Westfälische
Wilhelms-Universität
Münster

› IV – Sicherheitshandbuch 2015

IV – Sicherheitsteam

20.03.2015

wissen.leben
WWU Münster

Vorwort

Der IT-Sicherheit wird schon seit langer Zeit ein hoher Stellenwert an der WWU Münster beigemessen. Bereits 2002 wurden mit Senatsbeschluss weitreichende und stringente Regelungen zur IV-Sicherheit der WWU Münster erlassen und in diesem Zuge auch ein IT-Sicherheitsteam zur Adressierung von sicherheitsrelevanten Themen etabliert.

Auf Basis dieser Strukturen wurden in den letzten Jahren zahlreiche Maßnahmen zur Förderung der IT-Sicherheit getroffen, sowohl durch weitergehende detaillierte Regelungen (Regelungen zur Netzsicherheit und Administratorenordnung), durch organisatorische Maßnahmen (Etablierung eines gemeinsamen Serverraumes für ZIV und IVVen sowie Durchführung eines Sicherheitsaudit) und durch technische Lösungen (speziell bei netzseitigen Sicherheitssystemen wie Firewall, IPS oder Virenfilter). Bei dennoch unvermeidlichen Sicherheitsproblemen kann auf ein gut organisiertes und technisch kompetentes CERT (Computer Emergency Response Team) zurückgegriffen werden.

Von vordringlicher Bedeutung ist es jedoch, den erreichten Stand aufrechtzuerhalten, die Maßnahmen zur IT-Sicherheit weiter zu verbessern und an aktuelle Entwicklungen anzupassen. Dazu muss vor allem das Sicherheitsbewusstsein der Nutzer gefestigt werden – ohne welches technische und organisatorische Maßnahmen nicht die volle Wirkung entfalten können.

Ein wesentlicher Aspekt dabei ist die einfache, schnelle, transparente und kompakte Verfügbarkeit von Informationen zu allen sicherheitsrelevanten Aspekten und deren aktive Verbreitung unter den Nutzern an der WWU Münster. Deshalb hat sich das Sicherheitsteam entschlossen, ein Sicherheitshandbuch zu erstellen, das alle Regelungen, Empfehlungen und Maßnahmen mit Sicherheitsrelevanz zusammenfasst und somit einen zentralen Punkt zur Informationsbeschaffung speziell für alle mit IT-Sicherheit befassten Personen (insbesondere Administratoren), aber auch für alle interessierten Nutzer darstellt.

Durch die Selbstverpflichtung zur Pflege und jährlichen Überarbeitung dieses Dokuments soll darüber hinaus ein Automatismus zur aktuellen Überprüfung der Regelungen und Maßnahmen selbst etabliert, und dadurch ein Beitrag zur Erhaltung und weiteren Verbesserung des Niveaus der IT-Sicherheit an der WWU und zur Vorbeugung von Schadensfällen geleistet werden.

Raimund Vogl

Inhaltsverzeichnis

Einleitung

In diesem Sicherheitshandbuch sollen alle Regelungen und Maßnahmen zusammengefasst werden, die die IV-Sicherheit an der Universität Münster betreffen.

Was bedeutet IV-Sicherheit im Umfeld einer Universität?

Der Einsatz des Computers als Arbeitsmittel hat sich in so gut wie allen Bereichen der Universität durchgesetzt. Viele Arbeitsabläufe sind ohne dieses Hilfsmittel praktisch undenkbar. Fällt dieses Arbeitsmittel aus, so sind in der Regel zeitraubende und kostspielige Folgen abzusehen. Ein Ausfall kann nicht nur durch einen simplen Defekt auftreten, sondern – da heutzutage so gut wie alle Rechner miteinander vernetzt sind – auch leicht von außen bewirkt werden. Wurde eine solche Störung bewirkt, spricht man von Kompromittierung.

Die Arten wie Computer und Computernetzwerke kompromittiert werden können sind vielfältig und haben Auswirkungen auf unsere tägliche Arbeit. Um mögliche Beeinträchtigungen abzuwenden, ist es notwendig die drei Kernbegriffe der IV-Sicherheit zu gewährleisten: **Verfügbarkeit**, **Vertraulichkeit** und **Integrität**.

Das Prinzip der **Verfügbarkeit** besagt, dass Rechnersysteme und die darauf gelagerten Daten immer einsatz-bereit sind bzw. bearbeitet werden können. Dies gilt sowohl für den lokalen Arbeitsplatz, aber auch für Serversysteme, sowie das verbindende Netzwerk. All diese drei Dinge müssen vor Ausfall geschützt werden. So kann über das Netzwerk in Arbeitsplatz- und Serversysteme eingebrochen und auf diesen Daten gelöscht oder die Rechner bzw. deren Betriebssysteme beschädigt werden. Ebenso kann ein Netzwerk z. B. durch Überlastung oder durch Manipulation der Routersysteme zum Ausfall gebracht werden.

Bei der **Vertraulichkeit** geht es um den Schutz der Daten, die auf einem Computer gespeichert sind oder mit diesem bearbeitet werden. Jeder Nutzer möchte sicher sein, dass seine E-Mail oder jeglicher anderer Datenverkehr nicht mitgelesen wird, ebenso sollen z. B. wichtige Forschungs- oder Personaldaten nicht von Dritten ausgespäht oder gar gestohlen werden können.

Bei der **Datenintegrität** gelten ähnliche Umstände. Hier ist die Unversehrtheit bzw. die Verlässlichkeit von Daten wichtig. Die Daten müssen vor Manipulationen von außen geschützt werden.

Um Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten, müssen u. a. folgende Dinge geschützt werden:

- Netzwerke (Ausfallsicherheit)
- Arbeitsplatzcomputer und Serversysteme (Ausfallsicherheit, Schutz der Daten)
- Räume (Schutz vor Diebstahl und Sabotage)

Dieses Sicherheitshandbuch zeigt auf, wie die Universität Münster vorgeht, um den Schutz vor finanziellen, materiellen und personellen Schäden in der WWU zu gewährleisten, ferner soll es das Sicherheitsbewusstsein der Angehörigen der Universität und dem Universitätsklinikum Münster stärken.

Organisatorisch sind Anlaufpunkte und Arbeitsgruppen geschaffen worden, die Mitarbeitern im Umgang mit der IV-Sicherheit zur Seite stehen und ihnen Mittel zur Verfügung stellen, mit dem Zweck die IV-Sicherheit zu erhöhen, sowie für die Weiterentwicklung und Umsetzung der IV-Sicherheit sorgen.

Um IV-Sicherheit zu erreichen, sind von der Universität eine Reihe von Maßnahmen ergriffen worden. So gibt es zunächst einen Katalog von Vorschriften und Regeln, die von Mitarbeitern und Studierenden im Umgang mit der Informationstechnik zu beachten sind und es wurde ein IV-Sicherheitsteam eingerichtet, welches Sicherheits- und Betriebsregelungen erarbeiten und umsetzen bzw. bei deren Umsetzung mitwirken soll.

Der verbleibende Teil diese Handbuches ist wie folgt gegliedert: das Kapitel „Organisation“ befasst sich mit der Organisation der IV-Infrastruktur. Im Kapitel „Regelungen“ werden Regelungen aufgeführt, die für das Universitätsumfeld gelten. Das Kapitel „Sicherheitskonzepte“ betrachtet speziell die Sicherheitskonzepte an der WWU, welche sich unter anderem in die Thematik der Absicherung des Betriebes von IV-Systemen aus Kapitel „Absicherung von IV-Systemen und -Diensten“ eingliedert. Geschlossen wird das Handbuch durch das Kapitel „Empfehlungen für Anwender“ welches dem Anwender konkrete Empfehlung zur Verbesserung der Sicherheit in die Hand gibt.

In den Anhängen sind die wichtigsten Ordnungen bzgl. der IV-Sicherheit zusammengefasst, u. a. die Nutzungsordnung, sowie die Regelungen zur IV-Sicherheit.

Organisation

Dieses Kapitel gibt einen Überblick über die Organisation der IV-Infrastruktur an der WWU Münster.

Organisation der IV-Infrastruktur an der WWU

Bei der Entwicklung der Informationsverarbeitung (IV) an der Universität Münster hat es sich gezeigt, dass eine zentrale Einrichtung allein nicht die individuellen Bedürfnisse aller befriedigen kann. Das IV-Versorgungskonzept ist somit durch eine geregelte Dezentralisierung der Informationsverarbeitung geprägt. Mehrere gleichwertig gelagerte IV-Versorgungseinheiten (kurz: IVV) zeigen sich für individuelle Belange vor Ort verantwortlich. Zusätzlich gibt es zahlreiche Aufgabenbereiche die alle gleichermaßen betreffen; diese Arbeiten werden weiterhin von einer zentralen Einrichtung in enger Kooperation mit allen Versorgungseinheiten geleistet.

Quasi als Klammer des gesamten IV-Systems der Universität besteht somit das Zentrum für Informationsverarbeitung (ZIV). Das ZIV ist eine zentrale Betriebseinheit der Universität.

Auf der dezentralen Ebene existieren für die IV-Versorgung der Fachbereiche folgende IV-Versorgungseinheiten:

- IVV 1: Geisteswissenschaften
- IVV 2: Wirtschaftswissenschaften
- IVV 3: Rechtswissenschaften
- IVV 4: Naturwissenschaften (ohne Geowissenschaften)
- IVV 5: Mathematik und Psychologie
- IVV 6: Geowissenschaften und Geologie
- IVV 7: Theologie, Erziehungs- und Sozialwissenschaften
- IVV 8: Medizinische Einrichtungen
- IVV 9: Zentrale Universitätsverwaltung
- IVV 10: Universitäts- und Landesbibliothek

Für Entscheidungs- und Koordinierungsaufgaben, Aufgaben des Controllings sowie für das Beschaffungs- und Finanzwesen des IV-Systems sind zuständig:

- IV-Kommission[1]
- IV-Lenkungsausschuss[2]
- IV-Beschaffungsabteilung der zentralen Universitätsverwaltung (ZUV) und der Verwaltung der medizinischen Einrichtungen (VME)

Aufgabenaufteilung und Verantwortlichkeiten der einzelnen Einrichtungen sind durch einen Senatsbeschluss der Universität klar geregelt. Weiterführende Information hierzu finden sich in

- dem Senatsbeschluss vom 8.7.1996: Das System der Informationsverarbeitung der WWU Münster[3],
- der Kooperation zwischen IV-Versorgungseinheiten und ZIV[4],
- der Aufgabenteilung zwischen IV-Versorgungseinheiten und ZIV[5],
- bei dem IV-Lenkungsausschuss,
- im Statut des IV-Lenkungsausschusses[6] und
- in der Ordnung für die IV-Kommission[7].

[1] https://www.uni-muenster.de/Senat/iv_komm.html
[2] https://www.uni-muenster.de/wwu/leitung/ausschuesse/iv-lenkung.shtml
[3] Diese Regelung steht zurzeit nicht elektronisch zur Verfügung und wird in einer Aktualisierung nachgetragen.
[4] Diese Regelung steht zurzeit nicht elektronisch zur Verfügung und wird in einer Aktualisierung nachgetragen.
[5] Die Aufgabenverteilung ist im Anhang zur IT-Strategie der WWU enthalten und auf den Seiten des ZIV einsehbar:
Dienste des ZIV: https://www.uni-muenster.de/ZIV/Service/Dienste/index.html
Dienste der IVVen: https://www.uni-muenster.de/ZIV/Service/Dienste_der_IVVen.html
[6] https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/2008/ausgabe16/statut_lenkungsausschuss.pdf
[7] https://www.uni-muenster.de/Rektorat/abuni/ab70603.htm

Sicherheitsteams

IV-Sicherheitsteam der WWU

Aufgrund der vom Rektorat beschlossenen Regelungen zur IV-Sicherheit in der Universität Münster wurde am 18.04.2002 ein IV-Sicherheitsteam[8] eingerichtet (siehe Anhang B | Regelungen zur IV-Sicherheit in der Universität Münster, § 4), welches Sicherheits- und Betriebsregelungen erarbeiten und umsetzen bzw. bei deren Umsetzung mitwirken soll. Zu seinen Aufgaben gehören:

- Definition wirksamer Sicherheitsstandards und Betriebsregelungen in Abstimmung mit den IVVen.
- Landesweite Abstimmung der Sicherheitsstandards und Betriebsregelungen.
- Überwachung der Umsetzung der Sicherheitsstandards. Dazu können in den Einrichtungen der Universität Sicherheitsüberprüfungen vorgenommen werden.
- Aufstellung eines Ausbildungs- und Schulungskonzepts zur IV-Sicherheit für Nutzer, Administratoren und Mitglieder des IV-Sicherheitsteams, das auch für die Maßnahmen zur Verbesserung der IV-Sicherheit sensibilisieren soll.
- Ansprechpartner für alle sicherheitsrelevanten Fragen zu sein.
- Entgegennahme und Dokumentation aller sicherheitsrelevanten Vorfälle, die zusätzlich an externe Stellen (z. B. das DFN-CERT) zu berichten sind.
- Zusammenstellung der jährlichen Finanzbedarfe und Vorbereitung des jährlichen Berichts.

IVV-Administratoren

Ähnlich wie das ZIV-Sicherheitsteam ist die Gruppe der Administratoren der IVVen für die Umsetzung und Ein-haltung der Sicherheitsstandards in den IVVen verantwortlich.

Computer Emergency Response Team (CERT) der WWU

Das Computer Emergency Response Team (CERT)[9] der WWU (kurz: WWU-CERT) ist verantwortlich für die Bearbeitung von sicherheitsrelevanten Vorfällen im Zusammenhang mit der Nutzung von Rechnern und Kennungen in bzw. an der Universität Münster.

Ziel ist es, die Reputation der WWU vor fahrlässiger oder illegaler Nutzung der IP-Adressen und Ressourcen der WWU zu schützen. Dazu gehören u.a. folgende Aufgaben:

- Möglichst schnelle und effiziente Hilfe als Reaktion auf eintretende Vorfälle (z. B. bei Hack-Angriffen, kritischen Sicherheitslücken, Computerviren und -Würmern etc.).
- Sperrung von Rechnern bzw. Kennungen bei akuten Vorfällen.
- Aufbereitung von Informationen und Durchführung von Untersuchungen soweit dies der Vorbeugung dient oder für die Überprüfung von Hinweisen notwendig ist.
- Prüfung und ggfs. Reaktion auf Urheberrechtsverletzungen.
- Bearbeitung von staatsanwaltlichen und polizeilichen Anfragen.
- Betrieb von Intrusion Detection und Intrusion Prevention Systemen (IDS/IPS).
- Kooperation mit dem CERT des Deutschen Forschungsnetzwerks (DFN-CERT) und allen an der WWU für Sicherheit Verantwortlichen.
- Mitarbeit bei der Konzeption sicherheitsrelevanter Regelungen.

Wie geht das CERT vor?

Sobald das WWU-CERT den Hinweis auf einen Vorfall erhält, wird bei Arbeitsplatzrechnern von Mitarbeitern, Poolrechnern o.ä. versucht, den technisch Verantwortlichen telefonisch zu erreichen, um mit ihm die nötigen Maßnahmen und ggf. die Abschaltung des Rechners abzusprechen. Ist kein Verantwortlicher erreichbar, wird der Rechner netzseitig getrennt und der technisch Verantwortliche und die zuständige IVV werden per E-Mail mit Informationen zum Vorfall und den bereits ergriffenen und vom Nutzer zu ergreifenden Maßnahmen benachrichtigt.

Bei Vorfällen im Einwahlbereich (VPN, WLAN etc.) wird direkt eine evtl. bestehende Verbindung getrennt und eine Einwahlsperre gesetzt. Die Nutzerkennung ist durch diese Sperre nicht in ihrer sonstigen Benutzung eingeschränkt. Auch in diesem Fall wird eine E-Mail mit genauen Hinweisen auf die Art des Vorfalls und auf die zur Freischaltung zu ergreifenden Maßnahmen an den betroffenen Nutzer versendet.

Alle IVVen und Einrichtungen sind angehalten, Sicherheitsvorfälle dem CERT zu melden. In der Regel ist ein Sicherheitsbruch selten lokal begrenzt sondern hat meist universitätsweite Auswirkungen. Das WWU-CERT

---

[8] https://www.uni-muenster.de/Rektorat/abuni/ab020507.html und
https://www.uni-muenster.de/Rektorat/abuni/ab040107.html

[9] https://www.uni-muenster.de/ZIV/CERT

ist in diesem Fall die zentrale Anlaufstelle, um ggf. Maßnahmen zu koordinieren und alle potentiell Betroffenen zu informieren und vor Folgeproblemen zu warnen. Mögliche Vorfälle sollen unter Angabe aller relevanten Informationen (z. B. Log-Dateien oder E-Mail-Header) per E-Mail an cert@uni-muenster.de gemeldet werden.

Das WWU-CERT arbeitet eng mit dem DFN-CERT des Deutschen Forschungsnetzes (DFN) zusammen. Das DFN-CERT koordiniert den Austausch von Beschwerden und Informationen über kompromittierte Systeme anderer Einrichtungen des DFNs.

Zertifizierungsstelle der WWU

Die Zertifizierungsstelle (Certification Authority, CA) der WWU, kurz WWUCA[10], wird vom Zentrum für Informationsverarbeitung (ZIV) betrieben und arbeitet im Rahmen der Public Key Infrastruktur des Deutschen Forschungsnetzes (DFN-PKI).

Als offizielle Zertifizierungsinstanz steht die WWUCA allen Einrichtungen und Angehörigen der Universität Münster und des Universitätsklinikums Münster zur Verfügung.

Die WWUCA bietet die folgenden Dienstleistungen an:

- Ausstellen von X.509-Zertifikaten für SSL-/TLS-Server
- Ausstellen von X.509-Zertifikaten für Personen (SSL-/TLS-Clients, S/MIME u. a.)
- Ausstellen von X.509-Zertifikaten für Gruppen und Amtsträger (SSL-/TLS-Clients, S/MIME u. a.)

Hierbei werden X.509-Zertifikate im Rahmen der Global- und der Grid-Hierarchien der DFN-PKI ausgestellt.

Die Mitarbeiter der WWUCA und die von der WWUCA als Registrierungsstelle eingesetzten Mitarbeiter aus der WWU und dem UKM wurden ausdrücklich belehrt und verpflichtet, sich beim Ausstellen von Zertifikaten strikt an die Zertifizierungsrichtlinien und diejenigen der DFN-PKI zu halten.

Die Zertifizierungsstelle für X.509-Zertifikate wird von der DFN-PCA betrieben, der sogenannten Wurzelinstanz (Policy Certification Authority). WWUCA-Mitarbeiter und Registrierungsstellen führen die Registrierung über eine von der DFN-PCA bereit gestellte Weboberfläche durch und weisen sich dabei mit Client-Zertifikaten aus. Diese liegen im verschlüsselten Browser-Zertifikatspeicher in virtuellen Maschinen mit verschlüsseltem Dateisystem, welche auf den sorgfältig abgesicherten persönlichen Arbeitsplatzrechnern liegen, ausschließlich zur Registrierung gestartet werden und beim Abschalten komplett in den ursprünglichen Zustand zurückversetzt werden.

Datenschutzbeauftragter der WWU

Die Universität Münster beschäftigt einen Datenschutzbeauftragten. Die/der aktuelle Beauftragte ist im Organisationsplan[11] hinterlegt.

Bei der Erfüllung der Aufgaben sind der Datenschutzbeauftragte sowie seine Vertreterin von allen Organisationseinheiten zu unterstützen. Soweit sie personenbezogene Daten verarbeiten, sind die Mitarbeiter verpflichtet, bei der Einführung neuer Verfahren oder Änderung bestehender Verfahren sowie bei der Erarbeitung interner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten den Datenschutzbeauftragten frühzeitig zu beteiligen.

[10] https://www.uni-muenster.de/WWUCA
[11] https://www.uni-muenster.de/intern/organisation/index.html (Intranet) und https://www.uni-muenster.de/Verwaltung/index.html (öffentliche Seite)

Regelungen

Dieses Kapitel gibt einen Überblick der geltenden Regelungen für Nutzer der IV-Infrastruktur der Universität Münster. Für die Universität Münster wurden mehrere die IV-Sicherheit betreffende Vorschriften verfasst und z. T. als amtliche Bekanntmachungen veröffentlicht. Zusätzlich zu den allgemein gültigen Gesetzen sind die-se somit rechtsverbindlich.

Gesetze und Vorschriften

Allgemeine Gesetzgebung

Übergreifend sind bei der Einführung und Aufrechterhaltung der Sicherheit im IT-Umfeld folgende Gesetze zu beachten:

- Datenschutzgesetz (BDSG bzw. DSG-NRW)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)

Bei Verstößen und um einem Missbrauch der IT-Systeme entgegen zu wirken kommen außerdem folgende Gesetze zur Anwendung:

- Strafgesetzbuch (StGB)
- Urheberrechtsgesetz (UrhG)

Benutzungsordnung

In der allgemeinen Benutzungsordnung wird der Umgang mit der IV-Infrastruktur festgelegt.

- Anhang A | Benutzungsordnung des Zentrums für Informationsverarbeitung und der IV-Versorgungseinheiten der Universität Münster[12]

Im Sinne der Sicherheit finden sich dort vor allem die Rechte und Pflichten der Nutzer sowie des ZIV und der IVVen. Insbesondere ist der Missbrauch (durch Nutzer), der zu Sicherheitsvorfällen führen kann, klar definiert und auch die möglichen rechtlichen Schritte im Falle des Zuwiderhandelns. Für ZIV und IVVen finden sich vor allem betriebliche Rahmenbedingungen, die einen möglichst stabilen und dadurch sicheren Betrieb der IV-Infrastruktur gewährleisten sollen. Auch ist der Umgang mit potentiell personenbezogenen Daten festgelegt, um auf der einen Seite den Anforderungen des Datenschutzes zu genügen und um auf der anderen Seite im Falle eines Sicherheitsvorfalls gegen mutmaßliche Täter vorgehen zu können.

Regelungen zur IV-Sicherheit

Die Universitätsleitung hat als Grundlage für die Sicherheit in der Informationsverarbeitung die Regelungen zur IV-Sicherheit in der Universität Münster als amtliche Bekanntmachungen veröffentlicht.

- Anhang B | Regelungen zur IV-Sicherheit in der Universität Münster[13]
- Änderung der Regelungen zur IV-Sicherheit in der Universität Münster[14] (in „Anhang B | Regelungen zur IV-Sicherheit in der Universität Münster“ enthalten)

In dieser Bekanntmachung werden die Rahmenbedingungen festgelegt, die einen möglichst sicheren Betrieb gewährleisten sollen. So finden sich dort u. a.

- Betriebsregelungen für Netzwerke und Server
- Benennung der Verantwortlichen und deren Verpflichtungen
- Grundlegende Sicherheitsmaßnahmen insbesondere der Schutz personenbezogener Daten
- Methoden für Maßregelungen bei Gefährdung der Sicherheit
- Bestellung eines Sicherheitsteams und dessen Aufgabenbereiche
- Grundlegende Maßnahmen für die Notfallvorsorge

Netzordnung

Die Netzordnung richtet sich zunächst an das ZIV, da sie Betriebsparameter für die Netzinfrastruktur und die Zusammenarbeit mit dem DFN-Verein regelt.

---

[12] https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2010/ausgabe25/beitrag_03.pdf
[13] https://www.uni-muenster.de/Rektorat/abuni/ab020507.html
[14] https://www.uni-muenster.de/Rektorat/abuni/ab040107.html

› Betriebsregelung für die Nutzung der Netzdienste[15]

Es findet sich dort auch eine Definition über die missbräuchliche Nutzung der Netzinfrastruktur, Empfehlungen, wie dies zu verhindern ist, sowie die möglichen Konsequenzen bei Zuwiderhandlung.

Die Netzordnung ist eine Ergänzung zur Benutzerordnung und die dort definierten Sicherheitsvorschriften und Sicherheitsmaßnahmen sind gleichermaßen als verbindlich zu beachten.

Des Weiteren gibt es die

› Anhang C | Betriebsregelung für das Datennetz der Universität Münster[16]

Ordnung für Technisch Verantwortliche und Administratoren

In der Ausführung der Regelungen zur IV-Sicherheit der Universität Münster wurde die Rolle des Technischen Verantwortlichen eingeführt.

Der Technisch Verantwortliche stellt die Schnittstelle zwischen ZIV/IVV und den Anwendern von IV-Systemen dar. Er ist zunächst für den netzseitigen Anschluss und den Betrieb der Geräte verantwortlich und auch für deren (netzseitige) Sicherheit. In diesem Zusammenhang hat er auch eine Aufsichtspflicht über den Administrator oder, falls dieser nicht existiert, über den Besitzer, den Nutzer oder den Einrichter des Endgerätes.

› Anhang D | Die/der Technisch Verantwortliche für vernetzte IV-Systeme an der Universität Münster[17]

Zusätzlich zur Rolle des Technisch Verantwortlichen ist die Rolle des Administrators definiert, der gleichermaßen für den Schutz des Betriebssystems, der Software und der Daten des Endgerätes verantwortlich ist.

› Anhang E | Ordnung für IT-Administratoren an der Universität Münster[18]

Interne Leitlinien der Universität Münster

Richtlinien für Accountvergabe/Netzzugang

Die Vergabe der Nutzerkennungen (Accounts) an der Universität erfolgt, soweit möglich, automatisiert über die Studierenden- oder Personalverwaltung der Universität. Zusätzlich kann jede Institution weitere Nutzerkennungen beim ZIV beantragen und einrichten lassen. Die auf dem Antragswege erteilten Nutzerkennungen sind stets zeitlich befristet.

Eine Nutzerkennung alleine reicht nicht aus, um die IT-Systeme nutzen zu können. Der Zugriff auf die IT-Systeme wird rollenbasiert gesteuert. So ist der Zugriff auf bestimmte Systeme nur dann möglich, wenn der Nutzer bzw. die Nutzerkennung einer dazu berechtigten Nutzergruppe (Rolle) zugeordnet ist. Dies gilt insbesondere für den Netzzugang. Um sich in das Netzwerk der Universität einwählen zu können, ist ein separates Passwort nötig, und auch hier kann dieser Zugang je nach Nutzergruppe erlaubt oder verweigert werden.

Nutzern, deren Netzzugangskennung missbraucht wurde, kann der Netzzugang gesperrt werden. Ausgewählte Mitglieder der IVVen oder der Institute können vorhandene Accounts in die von Ihnen betreuten Nutzer-gruppen selbst eintragen und verlängern.

Wer hat Anspruch auf Zugang?

Es gibt diverse Teilnehmergruppen, die Anspruch auf Zugang zu den IT-Systemen und dem Netzwerk der Universität Münster haben und diesen benötigen. Dabei wird basierend auf dem Identitätsmanagement oft ein eingeschränktes Nutzungsrecht definiert.

Universitätsangehörige

Hauptgruppe der Nutzer sind die Mitarbeiter und die Studierenden der Universität. Diesen Nutzern wird ein umfangreiches Nutzungsrecht zu allen IT-Diensten der Universität gewährt. Je nach Zugehörigkeit zu Instituten oder Einrichtungen können die Standardzugangsrechte erweitert werden, um auch Spezialsysteme oder institutseigene Systeme benutzen zu können.

---

[15] https://www.uni-muenster.de/ZIV/Organisation/RegelungNetzdienste.html
[16] Diese Regelung steht zurzeit nicht elektronisch zur Verfügung und wird in einer Aktualisierung nachgetragen.
[17] https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/abuni2004/ausgabe7/ab040705.pdf
[18] https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2009/ausgabe18/beitrag9.pdf

Mitarbeiter

Für die Mitarbeiter, die in der Personalverwaltung der Universität geführt werden, wird die Nutzungsberechtigung für die IT-Systeme, deren Nutzeradministration zentral über das ZIV erfolgt, bei der Einstellung automatisch eingerichtet. Bei diesen Mitarbeitern ist die bei der Einstellung übliche Belehrung unter besonderer Berücksichtigung der Maßnahmen zur IV-Sicherheit und des Datenschutzes vorzunehmen.

Nutzungsberechtigungen für Personen, die nicht in der Personalverwaltung der Universität geführt werden, müssen beim ZIV beantragt werden.

Scheiden Mitarbeiter aus, wird die Nutzungsberechtigung eingeschränkt und nach einer Übergangszeit gesperrt. Die Berechtigung zur IV-Nutzung kann nur beibehalten werden, wenn sie von der Leitung des Instituts oder der Einrichtung ausdrücklich beantragt wird. Andernfalls kann lediglich die E-Mail-Adresse durch Beitritt zum Alumni-Club beibehalten werden.

Studierende

Die Nutzungsberechtigung für die IT-Systeme, deren Nutzeradministration zentral über das ZIV erfolgt, wird automatisch mit der Immatrikulation eingerichtet. Nach der Exmatrikulation wird die Nutzungsberechtigung nach einer Übergangszeit gesperrt. Danach kann lediglich die E-Mail-Adresse durch Beitritt zum Alumni-Club beibehalten werden.

Alumni

Als Alumni an der Universität Münster gelten diejenigen Personen, die hier studierten, promoviert wurden, lehrten oder in einem anderen Bereich der Universität arbeiteten. Auf Antrag erhalten die Mitglieder des Alumni-Clubs eine Nutzerkennung, können diese jedoch nur für den Zugriff auf das E-Mail-System der Universität benutzen. Ein Zugriff auf die für Forschung und Lehre eingeschränkten Systeme ist nicht möglich. Insbesondere können Alumni auch nicht den Netzzugang benutzen.

Wohnheime

Ein Teil der Wohnheime, die nicht vom Studentenwerk Münster verwaltet werden (private Träger), ist direkt an das Netzwerk der Universität Münster angeschlossen.

Universitäts- und Landesbibliothek (ULB)

Die Universitäts- und Landesbibliothek Münster (ULB) ist die Zentralbibliothek der WWU und gleichzeitig Landesbibliothek für den Landesteil Westfalen. Da die ULB nicht nur die Angehörigen der Universität bedient, sondern auch allen übrigen Personen zur Nutzung offen steht, werden hier eingeschränkte Nutzerkennungen vom ZIV zur Verfügung gestellt. Diese Kennungen (sog. Bürger-Kennungen) sind in Ihrer Nutzung so eingeschränkt, dass sie nur in der ULB an den dafür vorgesehenen PC-Arbeitsplätzen genutzt werden können. Diese Kennungen werden von der ULB verwaltet.

Externe Firmen

Für Mitarbeiter von externen Firmen, die etwa zum Zweck der Dateneingabe oder der Kontrolle und Überwachung ihrer Geräte einen Zugang zum Netz der Universität benötigen, ist nur ein Zugang zu gewähren, der netzseitig vom Rest der universitären IT-Systeme getrennt ist. Für externe Mitarbeiter, die vor Ort in den Instituten arbeiten, ist ein Arbeitsplatz einzurichten, der nur in abgeschotteten VLANs agieren kann. Für Firmen, die von außerhalb ihre Geräte verwalten und überwachen wollen, wird ein spezieller VPN Zugang eingerichtet, der ausschließlich den Zugriff auf die firmeneigenen Geräte ermöglicht und komplett getrennt vom Netzwerk der Universität betrieben wird.

Da die Abschottung lediglich auf der Netzwerkebene erfolgt, können solche Zugänge immer nur in Absprache mit dem ZIV erfolgen. Sollen für externe Firmen derartige Zugänge eingerichtet werden, so ist stets das ZIV hinzuzuziehen.

Mitversorgte Einrichtungen

Externe Einrichtungen, die vom ZIV aufgrund besonderer Absprachen mitversorgt werden, können Benutzer-kennungen beantragen.

Gäste

Für Gäste der Universität – etwa Konferenzteilnehmer oder Institutsgäste – können Gastkennungen eingerichtet werden.

Zugangsrechte dieser Kennungen werden in Absprache mit dem verantwortlichen Konferenz- oder Institutsleiter festgelegt. Im Standardfall berechtigen die Kennungen nur für den Zugang zum Netzwerk der Universität und gewähren ansonsten keinerlei Zugang zu weiteren Diensten oder passwortgeschützten Systemen.

Diese Abschottung erfolgt z. T. dadurch, dass Gastkennungen nicht in das Active-Directory-System übertragen werden.

Anonyme Rechnerzugänge

Anonyme Rechnerzugänge sind nicht erlaubt. Jeder Zugriff auf die Systeme der Universität muss mit einer eindeutigen und einer Person zugeordneten Identität erfolgen. Dies ist notwendig, um eingeschränkte Bereiche rollenbasiert schützen zu können und im Fall des Missbrauchs angepasste Präventiv-Maßnahmen sowie ggf. rechtliche Schritte einleiten zu können. Für angemeldete Konferenzkennungen hat der Leiter der Konferenz nachzuhalten, wer die entsprechenden Kennungen genutzt hat.

Zutrittsregelungen, Zutrittskontrolle und Alarmanlagen

Da ein Einbruch in ein IT-System nicht nur über das Netzwerk geschehen kann, ist auch der Fall des physischen Einbruchs zu bedenken. Sicherheitskritische Systeme dürfen nicht in öffentlich zugänglichen Räumlichkeiten aufgebaut werden, in denen die Gefahr des Diebstahls oder der Beschädigung durch Dritte besteht. Insbesondere Serversysteme und Netzwerkkomponenten, deren Diebstahl oder Ausfall verheerende Konsequenzen nach sich ziehen könnte, müssen zwingend in abschließbaren Räumlichkeiten untergebracht wer-den.

Allen Betreibern von solchen Systemen wird dringend nahegelegt, für derartig gesicherte Räumlichkeiten zu sorgen und durch angemessene Schließ- und Kontrollsysteme sicherzustellen, dass nur berechtigtes Personal Zutritt zu diesen Geräten bekommt.

Für Systemräume sind geeignete Zutrittsregelungen zu erlassen und angemessene Sicherungen vorzusehen. Für die ZIV-Gebäude wurden z. B. eine Zugangssicherung zum Einbruch- und Sabotageschutz und eine Feuer-alarmierung eingerichtet. Der Zutritt zu den Räumen wird in den Technischen Diensten der WWU protokolliert; die Protokolle werden gemäß einer Regelung zwischen Personalräten und Universitätsleitung aufbewahrt.

Die zentralen gemeinsam genutzten Serverräume der Universität am Schlossplatz und der Einsteinstraße verfügen ebenfalls über ein solches Zutrittskontrollsystem. Es liegt in der Verantwortung der Betreiber dezentraler Serverräume, selbst für entsprechende Maßnahmen zu sorgen.

Falls ein besonderer Schutzbedarf besteht, etwa weil sich wichtige Forschungs- oder Patienten-Daten auf den Geräten befinden, oder weil ein Ausfall kritische Folgeschäden verursachen würde, so ist gegebenenfalls ein Alarmmeldesystem zu installieren.

Verhalten bei Sicherheitsvorfällen und Notfallkonzept

Bei Sicherheitsvorfällen ist nach einem Notfallkonzept vorzugehen, das ggf. erstellt werden muss. Die entsprechenden Unterlagen sind so aufzubewahren, dass sie jederzeit auch bei Ausfall der Rechner zugänglich sind. Als Beispiel eines derartigen Notfallkonzeptes kann auf die Notfallmaßnahmen des ZIV[19] zurückgegriffen werden, die im Intranet des ZIV abgelegt sind und nur in schematischer Form abgegeben werden können.

Weitere Einzelregelungen für den Betrieb und seinen Wiederanlauf nach Störungen sowie der Umgang mit Angriffen gegen die IV-Sicherheit sind in den zuständigen Abteilungen des ZIV und in den IVVen nach den Regeln der IV-Kunst zu organisieren und soweit erforderlich zu dokumentieren, damit auch Vertreter die Auf-gaben wahrnehmen können.

Sanktionen bei Nichtbeachtung der Sicherheitsmaßnahmen

Personen oder Institutionen, die sich über die vorgegebenen Regeln zur IV-Sicherheit hinwegsetzen, können erhebliche Schäden und Kosten verursachen. Die Einhaltung dieser Vorgaben wird – wo immer das möglich ist – bei jedem Netzzugang und durch regelmäßige Sicherheitsbegehungen überprüft. Die verursachten Schäden und der zusätzliche Aufwand zu ihrer Beseitigung kann gemäß der Benutzerordnung in Rechnung gestellt werden.

Aus- und Weiterbildung

Eine umfassende Aus- und Weiterbildung zu allen Themen der IV-Sicherheit ist für die große Anzahl der Universitätsmitglieder und die damit verbundene Fluktuation nicht zu leisten. Jedes Mitglied der Universität ist daher verpflichtet, selbst für das notwendige Wissen zu sorgen. Die einschlägige Literatur ist umfassend. Besonders wird auf das Grundschutzhandbuch des BSI[20] verwiesen. Firmenspezifische Berichte

---

[19] https://www.uni-muenster.de/ZIVwiki/bin/view/ZIV/Notfallplan (ZIV-Intranet)
[20] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

stehen darüber hinaus für die relevanten Produkte zur Verfügung. Administratoren, technisch Verantwortlichen und Institutsdirektoren kommt dabei, zusätzlich zur Verantwortung der Nutzer selbst, eine besondere Verantwortung zu.

Detailregelungen

Richtlinien für sichere Passwörter

Nur persönliche Passwörter schützen davor, dass Unbefugte auf fremde Daten zugreifen oder gar im Namen anderer Straftaten begehen. Daher sind Passwörter unbedingt mit größter Sorgfalt zu behandeln:

- Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.
- Passwörter sollten alle vier Wochen, spätestens alle sechs Monate geändert werden.
- Passwörter sollten nicht trivial sein – also in keinem Wörterbuch stehen – keinen persönlichen Bezug zum Besitzer aufweisen und im Idealfall mehrere Sonderzeichen enthalten.

Um ein möglich sicheres Passwort zu generieren sind folgende Tipps hilfreich:

- Bedingungen an sichere Passwörter[21]
- Weitere Hinweise und Bedingungen für Passwörter an der WWU werden in MeinZIV -› Passwörter und PINs genannt.

Endsysteme mit Mehrfachnetzanbindungen

Mehrfachnetzverbindungen von Endsystemen können erforderlich sein, wenn z. B. Verbindungen zur Erhöhung der Ausfallsicherheit redundant ausgelegt werden, mehrere Verbindungen zur Erhöhung von Ausfallsicherheit und Durchsatz gebündelt werden oder ein Endsystem gleichzeitig in mehrere Netzzonen des Rechnernetzes angeschlossen werden soll.

Insbesondere durch den starken Trend zur Virtualisierung auch im Endsystembereich (Stichworte: VMware, ESX-Server, Blade-Center-Architekturen etc.) entsteht immer häufiger aus den bereits genannten Gründen die Anforderung an Mehrfachnetzverbindungen. Dabei gibt es ein relativ umfangreiches Spektrum an technischen Realisierungsmöglichkeiten (Stichworte: Link-Aggregation, VLAN-Technologie etc.), aber auch an möglichen Risiken sowohl hinsichtlich der Sicherheit (Verfügbarkeit, Vertraulichkeit und Integrität der Netzzonen inner-halb der Netzsicherheitsarchitektur) als auch der Betriebsstabilität der betroffenen Teilnetze als auch des Gesamtnetzes.

Eine Detailregelung Endsysteme mit Mehrfachnetzverbindungen innerhalb der Netzsicherheitsarchitektur ist im Entwurf und wird nach Verabschiedung veröffentlicht werden.

WLAN Bereitstellung bei Konferenzen, Tagungen und Veranstaltungen

Für Konferenzen und ähnliche Veranstaltungen bietet das ZIV die Möglichkeit die Funkzellen VPN/WEB zu nutzen. Um für die Konferenzteilnehmer einen sehr einfachen Zugang zum WLAN der Universität Münster zu ermöglichen, d. h. ohne großen Konfigurationsaufwand, ist die Funkzelle unverschlüsselt (ohne WPA bzw. WPA2 Verschlüsselung). Der Name der Funkzelle (sogenannte „SSID“) lautet VPN/WEB. Die Konferenzteilnehmer müssen sich mit der SSID verbinden und beim Öffnen eines beliebigen Browsers (z. B. Internet Explorer) wird der Konferenzteilnehmer automatisch auf eine Anmeldeseite geführt, auf der er seine Konferenzkennung und Passwort eingibt. Nach erfolgter Authentifizierung hat er Zugang zum Internet. Die Beantragung von Konferenzkennungen kann der Veranstalter der Konferenz vornehmen.

