolgenden Maßnahmen sind bei jeglicher, auch testweiser Bereitstellung zentraler IT-Dienste zu beachten.

1. Der zentrale IT-Dienstleister der Ruhr-Universität Bochum führt eine aktuelle Liste der zentral bereitgestellten IT-Grunddienste und erweiterten IT-Dienste und stellt sie den Nutzern zur Verfügung. (☞ Zentrale IT-Dienste)
2. Für alle zentralen IT-Dienste muss ein Informationssicherheitskonzept in Anlehnung an anerkannte Standards (z.B. BSI IT-Grundschutz) vorhanden sein, das der/dem zentralen Be-

auftragten für Informationssicherheit zur Kenntnis zu geben und den Nutzern (Anwender und Einrichtungen) in erforderlichem Umfang zur Verfügung zu stellen ist. (☞ Erstellung eines Informationssicherheitskonzepts)

3. Für die zentralen IT-Dienste werden Service Level Agreements (SLA) und Security SLA (SSLA) veröffentlicht. Die Nutzer werden dadurch über den Leistungsumfang, die Informationspflichten des Betreibers (z.B. bei Störungen), die zur Verfügung gestellten Schnittstellen und das Sicherheitsniveau informiert.
4. Werden zentrale IT-Dienste von Dritten und/oder für Dritte (z.B. Cloud-Dienste) angeboten, sind die Anforderungen dieses Rahmenkonzeptes durch gesonderte Vereinbarungen festzulegen. In solchen Fällen sind insbesondere die Regelungen aus Kapitel 12 „Leistungserbringung durch und für Dritte“ zu berücksichtigen.

5 GRUNDSICHERUNG DER NETZINFRASTRUKTUR

5.1 Motivation, Begriffe und Erläuterungen

Die Ruhr-Universität Bochum betreibt eine moderne, am aktuellen technischen Wissensstand orientierte Netzinfrastruktur, die dem Zugang zu IT-Systemen und IT-Diensten/-Anwendungen sowie der Datenübertragung und Kommunikation zwischen den Systemen (Intranet) und mit externen Endpunkten (Internet) dient. Auch Telekommunikation und Gebäudeleittechnik werden zunehmend auf diese Netzinfrastruktur gestützt.

Die Sicherheit, Funktions- und Leistungsfähigkeit der Netzinfrastruktur ist grundlegende Voraussetzung für den reibungslosen Ablauf der IT-gestützten Geschäftsprozesse in Forschung, Lehre und Verwaltung. Daher gilt es, sie durch angemessene Administration und Kontrolle vor Bedrohungen zu schützen und nur berechtigten Personen Zugang zu ermöglichen.

Die im Folgenden betrachtete Netzinfrastruktur umfasst grundsätzlich alle Kommunikations- und Datennetze der Ruhr-Universität Bochum. Dazu gehören auch zentrale Infrastrukturnetze wie das Telekommunikationsnetz (ISDN-Anlage), die Gebäudeleittechnik (GLT-Netz), die Brandmeldetechnik und das Stromnetz. Es bleibt zusätzlich zu berücksichtigen, dass zunehmend Querverbindungen zwischen diesen Netzen entstehen.

5.2 Allgemeine Risikobetrachtung

Die Netzinfrastruktur unterliegt einer Vielzahl von **Bedrohungen**, zum Beispiel durch
- Beschädigung der Verkabelung durch Baumaßnahmen, Umgebungseinflüsse (z.B. Starkstromkabel), Wasser-, Brandschäden oder Sabotage,
- Störung der Netzelektroniken durch Umgebungseinflüsse (z.B. Stromausfall), Maintenance-Vorgänge, Sabotage, Fehlkonfigurationen oder fehlerhafte Netzelektroniken,
- Überlastsituationen durch exzessive Nutzung, Schadcode, Fehlfunktionen,
- verändertes Benutzeraufkommen oder –verhalten
- Ausfall wichtiger externer Netzanschlüsse (z.B. Internet) oder
- Rechtemissbrauch.

Durch die nachfolgend beispielhaft genannten **Schwachstellen** erhöht sich die Anfälligkeit der Netzinfrastruktur der Ruhr-Universität Bochum für die genannten Bedrohungen:
- mangelnde Redundanz kritischer Komponenten,
- unzureichender Zugangsschutz, begünstigt durch unklare Verantwortlichkeiten sowie die Komplexität der Netzinfrastruktur mit abgesetzten Standorten.

Dies kann sicherheitsrelevante **Auswirkungen** nach sich ziehen:
- Das Universitätsnetz kann als Ganzes oder in Teilen für mehrere Stunden oder gar Tage ausfallen.
- Unberechtigte können Zugang zur Netzinfrastruktur erhalten und Integrität und Vertraulichkeit aller im Netz verarbeiteten und übermittelten Informationen gefährden.

Als **Schäden** können
- der Forschungs-, Lehr- und Verwaltungsbetrieb in erheblichem Maße beeinträchtigt werden,
- Verstöße gegen Gesetze, Verträge und Vorschriften,
- finanzielle Schäden,
- negative Innen- und Außenwirkungen
- oder Schäden für Leib und Leben (Gebäudeleittechnik) entstehen.

Durch geeignete Maßnahmen ist sicherzustellen, dass Schadensereignisse vermieden oder in ihrer Auswirkung minimiert werden. Die Durchsetzung der Maßnahmen wird durch die Hetero-

genität der Benutzerschaft in einem universitären Umfeld (Studierende, Mitarbeiterinnen und Mitarbeiter, Gäste und Dritte) erschwert.

5.3 Verantwortlichkeiten

Die Ruhr-Universität Bochum stellt zentral eine hochschulweite kabelgebundene wie auch kabellose Netzinfrastruktur bereit und ist für deren Betrieb verantwortlich. Für weitere zentrale und dezentrale Netzinfrastrukturen ist die betreibende Einrichtung zuständig. Diese Zuständigkeit umfasst insbesondere die Zulassung von Nutzerinnen und Nutzern, die über die Netzzugänge der Einrichtung Zugang zur Netzinfrastruktur erhalten. Dies schließt die Verpflichtung ein, durch geeignete Vorkehrungen sicherzustellen, dass nur Berechtigte Zugang erhalten.

5.4 Maßnahmen

5.4.1 Sicherheit der Verkabelung und der Netzkomponenten

Alle kabelgebundenen oder kabellosen Netzleitungen und -komponenten müssen vor Beschädigungen und Störungen geschützt werden.

1. Netzkomponenten dürfen grundsätzlich nur für Berechtigte zugänglich sein (z.B. durch Verwendung verschlossener Schränke oder Räume, Einschränkung des Zugangs für Konfigurations- und Diagnosearbeiten).
2. Normvorgaben für Netzkomponenten sind einzuhalten.

Detaillierte Vorkehrungen zur Sicherung der Netzinfrastruktur gegen Störungen und Ausfälle (z.B. Redundanzen, Wartungsverträge) werden gesondert festgelegt. (☞ Netzsicherheitskonzept der RUB)

5.4.2 Verwaltung und Überwachung der Netzinfrastruktur

Zur Sicherung der Netzinfrastruktur muss diese angemessen verwaltet und überwacht werden.

1. Zugänge zur hochschulweiten Netzinfrastruktur (z.B. über Netzdosen, Einwahlleitungen) werden ausschließlich vom jeweiligen Betreiber bereitgestellt. Der Betrieb von Funknetzen (z.B. WLAN, DECT, GSM) bedarf einer ausdrücklichen Genehmigung. (☞ Netzsicherheitskonzept der RUB)
2. Der jeweilige Betreiber überwacht die Netzinfrastruktur. Protokolldaten werden zur Bearbeitung von Störfällen gespeichert. Art, Umfang und Verarbeitung der Daten entsprechen den gesetzlichen Vorgaben und werden mit der/dem behördlichen Datenschutzbeauftragten und den Personalvertretungen abgestimmt.
3. Werden Räume der Ruhr-Universität Bochum mit Netzanschlüssen fremdvermietet oder ihre organisatorische Zuordnung geändert, so ist sicherzustellen, dass die jeweiligen Betreiber dieser Anschlüsse hiervon informiert sind.
4. Insbesondere zur Wartung der Netzinfrastruktur sind organisatorische und personelle Maßnahmen gemäß Kapitel 3 zu berücksichtigen.

5.4.3 Kontrolle der Netzinfrastruktur

Es ist sicherzustellen, dass nur Berechtigte Zugang zur Netzinfrastruktur erhalten.

1. Räume mit aktiven Zugängen zur Netzinfrastruktur, die nicht für den öffentlichen Gebrauch bestimmt sind, sind grundsätzlich verschlossen zu halten, solange keine zuständigen Personen anwesend sind.
2. Öffentlich zugängliche Netzzugänge (einschließlich Funknetze) sind mit einem angemessenen Authentifizierungsverfahren, mindestens durch Verwendung einer persönlichen LoginID mit Passwort, zu schützen (siehe Kapitel 3).
3. Alle Netze oder Netzsegmente müssen ihren Kommunikationsanforderungen entsprechend gesichert werden. Für den Anschluss privater Systeme sind spezielle Netzsegmente vorgesehen. Detaillierte Regeln für den Betrieb sind in einem separaten Netzsicherheitskonzept (☞ Netzsicherheitskonzept der RUB) formuliert.
4. Der direkte Zugriff aus dem Internet auf Systeme im Intranet der Ruhr-Universität Bochum bedarf eines geregelten Freigabeverfahrens. Zusätzlich wird ein gesicherter Zugang (z.B. VPN) bereitgestellt, dessen Verwendung für bestimmte Anwendungen vorgeschrieben werden kann. (☞ Netzsicherheitskonzept der RUB)
5. Ein Zugang zur Netzinfrastruktur der Ruhr-Universität Bochum oder zum Internet, der durch einen Netzdienst vermittelt wird (Zugangsserver, z.B. VPN-Server, Proxy-Server), muss eine angemessene Authentifizierung (mindestens durch Verwendung einer persönlichen LoginID und Passwort) vorsehen. Auf die Authentifizierung kann verzichtet werden, wenn nur bestimmte, explizit freigegebene Dienste, die der Aufgabenerfüllung der Hochschule dienen, zugänglich gemacht werden (z.B. Kioskserver).

