Juli 2002

Rahmenregelungen zur IT-Sicherheit in der Universität Bonn

(Diese Regelungen basieren auf einem Entwurf des Arbeitskreises der Leiter Wissenschaftlicher Rechenzentren in NRW (ARNW) und von der DV-Kommission gutgeheißenen Vorschlägen des hiesigen Rechenzentrums.)

§ 1 Präambel und Geltungsbereich

Diese Regelungen gelten für die IT in der Universität[1], d.h. für alle technischen Kommunikationssysteme, alle am Netz als Server oder Arbeitsplatzrechner genutzten Rechner, alle eingesetzten Softwareprodukte und alle gespeicherten oder zu bearbeitenden Daten[2]. Sie umfassen auch verpflichtende Verhaltensmaßnahmen aller Nutzer der IT sowie aller Mitarbeiter, die IT-Leistungen bereitstellen.

Forschung und Lehre sind von der verläßlichen Nutzung der IT, 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 IT-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 im allgemeinen 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 IT kann daneben durch Stromunterbrechungen, Feuer, Blitzschlag, technische Defekte, Diebstahl, Sabotageakte und Zerstörung von Geräten gefährdet werden. Gefährdungen entstehen auch durch Fehler oder Nachlässigkeiten von Mitarbeitern sowie durch die Inanspruchnahme externer Personen.

Diese Regelungen zur IT-Sicherheit sollen das Gefahrenpotential mindern.

§ 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 sind[3].

---

[1] Im UKB finden vorrangig die „EDV-Sicherheitsrichtlinien des UKB“ und in der Verwaltung die „Dienstanweisung: Datenschutz und Datensicherheit beim Einsatz von DV-Anlagen und -Geräten in der Verwaltung der Rheinischen-Friedrich-Wilhelms-Universität Bonn“ Anwendung.

[2] Der Einsatz dieser Ressourcen wird zusammenfassend Informationstechnik (IT) genannt.

[3] 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

Alle Kommunikationssysteme (campusweites LAN, WAN, Einwahleinrichtungen usw.) werden grundsätzlich vom IT-Service (ITS) betrieben. An definierten Übergabepunkten kann die Verantwortung für lokale Kommunikationssysteme einer universitären Einrichtung an diese übergehen, wenn der Betrieb, der Zugang und das Diensteangebot nach den Vorgaben des ITS erfolgen. Externe Zugänge (z.B. Wählzugänge, VPNs und IP-Tunnel) werden für Mitarbeiter und Studierende zentral am ITS zur Verfügung gestellt. In begründeten Ausnahmefällen können externe Zugänge auch von Instituten betrieben werden, wenn sichergestellt ist, daß die lokalen Netze vom Kommunikationsnetz abgeschottet sind und die Einrichtung und der Betrieb mit dem ITS abgestimmt sind. Die „Betriebsregelung für das BONNET der Universität Bonn“ findet vorrangig Anwendung.

(2) Betrieb von Servern und hochschulöffentlichen Arbeitsplatzrechnern

Im LAN der Universität kann grundsätzlich jedes Institut eigene Server betreiben. Der Betrieb derartiger Server, deren Dienstleistungsangebot wie z.B. E-Mail-Server nicht nur auf das eigene Intranet angelegt ist, wird nur bei begründetem Bedarf zugelassen. Andernfalls ist das entsprechende Dienstleistungsangebot des ITS zu nutzen. Alle Server müssen in besonderer Weise dauerhaft und regelmäßig gepflegt werden. Server mit besonderem Verfügbarkeitsbedarf sind besonders vor dem Zugang Unbefugter zu sichern. Sicherheitsrelevante Dienste (z.B. Verzeichnisdienste) sind auf einige wenige und besonders gut gepflegte Server zu konzentrieren. Das ITS schafft die technischen Voraussetzungen, um Server oder von den Instituten betriebene Kommunikationssysteme auf das beabsichtigte Dienstespektrum einzuschränken.

Zu jedem Server sind ein verantwortlicher Administrator sowie ein Stellvertreter als technisch Verantwortliche zu benennen. Die Zuweisung der Administrator-Funktion muß schriftlich erfolgen. Administratoren und ihre Vertreter müssen einen ihren Aufgaben entsprechenden Qualifikations- und Informationsstand haben.
Beim Betrieb von hochschulöffentlichen Arbeitsplatzrechnern ist dafür Sorge zu tragen, daß kein unberechtigter Benutzer Zugang zum Netz 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 IT-Sicherheit nicht möglich sind.