Zu beachten ist, dass das WLAN-Netz unverschlüsselt ist und der Datenverkehr daher *abhörbar* ist. Die Einrichtung dieser speziellen WLAN-Netze ist auch nur dort möglich, wo die WLAN-Infrastruktur mit den neuen Access Points der Firma Cisco ausgestattet ist.

Gastzugänge im WLAN

Grundsätzlich gilt, dass alle Nutzerkennungen realen Personen zugeordnet sein müssen und nicht anonym sein können. Um für Veranstaltungen der WWU, deren Teilnehmer für die Dauer der Veranstaltung Zugang zum Rechnernetz (insbesondere über WLAN) benötigen, rechtzeitig Nutzerkennungen zur Verfügung stellen zu können, besteht die Möglichkeit, diese Kennungen in benötigter Anzahl vorab zu erstellen. Die Erfassung der Namen der Teilnehmer und die Zuordnung zu den Nutzerkennungen müssen dann nachträglich erfolgen. Das Antragsverfahren ist nicht formalisiert; es reicht ein Brief auf dem offiziellen Briefbogen der ausrichtenden Ein-richtung, unterschrieben von deren Leiter oder vom Leiter der zuständigen IVV, mit den folgenden Angaben:

[21] https://www.uni-muenster.de/IV-Sicherheit/passwoerter.html

- Name der Veranstaltung
- Angaben zum Veranstalter: Name der Einrichtung, die eine Einrichtung der WWU sein muss, und deren Adresse
- Zeitraum der Veranstaltung
- Anzahl der benötigten Kennungen
- Verantwortliche(r) Mitarbeiter(in) der WWU (keine Hilfskräfte). Der/die Verantwortliche muss eine ZIV-Nutzerkennung besitzen und den Brief ebenfalls unterschreiben.

Der Antrag ist mindestens eine Woche vor Veranstaltungsbeginn an das

Zentrum für Informationsverarbeitung (ZIV), Nutzerverwaltung, Einsteinstr. 60, 48149 Münster

(auch per Hauspost) zu richten. Nach dem Erstellen der Kennungen (etwa eine Woche vor Veranstaltungsbeginn) werden Formulare erstellt, die dem Veranstalter per Hauspost zugeschickt oder ggf. persönlich am Serviceschalter abholt werden. Jedes Formular enthält eine Konferenzkennung, das zugehörige Anfangspasswort und Felder zum Erfassen der Daten des Nutzers. Der Veranstalter verpflichtet sich nachzuhalten, wem welche Kennung ausgehändigt wird, z. B. indem er die o. g. Formulare ausfüllen lässt.

Ferner besteht die Möglichkeit für Gäste, soweit ihre jeweiligen Heimat-Einrichtungen (z. B. Universitäten) am eduroam-Projekt (s. u.) teilnehmen, sich mit ihren persönlichen Heimat-Kennungen verschlüsselt über die Funkzelle mit der SSID „eduroam“ zu verbinden.

DFNRoaming / eduroam

Mit DFNRoaming können registrierte Nutzer einfach, kurzfristig und ohne zusätzliche Anmeldung einen Zugang zum Wissenschaftsnetz nicht nur in ihrer eigenen, sondern auch bei anderen wissenschaftlichen Einrichtungen bekommen. DFNRoaming[22] ist dabei in entsprechende europäische Vorhaben (eduroam[23]) eingebettet, die auch grenzüberschreitend eine transparente Nutzung der Wissenschaftsnetze ermöglichen soll.

DFNRoaming wird in enger Zusammenarbeit zwischen dem DFN-Verein und den Rechenzentren der am Wissenschaftsnetz angeschlossenen Einrichtung en aufgebaut. Zunächst wird DFNRoaming für den Zugang zum Wissenschaftsnetz über ein WLAN angeboten. Bei Bedarf kann DFNRoaming auch für einen kabelgebundenen Zugang eingesetzt werden.

An der WWU Münster wird dazu als Funkzellenname (SSID) „eduroam“ verwendet. Darüber hinaus ist die WLAN-Konfiguration praktisch identisch zu der Konfiguration für die universitätsintern verwendete SSID „uni-ms“ bzw. „wwu“. Als Login-Daten dienen Ihre altbekannte Nutzerkennung (die um den sogenannten „Realm“ „@uni-muenster.de“ ergänzt werden muss) und Ihr Netzzugangspasswort.

Aufbewahrungsregeln für Log-Daten

Die kurzzeitige Aufbewahrung der Logfiles ist für nachträgliche Fehleranalysen unverzichtbar, da ohne eine solche kurzzeitige Aufbewahrung eine nachträgliche Fehleranalyse bei Problemen, die einzelne Nutzer - d. h. nicht das Gesamtsystem - betreffen, unmöglich ist. Die Logfiles werden im Rotationsverfahren überschrieben. Eine personenbezogene Verarbeitung der Daten wird nicht vorgenommen. Es wird eine automatische Löschung alter Daten durch Überschreiben mit neueren Daten durchgeführt.

Unter Beachtung von Telekommunikations- (TKG), Telemedien- (TMG) und Datenschutzgesetz (DSG) gelten folgende Aufbewahrungszeiten:

Bereich Kommunikationssysteme

RADIUS-Systeme

RADIUS dient zur Authentifizierung und zum Accounting bei jeder Art von Einwahl, konventionell über Modem oder ISDN, VPN oder WLAN.

Bei der Authentifizierung werden alle Aktivitäten der RADIUS-Server mitprotokolliert. Diese Daten werden nach typischerweise max. zwei Tagen automatisch überschrieben. Erkennbar sind die Sitzungen einzelner Nutzer. Es werden folgende Daten erfasst:

- Nutzerkennung,
- Start und Ende der Sitzung,
- Art der Nutzung (z. B. Modem, ISDN),
- eigene Rufnummer bzw. MAC-Adresse, soweit diese übermittelt wird.

[22] https://www.dfn.de/dienstleistungen/dfnroaming/
[23] https://www.eduroam.org/

Das WWU-CERT nutzt diese Daten, um Missbrauchsfälle bearbeiten zu können (siehe§ 100 TKG).

Zu Abrechnungszwecken (Accounting) werden die Daten in einer Form gespeichert, welche die zurückliegen-den drei Kalendermonate komplett erfasst (siehe § 97 TKG). Dies betrifft sämtliche Einwahldienste. Die Sitzungen einzelner Nutzer sind zu erkennen. Aufgezeichnete werden die gleichen Daten wie sie bei der Authentifizierung anfallen.

Einwahlrouter

Logfiles: Protokollierung von Einwahlsitzungen einzelner Nutzer (der Informationsgehalt ist weniger umfang-reich als bei den Radius-Servern), automatisches Überschreiben alter Daten nach typischerweise max. fünf Tagen. Erfasste Daten:

- Nutzerkennung,
- Sitzungsbeginn und Sitzungsende

DHCP-Server (Dynamic Host Configuration Protocol)

Die DHCP Server dienen der Zuordnung von IP-Adressen. Logfiles: Protokollierung des Neustarts von PCs an Festanschlüssen, automatisches Überschreiben alter Daten nach typischerweise max. zwei Tagen.

Erfasste Daten:

- Zeitpunkt, seit dem die IP-Adresse eines Rechners am Netz betrieben wird,
- IP-Adresse und (MAC)Adresse der Netzwerkkarte

Bei DHCP kommt kein unmittelbarer Personenbezug zustande.

WINS-Server (Windows Internet Name Service)

Zuordnung von IP-Adressen zu Computer-Namen zur vereinfachten Ansprache der Rechner. Logfiles: Protokollierung von Nutzeraktivitäten durch Anmeldung von PCs und Nutzerkennungen beim WINS-Server bei PC-Neustart und später in regelmäßigen Abständen, mehrfaches automatisches Überschreiben alter Daten inner-halb eines Tages.

Erfasste Daten:

- IP-Adresse,
- Computer-Name,
- Zeitpunkt der Anmeldung durch Login und Benutzerkennung.

Netzwerkdatenbank

Die Netzwerkdatenbank ist eine umfassende Datenbank für alle administrativen Aufgaben des Netzbetriebes. Sie enthält u. a. Namen der technisch und leitend (technisch/juristisch) für die Rechner verantwortlichen Personen, deren E-Mail-Adressen, Anschriften und Telefonnummern. Die genannten Personen können diverse Angaben in der Datenbank ändern. Sie können auch Dritten erlauben, derartige Änderungen vorzunehmen. Die durchgeführten Änderungen werden protokolliert und archiviert, da für den Netzbetrieb relevante Daten verändert werden. Der Nutzer wird bei der Anmeldung auf die Protokollierung hingewiesen.

Unix- / Linux-Server

Log-Dateien/-Files

Log-Dateien (sog. Logs) der Unix-Server werden im Rotationsverfahren betrieben. Ist die Kapazität einer Log-Datei erreicht, so wird eine zweite begonnen usw. Sobald es vier Generationen einer Datei gibt, wird die erste überschrieben. Einstellen kann man dabei die Größe der Log-Datei und die Anzahl der Generationen. In der Regel enthalten dieses Logs keine personenbezogenen Daten. Sie dienen im Fehlerfall der Analyse. Ausnahmen sind:

E-Mail-Logs

Die E-Mail-Log-Dateien werden täglich ausgewertet und als statistische Summen abgelegt. Rückschlüsse auf Einzelpersonen sind nicht möglich, sondern es sind lediglich Aussagen der Form möglich wie: Nutzer des Fachbereiches Chemie verursachten 25 % der POP3-Anfragen.

perMail-Logs

In den Log Dateien der Webmailanwendung perMail sind Nutzerkennungen grundsätzlich durch MD5-Hashes unkenntlich gemacht. Es sind nur noch statistische Auswertungen möglich.

Accounting

Accounting-Daten werden lediglich mit dem Ziel gesammelt, die durchschnittlichen Server-Auslastungen zu messen und die prozentuale Nutzung durch die Fachbereiche zu ermitteln. Derzeit werden Accounting-

Daten dieser Art ausschließlich für den Parallelrechner[24] gesammelt. Die Anonymisierung der personenbezogenen Inhalte erfolgt einmal im Monat. Zu den erfassten Daten zählen u. a. Benutzerkennung, verwendete Pro-gramme und Verbrauch an Ressourcen.

Nutzerdatenbank-WWUBEN

Daten, die im Rahmen der WWUBEN erfasst wurden, werden dauerhaft gespeichert. Aus ihnen werden Account-Namen generiert. Aus dieser zentralen Datenbank werden die notwendigen Nutzerdaten zum Betrieb anderer Server wie Active Directory Service (ADS-) und Radius-Server oder Server in den Fachbereichen abgeleitet und verteilt. Für Studierende erfolgt ein Abgleich mit dem Studierendensekretariat. In Zusammenarbeit mit der Universitätsverwaltung sind sie die Basis für Abrechnungen im Print & Pay-Projekt.

Web-Dienste

Die hintere vierte Ziffer der IP-Adressen wird bei der nächtlichen Log-Datei-Rotation durch einen Stern ersetzt und die Zugriffe werden somit anonymisiert (Beispiel: 128.176.184.*). Da zwischen Zugriffen durch Proxy-Server und durch Endnutzer unterschieden werden muss, ist dies der frühestmögliche Zeitpunkt.

Zu den erfassten Daten zählen:

- IP-Adresse,
- Datenvolumen,
- Häufigkeit der Nutzung.

Windows-Systeme

Auf jedem Windows-Server und auf manchen Windows-Clients werden Ereignisse für Login und Zugriffsversuche (Nutzerkennung des Zugreifenden und Identifikation seines Rechners) grundsätzlich über Event-Logger gespeichert. Daneben gibt es diverse Protokollierungen mit Aufzeichnung der Rechnerkennung und des Rechnernamens, z. B. Firewall-Aktivitäten. Diese Daten dienen im Fehlerfall der Diagnose. Diese Daten wer-den im Rotationsverfahren regelmäßig überschrieben. Je nach Aktivitäten – und damit abhängig von der Anzahl der Vorgänge – können diese Überschreibungen nach drei Tagen oder erst nach drei Monaten erfolgen. Eine Einstellung auf eine feste Zeitdauer zum Überschreiben wäre zwar möglich, ist aber aus betrieblichen Gründen nicht akzeptabel.

Zur Steuerung der betrieblichen Abläufe wird darüber hinaus das Active Directory Service (ADS) der Firma Microsoft standardmäßig eingesetzt.

Backup und Archivierung

Im Rahmen der normalen Datensicherung (Backup) werden alle oben genannten Daten in Form einer Sicherheitskopie auf dem Datensicherungsserver aufbewahrt. Diese Backup-Daten werden spätestens 100 Tage nach dem Löschen der entsprechenden Originaldatei gelöscht. Die Backup-Organisation (Wiederauffinden verlorengegangener Daten) erfolgt über den Namen des sichernden Rechners.

Archiviert werden diese Daten solange nicht, bis die personenbezogenen Daten anonymisiert sind.

Zur Behandlung konkreter Missbrauchsfälle oder zur Klärung betrieblicher Probleme wird notwendigerweise auf Daten aus den oben genannten Segmenten zugegriffen.

Das Backup- und Archivsystem protokolliert für Accounting- und Statistikzwecke die Nutzung des Systems. Für jede Backup- oder Archivsitzung werden die Zeit, der Umfang der übertragenen Daten und der ausführende Account aufgezeichnet. Diese Daten werden zum Jahresende anonymisiert.

Behandlung von mit Viren infizierten E-Mails

Der Umgang mit von Viren infizierten E-Mails wird in Anlehnung an die Betriebsregelung vom 14. November 2002[25] geregelt.

Auf den E-Mail-Servern des Zentrums für Informationsverarbeitung (ZIV) werden alle aus- und eingehenden E-Mails, die von der oder an die Domain „uni-muenster.de“ bzw. „wwu.de“ gesendet werden, mit Hilfe eines Virenscanners auf einen möglichen Virenbefall untersucht. Ebenso werden Sub-Domains, die ihre E-Mails über Server des ZIV empfangen, in diese Untersuchung einbezogen. Der E-Mail-Verkehr an andere Sub-Domains wird i. A. nicht untersucht.

Bei der Untersuchung wird folgendermaßen verfahren:

---

[24] https://www.uni-muenster.de/ZIV/Technik/Server/HPC.html
[25] https://www.uni-muenster.de/imperia/md/content/ziv/pdf/intern/behandlung_virenverseuchter_e-mails.pdf (Intranet)

- Viren in E-Mails werden gelöscht. Der Adressat wird hierüber via E-Mail informiert. Zugleich werden ihm die im Rahmen des Virenscans angefallenen Informationen wie beispielsweise Adressen, Scan-Protokolle und Virustyp(en) mitgeteilt.
- Alternativ hat jeder Nutzer die Möglichkeit, durch einen Virus infizierte E-Mails ohne weitere Benachrichtigung unverzüglich löschen zu lassen. Die Genehmigung hierzu kann über das Portal MeinZIV erteilt und jederzeit widerrufen werden.

In einem detaillierten Schriftverkehr mit der Landesbeauftragten für Datenschutz und Informationsfreiheit in NRW wurde das o. g. Verfahren geprüft und genehmigt (Dokumentation im Intranet):

- Rechtsgrundlage für Viren- und Spam-Schutz[26]

Betrieb von E-Mail-Servern

Um Bedrohungen und Belästigungen durch E-Mails (etwa Spam- und Virenversand) entgegen zu wirken, ist der E-Mail-Verkehr im Netzwerk der Universität reglementiert.

Der eingehende E-Mail-Verkehr ist für nicht angemeldete Server netzwerkseitig blockiert. Nur durch vorhergehende Anmeldung eines E-Mail-Servers kann und wird dieser Traffic für die entsprechenden E-Mail-Server freigeschaltet werden.

Der Großteil aller E-Mails wird zentral vom ZIV verwaltet. Dies betrifft den eingehenden sowie den ausgehen-den E-Mail-Verkehr. Es steht weiteren Gruppen – etwa IVVen oder einzelnen Instituten – frei, selbst E-Mail-Server zu betreiben, allerdings müssen diese beim ZIV angemeldet werden.

Für ausgehenden E-Mail-Verkehr bestehen derzeit keine Beschränkungen.

Die detaillierten Rahmenbedingungen für den Einsatz von E-Mail-Servern sind in einer entsprechenden E-Mail-Server-Betriebsordnung geregelt:

- Regelungen zum Betrieb vom E-Mail-Servern im LAN der WWU[27]

Betrieb von Intrusion Prevention Systemen (IPS)

Im Netzwerk der Universität Münster ist ein Intrusion Prevention System implementiert, das frühzeitig Angriffe über das Netzwerk erkennen und direkt unterbinden soll. Durch diese Systeme sollen Angriffe durch Würmer, Viren, Trojaner, Denial-of-Service-Attacken usw., die zu erheblichen Störungen der IT der Universität, zu Schädigungen der Rechnerkonfigurationen sowie zu Datenverfälschungen und -verlusten führen können, abgewehrt werden. Die Abwehr dieser Angriffe erfolgt durch definierte Signaturen, also bekannte Angriffsmuster, aber auch durch Analyse des Datenverkehrs und hieraus abgeleiteter Verhaltensmuster schädlicher Angriffe.

Im Datennetz der Universität Münster sind netzwerkbasierte IPS im Einsatz, die an genau ausgewählten Stellen im Netzwerk integriert werden.

Das ZIV betreibt mehrere Intrusion Prevention Systeme, deren Betriebsrahmenbedingungen im Intranet dokumentiert sind:

- Hinweise zu Intrusion Prevention Systemen an Hochschulen[28]

[26] https://www.uni-muenster.de/imperia/md/content/ziv/pdf/intern/rechtsgrundlage_f__r_viren-_und_spam-schutz.pdf (Intranet)
[27] https://www.uni-muenster.de/imperia/md/content/ziv/pdf/betrieb_e-mail-server.pdf
[28] https://www.uni-muenster.de/imperia/md/content/ziv/pdf/intern/intrusionprevention1v2.pdf (Intranet)

Sicherheitskonzepte

In diesem Kapitel werden Konzepte für unterschiedliche IV-Bereiche vorgestellt, die auf Probleme bei der Nutzung von IV-Systemen aufmerksam machen und damit die IV-Sicherheit verbessern sollen.

Regeln für den administrativen Arbeitsplatz

Der sichere Administrator-Arbeitsplatz

Der Rechner, über den ein Administrator seine Server oder Netzkomponenten administriert, verdient besondere Beachtung und Sicherung. Eine kompromittierte Admin-Workstation, in der ein Angreifer die Tastatureingaben mitschneidet oder den privaten Teil von Zertifikaten ausspäht, kann der Anfang einer Sicherheitskatastrophe sein.

Das Passwort-Problem

Ein Administrator ist häufig für zahlreiche Server, Dienste oder Netzkomponenten zuständig. Im Laufe eines Arbeitstages (oder einer Arbeitswoche) steigt die Anzahl der gleichzeitig offenen Verbindungen zu den administrativen Schnittstellen der Systeme, weil es bequemer ist, eine bestehende Verbindung für ein zweites Problem zu nutzen, als nach jeder Aktion die Verbindung zu schließen und bei Bedarf wieder aufzubauen.

Eine unbeaufsichtigte Admin-Workstation stellt daher ein Problem dar. Administratoren sollten den Zugriff auf ihre Workstation vor jedem Verlassen ihres Büros sperren oder sich vom Betriebssystem abmelden. Das Büro zu verschließen allein reicht nicht, denn der Personenkreis, der legal Zugang zu einem Büro hat, ist in der Regel nicht überschaubar.

Administratoren geben häufiger Passwörter ein als andere, und administrative Passwörter sind in der Regel kompliziert aufgebaut, sodass die ständige Eingabe lästig fällt. Die Verwendung von Zertifikaten zur Vermeidung von Passworteingaben liegt hier nahe und ist sogar sicherer, solange sichergestellt wird, dass die Zertifikate nicht ausgespäht und von Unbefugten verwendet werden können.

Zertifikate gehören folglich auf Speichermedien, die auch mit Systemrechten nicht ohne eine weitere Hürde gelesen werden können. Smart-Cards oder eToken, die eine PIN-Eingabe erfordern, oder Krypto-Dateisysteme, deren Zugriff eine zusätzliche Passworteingabe benötigt, sind geeignete Kandidaten. Solange die PIN- oder Passwort-Eingabe über die System-Tastatur erfolgt, bleibt jedoch ein Restrisiko bestehen, so können bspw. die Tastatureingaben aufgezeichnet werden.

System- und Netz-Anforderungen

Es muss sehr unwahrscheinlich sein, dass die Workstation kompromittiert wird. Dazu sollte die installierte Software auf aktuellem Stand sein und bleiben. Weiterhin sollte die Workstation von außen über das Netz nicht erreichbar sein. Besonders wichtig ist es, keine Dialogdienste anzubieten. Das schließt den Remote Desktop unter Windows oder die ssh-Kommandozeile unter Linux ausdrücklich ein. Kann die Workstation nur noch am Aufstellungsort genutzt werden, ist das Restrisiko ebenso groß wie es wahrscheinlich ist, dass ein Angreifer die Workstation und den eToken oder die Smart-Card gleichzeitig physisch in Besitz nehmen kann und die PIN kennt. Ferner sollte ein Administrator auf der Workstation ausschließlich einen nicht-privilegierten Account nutzen.

Admin-Workstations gehören in ein spezielles Administrations-VLAN, dem nur Workstations angehören dürfen, die im Sinne dieses Dokuments sicher sind. Die administrativen Zugänge der Server und Komponenten werden so eingestellt, dass sie nur noch Verbindungen aus diesem VLAN zulassen.

Die Firewall zum Schutz der Admin-Workstation sollte netzseitig umgesetzt werden. Zusätzlich eingesetzte Intrusion Prevention und Detection Systeme ergänzen die lokalen Virenscanner für den Fall, dass ein erfolgreicher Angriff lokale Sicherheitsmaßnahmen ganz oder teilweise außer Kraft setzt.

Kompromisse

Fehleranzeigen kommen häufig über E-Mail. Aktuelle Herstellerinformationen oder Fehlerbeschreibungen werden im Web gesucht. In der Praxis werden häufig Textstellen aus einem Fenster in ein anderes übertragen (copy & paste), was sowohl bequem ist als auch vor Schreibfehlern schützt. Der Administrator braucht also Zugriff auf das Web und seine E-Mails, was die Integrität der Workstation prinzipiell gefährdet. Die üblichen Maßnahmen – aktueller Browser, E-Mail-Programm und Virenscanner; Arbeiten ohne administrative Rechte – machen dieses Risiko kalkulierbar.

Nebenwirkungen

Mitarbeiter der System- und Netzwerkgruppe haben nicht nur administrative Aufgaben. Dazu gehören der Aufbau und Test neuer Server oder Dienste. Diese Aufgaben können nicht mehr auf der Admin-Workstation wahrgenommen werden, sondern müssen auf Zweit-Rechnern oder virtuellen Servern erfolgen. Neben ausreichender Hardware ist hier die Selbstdisziplin der Administratoren gefordert.

Häusliche Arbeitsplätze

Administratoren mit Rufbereitschaft nehmen eine erste Fehleranalyse von zu Hause aus vor. Manchmal erübrigt sich damit die zeitkostende Fahrt zum Arbeitsplatz. Nun kann man häusliche Rechner, insbesondere wenn sie von Familienmitgliedern mitgenutzt werden, im oben definierten Sinne nicht als sicher bezeichnen.

Wenn man nicht auf die mögliche Zeitersparnis bei der Problembehebung verzichten will, und gleichzeitig einen hohen Sicherheitsstand erhalten will, könnte man dies beispielsweise durch den Einsatz von einfach ausgestatteten Admin-Notebooks erreichen, die so installiert sind, dass sie ausschließlich für den Remote Zugang genützt werden können. Die Einwahl würde dann direkt in das Administrations-VLAN erfolgen und die administrativen Schnittstellen wären von zu Hause aus nutzbar. Ebenso denkbar ist die Nutzung von entsprechend abgesicherten virtuellen Desktops.

Regelmäßige Datensicherung relevanter Daten

Bei der Planung von Maßnahmen zur Sicherung von Daten gilt es, unterschiedlichste Gefahrenquellen zu berücksichtigen: Physische Störfälle, wie Gerätedefekte oder Brände, der Einsatz fehlerhafter Programme oder gezielter Schadsoftware, Fehlbedienung oder Sabotage können zu Datenverlusten, in einigen Fällen auch zur ungewollten Veränderung von Daten führen. In vielen dieser Fälle helfen hardwarenahe Maßnahmen zur Erhöhung der Redundanz (z. B. RAID) oder zur Synchronisation der Daten nicht weiter. Es ist daher wichtig, stets über Sicherungskopien (Backups) der Daten zu verfügen. Die Kopien müssen vor dem Verlust oder der ungewollten Veränderung erstellt worden sein. Das kann einige Tage zurück liegen.

Zur gelegentlichen oder regelmäßigen Durchführung von Backups wird die Tivoli Storage Manager (TSM; siehe Abschnitt „Tivoli Storage Manager (TSM)“) Software genutzt. Das ZIV bietet zu diesem Zweck mehrere TSM-Server an, die Backup- und (in eingeschränktem Maße) Archivdaten entgegennehmen. Die Daten werden von den TSM-Servern zunächst auf Magnetplatten zwischengespeichert, danach auf Magnetbandkassetten abgelegt. Alle TSM-Server benutzen dazu dasselbe Kassettenarchivsystem, das die Laufwerke und Magnetbandkassetten enthält.

Netzseitige Sicherheitsmaßnahmen

Das Zentrum für Informationsverarbeitung hat im Auftrag der Universität und des Universitätsklinikums Münster seine Bemühungen intensiviert, durch netzseitige Maßnahmen die Gefährdung der Informationsverarbeitung, ihrer Verarbeitungsprozesse, IT-Systeme und Daten zu reduzieren und damit die direkten und indirekten Aufwendungen für eingetretene Schäden zu reduzieren. Konzeptionell sind diese Maßnahmen selbstverständlich nur ein Teil der Gesamtmaßnahmen – Maßnahmen auf den IT-Endgeräten selbst, organisatorische Maßnahmen, Ausbildungsmaßnahmen usw. wird in der Gesamtheit ein noch größeres Gewicht zugesprochen. Netzseitige Maßnahmen erlauben jedoch in wichtigen Fällen und gezielt für wichtige Bereiche, das Gefährdungspotential auch dann zu begrenzen, wenn lokale, organisatorische und sonstige Maßnahmen nicht aus-reichend umgesetzt werden konnten. In bestimmten Fällen können auch nur netzseitige Maßnahmen Schutz bieten, z. B. zur Abwehr bestimmter Denial-of-Service (DoS)-Angriffe.

Der Grundgedanke einer netzseitigen Sicherheitsmaßnahme ist die Einbettung von Sicherheitsfunktionen in ein strukturiertes Netz. Zu den Grundelementen zählen:

- ein strukturiertes Netz mit Netzzonen (siehe Anhang H | Das Konzept der Netzstrukturierung), die den Kommunikations- und Sicherheitsbedürfnissen der Teilnehmersysteme mit ihren Anwendungen und Daten entsprechen.
- Hierarchisierung der Netzzonen: Erlaubt übergeordnete Netzzonen – auch mehrstufig – zu bilden. Netzzonen können so entsprechend den Bedürfnissen ganzheitlich gegenüber anderen übergeordneten Netzzonen sicherheitstechnisch definiert und betrieben werden. Eine solche Strukturierung entspricht den vorhandenen IV-Strukturen, die häufig auch vielstufig ausgeprägt sind.
- die Einbettung von Sicherheitsfunktionen in das Netz: Insbesondere in großen bis sehr großen Netzen ist eine einzige Firewall am Netzperimeter als alleinige netzseitige Sicherheitsmaßnahme unzureichend. Vielmehr sind alle netzseitigen Sicherheitsmaßnahmen möglichst überall dort in das Netz zu integrieren, wo eine sicherheitstechnische Abgrenzung eines informationsverarbeitenden Bereiches gegenüber anderen Bereichen erwünscht ist. Damit werden Verbände von Netzzonen aufgebaut, die nicht nur nach

außen geschützt sind, sondern für die auch in über-schaubaren Bereichen innerhalb eines Zonenverbundes gleichermaßen Sicherheitsfunktionen bereitgestellt werden können.

Digitale Zertifikate

Zertifikate

Bei der Kommunikation im Netzwerk, ist es oft unerlässlich, der Gegenseite zuverlässig vertrauen zu können. Hierfür werden in der Regel digitale Zertifikate verwendet, mit deren Hilfe ein Kommunikationspartner (bspw. der Absender einer E-Mail oder die Webseite des Onlinebanking-Dienstes) eindeutig identifiziert werden kann. Solche Zertifikate kommen in der Universität sowohl zur Identifikation von Diensten, aber auch von Personen zum Einsatz. Wo immer möglich werden Zugänge zu allen Serverdiensten auch über einen sicheren SSL/TLS-Kanal angeboten. Auch diese verschlüsselten Verbindungen benutzen den Zertifikatsmechanismus zum Aufbau der Verbindung. Persönliche Zertifikate werden als digitale Unterschrift als S/MIME-Signatur in E-Mails verwendet, aber auch, um sich gelegentlich gegenüber einem Serverdienst zu authentifizieren.

Public-Key-Infrastruktur (PKI)

Wenn es allein um den Austausch von Daten über eine verschlüsselte Verbindung geht, d. h. das Mithören der Daten unterbunden werden soll, reicht ein einfaches selbst generiertes Zertifikat. Hierbei wird aber eine wichtige Eigenschaft von Zertifikaten nicht benutzt: Die Identifikation des Kommunikationspartners kann durch solche Zertifikate nicht sichergestellt werden. Hierzu bedarf es eines vertrauenswürdigen Dritten, der die Angaben im Zertifikat (bspw. Rechnernamen oder E-Mail-Adresse) bestätigt. Es wird hierfür eine vertrauens-würdige Public-Key-Infrastruktur (PKI) benötigt. Diese Rolle übernimmt an der Universität Münster die WWUCA (siehe Abschnitt „Zertifizierungsstelle der WWU“), die zentral durch das ZIV betrieben wird. Sie kann bspw. persönliche Zertifikate nach Vorlage des Personalausweises zertifizieren und stellt damit die Identität des Zertifikatinhabers sicher.

Im Windows-Umfeld können Zertifikate zum Anmelden in der Domäne genutzt werden. Hierzu kann nach der Anmeldung über eine spezielle Webseite der öffentliche Teil des Zertifikats im Active Directory abgelegt und der Nutzerkennung zugeordnet werden. Das Active Directory übernimmt hierbei nun die Stelle der PKI.

Smartcards und eTokens

Digitale Zertifikate haben neben einem öffentlichen auch immer einen privaten Schlüssel. Um einen Identität-Diebstahl zu verhindern, muss dieser private Teil vor dem Zugriff Dritter geschützt werden.

Eine sehr gute Methode, um den privaten Schlüssel zu sichern, ist die Verwendung von Smartcards oder eTokens. Diese kommen z. T. in der Systemadministration zum Einsatz. Ist dies nicht möglich, müssen besondere Vorsorgemaßnahmen getroffen werden. Hier ist es hilfreich, wenn private Schlüssel nur in verschlüsselten Dateisystemen vorgehalten werden. Dies geschieht z. T. bspw. bei SSH- oder GPG/PGP-Keys.

Richtlinie zur Auslagerung von Daten in Cloudspeicherdiensten

2013 wurde eine Cloud-Richtlinie[29] beschlossen, die die Auslagerung von Daten in, und die Benutzung von Cloud-Diensten handhabt. Die Richtlinie ist im Anhang I | Cloud-Richtlinie zu finden.

Für sciebo[30], den Cloudspeicherdienst der NRW-Hochschulen, unter der Konsortialführung der WWU, gilt eine angepasste Empfehlung: Empfehlungen für die Verwendung des Cloudspeicherdienstes „sciebo“[31] (siehe Anhang J | Empfehlungen für die Verwendung des Cloudspeicherdienstes „sciebo“).

Online-Security-Audit „ISidoR“ an der Universität Münster

Zielsetzung

Beim Online-Security-Audit handelt es sich um einen Fragenkatalog, der vom Betreiber eines IT-Endsystems fordert, gewisse Fragestellungen bezüglich System-Verfügbarkeit sowie Daten- Vertraulichkeit und -Integrität zu beantworten. Die gestellten Fragen sind dabei angelehnt an die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Empfehlungen zum IT-Grundschutz.

Das Ziel des Security-Audits ist die Feststellung

[29] https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2015/ausgabe02/beitrag03.pdf
[30] https://www.sciebo.de/
[31] https://www.uni-muenster.de/imperia/md/content/ziv/pdf/sicherheit/sciebo-empfehlungen_zum_datenschutz.pdf

› des Schutzbedarfs aller untersuchten IT-Systeme,
› der vorhandenen Sicherheitsvorkehrungen und
› der Sicherheitsdefizite.

Übergeordnetes Ziel ist es, Grundlagen für die Einführung weitergehender Sicherheitsmaßnahmen zu ermitteln und dadurch eine Anhebung des IV-Sicherheitsniveaus zu bewirken.

Weiteres Teilziel ist es, technisch Verantwortlichen und Administratoren bereits bei der Anmeldung von IT-Systemen für die Thematik der Sicherheit zu sensibilisieren. Bereits beim Durchlesen der Antworten wird deutlich, welche Möglichkeiten der Absicherung bestehen und welchem Sicherheitsstand der Ist-Zustand entspricht. Über die Darstellung der Konsequenzen, die eine Verletzung der Integrität, Vertraulichkeit oder Verfügbarkeit der Daten und Dienste nach sich ziehen würde, wird ihnen die Notwendigkeit von Sicherheitsvorkehrungen vor Augen geführt und an Beispielen verdeutlicht.

Vorgehensweise

Das Security-Audit wird mittels Webseiten, die Fragenkataloge aufzeigen, durchgeführt. Zu jeder Frage werden fünf Antworten zur Auswahl angeboten. Die Nutzerin oder der Nutzer wählt die Antwort, die am ehesten den Ist-Zustand beschreibt. Die Antworten werden in einer Datenbank vorgehalten, damit langfristige Entwicklungen bzgl. der IV-Sicherheit zu verfolgen sind.

Ermittlung des Schutzbedarfs

Für jedes Datenendgerät wird zunächst der Schutzbedarf ermittelt, d. h. die Wertigkeit und Wichtigkeit der Daten und Dienste, die über das Datenendgerät erreichbar sind, werden festgestellt. Dabei wird zwischen Integrität und Vertraulichkeit der Daten sowie Verfügbarkeit der Daten und Dienste unterschieden.

Nach der Auswertung der Antworten steht für das Datenendgerät der Schutzbedarf bzgl. der ermittelten Informationen fest und es wird zusammenfassend einer Schutzbedarfskategorie zugeordnet.

Ermittlung der Sicherheitsvorkehrungen

In Abhängigkeit vom ermittelten Schutzbedarf werden nun automatisch Fragenkataloge zusammengestellt, die die Sicherheitsvorkehrungen für das Datenendgerät und dessen Umfeld ermitteln. Je höher der Schutzbedarf eines Datenendgerätes ist, umso ausführlichere Fragen werden gestellt, um den Status der Sicherheits-vorkehrungen festzustellen.

Fortlaufende Bestandsaufnahme

Die Sicherheit in der Informationsverarbeitung (IV) ist kein statischer Faktor, sondern unterliegt einer ständigen Veränderung. Alle mit der IV zusammenhängenden Komponenten werden immer komplexer und damit häufig auch immer anfälliger. Außerdem verbessern auch Angreifer permanent ihr Wissen und erarbeiten neue Methoden, um z. B. in IV-Systeme einzudringen. Es ist daher unumgänglich, ein Security-Audit stetig zu aktualisieren, um den aktuellen Stand zu erfassen.

In diesem Sinne ist das vorgestellte Online-Security-Audit-Verfahren auf Nachhaltigkeit ausgelegt, indem neue Fragenversionen erstellt werden können, um die Fragenkataloge zu aktualisieren und der jeweiligen Entwicklung anzupassen. Dabei bleiben ältere Fragenversionen bestehen, um Tendenzen aufzeigen zu können.

ISidoR

Die IV-Gremien der Universität Münster haben die Durchführung eines Security-Audits befürwortet, das ZIV hat dazu ein entsprechendes interaktives Programm entwickelt und das Security-Audit-Verfahren unter dem Namen ISidoR (*Informationssicherheit ist die oberste Regel*) eingeführt.

Da das IV-Umfeld an der Universität nicht unmittelbar mit dem von Industriebetrieben, sonstigen Unternehmen oder Behörden zu vergleichen ist, konnte nicht auf kommerzielle Produkte zurückgegriffen werden. Vielmehr wurde ein eigenes Programm durch das ZIV entwickelt, um diesen Besonderheiten der Universität gerecht zu werden. Außerdem sind viele Informationen bzgl. des Netzes der Universität (z. B. geräteseitige Netzanschlüsse, Datenendgeräte und deren Standorte) in der bestehenden Netzdatenbank LANbase bereits vorgehalten und das Security-Audit konnte so auf den vorhandenen Informationen aufsetzen. In Anhang F | Security Audit ISidoR wird ISidoR detailliert vorgestellt.

Sicherheitsbegehungen

In den Statuten des IV-Systems der Universität Münster (siehe Anhang B | Regelungen zur IV-Sicherheit in der Universität Münster) ist als eine der Aufgaben des IV-Sicherheitsteams der WWU die Überwachung der Umsetzung von Sicherheitsstandards festgelegt. Dazu können in den Einrichtungen der Universität Sicherheitsüberprüfungen vorgenommen werden. Insbesondere soll durch Sicherheitsbegehungen vor Ort, bei-

spielsweise in den IVVen, überprüft werden, ob die Eintragungen im Rahmen der Schutzbedarfsermittlung mit Hilfe des Security Audits ISidoR den örtlichen Begebenheiten entsprechen. Ferner kann sich bei den durchzuführenden Begehungen herausstellen, dass manche Fragestellungen noch nicht ausreichend im Security Audit behandelt wurden und eine Nachbesserung benötigt wird.

In der Sitzung der IV-Kommission vom 02.07.2008 wurde beschlossen, dass Sicherheitsbegehungen ab dem 1. Quartal 2009 stattfinden sollen.[32]

Die Sicherheitsbegehungen werden durchgeführt mit

- Vertretungen der zuständigen IVVen,
- Mitglied(ern) des IV-Sicherheitsteams,
- Vertretungen der lokal für die Endgeräte (Arbeitsplatzrechner, Server etc.) zuständigen Technisch und Leitend Verantwortlichen und
- Mitarbeitern des ZIV
    - der Abteilung Kommunikationssysteme in Verantwortung für (Netz-) Infrastruktur und zentrale IT-Sicherheitsfragen sowie
    - der Abteilung Systembetrieb in Verantwortung für zentrale Server-Infrastrukturen und Endsystem-Sicherheit.

Die Mitwirkung der Personalvertretungen ist wünschenswert oder ggf. erforderlich (kongruent zu den Sicherheitsbegehungen der üblichen Art in den Gebäuden bzgl. des Brandschutzes und dergleichen).