5.4.4 Sichere Anbindung campusferner Standorte

Es dürfen nur definierte Übergänge zwischen der Netzinfrastruktur der Ruhr-Universität Bochum und der Netzinfrastruktur anderer Organisationen existieren.

1. Campusferne Standorte der Ruhr-Universität Bochum werden über universitätseigene oder angemietete Leitungen oder Wahlverbindungen an die Netzinfrastruktur der Ruhr-Universität Bochum angebunden.
2. Die Übergabepunkte und die Netzinfrastruktur an campusfernen Standorten werden nach Möglichkeit von der Ruhr-Universität Bochum verwaltet und überwacht. Sobald diese Zuständigkeit nicht realisierbar ist, ist sicherzustellen, dass die Vorgaben dieses Rahmenkonzepts beachtet werden.
3. In Abhängigkeit von der Schutzbedürftigkeit der Daten ist eine verschlüsselte Kommunikation (z.B. anwendungsbezogen oder über separate VPN-Tunnel) zu verwenden. Es ist zu beachten, dass der Datentransport zwischen den Übergabepunkten in die Fremdnetze standardmäßig unverschlüsselt erfolgt.

6 GRUNDSICHERUNG DER IT-ARBEITSPLÄTZE

6.1 Motivation, Begriffe Und Erläuterungen

Im Spannungsfeld zwischen größtmöglicher Handlungsfreiheit für Forschung und Lehre und der unabdingbaren Pflicht, IT-Systeme mit der gebotenen Sorgfalt und Sicherheit zu betreiben, hat die Eigenverantwortung der Benutzerinnen und Benutzer einen hohen Stellenwert. Jeder Nutzer soll sich – z.B. durch Inanspruchnahme dienstlich angebotener Schulungen und Informationsmaterialien – ein Grundverständnis für die Belange der Informationssicherung aneignen und Grundsicherungen der selbstgenutzten IT-Arbeitsplätze vornehmen.

Ungeachtet der Eigenverantwortung muss durch technische und organisatorische Maßnahmen dafür gesorgt werden, dass die Auswirkungen von Fehlverhalten, Unachtsamkeit oder von Schadcode weitgehend minimiert werden.

Unter einem IT-Arbeitsplatz wird im Folgenden ein IT-System verstanden, an dem Personen arbeiten können. Dieses System ist typischerweise vernetzt und fungiert als Klient im Netzwerk, d.h. es kann Dienste eines Servers (z.B. eines Webservers) über das Netzwerk anfordern, stellt aber selbst Dienste allenfalls im lokalen Netzwerk zur Verfügung. Soweit sich aus den angebotenen Diensten eine besondere Risikolage ergibt, z.B. dadurch, dass sie nicht lokal begrenzt sind oder sich an einen weiten Personenkreis wenden, sind zusätzlich die Regelungen aus Kapitel 8 zu beachten.

6.2 Allgemeine Risikobetrachtung

IT-Arbeitsplätze eröffnen den Zugang zur Netzinfrastruktur der Ruhr-Universität Bochum. Auf den IT-Systemen befinden sich zum Teil schutzwürdige Informationen wie Forschungsergebnisse oder personenbezogene Daten.

IT-Arbeitsplätze sind unter anderem folgenden **Bedrohungen** ausgesetzt:
- Ausfall des Systems durch technisches Versagen, Diebstahl oder fahrlässige Handlungen,
- fehlerhafte Administration (z.B. fehlendes Anti-Virus-Toolkit),
- menschliches Fehlverhalten (z.B. Hinterlegung von Zugangstoken am Arbeitsplatz, unerlaubte Verwendung geschützter Werke, versehentliches Löschen von Daten),
- unzulässige Nutzung (auch Nutzung des dienstlichen Arbeitsplatzes durch Unberechtigte),
- Angriffe von Hackern oder Computerkriminellen,
- Schadsoftware (z.B. schädliche E-Mail-Anhänge, Drive-by-Downloads).

Diese Bedrohungen werden durch eine Reihe von **Schwachstellen** im universitären Umfeld verstärkt:
- mangelnde administrative und organisatorische Kontrolle über die ans Netz angeschlossenen IT-Arbeitsplätze,
- unzureichend in IT-Sicherheitsfragen geschulte Benutzerinnen und Benutzer,
- unklare Verantwortlichkeiten und nicht oder mangelhaft geregelte Verfahren,
- unzureichende Ressourcen, z.B. mangelnde Zeit der Administratoren zur angemessenen Pflege der Systeme.

Die bestehenden Bedrohungen und Schwachstellen können vielfältige **Auswirkungen** zur Folge haben:
- die Übernahme und den Missbrauch eines Systems durch Angreifer,
- den Verlust, das Abhören, Ausspähen, Stehlen oder Manipulieren von Informationen,
- die unrechtmäßige Benutzung von urheber- oder lizenzrechtlich geschützten Werken,
- die Störung der Verfügbarkeit der Netzinfrastruktur, z.B. durch extensive private Kopiervorgänge.

Mögliche **Schäden** für die Ruhr-Universität Bochum sind:
- Haftung für Schäden Dritter,
- Haftung bei Verletzungen geltenden Rechts (Urheberrecht, Lizenzrecht etc.),
- Imageverlust in der Öffentlichkeit,
- Vertrauensverlust in den sachgerechten Umgang mit Informationen.

6.3 Verantwortlichkeiten

Die Leitung jeder Einrichtung der Ruhr-Universität Bochum ist für die von ihrer Einrichtung betriebenen IT-Arbeitsplätze zuständig. Sie hat durch geeignete Maßnahmen dafür zu sorgen, dass nur Berechtigte die IT-Arbeitsplätze nutzen können.

Alle Anwenderinnen und Anwender haben bestimmungsgemäß und sachgerecht mit den von ihnen genutzten IT-Arbeitsplätzen umzugehen. Sie sind verpflichtet, die für ihren Arbeitsbereich geltenden Regeln zur Informationssicherheit anzuwenden.

6.4 Maßnahmen

6.4.1 Management von IT-Arbeitsplätzen

1. IT-Arbeitsplätze müssen sachgerecht verwaltet werden. Dabei sind die Regelungen zur ordnungsgemäßen Verwaltung von IT-Betriebsmitteln nach Kapitel 3 einzuhalten.
2. IT-Arbeitsplätze stellen grundsätzlich keine IT-Dienste übers Netzwerk bereit. Ausnahmen sind nur in einem lokalen Netz oder über einen gesicherten Zugang (z.B. VPN der RUB) zulässig. *(☞ Netzsicherheitskonzept der RUB)*
3. Die Bereitstellung von Diensten durch IT-Arbeitsplätze ist sorgfältig unter Berücksichtigung von Vor- und Nachteilen (z.B. mangelnde Ausfallsicherheit, Sicherheitsmängel) abzuwägen. Abhängig von der Risikolage ist im Zweifel die/der zuständige Beauftragte für Informationssicherheit zu informieren. Eine angemessene Beschränkung des Zugangs (ausgewählte IP-Adressen, Benutzerkennungen) ist zu treffen.

6.4.2 Benutzerverantwortung

Die Mitarbeit von Benutzerinnen oder Benutzern ist für die Sicherstellung von Informationssicherheit essentiell. Insbesondere hat jede Benutzerin und jeder Benutzer Maßnahmen zu treffen, die den unberechtigten Zugriff auf Informationen bzw. deren Verlust oder Beschädigung verhindern.

1. Benutzerinnen und Benutzer sind verpflichtet, die für ihren Arbeitsplatz geltenden gesetzlichen und vertraglichen Regelungen sowie Verordnungen und Dienstvereinbarungen einzuhalten, sowie die Vorgaben dieses Rahmenkonzeptes und den darauf aufbauenden Maßnahmenkatalogen zu berücksichtigen. (☞ Gesetze und Regelungen)
2. Persönliche Passworte und Zugangstoken (z.B. Chipkarten) oder entsprechende Authentifizierungsmerkmale dürfen nicht weitergegeben werden. Es müssen qualitativ hochwertige Passworte verwendet werden. Bei der Auswahl der Authentifizierungsmerkmale ist der Schutzbedarf zu berücksichtigen. Authentifizierungsmerkmale dürfen nicht ungeschützt am Arbeitsplatz hinterlassen werden. (☞ Hinweise zum Passwortgebrauch)
3. Bei kurzzeitigem Verlassen des IT-Arbeitsplatzes ist dieser vor unberechtigtem Zugang zu schützen (z.B. durch Bildschirmschoner mit Authentifizierung). Bei längerfristigem Verlassen des Arbeitsplatzes, z.B. zu Dienstschluss, sind IT-Arbeitsplätze grundsätzlich herunterzufahren. Räume mit IT-Arbeitsplätzen, die nicht für den öffentlichen Gebrauch bestimmt sind, sind bei Nichtbenutzung grundsätzlich verschlossen zu halten.

