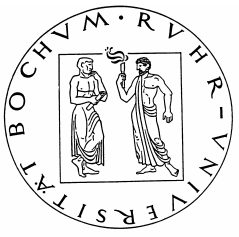
Leitlinie zur IT-Sicherheit

Ruhr-Universität Bochum

STABSSTELLE IT-SICHERHEIT



Einleitung

Forschung und Lehre an der Ruhr-Universität sind zunehmend von der Nutzung der Informationstechnologie (IT) als modernes Lehr-, Informations- und Kommunikationsmedium abhängig geworden. Daraus entsteht ein hoher Anspruch an die Verfügbarkeit und Sicherheit der an Verarbeitung und Kommunikation beteiligten Arbeitsstationen, Server und Netzwerke sowie an die Verfügbarkeit, Integrität und Vertraulichkeit der zu verarbeitenden Informationen und der verwendeten Software. Bedingt durch Schwachstellen in den Datenübertragungsprotokollen, durch Schwachstellen in den verwendeten Betriebsystemen und Programmen und durch fehlerhafte Konfiguration von Servern und Arbeitsstationen sind insbesondere vernetzte Rechnersysteme erheblichen Gefährdungen und Risiken ausgesetzt.

Ein Universitätsnetz bietet wegen der Heterogenität seiner Systeme und Benutzer sowie der verteilten Verantwortlichkeiten ein besonders breites Angriffsziel und die Erfahrung zeigt, dass dieses Risiko nicht nur theoretisch existiert. Neben Angriffen von außen auf Systeme der Universität sind Attacken von innen, zum Beispiel durch Mitarbeiter und Studierende, von Bedeutung. Fehlerhaftes oder fahrlässiges Verhalten beim Umgang mit den Systemen ist hier ebenso zu registrieren wie mangelndes Risikobewusstsein und hohe Risikobereitschaft. 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 beziehungsweise Manipulieren von schutzwürdigen Forschungsdaten und -ergebnissen kann einen hohen finanziellen Schaden darstellen. Der Schutz personenbezogener Daten gegen unbefugten Zugriff muss gesetzlichen Anforderungen genügen. Angriffe gegen fremde Systeme, die über das Universitätsnetz unter Ausnutzung der hiesigen Schwachstellen laufen, bewirken einen hohen Imageverlust der Universität in der Öffentlichkeit.

Die Hochschulleitung ist davon überzeugt, dass das geschilderte Gefahrenpotenzial durch die konsequente Umsetzung geeigneter Sicherheitsmaßnahmen erheblich gemindert werden kann. Das Rektorat hat daher die folgende Leitlinie zur IT-Sicherheit beschlossen. Sie beschreibt die Ziele und Strategien eines IT-Sicherheitskonzeptes für die Ruhr-Universität.

Sicherheitsziele

Rechnersysteme, IT-Dienstleistungen und hochschulinternes Rechnernetz sind zur Unterstützung der universitären Aufgaben in den Bereichen Lernen, Lehre, Forschung und Administration bestimmt. Der zuverlässige Einsatz dieser Einrichtungen hängt davon ab, dass die Anwender kooperativ und in gegenseitigem Respekt handeln. Alle Anwender sind für einen bestimmungsgemäßen Umgang mit diesen Einrichtungen und Dienstleistungen verantwortlich. Gerade wegen der zunehmenden Abhängigkeit von den IT-Systemen verfolgt das IT-Sicherheitskonzept notwendigerweise folgende Ziele:

- Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen und Informationen,
- Schutz von Netzwerk, Rechnersystemen und Informationen (Hardware und Software) gegen Missbrauch von innen und außen,
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen des Datenschutzes,
- Sicherstellung eines reibungslosen Lehr-, Forschungs- und Verwaltungsbetriebes sowie
- die Gewährleistung des guten Rufs der Universität in der Öffentlichkeit.

Zur Erreichung dieser Ziele werden vom Rechenzentrum unter Einbeziehung der Einrichtungen der Ruhr-Universität Sicherheitsrichtlinien festgelegt und fortgeschrieben. Im Geiste des kooperativen und respektvollen Miteinanders der universitären Gemeinschaft werden in den Sicherheitsrichtlinien Nutzungseinschränkungen der IT-Systeme und Dienstleistungen nur in dem Maße festgelegt, das zur Erreichung der Sicherheitsziele unabdingbar notwendig ist. Alle Sicherheitsrichtlinien für Verantwortliche, Systembetreuer und Endbenutzer werden im Intranet der Ruhr-Universität abgelegt.

Sicherheitsniveau

Die Sicherheitsrichtlinien beziehen sich auf Systeme mit normalem Schutzbedarf. Ein System hat einen *normalen* Schutzbedarf, wenn durch den Verlust an Vertraulichkeit, Integrität und Verfügbarkeit des Systems

- nur ein geringfügiger Verstoß gegen Vorschriften und Gesetze möglich ist,
- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen nicht möglich ist oder für diesen tolerabel bleibt,
- eine Beeinträchtigung der persönlichen Unversehrtheit des Einzelnen nicht möglich ist,
- die Aufgabenerfüllung nur geringfügig beeinträchtigt ist,
- nur eine geringe Ansehens- und Vertrauensbeeinträchtigung zu befürchten ist und
- der finanzielle Schaden tolerabel bleibt.

Diese Richtlinien stellen für Systeme mit hohem oder sehr hohem Schutzbedarf eine Basis-Sicherung dar, reichen aber möglicherweise nicht alleine zur Sicherung aus. Hier müssen ergänzende Maßnahmen auf Basis einer differenzierten Sicherheitsanalyse ergriffen werden.