Gegenstände der Sicherheitsüberprüfungen sind

- systematisch, d. h. regelmäßig und nach Plan
    - zentrale Serverstandorte in ZIV, ITZ[33] und vergleichbaren Einrichtungen
    - Serverstandorte von IVVen
    - zentrale Standorte der Netztechnik (LAN- bzw. TK-Verteilungen)
- stichpunktartig überall, jedoch mit besonderer Berücksichtigung von
    - lokalen Servern in Fachbereichen, Instituten, Kliniken oder Abteilungen
    - Computer Labs (CLABs)
    - dezentrale Standorte der Netztechnik (LAN- bzw. TK-Verteilungen)
- bedarfsweise ausgewählte Bereiche mit besonders hohem Sicherheitsbedarf, ggf. auch auf Anforderung aus diesen Bereichen (z. B. Personaldezernate, Prüfungsämter, medizinische Systeme)

Katastrophenfälle

Für den Bereich ZIV existiert ein Alarmierungskonzept[34]. Detailliertere Lösungen zu speziellen Katastrophen und Notfällen sind in Arbeit. So existiert z. B. bereits eine Alarmierungsplan für die wichtigsten Systemdienste sowie eine mit dem UKM abgestimmte Verfahrensanweisung zur Kommunikation im Störungsfall.

[32] https://www.uni-muenster.de/imperia/md/content/ziv/pdf/intern/auszug_iv-k_top_4_02.07.2008.pdf (Intranet)
[33] IT-Zentrum Forschung und Lehre, http://campus.uni-muenster.de/68.html
[34] Dieses Konzept steht zurzeit nicht elektronisch zur Verfügung und wird in einer Aktualisierung nachgetragen.

Absicherung von IV-Systemen und -Diensten

Dieses Kapitel stellt praktische Konzepte vor, wie das ZIV IV-Systeme und -Dienste betreibt. Dabei wird insbesondere auf die Absicherung bzgl. Ausfällen eingegangen.

Webserverpark

Das zentrale Webangebot der Universität Münster verteilt sich auf mehrere Rechner-Systeme mit unterschiedlichen Aufgaben und Funktionen, die zu dem sog. Webserverpark zusammengefasst sind. Um höchste Ausfallsicherheit zu gewährleisten, teilt sich der Webservicedienst in mehrere Komponenten auf, die zusätzlich alle redundant ausgelegt sind:

Die Frontend-Server nehmen alle Anfragen an die zentrale Adresse www.uni-muenster.de und einigen anderen Adressen aus dem Internet entgegen. Ein vorgeschaltetes Lastverteilungssystem verteilt ankommende Anfragen auf die Frontend-Server und sorgt dafür, dass nur aktive Frontend-Server bei der Verteilung berücksichtigt werden. Sofern Anfragen von den Frontend-Servern nicht unmittelbar mit einem Verweis auf ein anderes Angebot beantwortet werden können, arbeiten diese als Reverse-Proxy-Server und verteilen die Anfragen auf mehrere Backend-Server. Erst die Backend-Server leisten die Hauptarbeit und liefern die Webseitenaufrufe an den Anfragenden aus.

Alle Backend-Server greifen auf ein gemeinsames Dateisystem (General Parallel File System, GPFS) zu, auf dem alle WWW-Daten vorgehalten werden. Drei File-Server sorgen ausfallsicher für den Zugriff auf das GPFS-Dateisystem. Das GPFS-Dateisystem wiederum befindet sich in einem in allen Teilen redundant aufgebauten Storage Area Network (SAN) von dem täglich Backups erzeugt werden. Zusätzlich werden alle Daten auf spezielle Notfallsystemen an einem räumlich entfernten Standort gespiegelt, um im Falle größerer Katastrophen zumindest einen eingeschränkten Betrieb zu ermöglichen.

Bei den verwendeten Servern handelt es sich z. T. um reale Hardware, z. T. um virtuelle Maschinen aus dem ausfallsicheren VMware ESX-Server-Park. Je nach Bedarf kann der Webserverpark um beliebige Komponenten (Dispatcher, Frontend-Webserver, Backend-Webserver, Speicher, CPU etc.) dynamisch erweitert werden. Ausgefallene Systeme werden so schnell ersetzt und Leistungsengpässe können leicht kompensiert werden.

Die Daten, die sich auf dem GPFS-Dateisystem befinden und letztendlich die Webseiten der Universität dar-stellen, werden entweder durch das Content Management System „Imperia“ eingepflegt oder individuell durch eine Vielzahl von Infoanbietern. Für die manuelle Pflege ihres Internetauftrittes steht den Infoanbietern ein spezieller Upload-Server zur Verfügung. Auf den Upload-Server kann per SSH/SCP/SFTP zugegriffen wer-den. Zur Anmeldung wird zwingend die Public-Key-Authentifizierung verlangt, eine Anmeldung nur mit der Nutzerkennung und dem Passwort ist nicht möglich. Zusätzlich wird mittels Samba für Nutzer aus der Windows-Domäne „UNI-MUENSTER“ ein entsprechendes Netzwerklaufwerk angeboten.

Jeder Informationsanbieter erhält seinen eigenen, unter einer speziell dafür eingerichteten Nutzerkennung laufenden virtuellen Server auf den Backend-Servern. Die Frontend-Server sorgen für die korrekte Abbildung der Webadressen auf die virtuellen Server.

Als wesentlicher Beitrag zum Thema Sicherheit werden alle Zugriffe von außen auf den Webserverpark durch restriktiv konfigurierte Paketfilter auf den verschiedenen Servern blockiert. Ausgenommen sind nur HTTP- und HTTPS-Zugriffe auf die Frontend-Server und SSH- und SMB-Zugriffe auf den Upload-Server sowie SSH-Zugriffe (von wenigen ausgewählten Admin-Systemen auf alle Server). Auch zwischen den Servern des Webserver-parks werden durch die Paketfilter nur die benötigten Zugriffe gestattet, sodass die Frontend-Server gleich-zeitig die Funktion einer Application Firewall ausüben.

Content Management System (CMS) – Imperia

Das Content-Management-System „Imperia“ (ein Produktionssystem und mehrere Testsysteme) ist als normaler Webspace im Webserverpark realisiert und profitiert daher von allen dort realisierten Schutzmechanismen gegen Zu- und Angriffe von außen. Darüber hinaus ist der Zugriff auf durch Infoanbietern (Redakteure der einzelnen Webauftritte) eingebrachte Skripte im Imperia-Webspace der Testsysteme komplett verboten, damit interne Zugriffsbeschränkungen des CMS nicht umgangen werden können. Zugriffe auf das Backend des CMS sind nur von Anschlüssen am Wissenschaftsnetz Münster und über VPN aus möglich.

Das Produktionssystem wird als eigenständiges System von der zentralen Nutzerverwaltung provisioniert. Die zentrale Passwortänderung im Nutzerportal MeinZIV überträgt geänderte Passwörter auch in die Passwortverwaltung von Imperia. Eine spezielle Gruppenstruktur (unabhängig von allen anderen Nutzergruppen) regelt die Zugriffsrechte innerhalb des Imperia-Systems.

Ein selbst entwickeltes Publikationsmodul, getrennte Nutzergruppen für jeden Infoanbieter und eine ausgefeilte Struktur aus symbolischen Links und Zugriffsrechten auf Verzeichnissen sorgen beim Freischalten von Dokumenten für sichere Zugriffsrechte. Mitglieder von Nutzergruppen mit gemischten Webspaces (teilweise mit Imperia, teilweise manuell gepflegt) können auf die über Imperia eingepflegten Dokumente über das Dateisystem nur lesend zugreifen, Mitglieder von Nutzergruppen mit reinen Imperia-Webspaces haben über-haupt keinen Zugriff auf das Dateisystem. Für jeden Infoanbieter ist ein eigener virtueller Webserver mit eigener Nutzergruppe eingerichtet. Der zentrale Webserver darf alles lesen, von Infoanbietern publizierte Skripte laufen auf dem Produktivsystem jedoch mit eingeschränkten Rechten und können nur auf Dateien des Infoanbieters zugreifen.

Jeder Informationsanbieter erhält unter Imperia einen eigenen Bereich, der über Gruppenrechte geschützt wird. Über die feste Zuordnung eines sogenannten Basispfads wird sichergestellt, dass der jeweilige Infoanbieter seine Webseiten nur auf dem virtuellen Server veröffentlichen kann, der ihm zugewiesen wurde.

E-Mail-System

Es wird empfohlen grundsätzlich das zentrale vom ZIV betriebene E-Mail-System der WWU zu nutzen. Dieses gliedert sich in drei Bereiche:

- E-Mail-Empfang
- Abruf der E-Mail durch Nutzer
- E-Mail-Versand

Aufgrund der verschiedenen Aufgaben ist die Sicherung der Systeme unterschiedlich. Allen gemeinsam ist, dass durch netzwerkseitige Filterregeln und lokale Firewalls nur die jeweils benötigten Dienste freigegeben sind.

E-Mail-Empfang

Der zentrale E-Mail-Empfang wird durch Appliances der Firma Ironport dargestellt. Diese befinden sich in speziellen VLANs welche SMTP-Zugriffe weltweit zulassen. Alle anderen Ports sind auf das jeweils notwendige Maß beschränkt. Nutzer haben keine Möglichkeit, sich an der Maschine anzumelden. Alle notwendigen Nutzerinformation (E-Mail-Adressen und -Aliase sowie die SPAM-Policies) werden aus einem speziell für das E-Mail-System eingerichteten LDAP-Server bezogen.

Auf den Appliances wird bei der Annahme von E-Mails auf das Senderbase -Reputationssystem der Firma Ironport zurückgegriffen. Dieses klassifiziert IP-Adressen anhand der von dieser Adresse versandten SPAM- und Malware-E-Mails. Falls der einliefernde Server eine entsprechend schlechte Reputation hat, wird die Verbindung noch vor der Übertragung der E-Mail mit einer Fehlermeldung abgebrochen. Bei durch die Reputation verdächtigen Servern wird nur eine begrenzte Anzahl von E-Mails pro Stunde mit einer reduzierten Anzahl an Empfängern entgegengenommen. Bei Überschreitung der Grenzwerte werden weitere E-Mails mit einer temporären Fehlermeldung abgelehnt.

Es werden nur E-Mails mit bekannten Empfängeradressen angenommen. Directory-Harvest-Attacken (d. h. das Durchprobieren vieler geratener Adressen) werden erkannt und blockiert.

Nach der Annahme von E-Mails werden diese auf Viren und SPAM geprüft. Hierfür kommt Sophos Antivirus und Ironport Antispam zum Einsatz. Erkannte Viren werden entfernt und die E-Mail mit einer Ergänzung im Subject/Betreff gekennzeichnet. Erkannte SPAM wird durch eine zusätzliche Kopfzeile markiert. Anhand der über MeinZIV einstellbaren SPAM-Policy kann jeder Nutzer individuell entscheiden ob erkannte Viren- und SPAM-E-Mails zugestellt oder ohne weitere Benachrichtigung vernichtet werden.

Die Appliances leiten die so verarbeiteten E-Mails an die Zielsysteme weiter. Diese werden beim zentralen E-Mail-System von zwei Linux-Servern, auf denen der MTA postfix läuft, gebildet. Diese nehmen E-Mails aufgrund von netzseitig vorgegebenen ACLs nur aus den VLANs der Appliances an und befinden sich in einem privaten Subnetz. Auch diese Maschinen lassen keine Nutzerinteraktion zu und sind per ssh nur aus dem Administrations-VLAN erreichbar.

Die Zielsysteme verarbeiten mögliche Weiterleitungen und stellen die E-Mails in die Postfächer auf dem dafür exklusiv bereitgestellten GPFS-Dateisystem zu. Weiterleitungen werden über einen auf den Appliances eingerichteten Relay-E-Mail-Server abgewickelt.

Abruf von E-Mails durch die Nutzer

Der E-Mail-Abruf durch die Nutzer erfolgt durch dediziert hierfür bereitgestellte Server. Auf ihre E-Mails können Nutzer nur über die Protokolle POP3 und IMAP sowie über den Webmailer perMail[35] zugreifen. Zugriff per IMAP und perMail erfolgen über SSL-verschlüsselte Zugänge. Ein Zugriff per SSH oder ähnliche Login-Methoden ist für Nutzer nicht möglich.

Die Server befinden sich in einem abgesicherten Netzbereich, der Zugriffe von außen nicht erlaubt. Der E-Mail-Abruf selbst erfolgt über zwei Dispatcher-Rechner, die nur diese drei Protokolle (POP, IMAP, perMail) an die Server weiterleiten. Administrationszugriff auf die für den E-Mail-Abruf zuständigen Server erfolgt über die Server des E-Mail-Annahmesystems. Die Dispatcherrechner sind vor unberechtigten Zugriffen durch entsprechende Konfiguration der lokalen Firewall geschützt.

Versand von E-Mails

E-Mail-Versand ist für Nutzer über drei Wege möglich: Der Versand ist über den Webmailer perMail möglich. Zum Versand über lokal installierte E-Mail-Programme stehen dem Nutzer zwei SMTP-Relay-Server zur Verfügung:

- mail.uni-muenster.de: Dieser Server erlaubt das nicht authentifizierte Versenden von E-Mails. Er nimmt E-Mails nur aus dem von der WWU versorgten IP-Addressbereich an. Er ist von Netzen außerhalb des Universitätsnetzes nicht erreichbar.
- secmail.uni-muenster.de: Dieser Server erlaubt das Versenden von E-Mails von Rechnern innerhalb des Universitätsnetzes wie auch von außerhalb. Er ist über Port 25 (SMTP) und 587 (Submission) ansprechbar. Nach dem Verbindungsaufbau wird zwingend auf das verschlüsselte TLS-Protokoll umgeschaltet, um ein Abhören von Passwörtern zu verhindern. Zur Annahme von E-Mails verlangt der Server eine Authentifizierung des Absenders mit seiner zentralen Nutzerkennung und dem Standardpasswort. Um einen möglichen Missbrauch zu verhindern, wird zusätzlich die Absenderangabe (genauer der Envelope-Sender) mit der Nutzerkennung abgeglichen. Nur die Nutzerkennung oder die ihr zugeordneten Aliase werden als Absender zugelassen.

Datenbanken

Datenbanken werden sowohl für interne Zwecke des ZIVs benötigt als auch als Service für andere Einrichtungen der WWU (z. B. LearnWeb, Forschungsdatenbank, Nutzerverwaltung) angeboten. Als Software kommen u. a. MySQL, Oracle und PostgreSQL zum Einsatz.

Für alle Datenbanken gilt, dass der Zugriff nur verschlüsselt möglich ist und der Zugang weitestgehend eingeschränkt und durch Firewalls geschützt wird. Zudem ist ein direkter Zugriff, sofern notwendig, nur aus dem Netzbereich der WWU heraus möglich.

Das Backup der Daten erfolgt zweistufig: Täglich wird zunächst eine Kopie (Dump) aller Datenbanken erzeugt, danach wird dieses zusammen mit den übrigen Dateien des Systems im TSM-Backup abgelegt.

Backup und Archivierung

Tivoli Storage Manager (TSM)

Das ZIV stellt für Server- und Arbeitsplatzsysteme als Backupsystem den Tivoli Storage Manager (TSM) zur Verfügung. Jeder, der kritische Daten vor Verlust sichern muss, kann diesen Dienst nutzen. Der Zugang zum TSM-Server wird zudem vor unbefugtem Zugriff geschützt.

Ein Rechner, für den das Backupsystem des ZIV genutzt werden soll, benötigt die Installation der TSM-Client-Software und muss bei einem TSM-Server registriert sein. Dafür werden ihm eine Kennung und ein Passwort zugeordnet. Die Backup- und Archivdaten eines TSM-Clients gehören dieser Kennung. Die korrekte Angabe von Kennung und Passwort legitimieren den Abruf und das Überschreiben von Backup- und Archivdaten, auch wenn diese Operation von einem anderen Rechner als dem ursprünglichen TSM-Client aus durchgeführt wird. Eine Rücksicherungs-Operation ist somit auch dann möglich, wenn der Rechner, der das Backup durchgeführt hat, nicht zur Verfügung steht.

Die Erreichbarkeit einiger TSM-Server ist durch netzwerkseitige Filterregeln und/oder lokale Firewalls eingeschränkt: Der TSM-Server der universitären Verwaltung gehört zu einem abgeschotteten VLAN der Universitätsverwaltung. Der TSM-Server der IVV4 kann nur aus dem Universitätsnetz erreicht werden. Der Zu-

[35] https://permail.uni-muenster.de/

gang zu den anderen TSM-Server ist nicht eingeschränkt, sodass ein als TSM-Client eingetragener Laptop selbst dann den TSM nutzen kann, wenn er unterwegs ist.

Aufbewahrungszeit für Backups

Solange die Backup-Kopie einer Datei aktuell ist, wird sie nicht gelöscht. Erst wenn eine Backup-Kopie veraltet ist, es also entweder eine aktuellere Kopie gibt oder die Originaldatei auf dem Client nicht mehr existiert, wird sie gelöscht, und zwar

- spätestens nach 100 Tagen (wenn es sich um die letzte Backup-Kopie einer nicht mehr existierenden Datei handelt),
- bereits nach 30 Tagen, wenn es aktuellere Backup-Kopien gibt,
- sobald es 6 aktuellere Backup-Kopien gibt (und das Original noch existiert),
- sobald es 4 aktuellere Backup-Kopien gibt und das Original gelöscht ist.

Andere Aufbewahrungsfristen können bis zur Dateiebene individuell eingestellt werden. Bei den o. g. Fristen handelt es sich um die Voreinstellung.

Die Haltbarkeit der Daten auf den eingesetzten Magnetbandkassetten wird mit 10 bis 30 Jahren angegeben. Um auf der sicheren Seite zu sein, werden Magnetbandkassetten spätestens 5 Jahre nach dem Beschreiben auf ein neues Medium kopiert.

Aufbewahrungszeit für Archivdateien

Archivierung ist eine gesonderte Funktion der TSM-Software. Archivdaten werden 10 Jahre aufbewahrt.

Archivdaten werden auf Magnetbandkassetten gespeichert. Von jeder archivierten Datei werden innerhalb eines Tages zwei Kopien erstellt, eine auf einer separaten Magnetbandkassette und eine auf einem TSM-Server an der RWTH Aachen.

Um sicherzustellen, dass die Archivdaten nach längeren Zeiträumen noch lesbar sind, werden die Magnetbandkassetten spätestens 5 Jahre nach dem Beschreiben kopiert.

Revisionssicherheit (Medien)

Die eingesetzten Magnetbandkassetten sind jederzeit wieder beschreibbar und somit nicht revisionssicher.

Authentifizierung

Identity Management

Mit dem Identity Management (IdM)-System werden die in der Benutzerordnung des ZIV[36] gesetzten Ziele sowie die im Abschnitt „Richtlinien für Accountvergabe/Netzzugang“ formulierten Ziele umgesetzt; insbesondere:

- die Erzeugung von Identitäten als Abbilder realer Personen,
- die Zuordnung der aktiven Kennungen zu diesen Identitäten,
- die Abbildung der Organisationsstruktur der Universität,
- die rollenbasierte Versorgung der Nutzerkennungen mit den benötigten Dienstzugängen und Rechten.

Die Personen-, Rollen-, Organisationsstruktur- und Nutzerdaten sind in einer Oracle-Datenbank abgelegt (siehe Abschnitt „Datenbanken“).

Verwaltungs- und Synchronisationsprozesse holen die benötigten Informationen direkt aus den maßgeblichen Datenbanken der Universitäts-Verwaltung (SOS, SVA, UKM-SIP etc.), administrative Oberflächen gestatten die manuelle Pflege der Daten durch wenige ausgewählte Administratoren. Diese Dienste und Prozesse sind auf Servern realisiert, die in einem separaten, stark abgeschotteten VLAN angesiedelt sind.

Active Directory (AD)

Das ZIV bietet zentrale Active Directory Services zur Verwaltung von Benutzern, Gruppen und Ressourcen an. Als zentraler Verzeichnisdienst bildet das AD die Struktur der Organisation ab und ermöglicht die Delegation von Administrationsrechten. Die Nutzer- und Gruppenkennungen im AD werden mehrmals am Tag mit der zentralen Nutzerdatenbank des ZIV synchronisiert. Innerhalb einer Domäne können Organisationseinheiten angelegt werden, die mit Einschränkungen dezentral verwaltet werden können. Fachbereiche und Arbeits-gruppen besitzen so die Möglichkeit, eigene Ressourcen (Arbeitsplatzrechner, Drucker, Server

[36] https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2010/ausgabe25/beitrag_03.pdf

etc.) zu administrieren, ohne eine aufwendige Nutzerverwaltung organisieren zu müssen. Aufgrund der automatisch aufgebauten Vertrauensverhältnisse (Trusts) stehen die zentralen Kennungen auch in untergeordneten Windows Domänen (Child Domains) zur Verfügung. Fremde Active Directory Domänen können über manuell eingerichtete Vertrauensstellungen angebunden werden, sodass auch in diesen Bereichen ein Zugriff auf die zentralen Kennungen möglich ist.

Betrieb der Domain Controller (DC)

Domänencontroller stellen jeweils ein Replikat der AD-Datenbank bereit und sind untereinander gleichwertig (Multi-Master-Modell, Ausnahme: Masterrollen). Datenbankänderungen sind auf jedem DC möglich, diese werden dann möglichst effizient unter den Domänencontrollern repliziert. Der Ausfall eines DC führt nicht zu Ausfallzeiten oder Einschränkungen der Betriebsabläufe. Dieses Modell gewährleistet eine hochredundante Bereitstellung des Active Directory.

Sicherheit des Active Directory

Neben den üblichen Sicherheitsanforderungen für Windowssysteme (zeitnahes Einspielen von Windows-Hotfixes und Service Packs, aktuelle Virenscanner, ggf. Einsatz einer Firewall, Absicherung des Systems über Windows Gruppenrichtlinien etc.) gelten am ZIV zusätzliche Regeln für Administratoren eines Active Directory:

- Domänenadministratoren des ZIV melden sich grundsätzlich nur mit einer Smartcard oder einem eToken (2-Faktor-Authentifizierung) an einem Domänencontroller an. Für den Notfall besitzt jeder Administrator ein komplexes Passwort falls eine Smartcard-Anmeldung nicht möglich sein sollte (PKI-Fehler, o. ä.).
- Zusätzlich können sich Domänenadministratoren nur an Domänencontrollern und wenigen speziell dafür vorgesehenen Verwaltungsservern (AD-Zertifizierungsstelle, Dienst für Nutzer-Synchronisation) anmelden.

Single Sign-On (SSO)

Am ZIV wurde ein vom Ansatz her sehr einfaches Single-Sign-On-System implementiert, das die besondere Struktur des Webangebotes bzw. des Webserverparks ausnutzt (siehe Abschnitt „Webserverpark“).

Die Webserverpark-Frontend-Systeme arbeiten als Reverse Proxy und können daher verschiedenste Dienste unter einem gemeinsamen Rechnernamen anbieten. Neben Diensten auf Webserverpark-Backend-Systemen (z. B. das Nutzerportal MeinZIV) sind auch Dienste auf anderen Systemen (z. B. der Webmailer perMail oder das Lehrversanstaltungsportal HISLSF/QISPOS) integriert.

Wird ein Dienst, für den eine Authentifizierung nötig ist, mit einem speziellen URL-Präfix angesprochen, so muss der Nutzer sich nur einmal ausweisen. Der Browser des Nutzers sorgt unsichtbar dafür, dass bei nach-folgenden Zugriffen auf beliebige Dienste mit gleichem URL-Präfix immer alle zur Authentifizierung notwendigen Informationen mitgeschickt werden. Zur Authentifizierung stehen drei Methoden zur Auswahl, die über unterschiedliche URL-Präfixe angesprochen werden: HTTP-Basic-Authentifizierung (Passwortkontrolle), X.509-Client-Zertifikat-Kontrolle (optional per Smartcard) und Shibboleth-Authentifizierung.

Die Frontend-Systeme weisen sich gegenüber den eingebundenen Backend-Systemen per HTTP-Basic Authentifizierung mittels einer internen Nutzerkennung und zugehörigem Passwort aus und übergeben zusätzlich die Nutzerkennung des authentifizierten Nutzers. Die Frontend-Systeme stellen sicher, dass diese nur dann übermittelt wird, wenn auch tatsächlich eine erfolgreiche Authentifizierung stattgefunden hat. Dazu können die Frontend-Systeme für einzelne Dienste vertrauliche Eigenschaften des authentifizierten Nutzers an den Backend-Server übergeben, falls es aus Datenschutzgründen unerwünscht ist, dass der Betreiber des Backend-Servers diese Daten für alle Nutzer bereitstellt.

Die Backend-Systeme kontrollieren, ob die Anfrage tatsächlich über die vertrauenswürdigen Frontend-Systeme gelaufen ist, ersetzen nach der Kontrolle des Passworts der internen Nutzerkennung – aber vor allen Autorisierungsschritten – die interne Kennung durch die übergebene Nutzerkennung des authentifizierten Nutzers und führen mit dieser dann alle weiteren Kontrollen (Gruppenmitgliedschaften usw.) durch.

Jede Anwendung, die in der Lage ist, einer bereits vom Webserver vorgenommenen Authentifizierung zu vertrauen, kann ohne weitere Anpassung in das Single Sign-On integriert werden; andere Anwendungen erfordern meist nur einen geringen Anpassungsaufwand.

Administrative Schnittstellen von Servern und Speichersystemen

Im ZIV sind die administrativen Schnittstellen von Servern und Speichersystemen in einem besonders geschützten VLAN zusammengefasst, dass nur von zwei Gateway-Rechnern aus für betriebliche Arbeiten genutzt werden kann.

Sicherheitsfunktionen im Netz

Innerhalb des universitären Intranets kommen diverse Technologien zur Absicherung auf der Netzwerkebene zum Einsatz.

Stateless-Packet-Screening (ACL)

Stateless-Packet-Screening – insbesondere auf den Layer-3-Switches (Routern) – kontrolliert die Konnektivität im Wesentlichen auf der Basis von Kommunikationsquellen und -zielen (IP-Adressen und logische Interfaces von Routern) sowie bestimmter höherer Protokollmerkmale (Anwendungsprotokolltypen, d. h. z. B. TCP-/UDP-Ports, und einige weitere Protokollelemente).

Diese Methode kommt überall dort zum Einsatz, wo die über Zugangskontrolllisten in Routern (ACLs, Access Control Lists) erreichbare Grundsicherheit ausreichend ist oder wo ein hoher Durchsatz als vorrangig betrachtet werden muss. Hier kann in Zusammenhang mit besonderen Zonen, in denen Applikation-Gateways mit Sicherheitsfunktionen (Application-Proxies, auch Terminal-Server, Web- und FTP-Server mit Sicherheitsfunktionen usw.) installiert werden, bereits eine sehr hohe Sicherheit erreicht werden, ohne dass besondere Kosten anfallen würden, da moderne Router meistens dazu geeignet sind und ohnehin Bestandteil der Netze sind. Ein Einsatz solcher Funktionen ist technisch praktisch immer möglich, sofern der erforderliche Verwaltungs-aufwand dazu erledigt wurde (siehe Anhang H | Das Konzept der Netzstrukturierung).

Firewall

Auch in Layer-3 kommen aktive Firewalls im Sinne eines Stateful-Packet-Screening unter Berücksichtigung port-agiler Protokolle (wie z. B. FTP, SIP, H.323) zum Einsatz. Diese ist sicherheitstechnisch den Möglichkeiten der ACLs der Router deutlich überlegen, da die Blockierung unerwünschter Konnektivität sitzungsbezogen (Flow-basiert) ist.

Hier kann wie bei den Stateless-Paket-Filtern eine noch weitergehende Sicherheitsqualität im Zusammenhang mit besonderen Zonen für Applikations-Gateways erreicht werden. Der Nachteil solcher Firewalls sind die vergleichsweise geringen Durchsatzmöglichkeiten, die weit hinter den Möglichkeiten von reinem Routing zurückbleiben. Deshalb können solche Systeme nur dann eingesetzt werden, wenn die Durchsatzbeschränkungen unkritisch sind oder wenn die Erhöhung der Sicherheit gegenüber den ACL-basierten Funktionen vor der Performance Vorrang hat.

Application-Gateways oder Application-Proxies

Application-Gateways oder Application-Proxies sorgen auf der Ebene von Anwendungsprotokollen und unter Berücksichtigung der Inhalte für besondere Sicherheitsfunktionalitäten, z. B. E-Mail-Relays bzw. SMTP-Gateways mit Virenschutzfunktionen, Systeme für HTTP (Web-Proxies) oder FTP (FTP-Proxies). Auch Terminalserver stellen eine häufig geeignete und sichere Übergangsmöglichkeit in fremde Netzbereiche da.

Solche Funktionalitäten werden in der Regel durch die Verantwortlichen bereitgestellt, die auch sonst für den Bereich der IV-Anwendungen zuständig sind, und können nicht im Sinne eigentlicher netzseitiger Sicherheitsmaßnahmen betrachtet werden. Netzseitig ist hier jedoch für die Abstimmung und entsprechende Bereitstellung von Netzzonen zu sorgen.

Intrusion Detection- und Prevention-Systeme (IPS)

IPS analysieren Datenströme und können Dateneinheiten oder Flows aufgrund bestimmter Datenmuster (Signaturen), Verhaltensanomalien oder Kombinationen beider Merkmale automatisch erkennen und blockieren.

Damit werden Angriffe abgewehrt, die z. T. über hostbasierte Abwehrmöglichkeiten hinausgehen; die Abwehr erfolgt häufig frühzeitiger, d h. insbesondere bevor weite Infrastrukturbereiche in Mitleidenschaft gezogen wurden. Sogenannte Zero-Day-Attacken, also bisher unbekannte Angriffstypen, werden oft erkannt und abgewehrt. Auch Denial of Service (DoS) Angriffe, die von den betroffenen Systemen kaum selbst beherrscht werden können, sollten damit weitestgehend abgewehrt werden können.

VPN-Technologie

Ein sicherer Zugang zu Netzzonen durch verschlüsselte Tunnel mit Hilfe der VPN-Technologie ermöglicht den kontrollierten Zugang (authentifiziert, unter Autorisierungsüberwachung) zu Ressourcen auch in geschützten Bereichen.

Die im ZIV eingesetzte VPN-Technologie basiert auf IPSec (IP Security). IPSec ist eine Erweiterung des Internetprotokolls (IP), um Vertraulichkeit, Authentizität und Integrität der Datenkommunikation zu ermögli-

chen. IPSec ermöglicht eine sichere Kommunikation über ungesicherte Netzwerke, wie z. B. das Internet, indem u. a. die Daten mit 3DES oder AES verschlüsselt werden.

Neben einem allgemeinen VPN-Gateway für die Universität, gibt es auch dedizierte VPN-Gateways für einzelne Fachbereiche. Nach dem Aufbau einer VPN-Verbindung z. B. zu einem VPN-Gateway eines Fachbereichs befindet sich der Rechner in der Netzzone des Fachbereichs. Somit können berechtigte Nutzer auch von außerhalb Dienste eines internen Netzwerkes des Fachbereiches nutzen, die sonst aus Sicherheitsgründen (oder anderen Gründen) über das Internet nicht unmittelbar zur Verfügung stehen.

Für den Aufbau einer VPN-Verbindung muss der Nutzer den VPN-Client der Firma Cisco, oder einen anderen IPSec unterstützenden Einwahlclienten, installiert haben. Für alle gängigen Betriebssysteme (Windows, Linux, Mac OS) stehen den Angehörigen der Universität und des UKM der Cisco-VPN-Client auf den Webseiten des ZIV zum Download[37] zur Verfügung.

Der Nutzer muss sich gegenüber dem allgemeinen VPN-Gateway der Universität mit seiner ZIV-Kennung und seinem Netzzugangspasswort authentifizieren. Für bereichsbezogene VPN-Gateways muss sich ein Nutzer als user@xyz mit seinem Netzzugangspasswort einloggen, wobei xyz für den Namen des entsprechenden VPN-Gateways steht. Ob ein Nutzer die Berechtigung hat, sich in ein bestimmtes VPN-Gateway einzuwählen, hängt davon ab, ob der Nutzer in eine zum VPN-Gateway gehörigen Nutzergruppe im Identity Management zugeordnet ist. Diese Nutzergruppen können online von den zuständigen Projektleitern verwaltet werden.

High Performance Computing (HPC)

Der Zugang zum HPC-System ist auch von außerhalb des Universitätsnetzes, jedoch ausschließlich über Secure Shell möglich. Dateitransfers erfolgen nur verschlüsselt (sftp/scp). Für das webbasierte Monitoring des HPC-Systems ist darüber hinaus nur noch Port 443 nach außen hin geöffnet. Alle anderen Dienste sind lokal durch Firewalls abgesichert.

Zur Nutzung ist die Mitgliedschaft in einer von 23 Projektgruppen sowie in der Gruppe uoclstr erforderlich. Die Mitgliedschaft besteht maximal bis zum Ablauf der Nutzerkennung.

Die „/home-Verzeichnisse“ werden von einem SoFS-Server gemountet. Für die Endsicherung der Daten über-nimmt der Nutzer selbst die Verantwortung. Es werden kurzfristige Backups der Nutzerdaten angelegt. Diese stellen aber keine Langzeit-Archivierung dar. Zum Speichern großer Datenmengen steht eine „/scratch-Partition“ bereit, deren Inhalt periodisch gelöscht wird.

[37] https://www.uni-muenster.de/ZIV/Anleitungen/VPN/VPN_Anleitung.html

Empfehlungen für Anwender

Das CERT der Universität Münster (WWU-CERT) verzeichnet regelmäßig eine gewisse Menge von Virusinfektionen (darunter auch Trojaner und Bots) im Einwahlbereich (VPN und WLAN). Viele private Computer sind nicht ausreichend abgesichert und bedrohen damit auch die Rechner aller anderen Universitätsangehörigen. Immer wieder kommt es zu Epidemie-artigen Virusinfektionen, der auch schlecht gewartete Universitätsrechner erliegen. Das WWU-CERT hat aus diesem Grund einige Empfehlungen zur Absicherung von Rechner-Systemen und zusätzlich Ratschläge für das Verhalten im Internet zusammengetragen. Die folgenden Abschnitte richten sich sowohl an Mitarbeiter und Studierende der Universität als auch an alle, die mit einem PC arbeiten, und orientieren sich an dem vom IV-Sicherheitsteam erarbeiteten IV-Sicherheitsflyer[38], der für aktuelle Informationen und Hilfestellungen im Internet eingesehen werden kann.

Persönliche Daten schützen

Sowohl personenbezogene Daten als auch persönliche Dateien, wie bspw. die in einem Textprogramm erstellte Diplomarbeit, können unter diesem Oberbegriff zusammengefasst werden. Zu den sog. Personenbezogenen Daten zählen gemäß dem Landesbeauftragten für Datenschutz und Informationssicherheit in NRW „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Einzelangaben (...) sind beispielsweise“[39].

- Name, Alter, Familienstand, Geburtsdatum,
- Anschrift, Telefonnummer, E-Mail-Adresse,
- Konto-, Kreditkartennummer,
- Kraftfahrzeugnummer, Kfz-Kennzeichen,
- Personalausweisnummer, Sozialversicherungsnummer,
- Vorstrafen,
- genetische Daten und Krankendaten und
- Werturteile, wie zum Beispiel Zeugnisse.

Zugangsdaten und Passwörter

Das Passwort bzw. Kennwort dient zur Authentifizierung und zur eindeutigen Identifizierung (Anmeldung). In der IT-Sicherheit wird durch die Anwendung eines Benutzernamens in Kombination mit einem Benutzerpasswort sichergestellt, dass nur derjenige Zutritt zu einem System, zu Daten oder zu Dateien, erhält, dessen Namen in der „Gästeliste“ verzeichnet ist und der zugleich das entsprechende Kennwort nennen kann.

Das Abmelden, sog. Log-out, ist natürlich bei allen Diensten anzuraten, bei denen man sich im Internet anmeldet, sich also bei jeder Sitzung mit einem Benutzernamen und einem Zugangskennwort verifiziert. Nur so weiß der Anbieter, dass eine Sitzung vorüber ist und keine Kommunikation mehr stattfindet. Ohne eine Abmeldung könnten Dritte die Sitzung weiterführen und den entsprechenden Account missbrauchen.

Auf den Webseiten des ZIV können Sie im Nutzerportal MeinZIV[40] ihre Passwörter verwalten und Sie erhalten weitere Hinweise und Regeln zur Passwortwahl im ZIV und Hilfestellungen, falls Sie ihr Standardpasswort für Dienste des ZIV vergessen haben.

Hinweise zum Umgang mit Zugangsdaten und Passwörtern

- Geben Sie niemals und unter keinen Umständen Ihre Passwörter weiter!
- Wenn Ihr Computer von einem Schadprogramm infiziert worden ist, ändern Sie alle Passwörter über einen virenfreien PC. Sie müssen davon ausgehen, dass das Kennwort durch ein Schadprogramm ausgespäht ist.
- Wenn Ihr Passwort bekannt geworden ist, ändern Sie es sofort oder lassen Sie vorrübergehend Ihren Zugang sperren (über MeinZIV sperren).
- Verwenden Sie für verschiedene Dienste unterschiedliche Zugangsdaten, d. h. verschiedene Benutzernamen und Passwörter.

[38] https://www.uni-muenster.de/IV-Sicherheit/flyer/index.html
[39] https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/FAQ/PersonenbezogeneDaten.php (Stand: Sept. 2012)
[40] https://www.uni-muenster.de/MeinZIV/

Sichere Passwörter erzeugen

Sichere Passwörter lassen sich am besten durch einen Merksatz erzeugen, bei dem die Anfangsbuchstaben der Wörter, Interpunktionszeichen und ggf. Sonderzeichen zu einem neuen Passwort kombiniert werden.

So entspricht der Satz „Ich studiere gerne & fahre viel Zweirad in Münster." dem Passwort „Isg&fvZiM."

Eventuell müssen Sie die Kombination den Erfordernissen, wenn bspw. Sonderzeichen oder Umlaute verboten sind, durch Ändern des Merksatzes anpassen. Die Anführungszeichen im Beispiel dienen der optischen Eingrenzung der Phrase sowie des Passwortes und sind nicht erforderlich.

Sperren des Systems

Sie sollten sich, auch bei kurzen Pausen, vom System abmelden, damit kein Unbefugter Zugriff auf Ihren PC, Ihre Dateien und Ihre Daten (speziell Zugangsdaten) erhält.[41]

Sperren des Computers

Bei kurzen Arbeitspausen empfiehlt es sich, den PC zu sperren, sodass kein anderer Benutzer in Ihrer Abwesenheit Ihr Konto benutzen und Schaden anrichten kann. Sollte ein zweiter Benutzer in der Zwischenzeit am Computer arbeiten wollen, so kann dieser sich normalerweise mit seinem eigenen Konto oder dem Gastkonto anmelden. Durch das Sperren bleiben alle Programme und Fenster im aktiven Zustand und stehen nach der Rückkehr sofort wieder bereit.

Sie können einen Windows-PC sperren, indem Sie die Startleiste aufklappen und mit der Maus auf den Pfeil rechts neben dem Eintrag „Herunterfahren" zeigen.[42] Es öffnet sich ein Auswahlfeld, in dem Sie die Option Sperren auswählen können. Unter Windows 8.1 können Sie alternativ auch über den Start-Bildschirm den Computer sperren: Klicken Sie dazu auf das Ausschalten-Icon und wählen Sie dann „Sperren". Auf allen (aktuellen) Windows-Systemen kann der Computer über die on Strg + Alt + Entf und einem Klick auf „Sperren" oder über die Tastenkombination Windows- (⊞) und L-Taste ebenfalls gesperrt werden.

Abmelden / Log-out vom Computer

Haben Sie Ihre Arbeit abgeschlossen und benötigen den PC vorerst nicht mehr, sollten Sie sich vom Betriebs-system abmelden, sog. Log-out, um unbefugte Zugriffe zu verhindern. Durch das Abmelden werden alle vom Benutzer gestarteten Programme beendet und der Anmeldebildschirm eingeblendet.

Sie können sich vom Windows-PC abmelden, indem Sie die Starteiste aufklappen und auf den Pfeil neben dem Eintrag „Herunterfahren" zeigen. Es öffnet sich ein Auswahlfeld, in dem Sie die Option Abmelden auswählen können.