Verantwortliche für den Betrieb von Servern oder hochschulöffentlichen Arbeitsplatzrechnern 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 und Administratoren

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 ITS 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 alle an das Kommunikationssystem angeschlossenen Geräte sind technisch Verantwortliche zu benennen.

Paßwörter sind grundsätzlich verschlüsselt zu übertragen.

(4) Verantwortung der Leiter der Organisationseinheiten
Die Leiter der Organisationseinheiten der Universität sind zur Einhaltung der geltenden Sicherheits- und Betriebsregelungenverpflichtet. Sie sind für die operative Umsetzung der Richtlinien in ihrem Zuständigkeitsbereich verantwortlich.

(5) Schutz personenbezogener Daten und weitere Einzelmaßnahmen
Werden personenbezogene Daten verarbeitet, so sind diese durch zusätzliche technische Maßnahmen zu schützen; die Übertragung solcher Daten sollte verschlüsselt erfolgen. Für die Speicherung und Verarbeitung personenbezogener Daten sind die geltenden Datenschutzgesetze sowie die örtlichen Dienstvereinbarungen zu beachten.

§ 4 Zuwiderhandlungen

Server, Subnetze und Arbeitsplatzsysteme, die nicht den Sicherheitsregelungen entsprechend betrieben werden, können vom ITS vom Netz genommen werden. Zur Abwehr akuter schwerwiegender Störungen oder Gefahren können Server, Subnetze und Arbeitsplatzsysteme darüber hinaus vorübergehend vom Netz genommen werden. Nutzern, die die Sicherheit gefährden, kann vorübergehend die Nutzungsberechtigung entzogen werden. Zuwiderhandlungen können darüber hinaus Verstöße u.a. gegen das Strafgesetzbuch (StGB), das Bürgerliche Gesetzbuch (BGB) und das Landes- und Bundesdatenschutzgesetz darstellen.

§ 5 Sicherheitskonzept

Zur Erarbeitung, fortlaufender Aktualisierung und Überwachung der Umsetzung eines Sicherheitskonzepts und (den daraus abgeleiteten) Betriebsregelungen wird vom Rektorat ein *Technisches Komitee „IT-Sicherheit“* eingerichtet. Darin sollten Mitarbeiter aus dem ITS sowie Vertreter aus den Instituten mitwirken. Bei Bedarf können weitere Personen hinzu gezogen werden.

Der ITS bildet für die ständig anfallenden sicherheitsrelevanten Arbeiten ein *Sicherheitsteam.* Zu dessen Aufgaben gehören:

- Entgegennahme und Dokumentation aller sicherheitsrelevanten Vorfälle, die zusätzlich an externe Stellen (z.B. das DFN-CERT) zu berichten sind.
- Aufstellung eines Ausbildungs- und Schulungskonzepts zur IT-Sicherheit für Benutzer, Administratoren und Mitglieder des Sicherheitsteams, das auch für die Maßnahmen zur Verbesserung der IT-Sicherheit sensibilisieren soll.
- Ansprechpartner für alle sicherheitsrelevanten Fragen.
- Unterstützung bei der Gefahrenanalyse.
- Landesweite Abstimmung der Sicherheitsstandards und Betriebsregelungen.

§ 6 Notfallvorsorge

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

- Ein einfacher Benachrichtigungsplan für Probleme und Notfälle, der allen Nutzern zugänglich ist.
- Ein detaillierter Notfallplan, der innerhalb des ITS 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.
- Notfallvorsorgekonzept zur sicheren Aufbewahrung von Daten (Backup, Archivierung usw.).

§ 7 Inkrafttreten

Diese Regelungen zur IT-Sicherheit wurden vom Rektorat der Universität Bonn verabschiedet (Rektoratsbeschluß vom 11.06.2002) und treten . . . . . in Kraft.

gez. Der Rektor

Anlage: Festlegung der Sicherheitsniveaus

Zur Festlegung der Sicherheitsniveaus in den IV-Versorgungseinheiten hat das Sicherheitsteam Kriterien aufzustellen. Hierzu sind die vier vom BSI[4] 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 IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.

Insgesamt gilt: Der Ausfall der IT 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 IT-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.

[4] 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 IT-Versorgungseinheiten?
- An Servern des ITS?
- Im LAN?
- In der Verbindung des LAN mit dem G-WiN-Zugang?
- In der Verbindung des LAN mit Einwahlleitungen? Gibt es solche (außerhalb der Einwahlleitungen des ITS) 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?