4. Dienstlich relevante Datenbestände müssen abhängig vom Schutzbedarf gesichert werden. Dabei können zum Beispiel Verschlüsselungsverfahren nach dem Stand der Technik oder eine zentrale Verarbeitung unter Verwendung virtueller Desktops eingesetzt werden. Datenträger oder Unterlagen sind z.B. in verschließbaren Staumöglichkeiten aufzubewahren. Insbesondere bei Verlassen des Arbeitsplatzes ist sicherzustellen, dass schutzwürdige Informationen auf Datenträgern oder gedruckten Unterlagen nicht für Unberechtigte zugreifbar sind.
5. Dienstlich relevante Datenbestände (z.B. auch E-Mail) sollen im Verantwortungs- und Zugriffsbereich der Ruhr-Universität Bochum liegen. Unabhängig vom einzelnen Anwender müssen sie in angemessener Zeit für Berechtigte zugreifbar sein. Die Ablage solcher Daten auf Systemen Dritter (z.B. Cloud-Diensten) ist nur unter Berücksichtigung des Schutzbedarfs und möglicher rechtlicher Anforderungen zulässig. Ggfs. ist es erforderlich, dass zwischen Hochschule und Dritten gesonderte Vereinbarungen bestehen. (siehe Kapitel 12)
6. Bei Installation von Software ist unter Abwägung der potentiellen Risiken vorzugehen; entsprechende Nutzungsberechtigungen (z.B. Lizenzen) müssen vorliegen. Erscheint die Herkunft einer Software als nicht vertrauenswürdig, ist die/der zuständige Beauftragte für Informationssicherheit hinzuzuziehen.
7. IT-sicherheitsrelevante Vorfälle sind dem/der zuständigen Beauftragten für Informationssicherheit unverzüglich zu melden. (☞ Sicherheitsrelevante Vorfälle)

6.4.3 Administration des IT-Arbeitsplatzes

Alle IT-Arbeitsplätze müssen fachkundig administriert werden (☞ Grundsicherung von IT-Systemen). Den Organisationseinheiten der Ruhr-Universität Bochum wird empfohlen, die Administration der IT-Arbeitsplätze geschultem Personal zu übertragen. Ist dies nicht möglich, so sollten die zentralen Angebote der Ruhr-Universität Bochum zur Administration von IT-Arbeitsplätzen genutzt werden. (☞ Zentrale IT-Dienste)

1. IT-Arbeitsplätze sind so zu konfigurieren und administrieren, dass Benutzer ihre Verantwortung (siehe 6.4.2) wahrnehmen können. Benutzerinnen und Benutzer müssen über eingerichtete Schutzmaßnahmen und Protokollierungsfunktionen informiert sein.
2. Jeder IT-Arbeitsplatz ist nach Möglichkeit mit geeigneten Schutzmaßnahmen gegen Malware auszustatten, die in geeigneter Weise auf aktuellem Stand zu halten sind. Allen Mitgliedern und Angehörigen der Ruhr-Universität Bochum werden entsprechende Werkzeuge zentral zur Verfügung gestellt.
3. Betriebssystem und Anwendungsprogramme sind nach Möglichkeit regelmäßig und zeitnah mit Updates (Patches) auf aktuellem Stand zu halten. Dies gilt insbesondere für weit verbreitete Software wie Webbrowser, Office-Produkte oder auch Mediaplayer. Es empfiehlt sich, automatisierte Verfahren zur Aktualisierung zu verwenden.
4. Zur Sicherstellung der Integrität und Verfügbarkeit von Daten ist in Abhängigkeit des Schutzbedarfs eine regelmäßige Datensicherung (Backup) einzurichten. Dabei sind mindestens diejenigen Daten zu sichern, die nicht aus anderen Quellen (z.B. Installationsmedien) wieder abgeleitet werden können. Datensicherungen sollen auf angemessen gesicherten Medien vorzugsweise automatisiert erfolgen und regelmäßig auf Funktionsfähigkeit überprüft werden. Die Nutzung zentraler Angebote zur Datensicherung wird empfohlen. (☞ Zentrale IT-Dienste)

7 EXTERNER ARBEITSPLATZ UND PRIVATE SYSTEME

7.1 Motivation, Begriffe und Erläuterungen

Der Einsatz privater (mobiler) Systeme für dienstliche Zwecke ist im universitären Umfeld seit jeher üblich und wird in Zukunft durch die zunehmende Verbreitung mobiler Geräte (Smartphones, Tablets, etc.) weiter steigen. Im Bereich Forschung und Lehre ist es gängige Praxis, dass Mitarbeiterinnen und Mitarbeiter Arbeitsleistungen sowohl am universitären wie auch am externen Arbeitsplatz unter Nutzung privater sowie universitätseigener (mobiler) Systeme erbringen.

Während diese Entwicklung im Hinblick auf die Produktivität und Zufriedenheit der Anwenderinnen und Anwender sowie die zeitliche und räumliche Flexibilisierung der Arbeitsorganisation zielführend ist, ergeben sich dadurch erhebliche Risiken für die IT-Infrastruktur der Ruhr-Universität Bochum und für die sowohl auf privaten als auch auf universitätseigenen Systemen verarbeiteten Daten.

Durch geeignete Maßnahmen muss sichergestellt werden, dass das berechtigte Interesse des Anwenders, möglichst wenige Fremdzugriffe auf sein privates Umfeld zu gestatten, mit der Pflicht der Ruhr-Universität Bochum, Integrität, Verfügbarkeit und Vertraulichkeit der dienstlichen Informationen zu gewährleisten, vereinbart werden kann.

Unter einem **externen IT-Arbeitsplatz** wird die Nutzung von IT-Systemen für dienstliche Zwecke außerhalb der Einrichtungen der Ruhr-Universität Bochum verstanden. Dazu gehört auch die vertraglich vereinbarte Erbringung von Arbeitsleistungen außerhalb der Ruhr-Universität Bochum. (☞ z.B. Dienstvereinbarung zur alternierenden Telearbeit an der Ruhr-Universität Bochum)

Unter dem Fachbegriff Bring Your Own Device (**BYOD**) versteht man die Nutzung von privaten Systemen wie z.B. Smartphones und Tablets zur Verarbeitung dienstlicher Daten (z.B. dienstliche E-Mails) unabhängig vom Verwendungsort. Durch das private Eigentum ist die Einflussmöglichkeit der Ruhr-Universität Bochum beschränkt.

7.2 Allgemeine Risikobetrachtung

Die in Kapitel 6 aufgeführte allgemeine Risikobetrachtung für IT-Arbeitsplätze gilt sinngemäß auch für die in diesem Kapitel betrachteten Einsatzszenarien.

Einige der **Bedrohungen** können allerdings gerade in diesem Umfeld extremer in der Ausprägung sein, wie z.B.

- Verlust oder Missbrauch der Daten durch Abhandenkommen des IT-Systems (z.B. Diebstahl) oder durch nicht sachgerechte Administration, insbesondere privater oder mobiler IT-Systeme,
- unzulässiger Zugriff durch Dritte auf dienstliche Datenbestände (z.B. Einsicht durch Familienmitglieder oder Mitreisende),
- leichtfertig Zustimmung, dass Dritte Zugriff auf Datenbestände erhalten (z.B. Dienstleister, APP-Nutzungsbedingungen)
- Lizenz- und Urheberrechtsverletzungen aufgrund mangelnder Abgrenzung der privaten und dienstlichen Sphäre,
- mangelnde Verfügbarkeit dienstlicher Datenbestände für Berechtigte der Ruhr-Universität Bochum.

7.3 Verantwortlichkeit

Die Leitung jeder Einrichtung hat dafür zu sorgen, dass der Schutzbedarf (☞ Klassifikation von Informationen) der zum Einsatz kommenden IT-Anwendungen und IT-Komponenten sowie der dabei verarbeiteten Informationen korrekt festgestellt wird und alle eingesetzten IT-Systeme mit

angemessenen Sicherheitsmaßnahmen ausgestattet sind. Insbesondere im Falle der Nutzung privater IT-Systeme hat der entsprechende Eigentümer dies zu ermöglichen.

7.4 Maßnahmen

Die Möglichkeit der Verarbeitung dienstlicher Daten auf privaten Systemen und/oder am externen Arbeitsplatz richtet sich nach deren Schutzbedarf und den zu erfüllenden rechtlichen Anforderungen (z.B. Datenschutzrecht, Lizenzrecht). Bei einem solchen Einsatzszenario kann eine Verarbeitung auch grundsätzlich ausgeschlossen sein.

Die in Kapitel 6 aufgeführten Maßnahmen zur Grundsicherung von IT-Arbeitsplätzen sowie zur Benutzerverantwortung sind sinngemäß einzuhalten. Ggfs. sind zusätzliche Schutzmaßnahmen (z.B. Verschlüsselungsverfahren nach dem Stand der Technik oder eine zentrale Verarbeitung unter Verwendung virtueller Desktops) zu treffen.

7.4.1 Sicherung des externen Arbeitsplatzes

1. Die Ruhr-Universität Bochum soll für die Arbeit an externen Arbeitsplätzen ein dienstliches IT-System zur Verfügung stellen, um die Umsetzung der erforderlichen Sicherheitsmaßnahmen verlässlich gewährleisten zu können. Die Nutzung eines solchen Systems ist auf autorisierte Personen zu beschränken.
2. Der Zugriff auf dienstliche Informationen und der Zugang zu dienstlichen Ressourcen sind auf berechtigte Personen zu beschränken. Dazu sind entsprechende Schutzmaßnahmen vorzusehen (z.B. Aufbewahrung an einem sicheren Ort, Schutz vor Einsichtnahme Dritter, Nutzung einer sicheren Datenübertragung, Einsatz einer Datenträgerverschlüsselung).