Softwareaktualisierungen

Um ein bestimmtes Mindestmaß an Sicherheit auf Ihrem Computer zu gewährleisten, sollten Sie Softwareaktualisierungen (Updates) und sicherheitskritische Nachbesserungen (Patches) seitens der Softwareentwickler ausführen.[43] Entdeckt ein Hersteller eine potenzielle Schwachstelle im Programmcode seiner Software, veröffentlich er einen Patch, um diese Sicherheitslücke zu schließen, sodass Aggressoren diese nicht mehr ausnutzen können.

Hinweise zum Aktualisieren der Software

Für Hilfestellungen bei der Softwareaktualisierung wenden Sie sich an die Benutzerberatung des ZIV[44] oder telefonisch an die ZIVline[45].

---

[41] An den Rechnern der Universität haben Sie i.d.R. nur die Möglichkeit, sich vom Rechner abzumelden. Tragen Sie unbedingt dafür Sorge, sich abzumelden, damit kein Dritter ihren Account missbrauchen kann! Die Möglichkeit, den PC vorrübergehend zu sperren, haben Sie nicht. Mitarbeiter, sofern ihr PC in die Domäne der Universität (uni-muenster.de oder wwu.de) aufgenommen ist, können sämtliche o. g. Möglichkeiten verwenden.

[42] Diese Informationen beziehen sich auf Windows-Systeme bis einschließlich Windows 7.

[43] Mitarbeiter der Universität können Softwareaktualisierungen über die internen Update-Mechanismen der Programme beziehen (meist ist hier kein Benutzerkonto mit administrativen Rechten vonnöten) oder Updates über die Netzwerkschnittstelle der betreuenden IVV einpflegen.

[44] https://www.uni-muenster.de/ZIV/Hilfe/Benutzerberatung.html

[45] https://www.uni-muenster.de/ZIV/Hilfe/ZIV_line.html

- Vor dem Arbeiten mit einem neuen oder neu installierten PC, Notebook, PDA oder Smartphone sollten alle Updates installiert[46] und die Funktionen für automatische Updates[47] aktiviert worden sein.
- Sicherheitskritische Programme, besonders der Browser, das E-Mail-Programm und evtl. die Software für das Online-Banking, müssen richtig und vor allem gewissenhaft konfiguriert werden.
- Prüfen Sie ggf. die Echtheit der Programme durch einen Prüfsummencheck.
- Das BSI veröffentlicht Informationen zum Update-und Patch-Management[48].
- Viele Software-Produkte bieten integrierte Update-Routinen an, bei denen die Updates im Hinter-grund heruntergeladen und bei Programmstart ohne weitere Rückfrage installiert werden.
- Es gibt Programme, wie Secunia Software Inspector (PSI)[49], die selbstständig nach Aktualisierungen suchen und diese auf Wunsch durchführen.
- Bei einigen Programmen müssen Sie manuell nach Updates suchen und diese selbst installieren. Meistens findet sich in den Programmmenüs unter dem Eintrag „Extras“ oder „Hilfe“ / „Über“ eine Update-Funktion.
- Manchmal kann Software nur dadurch aktualisiert werden, dass eine neue Installationsdatei vom Hersteller bezogen wird. Dies ist eine unkomfortable Update-Methode, aber besser als eine Sicherheitslücke zu riskieren.
- Für Produkte der Firma Microsoft (u. a. Microsoft Office, Internet Explorer und Windows selbst) steht unter Windows-Betriebssystemen ein eingebauter Update-Mechanismus bereit.[50]

Virenschutz

Sie benötigen einen wirksamen Virenschutz, damit Sie die Integrität und Verfügbarkeit Ihrer Dateien und Daten sicherstellen können. So hilft ein aktives Antivirenprogramm zu vermeiden, dass Schadprogramme ihre Dateien oder persönlichen Daten verändern, löschen oder an Dritte übermitteln, was besonders im Fall von Passwörtern auf vielfältige Weise Schaden anrichten kann.

Ein Virenprogramm hat dabei mindestens zwei Aufgaben: Es untersucht (scannen) zunächst den PC auf schädliche Programme und versucht bei einer Infektion den PC zu säubern (desinfizieren). Die zweite Aufgabe besteht darin, den PC permanent mit einer sog. Wächterfunktion (Guard) gegen Gefahren durch Schadpro-gramme zu schützen.

Sophos Antivirensoftware

Studierende und Mitarbeiter können das Antivirenprogramm namens Sophos Antivirus[51] kostenlos herunterladen, solange Sie an der Universität studieren bzw. beschäftigt sind, und über den gesamten Zeitraum die benötigten Viren-Definitionsdateien für eine Virensuche über den integrierten Updater des Programms beziehen.

Die Installationsdatei für Windows 7/8 ist von den Mitarbeitern des ZIV so vorbereitet worden, dass Anwender Sie nur herunterzuladen und auszuführen brauchen. Alle weiteren Einstellungen, wie das Eintragen der Update-Mechanismen werden automatisch vorgenommen. Akzeptieren Sie bei der Installation die Rückfrage der Benutzerkontensteuerung.

Zwölf-Punkte-Plan nach einem Virenbefall des PC

Nachdem ein Antivirenprogramm Schadsoftware auf dem PC gefunden hat, ist es ratsam, den Rechner neu aufzusetzen, da niemand zweifelsfrei nachvollziehen kann, welche Auswirkungen das Schadprogramm auf den PC hatte und ob es tatsächlich restlos durch das Antivirenprogramm gelöscht werden konnte.

1. Bewahren Sie Ruhe!

---

[46] Mittels „WSUS Offline Update“ können Sie Microsoft Windows- und Office-Computer sicher aktualisieren. Offline-Updates sind komfortabel zu benutzen und erweisen sich als Zeitersparnis, da alle benötigten Dateien in einem großen Paket heruntergeladen werden. Laden Sie auf einem nicht von Schadsoftware befallenem System das Update-Programm herunter und führen Sie es aus. Befolgen Sie die weiteren Schritte im Programm, bei denen ein Installationsmedium erstellt wird, das Sie zum Einspielen der Updates auf dem neu installierten PC benutzen können. Quelle: http://www.wsusoffline.net (Stand: Januar 2015).

[47] Im ZIV-Wiki finden Sie eine bebilderte Anleitung: https://www.uni-muenster.de/ZIVwiki/bin/view/Anleitungen/SoftwareAktualisierung.

[48] https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/UpdatePatchManagement/updatePatchManagement_node.html (Stand: Juni 2013).

[49] Unter den Programmempfehlungen des IV-Sicherheitsteams ist das Programm verlinkt: https://www.uni-muenster.de/IV-Sicherheit/flyer/downloads.html

[50] Siehe Fußnote 47 (Seite 34).

[51] https://www.uni-muenster.de/ZIV/Software/SophosDownload.html

2. Benutzen Sie einen anderen PC, um ihre Kennwörter, die Sie auf dem befallenen System benutzt haben, zu ändern. Die alten Passwörter müssen als kompromittiert, d. h. als unsicher, bewertet werden.
3. Fertigen Sie ein Backup[52] der Daten des befallenen Computers an.
4. Installieren Sie den befallenen Computer neu. Formatieren Sie dabei die Festplatte komplett und installieren Sie das Betriebssystem neu. Achten Sie darauf, nur Originalsoftware zu verwenden, d. h. Software aus einer legalen Quelle mit legalem Installationsschlüssel.
5. Prüfen Sie ggf. die Echtheit der Programme durch einen Prüfsummencheck[53].
6. Verbinden Sie den frisch installierten Rechner vorerst nicht mit dem Internet: Trennen Sie das Netzwerkkabel vor der Installation des Betriebssystems und erstellen Sie keine WLAN-Verbindung.
7. Installieren Sie zuerst die Windows-Updates. Am besten nutzen Sie dafür eine Offline-Quelle[54].
8. Installieren Sie ein Antivirenprogramm. Erwerben Sie eines im Handel oder laden Sie eines über einen sicheren Computer herunter und führen Sie die Installation auf dem ehemals befallenen System durch.
9. Nun können Sie sich „gefahrenfrei“ mit dem Netzwerk bzw. Internet verbinden.
10. Wenn Sie die restlichen Windows-Updates eingespielt und ihre Antivirenlösung aktualisiert haben, installieren Sie die restlichen von Ihnen benötigten Programme.
11. Führen Sie noch einmal alle Update-Routinen aus.
12. Kopieren Sie die zuvor gesicherten Daten zurück auf Ihren PC.

Firewall

Eine Firewall funktioniert im Prinzip wie ein Durchlass an einer Grenze: Anhand von eingestellten Regeln wird die Kommunikation, also das Passieren von Informationen zwischen Intranet und Internet (oder einem anderem Intranet), erlaubt oder verboten. Diese Arbeitsweise bedingt, dass eine Firewall immer nur so gut arbeiten kann, wie es die Regeln erlauben. Wenn diese den eigenen Bedürfnissen entsprechend und hinsichtlich der Sicherheitsprinzipien angepasst werden, bietet die Firewall eine effektive Maßnahme gegen Trojaner und Hackangriffe aus dem Internet. Ein Allheilmittel ist sie aber nicht, da ein Kontakt mit Schadsoftware durch sie nicht unterbunden werden kann.

Einrichten der Firewall

Seit Windows XP mit dem Servicepack 2 ist eine Firewall-Lösung in das Betriebssystem integriert und sofern Sie für die verschiedenen Netzwerke eine korrekte Klassifizierung getroffen haben[55], für die meisten Szenarien richtig konfiguriert. Sollten dennoch manuelle Änderungen vonnöten sein, sind diese über das Modul „Windows-Firewall“ in der Systemsteuerung möglich.[56]

Datensicherung, sogenanntes Backup

Erstellen Sie regelmäßig eine Kopie (Backup) Ihrer Dateien, damit im Notfall z. B. nach einem Virenbefall, einem Defekt des PCs durch eine Stromspitze, bei Diebstahl oder durch unbeabsichtigtes Löschen Ihre Dateien nicht unwiederbringlich verloren sind.

› Benutzen Sie externe Medien, wie z. B. externe Festplatten, USB-Sticks oder CD-ROM / DVDs.
› Bewahren Sie diese an einem sicheren Ort, am besten außerhalb der eigenen Wohnung, auf. Nur so können Sie sicherstellen, dass die Dateien bspw. bei einem Wohnungsbrand oder Einbruch noch verfügbar sind.
› Machen Sie ggf. von einer Verschlüsselung des Backups Gebrauch.

---

[52] Im Allgemeinen wird ein Schadprogramm keine ihrer persönlichen Dateien so infizieren, dass ein Kopieren der Daten auch vom befallenen System auf einen externen Speicher unmöglich und inakzeptabel ist. Sollten Sie dadurch aber einen Sicherheitsverlust befürchten, können Sie entweder das Speichermedium mit den Daten ausbauen und in einen vor Schadprogrammen geschützten PC einbauen oder mit einer sog. Boot-CD virenfrei starten und dann die Daten kopieren. Beide Möglichkeiten gelten auch, wenn ein Zugriff auf das Betriebssystem nicht mehr möglich ist. Quelle für Boot-CDs: http://www.knoppix.org/ oder http://www.nu2.nu/pebuilder/ (Stand Oktober 2012).
[53] https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Schutzprogramme/Pruefsummen/pruefsummen_node.html (Stand Juni 2013).
[54] Siehe Fußnote 46 (Seite 34).
[55] Eine korrekte Klassifizierung bedeutet, dass Sie beim Anlegen eines neuen Netzwerkes dieses entweder als Arbeitsplatz- bzw. Domänennetzwerk (beispielsweise uni-muenster.de) oder als privates Netzwerk (beispielsweise das eigene häusliche WLAN) oder als öffentliches Netzwerk (beispielsweise das Netzwerk in Ihrem Straßencafé) kategorisiert haben. Diese Einstellungen können im Modul „Netzwerk- und Freigabecenter“ in der Systemsteuerung nachträglich geändert werden (gilt für Windows 7).
[56] Im ZIV-Wiki finden Sie eine bebilderte Anleitung: https://www.uni-muenster.de/ZIVwiki/bin/view/Anleitungen/WindowsFirewall.

- Eine Sicherungskopie in die Cloud (Dropbox etc.) auszulagern, kann unter Umständen problematisch sein. Zum einen ist der Speicherplatz und die Bandbreite zum Hinauf- und Herunterladen (Up- und Download) begrenzt oder kostet Geld, zum anderen ist das Speichern von Informationen bei Anbietern außerhalb Deutschlands bzw. der EU datenschutzrechtlich als problematisch zu bewerten. Schutzbedürftige Daten Dritter dürfen keinesfalls, auch an keinen deutschen Dienst, ausgelagert sein!
- Für das Sichern auf einem externen Datenträger kann die in das Windows-Betriebssystem integrierte Komponente namens „Sichern und Wiederherstellen“ genutzt werden. Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) bietet eine umfangreiche Hilfeseite[57] mit Anleitungen zur Datensicherung unter Windows an.

TSM-Dienst für Mitarbeiter/-innen der Universität

Neben dem persönlichen Plattenplatz steht Bediensteten der WWU der Dienst TSM (Tivoli Storage Manager) im ZIV zur Verfügung. Ihre Daten werden bei Bedarf oder automatisch von Ihrem Arbeitsplatzrechner auf ein Kassettenarchivsystem übertragen und können über ein Zugriffsprogramm selbst wieder heruntergeladen werden, falls eine lokale Datei verloren gegangen ist. Mehr dazu finden sie im Abschnitt „Tivoli Storage Manager (TSM)“.

Dateien verschlüsseln

Sie sollten beim Abspeichern von persönlichen Daten auf dem lokalen PC oder nach Möglichkeit auch auf dem Mobiltelefon eine Verschlüsselung nutzen. Ohne Chiffrierung können diese Informationen ausgespäht und von Online-Betrügern missbraucht werden.

Verschlüsselung mit dem Programm TrueCrypt

Ihren persönlichen Computer, Notebook und Tablet/Smartphone sollten Sie nach Möglichkeit immer verschlüsseln. Für Computer/Notebooks gibt u. a. das Open Source Programm TrueCrypt[58], das unter allen gängigen Betriebssystemen (Windows, Linux, MacOS) lauffähig ist. Diese Software legt einen Datei-Container an, welcher als neues Laufwerk zur Verfügung gestellt wird und mit Daten befüllt werden kann. Sobald die Daten nicht mehr im Arbeitsprozess bereit stehen müssen, kann der Container geschlossen und die Dateien so vor jedem weiteren Zugriff geschützt werden. Niemand kann diese dann lesen oder benutzen, bis der Container durch die Eingabe eines vorher festgelegten Passwortes wieder geöffnet wird. Obwohl die Entwicklung eingestellt wurde, die Entwickler sogar von einer Nutzung abraten[59], kann zurzeit davon ausgegangen werden, dass die Verschlüsselung sicher und keine Hintertüren vorhanden sind. Bestätigt wird dies durch eine erste Auditierung durch das Open Crypto Audit Project[60]. Aus diesem Grund kann TrueCrypt aktuell noch genutzt werden, insbesondere auch deshalb, weil es (noch) keine alternative Open Source Software gibt, die den Funktionsumfang und Qualität der Verschlüsselung besitzt.

Verschlüsselte Kommunikation via E-Mail

E-Mails im Internet kann man sehr gut mit Postkarten vergleichen. Jeder mit etwas Fachwissen kann:

- einen Blick auf die Postkarten werfen, also mitlesen,
- auf den Postkarten herum malen, also verändern, und
- Postkarten unter falschem Namen absenden, also fälschen.

Jede aktuelle E-Mail-Software bietet Ihnen die Möglichkeit, Ihre Unterhaltung zu verschlüsseln und zu signieren (elektronisch zu unterschreiben) und so Ihre Unterhaltung vor Mitlesen, Verändern und Fälschen zu schützen. Zum Verschlüsseln und zur Unterschriftenkontrolle benötigt die Software den sog. öffentlichen Schlüssel Ihres Gegenübers. Dieser ist häufig mit einem Zertifikat versehen; das ist eine elektronische Beglaubigung, dass der öffentliche Schlüssel tatsächlich Ihrem Gegenüber gehört.

Die Zertifizierungsstelle der Universität Münster (WWUCA[61]) erstellt u. a. solche Zertifikate für S/MIME-Schlüssel. Die folgenden Anleitungen beschreiben für ausgewählte Software, wie Sie zu einem zertifizier-

---

[57] https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datensicherung/datensicherung_node.html (Stand Juni 2013).
[58] http://www.heise.de/download/truecrypt.html (Version 7.1a)
[59] Hintergründe zu der Einstellung der Entwicklung können bei Heise Online nachgelesen werden:
http://heise.de/-2211037 (News) und http://heise.de/-2211475 (Kommentar)
[60] https://opencryptoaudit.org/
Zusammenfassung des Audits auf Heise Online: http://heise.de/-2170398
Der erste Audit-Bericht kann hier eingesehen werden:
https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf
[61] https://www.uni-muenster.de/WWUCA

ten Schlüsselpaar kommen, wie Sie dieses Ihrem E-Mail-Programm beibringen können und wie Sie dann E-Mails signieren, verschlüsseln sowie entschlüsseln und Signaturen überprüfen können.

E-Mails digital unterschreiben / signieren

Sie haben darüber hinaus die Möglichkeit, ein Zertifikat der Universität Münster zu beantragen und damit Ihre E-Mails zu signieren (die Echtheit des Absenders nachzuweisen) und bei Bedarf die E-Mails zu verschlüsseln[62]. Es wird für die folgenden Anleitungen vorausgesetzt, dass Sie über ein Zertifikat der Zertifizierungsstelle der Universität Münster (WWUCA) verfügen. Falls Sie noch keines besitzen, können Sie eines beantragen.

Absichern der E-Mail-Kommunikation

Sie können Ihr E-Mail-Programm für die Universität Münster so einrichten[63], dass jede Kommunikation des Programms mit dem E-Mail-Server verschlüsselt stattfindet.

Mobile Sicherheit

Bei der Nutzung des Internets über mobile Geräte, wie Smartphones, PDAs oder Tablet-PCs, muss mit denselben Gefahren gerechnet werden, wie sie auch für den PC zutreffen. Zusätzlich sind aber weitere Maßnahmen zu ergreifen, vgl. Empfehlungen zum dienstlichen Umgang mit Mobilgeräten. Das BSI hat hierzu auch einen Leitfaden[64] erstellt, in dem die meisten schutzbedürftigen Punkte thematisch zusammengetragen sind.

[62] Auf den Internetseiten der Zertifizierungsstelle finden Sie Anleitungen, wie Sie E-Mails signieren und bei Bedarf verschlüsseln können: https://www.uni-muenster.de/WWUCA/info/howto-email.html.
[63] Im ZIV-Wiki finden Sie für die verschiedenen E-Mail-Programme bebilderte Anleitungen: https://www.uni-muenster.de/ZIVwiki/bin/view/Anleitungen/EmailKonf.
[64] https://www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/mobileSicherheit_node.html (Stand Juni 2013).

Abkürzungsverzeichnis

3DES	Triple Data Encryption Standard
ACL	Access Control List
ADS	Active Directory Service
AES	Advanced Encryption Standard
BSI	Bundesamtes für Sicherheit in der Informationstechnik
CA	Certification Authority
CERT	Computer Emergency Response Team
CMS	Content Management System
DC	Domain Controller
DFN	Deutsches Forschungsnetz
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarisierte Zone
DoS	Denial-of-Service
DSG	Datenschutzgesetz
DV	Datenverarbeitung
EFS	Encrypted Filesystem
FTP	File Transfer Protocol
GnuPG	GNU Privacy Guard
GPFS	General Parallel File System
HPC	High Performance Computing
HTTP	Hypertext Transfer Protocol
IdM	Identity-Management
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP-Security
ISidoR	Online-Security-Audit der WWU ("Informations-Sicherheit ist die oberste Regel")
ISM	Informationssicherheitsmanagement
IT	Informationstechnik
ITZ	IT-Service-Zentrum der Universitätskliniken
IV	Informationsverarbeitung

IVV	Informationsverarbeitungs- und Versorgungseinheit
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MD5	Message Digest Algorithm 5
NIC	Network Information Center
NOC	Network Operation Center
NWZ	Naturwissenschaftliches Zentrum
PGP	Pretty Good Privacy
PIN	Persönliche Identifikations-Nummer
PKI	Public Key Infrastruktur
POP3	Post Office Protocol 3
RAC	Real Application Cluster
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independant Disks
RAS	Remote Access Service
RDP	Remote Desktop Protocol
SAN	Storage Area Network
SIP	Session Initiation Protocol
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Secure Session ID
SSL	Secure Session Layer
SSO	Single-Sign-On
TCP	Transmission Control Protocol
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TSM	Tivoli Storage Manager
UDP	User Datagram Protocol

UKM	Universitätsklinikum Münster
ULB	Universitäts- und Landesbibliothek
VLAN	Virtual Local Area Network
VME	Verwaltung der medizinischen Einrichtungen
VPN	Virtuelles Privates Netzwerk
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWU	Westfälische Wilhelms-Universität
WWU-CA	Zertifizierungsstelle (Certification Authority, CA) der WWU
WWU-CERT	Computer Emergency Response Team (CERT) der WWU
WWW	World Wide Web
ZIV	Zentrum für Informationsverarbeitung
ZUV	Zentrale Universitätsverwaltung

Anhang A | Benutzungsordnung des Zentrums für Informationsverarbeitung und der IV-Versorgungseinheiten der Universität Münster

vom 15. November 2010

Aufgrund der §§ 2 Abs. 4, 29 Abs. 2 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG) vom 31.10.2006 in Verbindung mit dem Organisationskonzept „Das System der Informationsverarbeitung der WWU Münster“ (Senatsbeschluss vom 8.7.1996, zuletzt geändert durch die Änderungsverordnung vom 11. März 2004[65]) hat der Senat der Westfälischen Wilhelms-Universität Münster (WWU) die folgende Benutzungsordnung für das Zentrum für Informationsverarbeitung (ZIV) und die IV-Versorgungseinheiten (IVVen) beschlossen:

Präambel

Diese Benutzungsordnung soll die möglichst störungsfreie, ungehinderte und sichere Nutzung der Infrastruktur zur Kommunikation und Informationsverarbeitung (IV-Infrastruktur) des ZIV und der IVVen der WWU gewährleisten. Sie stellt Grundregeln für einen ordnungsgemäßen Betrieb der gesamten IV-Infrastruktur auf und regelt so das Nutzungsverhältnis zwischen den einzelnen Nutzenden und dem ZIV sowie mit den IVVen.

§ 1 Geltungsbereich

Diese Benutzungsordnung gilt für die Nutzung der IV-Infrastruktur der WWU, bestehend aus den Datenverarbeitungsanlagen, Kommunikationssystemen und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung (IV), die dem Zentrum für Informationsverarbeitung und/oder den IV-Versorgungseinheiten der WWU unterstellt sind (kurz: IV-System); soweit einzelne Komponenten des IV-Systems nicht ausdrücklich dem ZIV oder einer IVV unterstellt sind, gilt diese Regelung für diese Teile des IV-Systems entsprechend.

§ 2 Nutzungsberechtigung und Zulassung zur Nutzung, Identitätsmanagement

(1) Zur Nutzung des IV-Systems können zugelassen werden:
1) Mitglieder und Angehörige, Einrichtungen und Verwaltungen der Hochschulen sowie andere Einrichtungen des Landes Nordrhein-Westfalen, für die das IV-System mit er-richtet worden ist, zur Erfüllung ihrer Aufgaben,
2) Mitglieder und Angehörige von anderen Hochschulen des Landes Nordrhein-Westfalen oder staatlichen Hochschulen außerhalb des Landes Nordrhein-Westfalen aufgrund von besonderen Vereinbarungen der Hochschule oder Weisungen des zuständigen Ministeriums,
3) Studentenwerke im Lande Nordrhein-Westfalen,
4) Sonstige juristische oder natürliche Personen, sofern nach vorrangiger Inanspruchnahme des IV-Systems durch die unter Nr. 1 bis 3 genannten Benutzer noch freie Kapazitäten vorhanden sind.

Bei Nutzung aus Anlass von Nebentätigkeiten gelten die Nebentätigkeitsvorschriften für den Hochschulbereich des Landes Nordrhein-Westfalen.

(2) Die Zulassung erfolgt ausschließlich zu Zwecken in Forschung, Lehre und Studium, für Zwecke der Medizin, der Bibliothek und der universitären Verwaltung, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der WWU. Eine hiervon abweichende Nutzung kann zugelassen wer-den, wenn sie geringfügig ist und die Zweckbestimmung des IV-Systems sowie die Belange der an-deren Nutzenden nicht beeinträchtigt werden. Eine kommerzielle Nutzung gemäß Abs. 1 Nr. 4 ist nur nach Rücksprache mit dem ZIV bzw. den IVVen für ihre jeweiligen Zuständigkeiten möglich.

(3) Die Zulassung zur Nutzung der Einrichtungen und Dienste des IV-Systems erfolgt im Rahmen des Identitätsmanagements durch Erteilung einer oder mehrerer Accounts auf den Zielsystemen, auf die der/die Nutzende auf Grund seiner/ihrer Rolle zugriffsberechtigt sein soll (Provisionierung). In der Regel werden alle Accounts eines/einer Nutzenden durch dieselbe Kennung identifiziert. In Aus-

[65] https://www.uni-muenster.de/Rektorat/abuni/2004/ab040402.html

nahmefällen können es die verschiedenen Rollen eines/einer Nutzenden erfordern, dass er/sie mehrere Kennungen erhalten muss.

1) automatisierte Kennungserstellung

Kennungen werden in der Regel automatisiert aus den Daten, die in den Personenverzeichnissen der Einrichtungen der Universität geführt werden, erzeugt.

Für Mitarbeiter/Mitarbeiterinnen werden hierbei Daten gemäß „Anlage Mitarbeiter“ in das Identitätsmanagementsystem übertragen.

Für Studierende werden hierbei Daten gemäß „Anlage Studierende“ in das Identitätsmanagementsystem übertragen.

2) Kennungserstellung auf Antrag

Ist eine automatisierte Kennungserstellung nicht möglich, kann daneben vom ZIV auf schriftlichen Antrag oder auf eine formgerechte Online-Anmeldung eine Kennung erteilt werden. Das Antragsverfahren ist zweistufig:

a) Nutzergruppe

Ein für die Finanzierung Verantwortlicher (Hochschullehrerin / Hochschullehrer oder Leiterin / Leiter einer Einrichtung) stellt einen Antrag auf Einrichtung einer Nutzergruppe.

Im Rahmen einer Nutzergruppe können dann Nutzende die Zulassung beantragen. Soweit IVVen eine eigene Nutzerzulassung haben, wird die Erlaubnis von deren Leiterinnen/Leitern entsprechend erteilt.

Bei der Zulassung sollen unter Verwendung eines vorgegebenen Formblatts bzw. bei der Online-Anmeldung neben der Beschreibung der Nutzergruppe die gemäß Anlage aufgeführten Angaben erfasst werden. Hinzu kommen:

› Unterschrift der Nutzergruppenleiterin/des Nutzergruppenleiters
› Angaben zur Person und Unterschrift des für die Finanzierung Verantwortlichen

b) Nutzerantrag

› Angaben zur Person gemäß Anlage als Mitarbeiter/Mitarbeiterin bzw. Studierender
› Unterschrift des/der Nutzenden
› Angaben zur Person und Unterschrift der Nutzergruppenleiterin/des Nutzergruppenleiters

3) Rollenverwaltung

Die Rollen eines/einer Nutzenden werden, soweit sie für die Provisionierung relevant sind und sich nicht aus den bei der Kennungserstellung erhobenen Daten ergeben, separat erfasst.

4) Kennungsaktivierung

Der/die Nutzende erhält mit der Eintragung im Identitätsmanagement ein Passwort. Studierenden wird dazu im Anschreiben bei der Immatrikulation mitgeteilt, dass die über ihn/sie gespeicherten Daten gemäß § 7 sowie der nach § 7 Abs. 8 erlassenen Betriebsregelungen Grundlage des Nutzungsverhältnisses sind.

5) Kennungsdeaktivierung/Kulanzzeiten

Verliert der/die Nutzende den Status oder die Rolle, auf dessen/deren Basis der Account gewährt wurde, so wird der Account innerhalb von in Betriebsregelungen festzulegenden Fristen deaktiviert.

§ 3 Mapping, Provisionierung, Administration

(1) Mapping

Jedem Nutzendem wird eine eindeutige Identität zugeordnet. Zur Festlegung dieser eindeutigen Identität werden die Daten im Identitätsmanagement – soweit notwendig – konsolidiert.

(2) Provisionierung

Zur Erzeugung von Kennungen auf den zu versorgenden Zielsystemen (z. B.: Active Directory Services) werden in der Regel folgende Daten übertragen:

1) Kennung

2) Passwort
3) Rollen und Rechte
4) Vor- und Zuname und organisatorische Informationen
5) Technische Informationen

Die zurzeit verfügbaren Zielsysteme werden im Identitätsmanagementsystem verwaltet und dokumentiert.

Das ZIV und die IVVen können – soweit erforderlich – weitere Zielsysteme in das Identitätsmanagement aufnehmen.

Bei der gemeinsamen Wahrnehmung von Aufgaben durch mehrere Hochschulen ist eine Datenübertragung aus dem Identitätsmanagement zulässig, wenn dies zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

(3) Schnittstelle für Administratoren

Die Verwaltung im Provisionierungssystem wird im Identitätsmanagementsystem dokumentiert und ist ausschließlich zugelassenen Administratoren vorbehalten. Neben zentralen Administratoren aus der Verwaltung und des ZIV können auch dezentrale Administratoren ernannt werden, die lokale Zielsysteme provisionieren können.

(4) Selbstadministration

Die Selbstadministration ermöglicht es dem/der Nutzenden, sein/ihr informationelles Selbstbestimmungsrecht wahrzunehmen und Einsicht in die über ihn/sie gespeicherten Daten zu nehmen.

Im Rahmen der Selbstadministration können Nutzende ihrerseits ihre Daten in festgelegtem Umfang eigenständig ändern. Der Umfang der Änderungsberechtigung wird im Identitätsmanagementsystem dokumentiert.

§ 4 Ordnungsgemäßer und störungsfreier Betrieb

(1) Die Nutzungsberechtigung sowie der Zugang zu den verschiedenen Zielsystemen kann beschränkt und zeitlich befristet werden.
(2) Zur Gewährleistung eines ordnungsgemäßen und störungsfreien Betriebs kann die Nutzungserlaubnis überdies mit einer Begrenzung der Rechen- und Onlinezeit sowie mit anderen nutzungsbezogenen Bedingungen und Auflagen verbunden werden.
(3) Wenn die Kapazitäten der IV-Ressourcen nicht ausreichen, um allen Nutzungsberechtigten gerecht zu werden, können die Betriebsmittel für die einzelnen Nutzenden entsprechend der Reihenfolge in § 2 Abs. 1 kontingentiert werden.
(4) Die Nutzungserlaubnis oder der Zugang zu bestimmten Zielsystemen kann ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn
1) die persönlichen Voraussetzungen nicht oder nicht mehr zutreffen;
2) die Voraussetzungen für eine ordnungsgemäße Benutzung des IV-Systems nicht oder nicht mehr gegeben sind;
3) die nutzungsberechtigte Person nach § 6 von der Benutzung ausgeschlossen worden ist;
4) das geplante Vorhaben des/der Nutzenden nicht mit den vorgesehenen Aufgaben des IV-Systems und den in § 2 Abs. 2 genannten Zwecken vereinbar ist;
5) die vorhandenen IV-Ressourcen für die beantragte Nutzung ungeeignet, unzureichend o-der für besondere Zwecke reserviert sind;
6) die zu benutzenden IV-Komponenten an ein Netz angeschlossen sind, das besonderen Datenschutzerfordernissen genügen muss und kein sachlicher Grund für die geplante Nutzung ersichtlich ist;
7) zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Vorhaben in unangemessener Weise beeinträchtigt werden.

§ 5 Rechte und Pflichten der Nutzenden

(1) Die Nutzenden haben das Recht, die Einrichtungen des IV-Systems im Rahmen der Zulassung und nach Maßgabe dieser Benutzungsordnung sowie der nach § 7 Abs. 8 erlassenen Regelungen zu nutzen.
Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung.
(2) Die Nutzer sind verpflichtet,
(Allgemein)
1) die Vorgaben der Benutzungsordnung zu beachten und die Grenzen der Nutzungserlaubnis einzuhalten, insbesondere die Nutzungszwecke nach § 2 Abs. 2 zu beachten;

2) alle notwendigen Maßnahmen, die durch das IV- Sicherheitsteam in Abstimmung mit den IV-Ven und dem ZIV festgelegt und den Nutzern rechtzeitig durch E-Mail und durch Einstellung in das Netz zur Kenntnis gebracht wurden, durchzuführen;
3) alles zu unterlassen, was den ordnungsgemäßen Betrieb des IV-Systems der WWU stört;
4) alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen des IV-Systems sorgfältig und schonend zu behandeln;

(Umgang mit Nutzerkennungen)

5) ausschließlich mit den Kennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung und der Provisionierung zugewiesen wurden;
6) dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von den Nutzerpasswörtern erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu den DV-Ressourcen des IV-Systems der WWU verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d. h. nicht einfach zu erratendes Passwort, das möglichst regelmäßig geändert werden sollte;
7) fremde Nutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen;
8) keinen unberechtigten Zugriff auf Informationen anderer Nutzender zu nehmen und bekannt gewordene Informationen anderer Nutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern. Dies gilt auch für den Zugang zu IV-Systemen Dritter über das Wissenschaftsnetz oder das Internet. Bei Zuwiderhandlungen kann der Aus-schluss einzelner Nutzender erfolgen.

(Software- und Hardwarenutzung)

9) bei der Benutzung von Software, Hardware, Dokumentationen und Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten vom ZIV und den IVVen zur Verfügung gestellt werden, zu beachten;
10) vom ZIV oder den IVVen bereitgestellte Software, Dokumentationen und Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als den erlaubten Zwecken zu nutzen;
11) in den Räumen des ZIV und der IVVen den Weisungen des Personals Folge zu leisten und die jeweils in Frage kommende Hausordnung zu beachten;
12) die Nutzungsberechtigung auf Verlangen nachzuweisen;
13) Störungen, Beschädigungen und Fehler am IV-System und an Datenträgern des IV-Systems nicht selbst zu beheben, sondern unverzüglich den Mitarbeitern des ZIV bzw. der zuständigen IVV zu melden;
14) ohne ausdrückliche Einwilligung des ZIV bzw. der IVVen keine Eingriffe in die Hardwareinstallation des IV-Systems vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Netzwerks nicht zu verändern;

(Sonstiges)

15) der Leitung des ZIV bzw. der IVVen auf Verlangen in begründeten Einzelfällen – insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren. Von dieser Regelung werden nicht die Nutzerdaten erfasst, die durch das Telekommunikationsgeheimnis oder das Datengeheimnis geschützt sind, z. B. E-Mails, persönliche Dateien oder personenbezogene Daten Dritter (z. B. Patientendaten).
16) eine Verarbeitung personenbezogener Daten mit dem ZIV bzw. der zuständigen IVV, abzustimmen und - unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen des/der Nutzenden - die vom ZIV bzw. der IVVen vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen;
17) zur Nutzung bereitgehaltene Inhalte (z. B. WWW-Seiten) mit einem Impressum zu versehen, welches auch Namen und Anschrift der für den Inhalt verantwortlichen Person enthält (§ 5 TMG, § 55 Abs. 2 RStV).

(3) Auf die folgenden Straftatbestände wird besonders hingewiesen:
1) Ausspähen von Daten (§ 202a StGB), Abfangen von Daten (§ 202b StGB), Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)
2) Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB)
3) Computerbetrug (§ 263a StGB)
4) Verbreitung pornographischer Darstellungen (§ 184 StGB), insbesondere
5) Verbreitung, Erwerb oder Besitz kinderpornographischer Darstellungen (§ 184b StGB) so-wie Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste (§ 184c StGB)

6) Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB)
7) Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB)
8) Strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG)

§ 6 Ausschluss von der Nutzung

(1) Nutzende können vorübergehend oder dauerhaft in der Benutzung der DV-Ressourcen beschränkt oder hiervon ausgeschlossen werden, wenn sie
1) schuldhaft gegen diese Benutzungsordnung, insbesondere gegen die in § 5 aufgeführten Pflichten, verstoßen (missbräuchliches Verhalten) oder
2) die Ressourcen des IV-Systems für strafbare Handlungen missbrauchen (das gilt auch für Missbrauch anderer Einrichtungen von den IV-Ressourcen der WWU aus) oder
3) der Hochschule durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen.

(2) Maßnahmen nach Abs. 1 sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Bei sehr schwerwiegenden Verstößen ist die Abmahnung im Einzelfall entbehrlich. Dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben. Er kann den Vorsitzenden der IV-Kommission um Vermittlung bitten.

(3) Vorübergehende Nutzungseinschränkungen, über die die Leiterin/der Leiter des ZIV bzw. der zuständigen IVV entscheidet, sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint.

(4) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss eines/einer Nutzenden von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen i. S. v. Abs. 1 in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Die Entscheidung über einen dauerhaften Ausschluss trifft die/der Kanzler(in) auf Antrag des Leiters des ZIV bzw. der IVVen und nach Anhörung der IV-Kommission durch Bescheid. Mögliche Ansprüche des ZIV oder der IVVen aus dem Nutzungsverhältnis bleiben unberührt.

§ 7 Rechte und Pflichten des ZIV und der IVVen

(1) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, können das

(2) ZIV bzw. die IVVen die Nutzung ihrer Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzenden hierüber im Voraus zu unterrichten. Dies gilt auch gegenüber Nutzern, die der Pflicht zur Durchführung der erforderlichen Maßnahmen nach § 5 Abs. 2 Nr. 2 nicht nachkommen. Diese werden nur eingeschränkten Zugang zum Netz und begrenzte Handlungs- und Nutzungsmöglichkeiten der Ressourcen der Universität erhalten.

(3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Nutzender auf den Servern des IV-Systems rechtswidrige Inhalte zur Nutzung bereithält, können das ZIV bzw. die IVVen die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist. Die Einsichtnahme oder Sperrung "normaler" Nutzerdaten, die vom Nutzer nicht zum allgemeinen Abruf freigegeben sind, wird von der vorstehenden Regelung jedoch nicht erfasst.

(4) Das ZIV bzw. die IVVen sind berechtigt, die Sicherheit der System-/Nutzerpasswörter und der Nutzerdaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, z. B. Änderungen leicht zu erratender Passwörter, zu erzwingen, um die Ressourcen des IV-Systems und Nutzerdaten vor unberechtigten Zugriffen Dritter zu schützen. Bei erforderlichen Änderungen der Nutzerpasswörter, der Zugriffsberechtigungen auf Nutzerdatei-en und sonstigen nutzungsrelevanten Schutzmaßnahmen ist der/die Nutzende hiervon unverzüglich in Kenntnis zu setzen.
Das ZIV bzw. die IVVen sind nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme des IV-Systems durch die einzelnen Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist
1) zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2) zur Ressourcenplanung und Systemadministration,
3) zum Schutz der personenbezogenen Daten anderer Nutzender,
4) zu Abrechnungszwecken,
5) für das Erkennen und Beseitigen von technischen Störungen und Fehlern sowie
6) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung bei Vorliegen von tatsächlichen Anhaltspunkten. Diese sind schriftlich zu dokumentieren.

Unter den Voraussetzungen von Abs. 4 sind das ZIV und die IVVen auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die Benutzerdateien zu nehmen, soweit dies erforderlich ist zur

Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen, sofern hierfür tatsächliche Anhaltspunkte vorliegen.
Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist.
In jedem Fall ist die Einsichtnahme zu dokumentieren, und der betroffene Benutzer ist nach Zweckerreichung unverzüglich zu benachrichtigen.

(5) Unter den Voraussetzungen von Absatz 4 können auch die Verbindungs- und Nutzungsdaten im Nachrichtenverkehr (insbesondere E-Mail-Nutzung) dokumentiert werden. Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nicht-öffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden.

(6) Die Verbindungs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Teledienste, die das ZIV oder die IVVen zur Nutzung bereithalten oder zu denen sie den Zugang zur Nutzung vermitteln, sind frühest möglich zu löschen, soweit es sich nicht um Abrechnungsdaten handelt.

