



Regelungen zur IV-Sicherheit in der Universität ...

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**

15. März 2001,v.2

§ 1 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 Daten¹. Sie umfassen auch verpflichtende Verhaltensmaßnahmen 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.

§ 2 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 sind².

¹ Der Einsatz dieser Ressourcen wird zusammenfassend Informationsverarbeitung (IV) genannt.

² 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.

§ 3 Betriebsregelungen

(1) Kommunikationssysteme (Variante A)³
Alle Kommunikationssysteme (campusweites LAN, WAN, Einwahleinrichtungen usw.) werden ausschließlich vom Hochschulrechenzentrum (HRZ) 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 anzumelden⁴. Neben den zentral bereitgestellten Netzzugängen (z.B. Einwahlzugängen) dürfen keine weiteren geschaffen werden⁵. Spezielle Netzzugänge sind mit dem HRZ abzustimmen.

(1) Kommunikationssysteme (Variante B)
Alle Kommunikationssysteme (campusweites 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 Dienstangebot 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 Datendienstordnung genannt) existiert, findet diese vorrangig Anwendung⁶.

(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 zugelassen⁷. Gegebenenfalls sind entsprechende Server ohne begründbaren Bedarf in das HRZ zu verlagern. Alle Server müssen in besonderer Weise dauerhaft und regelmäßig gepflegt werden⁸. 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 erfolgen⁹. 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 Sicherheitslücken¹⁰ zu verfolgen und sich entsprechend weiterzu-

³ Variante A bzw. Variante B sind in Abhängigkeit von der Organisation der IV in den Universitäten zu wählen.

⁴ Dadurch sollen Betriebsstörungen durch Leitungsengpässe und andere Sicherheitsfragen rechtzeitig gelöst werden.

⁵ Sie stellen ein hohes Gefährdungspotenzial dar.

⁶ Bereits existierende Ordnungen und Regelungen sind widerspruchsfrei zu den vorliegenden Regelungen zu gestalten.

⁷ Sie stellen ebenfalls ein hohes Gefährdungspotential dar.

⁸ Etwa durch das aktuelle Einspielen von Updates und Sicherheitspatches.

⁹ Beispielsweise im Geschäftsverteilungsplan.

¹⁰ Informationen sind z.B. unter <http://www.cert.dfn.de/> zu finden.

bilden. 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 im HRZ anzumelden.

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.

(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) zusammengestellt und über das HRZ der Universitätsleitung vorgeschlagen und nach deren Zustimmung als Betriebsregelungen verbindlich gemacht¹¹.

§ 4 Zuwiderhandlungen

Server, Pools und Arbeitsplatzsysteme, die nicht den Sicherheitsregelungen entsprechend betrieben werden, können vom HRZ 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 HRZ 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.

§ 5 Sicherheitsteam

Zur Erarbeitung und Umsetzung der Sicherheits- und (den daraus abgeleiteten) Betriebsregelungen wird ein Sicherheitsteam eingerichtet¹². Zu seinen Aufgaben gehören:

- Definition wirksamer Sicherheitsstandards und Betriebsregelungen (gemäß §3 in Abstimmung mit den dezentralen IV-Versorgungseinheiten.
- 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 HRZ eingerichtet.

Die Kontrolle der Sicherheitsmaßnahmen und des Sicherheitsteams wird im Abstand von 2 bis 3 Jahren durch eine Evaluierung zwischen den HRZ erfolgen.

¹¹ Betriebsregelungen werden im WEB unter <http://www...> 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.

§ 6 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 NutzernInnen zugänglich ist.
- Ein detaillierter Notfallplan, der innerhalb des HRZ bzw. innerhalb der dezentralen Versorgungseinheiten 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.).

§ 7 Personalbedarf und Haushaltsmittel

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

§ 8 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 Senats der Universität ... vom ...

..., den ...

Die Rektorin/der Rektor

...

Anlage: Festlegung der Sicherheitsniveaus

Zur Festlegung der Sicherheitsniveaus in den IV-Versorgungseinheiten hat das Sicherheitsteam Kriterien aufzustellen. Hierzu sind die vier vom BSI¹³ 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 erkennbar 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.

¹³ BSI = Bundesamt für die Sicherheit in der Informationsverarbeitung

- 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:

1. Welche Bedeutung hat die Vertraulichkeit der Informationen aus der IV für Ihren Bereich? Was geschieht, wenn die Vertraulichkeit verletzt wird?
2. 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?
3. Gibt es Aufgaben, die nur mit der Unterstützung der IV möglich sind?
4. 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 IV-Versorgungseinheiten?
- An Servern des HRZ?
- 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 HRZ) auch im jeweiligen Bereich?
- Werden im jeweiligen Bereich Kommunikationssysteme (E-Mail, WWW, FTP usw.) eingesetzt?
- Gibt es im jeweiligen Bereich besondere Sicherheitslöcher? Sind dort bereits konkrete Gefährdungen beobachtet worden?