7.4.2 BYOD

1. Der Anschluss dienstlich genutzter privater IT-Systeme an die Netzinfrastruktur der Ruhr-Universität Bochum ist in der Regel nur über speziell ausgewiesene Netzsegmente vorzunehmen. Wird der Zugang über ein anderes Netzsegment gewährt, so ist die entsprechende Einrichtung der Ruhr-Universität Bochum verantwortlich für den Betrieb und die sich daraus ergebenden Gefährdungen.
2. Dienstliche und private Datenbestände sind zu trennen. Werden dienstliche Daten auf dem IT-System nicht mehr benötigt, sind sie in Abwägung des Schutzbedarfs und rechtlicher Anforderungen sicher zu löschen. Dabei ist mindestens der von der Leitung der Einrichtung festgesetzte Schutzbedarf zugrunde zu legen.
3. Bei Verlust oder anderen Schadensereignissen, die das dienstlich genutzten privaten IT-Systems (z.B. Kompromittierung) betreffen, ist die oder der dezentrale Beauftragte für Informationssicherheit unverzüglich zu informieren.
4. Zur dienstlichen Nutzung privater IT-Systeme werden von der Ruhr-Universität Bochum Sicherheitskomponenten für den Schutz des IT-Systems und der Datenübertragung sowie Installations- und Konfigurationshinweise zur Verfügung gestellt. Bei der Auswahl privater IT-Systeme sollte die Kompatibilität zu diesen Komponenten berücksichtigt werden.

8 GRUNDSICHERUNG VON SERVERN UND SYSTEMEN MIT BESONDEREM SCHUTZBEDARF

8.1 Motivation, Begriffe und Erläuterungen

Server sind physische oder logische IT-Systeme (virtuelle Server), die Dienste (Services) für andere IT-Systeme (Klienten) im Netz anbieten und dienen häufig der zentralen Speicherung schutzwürdiger Daten. Serversysteme, insbesondere wenn sie weltweit erreichbar sind, stellen eine besondere Bedrohung für die Sicherheit der Daten und der Netzinfrastruktur dar. Für eine konsistente und sichere Administration von Servern und für deren Betrieb sind detaillierte Fachkenntnisse erforderlich. In gleicher Weise wie Server können z.B. auch Systeme, mit denen sensible oder risikobehaftete Daten verarbeitet werden, einem besonderen Schutzbedarf unterliegen.

8.2 Allgemeine Risikobetrachtung

Serversysteme unterliegen grundsätzlich denselben Bedrohungen wie IT-Arbeitsplätze. Anders als IT-Arbeitsplätze bieten sie Dienste per Fernzugriff übers Intranet oder Internet für viele Benutzerinnen und Benutzer an.

Serversysteme sind einer Reihe von inhärenten **Bedrohungen** ausgesetzt, zum Beispiel:
- Technisches Versagen / Hardwareausfälle
- unberechtigter Datenzugriff durch fehlerhafte Administration (z.B. unzureichende Abgrenzung von Benutzerumgebungen/-rechten),
- Überlastsituationen (z.B. Denial-of-Service-Angriffe, Speicherplatzüberlauf),
- Störungen durch Softwarefehler in den angebotenen Diensten,
- höhere Gewalt (z.B. krankheitsbedingter Ausfall des Administrators, Stromausfall).

Diese Bedrohungen können sich in Verbindung mit folgenden beispielhaft genannten **Schwachstellen** auswirken:
- mangelnde Zeit und Kenntnis der Administratoren,
- fehlende Planung und Dokumentation von Konfiguration und Installation,
- Häufung von Anwendungsdiensten auf einem Server, unzureichendes Ressourcen Monitoring
- ungeeignete Aufstellungsorte und Infrastrukturen (z.B. unzureichende Stromversorgung, Brandschutzmaßnahmen oder Klimatisierung),
- fehlende Betriebsregelungen, Notfallpläne oder Vertreterregelungen.

Mögliche **Auswirkungen** sind:
- Ausfall des gesamten Servers oder eines Anwendungsdienstes,
- die Übernahme des Systems durch Angreifer,
- das Abhören, Ausspähen, Stehlen oder Manipulieren von schutzwürdigen Informationen

Abhängig von der Funktion wirkt sich die Beeinträchtigung eines Serversystems unterschiedlich stark auf den Betrieb aus. Handelt es sich beispielsweise um einen Dateiserver für ein Institut, so sind die Auswirkungen in der Regel lokal begrenzt. Handelt es sich um einen Server, der zentrale Dienste für mehrere IT-gestützte Geschäftsprozesse rund um die Uhr liefert, wie zum Beispiel einen zentralen Authentifizierungsserver, so wirken sich die Beeinträchtigungen auf den Geschäftsbetrieb der Ruhr-Universität Bochum insgesamt aus.

Mögliche **Schäden** für die Ruhr-Universität Bochum sind:
- erhebliche Beeinträchtigungen des Lehr- und Forschungsbetriebs,
- Haftung der Ruhr-Universität Bochum für Schäden Dritter,
- strafrechtliche Folgen bei Verletzungen des geltenden Rechts,
- Imageverlust in der Öffentlichkeit,
- Vertrauensverlust in den sachgerechten Umgang mit Informationen.

8.3 Verantwortlichkeiten

Die Leitung jeder Einrichtung der Ruhr-Universität Bochum ist für die von ihr betriebenen Server zuständig. Sie hat durch geeignete Maßnahmen dafür zu sorgen, dass Server insbesondere unter dem Aspekt der Sicherheit fachkundig geplant, verwaltet und betrieben werden. Sie hat ggfs. entsprechende Betriebsregelungen aufzustellen.

8.4 Maßnahmen

Die in Kapitel 6 genannten Maßnahmen zur Grundsicherung von IT-Arbeitsplätzen sowie zur Benutzerverantwortung sind sinngemäß anzuwenden. Darüber hinaus sind die folgenden Punkte zu berücksichtigen.

8.4.1 Planung und Management

1. Für den Einsatz von Servern und Systemen mit besonderem Schutzbedarf ist insbesondere unter dem Aspekt der Informationssicherheit eine angemessene Planung durchzuführen und zu dokumentieren (Umsetzung-, Betriebs- und Informationssicherheitskonzept). Die Planung soll einmal jährlich auf Aktualität überprüft werden, mindestens aber bei Veränderung der Konfiguration oder Austausch des Servers. (☞ Handlungsempfehlung zur Serveradministration)
2. Server, die von außerhalb der Netzinfrastruktur der Ruhr-Universität Bochum erreichbar sind, müssen über ein geregeltes Freigabeverfahren für diese Nutzung freigeschaltet werden. (☞ Netzsicherheitskonzept der RUB)
3. Bei der Bereitstellung von Diensten mittels eigener Server dezentraler Einrichtungen ist zu prüfen, ob die Aufgaben nicht bereits ausreichend durch zentrale Angebote erbracht werden.
4. Eine dauerhafte und fachkundige Administration des Servers ist sicherzustellen und Verantwortliche für die auf dem Server betriebenen Dienste sind zu benennen. Angemessene Stellvertreterregelungen sind zu treffen.
5. Für Server ist vorzusehen, dass sie räumlich angemessen untergebracht sind, etwa in speziellen Serverräumen oder abschließbaren Serverschränken.

8.4.2 Administration

Alle Serversysteme an der Ruhr-Universität Bochum müssen, insbesondere unter dem Aspekt der Informationssicherheit, fachkundig administriert werden. Den Einrichtungen wird empfohlen, die Administration einem geschulten Administrator zu übertragen. Ist dies nicht mit vertretbarem Aufwand möglich, so sollten die zentralen Dienste und/oder Angebote zur Administration genutzt werden. (☞ Zentrale IT-Dienste)

Zu einer sicheren Administration von Servern gehören neben der Beachtung allgemeiner Sicherheitsanforderungen für IT-Systeme insbesondere die angemessene Protokollierung und Überwachung des Betriebs. Dabei ist die Protokollierung (Logging) auf den Umfang zu beschränken, der für den sicheren Betrieb des Servers erforderlich ist. Wenn Protokolldaten personenbezogene Daten beinhalten, ist sicherzustellen, dass die Aspekte des Datenschutzes berücksichtigt und dokumentiert werden. Detaillierte Hinweise sind der ☞ Handlungsempfehlung zur Serveradministration zu entnehmen.

8.4.3 Sicherung von Serverräumen

Serverräume sind speziell ausgestattete Räume, deren Infrastruktur dem sicheren Betrieb von Servern dient. (☞ Einrichtung und Betrieb von Serverräumen)C:\daten\management\ordnungen\Rahmenkonzept-endgültig\Klassifikation.docx

1. Serverräume müssen mit der für den Dauerbetrieb von IT-Systemen erforderlichen technischen Infrastruktur und organisatorischen Vorkehrungen ausgestattet sein. Sie müssen angemessen auch vor Umwelteinflüssen (z.B. Wassereinbruch jeglicher Art, Feuer) und Versorgungsstörungen (z.B. der Klimatisierung oder der Stromversorgung) geschützt sein.
2. Serverräume müssen einen angemessenen Schutz gegen unautorisierten Zutritt bieten (z.B. bauliche Konstruktion, sicheres Zutrittsverfahren).
3. Die für den sicheren Betrieb der Serverräume notwendigen technischen und organisatorischen Vorkehrungen sind zu dokumentieren und zu überwachen (u.a. durch Monitoring).

Den Einrichtungen stehen zentrale Serverräume für die Unterbringung der von ihnen betriebenen Server zur Verfügung.

Für alle anderen Räume, in denen Server untergebracht sind, ist der Schutzbedarf (☞ Klassifikation von Informationen) in Abhängigkeit von den potentiellen Risiken festzustellen. Die sich daraus ergebenden Maßnahmen sind für den Einzelfall festzulegen und haben sich ebenfalls an den vorgenannten Punkten zu orientieren.