(7) Nach Maßgabe der gesetzlichen Bestimmungen ist das Personal des ZIV und der IVVen zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.

(8) Zur Gewährleistung eines ordnungsgemäßen Betriebs des IV-Systems kann die Leitung des ZIV bzw. der IVVen weitere Regelungen für die Nutzung des IV-Systems im jeweiligen Zuständigkeitsbereich erlassen.

§ 8 Haftung des/der Nutzenden

(1) Der/die Nutzende haftet für alle Nachteile, die der Universität durch missbräuchliche oder rechtswidrige Verwendung der Ressourcen des IV-Systems und ihre Nutzungsberechtigung oder dadurch entstehen, dass der/die Nutzende schuldhaft seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt.

(2) Der/die Nutzende haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er/sie diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner Benutzerkennung an Dritte. In diesem Fall kann die WWU vom Nutzer nach Maßgabe der Entgeltordnung ein Nutzungsentgelt für die Drittnutzung verlangen.

(3) Der/die Nutzende hat die Hochschule von allen Ansprüchen freizustellen, wenn durch Dritte die WWU wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des/der Nutzenden auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch genommen wird. Die WWU wird dem/der Nutzenden den Streit erklären, sofern Dritte gegen das ZIV oder die IVVen gerichtlich vorgehen.

§ 9 Haftung der Hochschule

(1) Die WWU übernimmt keine Garantie dafür, dass das IV-System fehlerfrei und jederzeit ohne Unterbrechung läuft. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

(2) Die WWU übernimmt keine Verantwortung für die Fehlerfreiheit der zur Verfügung gestellten Programme. Die WWU haftet auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(3) Im Übrigen haftet die WWU nur bei Vorsatz oder grober Fahrlässigkeit ihres Personals, es sei denn, dass eine schuldhafte Verletzung wesentlicher Kardinalpflichten vorliegt. In diesem Fall ist die Haftung der WWU auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt.

(4) Mögliche Amtshaftungsansprüche gegen die WWU bleiben von den vorstehenden Regelungen unberührt.

§ 10 Inkrafttreten

Diese Benutzungsordnung tritt mit ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Westfälischen Wilhelms-Universität Münster am Tage nach Aushang in Kraft.

Ausgefertigt aufgrund des Beschlusses des Senats der Westfälischen Wilhelms-Universität vom 10. November 2010

Münster, den 15. November 2010

Die Rektorin

Prof. Dr. U. Nelles

Die vorstehende Ordnung wird gemäß der Ordnung der Westfälischen Wilhelms-Universität über die Verkündung von Ordnungen, die Veröffentlichung von Beschlüssen sowie die Bekanntmachung von Satzun-

gen vom 8.2.1991 (AB UNI 91/1), geändert durch die Ordnung vom 23.12.1998 (AB Uni 99/4), hiermit verkündet.

Münster, den 15. November 2010

Die Rektorin

Prof. Dr. U. Nelles

Anlage zu § 2 Abs. 3

Kennungen werden in der Regel automatisiert aus den Daten, die in den Personenverzeichnissen der Einrichtungen der Universität geführt werden, erzeugt. (Pflichtfelder sind durch * gekennzeichnet.)

(1) Anlage Mitarbeiter
Für Mitarbeiter werden hierbei folgende Daten in das Identitätsmanagementsystem übertragen:

- Ordnungsnummer (Kennung) *
- Personenstatus *
- Nachname *
- Vorname *
- Geburtsdatum *
- Geburtsort *
- Geschlecht *
- Titel
- Straße, Hausnummer
- Postleitzahl
- Ort
- Land/Wohnort
- Personalnummer *
- Kategorie des Beschäftigungsverhältnisses *
- Enddatum des Beschäftigungsverhältnisses *
- Einrichtung * (multivalue)
- Telefon (dienstlich) *
- Kostenstelle
- Bankverbindung
- Bankleitzahl
- Kontonummer

(2) Anlage Studierende
Für Studierende werden hierbei folgende Daten in das Identitätsmanagementsystem übertragen:

- Ordnungsnummer (Kennung) *
- Personenstatus *
- Nachname *
- Vorname *
- Geburtsdatum *
- Geburtsort *
- Geschlecht *
- Titel
- Straße, Hausnummer *
- Postleitzahl *
- Ort *
- Land/Wohnort *
- Telefonnummer (privat)
- Kontakt E-Mail
- Matrikelnummer *
- Studierendenstatus *
- Studiengang * (multivalue)
- Einschreibedatum *
- Einrichtung

Anhang B | Regelungen zur IV-Sicherheit in der Universität Münster

Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren in NRW (ARNW)

Erstellt von

› W. A. Franck, Aachen
› B. Wojcieszynski, Bochum
› H. Ziegler, Dortmund
› W. Held und St. Ost, Münster
› J. W. Münch, Siegen

21.02.2002 (geändert am 15.01.2004)

Präambel und Geltungsbereich

Diese Regelungen gelten für die IV in der Universität, d.h. für alle technischen Kommunikationssysteme, alle vernetzten Rechner, die als Server und am Arbeitsplatz genutzt werden, alle eingesetzten Softwareprodukte und alle gespeicherten oder zu bearbeitenden Daten[66]. Sie umfassen auch verpflichtende Verhaltensmaß-nahmen aller Nutzer und Nutzerinnen der IV sowie aller Mitarbeiterinnen und Mitarbeiter, die IV-Leistungen bereitstellen.

Forschung und Lehre sind von der verlässlichen Nutzung der IV, insbesondere des Internets als modernem Lehr-, Informations- und Kommunikationsmedium, zunehmend abhängig geworden. Folglich entsteht daraus ein hoher Anspruch an Betriebsstabilität und Verfügbarkeit. Bedingt durch Schwachstellen im Internet, in den verwendeten Betriebssystemen und Programmen sowie durch fehlerhafte Konfiguration von Servern und Rechnern an Arbeitsplätzen oder durch fehlende Redundanzen sind vernetzte IV-Ressourcen erheblichen Gefährdungen ausgesetzt.

Ein Universitätsnetz bietet wegen der Heterogenität seiner Systeme und der verteilten Verantwortlichkeiten ein besonders breites Angriffsspektrum. Neben Angriffen von außen auf Systeme der Universität haben Attacken von innen einen besonderen Stellenwert. Die Auswirkungen eines Einbruchs in das Intranet einer Universität reichen vom Ausfall einzelner Endsysteme oder Server bis hin zum Zusammenbruch des gesamten Netzes. Der Lehr- und Forschungsbetrieb kann dadurch in erheblichem Maße auch längerfristig behindert werden. Das Ausspähen von schutzwürdigen Forschungsdaten stellt i. Allg. einen erheblichen immateriellen, teilweise auch finanziellen Schaden dar. Der Schutz personenbezogener Daten gegen unbefugten Zugriff muss gewährleistet sein. Erfolgt ein Angriff aus dem Intranet der Universität gegen fremde Systeme, so sind Schadensersatzforderungen nicht auszuschließen. Nicht bezifferbar ist der Imageverlust, der entsteht, wenn eine Universität in einen Störfall verwickelt worden ist.

Die Sicherheit der IV kann daneben durch Stromunterbrechungen, Feuer, Blitzschlag, technische Defekte, Diebstahl, Sabotageakte und Zerstörung von Geräten gefährdet werden. Gefährdungen entstehen auch durch Fehler oder Nachlässigkeiten von Mitarbeiterinnen/Mitarbeitern sowie durch die Inanspruchnahme externer Personen.

Diese Regelungen zur IV-Sicherheit sollen das Gefahrenpotential mindern. Angestrebt wird ein für die Universitäten in NRW verbindliches Zertifikat für die IV-Sicherheit.

§ 1 Gefahrenanalyse

Grundlage der Sicherheitsregelungen ist eine Gefahrenanalyse, die festhält, welche Kommunikationssysteme, Server, Arbeitsstationen, Software und schutzwürdige Daten vorhanden und welchen Gefahren diese Bestände bezüglich Vertraulichkeit, Integrität und Verfügbarkeit (Sicherheitsniveau) ausgesetzt sind[67].

§ 2 Betriebsregelungen

(1) Kommunikationssysteme (Variante **A gilt in der WWU**)[68] Alle Kommunikationssysteme (campus-

(1) Kommunikationssysteme (Variante **B, gilt nicht in der WWU**) Alle Kommunikationssysteme (campus-

[66] Der Einsatz dieser Ressourcen wird zusammenfassend Informationsverarbeitung (IV) genannt.
[67] Da die Implementierung von Schutzmaßnahmen Zeit, Mühe und Geld erfordert, ist eine realistische Abschätzung des Schutzbedarfs (Sicherheitsniveau) sehr wichtig; zur Erleichterung kann dafür die Anlage „Festlegung des Sicherheitsniveaus“ verwendet werden.
[68] Variante A bzw. Variante B sind in Abhängigkeit von der Organisation der IV in den Universitäten zu wählen.

weites LAN, WAN, Einwahleinrichtungen usw.) werden ausschließlich vom Zentrum für Informationsverarbeitung (ZIV) betrieben. Eigene LAN-Installationen und unerlaubte Betriebsformen dürfen von Dritten nicht vorgenommen werden. Alle an das Kommunikationssystem anzuschließenden Endgeräte außerhalb von besonders ausgewiesenen Netzbereichen, die eine netzbasierte Authentifizierung erlauben (z. B. VPN) sind anzumelden[69]. Neben den zentral bereitgestellten Netzzugängen (z. B. Einwahlzugängen) dürfen keine weiteren geschaffen werden[70]. Spezielle Netzzugänge sind mit dem ZIV abzustimmen.

weites LAN, WAN, Einwahleinrichtungen usw.) werden ausschließlich vom Hochschulrechenzentrum (HRZ) betrieben. An definierten Übergabepunkten kann die Verantwortung für das örtliche LAN einer universitären Einrichtung an diese übergehen, wenn der Betrieb, die Nutzung, der Zugang und das Diensteangebot nach den Vorgaben des HRZ erfolgen. Neben den zentral bereitgestellten Einwahlzugängen dürfen keine weiteren geschaffen werden. Spezielle Netzzugänge (z. B. Funk-LAN-Einrichtungen) sind mit dem HRZ abzustimmen.

Sofern in einer Universität eine Netzordnung (z. B. auch Datendiensteordnung genannt) existiert, findet diese vorrangig Anwendung[71].

(2) Server-Betrieb und Rechner-Pools

Im LAN der Universität kann grundsätzlich jedes Institut eigene Server betreiben. Der Betrieb derartiger Server, deren Dienstleistungsangebot wie z. B. E-Mail-Server und Web-Server nicht nur auf das eigene Intranet angelegt ist, wird nur bei begründetem Bedarf zugelassen[72]. Gegebenenfalls sind entsprechende Server ohne begründbaren Bedarf in das ZIV bzw. die zuständigen IV-Versorgungseinheiten (IVV) zu verlagern. Alle Server müssen in besonderer Weise dauerhaft und regelmäßig gepflegt werden[73]. Server mit besonderem Verfügbarkeitsbedarf sind besonders vor dem Zugang Unbefugter zu sichern. Sicherheitsrelevante Dienste sind auf einige wenige und besonders gut gepflegte Server zu konzentrieren.

Zu jedem Server sind ein verantwortlicher Administrator sowie ein Stellvertreter als technisch Verantwortliche zu benennen, die in Notfällen erreichbar sind. Die Zuweisung der Administrator-Funktion muss schriftlich erfolgen[74]. Administratoren und ihre Vertreter müssen mindestens einen ausführlichen Lehrgang für Administratoren oder eine gleichwertige Ausbildung absolviert oder eine ausreichende berufliche Praxis im Umgang mit Betriebssystemen haben; sie sollen regelmäßig auch im Bereich der IV-Systeme arbeiten. Sie müssen sich verpflichten, ständig die Diskussion um Sicherheitslücken[75] zu verfolgen und sich entsprechend weiterzubilden. Der Administrator und seine Vertreter haben neben der Administratorkennung jeweils eine "gewöhnliche" persönliche Benutzerkennung, unter der Standardaufgaben durchgeführt werden, sie arbeiten nur dann unter der Administratorkennung, wenn die Administratorrechte benötigt werden.

Beim Betrieb von Rechnerpools ist dafür Sorge zu tragen, dass kein unberechtigter Benutzer Zugang erhält. Anonyme Zugänge sind in der Regel zu unterbinden. Endgeräte, für die aus zwingenden Gründen ausnahmsweise ein anonymer Zugang zu einem Server im Intranet erlaubt werden muss, sind durch technische Maßnahmen in ihrem Funktionsumfang so einzuschränken, dass Beeinträchtigungen der IV-Sicherheit nicht möglich sind.

Verantwortliche für den Betrieb von Servern oder Pools sind verpflichtet, die vom Sicherheitsteam (gemäß § 5) vorgegebenen Sicherheitsstandards bei der Konfiguration der Rechner zu beachten und dem Sicherheitsteam alle sicherheitsrelevanten Vorfälle zu melden.

(3) Verantwortung der Benutzer

Benutzer sind verpflichtet, die Vertraulichkeit von Passwörtern zu wahren. Jeder Endanwender trägt persönliche Verantwortung für den gewissenhaften Umgang mit den Informationen, die auf seiner Arbeitsstation verarbeitet werden. Der Endanwender ist verpflichtet, sich über mögliche Sicherheitsrisiken zu informieren.

Rechner, die im Festnetz betrieben werden, sind über die zuständige IVV im ZIV anzumelden.

---

[69] Dadurch sollen Betriebsstörungen durch Leitungsengpässe und andere Sicherheitsfragen rechtzeitig gelöst werden.
[70] Sie stellen ein hohes Gefährdungspotenzial dar.
[71] Bereits existierende Ordnungen und Regelungen sind widerspruchsfrei zu den vorliegenden Regelungen zu gestalten.
[72] Sie stellen ebenfalls ein hohes Gefährdungspotential dar.
[73] Etwa durch das aktuelle Einspielen von Updates und Sicherheitspatches.
[74] Beispielsweise im Geschäftsverteilungsplan.
[75] Informationen sind z. B. unter https://www.cert.dfn.de/ zu finden.

Benutzer sind verpflichtet, die vom Sicherheitsteam (gemäß § 5) vorgegebenen Sicherheitsstandards bei der Konfiguration ihrer Rechner zu beachten und dem Sicherheitsteam alle sicherheitsrelevanten Vorfälle zu melden.

Für jedes an das Kommunikationssystem angeschlossene Endgerät ist ein technisch Verantwortlicher zu benennen.

Zur deutlichen Verbesserung der IV-Sicherheit und damit zur möglichst weitreichenden Vermeidung von Schäden in der Universität, wird die Nutzung von IV-Arbeitsplatzsystemen im/am Netz der Universität durch Regelungen und Verpflichtungen, die mit Durchsetzungsrechten und Reglementierungen verbunden sind, abgesichert. Notwendige Maßnahmen werden den technischen Entwicklungen folgend durch das IV-Sicherheitsteam in Abstimmung mit den Informationsverarbeitungsversorgungseinheiten und dem ZIV festgelegt und der IV-Kommission zur Kenntnis gebracht. Die Benutzer der IV-Arbeitsplatzsysteme werden auf elektronischem Wege (Veröffentlichung auf den zentralen Webservern der Universität, der IVVen und per E-Mail) von den erforderlichen Maßnahmen rechtzeitig in Kenntnis gesetzt. Wer den durch das IV-Sicherheitsteam angeordneten Maßnahmen und Verpflichtungen nicht nachkommt, wird nur eingeschränkte Zugänge zum Netz und begrenzte Handlungs- und Nutzungsmöglichkeiten der Ressourcen der Universität erhalten.

(4) Verantwortung der Leiterin/Leiter der Organisationseinheiten

Die Leiterin/der Leiter der Organisationseinheiten der Universität sind verpflichtet, sich über die geltenden Sicherheits- und Betriebsregelungen zu informieren. Sie sind für die operative Umsetzung der Richtlinien in ihrem Zuständigkeitsbereich verantwortlich.

(5) Schutz personenbezogener Daten und weitere Einzelmaßnahmen

Werden personenbezogene Daten auf vernetzten Servern bearbeitet, so sind diese durch zusätzliche technische Maßnahmen zu schützen; der Datentransfer zu solchen Servern sollte verschlüsselt erfolgen. Arbeitsstationen, auf denen besonders schutzwürdige Daten verarbeitet werden, müssen über ein Passwort vor unberechtigtem Zugriff geschützt werden. Sofern PCs im Netzwerk mit einer Festplatte ausgestattet sind, dürfen auf der Festplatte keine personenbezogenen Daten gespeichert werden. Personenbezogene Daten dürfen nur auf Servern gespeichert werden. Gegebenenfalls sind die Daten zu verschlüsseln. Für die Speicherung und Verarbeitung personenbezogener Daten sind außerdem die geltenden Datenschutzgesetze sowie die örtlichen Dienstvereinbarungen zu beachten.

Weitere aus den Ziffern (1) bis (4) folgende Einzelmaßnahmen werden vom Sicherheitsteam (gemäß § 5) nach Abstimmung mit den IVVen zusammengestellt und über das ZIV der Universitätsleitung vorgeschlagen und nach deren Zustimmung als Betriebsregelungen verbindlich gemacht[76].

§ 3 Zuwiderhandlungen

Server, Pools und Arbeitsplatzsysteme, die nicht den Sicherheitsregelungen entsprechend betrieben werden, können vom ZIV bzw. den IVVen vom Netz genommen werden. Zur Abwehr akuter schwerwiegender Störungen oder Gefahren können Server, Pools und Arbeitsplatzsysteme darüber hinaus gehend vorübergehend vom Netz genommen werden. Nutzerinnen und Nutzern, die gegen diese Regelungen verstoßen, kann vom ZIV bzw. der zuständigen IVV vorübergehend die Nutzungsberechtigung entzogen werden. Bei sehr schweren Verstößen gegen die Sicherheitsregelungen kann die Universitätsleitung eine dauerhafte Trennung vom Netz bzw. den dauerhaften Ausschluss von der Nutzung verfügen. Zuwiderhandlungen können darüber hinaus Verstöße u. a. gegen das Strafgesetzbuch (StGB), das Sozialgesetzbuch (SGB), das Landes- und Bundesdatenschutzgesetz, das Teledienstgesetz sowie, für Kliniken wichtig, das Landeskrankenhausgesetz darstellen.

Zusatzaufwand, der durch Zuwiderhandlungen entsteht, wird kostenpflichtig in Rechnung gestellt.

§ 4 Sicherheitsteam

Zur Erarbeitung und Umsetzung der Sicherheits- und (den daraus abgeleiteten) Betriebsregelungen wird ein Sicherheitsteam eingerichtet[77]. Zu seinen Aufgaben gehören:

---

[76] Betriebsregelungen werden im WEB unter https://www.uni-muenster.de/ZIV/DasZIV/Ordnungen/index.html veröffentlicht. Betriebsregelungen können unterschiedliche Gewichtung haben; für Systeme mit besonderem Schutzbedarf ist die Umsetzung einiger Regelungen verbindlich zu machen, während dieselbe Regelung für weniger wichtige Systeme möglicherweise nur empfehlenden Charakter hat. Ebenso sind Regelungen, die Auswirkungen auf das gesamte Netzwerk haben, bindend von allen Benutzern zu befolgen.

- Definition wirksamer Sicherheitsstandards und Betriebsregelungen (gemäß § 3) in Abstimmung mit den IVVen.
- Landesweite Abstimmung der Sicherheitsstandards und Betriebsregelungen.
- Überwachung der Umsetzung der Sicherheitsstandards. Dazu können in den Einrichtungen der Universität Sicherheits-Überprüfungen vorgenommen werden.
- Aufstellung eines Ausbildungs- und Schulungskonzepts zur IV-Sicherheit für BenutzerInnen, Administratoren und Mitglieder des Sicherheitsteams, das auch für die Maßnahmen zur Verbesserung der IV-Sicherheit sensibilisieren soll.
- Ansprechpartner für alle sicherheitsrelevanten Fragen.
- Entgegennahme und Dokumentation aller sicherheitsrelevanten Vorfälle, die zusätzlich an externe Stellen (z. B. das DFN-CERT) zu berichten sind.
- Zusammenstellung der jährlichen Finanzbedarfe und Vorbereitung des jährlichen Berichts.

Die Geschäftsstelle des Sicherheitsteams wird beim ZIV eingerichtet.

Die Kontrolle der Sicherheitsmaßnahmen und des Sicherheitsteams wird durch eine Evaluierung zwischen den Hochschulrechenzentren erfolgen.

§ 5 Notfallvorsorge

Ein Notfallkonzept für akute Störfälle und den geordneten Betrieb nach Beseitigung der Störungen ist bekannt zu geben. Dazu sind zwingend erforderlich:

- Ein einfacher Benachrichtigungsplan für Probleme und Notfälle, der allen NutzerInnen zugänglich ist.
- Ein detaillierter Notfallplan, der innerhalb des ZIV bzw. innerhalb der IVV der Einrichtungen zum internen Dienstgebrauch verwendet wird.
- Informationen zu Administratoren und deren Stellvertretern, die in Notfällen benachrichtigt werden müssen.
- Backup-Konzepte für wichtige Server und Komponenten der Kommunikationssysteme, die regelmäßig zu überprüfen sind.
- Katastrophensichere Konzepte zur Aufbewahrung von Daten (Backup, Archivierung usw.).

§ 6 Personalbedarf und Haushaltsmittel

Das ZIV fasst die vom Sicherheitsteam genannten und mit den IVVen abgestimmten personellen und sachlichen Haushaltsbedarfe für alle vorhandenen Maßnahmen zur Sicherheit der IV in der Universität zusammen und meldet den begründeten Bedarf für das jeweils nächste Haushaltsjahr im Rahmen der Haushaltsanmeldung an. Dabei berichtet es über die Verwendung der entsprechenden Mittel im vorherigen Haushaltsjahr.

§ 7 Inkrafttreten

Diese Regelungen zur IV-Sicherheit treten mit ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Universität am Tage nach Aushang in Kraft.

Ausgefertigt aufgrund des Beschlusses des IV-Lenkungsausschusses vom 31.1.2002 und Genehmigung des Rektorats der Westfälischen Wilhelms-Universität Münster vom 21.02.2002.

Münster, den 16. April 2002

Der Rektor

Prof. Dr. J. Schmidt

Die vorstehende Ordnung wird gemäß der Ordnung der Westfälischen Wilhelms-Universität über die Verkündung von Ordnungen, die Veröffentlichung von Beschlüssen sowie die Bekanntmachung von Satzungen vom 08. Februar 1991 (AB Uni 91/1), geändert am 23. Dezember 1998 (AB Uni 99/4), hiermit verkündet.

Münster, den 18. April 2002

Der Rektor

---

[77] Es könnten z. B. zwei Mitarbeiterinnen/Mitarbeiter aus dem ZIV (einmal Abteilung Kommunikationssysteme und einmal Abteilung Betriebssysteme) und ein Mitarbeiterin/Mitarbeiter aus der Abteilung, die für die Datenverarbeitung der Universitätsverwaltung zuständig ist, mitwirken; bei Bedarf müssen weitere Personen hinzu gezogen werden.

Prof. Dr. J. Schmidt

Anlage: Festlegung der Sicherheitsniveaus

Zur Festlegung der Sicherheitsniveaus in den IVVen hat das Sicherheitsteam Kriterien aufzustellen. Hierzu sind die vier vom BSI vorgeschlagenen Sicherheitsniveaus a) bis d) hilfreich. Die Einschätzung und Einordnung der Sicherheitsbedürfnisse ist weitgehend intuitiv; eine Objektivierung ist schwierig.

Die Zuordnung zu einem Sicherheitsniveau

a) Maximales Sicherheitsniveau

› Der Schutz vertraulicher Informationen muss gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen.
› Die Informationen müssen im höchsten Maße korrekt sein.
› Die zentralen Aufgaben der Institution sind ohne IV-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.

Insgesamt gilt: Der Ausfall der IV führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

b) Hohes Sicherheitsniveau

› Der Schutz vertraulicher Informationen muss hohen gesetzlichen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein.
› Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkenn-bar und vermeidbar sein.
› In zentralen Bereichen der Institution laufen zeitkritische Vorgänge oder es werden dort Massenaufgaben wahrgenommen, die ohne IV-Einsatz nicht zu erledigen sind; es können nur kurze Ausfallzeiten toleriert werden.

Insgesamt gilt: Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.

c) Mittleres Sicherheitsniveau

› Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
› Kleinere Fehler können toleriert werden. Fehler, welche die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkennbar oder vermeidbar sein.
› Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.

Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

d) Niedriges Sicherheitsniveau

› Vertraulichkeit von Informationen ist nicht gefordert.
› Fehler können toleriert werden, solange sie die Erledigung der Aufgaben nicht völlig unmöglich machen.
› Dauernder Ausfall ist zu vermeiden, längere Ausfallzeiten sind jedoch hinnehmbar.

Insgesamt gilt: Schäden haben nur eine unwesentliche Beeinträchtigung der Institution zur Folge.

Bei der Festlegung des Sicherheitsniveaus können die folgenden Fragen und Zusatzfragen hilfreich sein:

Fragen:

› Welche Bedeutung hat die Vertraulichkeit der Informationen aus der IV für Ihren Bereich? Was geschieht, wenn die Vertraulichkeit verletzt wird?
› Welche Bedeutung hat die Verfügbarkeit, Richtigkeit und Aktualität der Informationen für Ihren Bereich? Was ist, wenn die Informationen zeitweise nicht zur Verfügung sind? Was geschieht, wenn sie dauerhaft verschwunden sind? Hängen wichtige Entscheidungen von den Informationen ab?
› Gibt es Aufgaben, die nur mit der Unterstützung der IV möglich sind?
› Gibt es Informationen, die einen großen Anreiz auf mögliche Täter ausüben könnten? Könnten die Informationen einem potentiellen Täter finanzielle oder andere Vorteile verschaffen?

Zusatzfragen:

Wichtig wären für die jeweils vorzuschlagenden Schutzmaßnahmen noch die Antworten zu der Frage, wo im jeweiligen Bereich besondere Gefährdungspunkte gesehen werden:

› An Rechnern der Arbeitsplätze?

- An Servern der dezentralen IVVen?
- An Servern des ZIV?
- Im LAN?
- In der Verbindung des LAN mit dem GWIN-Zugang?
- In der Verbindung des LAN mit Einwahlleitungen? Gibt es solche (außerhalb der Einwahlleitungen des ZIV) auch im jeweiligen Bereich?
- Werden im jeweiligen Bereich Kommunikationssysteme (E-Mail, WWW, FTP usw.) ein-gesetzt?
- Gibt es im jeweiligen Bereich besondere Sicherheitslöcher? Sind dort bereits konkrete Gefährdungen beobachtet worden?

Anhang C | Betriebsregelung für das Datennetz der Universität Münster

Anmerkung: Die Betriebsregelung für das Datennetz der WWU Münster in der Fassung vom September 1993, insbesondere aber auch die im gleichen Zusammenhang entstandenen Detailregelungen für den Zugang zum Datennetz der WWU nehmen in ihrem Wortlaut naturgemäß Bezug auf damals aktuelle Technologien. Durch den raschen Wandel der Technik ist in einigen Fällen eine sinngemäße Anwendung der Regelungen erforderlich. Insbesondere hinsichtlich der Details zur LAN-Technik kann eine Rückfrage beim Universitätsrechenzentrum oder die Beachtung der Web-Seiten zum Rechnernetz der WWU ratsam sein.

4. Februar 1998, Georg Richter

Einordnung

(1) Das Datennetz (DANE) ist eine zentrale, nachrichtentechnische Infrastruktureinrichtung der WWU Münster. Es dient der allgemeinen Datenkommunikation und ist anderen Infrastrukturmaßnahmen, wie z. B. Elektrizitätsversorgung, Wasserversorgung, Telefon, gleichgestellt. Es wird vom Universitätsrechenzentrum im Sinne der Verwaltungs- und Benutzungsordnung für das Universitätsrechenzentrum vom 7. Juni 1993 sowie der „Organisation der DV-Nutzung in der Westfälischen Wilhelms-Universität (Stand 26.09.1991)“ betrieben.

(2) Das Datennetz ist eine komplexe technische Einrichtung, die nur bei hohen Anforderungen an die Sorgfalt und das Wissen geplant, installiert, betrieben, gewartet und repariert werden kann. Daher wird diese Betriebsregelung nach § 3 Ziffer 2 der Verwaltungsordnung erlassen. Sie tritt am 1. September 1993 in Kraft.

Begriffsbestimmungen und Anschluss von Geräten

(1) Das Datennetz umfasst alle Übertragungseinrichtungen (Kabel, Vermittler usw.) einschließlich der Anschlusspunkte für Endgeräte. Ausgenommen davon sind Übertragungseinrichtungen in der Zuständigkeit anderer Stellen (z. B. das Telefonnetz). Das Datennetz beruht auf den Standards IEEE 802.3 (10 Base 5 und FOIRL) und ANSI X.3 T95, d. h. Ethernet und FDDI; der Einsatz herkömmlicher Techniken wird entsprechend schrittweise ersetzt. Das Datennetz hat Verbindungen zum Wissenschaftsnetz (WIN) und öffentlichen Netzen (z. B. Telex, Telefax).

(2) Das Datennetz wird einschließlich der Anschlusspunkte im Rahmen der verfügbaren zentralen (Bau-) Mittel bereitgestellt und betrieben. Die im Rechner erforderlichen Hardware- und Software-Komponenten sind von dessen Betreiber zu finanzieren.

(3) Das Datennetz erlaubt durch Einsatz geeigneter Kopplungseinrichtungen (z. B. Bridges) eine Strukturierung und bietet dabei eine transparente, wahlfreie und leistungsfähige Kommunikation aller Teilnehmer untereinander. Von Einrichtungen selbständig betriebene Netze, die am Übergabe-punkt z. B. durch Router an das Datennetz angekoppelt werden können, sind nicht Teil dieses Datennetzes. Auf Router kann nur verzichtet werden, wenn der Netzbetrieb nicht gestört wird, für das Universitätsrechenzentrum keine nennenswerte Mehrbelastung entsteht und keine Hard- und Software eingesetzt wird, die geeignet wäre, den Informationsfluss im Datennetz zu beobachten oder mitzulesen.

(4) Kommunikation ist nur möglich, wenn die eingesetzten Protokolle bei Sender und Empfänger gleich sind. Die Protokollvielfalt ist auf das unbedingt notwendige Maß zu begrenzen, damit die Kommunikation technisch erleichtert und die Komplexität so gering wie möglich gehalten wird. Insbesondere sollte die Verwendung unterschiedlicher Protokolle für vergleichbare Leistungen möglichst vermieden werden. Unter Umständen können Netze entstehen, die wie unter 2(c) selbständig betrieben werden müssen und über Router mit dem Datennetz verbunden werden können.

(5) Der Anschluss von Rechnern oder anderen Endgeräten, die vom Nutzer korrekt zu konfigurieren sind, erfolgt auf Antrag durch das Universitätsrechenzentrum im Rahmen der technischen Möglichkeiten. Änderungen (z. B. Austausch des Rechners) sind dem Universitätsrechenzentrum unverzüglich anzuzeigen.

(6) Die Anschlusspunkte dürfen nur vom Universitätsrechenzentrum oder in dessen Auftrag eingerichtet oder verändert werden. Rechner dürfen nur an den Anschlusspunkten betrieben werden, für die eine Nutzungserlaubnis besteht.

(7) Wird der Netzbetrieb über einen Anschlusspunkt oder ein angeschlossenes Endgerät gefährdet, unzumutbar behindert oder gestört, so kann das Universitätsrechenzentrum geeignete Auflagen machen oder die Anschlussstrecken stilllegen.

Verpflichtungen des Universitätsrechenzentrums

(1) Das Universitätsrechenzentrum ist verpflichtet, einen sicheren und ununterbrochenen Netzbetrieb zu gewährleisten. Nicht vermeidbare Störungen sind auf ein Minimum zu beschränken.
(2) Das Universitätsrechenzentrum vergibt die Netzadressen, ist für das Netzwerkmanagement zuständig, berät in Fragen der Nutzung des Datennetzes und sorgt für eine Dokumentation des Netzes und seiner Nutzungsmöglichkeiten.
(3) Die verfügbaren und einsetzbaren Netzdienste und Protokolle werden vom Universitätsrechenzentrum bekanntgemacht. Kosten, die durch Einsatz anderer Protokolle eventuell entstehen, gehen dabei in jedem Fall zu Lasten der einsetzenden Einrichtung, die auch dafür zu sorgen hat, dass der übrige Netzbetrieb nicht gestört wird.
(4) Das Universitätsrechenzentrum übernimmt keine Verantwortung für Beeinträchtigungen, die über das Datennetz an die angeschlossenen Rechner herangetragen werden.
(5) Das Universitätsrechenzentrum sorgt für einen angemessenen Ausbau des Datennetzes.
(6) Das Universitätsrechenzentrum hat dafür Sorge zu tragen, dass nur seine besonders verpflichteten Mitarbeiter bei Fehlererkennung, Fehlerverfolgung und Netzverwaltung eingesetzt werden.

Verpflichtungen der Benutzer

(1) Für jeden an das Datennetz angeschlossenen Rechner ist dem Universitätsrechenzentrum ein technisch Verantwortlicher zu benennen.
(2) Bei der Übermittlung von Daten ist zu beachten, dass Dritte insbesondere durch Missbrauch mithören könnten. Der Benutzer hat bei der Datenübertragung die Datenschutzgesetze zu beachten. „Mithören“, Ausspionieren und Aufzeichnen fremder Daten aus dem Datennetz sowie das Stören der Kommunikation sind verboten. Davon ausgenommen sind Maßnahmen der Fehlerverfolgung durch das Universitätsrechenzentrum. Benutzer oder Dritte dürfen keine Modifikationen am Datennetz vornehmen. Identifikationsmerkmale von Rechnern (Netzadressen, Namen usw.) dürfen nicht verändert werden.
(3) Bei den an das Datennetz angeschlossenen Rechnern obliegt der Schutz vor unberechtigtem Zugang und unberechtigtem Zugriff auf gespeicherte Daten dem jeweiligen Rechner-Betreiber. Der Benutzer darf aus dem Datennetz nur diejenigen Daten auf seinen Rechner leiten, die für ihn bestimmt sind. Beschaffung und Einsatz von Geräten und Programmen, die einen Missbrauch ermöglichen, sind unzulässig.
(4) Der Benutzer ist verpflichtet, dem Universitätsrechenzentrum Unregelmäßigkeiten, Störungen und Missbrauchsversuche anzuzeigen.
(5) Der Datenverkehr eines Benutzers darf den anderer Benutzer nicht unangemessen beeinträchtigen. Der Einsatz besonders netzbelastender Übertragungen ist mit dem Universitätsrechenzentrum abzustimmen. Das Datennetz darf nicht zur Überwachung oder Leistungskontrolle von Mitarbeitern verwendet werden.
(6) Ein Verstoß gegen diese Betriebsregelung gilt unbeschadet weitergehender Gesetze (z. B. in Analogie zum Fernmeldegesetz) auch als Missbrauch im Sinne des § 8 der Verwaltungs-und Benutzungsordnung.

Technische Detailregelungen

Detailregelungen für den Zugang zum Datennetz der WWU, die weitergehende technische Randbedingungen festlegen, sind in einem gesonderten Papier beschrieben und werden dem Bedarf entsprechend fortgeschrieben.

Münster, 1. September 1993

Anhang D | Die/der Technisch Verantwortliche für vernetzte IV-Systeme an der Universität Münster

vom 08. Juni 2004

Aufgrund des § 2 Abs. 4 des Gesetzes über die Hochschulen des Landes Nordrhein- Westfalen (Hochschulgesetz - HG) vom 14. 2000 (GV.NW. S. 190), zuletzt geändert durch das Gesetz vom 28. Januar 2003 (GV.NW. S. 36 und des Artikels 73 Abs. 1 der Verfassung der Westfälischen Wilhelms-Universität in der Fassung der Bekanntmachung vom 25. März 2002 (AB Uni 2002 Nr. 3) hat die Westfälische Wilhelms- Universität Münster die folgende Ordnung erlassen:

§ 1 Bestellung einer/s Technisch Verantwortlichen

(1) In Ausführung der Regelungen zur IV-Sicherheit in der Universität Münster, hier insbesondere § 3 (3) und (4), werden in Einrichtungen, die Objekte im Kommunikationssystem betreiben wollen, ein/e oder mehrere Technische Verantwortliche für vernetzte IV-Systeme sowie ein Vertreter/eine Vertreterin bestellt. Die Bestellung erfolgt in der Regel durch die Leiterin/den Leiter der jeweiligen Einrichtung sofern nicht durch übergeordnete Instanzen anderes bestimmt wird; die/der Technische Verantwortliche wird dem ZIV im Rahmen seiner Zuordnung zu den zu betreuenden Objekten im Kommunikationssystem schriftlich benannt. Die Leiterin/der Leiter der Einrichtung kann ihre/seine Zuständigkeit auf die Dekanin/den Dekan oder andere, z. B. die IVV-Leiterin/den IVV-Leiter über-tragen.

(2) Die den Technisch Verantwortlichen zuzuordnenden Objekte sind die zu betreuenden Endgeräte und Zugangseinrichtungen im Kommunikationssystem in allen Formen (Rechner, Drucker oder Laborgeräte mit Netzanschluss, Anschlussdosen bei Festnetzzugängen usw.). Darüber hinaus können der/dem Technischen Verantwortlichen durch die Leiterin/den Leiter der jeweiligen Einrichtung übergeordnete Objekte zugeordnet werden Solche Objekte können im Rahmen von besonderen Vereinbarungen mit dem ZIV (als Betreiber des Kommunikationssystems) für IV-Leistungen jeglicher Art definiert werden. Insbesondere können solche Objekte Zusammenfassungen von Endgeräten oder Anschlusseinrichtungen sein, für die bestimmte quantitative oder qualitative Betriebsgrößen innerhalb des Kommunikationssystems erzielt werden sollen (z. B. Übertragungsqualität oder Verfügbarkeit wegen besonderer Dienstgüteanforderungen, Zugangsbeschränkungen oder Verkehrsfilterung aus Sicherheitsgründen). Wenn die Zuordnung übergeordneter Objekte an den Technischen Verantwortlichen aus rein technischen Gründen erfolgen soll, genügt die Abstimmung der/des für die untergeordneten Objekte zuständigen Technischen Verantwortlichen mit dem ZIV.

(3) Zur/Zum Technisch Verantwortlichen darf nur bestellt werden, wer in einem Beschäftigungsverhältnis zur Westfälischen Wilhelms-Universität Münster steht und die zur Erfüllung ihrer/seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Letztgenannte Voraussetzungen sollen durch anerkannte Zertifikate oder gleich zu wertende langjährige Erfahrungen nachgewiesen werden. Für die Bewertung der Nachweise sind die Detailregelungen, soweit vorhanden, und die Beurteilungskompetenz der IV-Versorgungseinheiten, des ZIV und des IV-Sicherheitsteams heran zu ziehen.

(4) Die Einrichtung hat die/den Technisch Verantwortlichen bei der Erfüllung ihrer/seiner Aufgaben zu unterstützen und ihr/ihm insbesondere, soweit dies zur Erfüllung ihrer/seiner Aufgaben erforderlich ist, Ressourcen zur Verfügung zu stellen. Auch ist sicherzustellen, dass sie/er die ihm obliegenden Aufgaben im Zusammenwirken mit den unmittelbaren Betreibern der ihr/ihm zugeordneten Endgeräte wahrnehmen kann. Als unmittelbare Betreiber gelten zunächst die Administratoren, die die Endgeräte einrichten, in das Kommunikationssystem integrieren und ihren Betrieb unter-stützen. Soweit unmittelbare Betreiber von Endgeräten nicht ausdrücklich benannt und tätig sind, gelten die Nutzer – notfalls die Einrichter der Endgeräte – als solche. Zur Gewährleistung einer effizienten Zusammenarbeit zwischen den Technischen Verantwortlichen der Einrichtungen und den IV-Infrastruktureinrichtungen sollte der Technische Verantwortliche jeweils für eine größere Zahl von Objekten (Rechnern, Zugängen usw.) zuständig sein. Andererseits muss der Einsatzbereich aber auch überschaubar bleiben, so dass eine wirksame Problemlösung jederzeit wenigstens koordinierend eingeleitet werden kann. In der Regel sollten durch die/den Technischen Verantwortlichen daher mindestens zwanzig und höchstens sechzig Endgeräte betreut werden.