9 SCHUTZ VOR SCHADSOFTWARE UND ANGRIFFEN

9.1 Motivation, Begriffe und Erläuterungen

Die IT-Infrastruktur der Ruhr-Universität Bochum muss angemessen vor Angriffen geschützt werden. Unter Angriff wird jegliche Handlung verstanden, die die Funktionsfähigkeit der Netzinfrastruktur oder IT-Systeme stört oder sich unerlaubt Zugang zu IT-Systemen oder Zugriff auf Informationen beschafft. Ebenso ist sie vor Schadsoftware zu schützen, die etwa durch E-Mail-Anhänge, aktive Browserinhalte oder mobile Datenträger in ein System eingeschleust werden kann.

Neben dem berechtigten Eigeninteresse bestehen auch rechtliche Verpflichtungen, angemessene Vorkehrungen zum Schutz vor Schadsoftware und Angriffen zu treffen, die dem Stand der Technik entsprechen. Technische Schutzmaßnahmen sind durch geeignete organisatorische und personelle Maßnahmen wie Benutzersensibilisierung, definierte Meldewege und Helpdesk-Unterstützung zu ergänzen.

9.2 Allgemeine Risikobetrachtung

Schädliche Inhalte können über zahlreiche Wege in die universitäre IT-Infrastruktur gelangen, z.B. über Webseiten, E-Mails oder mobile Datenträger. Schädliche Inhalte können vielfältiger Natur sein und sich z.B. auch in PDF- und Office-Dateien befinden. Den **Bedrohungen** kann im universitären Umfeld nicht umfassend durch zentrale Maßnahmen begegnet werden, da in diesem heterogenen IT-Umfeld vielfältige technische und prozessbedingte **Schwachstellen** existieren.

Mögliche **Auswirkungen** sind
- unkontrollierte Verbreitung von Schadcode ins Intranet und Internet,
- ungewollte Unterstützung von Straftaten (z.B. bei Beteiligung an Botnetzen),
- Ausspähung, Veränderung oder Verlust von Daten oder
- Verstoß gegen gesetzliche Vorgaben.

Als **Schäden** können für die Ruhr-Universität Bochum entstehen:
- Verlust von Arbeits- und Forschungsergebnissen,
- Kosten und Strafen durch Verletzung geltenden Rechts (z.B. Urheberrecht, Datenschutzrecht),
- Vertrauensverlust in den sachgerechten Umgang mit Informationen sowohl im Innen- wie im Außenverhältnis,
- finanzielle Aufwendungen für die Behebung von Schäden.

9.3 Verantwortlichkeiten

Netzbetreiber und Anbieter von IT-Diensten haben angemessene Schutzmaßnahmen für die von ihnen betriebenen Netze sowie Dienste zu definieren und für die Umsetzung zu sorgen. Systemverantwortliche haben für den Schutz ihrer Systeme Sorge zu tragen. Anwenderinnen und Anwender sind verpflichtet, die für ihren Arbeitsbereich geltenden Regeln zur Informationssicherheit anzuwenden.

Zentrale Angebote zur Unterstützung werden bereitgestellt. Die Beauftragten für Informationssicherheit übernehmen in ihrem Zuständigkeitsbereich die Koordination der Maßnahmen.

9.4 Maßnahmen

Technische Maßnahmen zur Erkennung von Schadcode und Verhinderung der Ausbreitung müssen mehrschichtig auf Netzwerk-, Server und Klientenebene implementiert werden. Diese sind durch organisatorische und personelle sowie Notfallmaßnahmen zu flankieren. Spezifische

Maßnahmen auf Server- und Klientenebene sind auch in den jeweiligen Kapiteln 6 und 8 genannt.

9.4.1 E-Mailserver-Datenverkehr

1. Der gesamte E-Mailserver-Datenverkehr der Ruhr-Universität Bochum wird grundsätzlich über zentrale Relais im Verantwortungsbereich des zentralen IT-Dienstleisters der Ruhr-Universität Bochum abgewickelt. Auf diesen Relais werden sämtliche eingehenden und ausgehenden E-Mails automatisiert überprüft.
2. Die Annahme von E-Mails mit schädlichen Inhalten wird verweigert und so der Absender benachrichtigt. Zur Abwehr von Angriffen kann auch die Annahme von eingehenden E-Mails mit bestimmten Eigenschaften (z.B. bestimmte Netzadresse des Versenders (Blacklisting), bestimmter Betreff, zentrale E-Mail-Adressen der Ruhr-Universität Bochum als Absender) verweigert werden.
3. Angenommene E-Mails werden auf den Relais daraufhin geprüft, ob sie Kennzeichen unverlangter Massen-E-Mails besitzen, werden im Header entsprechend gekennzeichnet und zugestellt. Als verdächtig markierte E-Mails werden weder weitergeleitet, noch dürfen darauf Fehlermeldungen oder automatische Antworten zurückgesandt werden.
4. Die Kommunikation zwischen E-Mailklienten, internen E-Mailservern der Ruhr-Universität Bochum und den zentralen E-Mailservern erfolgt grundsätzlich über verschlüsselte Verbindungen. Der E-Mailversand erfolgt erst nach gesicherter Authentifizierung des Senders, dezentrale E-Mailserver sind entsprechend zu konfigurieren.

9.4.2 Webserver-Datenverkehr

Es werden zentrale Web-Proxy-Dienste angeboten, die als Vermittler zwischen externen Webservern und Klienten aus dem Intranet der Ruhr-Universität Bochum fungieren. Durch diese werden Webinhalte automatisiert auf Schadcode geprüft und schädliche Inhalte ausgefiltert. Die Nutzung der zentralen Proxy-Dienste wird dringend empfohlen.

9.4.3 Domain Name Service

Es wird ein zentraler, redundant ausgelegter Domain Name Service (DNS) angeboten, der die Überprüfung von Authentizität und Datenintegrität unterstützt. Dazu gehören DNS-Resolver und (autoritative) DNS-Server, die den Nameservice für Einrichtungen übernehmen. Die Nutzung dieser zentralen Dienste wird dringend empfohlen.

9.4.4 Frühwarn- und Abwehrsysteme

1. Zum Schutz der Netzsegmente vor unerlaubten Zugriffen wird eine zentrale Sicherheitsinfrastruktur z.B. auf Basis von Firewalls betrieben.
2. Der Zugang zur Netzinfrastruktur der Ruhr-Universität Bochum wird ggfs. erst nach Prüfung des Sicherheitszustands (z.B. Aktualität der Virensignaturen, Updatestand des Betriebssystems) eines Systems gewährt.
3. Zum Schutz der IT-Infrastruktur können Sensoren und Scanner eingesetzt werden, die die Erkennung von Netzwerkanomalien und Schwachstellen unterstützen und ggfs. Alarmmeldungen erzeugen.

Diese Maßnahmen werden mit den betroffenen Einrichtungen, den Personalräten, der oder dem behördlichen Datenschutzbeauftragten sowie den Beauftragten für Informationssicherheit abgestimmt. Die Regelungen für die Umsetzung der Maßnahmen sind im ☞ Netzsicherheitskonzept der Ruhr-Universität Bochum formuliert.

10 SCHUTZ DER DATEN BEI TRANSPORT UND ABLAGE

10.1 Motivation, Begriffe und Erläuterungen

Ein angemessener Schutz von Informationen muss auch außerhalb der gesicherten IT-Systeme bei jedweder Art der Übertragung oder Speicherung gewährleistet sein. Die externe Speicherung kann digital erfolgen (z.B. auf USB-Sticks oder in Clouds) oder durch Überführung auf ein analoges Medium (z.B. Ausdruck, Mikrofilme). Beispiele für die Übertragung sind E-Mail, Telefon, Fax, physischer Transport oder Versand von Medien. Die Art der Übertragung und Speicherung von Daten muss auch dabei dem jeweiligen Schutzbedarf entsprechen. (☞ Klassifikation von Informationen)

10.2 Allgemeine Risikobetrachtung

Für Daten außerhalb geschützter IT-Systeme sind insbesondere die **Bedrohungen** Diebstahl oder unzulässige Nutzung zu betrachten.

Durch **Schwachstellen** werden die Bedrohungen begünstigt, hierzu gehören:
- unzureichende Sensibilisierung des Personals,
- ungeeignete Auswahl von Übertragungswegen und Übertragungsmethoden (z.B. Austausch sensitiver Informationen per unverschlüsselter Verfahren),
- ungeeignete Auswahl von Datenträgern (z.B. Beschädigung, Verschleiß, mangelnde Haltbarkeit),
- unzureichend kontrollierter Zutritt zu Ausgabegeräten und Datenträgern (z.B. Archivräume, Fax-Geräte und Drucker).

Mögliche **Auswirkungen** sind der unberechtigte Zugang zu Informationen, die Manipulation oder der Verlust von Informationen.

Als **Schäden** können für die Ruhr-Universität Bochum entstehen:
- finanzielle Aufwendungen für die Behebung von Datenverlusten,
- Kosten oder Strafen aufgrund der Verletzung geltenden Rechts oder vertraglicher Vorgaben (z.B. Urheberrecht, Datenschutzrecht, Archivierungsfristen, Aufbewahrungspflichten),
- Vertrauensverlust in den sachgerechten Umgang mit Informationen sowohl im Innen- wie im Außenverhältnis.

10.3 Verantwortlichkeiten

Die Leitung jeder Einrichtung ist für die in ihrem Bereich verarbeiteten Daten und Informationen zuständig. Sie hat dafür zu sorgen, dass die Schutzbedarfe der Daten und Informationen (☞ Klassifikation von Informationen) korrekt festgestellt und angemessene Sicherheitsmaßnahmen implementiert werden. Dies bezieht sich insbesondere auch auf den Export und die Weitergabe von Daten.

10.4 Maßnahmen

1. Für den Transport von Daten ist abhängig vom Schutzbedarf festzulegen, welche Personen auf welche Art und Weise den Austausch vornehmen. Weitere Erläuterungen dazu finden sich in der ☞ Handlungsempfehlung für den Datenaustausch.
2. Die Rechtmäßigkeit des Transports und der Ablage muss gegeben sein, dabei sind insbesondere Aufbewahrungs- und Löschfristen sowie die rechtlichen Anforderungen bei der Benutzung von Systemen Dritter (z.B. Cloud-Dienste) zu berücksichtigen. Eine Dokumentation des Transports und der Ablage kann für den Nachweis der Rechtmäßigkeit sinnvoll, teilweise sogar erforderlich sein.

3. Auch beim Transport auf oder von (netzfähigen) Peripheriegeräten (z.B. Drucker, Scanner, Kopierer, Multifunktionsgeräte) sowie bei der Übertragung per Telefon oder Fax ist der Schutz der Informationen zu gewährleisten
4. Die Mitarbeiterinnen und Mitarbeiter sind über die Regelungen zu informieren und ausreichend und regelmäßig zu schulen.

11 DATENSCHUTZ UND IT-COMPLIANCE

11.1 Motivation, Begriffe und Erläuterungen

Der Begriff Compliance stammt aus der angelsächsischen Rechtsterminologie. Eine Organisation handelt compliant (regelkonform), wenn sie die für sie relevanten Regeln befolgt. Diese Regeln ergeben sich nicht allein aufgrund von Rechtsnormen, also gesetzlichen Regelungen und Verordnungen, sondern auch aus der Rechtsprechung, aus Verwaltungsvorschriften, anerkannten Standards, organisationsinternen Richtlinien und vertraglichen Verpflichtungen. Nur wenn IT-Verfahren regelkonform implementiert und kontrolliert werden, können auch die darauf aufbauenden Geschäftsprozesse regelkonform ablaufen.

Ein besonders relevanter Bereich dieser Regeln ist der Datenschutz. Dieser hat das Ziel, Bürger vor Beeinträchtigungen von Persönlichkeitsrechten, die durch Datenverarbeitung entstehen können, zu schützen. Zusätzlich machen es die Diversität und die Dynamik des IT-Einsatzes sowie die Vielzahl von unterschiedlichen Vorschriften notwendig, Prozesse für das Management der IT-Compliance und speziell für den Datenschutz zu definieren.

11.2 Allgemeine Risikobetrachtung

Die Nichteinhaltung von Regeln muss als eigenständige **Bedrohung** bewertet werden. Zentrale **Schwachstellen** liegen im Bereich der Organisation (z.B. unzureichende Information oder Überlastung der Beteiligten, fehlende Ressourcen).

Mögliche **Auswirkungen** sind z. B. Verstöße gegen gesetzliche Regelungen (z.B. das Datenschutzrecht, das Urheberrecht oder das Telekommunikationsrecht), gegen Vorschriften zur Aufbewahrung und Beweiskraft von Aufzeichnungen, gegen anerkannte Standards und nicht zuletzt gegen dieses Rahmenkonzept und an der Ruhr-Universität Bochum gültige Ordnungen und Dienstvereinbarungen. Diese können nicht nur die Gesamtstruktur der Ruhr-Universität Bochum, sondern insbesondere im Rahmen von Datenschutzverstößen auch die Persönlichkeitsrechte von Einzelnen beeinträchtigen.

Schäden können beispielsweise Geldstrafen, Schadensersatzpflichten, Geldbußen oder Zwangsgelder sein, die sich aus Verstößen gegen Rechtsnormen ergeben. Bei zunehmender Abhängigkeit der Ruhr-Universität Bochum von der Informations- und Datenverarbeitung steigt bei Defiziten der IT-Compliance auch die potentielle Höhe der Schäden. Darüber hinaus sind auch strafrechtliche Konsequenzen bei Verletzung geltenden Rechts möglich.

11.3 Verantwortlichkeiten

Die Gesamtverantwortung für die ordnungsgemäße Organisation der Geschäftsprozesse an der Ruhr-Universität Bochum liegt bei der Hochschulleitung; dies schließt die Verantwortung für die Compliance, speziell die IT-Compliance und den Datenschutz ein. Die Leitung jeder Einrichtung der Ruhr-Universität Bochum hat die Verpflichtung, die in ihrem Bereich betriebenen IT-gestützten Geschäftsprozesse entsprechend zu organisieren.

Die Einhaltung von rechtlichen Bestimmungen und insbesondere des Datenschutzes obliegen jeder Mitarbeiterin und jedem Mitarbeiter der Ruhr-Universität Bochum. Die dafür notwendigen organisatorischen Voraussetzungen müssen durch die Leitung der jeweiligen Organisationseinheit geschaffen werden. Für Tätigkeiten von Personen, die Aufgaben für die Ruhr-Universität Bochum übernehmen und nicht dort beschäftigt sind, ist unbeschadet der Gesamtverantwortung der Hochschulleitung die jeweils beauftragende Einrichtung verantwortlich (siehe auch „Kapitel 12: Leistungserbringung durch und für Dritte“).

Die oder der Datenschutzbeauftragte ist für die Überprüfung der Einhaltung der datenschutzrechtlichen Bestimmungen zuständig, sie bzw. er berät alle Mitglieder und Angehörigen der

Ruhr-Universität Bochum und ist Ansprechpartner für alle, deren Daten verarbeitet werden (Betroffene). Die Dienststelle stellt entsprechende Ressourcen bereit. Die oder der Datenschutzbeauftragte kann durch dezentrale Datenschutzkoordinatoren unterstützt werden. Diese können vom Leiter der verantwortlichen Stelle benannt werden und sind für diese Aufgabe angemessen zu schulen.

11.4 Maßnahmen zum Datenschutz

In einer Hochschule sind vielfältigste Daten zu finden, die unterschiedlichen Schutzstufen zugeordnet werden können. Insbesondere im Forschungsbereich finden sich Daten mit höchstem Schutzbedarf, zum Beispiel Gesundheitsdaten, im Verwaltungsbereich finden sich Daten mittleren Schutzbedarfs, zum Beispiel Personaldaten. (☞ Klassifikation von Informationen)

Auf dieser Grundlage sind folgende Maßnahmen zu treffen, um ein angemessenes Datenschutzniveau zu erreichen:

1. In allen Fällen der Verarbeitung von personenbezogenen Daten, ungeachtet ihrer Sensibilität, ihres Umfangs, ihrer Menge oder des Grades der Automatisierung, sind die rechtlichen Rahmenbedingungen zum Datenschutz einzuhalten. Die oder der behördliche Datenschutzbeauftragte berät zur Einhaltung der rechtlichen Verpflichtungen. Dezentrale Datenschutzkoordinatoren können die oder den behördliche(n) Datenschutzbeauftragte(n) und die Einrichtung unterstützen.
2. Alle Mitarbeiterinnen und Mitarbeiter werden schriftlich und persönlich auf das Datengeheimnis aus dem Datenschutzgesetz NRW (DSG NRW) verpflichtet. Mitarbeiterinnen, Mitarbeiter und auch sonstige Personen, die personenbezogene Daten für die Ruhr-Universität Bochum verarbeiten, müssen zusätzlich in technischen, organisatorischen und rechtlichen Aspekten unterwiesen werden. Die Leitung jeder Einrichtung ist dafür verantwortlich, dies sicherzustellen. Die Ruhr-Universität Bochum bietet entsprechende Schulungsangebote an.
3. Personenbezogene Daten dürfen grundsätzlich nur für die Zwecke verarbeitet werden, für die sie ursprünglich erhoben wurden, Abweichungen bedürfen einer rechtlichen Grundlage. Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind voneinander getrennt zu verarbeiten und dürfen nicht zusammengeführt werden. Daten sind zu löschen, wenn der Zweck, für den sie ursprünglich erhoben wurden, nicht mehr besteht (Löschungsgrundregel) und dem Löschen keine sonstigen Regelungen entgegenstehen (☞ Aufbewahrungsfristen). Eine Löschung ist nachvollziehbar zu dokumentieren.
4. Das Übermitteln von personenbezogenen Daten innerhalb und außerhalb der Ruhr-Universität Bochum ist nur in rechtlich bestimmten Ausnahmefällen erlaubt. Die Bedingungen dazu sind in der Regel vorab durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu prüfen.
5. Bei besonderen Gefährdungen durch Verarbeitung personenbezogener Daten ist eine Stellungnahme der bzw. des Datenschutzbeauftragten einzuholen. Alle längerfristigen automatisierten Verfahren, bei denen personenbezogene Daten verarbeitet werden, sind zu dokumentieren (Verfahrensverzeichnis gemäß DSG NRW) und müssen durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten vor Inbetriebnahme und bei wesentlichen Änderungen überprüft werden (Vorabkontrolle).
6. Insbesondere wenn personenbezogene Daten von Mitarbeiterinnen und Mitarbeiter verarbeitet werden, unterliegt dies der Mitbestimmung durch die Personalvertretung. Gemäß Rahmendienstvereinbarung ist der IT-Ausschuss der Ruhr-Universität Bochum zu konsultieren. Im Rahmen der Mitbestimmung werden zusätzliche datenschutzrechtliche Aspekte in Dienstvereinbarungen geregelt.

Weitere Details regelt die ☞ Handlungsempfehlung zum Datenschutz.