§ 2 Aufgaben des Technisch Verantwortlichen

(1) Die/der Technisch Verantwortliche ist vorrangige Kontaktperson mit entsprechender technischer Koordinierungsfunktion zwischen dem jeweiligen unmittelbaren Betreiber der IV-Systeme einerseits und der/dem jeweiligen Leiter/Leiterin der Einrichtung und den zentralen sowie dezentralen IV-Einrichtungen andererseits. Ihr/sein Aufgabenbereich umfasst den Bereich der Verwaltung, der Integration, des Betriebes und der Sicherheit von IV-Systemen innerhalb des Kommunikationssystems

der Universität. Soweit durch die von ihm betreuten Objekte mit der Universität verbundene Kommunikationssysteme Dritter (Wissenschaftsnetz, Internet, lokale Drittnetze usw.) erreicht wer-den können, ist der genannte Aufgabenbereich auch innerhalb des so erweiterten Kommunikationssystems definiert.

(2) Die/der Technische Verantwortliche

a) führt alle in diesem Kontext entstehenden latenten und akuten Problemstellungen selbst oder unter Inanspruchnahme fachkundiger Hilfe wirksam und zeitgerecht einer Lösung zu. Er soll sich daher ständig über die Verwendung der ihm zugeordneten IV-Systeme informieren und soll von der jeweiligen Einrichtung auch diesbezüglich informiert werden. Hierbei erkannte Mängel in der Betreuung der Systeme behebt sie/er selbstständig oder in der Zusammenarbeit mit der/dem Leiterin/Leiter der jeweiligen Einrichtung, und führt auftretende Probleme zumindest koordinierend einer Behebung zu.

b) leitet bei Gefahr im Verzuge die notwendigen Abwehrmaßnahmen umgehend ein und setzt notfalls eigenständig die Gefahrenquelle außer Betrieb.

c) ist für die Durchführung aller in diesem Kontext entstehenden notwendigen technischen Verwaltungsaufgaben, wie beispielweise die Dokumentation der Objekte mit technischen Parametern in lokalen und externen Datenbanken, verantwortlich.

(3) Die/der Technisch Verantwortliche hat zur Erfüllung seiner Aufgaben den notwendigen Zugriff zu allen Informationen, die in den IV-Versorgungseinheiten oder dem ZIV verfügbar sind und die ihm zugeordnete Objekte betreffen. Ferner müssen ihr/ihm die unmittelbaren Betreiber der Endgeräte, die ihm zugeordnet sind, bekannt gemacht werden.

§ 3 Haftungsausschluss

(1) Die/der Technisch Verantwortliche haftet lediglich für seinen Aufgabenbereich. Die Verantwortung für die IV-Sicherheit eines Endgerätes und der dort zur Verfügung gestellten Dienste und Informationen und für die von dort ausgehenden Bedrohungen und Schadwirkungen liegt in erster Linie bei den zuständigen unmittelbaren Betreibern (zumeist Administratoren), in dem Maße wie diese das System einrichten und in das Kommunikationssystem integrieren. Zudem sind auch die Nutzer in dem Maße verantwortlich, in welchem sie Ressourcen in Anspruch nehmen. Die Gesamt- Verantwortung trägt die/der Leiterin/Leiter der jeweiligen Einrichtung, soweit ihnen die Aufsicht über diese Systeme und Anwendungen einschließlich ihrer Administration und Nutzung obliegt.

§ 4 Inkrafttreten

(1) Diese Regelung tritt mit ihrer Verkündung in Kraft.

(2) Technische Verantwortliche, die durch die bisher übliche Verpflichtungserklärung ihre Aufgabe übernommen haben, können nach Inkrafttreten dieser Regelungen innerhalb von zwei Monaten von ihrem Amt zurücktreten. Nach Ablauf der Frist gilt für die im Amt verbliebenen Technischen Verantwortlichen die vorliegende Ordnung.

Ausgefertigt aufgrund des Beschlusses des Senats der Westfälischen Wilhelms-Universität Münster vom 28. April 2004.

Münster, den 08. Juni 2004

Der Rektor

Prof. Dr. Jürgen Schmidt

Die vorstehende Ordnung wird gemäß der Ordnung der Westfälischen Wilhelms- Universität über die Verkündung von Ordnungen, die Veröffentlichung von Beschlüssen sowie die Bekanntmachung von Satzungen vom 08. Februar 1991 (AB Uni 91/1), geändert am 23. Dezember 1998 (AB Uni 99/4), hiermit verkündet.

Münster, den 08. Juni 2004

Der Rektor

Prof. Dr. Jürgen Schmidt

Anhang E | Ordnung für IT-Administratoren an der Universität Münster

vom 29. April 2009

Präambel

Notwendigkeiten und Zielsetzungen der Administration von IT-Systemen

Zu Betrieb und Nutzung von IT-Systemen gelten, neben gesetzlichen Bestimmungen, die Regelungen der Universität Münster und ihrer Einrichtungen, die diese Systeme betreiben (insbesondere die Benutzungsordnung des ZIV und der IV-Versorgungseinheiten der WWU sowie die Betriebsregelungen).

Der ordnungsmäßigen Einrichtung, dem Betrieb und der funktionalen Überwachung der IT-Systeme, im Folgenden insgesamt kurz als IT-Administration bezeichnet, kommt deshalb eine herausragende Bedeutung im IV-System der Universität Münster zu. Die verschiedenen Aufgaben der IT-Administration werden von dem IT-Administrator wahrgenommen (zu den Einzelheiten siehe „Erläuterungen zur Ordnung für IT-Administratoren an der Universität Münster“).

§ 1 Bestellung einer IT-Administratorin/eines IT-Administrators

(1) Einrichtungen, die IT-Systeme unter ihrer Aufsicht betreiben wollen, bestellen diesen zugeordnete IT-Administratorinnen/IT-Administratoren und jeweils mindestens eine Vertreterin/einen Vertreter. Die Bestellung erfolgt in der Regel durch die Leiterin/den Leiter der jeweiligen Einrichtung, sofern nicht durch übergeordnete Instanzen anderes bestimmt wird. Die Leiterin/der Leiter der Einrichtung kann ihre/seine Zuständigkeit auf die Dekanin/den Dekan oder andere, z. B. die IVV-Leiterin/den IVV-Leiter übertragen. Die IVV-Leiterin/der IVV-Leiter kann der Bestellung widersprechen. Die Bestellung ist zu dokumentieren und dem ZIV über die IVV-Leiter/innen bekannt zu geben. Eine Liste der bestellten IT-Administratoren wird am ZIV geführt.

(2) Zum IT-Administrator/zur IT-Administratorin darf nur bestellt werden, wer in einem Beschäftigungsverhältnis zur Westfälischen Wilhelms-Universität Münster steht und die zur Erfüllung ihrer/seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Letztgenannte Voraussetzungen sollen durch anerkannte Zertifikate (z. B. Teilnahme an Veranstaltungen zur Administratorenschulung) oder gleich zu wertende langjährige Erfahrungen nachgewiesen werden. Für die Bewertung der Nachweise sind die Detailregelungen, soweit vorhanden, und die Beurteilungskompetenz der IV-Versorgungseinheiten und des ZIV heran zu ziehen.

(3) IT-Administratoren sind bei ihrer Bestellung in ausreichendem Maße in Übereinstimmung mit der Präambel über ihre Verantwortung und Verpflichtung zu belehren (vgl. Anlage „Inhalte der Belehrung des IT-Administrators“). Die erfolgte Belehrung ist von der IT-Administratorin/dem IT-Administrator im Rahmen der „Übertragung von Unternehmerpflichten“ schriftlich zu bestätigen.

(4) Die Einrichtung hat die IT-Administratorin/den IT-Administrator bei der Erfüllung ihrer/seiner Aufgaben zu unterstützen. Dies betrifft insbesondere die Bereitstellung der zur Erfüllung ihrer/seiner Aufgaben erforderlichen Ressourcen und Informationen sowie die Sicherstellung von ausreichen-den Weiterbildungen.

(5) Die IT-Administratorinnen/IT-Administratoren erfüllen ihre Aufgabe in Zusammenarbeit mit den zuständigen Technisch Verantwortlichen und werden diesen benannt.

(6) Die Bestellung der IT-Administratoren erfolgt in Form einer Übertragung von Unternehmerpflichten (vgl. Anlage „Übertragung von Unternehmerpflichten“).

§ 2 Aufgaben der IT-Administratorin/des IT-Administrators

(1) Die IT-Administratorin/der IT-Administrator führt alle IT-Administrationsaufgaben für die anvertrauten IT-Systeme entsprechend den Notwendigkeiten und Zielsetzungen der Einrichtung nach Anweisung der/des Dienstvorgesetzten und in dem ihr/ihm durch die Einrichtung eingeräumten Maße in eigenständiger Ausgestaltung aus.

(2) Im Zuge der unmittelbar mit der IT-Administration verbundenen Aufgaben zur Sicherheit der Informationsverarbeitung arbeitet die IT-Administratorin/der IT-Administrator an den diesbezüglichen organisatorischen Aufgaben mit, wie beispielsweise der Erstellung von Notfallplänen und der Unterweisung der Nutzer. Die Benennung einer/eines zuständigen IT-Administratorin/IT-Administrators für ein IT-System ist aus Sicherheitsgründen Voraussetzung für dessen Freigabe im Netzwerk der Universität.

(3) Soweit dies nicht auf anderem Wege gesichert geschieht, stellt die IT-Administratorin/der IT-Administrator die Information der Nutzer oder sonst betroffener Personen sicher, wenn deren Arbeitsmöglichkeiten oder sonstige Belange durch ihre/seine Aufgabenwahrnehmung tangiert sind. Sie/er

informiert diese deshalb zeitnah über Maßnahmen, möglichst auch im Voraus, so dass die betroffenen Personen ggf. ausreichende Möglichkeiten der Einflussnahme haben.

(4) Die IT-Administratorin/der IT-Administrator bildet sich weiter und informiert sich, so dass sie/er stets fach- und sachgerecht ihr/seine Aufgaben nach dem Stand der Technik und nach den Zielsetzungen und sonstigen Vorgaben der Einrichtung, der Universität, der IV- Versorgungs-einrichtung und des ZIV erfüllen kann (zu den Einzelheiten siehe „Erläuterungen zur Ordnung für IT-Administratoren an der Universität Münster“ und „Übertragung von Unternehmerpflichten“).

§ 3 Inkrafttreten

(5) Diese Regelung tritt mit ihrer Verkündung in Kraft.

(6) Personen, die bisher IT-Administrationsaufgaben in vergleichbarer Art wie beschrieben wahrgenommen haben, sind binnen zwei Monaten nach Verkündung dieser Ordnung entsprechend den Regelungen unter § 1 (1), (2) und (3) formal zu bestellen, sofern sie die unter § 1 (2) genannten Voraussetzungen erfüllen und die bisherigen IT-Administratoren-Tätigkeiten auch weiterhin ausüben sollen.

Ausgefertigt aufgrund des Beschlusses des Senats vom 22. April 2009.

Münster, den 29. April 2009

Die Rektorin

Prof. Dr. Ursula Nelles

Die vorstehende Ordnung wird gemäß der Ordnung der Westfälischen Wilhelms-Universität über die Verkündung von Ordnungen, die Veröffentlichung von Beschlüssen sowie Bekanntmachungen von Satzungen vom 08.02.1991 (AB Uni 91/1), zuletzt geändert am 23.12.1998 (AB Uni 99/4), hiermit verkündet.

Münster, den 29. April 2009

Die Rektorin

Prof. Dr. Ursula Nelles

Anlage zur Anhang E | Ordnung für IT-Administratoren an der Universität Münster

Übertragung von Unternehmerpflichten

Die Leiterinnen/die Leiter können in ihrem jeweiligen Verantwortungsbereich geeignete Personen schriftlich und unter Festlegung des Umfangs beauftragen, ihnen obliegende Aufgaben und Befugnisse in eigener Verantwortung wahrzunehmen. Die Übertragung hat die Befugnisse zur Durchführung von Abhilfemaßnahmen (z. B. Ressourceneinsatz, Entscheidungskompetenz) zu enthalten sowie die Vorgehensweise (z. B. Antrags-, Hinweis- und Meldepflichten) bei mangelnden eigenen Möglichkeiten. Bei der Übertragung von Aufgaben hat der Übertragende je nach Art der Tätigkeiten zu berücksichtigen, ob die mit der Aufgabe betrauten in der Lage sind, die für die Sicherheit bei der Aufgabenerfüllung zu beachtende Bestimmungen einzuhalten und notwendigen Maßnahmen durchzuführen. Unabhängig davon verbleiben jedoch die Organisations-, Auswahl- und Kontrollverantwortung bei dem Übertragenden.

Die Pflichtenübertragung beinhaltet grundsätzlich die Freistellung von anderen Dienstaufgaben im erforderlichen zeitlichen Umfang, die Übertragung ausreichender Weisungsbefugnis sowie die Bereitstellung der erforderlichen Sach- und Personalmittel (vgl. GUV SR 2005 „Regeln für Sicherheit und Gesundheitsschutz“, Ziff. 3.6).

Herrn/Frau _____

werden für die Abteilung / den Arbeitsbereich

_____

des/der

(Name der wiss- Einrichtung) _____

die der/dem Bereichsverantwortlichen (geschf. Direktor/in, Leiter/in, Professor/in)

(Name der/des Bereichsverantwortlichen) _____

hinsichtlich der IT-Administration obliegenden und nachfolgend im Einzelnen aufgeführten Unternehmerpflichten übertragen:

Nr.	Kurzbezeichnung	Anmerkungen

Eine Belehrung über die Pflichten und Verantwortung eines IT-Administrators, insbesondere die aktuellen Beschlüsse des Rektorats und die notwendigen Maßnahmen zur Gewährleistung der IV-Sicherheit gemäß den Veröffentlichungen im Sicherheitsportal

https://www.uni-muenster.de/ZIV/Sicherheit/Sicherheit.html

ist erfolgt.

Münster, den

_____ _____

(Unterschrift der/des Bereichsverantwortlichen) (Unterschrift der/des Verpflichteten)

_____ _____

(Personalrat) (Universitätsverwaltung)

Anlage zur Anhang E | Ordnung für IT-Administratoren an der Universität Münster

Inhalte der Belehrung des IT-Administrators

Der/die IT-Administrator/Administratorin sind bei ihrer Bestellung auf folgendes hinzuweisen:

(1) Grundsätzlich:

Beschlüsse des Rektorats und Maßnahmen zur Gewährleistung der IV-Sicherheit entsprechend: https://www.uni-muenster.de/ZIV/Sicherheit/Sicherheit.html

(2) Einhaltung des Datenschutzes, sowie der Grundregeln des Fernmeldegesetzes soweit anwendbar.

(3) Strikte Gewährleistung der Vertraulichkeit und Integrität der Daten.

(4) Beachtung der rechtlichen Vorgaben zur Einhaltung von Lizenzverträgen und Urheberrechten.

Eine Zusammenstellung der vielfältigen Rechtsfragen findet sich unter:
https://www.uni-muenster.de/ZIV/Recht/Rechtsfragen.html

Anlage zur Anhang E | Ordnung für IT-Administratoren an der Universität Münster

Erläuterungen zur Ordnung für IT-Administratoren an der Universität Münster

(1) Zielsetzungen der Administration von IT-Systemen

Die Bereitstellung eines funktionierenden IT-Systems ist eine unabdingbare Grundlage für Forschung, Lehre und Verwaltung der Universität. Arbeitsplatzsysteme, Server und Netzwerk bilden im Kontext eine Infrastruktur für die Erstellung und Verteilung von Information, Kommunikation sowie die Verarbeitung von Daten der verschiedensten Art (Computing, Statistik, Bildverarbeitung, Präsentation u. a.). Ein solches vernetztes System erfordert eine besondere Sorgfalt bei der Einrichtung, der Nutzung und der funktionalen Überwachung insbesondere im Hinblick auf das Zusammenspiel mit anderen IT-Systemen. Nur dadurch kann die Sicherheit des gesamten IT-Systems bezüglich Datenintegrität, Vertrauenswürdigkeit und Verfügbarkeit gewährleistet werden.

Von besonderer Bedeutung ist die Administration der Arbeitsplatzsysteme, für die die Administratorenordnungen den Rahmen absteckt. Während der Technische Verantwortliche in erster Linie eine koordinierende Aufgabe in Arbeitsgruppen oder Instituten wahrnimmt und vor allem auch Ansprechpartner des ZIV ist, erfordert die IT-Administration jedes solchen Arbeitsplatzsystems die sachkundige und ordnungsgemäße Installation sowie Pflege im Hinblick auf die Nutzung des Betriebssystems, aller Applikationen und der Datenhaltung.

In diesem Sinne sind die IT-Administratoren in ihrem Verantwortungsbereich inhaltlich auf die Administration der Arbeitsplatzsysteme einer Universitätseinrichtung (e. g. Institut, Arbeitsgruppe) beschränkt.

Für Bereichs-Administratoren, die IT-Systeme (Server) der IVVen, Verwaltung oder zentraler Betriebseinheiten betreuen, sowie für zentrale Administratoren im ZIV, die Administrationsaufgaben für die gesamte Universität wahrnehmen, sind weitergehende Anforderungen zu stellen.

Entsprechend dem Aufgabenbereich des IT-Administrators ergeben sich unterschiedliche Anforderungen an die Qualifikation. Während die IT-Administration eines einfachen Arbeitsplatzsystems noch als Nebentätigkeit wahrgenommen werden kann, erfordert die Administration von umfangreichen IT-Systemen (z. B. Messdatenerfassung, Datenbanken, Anwendungssysteme, Fileservices, Publishing, etc.) einer Universitätseinrichtung den Einsatz von entsprechend ausgebildetem Fachpersonal.

Zusammengefasst sind die Ziele der IT-Administration:

- Sicherstellung der beabsichtigten Nutzbarkeit oder Funktion von IT-Systemen in Forschung, Lehre, Verwaltung etc. für die nutzenden bzw. betroffenen Einrichtungen und Personen
- Sicherung der Grundwerte der IV-Sicherheit
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

Erschwernisse in der Erreichung dieser Zielsetzungen sind in vielfältiger Weise gegeben. Dazu zählen

- die Komplexität der IT-Systeme und ihr Vernetzungsgrad
- Fehlerquellen und Schwachstellen in Hardware und in Software
- kurze Innovations- und Anpassungszyklen
- Bedrohungen der IV-Sicherheit durch unbedachte Nutzer und Hacker-Angriffe von inner- halb und außerhalb der Universität
- beschränkte finanzielle Ressourcen, insbesondere nur wenig Personal in längerfristigen Dienstverträgen mit hinreichender Qualifikation

(2) Zu administrierende IT-Systeme

Gegenstand der Administration sind für den IT-Administrator diejenigen IT-Systeme, die den Arbeitsplätzen in den jeweiligen Einrichtungen zugeordnet sind. In diesem Sinne ist der Begriff IT-System nicht beschränkt auf Hardware-Strukturen und Betriebssysteme, sondern umfasst Anwendungssysteme und aktive, administrierbare informationstechnische Funktionssysteme jeglicher Art.

Dazu gehören auf den verschiedenen Administrationsebenen u. a. Datenbanken, Web-Server- Programme, verteilte File-Systeme, Dienste-Nutzungssteuerung, z. B. über Active Directory, zugangssteuernde oder zugangsüberwachende Systeme (z. B. Firewalls, Intrusion-Detection- und Intrusion-Prevention-Systeme, Netzmonitore oder -analysatoren, Authentifizierungs-und Authorisierungssysteme), Policy-Orchestrierungssysteme, Drucker und Kameras im Netz, Videokonferenzsysteme.

Zu unterscheiden sind IT-Systeme, die integraler Bestandteil des Informationsverarbeitungssystems der Universität sind, von solchen die weitgehend unabhängig betrieben werden (z. B. häusliche Arbeitsplätze) und damit nicht unmittelbar auf das Gesamtsystem zurückwirken können. Sofern eine qualifizierte IT-Administration (Personalmangel) eines in das Universitätsnetz integrierten Arbeitsplatzsystems nicht möglich ist, muss eine weitgehende Trennung vom Universitätsnetz technisch vorgenommen werden. Ziel ist es, das Bedrohungspotential durch das ungepflegte Endgerät weitgehend zu minimieren.

(3) Stellung der IT-Administratoren

Die Wahrnehmung von Administrationsaufgaben in den verschiedenen Stufen erfordert ein hohes Maß an Verantwortung.

Im Kontext der bestehenden Gesetzeslage und Rechtsprechung sind grundsätzlich die Anforderungen des Datenschutzes, die Grundregeln des Fernmeldegesetzes, die strikte Einhaltung von Vertraulichkeit sowie insbesondere auch die rechtlichen Vorgaben zur Einhaltung von Lizenzverträgen und Urheberrechten zu beachten. (vgl. hierzu Veröffentlichungen der Forschungsstelle Recht im DFN)

Darüber hinaus steht der IT-Administrator in Verpflichtung und Verantwortung gegenüber der Leitung der Einrichtung, in deren Auftrag er die ihm anvertrauten Arbeitsplatzsysteme administriert.

Konkret sorgt er in diesem Rahmen

- für die sachgerechte Installation und Pflege der Betriebssysteme und der Applikationssoftware. Dazu gehören auch die Einrichtung, der Betrieb und die Pflege der Ressourcen mit Datenbeständen, Funktionen, Anwendungen und Diensten,
- richtet entsprechend vorgegebenen Regelungen für Nutzung, Sicherheit und andere Gesichtspunkte geeignete Mechanismen (Policies) ein, die eine den Rollen der Nutzer und den Funktionen abhängiger IT-Systeme (Funktionsverbund) adäquate Nutzung der Ressourcen sichert,
- überwacht die Ressourcen-Nutzung und Policy-Umsetzung durch geeignete Verfahren (Logs, Audits, Reports, Accounting-Verfahren etc.) und
- sorgt insgesamt für die Einhaltung der Zielsetzungen der Einrichtung und der Universität (Compliance).

Gleichzeitig sind die Vorgaben bezüglich Sicherheit und Interoperabitlität der zuständigen IV-Versorgungseinrichtung, des ZIV und der Universitätsleitung zu gewährleisten.

Der IT-Administrator wird dabei von den IV-Versorgungseinrichtungen und dem ZIV unterstützt. Insbesondere arbeitet er mit dem jeweiligen Technischen Verantwortlichen für vernetzte IV-Systeme zusammen, um die ihm obliegende Koordinierungsfunktion zwischen Leitung der Universitätseinrichtung, IV-Versorgungseinrichtung und ZIV zu erfüllen.

Insbesondere steht der IT-Administrator in der Pflicht und Verantwortung gegenüber den Nutzern, die das von ihm administrierte IT-System (Arbeitsplatzsystem) nutzen oder deren Rechte und Belange in anderer Weise betroffen sind.

Durch die unterschiedlichen Anforderungen kann es leicht zu Konflikten zwischen der nutzenden Universitätseinrichtung, den Nutzern und den Vorgaben der Administration kommen. Z. B. steht oft die notwendige Sicherheit in Konkurrenz zur einfachen Nutzbarkeit des IT-Systems, oder es werden von Nutzern Anforderungen an den Administrator gestellt, die aus rechtlichen Gründen nicht gewährt werden dürfen. Lassen sich solche Konfliktfälle nicht in der betreibenden Universitätseinrichtung lösen, kann sich der Administrator nach Anhörung durch die zuständige IVV an die IV-Kommission, vertreten durch den Vorsitzenden, wenden. Die letztendliche Entscheidung über die Zulässigkeit gewisser Maßnahmen trifft der IV-Lenkungsausschuss.

Das Vertrauen in die Person des IT-Administrators seitens der Nutzer und durch die Leitung der Einrichtung ist Schlüsselvoraussetzung für die Rolle des IT-Administrators. Das Vertrauen bedingt eine entsprechende fachliche und persönliche Eignung, die durch Erfahrung und durch Weiterbildung abgesichert und eine angemessene Aufsicht kontrolliert wird. Weiterbildungsmaßnahmen sind von der jeweiligen Universitätseinrichtung in geeignetem Rahmen zu fördern.

Mit der so definierten Rolle des IT-Administrators wird in der Universität die Verantwortung der Universitätsleitung subsidiär durch die Einrichtungen wahrgenommen. Durch das Wirken im Verbund mit der IV-Versorgungseinheit und dem ZIV unter Koordination durch die Technisch Verantwortlichen kann die Fachaufsicht durch das ZIV wahrgenommen werden.

IT-Administratoren können in Personaleinheit auch Technisch Verantwortliche sein.

(4) Verantwortlichkeiten

Die Gesamtverantwortung trägt die Hochschulleitung. In den einzelnen Organisationseinheiten sind die jeweiligen Leiter für die IT-Sicherheit ihrer Systeme verantwortlich.

Anmerkung: *Der besseren Lesbarkeit wegen wurde jeweils die grammatikalisch männliche Form gewählt. Dies impliziert, dass in allen diesen Fällen auch die grammatikalisch weibliche Form gemeint ist.*

Anhang F | Security Audit ISidoR

Seit Ende 2005 steht allen technisch Verantwortlichen für Geräte im LAN der Universität und des UKM das IV-Sicherheits-Audit-Werkzeug „ISidoR“[78] zur Verfügung, welches in Anlehnung an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[79] eine Risikoanalyse durch Erfassung und Bewertung des IST-Zustands der IV-Sicherheit von IT-Endgeräten ermöglicht. Im Folgenden soll kurz und knapp auf Grundlagen, Konzepte der Datenerhebung mittels ISidoR eingegangen und eine Übersicht über weitere Inhalte - und Informationsquellen gegeben werden.

Einführung

Im Allgemeinen erfordern die existierenden einschlägigen IV-Sicherheits-Audit-Werkzeuge, wie das BSI-eigene GSTOOL bzw. das Open-Source Produkt „verinice.“, das Modellieren der zu auditierenden IT-Landschaft und somit das Schaffen einer eigenen Datenbasis. Da eine solche Erfassung mit einem enormen Zeitaufwand verbunden ist und bereits sämtliche vom Zentrum für Informationsverarbeitung (ZIV) betreuten Rechnersysteme innerhalb der NIC_online Datenbank LANbase samt zugehöriger Stammdaten, Verantwortlichkeiten und Lageangaben erfasst und verwaltet werden, wurde entschieden, sich zwar an den Vorgaben des BSI zu orientieren, aber trotzdem ein eigenes Sicherheits-Audit-Werkzeug (ISidoR - Informations-Sicherheit ist die oberste Regel) zu entwickeln, welches auf die vorhandene Datenbasis zurückgreift.

Neben dem Vermeiden der erneuten Datenerhebung und Modellieren der IT-Landschaft an Universität und Universitätsklinikum wurde die Nachhaltigkeit der Erfassung eine weitere fundamentale Grundlage des Sicherheits-Audit-Werkzeugs ISidoR. Nicht nur die Datenbasis, sondern auch die erhobenen Informationen während der Auditierung werden innerhalb der Netzdatenbank LANbase erfasst und gespeichert, sodass die erhobenen Daten über viele Auditierzyklen hinweg zur Verfügung stehen und somit zur zeitlichen Dokumentation der IV-Sicherheit dienlich sind.

Das ZIV kann aufgrund der vollen Kontrolle über den Programmcode flexibel auf neue Gegebenheiten, Wünsche und Anforderungen seitens der Auditoren eingehen, was sich unter anderem in einer Fülle von speziell entwickelten programmseitigen Hilfestellungen bei der Auditierung widerspiegelt, die es ermöglichen eine effiziente Auditierung durchzuführen.

Hilfestellungen zum Security-Audit gibt das Netz-Informations-Center (NIC)[80].

Konzepte

Sicherheit definiert sich dadurch, dass Risiken in dem Maße eingedämmt worden sind, dass die verbleiben-den Restrisiken vertretbar sind und ein angemessenes Verhältnis von Aufwand für die Sicherheitsmaßnahmen zu deren Nutzen gewährleistet ist. Dementsprechend empfiehlt es sich, grundsätzlich zunächst eine Risikoanalyse durchzuführen, den Nutzen und Aufwand bei Schutzmaßnahmen zu ermitteln, um schließlich nach einer Prioritätendefinition die als notwendig erachteten Maßnahmen durchzuführen; es müssen also verschiedene Faktoren bewertet werden. Das Verfahren insgesamt ist dabei nicht als einmaliger Prozess zu verstehen, sondern als nachhaltige zyklische Vorgehensweise, beginnend bei der Planung (mit einer Bestimmung der Sicherheitsziele) über die Umsetzung und der Kontrolle bis zur Anpassung. Mit der Einrichtung eines durchgängigen Security-Audit-Verfahrens an der Universität Münster und seiner erstmaligen Durchführung werden zwei wichtige Bestandteile in dieser Prozesskette des Informationssicherheitsmanagements (ISM) etabliert, die Feststellung des Schutzbedarfs und die Feststellung getroffener Sicherheitsvorkehrungen. Daraus kann der erreichte Stand der IV-Sicherheit abgeleitet und noch bestehende Defizite können sichtbar gemacht werden. Das Security Audit kann damit als Steuerungsinstrument benutzt werden – es ist Nachweis für getroffene Maßnahmen und Erreichtes, erlaubt die Überprüfung der Zielvorgabeneinhaltung (Compliance) und ist Planungsgrundlage für noch einzuleitende Maßnahmen. Dies gilt nicht nur für die obersten Gremien der Universität, sondern auch für alle Verästelungen der IV-Struktur.

Das Security-Audit-Verfahren für die Universität Münster ist als Online Verfahren angelegt, das unter Verwendung der Netzdatenbank im ZIV durch die für die IT-Endgeräte im Netz zuständigen Technisch Verantwortlichen bedient wird. Es wird also keine Befragung mit speziellem Personal mit Fragebögen durchgeführt, wie dies sonst häufig geschieht. Ein Nachteil ist dabei ist sicherlich, dass die Fragestellungen i. Allg.

---

[78] https://www.nic.uni-muenster.de/Sec_Uebersicht.asp
[79] https://www.bsi.de/
[80] https://www.uni-muenster.de/ZIV/Technik/Netz/NIC.html

nicht persönlich erläutert werden können – es gibt aber umfangreiche Online-Hilfen –, und die Qualität der Ergebnisse möglicherweise etwas geringer ist. Der Aufwand für zusätzliches Personal oder externe Dienstleister kann somit in Grenzen gehalten werden. Auch ist der entscheidende Vorteil in der gewünschten Nachhaltigkeit zu sehen: Die Durchführung kann nach Bedarf wiederholt werden, wobei soweit wie möglich auf die Antworten früherer Ermittlungen zurückgegriffen werden kann. Somit steht der WWU erstmals ein Instrument zur Verfügung, mit dem systematisch und durchgängig eine Revision der IV-Sicherheit durchgeführt werden kann.

Ziele des Sicherheits-Audits

Das Ziel des Security-Audits ist die Feststellung des Schutzbedarfs aller untersuchten IT-Systeme, der vorhandenen Sicherheitsvorkehrungen und der Sicherheitsdefizite mit dem übergeordneten Ziel, Grundlagen für die Einführung weitergehender Sicherheitsmaßnahmen zu ermitteln und letztendlich eine Anhebung des IV-Sicherheitsniveaus zu bewirken.

Als Nebeneffekt wird erwartet, dass den Nutzerinnen und Nutzern zu den einzelnen Themenbereichen Informationen zur Sicherheitstechnik vermittelt werden können. Beim Auswerten der Antworten wird deutlich, welche Möglichkeiten der Absicherung bestehen und welchem Sicherheitsstand der Ist-Zustand entspricht.

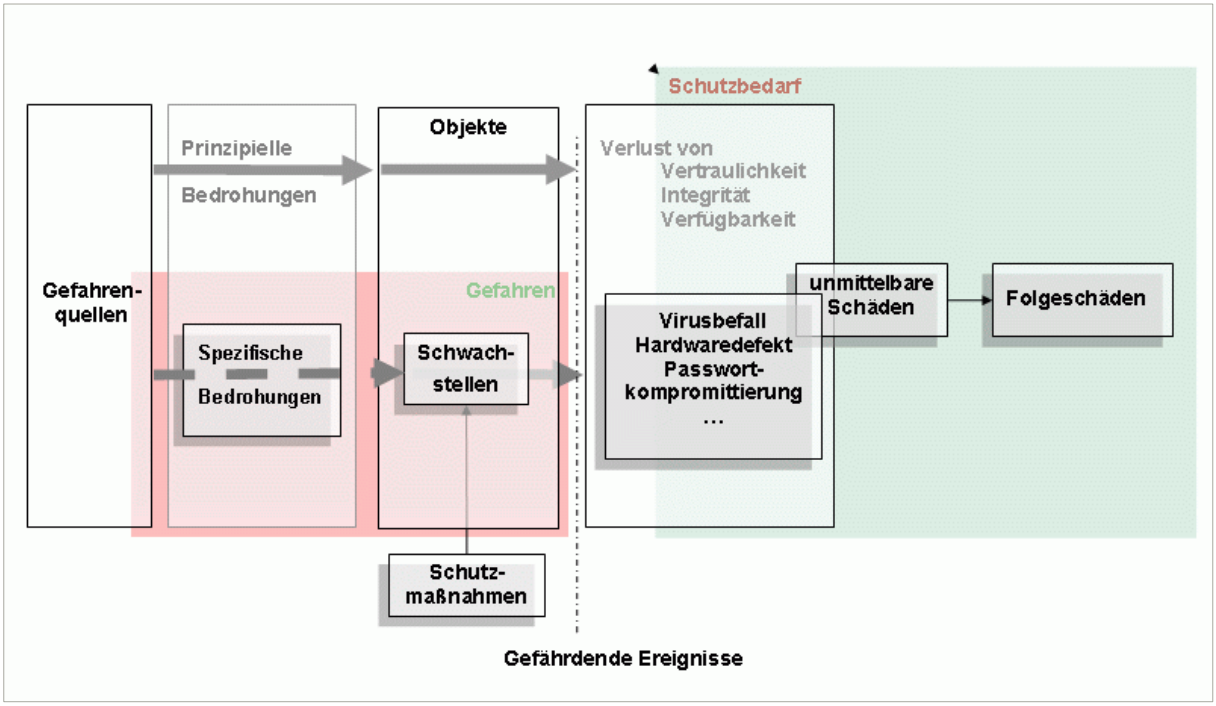
Außerdem werden die Nutzerinnen und Nutzer für sicherheitsrelevante Aspekte sensibilisiert. Über die Darstellung der Konsequenzen, die eine Verletzung der Integrität, Vertraulichkeit oder Verfügbarkeit der Daten und Dienste nach sich ziehen würde, wird ihnen die Notwendigkeit von Sicherheitsvorkehrungen vor Augen geführt und an Beispielen verdeutlicht.

Vorgehensweise bei der Auditierung

Das Security-Audit wird mittels Webseiten, die Fragenkataloge aufzeigen, durchgeführt. Zu jeder Frage werden fünf Antworten zur Auswahl angeboten. Die Nutzerin oder der Nutzer wählt die Antwort, die am ehesten den Ist-Zustand beschreibt. Die Antworten werden in einer Datenbank vorgehalten, damit langfristige Entwicklungen bzgl. der IV-Sicherheit zu verfolgen sind.

Ermittlung des Schutzbedarfs

Der Schutzbedarf eines Datenendgerätes ergibt sich aus den Schäden, die entstehen, wenn die Integrität und die Vertraulichkeit der Daten verletzt wird oder Daten und Dienste nicht verfügbar sind. Bei der Einstufung des Schutzbedarfs von Datenendgeräten ist zu beurteilen, welcher Schutzbedarfskategorie die Daten oder IT-Anwendungen auf dem Gerät zuzuordnen sind und auch auf welche Daten über dieses Datenendgerät zugegriffen werden kann. Wenn die einzelnen Anforderungen unterschiedlich sind, ist im Ergebnis die höchste Schutzbedarfskategorie für die Einstufung ausschlaggebend. Graphisch veranschaulicht wird dieser Sachverhalt durch die folgende Abbildung:



Für jedes Datenendgerät wird zunächst der Schutzbedarf ermittelt, d. h. die Wertigkeit und Wichtigkeit der

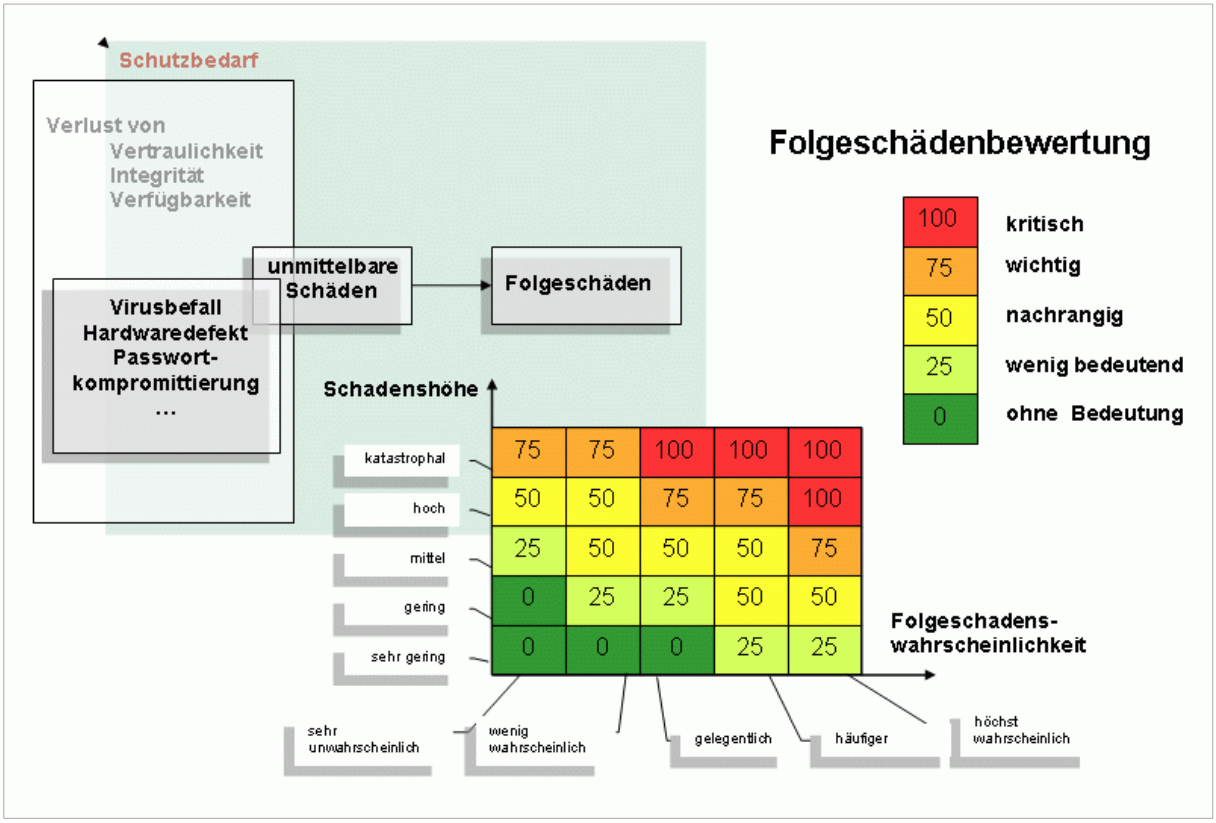
Daten und Dienste, die über das Datenendgerät erreichbar sind, werden festgestellt. Dabei wird unterschieden zwischen Integrität und Vertraulichkeit der Daten und Verfügbarkeit der Daten und Dienste.