11.5 Allgemeine Maßnahmen zur IT-Compliance

Das Rektorat stellt sicher, dass Mitglieder und Angehörige der Ruhr-Universität Bochum insbesondere in Bezug auf IT-Compliance in geeigneter Weise informiert, geschult und beraten werden, damit sie Gesetze und Regeln einhalten und damit compliant handeln können. (☞ Gesetze und Regeln)

Die Ruhr-Universität Bochum stellt gesonderte Handlungsanweisungen und -empfehlungen (z.B. Kryptokonzept, Archivierungskonzept) zur Einhaltung von IT-Standard-Compliance-Anforderungen zur Verfügung. (☞ IT-Compliance-Konzepte)

12 LEISTUNGSERBRINGUNG DURCH UND FÜR DRITTE

12.1 Motivation, Begriffe und Erläuterungen

Die Ruhr-Universität Bochum beauftragt in vielen Fällen externe Unternehmen mit IT-Dienstleistungen oder der Verarbeitung von Informationen. Andererseits ist die Ruhr-Universität Bochum in verschiedenen Kooperationszusammenhängen Leistungserbringer. In beiden Fällen kann die Verantwortung für Informationsverarbeitung nicht an den Auftragnehmer abgegeben werden. Das Sicherheitsniveau und die Anforderungen an den Datenschutz sind in Verträgen und spezifischen IT-orientierten Vereinbarungen, z.B. Service Level Agreements (SLA), festzulegen und können auf dieser Basis überprüft werden.

Typische Aufträge umfassen die Bereitstellung, Betrieb und Wartung von Anwendungen, Betriebssystemen, Infrastrukturkomponenten (z.B. Speicherplatz und Backup), die Entsorgung von Datenträgern sowie die Verarbeitung von Daten durch Dritte. Auch Beauftragungen ohne expliziten IT-Bezug, z.B. Reinigungsdienstleister, bei denen ein Zugriff auf oder eine Beeinflussung von Informationsinfrastrukturen nicht ausgeschlossen werden kann, können hierzu gehören.

12.2 Allgemeine Risikobetrachtung

Die besondere **Bedrohung** ergibt sich daraus, dass die Ruhr-Universität für Defizite, die außerhalb des Einflussbereichs des jeweiligen Verantwortlichen liegen, in Verantwortung genommen wird. Dies können z.B. mangelnde Sicherheitsvorkehrungen oder Serviceausfälle bei der Ruhr-Universität als Dienstleister oder einem ihrer Vertragspartner sein.

Schwachstellen wie fehlende oder unzureichend formulierte Verträge, die dann z.B. die Verantwortlichkeiten nicht eindeutig regeln, verstärken diese Bedrohungen zusätzlich.

Mögliche **Auswirkungen** sind Betriebsausfälle z.B. infolge schlecht gewarteter Software oder ein erhöhter Ressourcenbedarf zur Behebung nachträglich festgestellter Defizite.

Für die Ruhr-Universität können sich daraus diverse **Schäden** ergeben, die von einem Imageverlust bis hin zu konkreten finanziellen Mehrbelastungen (z.B. erhöhter Ressourcenbedarf und Schadensersatzforderungen oder Strafen als Folge von Gesetzesverstößen) reichen.

12.3 Verantwortlichkeit

Auftraggeber sind dafür verantwortlich, Vereinbarungen zu treffen, in denen die Risiken für die Informationssicherheit angemessen berücksichtigt und dokumentiert werden. Auftragnehmer haben eine Mitwirkungspflicht bei der Ausgestaltung der Vereinbarung. Beide Vertragspartner haben sicherzustellen, dass Rechte von Dritten (z.B. Vertraulichkeit der Daten von Dritten) durch die Vereinbarung nicht beeinträchtigt werden.

12.4 Maßnahmen

1. Generell sind potentielle Auftragnehmer bereits im Vorfeld einer Beauftragung hinsichtlich ihrer fachlichen Eignung auszuwählen. Im Prozess der Beauftragung (von der Formulierung von Ausschreibungsunterlagen bis hin zur vertraglichen Ausgestaltung) sind möglichst frühzeitig die Anforderungen der Informationssicherheit und des Datenschutzes zu beachten.
2. Falls die beauftragte Leistung sich auf Daten mit einem besonderen Schutzbedarf bezieht – beispielsweise bei der Verarbeitung personenbezogener Daten oder schützenswerter Forschungsdaten – sind Vereinbarungen zur Auftragsdatenverarbeitung zu treffen, die die datenschutzrechtlichen Anforderungen (z.B. §11 DSG NRW oder §11 BDSG) berücksichtigen. Gesonderte „Security SLA“ (SSLA) sind empfehlenswert.

3. Für besondere Fälle der Leistungserbringung von und für Dritte sind spezifische vertragliche Regelungen rechtlich vorgegeben. Hierzu bietet die Ruhr-Universität Bochum Vertragsvorlagen an, die auf die konkrete Dienstleistung anzupassen sind und deren Verwendung empfohlen wird.
4. Bei der Ausgestaltung von Verträgen sind die informationssicherheitsbezogenen Mitwirkungsrechte der Personalvertretungen, Dienstvereinbarungen und Ordnungen der Ruhr-Universität Bochum zu berücksichtigen. Gegebenenfalls sind entsprechende Regelungen in die Vertragstexte aufzunehmen.
5. Die Inhalte der vertraglichen Regelungen sind regelmäßig, mindestens aber bei Änderung der vertraglich vereinbarten Sachverhalte, zu überprüfen und ggfs. anzupassen.

Weitere Details regelt die ☞ Handlungsempfehlung zur Gestaltung von Verträgen.

13 IT-NOTFALLMANAGEMENT

13.1 Motivation, Begriffe und Erläuterungen

Ein Notfall ist ein Schadensereignis, bei dem die Vertraulichkeit, Verfügbarkeit oder Integrität wesentlicher Geschäftsprozesse oder Ressourcen einer Organisation nicht oder nur eingeschränkt gewährleistet sind. Im Gegensatz zu einer Störung können Notfälle nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine eigene Organisation zur Bewältigung.

Da die überwiegende Anzahl der Geschäftsprozesse der Ruhr-Universität Bochum durch Informationstechnologie gestützt wird, ist das IT-Notfallmanagement ein elementarer Bestandteil des übergreifenden Notfallmanagements. Notwendig ist die Identifizierung von kritischen Geschäftsprozessen und Ressourcen sowie deren Bedrohungen (Business Impact Analyse (BIA) bzw. Risikoanalyse). Unter Berücksichtigung der dabei ermittelten Prioritäten sind angemessene präventive Maßnahmen (Notfallvorsorgemaßnahmen) zu definieren und Pläne zur Bewältigung von Notfällen zu erarbeiten. Notfallmanagement ist ein kontinuierlicher Prozess der Planung, Erprobung, Umsetzung und Überprüfung.

13.2 Allgemeine Risikobetrachtung

Bedrohungen, die zu Notfällen führen können, leiten sich häufig aus akzeptierten Restrisiken ab – *das Unwahrscheinliche ist auch wahrscheinlich*. Ursachen sind z.B. höhere Gewalt (u.a. Feuer, Wassereinbruch, technische Katastrophen im Umfeld oder Umwelteinwirkungen), technisches bzw. organisatorisches Versagen oder vorsätzliche Handlungen (Vandalismus, Schadprogramme oder sonstige Angriffe auf IT-Systeme). Dabei können sich unzureichende Sicherheitsmaßnahmen oder die unzureichende Wahrnehmung von geänderten Bedrohungslagen als **Schwachstellen** erweisen.

Mögliche **Auswirkungen** erstrecken sich vom Ausfall des Forschungs-, Lehr-, und Verwaltungsbetriebs der Universität bis hin zur Gefahr für Leib und Leben. Notfallmanagement zielt darauf ab, die Auswirkungen und **Schäden** solcher Ereignisse möglichst gering zu halten und geordnet zum Regelbetrieb zurückzukehren.

13.3 Verantwortlichkeiten

IT-Notfallvorsorge ist Aufgabe aller Organisationseinheiten der Ruhr-Universität Bochum und ggfs. auch Dritter, die Leistungen für die Ruhr-Universität Bochum erbringen. Das Rektorat der Ruhr-Universität Bochum trägt die Gesamtverantwortung für das Notfallmanagement.

13.4 Maßnahmen

1. Für die Ruhr-Universität Bochum wird eine angemessene Notfallstrategie für kritische Prozesse und Ressourcen erarbeitet und regelmäßig überprüft, in der auch festgelegt wird, welche Einrichtungen IT-Notfallkoordinierende zu benennen haben. Die/der zentrale Beauftragte für Informationssicherheit sowie die/der behördliche Datenschutzbeauftragte sind einzubinden. Das Rektorat der Ruhr-Universität Bochum sorgt für die organisatorischen Voraussetzungen.
2. Auf der Basis der allgemeinen Notfallstrategie hat die Leitung jeder Einrichtung der Ruhr-Universität Bochum dafür zu sorgen, dass angemessene Notfallmaßnahmen für die von ihr betriebenen Geschäftsprozesse und -ressourcen definiert, umgesetzt und aufrechterhalten werden (IT-Notfallkonzept). Dabei sind die dezentralen IT-Sicherheitsbeauftragten einzubinden.

3. Durch regelmäßige Proben und Tests (z.B. Inbetriebnahme von Notfallsystemen, Rekonstruktion von Daten) ist die Wirksamkeit der getroffenen Maßnahmen zu überprüfen (Notfallübungen). Ergebnisse sind zu dokumentieren.