Die Einstufung eines Datenendgerätes in eine entsprechende Schutzbedarfskategorie erfolgt anhand der Folgeschäden, die ein Verlust der Integrität, der Vertraulichkeit oder der Verfügbarkeit benötigter Daten und Dienste nach sich ziehen würde sowie der Wahrscheinlichkeit, mit der ein Folgeschäden auslösende Ereignis zu erwarten ist.

Das bedeutet im Einzelnen, dass von der Nutzerin oder dem Nutzer das Ausmaß der Folgeschäden anzugeben ist, das eine Verletzung der Integrität oder Vertraulichkeit der Daten zur Folge hätte oder das sich ergäbe, wenn Daten und Dienste nicht zur Verfügung stünden.

Der Fragenkatalog zur Ermittlung des Schutzbedarfs gliedert sich in folgende sechs Abschnitte (nach BSI):

- Verstoß gegen Gesetze und Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Negative Außenwirkung
- Finanzielle Auswirkungen
- Beeinträchtigung der Aufgabenerfüllung



Nach der Auswertung der Antworten steht für das Datenendgerät der Schutzbedarf hinsichtlich der Aspekte bezüglich Vertraulichkeit und Integrität der Daten als auch hinsichtlich der Verfügbarkeit der Daten und Dienste fest. Insgesamt wurden folgende fünf Schutzbedarfskategorien festgelegt:

- Schutzbedarfskategorie: »Keine« (0 %, keine Folgeschäden) Schäden haben keine Beeinträchtigung der Institution zur Folge.
- Schutzbedarfskategorie: »Niedrig« (25 %, geringe Folgeschäden) Schäden haben nur eine unwesentliche Beeinträchtigung der Institution zur Folge.
- Schutzbedarfskategorie: »Mittel« (50 %, mittlere Folgeschäden) Schäden haben Beeinträchtigungen der Institution zur Folge.
- Schutzbedarfskategorie: »Hoch« (75 %, hohe Folgeschäden) Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.
- Schutzbedarfskategorie: »Sehr hoch« (100 %, sehr große Folgeschäden) Der Ausfall der IV führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche. Es besteht Gefahr für Leib und Leben von Personen.

Ermittlung der Sicherheitsvorkehrungen

In Abhängigkeit vom ermittelten Schutzbedarf für Integrität und Vertraulichkeit der Daten bzw. für Verfügbarkeit der Daten und Dienste werden nun automatisch Fragenkataloge zusammengestellt, die die Sicherheitsvorkehrungen bei dem Datenendgerät und dessen Umfeld ermitteln.

Im Einzelnen handelt es sich dabei um Fragenkataloge zu

› dem Datenendgerät,
› dem geräteseitigen Netzanschluss (z. B. Netzadapter),
› dem netzseitigen Anschluss (z. B. Anschlussdose),
› der zugeordneten Netzzone und
› dem Raum, in dem sich das Datenendgerät befindet.

Je höher der Schutzbedarf eines Datenendgerätes ist, umso ausführlicher werden Fragen gestellt, um den Status der Sicherheitsvorkehrungen festzustellen.

Jede Antwort entspricht einem bestimmten Sicherheitsniveau. Aus der Gesamtheit der Antworten wird für jeden einzelnen der o. g. Fragenkataloge ein Index für den Stand der Sicherheitsvorkehrungen berechnet. Wie beim Schutzbedarf wird auch hier unterschieden zwischen Maßnahmen zur Sicherung der Integrität und Vertraulichkeit der Daten und Maßnahmen zur Sicherung der Verfügbarkeit der Daten und Dienste, um später zielgerichteter entsprechende weitergehende Sicherheitsmaßnahmen einleiten zu können. Bei dem Datenendgerät, dem geräteseitigen und netzseitigen Anschluss, der Netzzone und dem Raum gibt es damit eine Beurteilung, welchem von den im Folgenden aufgeführten Zustände die jeweiligen Sicherheitsmaßnahmen entsprechen:

› Es wurden »keine« Sicherheitsvorkehrungen getroffen (0 %),
› Es wurden »geringe« Sicherheitsvorkehrungen getroffen (25 %),
› Es wurden »wichtige« Sicherheitsvorkehrungen getroffen (50 %),
› Es wurden »weit reichende« Sicherheitsvorkehrungen getroffen (75 %) oder
› Es wurden »umfassende«, durchgreifende Sicherheitsvorkehrungen getroffen (100 %).

Der Status der Sicherheitsvorkehrungen wird jeweils für Integrität und Vertraulichkeit der Daten und Verfüg-barkeit der Daten und Dienste ermittelt.

Berechnungsverfahren bei der Evaluation

Basierend auf den gegebenen Antworten werden nun der Schutzbedarf und die getroffenen Sicherheitsvorkehrungen ausgewertet und kategorisiert.

Resultierend aus einem Vergleich der jeweiligen ermittelten Werte zu Schutzbedarf und den getroffenen Sicherheitsvorkehrungen, können Aussagen zur IV-Sicherheit gemacht werden; die Diskrepanzen zwischen Schutzbedarf und Sicherheitsvorkehrungen werden deutlich. Nach dem Erfassen des Ist-Zustandes ist eine Anhebung des Sicherheitsniveaus durch angemessene Sicherheitsvorkehrungen in den ermittelten Punkten umzusetzen.

Dem Berechnungsverfahren liegt eine geometrische Mittelung zu Grunde, sodass das Beantworten einer Frage mit 0 % das Nullieren des gesamten Fragenkatalogs zur Folge hat. Dieses Berechnungsverfahren wurde gewählt, da eine Sicherheitslücke egal in welchem Bereich, eine Kompromittierung des Datenendgerätes zur Folge haben könnte und somit ein massives Risiko darstellt. Um dem Auditor die Möglichkeit zu geben, Fragen zurückzuweisen bzw. ihn nicht zwingen zu müssen, dem aktuellen Sachverhalt nicht gerecht werdende Fragen mit 0 % beantworten zu müssen, hat dieser die Möglichkeit als Antwort Trifft nicht zu bzw. Keine Angabe zu geben. Beide haben zur Folge dass die aktuelle Frage nicht gewertet wird, wobei die letzte Antwort die Anzahl der zur Mittelung zugrundeliegenden Fragen nicht verringert.

Eine Visualisierung der errechneten Werte erfolgt in folgenden Abstufungen:

Schutzbedarfskategorie		**Stufe Sicherheitsvorkerhrungen**	
kein Schutzbedarf		*keine Sicherheitsvorkehrungen*	
geringer Schutzbedarf		*geringe Sicherheitsvorkehrungen*	
mittlerer Schutzbedarf		*wichtige Sicherheitsvorkehrungen*	
hoher Schutzbedarf		*weit reichende Sicherheitsvorkehrungen*	
sehr hoher Schutzbedarf		*umfassende Sicherheitsvorkehrungen*	

Auswertung der erhobenen Daten

Sind zu einem Datenendgerät hinreichend viele Fragen (d. h. mindestens 80 %) zu Schutzbedarf und zugehörigen Sicherheitskategorien beantwortet, so werden die erhobenen Daten ausgewertet. Besteht eine Diskrepanz zwischen ermittelter Schutzbedarfskategorie und der Güte der zugehörigen Sicherheitsvorkehrungen, so wird der Auditor visuell auf diesen Umstand hingewiesen. Eine genauere, dem Einzelfall genügende Bewertung dieses pauschalen Hinweises bzw. des Sachverhaltes bleibt dem jeweiligen Auditor überlassen.

Bei der Bewertung der Ergebnisse ist zu beachten, dass die Art des eingesetzten Audit-Verfahrens, in Form von durch den Nutzer selbstständig zu beantwortenden Fragebögen eine gewisse Subjektivität bei der Evaluation bedingt. Durch diese Strategie ist es aber auf einfache, rasche und von Dritten unabhängige Art und Weise möglich, gewisse Indikatoren für vorherrschende Sicherheitsdefizite zu erlangen.

Hilfestellungen für Auditoren

Onlinedokumentation

Kommt ein Auditor zum ersten Mal mit der Benutzeroberfläche von ISidoR in Kontakt, gelingt es ihm häufig nicht, den gesamten Funktionsumfang direkt zu erschließen. Aus diesem Grund steht dem Auditor zu jedem Zeitpunkt eine ausführliche Onlinedokumentation zur Verfügung, welche ihm Hintergrundinformationen, Hilfestellungen, Tipps und ein Glossar mit Erläuterungen zu häufig verwendeten Begriffen zur Verfügung stellt. Durch einen permanenten Link im Seitenkopf einer jeden HTML-Seite kann die Onlinedokumentation jederzeit aufgerufen werden.

Für diejenigen, die Informationen lieber gedruckt vorliegen haben, steht das Handbuch auch in Form einer PDF-Version als Download[81] zur Verfügung.

Dynamischer Aufbau der Fragenkataloge

Art und Umfang der Fragenkataloge zu den getroffenen Sicherheitsvorkehrungen eines Datenendgerätes sind abhängig von den ermittelten Werten für den jeweiligen Schutzbedarf. Die untenstehende Abbildung stellt diesen Sachverhalt exemplarisch anhand zweier Auswertungen zum Sicherheits-Audit zweier Datenendgeräte dar.

Das erste Datenendgerät (Abb. i) weist hierbei einen geringen, das zweite Datenendgerät (Abb. ii) einen sehr hohen Schutzbedarf auf. Im ersten Fall sind Fragen zu vier Kategorien (Datenendgerät, Netzadapter, Anschlussdose und Raum) im zweiten Fall zu lediglich zwei Kategorien (Datenendgerät und Raum) zu beantworten. Zusätzlich werden sich die zugehörigen Fragebögen in der Anzahl der zu beantwortenden Fragen unterscheiden.

Fragenkategorien zu getroffenen Sicherheitsvorkehrungen bei ermitteltem Schutzbedarf

geringer Schutzbedarf

Abb. i

sehr hoher Schutzbedarf

Abb. ii

Zur weiteren Minimierung des Aufwands bei der Beantwortung der Fragenkataloge sind diese hierarchisch aufgebaut. Ein Fragenkatalog besteht somit aus sog. Pauschalfragen, die einen Sachverhalt pauschal behandeln, und sog. Detailfragen, die genauer auf einzelne Aspekte eingehen. Zur hinreichenden Beantwortung eines Fragenkatalogs genügt es dabei, 80 % der Pauschalfragen zu beantworten. Die zusätzliche Betrachtung der Detailfragen ermöglicht es, ein wesentlich differenzierteres Bild abzuliefern, ist aber für die korrekte Auditierung des Datenendgerätes nicht zwingend erforderlich.

[81] https://www.nic.uni-muenster.de/Sec_Glossar/sec_handbuch.pdf

Antwortmuster - automatisierte Behandlung ganzer Rechnerklassen

Eines der wesentlichen – den Auditor unterstützenden – Werkzeuge von ISidoR ist die Möglichkeit, Antwortmuster anzulegen und zu verwalten. Hierbei kann ein Auditor die bei einem Fragenkatalog gegebenen Antworten in einem sogenannten Antwortmuster abspeichern.

Gespeicherte Antwortmuster können bei Bedarf auf einen entsprechenden Fragenkatalog eines beliebigen Datenendgerätes angewendet werden. Der Auditor ist auf diese Weise nicht mehr gezwungen, die Fragen eines Fragenkatalogs einzeln zu beantworten, sondern lässt anhand des jeweiligen Antwortmusters die Antworten automatisiert eintragen.

Das ZIV stellt bereits einige vorgefertigte Antwortmuster zur Verfügung, dies sind u. a. Antwortmuster zu den Bereichen:

- Arbeitsplatzrechner mit Zugriff auf persönliche Daten oder vertrauliches Datenmaterial
- Netzwerkdrucker mit hoher Verfügbarkeitsanforderung
- Server mit Standardfunktionen (Zugriff auf persönliche Daten)
- Server mit Standardfunktionen (hohe Verfügbarkeit erforderlich)
- Standardarbeitsplatzrechner
- Arbeitsplatzrechner der Personalverwaltung

Das Anlegen und Verwalten von Antwortmustern ist mandantenfähig, d. h. Auditoren können selbstständig eigene Antwortmuster erstellen, bearbeiten und löschen. Antwortmuster können sowohl anhand von existierenden Antwortkatalogen eines gewissen Datenendgerätes als auch auf Basis eines anfänglich leeren Antwortenkatalogs erstellt werden. Selbstständig erstellte Antwortmuster können durch den jeweiligen Auditor für weitere NIC-online-Administrationsgruppen – und somit andere Auditoren – freigegeben werden, sodass die Auditoren gegenseitig von ihrer Arbeit profitieren können.

Ein weiterer Vorteil bei der Nutzung von Antwortmustern ist die Möglichkeit, ein geändertes Muster erneut auf Datenendgeräte bzw. Fragebögen anwenden zu können, deren Antworten anhand dieses Musters gegeben wurden. Hierzu speichert ISidoR die Information, dass ein gewisser Fragenkatalog eines Datenendgerätes anhand eines speziellen Musters beantwortet wurde. Wird nun ein Antwortmuster geändert, so erhalten die Auditoren die Information, dass sich dieses Antwortmuster geändert hat und können für den Einzelfall entscheiden, ob das geänderte Muster erneut angewendet oder die Verknüpfung zum Antwortmuster aufgehoben werden soll.

Kopierfunktion von Antworten auf andere Fragenkataloge

ISidoR gibt dem Auditor die Möglichkeit, sämtliche gegebenen Antworten eines Fragenkatalogs auf die Fragenkataloge weiterer Datenendgeräte zu übertragen. Hierbei können mehrere Datenendgeräte ausgewählt werden, sodass ein Katalog von Antworten in einem Arbeitsgang auf eine Vielzahl von Datenendgeräten übertragen werden kann.

Basieren hierbei die zu kopierenden Antworten auf einem Antwortmuster, so wird der Auditor deutlich auf diesen Sachverhalt hingewiesen und kann entscheiden, ob nur die Antworten oder ebenfalls die Information der Anwendung eines Antwortmusters übertragen werden sollen. Auf diese Weise ist es möglich, die Fragebögen mehrerer Datenendgeräte auf einen Schlag mit einem Antwortmuster zu versorgen.

Regelmäßige Bestandserfassung

Es ist sinnvoll, die Evaluation immer an gewissen Stichtagen durchzuführen, um das aktuelle Sicherheitsniveau zu bestimmen. Die bei der Befragung gegebenen Antworten und die Historie der jeweiligen ermittelten Kategorien werden in der NIC-Online-Datenbank vorgehalten, um langfristig Aussagen über die Entwicklung des Sicherheitsniveaus treffen zu können. Die beantworteten Fragenkataloge werden direkt ausgewertet und das Ergebnis auf einer Übersichtsseite aufgezeigt. Auf diese Weise können die Resultate und weiter-führenden Auswertungen direkt zur Kenntnis genommen werden.

Weiterführende Informationen

- IT-Grundschutzkataloge/-Handbuch des BSI[82]
- ISidoR - Online-Dokumentation[83]
- Inforum - 2005/01[84]
- Inforum - 2007/01[85]

[82] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[83] https://www.nic.uni-muenster.de/Sec_Glossar/sec_handbuch.pdf
[84] https://www.uni-muenster.de/ZIV/inforum/2005-1/Welcome.html

› Inforum - 2008/01[86]

[85] https://www.uni-muenster.de/ZIV/inforum/2007-1/Welcome.html
[86] https://www.uni-muenster.de/ZIV/inforum/2008-1/Welcome.html

Anhang G | Schutzbedarfsanalyse

Diese Anlage ist ein Auszug aus der Online-Dokumentation zum ISidoR Security-Audit an der Universität Münster.

Mit diesem Fragenkatalog soll der Schutzbedarf der betreuten Daten festgestellt werden. Der Schutzbedarf definiert sich dabei ausschließlich aus den anzunehmenden Schäden, die entstehen, wenn die Daten nach einem auslösenden Ereignis (durch spezifische Bedrohungen wie Passwortkompromittierung, Ausfall des Cloud-Dienstes etc.) beeinträchtigt werden und so mindestens einer der Grundwerte der IV-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) verletzt wird. Dabei ergibt sich der Schutzbedarf aus den unmittelbaren Schäden und durch die möglichen Folgeschäden (z. B. Schadensersatzforderungen, Produktionsausfall-kosten).

Eine quantitative Bewertung mit bezifferten Schadenshöhen wäre hier zu aufwendig und ist unter verschiedenen Aspekten auch kaum möglich (z. B. negative Außenwirkungen, „Ruf der Universität“, Schädigung durch Ansehensverlust). Vielmehr soll die persönliche Wertung helfen, eine relative Bewertung aufzustellen, die für die Notwendigkeit und Umsetzung von Schutzmaßnahmen eine Dringlichkeitsreihenfolge ergibt.

Insgesamt handelt es sich um vier Themenbereiche, die aus sicherheitsrelevanten Gesichtspunkten beleuchtet werden. Dies sind:

- Verstöße gegen Gesetze,
- Beeinträchtigungen der Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung und
- finanzielle Auswirkungen.

Diese Themenbereiche werden unter den Aspekten

- Integrität/Vertraulichkeit der Daten und
- Verfügbarkeit der Daten und Dienste

betrachtet.

Schutzbedarfskategorie: „Keine“

Schäden haben nur eine unwesentliche Beeinträchtigung der Institution zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze ohne nennenswerte Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts ist nicht nennenswert. Ein möglicher Missbrauch personenbezogener Daten hat keine nennenswerten Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung ist nicht nennenswert.
Negative Außenwirkung	Es ist keine nennenswerte Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	Es ist kein nennenswerter finanzieller Schaden zu erwarten.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Es ist keine oder nur eine äußerst geringe Beeinträchtigung zu erwarten. In Ausnahmefällen liegt die maximal tolerierbare Ausfallzeit bei bis zu zwei Tagen.

Schutzbedarfskategorie: „Normal“

Schäden haben Beeinträchtigungen der Institution zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Negative Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 8 Stunden.

Schutzbedarfskategorie: „Hoch“

Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen Vertragsverletzungen mit hohen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein mögliche Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Negative Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen betroffenen als nicht

	tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden.

Schutzbedarfskategorie: „Sehr hoch“

Der Schadensfall führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche. Es besteht Gefahr für Leib und Leben von Personen.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben.
Negative Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen unter einer Stunde.

Anhang H | Das Konzept der Netzstrukturierung

Die Integration und der Betrieb von Sicherheitsfunktionen in komplexen Unternehmensnetzen ist für die Netzbetreiber eine außerordentliche Herausforderung. Am ZIV der Universität Münster wurde ein ganzheitliches Konzept *Eingebettete Sicherheitsfunktionen in strukturierten Netzen* unter Berücksichtigung der technischen Machbarkeit, der Finanzierbarkeit und der Administrierbarkeit erstellt und weitgehend in Produktionsbetrieb übernommen.

Zweck

Große Netze können nicht alleine durch Firewalls vor den zunehmenden Bedrohungen geschützt werden. In diesen klassischen Modellen wurden Schutzmaßnahmen lediglich am Netz-Perimeter installiert, um das dahinter liegende Intranet vor Angriffen aus dem Internet zu schützen. Dazu wurden Demilitarisierte Zonen (DMZ) geschaffen, in denen von außen zugängliche Dienste wie z. B. Web- oder File-Server betrieben wurden. Schutzmaßnahmen alleinig am Netz-Perimeter sind heutzutage – insbesondere für größere und komplexere Netze – vollkommen unzureichend,

- Da auch innerhalb des Intranets vielfältige wechselseitige Schutzbedürfnisse bestehen,
- Weil das Intranet ebenso Gefahren aufweisen kann wie das Internet. Viele Angriffe finden auch innerhalb des eigenen Schutzbereiches statt, und das umso wahrscheinlicher, je größer das Netz und die Anzahl der Nutzer und Nutzergruppen ist. Auch sind Angriffe von innen oft gefährlicher, da zum einen nicht damit gerechnet wird und zum anderen Insider-Wissen zu gezielteren Versuchen und Methoden führen kann. Nicht zu unterschätzen ist auch die Auswirkung der in der Regel höheren Bandbreiten im Intranet und der damit potenziell erhöhten Wirksamkeit von beispielsweise Denial-of-Service (DoS) Attacken und
- weil i. Allg. die notwendigen Firewall-Regelwerke für die diversen Kommunikationsbeziehungen zwischen Internet und Intranet schnell komplex und unübersichtlich werden. Zur weiteren Absicherung, auch innerhalb des Intranets, wurde daher häufig damit begonnen, viele dedizierte Einzelgeräte zum Schutz von z. B. Abteilungen, Arbeitsgruppen oder Gebäuden in Betrieb zu nehmen. Es ist offensichtlich, dass dies insbesondere in größeren Netzen schnell zu Problemen führt, und zwar unter anderem bezüglich Verwaltbarkeit, Flexibilität, Betrieb und letztendlich auch der Kosten.

Aufbau

Eingebettete Sicherheitsfunktionen in strukturierten Netzen ist ein Konzept für netzseitige Sicherheitsmaßnahmen, das über isolierte Maßnahmen hinausgehend Sicherheitsbedürfnisse durch strukturelle Maßnahmen (*Strukturierung*) ganzheitlich bedienen kann. Grundelemente für eine solche Strukturierung sind *Netz-zonen*, die den Kommunikations- und Sicherheitsbedürfnissen der Teilnehmer und der IT-Systeme mit ihren Anwendungen und Daten entsprechen. Netzzonen können dabei beispielsweise technisch auf IP-Subnetze oder virtuellen LANs (VLANs) abgebildet sein und über Router oder Switches mit anderen Netzzonen verbunden werden. Sie können aber auch durch übergeordnete Netzzonen gruppiert und somit hierarchisch angeordnet sein. Dies ist insbesondere deswegen relevant, da üblicherweise unternehmensinterne Strukturen auch hierarchisch organisiert sind. Eine netztopologische Entsprechung ermöglicht es, den Netzbetreibern sowohl den jeweiligen Sicherheitsbedürfnissen effizient nachkommen zu können (aufgrund entsprechend klarer Kommunikationsbeziehungen) als auch Verantwortlichkeiten und ggf. Teile des Sicherheitsmanagements an die zuständigen Abteilungen delegieren zu können (*Mandantenfähigkeit*).

Die Überlegung, dass die *Firewall* im Sinne eines *Border Defense Gateways am Netz-Perimeter* für größere Netze als alleinige Maßnahme unzureichend ist, führt zu der Schlussfolgerung, dass vielmehr alle netzseitigen Sicherheitsmaßnahmen überall auch dort im Netz zu integrieren sind, wo eine sicherheitstechnische Abgrenzung eines Bereiches gegenüber anderen Bereichen notwendig ist. Damit werden Verbände von Netzzonen aufgebaut, die nicht nur nach außen *zum Internet* geschützt sind, sondern für die auch für überschaubare Bereiche innerhalb des Zonenverbundes gleichermaßen Sicherheitsfunktionen bereitgestellt werden können.

Netzseitig einzubettende Sicherheitsfunktionen sind beispielsweise:

- Stateless Packet Screens (insbesondere als hochperformante Filter wirksam an den Interfaces der aktiven Netzkomponenten)
- Firewalls mit Stateful Packet Inspection
- Application Gateways oder Application Proxies
- Intrusion-Prevention-Systeme (IPS)
- VPN-Technologien (zur Quasi-Erweiterung von Netzzonen über hochgradig verschlüsselte und zugangskontrollierte Verbindungen, die differenziert nach Ziel- und Ausgangsnetzzone aufgebaut werden können)

Eine bedarfsweise Einbettung der genannten Sicherheitsfunktionen in ein unter Sicherheitsaspekten strukturiertes Netz unterliegt stets drei wichtigen Gesichtspunkten:

Die *technische Machbarkeit*, die *Finanzierbarkeit* und die *Administrierbarkeit*. Die technologische Machbarkeit und die Finanzierbarkeit würden sehr schnell an ihre Grenzen stoßen, wenn Netzstrukturen und funktionale Instanzen 1:1 physisch auf das Netzinventar abgebildet werden müssten. Eine hierarchische Netz-struktur mit einer Vielzahl den einzelnen Netzzonen zugeordneter Geräte (Switches, Routern, Firewalls, IPS usw.) ist kaum vorstellbar. Selbst Kabelwege müssten in solchen Szenarien im schlimmsten Fall gesondert für die einzelnen Netzzonen errichtet werden. Die Administration und das Operating einer Vielzahl von Sicherheitsfunktionen in einem solchen Netz, das anforderungsgerecht betrieben werden soll, ist für Netzbetreiber ein Schreckensszenario.

Ein Weg aus diesem Dilemma ist die konsequente Virtualisierung und Mandantenfähigkeit aller eingesetzten Systeme und Technologien:

- Durch *virtuelle LANs* (VLANs), eine bewährte Layer-2-Netztechnologie, können Netzzonen auch gebäudeübergreifend und weitgehend beliebig für jeden Endgeräteanschluss gebildet werden, ohne dass dabei jedes Mal Kabelwege speziell geschaffen werden müssten.
- Durch *Virtualisierung von Routern* – eine recht junge Layer-3-Technologie – können flexibel auch komplexe Netzzonen-Topologien aufgebaut werden, ohne dass gleich bei neuen Sicherheitsbereichen neue (physische) Router beschafft werden müssen.
- Durch *Virtualisierung von Sicherheitsfunktionen*, wie z. B. *virtuelle Firewalls* oder *virtuelle IPS* – beides ebenfalls recht neue Möglichkeiten.
- Durch *virtuelle multiple VPN-Zugangsmöglichkeiten*. Wenige, dafür aber leistungsfähige VPN-Gateways, die es erlauben, unter Beachtung der Sicherheit, Authentifizierung und Autorisierung den gleichzeitigen Zugang von verschiedenen Nutzern (oder Sites) in verschiedene Netzzonen anzubieten.

Dabei stellen i. Allg. wenige (Hardware-) Systeme die virtualisierten Funktionen in vielfachen Instanzen bereit. Die Konzentration auf wenige zentrale Standorte ermöglicht in der Folge eine verbesserte und kosten-günstigere Betriebsführung.

In dem vorgestellten Virtualisierungsansatz kann die Rolle zentraler *und* dezentraler IV-Strukturen abgebildet werden. Das Netz sollte jedoch als einheitliche Infrastruktur zentral bereitgestellt werden als Grundvoraussetzung für die korrekte Funktion des Zonenkonzeptes. Auch die eingebetteten Sicherheitsfunktionen müssen grundsätzlich der zentralen (Netz-)Administration unterliegen. Vielfach ist es jedoch illusorisch, die Detail-Konfigurationen der Sicherheitsfunktionen wie z. B. Firewall Regeln für alle Netzzonen zentral pflegen zu können, wenn man komplexere IV-Strukturen (größere Unternehmen etc.) betrachtet. Dazu ist eine tiefe Kenntnis der jeweils erforderlichen zonenspezifischen Kommunikationsmuster notwendig. Auch sind in der Regel kurze Reaktionszeiten auf Änderungswünsche oder im Störfall erwünscht.

Daher ist die *Mandantenfähigkeit* (d. h. die Bereitstellung von User-Self-Care-Mechanismen) seitens der eingesetzten Managementplattformen (für die Sicherheitsfunktionen) eine elementare Option des Konzeptes. Die jeweiligen Netzzonenverantwortlichen sollen die Möglichkeit haben, selbständig Konfigurationen einzusehen, diese ggf. ändern zu können und die Einsicht in ein dazugehöriges Reporting zu bekommen, und zwar nur bzgl. der ihren Netzzonen zugeordneten (virtuellen) Sicherheitsinstanzen.

Nutzen

Das Konzept wurde durch die Abteilung Kommunikationssysteme des ZIV für große Teilbereiche der Universität und des Universitätsklinikums Münster beginnend Mitte 2005 konkretisiert, umgesetzt und kann als weitgehend erprobt gelten. Es versetzt das ZIV als Netzbetreiber in die Lage seinen Kunden (Fachbereichen, Instituten, Kliniken sowie den Studenten und Mitarbeitern) eine ganzheitlich konzipierte netzbasierte Sicherheitsarchitektur mit intrinsischen Sicherheitsfunktionen ohne Kompromisse anbieten zu können.

Eine Einführung des Konzeptes ist dabei leicht möglich, da diese in Etappen vorgenommen werden kann. Die Maßnahmen selbst (Strukturierung, Implementierung der Sicherheitsfunktionen) als auch die Reihenfolge der Einzelschritte können den Bedürfnissen und Möglichkeiten flexibel angepasst werden. Analyse und Planung hinsichtlich der möglichen Strukturierungs- und Sicherheitsmaßnahmen führen als positiver Nebeneffekt über die verfolgten Sicherheitsziele hinausgehend zu einer Revision der IT-Servicestrukturen und damit teilweise zu einer Restrukturierung und Optimierung.

Auch aus wirtschaftlicher Sicht ist eine Einführung leicht möglich, da das Konzept die Verwendung vorhandener Ressourcen berücksichtigt bzw. diese besser ausnutzt. So werden bspw. interfacebasierte Stateless-Packet-Screens als Sicherheitsmechanismen einbezogen, die ohne Leistungseinbußen für den Netzwerkdurchsatz arbeiten (im Gegensatz zu üblichen *Firewalls*) und die bei allen marktüblichen Switch-Routern vorhanden sind. Auch vorhandene herkömmliche Systeme (ohne Virtualisierungsfunktion) können einbezogen werden.

Die Wirtschaftlichkeit der Netz- und Sicherheitsarchitektur wird verbessert, weil durch die Virtualisierung viele Sicherheitsinstanzen auf sehr wenige, dafür aber leistungsfähige Systeme verteilt werden können, deren gesamte Performance auf diese Weise optimal ausgenutzt werden kann.

Von großem Nutzen ist auch, dass weitestgehend auf proprietäre *Lösungen* verzichtet wird, um möglichst frei in der Herstellerauswahl zu bleiben. Bspw. werden Standards wie das Routing Protokoll OSPF oder der Redundanzmechanismus VRRP eingesetzt und das Konzept erlaubt jederzeit die Ankopplung konventioneller Architekturen. Vorhandene Netzinfrastrukturen können deshalb auch sanft nach diesem Konzept erweitert werden.

Grundsätzlich werden alle relevanten Systeme mit ihren Funktionen doppelt ausgelegt. Es kann auf komplexe, zumeist teure und häufig herstellerspezifische Redundanz-Features verzichtet werden, da automatische Redundanz und effizientes Load-Sharing zwischen den Systemen eine inhärente Eigenschaft der aufgebauten Routing-Hierarchie sind.

Die Einführung eines hohen Niveaus an Netzsicherheit wird in grundsätzlicher Weise durch das Konzept gefördert, insbesondere durch die wahlfreie Einbettung gewünschter Sicherheitsfunktionen an strukturell relevanten Stellen im Zusammenspiel mit der Delegation an zugehörige Administration.

Netzstrukturierung im Naturwissenschaftlichen Zentrum (NWZ)

Dem Naturwissenschaftlichen Zentrum (NWZ) gehören die Fachbereiche Physik und Chemie nebst Pharmazie und Biologie an; insgesamt sind dies etwa 30 Institute. In Zusammenarbeit von ZIV mit der für das NWZ zuständigen IV-Versorgungseinheit 4 (IVV 4) und mit den IT-Verantwortlichen der jeweiligen Institute werden die Maßnahmen geplant und durchgeführt.

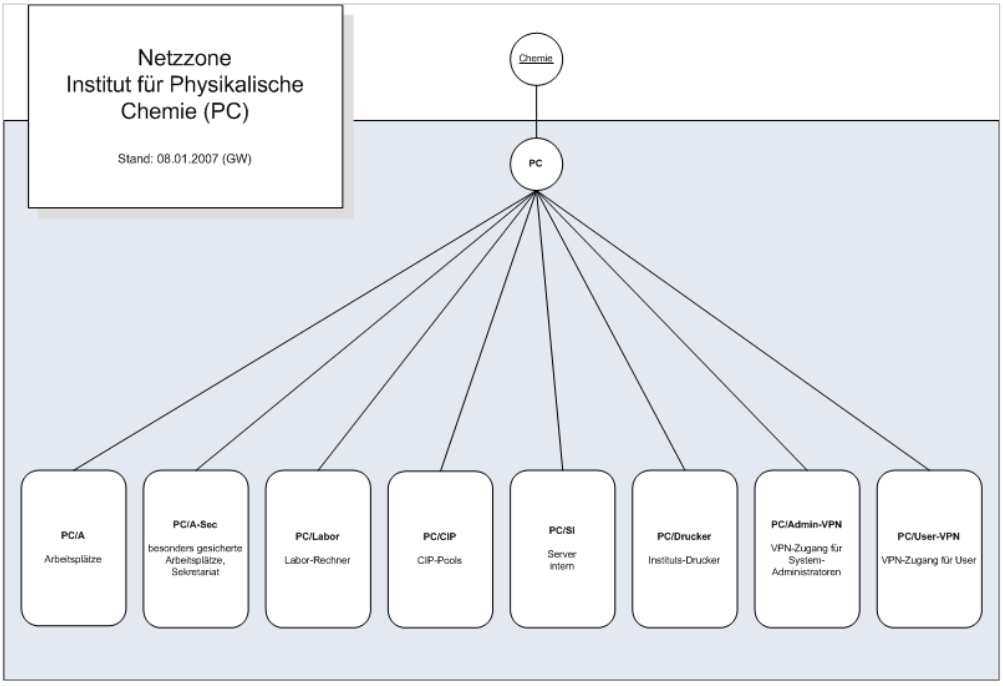
Im Wesentlichen liegt der Strukturierung jedes Institutes bzw. jeder (übergeordneten) Netzzone folgender Ablauf zugrunde:

- Treffen einiger Mitarbeiter des ZIV mit Instituts-IT-Verantwortlichen
- Vorstellung und Planung eines Instituts-Konzeptes (Netzzonenmodell)
- Feststellung der wesentlichen Verkehrsbeziehungen
- Erste Planungen für Filterregeln
- ZIV: Umsetzung des Netzzonenmodells
- Technische Änderungen/Erweiterungen der Netzinfrastruktur (ACLs, VLANs, Router, IP-Subnetze, VPN-Gateways usw.)
- Institut: Revision der eigenen Netzzone
    - Detailliertere Informationen über Verkehrsbeziehungen (für Filterregeln)
    - Vorbereitung von ggf. nötigen Umzügen von Systemen in andere oder neue Netzzonen
- Gemeinsame Durchführung der Umstellung in angekündigten Zeitfenstern
- Kontrolle und ggf. Verfeinerung des Modells

Zur Verdeutlichung der Maßnahmen und der damit zu gewinnenden IT-Sicherheit soll die Strukturierung des **Institutes für Physikalische Chemie (PC)** dienen. Die dortige Strukturierung kann auch als Prototyp verstanden und andernorts angewendet werden. So sind in der Physikalischen Chemie inzwischen folgende Netzzonen eingerichtet (vgl. Abbildung):

- **A**: allgemeine normale Arbeitsplätze, insbesondere für Instituts-Mitarbeiter.
- **A-Sec:** besonders zu sichernde Arbeitsplätze oder Endsysteme mit besonders vertraulichen Daten, wie z. B. Sekretariat, Prüfungsamt etc.
- **Labor:** Rechner in Labor- und Werkstattumgebungen. Häufig Spezialsysteme zur Geräte- und Messsteuerung. Oft keine Standard-Endsysteme, oft nicht mit Sicherheits-Updates versorgbar oder grundsätzlich leicht angreifbar.
- **CIP:** Rechner in PC-Pools für Studierende.
- **SI (Server-Intern)**: Ausschließlich für institutsinternen Zugriff installierte Server, zumeist File-, Web- oder Terminal-Server. Die Variante SE (Server-Extern) ist auch als Netzzone möglich, d. h. dann sinnvoll, wenn Instituts-Dienste Netzzonen übergeordnet angeboten werden sollen.
- **Drucker**: Netzwerkfähige institutseigene Drucker. Entweder von Arbeitsplatz-Netzzonen oder über Print-Server (in SI-Netzzone) ansprechbar.
- **User-VPN**: VPN-Gateway für die sichere Einwahl von Institutsmitgliedern von außerhalb (andere universitäre Netzzonen, Internet, Heimarbeitsplatz) in die eigenen institutsinternen Netzzonen. Die Möglichkeit des autorisierten und verschlüsselten Zugriffs via VPN bietet auch den Vorteil, die Filterregeln für die einzelnen Netzzonen gegen normalen Zugriff von außerhalb restriktiver verfassen zu können. Die Berechtigung zur Nutzung der Instituts-VPN-Gateways kann von den IT-Verantwortlichen der Institute selbständig den eigenen Mitgliedern (Studenten und Mitarbeitern) erteilt werden.

› **Admin-VPN:** VPN-Gateway zur ausschließlichen Nutzung für IT-Administratoren zum Management der Systeme in eigenen Instituts-Netzzonen (z. B. der Server). Alternativ oder ergänzend ist auch eine eigene Sysadmin-Netzzone mit fest installierten Rechnern möglich.



Die genannten Netzzonen sind inzwischen am Institut für Physikalische Chemie eingerichtet und die meisten Endgeräte-Umzüge in die neuen Bereiche vollzogen. Für jede Netzzone wurden Filterregeln abgesprochen und installiert. Im Wesentlichen wurden dabei folgende Kommunikationsregeln umgesetzt:

› Arbeitsplatzrechner dürfen (wie gewohnt) frei nach außen kommunizieren. Initiale Zugriffe von außerhalb sind nicht erlaubt.
› Server dürfen nur bzgl. ihrer Dienste erreicht werden. Wenn es Server für rein institutsinterne Dienste sind, so dürfen sie auch nur von den entsprechenden Netzzonen angesprochen werden.
› Für besonders zu sichernde Arbeitsplätze, Labor- und CIP-Pool-Rechner sind die Filterregeln sehr institutsspezifisch und müssen besprochen werden. Im Allgemeinen sind für diese Bereiche stärkere Einschränkungen sinnvoll.
› Die über User-VPN eingewählten Nutzer bekommen ähnliche Rechte wie lokale Arbeitsplätze bzw. besonders abgesicherte lokale Arbeitsplätze.

Häufig können für die Planungen der Filterregeln bereits gewonnene Erfahrungen und Regelsätze aus anderen Instituten als Vorlage genommen werden. Insbesondere sollte nicht versucht werden, gleich zu Anfang eine vollkommene Lösung anzustreben. Einfache Grundstrukturen mit einfachen Grundregeln bringen schon sehr viel. Eine feinere Justierung kann später immer noch durchgeführt werden.

Anhang I | Cloud-Richtlinie

Richtlinie der Universität Münster zur Auslagerung von Daten in Cloud-Dienste

Juni 2013

1 Einleitung

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder und Angehörige der Westfälischen Wilhelms-Universität Münster (WWU), die im Rahmen ihrer dienstlichen Tätigkeit öffentliche Cloud-Dienste (so genannte Public Clouds) zur Datenablage nutzen wollen. Sie soll der Sensibilisierung dienen, informiert über allgemeine Risiken und hilft bei der Klärung der Frage, in welchen Fällen oder unter welchen Bedingungen Cloud-Dienste genutzt werden dürfen.

Wenn Daten mit Hilfe von Cloud-Diensten gespeichert bzw. verarbeitet werden, drohen spezielle Gefahren. Insbesondere die dynamische Verteilung der Speicherkapazitäten über verschiedene Standorte, die in der Regel dem Nutzer nicht bekannt sind, verlangen eine spezifische Vorsorge hinsichtlich der Informationssicherheit und des Schutzes der Daten.

Für die Verarbeitung personenbezogener Daten in der Cloud gelten die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW). Es fordert entweder die Einwilligung der Betroffenen (im Fall der Datenverarbeitung außerhalb der EU), oder die Anwendung der Regelungen zur Auftragsdatenverarbeitung (Datenverarbeitung innerhalb der EU). Zusätzlich sind die universitätsinternen Regelungen zu beachten (vgl. Regelungen zur IV-Sicherheit an der WWU [1]).

Im privaten Umfeld werden Cloud-Dienste häufig relativ sorglos genutzt. Vor dem Hintergrund der sich immer mehr auflösenden Trennung von privaten und dienstlichen Belangen, speziell im IT-Umfeld, soll diese Richtlinie zur Sensibilisierung gegenüber den potentiellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

2 Geltungsbereich

Diese Richtlinie gilt für alle Mitglieder und Angehörige der WWU, wenn sie im Rahmen dienstlicher Tätigkeiten für die WWU Daten erheben, speichern oder verarbeiten.

3 Abgrenzung und Begriffsdefinition

IT-Dienste, die unabhängig von Ort und Zeit über ein Daten- oder Kommunikationsnetz genutzt werden können, werden allgemein als „Cloud Computing“ bezeichnet. Allerdings existieren verschiedene leicht variierende Definitionen des Begriffs. Im Folgenden benutzen wir eine Begriffsdefinition, die sich an die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegte Definition des Begriffs Cloud Computing anlehnt:

> *Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. In der Regel können diese IT-Dienstleistungen unabhängig von Ort und Zeit mit Hilfe aller gängigen IT-Geräte genutzt werden. Für die Nutzer bleibt die bereitgestellte IT-Infrastruktur verborgen. [2]*

Diese Richtlinie betrachtet Aspekte der Speicherung von Daten, also der kurzzeitigen oder längerfristigen Überlassung von Daten an externe Dienstanbieter, mit Hilfe von Cloud Services. Weitere Cloud-Angebote, wie zum Beispiel Office-Dienste oder Rechenleistung, werden nicht behandelt.

4 Datenkategorien und ihre Eignung zur Cloud-Nutzung

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in die Cloud in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur. Der Schutzbedarf von Daten ist an der WWU mittels der im ISidoR - Security-Audit festgelegten Schutzbedarfsanalyse[87] zu bestimmen.

[87] Siehe Anhang G | Schutzbedarfsanalyse

Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden. Daten lassen sich in die folgenden Kategorien einteilen

Kategorie	Hinweis auf typischen Schutzbedarf
Daten, die aus öffentlich zugänglichen Quellen stammen	Keinen
Dienstliche (nicht wissenschaftliche) Daten (z. B. aus den Bereichen Verwaltung und Lehre)	Hoch bis sehr hoch
Wissenschaftliche Daten (z. B. Untersuchungsergebnisse, Messreihen)	Normal bis sehr hoch
Personalaktendaten	Sehr hoch
Private Daten[88] (z. B. Kontaktdaten von Freunden)	Normal bis sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

› Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes.
› Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Ein Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele ***Verfügbarkeit***, ***Integrität*** und ***Vertraulichkeit*** differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in der Cloud:

Schutzbedarf	Eignung für die Ablage
Daten mit keinem oder normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	nein

5 Regelungen

Bevor Daten in der Cloud abgelegt werden, müssen die im vorangegangenen Abschnitt 4 - Datenkategorien und ihre Eignung zur Cloud-Nutzung betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden. Darüber hinaus gelten die in diesem Abschnitt aufgestellten Regelungen.

5.1 Sparsamer Umgang

Prinzipiell sollten bei der Nutzung entsprechender Cloud-Dienste, die in Frage kommen, die Datenmengen auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume in die Cloud leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der WWU nicht verlassen dürfen. Bevor Daten auf Speichersysteme externer Anbieter ausgelagert werden, müssen erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

5.2 Vorrangig Dienste der WWU nutzen

Services, die von IT-Dienstleistungszentren der WWU (insbesondere ZIV und IVVen) bereitgestellt werden, sind Cloud-Diensten externer Anbieter vorzuziehen. Nur wenn der benötigte Dienst nicht von Einrichtungen der WWU bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, darf unter Beachtung der hier formulierten Grundsätze auf Angebote externer Anbieter zurückgegriffen werden. Die

[88] Unter Berücksichtigung der Duldung der geringfügigen privaten Nutzung von Internet und E-Mail an der WWU (vgl. Benutzungsordnung des ZIV und der IVVen § 2 (2)) wird auch diese Datenkategorie berücksichtigt.

aktuell verfügbaren Dienste der universitären IT-Dienstleistungszentren können beispielsweise bei der IVV der jeweiligen Einrichtung erfragt werden.

5.3 Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

Aus dem Schutzbedarf der für eine Auslagerung vorgesehenen Daten folgt nicht nur, ob eine Auslagerung zulässig ist sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten:

5.3.1 Verfügbarkeit

Es muss vorab geprüft werden, welche Aussagen der Anbieter des Cloud-Dienstes zur Verfügbarkeit macht. Wenn sehr hohe Anforderungen an die Verfügbarkeit gestellt werden, kommt eine Datenablage in der Cloud nur in Frage, wenn der Anbieter des Cloud-Dienstes eine sehr hohe Verfügbarkeit garantiert.

5.3.2 Integrität

Die Unverfälschbarkeit der Daten (Integrität) wird im Allgemeinen von Anbietern von Cloud-Speichern nicht garantiert. Wenn in dieser Hinsicht hohe oder sogar sehr hohe Anforderungen bestehen, muss der Nutzer selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können Prüfsummen verwendet werden, mit deren Hilfe eine Veränderung an den Daten erkannt werden kann. In Systemen zur Datenverschlüsselung (siehe Absatz 5.3.3 - Vertraulichkeit) sind derartige Verfahren in der Regel bereits integriert.

5.3.3 Vertraulichkeit

Wenn *hohe Anforderungen* an die Vertraulichkeit gestellt werden, ist als adäquate Maßnahme der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Viele Anbieter von Speicherplatz in der Cloud bieten auch Dienste zur Datenverschlüsselung an. Bei der Nutzung dieser Verschlüsselungsdienste ist in der Regel nicht zuverlässig nachvollziehbar, wer Zugriff auf die Schlüssel und damit auf die Daten hat. Der Zugriff des Dienstanbieters auf die Schlüssel muss ausgeschlossen sein. Darum sollte die Verschlüsselung selbst vorgenommen werden, bevor die Daten in die Cloud übertragen werden. Die Sicherheit verschlüsselter Daten hängt u.a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung muss darauf geachtet werden, dass sie nach allgemein anerkannten Regeln als sicher gilt.

Bei Daten mit *sehr hohen Anforderungen* an die Vertraulichkeit ist grundsätzlich von der Ablage in der Cloud abzusehen. Wenn in sehr seltenen Fällen dennoch derartige Daten in die Cloud ausgelagert werden müssen, sind die Daten zwingend vorher zu verschlüsseln. In diesem Fall muss die Verschlüsselung inklusive des Schlüsselmanagements unter der vollständigen Kontrolle durch kompetente Stellen der WWU (z. B. ZIV) erfolgen.[89]

5.4 Löschung von Daten

Anbieter von Cloud-Speicher setzen normalerweise Speichertechniken zur effizienten Ausnutzung der physikalischen Speicherkapazitäten ein. Aufgrund dieser Speichertechnik können Daten oft erst nach einer gewissen Zeitspanne gelöscht werden. Grundsätzlich kann nicht ausgeschlossen werden, dass beim Absetzen des Löschbefehls die Daten lediglich für den Anwender ausgeblendet, aber nicht gelöscht werden. Daher sind Daten, die einer beispielsweise gesetzlichen Löschverpflichtung unterliegen, für die Ablage in der Cloud ungeeignet.

5.5 Dienstrechtliche Vorgaben beachten

Insbesondere für Daten der Verwaltung (vor allen Dingen Personal- und Haushaltsdaten) existieren oft detaillierte Vorschriften, wie mit diesen Daten umzugehen ist. Beispielsweise regeln verschiedene Vorschriften, dass Personalakten die Personalabteilung nicht ohne weiteres verlassen dürfen. Somit dürfen derartige Personaldaten auch nicht auf Speicher außerhalb der WWU abgelegt werden. Inwieweit bei der Datenspeicherung dienstrechtlich Vorschriften zu beachten sind, muss im Zweifel unter Einbeziehung des jeweiligen Vorgesetzten geklärt werden.

5.6 WWU-interne Regelungen beachten

Als Ergänzung oder Konkretisierung gesetzlicher Bestimmungen und Vorschriften gilt eine Reihe von universitätsinternen Regelwerken.

---

[89] Die WWUCA bietet allen Angehörigen und Einrichtungen der Universität Münster, des Universitätsklinikums Münster und der Kunstakademie Münster das Ausstellen von X.509-Zertifikaten an.

5.7 Allgemeine Empfehlungen

Ergänzend zu den zuvor angesprochenen Themenbereichen sollten noch weitere Punkte beachtet werden:

Cloud-Betreiber mit Firmensitz außerhalb der EU	Ein Umgang mit den Daten der Kunden gemäß den europäischen Datenschutzbestimmungen kann hier nicht vorausgesetzt werden. Insbesondere ist häufig unklar, welche Personen oder welche Stellen Zugriff auf die Daten erlangen. Für die Übermittlung personenbezogener Daten sind besondere Datenschutzvorschriften einzuhalten.
SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters	Vor der Inanspruchnahme eines Dienstes müssen die (vertraglichen) Bedingungen, unter denen der Dienst genutzt wird, bekannt und akzeptabel sein.
Zertifizierung des Anbieters	Wie ernst ein Anbieter die Sicherheit und den Schutz der Kundendaten nimmt, kann u.a. an dem Vorhandensein von anerkannten Prüfbescheinigungen (beispielsweise ISO 27001, entspricht BSI 100-1) abgelesen werden.

Weitere Aspekte können die Wahl des Anbieters bzw. des Cloud-Services beeinflussen (Performance, Bedienbarkeit und Handhabung der Anwendung, Kosten).

Siehe hierzu Abschnitt 7 - Weiterführende Dokumente.

6 Zusammenfassung

Der folgende Fragenkatalog soll bei der Eignungsprüfung des Cloud-Angebots helfen.

1 **Prüfung Interner Angebote**
   - Wurde das Angebot der inneruniversitären IT-Dienstleister (insbesondere ZIV, IVVen) geprüft?
   - Ist ein WWU-Service zur Ablage der Daten geeignet?

2 **Prüfung der Vertragsbedingungen des externen Anbieters**
   - Wurden die SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters angesehen?
   - Passen die Bedingungen des Anbieters zu den Anforderungen?

3 **Prüfung der Verfügbarkeit**
   - Erfüllt der Cloud-Dienst die Anforderungen an die Verfügbarkeit der Daten?

4 **Prüfung der Integrität**
   - Erfüllt der Cloud-Dienst die Anforderungen an die Integrität der Daten?
   - Wurden Vorkehrungen getroffen, hohe Integritätsanforderungen zu erfüllen?

5 **Unverschlüsselte Ablage**
   - Gestatten die Anforderungen hinsichtlich der Vertraulichkeit der Daten eine unverschlüsselte Ablage in der Cloud?

6 **Verschlüsselte Ablage**

   Wenn die Anforderungen hinsichtlich der Vertraulichkeit der Daten nur eine verschlüsselte Ablage in der Cloud erlauben:
   - Wird die Verschlüsselung vor der Abspeicherung durchgeführt?
   - Werden die Schlüssel im Bereich der WWU abgelegt?

7 **Personenbezug**

   Wenn personenbezogene Daten in der Cloud abgelegt werden sollen:
   - Wurde geprüft, ob alle datenschutzrechtlichen Anforderungen, insbesondere hinsichtlich der Auftragsdatenverarbeitung, erfüllt sind?

8 **Einhaltung der Vorschriften**
   - Wurde geprüft, ob gesetzliche oder andere Vorschriften die Ablage der Daten auf Systemen außerhalb der WWU erlauben?

9 Löschung

- Wurde geprüft, ob die Daten bestimmten Löschfristen unterliegen?
- Genügen die vom Cloud-Dienstanbieter bereit gestellten Dienste diesen Anforderungen?

7 Weiterführende Dokumente

[1] A. d. L. W. R. i. N. (ARNW), „Regelungen zur IV-Sicherheit in der Universität Münster," 21 02 2002. [Online]. https://www.uni-muenster.de/Rektorat/abuni/ab020507.html.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter," [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf.

[3] AG IT-Sicherheit, Freie Universität Berlin, Kaiserswerther Str. 16/18, 14195 Berlin, „Richtlinie zur Auslagerung von Daten in die Cloud," 2 Dezember 2011. [Online]. http://www.mi.fu-berlin.de/wiki/pub/IT/ItProcess/Richtlinie_Cloud-Datenablage_-_1_0.pdf.

[4] T. Weichert, „Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein," [Online]. https://www.datenschutzzentrum.de/cloud-computing/.

[5] Bundesministeriums für Wirtschaft und Technologie, „Sichere Internet-Dienste – Sicheres Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)," [Online]. http://www.trusted-cloud.de/.

[6] „Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder," [Online]. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf.

Impressum

Westfälische Wilhelms-Universität Münster

IV-Sicherheitsteam

Röntgenstr. 7-13

48149 Münster

Mit freundlicher Genehmigung der AG IT-Sicherheit der Freien Universität Berlin wurde diese Richtlinie auf Basis der entsprechenden Richtlinie der FU Berlin [3] erstellt.

Angepasst durch Michael Engemann für das IV-Sicherheitsteam der WWU.

Ansprechpartner: Thorsten Küfer, thorsten.kuefer@uni-muenster.de

Anhang J | Empfehlungen für die Verwendung des Cloudspeicherdienstes „sciebo“

IV-Sicherheitsteam der WWU – November 2014

Dieses Dokument soll darüber aufklären, welche Daten von Mitgliedern und Angehörigen der WWU in „sciebo“ verarbeitet werden dürfen und welche nicht. Es ist eine Anwendung der Cloud-Richtlinie [1] der WWU auf die speziellen Gegebenheiten des „sciebo“ genannten Cloudspeicherdienstes. Grundsätzlich ist darauf hinzuweisen, dass der Dienst nur zu Zwecken von Forschung, Lehre und Studium genutzt werden darf.

Die in „sciebo“ gespeicherten Daten befinden sich auf Servern der WWU in Münster oder ihrer Kooperationspartner in Bonn und Duisburg-Essen, für die Speicherung und Verarbeitung gilt daher das deutsche Datenschutzgesetz. Der Zugriff auf die Daten kann mittels einer Clientsoftware oder durch einen Webbrowser erfolgen. Die Clientsoftware hält die Daten auf allen mit einem „sciebo“-Konto verbundenen Geräten synchron. Dadurch passiert es schnell, das evtl. schützenswerte Daten auf unzureichend geschützte Endgeräte gelangen. Auf Grund der Regelungen zur IV-Sicherheit an der WWU [2] dürfen personenbezogene Daten nur auf Servern gespeichert werden und sind ggfs. zu verschlüsseln. Die Endnutzerordnung von „sciebo“ untersagt insbesondere die Speicherung personenbezogener Daten Dritter ohne deren Einwilligung. Über einen Webbrowser kann aus der ganzen Welt mittels einer Nutzername/Passwort-Kombination auf die Daten zugegriffen werden. Der Zugriff kann auch mit oder ohne Passwort über einen speziellen Link erfolgen, um Daten mit anderen zu teilen.

Schutzbedarf

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in „sciebo“ in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur. Der Schutzbedarf von Daten ist an der WWU mittels der am ISidoR - Security-Audit angelehnten Schutzbedarfsanalyse zu bestimmen (vgl. Seite 88).

Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden. Daten lassen sich in die folgenden Kategorien einteilen:

Kategorie	Hinweis auf typischen Schutzbedarf
Daten, die aus öffentlich zugänglichen Quellen stammen	Keinen
Dienstliche (nicht wissenschaftliche) Daten (z. B. Prüfungsergebnisse, Gutachten)	Normal bis sehr hoch
Wissenschaftliche Daten (z.B. Untersuchungsergebnisse, vertrauliche Forschungsdaten)	Normal bis sehr hoch
Personalaktendaten	Sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten gelten die Bestimmungen des Datenschutzes
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Der Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* differenziert bestimmt. Entsprechend differenziert sollten Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in „sciebo“:

Schutzbedarf	Eignung für die Ablage
Daten mit keinem oder normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	nein

Empfehlungen

Bevor Daten in „sciebo“ abgelegt werden, sollten die im vorangegangenen Abschnitt betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden.

Sparsamer Umgang

Prinzipiell sollte bei der Nutzung von „sciebo“ die Datenmenge auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume in die Cloud leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Einrichtung nicht verlassen dürfen. Bevor Daten auf Endgeräte synchronisiert werden, sollten erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

Aus dem Schutzbedarf der für eine Speicherung vorgesehenen Daten folgt nicht nur, ob eine Speicherung zulässig ist sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten.

Verfügbarkeit

Die Daten in „sciebo“ befinden sich an einem von drei Standorten in NRW. Es gibt keine serverseitigen Backups der Daten. Beim Ausfall eines Standorts könnten die Daten daher zeitweise oder dauerhaft nicht für den Webzugriff oder zur Synchronisation zur Verfügung stehen. Die WWU haftet nicht für Schäden aus dem Verlust von Daten. Der Endnutzer ist für Datensicherungen verantwortlich.

Wenn *sehr hohe Anforderungen* an die Verfügbarkeit gestellt werden, kommt eine Datenablage in „sciebo“ nicht in Frage.

Integrität

Die technische Sicherstellung der Datenintegrität erfolgt durch spezielle Speichersysteme. Die Wahrscheinlichkeit von unerkannten Fehlern in den Daten ist sehr gering aber nicht ausgeschlossen. Auf Grund der Nutzung über das Internet und der höheren Nutzerzahl bietet „sciebo“ eine größere Angriffsfläche als Dienste, die ausschließlich WWU-intern angeboten werden. Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten ist eine Datenmanipulation durch unberechtigte Personen möglich.

Wenn in dieser Hinsicht *hohe* oder sogar *sehr hohe Anforderungen* bestehen, sollte der Nutzer selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können Prüfsummen verwendet werden, mit deren Hilfe eine Veränderung an den Daten erkannt werden kann. In Systemen zur Datenverschlüsselung sind derartige Verfahren in der Regel bereits integriert.

Vertraulichkeit

Die Einhaltung der Datenschutzvorschriften wird durch die beteiligten Hochschulen sichergestellt. Insbesondere werden Daten nicht an Privatunternehmen weitergegeben, nicht durch diese verarbeitet und auch nicht außerhalb des Gebietes der Bundesrepublik Deutschland abgespeichert. „sciebo“ bietet eine größere Angriffsfläche als ein nur WWU-intern angebotener Dienst. Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten könnten unberechtigte Personen an vertrauliche Daten gelangen.

Wenn *hohe Anforderungen* an die Vertraulichkeit gestellt werden, ist als adäquate Maßnahme der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Es wird keine serverseitige Verschlüsselung angeboten, da diese keinen ausreichenden Schutz bietet. Darum sollte die Verschlüsselung selbst vorgenommen werden, bevor die Daten in die Cloud übertragen werden. Die Sicherheit verschlüsselter Daten hängt u.a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung sollte darauf geachtet werden, dass sie nach allgemein anerkannten Regeln als sicher gilt.

Bei Daten mit *sehr hohen Anforderungen* an die Vertraulichkeit ist grundsätzlich von der Ablage in „sciebo“ abzusehen. Wenn in sehr seltenen Fällen dennoch derartige Daten in die Cloud ausgelagert werden müssen, sind die Daten zwingend vorher zu verschlüsseln. In diesem Fall sollte die Verschlüsselung inklusive des Schlüsselmanagements unter der vollständigen Kontrolle durch kompetente Stellen der Einrichtung erfolgen.

Schutzbedarfsanalyse

Mit dem folgenden Fragenkatalog soll der Schutzbedarf der betreuten Daten festgestellt werden. Der Fragenkatalog ist angelehnt an die Richtlinien zum IT-Grundschutz des Bundesamts für Sicherheit in der In-

formationstechnik (BSI). Die Schutzbedarfsanalyse wird an der WWU mit dem Security-Audit ISidoR [3] durchgeführt.

Der Schutzbedarf definiert sich dabei ausschließlich aus den anzunehmenden Schäden, die entstehen, wenn die Daten nach einem auslösenden Ereignis (durch spezifische Bedrohungen wie Passwortkompromittierung, Ausfall eines Dienstes, Verlust eines Datenträgers etc.) beeinträchtigt werden und so mindestens einer der Grundwerte der IV-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) verletzt wird. Dabei ergibt sich der Schutzbedarf aus den unmittelbaren Schäden und durch die möglichen Folgeschäden (z.B. Schadensersatzforderungen, Produktionsausfallkosten).

Eine quantitative Bewertung mit bezifferten Schadenshöhen wäre hier zu aufwendig und ist unter verschiedenen Aspekten auch kaum möglich (z.B. negative Außenwirkungen, "Ruf der Institution", Schädigung durch Ansehensverlust). Vielmehr soll die persönliche Wertung helfen, eine relative Bewertung aufzustellen, die für die Notwendigkeit und Umsetzung von Schutzmaßnahmen eine Dringlichkeitsreihenfolge ergibt.

Insgesamt handelt es sich um vier Themenbereiche, die aus sicherheitsrelevanten Gesichtspunkten beleuchtet werden. Diese sind:

- Verstöße gegen Gesetze,
- Beeinträchtigungen der Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung und
- Finanzielle Auswirkungen.

Diese Themenbereiche werden betrachtet unter den Aspekten:

- Integrität/Vertraulichkeit der Daten und
- Verfügbarkeit der Daten und Dienste

Schutzbedarfskategorie: „Keine“

Schäden haben nur eine unwesentliche Beeinträchtigung der Institution oder anderer an „sciebo“ teilnehmenden Institutionen zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze ohne nennenswerte Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts ist nicht nennenswert. Ein möglicher Missbrauch personenbezogener Daten hat keine nennenswerten Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung ist nicht nennenswert.
Negative Außenwirkung	Es ist keine nennenswerte Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	Es ist kein nennenswerter finanzieller Schaden zu erwarten.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Es ist keine oder nur eine äußerst geringe Beeinträchtigung zu erwarten. In Ausnahmefällen liegt die maximal tolerierbare Ausfallzeit bei bis zu zwei Tagen.

Schutzbedarfskategorie: „Normal“

Schäden haben Beeinträchtigungen der Institution oder anderer an „sciebo“ teilnehmenden Institutionen zur Folge.

Vertraulichkeit und Integrität der Daten

Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Negative Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 8 Stunden.

Schutzbedarfskategorie: „Hoch“

Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution oder anderer an „sciebo“ teilnehmenden Institutionen ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst, anderer an „sciebo“ teilnehmenden Institutionen, oder betroffener Dritter zur Folge.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen Vertragsverletzungen mit hohen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein mögliche Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Negative Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden.

Schutzbedarfskategorie: „Sehr hoch“

Der Schadensfall führt zum totalen Zusammenbruch der Institution oder anderer an „sciebo“ teilnehmenden Institutionen, oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche, oder es besteht Gefahr für Leib und Leben von Personen.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben.
Negative Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.
Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen unter einer Stunde.

Weitere Informationen

[1] IV-Sicherheitsteam, „Cloud-Richtline,“ Juni 2013. [Online]. Available: https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2015/ausgabe02/beitrag03.pdf.

[2] A. d. L. W. R. i. N. (ARNW), „Regelungen zur IV-Sicherheit in der Universität Münster,“ 21 Feb 2002. [Online]. Available: https://www.uni-muenster.de/Rektorat/abuni/ab020507.html.

[3] T. Rensing, „ISidoR Onlinedokumentation,“ 24 November 2010. [Online]. Available: https://www.nic.uni-muenster.de/Sec_Glossar/sec_handbuch.asp.

Anhang K | Empfehlungen zum dienstlichen Umgang mit Mobilgeräten

Laptop, Smartphone, Tablet & Co.

IV-Sicherheitsteam, November 2014

1 Einleitung

Dieser Leitfaden beinhaltet grundsätzliche Empfehlungen für alle Mitglieder und Angehörige der Westfälischen Wilhelms-Universität Münster (WWU), die zu dienstlichen Zwecken mobile Endgeräte (u. a. Laptops, Smartphones, Tablet-PCs) einsetzen. Dieser Leitfaden soll der Sensibilisierung dienen. Es handelt sich dabei lediglich um die Übertragung von bereits bestehenden Regelungen der WWU auf die Neuerungen in der Informationsverarbeitung.

Mobilgeräte werden immer kleiner, leistungsfähiger und sind bei vielen Mitarbeitern nicht mehr aus dem Alltag wegzudenken. Die Benutzung solcher Geräte hat sich in den letzten Jahren vervielfacht und dieser Trend wird sich weiter fortsetzen.

Auf Laptops kommen dafür herkömmliche Desktop-Betriebssysteme (v. a. Windows und OS X) zum Einsatz und es lassen sich die dort üblichen Sicherheitsregelungen umsetzen. Auf Smartphones und Tablets laufen dagegen spezielle, an das Gerät angepasste Betriebssysteme (v. a. Android, iOS und Windows Phone), deren Bedienung sich von Desktop-Betriebssystemen unterscheidet. Heutige Smartphones werden hauptsächlich für den Consumer-Bereich entwickelt und sind auf einfache Benutzung ausgelegt, daher unterstützen sie teilweise nur rudimentäre Sicherheitsfeatures.

Darüber hinaus birgt die Nutzung von Mobilgeräten erhöhte Sicherheitsrisiken:

- Verlust oder Diebstahl des Gerätes und dadurch unter Umständen Zugriff auf vertrauliche Daten durch Unbefugte
- Manipulation des Gerätes durch bösartige Software/Apps
- Unbeabsichtigter, automatischer Datenabfluss an externe Cloud-Dienste

Dieser Leitfaden soll zur Sensibilisierung gegenüber potentiellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

2 Geltungsbereich

Die Empfehlungen dieses Dokuments richten sich an alle Mitglieder und Angehörige der WWU, die Mobilgeräte zu dienstlichen Zwecken nutzen. Sie gelten auch für dienstlich genutzte Privatgeräte, sofern diese eingesetzt werden.

Alle Nutzer eines Mobilgerätes sind für die Absicherung ihres Gerätes und der darauf befindlichen Daten in der Regel selbst verantwortlich. Durch den Nutzer muss sichergestellt werden, dass eine qualifizierte Person die Verantwortung für die sachgerechte Betreuung übernimmt. Dies kann grundsätzlich auch der Nutzer selbst sein, alternativ kann die Administration durch einen ausgewiesenen IT-Administrator der ihn DV-technisch betreuenden Einrichtung erfolgen (vgl. [1]).

2.1 Dienstliche Mobilgeräte

Für dienstliche Mobilgeräte wird die Umsetzung der in diesem Leitfaden aufgeführten Empfehlungen dringend angeraten. Die Empfehlungen sollen das Risiko des ungewollten Abflusses von Daten an Dritte verringern. Die wichtigste Regel lautet, so wenig dienstliche Daten wie möglich auf dem Gerät zu speichern (Prinzip der Datensparsamkeit). Vom Speichern von privaten Daten auf dienstlichen Geräten wird abgeraten. Bei Nutzung des zentralen Microsoft Exchange Systems werden durch den ActiveSync Client auf den meisten Mobilgeräten einige der empfohlenen Sicherheitseinstellungen und Anforderungen automatisch aktiviert.

2.2 Private Mobilgeräte

Auch für dienstlich genutzte Privatgeräte werden die in diesem Leitfaden beschriebenen Empfehlungen dringend angeraten. Es gelten zusätzlich alle allgemeinen Regelungen zu Datenschutz und Datensicherheit. Bei Nutzung des zentralen Microsoft Exchange Systems werden durch den ActiveSync Client auf den meisten Mobilgeräten einige der empfohlenen Sicherheitseinstellungen und Anforderungen automatisch aktiviert.

Es wird darauf hingewiesen, dass die dienstliche Nutzung von Privatgeräten, neben den Gefahren für die Informationssicherheit der WWU, auch ein Risiko für die Daten des Nutzers darstellt, da unter anderem die fehlerfreie Funktion der Geräte und des Verwaltungssystems (Microsoft Exchange etc.) nicht garantiert werden kann. Im Falle eines Defektes oder Anwenderfehlers kann es zum Verlust der auf dem Gerät gespeicherten Daten kommen. Von der dienstlichen Nutzung privater Geräte wird daher abgeraten. Die WWU schließt dies-bezüglich sämtliche Haftungsansprüche aus (vgl. Benutzungsordnung des ZIV und der IVVen [2] § 9).

2.3 Datenkategorien und ihre Eignung zur mobilen Nutzung

Im Allgemeinen sollten stets so wenige Daten wie möglich auf Mobilgeräten gespeichert werden. Zusätzlich sind bestimmte Daten für die Speicherung zur mobilen Nutzung von vorneherein ungeeignet. Für die Entscheidung, welche Daten auf Mobilgeräten gespeichert werden können, bildet ihr Schutzbedarf die grundlegende Richtschnur. Dazu wurde an der WWU im ISidoR - Security-Audit eine Schutzbedarfsanalyse[90] entwickelt, die hierzu herangezogen werden sollte. Die Schutzbedarfsanalyse weist lediglich auf einen typischen Schutzbedarf hin, der tatsächliche Bedarf ist jedoch vom Inhalt der Daten abhängig und kann vom Empfohlenen abweichen.

Daten lassen sich in die folgenden Kategorien einteilen:

Kategorie	Hinweis auf typischen Schutzbedarf
Daten, die aus öffentlich zugänglichen Quellen stammen	Keiner
Dienstliche (nicht wissenschaftliche) Daten (z. B. aus den Bereichen Verwaltung und Lehre)	Normal bis sehr hoch
Wissenschaftliche Daten (z. B. Untersuchungsergebnisse, Messreihen)	Normal bis sehr hoch
Personalaktendaten	Sehr hoch
Private Daten (z. B. Kontaktdaten von Freunden)	Normal bis sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Der Schutzbedarf der Daten wird grundsätzlich hinsichtlich der drei Schutzziele *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung auf dem Mobilgerät:

Schutzbedarf	Eignung für die Ablage
Daten mit keinem bis normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	nein

2.4 Empfehlungen für Laptops

Die folgenden Empfehlungen gelten für Laptops, Tablet-PCs etc., die mit herkömmlichen Betriebssystemen wie z. B. Windows, OS X oder Linux betrieben werden.

2.5 Absicherung des Gerätes gegen unbefugten Zugriff

Jeder Nutzer sollte folgende Sicherheits-Regelungen befolgen:

- Sperrung des Gerätes mithilfe einer PIN bzw. eines Kennwortes

[90] Siehe Anhang G | Schutzbedarfsanalyse

- Automatische Sperrung des Gerätes bei Inaktivität
- Die Festplatte des Gerätes sollte verschlüsselt sein, falls Daten mit hohem Schutzbedarf darauf gespeichert werden.
- Das Gerät sollte stets sicher verwahrt werden und es sollte keine Weitergabe des entsperrten Gerätes an Dritte erfolgen.
- Bei der Verwendung von öffentlichen, ungesicherten Netzen (z. B. WLAN-Hotspots) sollte eine sichere verschlüsselte Verbindung genutzt werden (z. B. VPN).
- Die Nutzung und der Anschluss von Datenträgern und Geräten aus unbekannter Herkunft sollte vermieden werden.

2.6 Umgang mit Betriebssystem und Software

Jeder Nutzer sollte bei der Installation und Verwendung von Betriebssystem und zusätzlicher Software folgende Punkte beachten:

- Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Programme
- Installation des vom ZIV empfohlenen Virenschutzes und einer Personal Firewall
- Installation von Software nur aus vertrauenswürdigen Quellen (z. B. Hersteller-Webseite)
- Überprüfung der Nutzungsbedingungen einer Software. Software, die nur für den Privatgebrauch kostenfrei zur Verfügung steht, muss für kommerzielle Nutzung, Forschung und dienstliche Zwecke gegebenenfalls ordnungsgemäß lizenziert werden.
- Deinstallation von Software, die nicht (mehr) benötigt wird

2.7 Nutzung von Cloud-Diensten

Cloud-Dienste sollten entsprechend der Cloud-Richtlinie [3] der WWU verwendet werden.

2.8 Verlust des Gerätes

Bei Verlust eines dienstlichen Mobilgerätes sollte umgehend die DV-technisch betreuende Einrichtung informiert werden, die das Gerät administriert (meist IVV oder IT-Administrator). Ferner sollte der Nutzer unmittelbar seine Passwörter von verwendeten Kennungen der WWU ändern, um eine unberechtigte Nutzung seines Zuganges auszuschließen.

2.9 Ausmusterung von nicht ausreichend abzusichernden Geräten

Mobilgeräte, die weder durch die DV-technisch betreuende Einrichtung noch durch den Nutzer hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken genutzt werden und fachgerecht ausgemustert werden (sichere Löschung der darauf vorhandenen Daten, Entsorgung über zuständige IVV).

3 Empfehlungen für Smartphones, Tablets etc.

Die folgenden Empfehlungen gelten für Smartphones, Tablets etc., die mit mobilen Betriebssystemen wie z. B. Android, iOS oder Windows Phone betrieben werden.

3.1 Absicherung des Gerätes gegen unbefugten Zugriff

Grundsätzlich sollten folgende Sicherheits-Regelungen beachtet werden:

- Sperrung des Gerätes mithilfe einer PIN bzw. eines Kennwortes
- Automatische Sperrung des Gerätes bei Inaktivität
- Der Festspeicher des Gerätes sollte verschlüsselt sein, falls Daten mit hohem Schutzbedarf darauf gespeichert werden; wenn zusätzlich zum Festspeicher Speicherkarten dauerhaft in dem Gerät eingesetzt werden, sollten diese ebenfalls verschlüsselt werden.
- Das Gerät sollte stets sicher verwahrt werden und es sollte keine Weitergabe des entsperrten Gerätes an Dritte erfolgen.
- Nicht benötigte Schnittstellen sollten bei Nichtnutzung deaktiviert werden (z. B. Bluetooth, WLAN, Entwicklermodus).
- Das Gerät sollte nicht über den USB-Anschluss an unbekannten Quellen angeschlossen werden; auch nicht um den Akku des Gerätes zu laden (z. B. öffentliche Ladestationen an Flughäfen).
- Bei der Verwendung von öffentlichen, ungesicherten Netzen (z. B. WLAN-Hotspots) sollte eine sichere verschlüsselte Verbindung genutzt werden (z. B. VPN).

3.2 Umgang mit Betriebssystem und Apps

Jeder Nutzer sollte bei der Installation und Verwendung von Betriebssystem und Apps folgende Punkte beachten:

- Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Apps
- Installation des vom ZIV empfohlenen Virenschutzes sofern möglich
- Installation von Apps nur aus den offiziellen App-Stores (z. B. Google Play für Android bzw. App Store für iOS)
- Überprüfung der Nutzungsbedingungen einer App. Apps, die nur für den Privatgebrauch kostenfrei zur Verfügung stehen, müssen für kommerzielle Nutzung, Forschung und dienstliche Zwecke gegebenenfalls ordnungsgemäß lizensiert werden.
- Überprüfung der Berechtigungen einer App bei Installation. Apps, die unnötigen Zugriff auf (dienstliche) E-Mails, Adressbuch oder Kalender erfordern, sollten vermieden werden (z. B. WhatsApp).
- Löschung von Apps, die nicht (mehr) benötigt werden
- Verzicht auf Jailbreak (iOS) oder Rooting (Android)

3.3 Abruf von E-Mails, Kalender, Adressbuch

Um dienstliche E-Mails, Kalender und Adressbuch zu synchronisieren, sollte ausschließlich der Exchange ActiveSync Client mit dem durch das ZIV bzw. die zuständige IVV betriebenen Microsoft Exchange Server verwendet werden. Der Abruf der dienstlichen E-Mails über IMAP/POP sollte vermieden werden. Die Nutzung von Exchange ActiveSync bietet die folgenden Möglichkeiten:

- Überblick für den Nutzer, welche Mobilgeräte mit seinem Exchange Zugang verbunden sind
- Fernlöschen eines Gerätes bei Verlust durch den Nutzer
- Zentrale Anwendung der vom ZIV empfohlenen Sicherheitseinstellungen
- Konfigurierbare Sicherheitseinstellungen für verschieden Nutzergruppen

3.4 Nutzung von Cloud-Diensten

Cloud-Dienste sollten entsprechend der Cloud-Richtlinie [3] der WWU verwendet werden.

3.5 Verlust des Gerätes

Bei Verlust eines dienstlichen Mobilgerätes sollte umgehend die DV-technisch betreuende Einrichtung informiert werden, die das Gerät administriert (meist IVV oder IT-Administrator). Ferner sollte der Nutzer unmittelbar seine Passwörter von verwendeten Kennungen der WWU ändern, um eine unberechtigte Nutzung auszuschließen.

Der Nutzer kann bei Bedarf über Exchange ActiveSync selbständig sein Gerät aus der Ferne auf Werkseinstellungen zurücksetzen und damit sensible Daten auf dem Gerät löschen. Daten auf einer Speicherkarte werden u.U. nicht bei jedem Gerät gelöscht. Die Fernlöschung wird erst ausgeführt, wenn sich das Gerät mit dem Exchange-Server verbindet. Das Gerät muss dafür über eine Netzanbindung und ausreichend Batteriekapazität verfügen.

Eine Fernlöschung darf nur durch den Benutzer oder mit seiner Zustimmung erfolgen.

3.6 Ausmusterung von nicht ausreichend abzusichernden Geräten

Mobilgeräte, die weder durch eine DV-technisch betreuende Einrichtung noch durch den Nutzer hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken oder mit dienstlichen Daten genutzt werden und fachgerecht ausgemustert werden (sichere Löschung der darauf vorhandenen Daten, Entsorgung über zuständige IVV). Privatgeräte sind in ausschließlich privater Nutzung zu belassen.

4 Weiterführende Dokumente

[1] Universität Münster, „Ordnung für IT-Administratoren an der WWU,“ 29 Apr 2009. [Online]. Available: https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2009/ausgabe18/beitrag9.pdf.

[2] Universität Münster, „Benutzungsordnung des ZIV und der IVVen der WWU,“ 15 Nov 2010. [Online]. Available: https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2010/ausgabe25/beitrag_03.pdf.

[3] IV-Sicherheitsteam der Universität Münster, „Cloud-Richtlinie,“ 2013. [Online]. Available: https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2015/ausgabe02/beitrag03.pdf.

[4] Universität Münster, „Regelungen zur IV-Sicherheit,“ 21 Feb 2002. [Online]. Available: https://www.uni-muenster.de/Rektorat/abuni/ab020507.html.

5 Impressum

Westfälische Wilhelms-Universität Münster
IV-Sicherheitsteam
Röntgenstr. 7-13
48149 Münster

Ansprechpartner:	Thorsten Küfel,	t.kuefer@wwu.de
Editor:	Dustin Demuth	d.demuth@wwu.de

Impressum

Westfälische Wilhelms-Universität Münster

IV-Sicherheitsteam

Röntgenstr. 7-13

48149 Münster

Editoren:

Dustin Demuth dustin.demuth@uni-muenster.de

Markus Tegeder markus.tegeder@uni-muenster.de

Ansprechpartner:

Thorsten Küfer thorsten.kuefer@uni-muenster.de

Die Texte der Dokumente im Anhang dieses Handbuches wurden neu formatiert, um der Formatierung dieses Handbuches zu entsprechen. Hierbei wurde auch die Worttrennung der Dokumente angepasst und gegebenenfalls korrigiert. Etwaige Rechtschreibfehler wurden in den Texten weitestgehend korrigiert. Daher entsprechen die Dokumente im Anhang nicht mehr den Originaldokumenten. Benötigen Sie rechtlich bindende Dokumente, verwenden Sie bitte die jeweils aktuelle Fassung des Dokumentes aus den amtlichen Bekanntmachungen der Universität[91].

Wir bitten um Verständnis, dass aus Gründen der besseren Lesbarkeit bei Gattungsbegriffen oft nur die grammatikalisch maskuline Form verwendet wird.

Thorsten Kuefer

Digital unterschrieben von Thorsten Kuefer
DN: c=DE, o=Universitaet Muenster, ou=Zentrum fuer Informationsverarbeitung, cn=Thorsten Kuefer
Datum: 2015.03.23 12:52:43 +01'00'

[91] https://www.uni-muenster.de/Rektorat/abuni/
[92] https://creativecommons.org/publicdomain/zero/1.0/deed.de