14 GLOSSAR

Angehörige der Ruhr-Universität
Angehörige der Ruhr-Universität sind gemäß Art. 4 der Verfassung, sofern sie nicht Mitglieder nach Art. 3 sind, die nebenberuflichen Professorinnen und Professoren, die entpflichteten oder in den Ruhestand versetzten Professorinnen und Professoren, die außerplanmäßigen Professorinnen und Professoren, die Honorarprofessorinnen und Honorarprofessoren, die nebenberuflich, vorübergehend oder gastweise an der Hochschule Tätigen, die Privatdozentinnen und Privatdozenten, die wissenschaftlichen Hilfskräfte, sofern sie nicht Mitglieder sind, die Ehrenbürgerinnen und Ehrenbürger, Ehrensenatorinnen und Ehrensenatoren sowie die Zweithörerinnen und Zweithörer, Gasthörerinnen und Gasthörer, Lehrbeauftragte, die in den Ruhestand versetzten, zuletzt hauptberuflich an der Ruhr-Universität Beschäftigten sowie die Absolventinnen und Absolventen der Ruhr-Universität auf Antrag. Die Ruhr-Universität kann hauptamtlich Beschäftigten in Einrichtungen an der Ruhr-Universität oder anderen mit der Universität verbundenen Einrichtungen den Status von Angehörigen zuerkennen.

Authentisierung
Authentisierung bezeichnet den Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

Authentizität
Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Authentifizierungsmerkmal
Ist ein Merkmal, mit dem ein Benutzer von einem geschützten System authentifiziert werden kann. Dieses Merkmal kann auf Wissen (Passwort, PIN), auf Besitz (Schlüssel, Karte) oder auf einer Eigenschaft (biometrisches Merkmal z. B. Stimme, Irisbild, Fingerabdruck) oder Original-Unterschrift basieren oder auf einer Kombination dieser Merkmale.

Betriebsmittel
Jegliche Art von Hilfsmitteln zur Ausführung der Arbeit. Angefangen von IT-Systemen, Software und Lizenzen, bis hin zu einfachen Kugelschreibern und Radiergummis fallen unter diese Kategorie.

Blacklisting (E-Mail)
Eine Negativliste wird erstellt, um E-Mailadressen von einem Dienst auszuschließen, zum Beispiel Spamadressen.

Bot/Botnetz
Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (einem sogenannten Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-und-Control-Servers (C&C-Server) kontrolliert und gesteuert.

Daten
Darstellungen von Informationen in kodierter Form (Verwendung bestimmter Zeichen und Symbole) die auf digitalen oder analogen Datenträgern existieren. Aus ihnen können durch Interpretation Informationen werden.

Denial-of-Service(DoS)
Wird ein System mit Anfragen überlastet, so kann es darauf folgend keine Anfragen mehr bearbeiten und stellt seinen Dienst vorübergehend ein.

Dokumentenlenkung
Ein Dokument gilt als gelenkt (ISO 9000/9001), wenn sein Werdegang (Erstellung, Bearbeitungsstand, Überprüfung, Freigabe, Verteilung, Einzug) jederzeit nachvollziehbar ist. Dies erfordert eine angemessene Kennzeichnung der Dokumente.

Drive-by-Download/Drive-by-Exploits
So genannte Drive-by-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (Plug-Ins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Geschäftsprozess
Menge logisch verknüpfter Einzeltätigkeiten, die ausgeführt werden um ein geschäftliches oder betriebliches Ziel zu erreichen.

Informationen
Die zweckbestimmte Interpretation von Daten durch kognitive Tätigkeit des Menschen.

Informationssicherheit
Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" ist daher umfassender als der Begriff IT-Sicherheit.

Informationssicherheitsmanagement(system) (ISMS)
Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement(system) bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Intranet
Ein Rechnernetz, das nicht öffentlich zugänglich ist, sondern nur von einer bestimmten Personenmenge benutzt wird.

IT-Arbeitsplatz,
Unter einem IT-Arbeitsplatz wird ein IT-System verstanden, an dem Personen arbeiten können. Dieses System ist typischerweise vernetzt und fungiert als Klient im Netzwerk, d.h. es kann Dienste eines Servers (z.B. eines Webservers) über das Netzwerk anfordern, stellt aber selbst Dienste allenfalls im lokalen Netzwerk zur Verfügung.

IT-Dienst
Unter IT-Diensten werden die verschiedenen Anwendungsmöglichkeiten verstanden, die IT-Systeme zur Nutzung bereitstellen (z.B. E-Mail, Web etc.)

IT-Grundschutz
IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Informationssicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen, Institutionen mit normalem Schutzbedarf hinreichend absichern.

IT-Infrastruktur
Gesamtheit aller zum Betrieb von (Anwendungs-) Software notwendigen technischen und logischen Komponenten wie z.B. Computer-, Storage-Systeme, Netzwerkinfrastruktur, Peripheriegeräte und Software.

IT-Sicherheit
IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

IT-System
IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

IT-Verfahren
Ein IT-Verfahren unterstützt Geschäftsprozesse oder Teile davon und bildet eine arbeitsorganisatorisch abgeschlossene Einheit. Es kann ein Fachverfahren, ein Querschnittsverfahren oder Basisverfahren sein (z.B. Personalmanagement, Kosten-/Leistungsrechnung, HelpDesk, Netzwerkmanagement, Inventarisierung). Ein IT-Verfahren beschreibt die Gesamtheit der zum Einsatz kommenden IT-Anwendungen, IT-Systemen, Arbeitsabläufe und Schnittstellen.

Mitarbeiterinnen und Mitarbeiter
Mitarbeiterinnen und Mitarbeiter sind Personen, die in einem Dienst- oder Beschäftigungsverhältnis stehen, oder über ein anderes Rechtsverhältnis (z.B. Lehrauftragsnehmer / Lehrauftragsnehmerinnen, Stipendiaten/Stipendiatinnen) entsprechende Funktionen für die Ruhr-Universität Bochum wahrnehmen.

Mitglieder der Ruhr-Universität Bochum
Mitglieder der Ruhr-Universität sind gemäß Art. 3 der Verfassung die Mitglieder des Rektorats, Dekaninnen oder Dekane, das an der Ruhr-Universität nicht nur vorübergehend oder gastweise hauptberuflich tätige Hochschulpersonal, die Doktorandinnen und Doktoranden, die eingeschriebenen Studierenden und die Mitglieder des Hochschulrats.

Netzinfrastruktur
Gesamtheit der für den Betrieb von Netzen notwendigen (technischen) Einrichtungen und Anlagen wie Kabel, Netzdosen, aktive Netzkomponenten (Router, Switches, Firewalls etc.).

Ressourcenmanagement
Eine Planung zum effektiven einsetzen von Ressourcen, wobei unzweckmäßige und nutzlose Benutzungen von Ressourcen erkannt und eliminiert oder gemindert werden.

Risiko
Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit eines Schadens und Schwere des Schadens.

Risikomanagement
Das Risikomanagement umfasst die Identifikation von Risiken, ihre Bewertung, ihre Steuerung und Überwachung.

Zugang
Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

Zugangstoken
Ein technologisches Mittel zur Authentifizierung, um zu einem IT-System Zugang zu erhalten (z.B. Chipschlüssel).

Zugriff
Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt
Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

Zweifaktor-Authentifizierung
Eine Authentifizierung mittels zweier Authentifizierungsmerkmale (siehe Authentifizierungsmerkmale).

15 DOKUMENTENVERZEICHNIS

Zugriff auf die in diesem Rahmenkonzept mit ☞ gekennzeichneten weiterführenden Informationen und Dokumente ist über das separate Dokumentenverzeichnis möglich. Es ist im Intranet über die Webseite der Stabsstelle für Informationssicherheit zugreifbar (☞ itsb.rub.de). Im Dokumentenverzeichnis sind alle Dokumente mit Kennzeichnung des Werdegangs (Dokumentenlenkung) aufgelistet.

16 AUTORENLISTE

Dieses Rahmenkonzept (Version 1.0-0.0 vom 19. Mai 2015) ist vom Koordinierungsausschuss für Informationssicherheit der Ruhr-Universität Bochum erstellt worden. Zum Koordinierungsausschuss gehören vier Vertreter der Fachbereiche Geistes-/Gesellschaftswissenschaften, Ingenieurwissenschaften, Medizin und Naturwissenschaften, die vom IT-Beirat der Ruhr-Universität Bochum benannt sind. Weitere Mitglieder sind die zentrale Beauftragte für Informationssicherheit der Ruhr-Universität Bochum (Vorsitz), der behördliche Datenschutzbeauftragte, sowie jeweils ein Vertreter des zentralen IT-Dienstleisters, der Universitätsbibliothek, der Hochschulverwaltung, der Personalräte und der Studierendenschaft.
Zurzeit sind folgende Mitglieder im Koordinierungsausschuss für Informationssicherheit

Name	**Einrichtung**
Brigitte Wojcieszynski	Zentrale IT-Sicherheitsbeauftragte der RUB (Vorsitz)
Jost Krieger	Zentraler IT-Sicherheitsbeauftragter der RUB (Stellv.)
Dr. Kai-Uwe Loser	Behördlicher Datenschutzbeauftragter
Rainer Wojcieszynski	Rechenzentrum der RUB
Dr. Jörg Albrecht	Universitätsbibliothek der RUB
Haiko te Neues	Universitätsverwaltung
Achim Henkel	Wissenschaftlicher Personalrat
Michael Jost	Wissenschaftlicher Personalrat
Marius Garnhartner	Vertretung der Studierendenschaft
Jan Heinrich	Vertretung der Studierendenschaft
Kristian Knierim	Vertretung der Geistes-/Gesellschaftswissenschaften
Dr. Christoph Wegener	Vertretung der Ingenieurwissenschaften
Dario Carluccio	Vertretung der Ingenieurwissenschaften
Dr. Ralf Sander	Vertretung der Medizin
Prof. Dr. Eckhard Hofmann	Vertretung der Naturwissenschaften

Ausgefertigt aufgrund des Rektoratsbeschluss vom 19. Mai 2015

Bochum, den 18.06.2015

Der Rektor
der Ruhr-Universität Bochum
Universitätsprofessor Dr. Elmar Weiler