Verantwortlichkeiten

IT-Sicherheit für die Ruhr-Universität lässt sich nur als Gesamtkonzept realisieren. Jeder Beteiligte einschließlich jedes Endbenutzers muss sich der Notwendigkeit von IT-Sicherheit bewusst sein und entsprechend handeln.

Verantwortung des Leiters der Organisationseinheiten

Die einzelnen Organisationseinheiten der Universität (z.B. Institut, Lehrstuhl, Fakultät) verwalten die ihnen zugeordneten Subnetze, Arbeitsstationen und Server eigenverantwortlich. Der Leiter jeder Einrichtung ist für die Sicherheit dieser IT-Systeme und der Informationen, die damit verarbeitet und übertragen werden, verantwortlich. Er ist verpflichtet, sich über die geltenden Sicherheitsrichtlinien zu informieren und für die operative Umsetzung der Richtlinien zu sorgen.

Verantwortung jedes Endbenutzers

Jeder Endbenutzer trägt die Verantwortung für den bestimmungsgemäßen und gewissenhaften Umgang mit den Informationen, die auf der von ihm genutzten Arbeitsstation verarbeitet werden. Er ist verpflichtet, sich über mögliche Sicherheitsrisiken zu informieren und Sicherheitsrichtlinien für seinen Arbeitsbereich umzusetzen.

Organisationsstruktur

Bei einer großen Organisation wie der Ruhr-Universität ist ein IT-Sicherheitskonzept nur in einer mehrstufigen Organisationsstruktur umzusetzen:

Sicherheitsteam im Rechenzentrum

Die Erarbeitung der Sicherheitsrichtlinien und die Koordination der Sicherheitsprozesse erfolgt durch ein Sicherheitsteam. Die Geschäftsstelle des Sicherheitsteams ist im Rechenzentrum der Ruhr-Universität eingerichtet. Zu den Aufgaben des Sicherheitsteams gehört es:

- wirksame Sicherheitsrichtlinien in Abstimmung mit den Einrichtungen der Universität zu definieren,
- die Umsetzung der Sicherheitsrichtlinien zu überwachen und zu dokumentieren,
- die Sicherheitsprozesse anzupassen, zu revidieren und fortzuschreiben,
- den IT-Sicherheitsbetreuern der Einrichtungen als Ansprechpartner für sicherheitsrelevante Fragen zur Verfügung zu stehen,
- mit den örtlichen IT-Sicherheitsbeauftragten anderer Hochschulen und Einrichtungen zu kooperieren,
- ein Sensibilisierungs-, Ausbildungs- und Schulungskonzept für Benutzer, Administratoren und Mitglieder des Sicherheitsteams aufzustellen,

- sicherheitsrelevante Vorfälle aufzunehmen und zu dokumentieren und gegebenenfalls an externe Stellen (z.B. DFN-CERT) zu berichten,
- die aktuellen Diskussionen und Forschungen über sicherheitsrelevante Fragen in angemessener Weise zu verfolgen,
- sicherheitsrelevante Beschwerden externer Stellen entgegenzunehmen und zu bearbeiten,
- Managementreports zu erstellen.

IT-Sicherheitsbetreuer der Einrichtungen

Jede Organisationseinheit (z.B. Institut, Lehrstuhl, Fakultät) der Ruhr-Universität benennt einen IT-Sicherheitsbetreuer, der für die Sicherheitsbelange der IT-Systeme und Anwendungen in der Organisationseinheit verantwortlich ist und dem Sicherheitsteam im Rechenzentrum namentlich bekannt gegeben wird. Ein Wechsel des IT-Sicherheitsbetreuers ist anzuzeigen. Es können Bereichs-IT-Sicherheitsbetreuer auch mehrere Organisationseinheiten betreuen. Zu den Aufgaben des (Bereichs-) IT-Sicherheitsbetreuers gehört es:

- als Ansprechpartner für das IT-Sicherheitsteam im Rechenzentrum und als erster Ansprechpartner in Sicherheitsfragen für die IT-Benutzer der Organisationseinheit zu fungieren,
- das IT-Sicherheitsbewusstsein bei den Anwendern der Organisationseinheit zu fördern,
- sich über die geltenden Sicherheitsrichtlinien zu informieren und für die gesicherte operative Umsetzung der relevanten IT-Sicherheitsrichtlinien zu sorgen (Sofern die konkrete Umsetzung Endbenutzern oder Betreuern übertragen wird, muss die Verantwortlichkeit klar geregelt sein.),
- notwendige Informationen über IT-Systeme zusammenzufassen und an das IT-Sicherheitsteam weiterzuleiten,
- Informationen über Schulungs- und/oder Sensibilisierungsbedarf von den IT-Nutzern der Organisationseinheit zu ermitteln und an das IT-Sicherheitsteam weiterzuleiten,
- sicherheitsrelevante Zwischenfälle an das IT-Sicherheitsteam zu melden.

Der IT-Sicherheitsbetreuer muss mindestens über Grundkenntnisse in IT-Sicherheit und über Grundkenntnisse in der Administration von IT-Systemen verfügen. Als Hilfestellung bietet das Rechenzentrum Einführungs- und Qualifizierungskurse an, die diese Kenntnisse vermitteln.

IT-Sicherheitsbetreuer für Studierende

Das Rechenzentrum stellt eine Ansprechstelle für IT-Sicherheitsfragen für Studierende bereit und bietet entsprechende Schulungen an.

Schulungskonzept

Die sachgerechte Erfüllung der Gemeinschaftsaufgabe „IT-Sicherheit" kann nur dann gelingen, wenn alle am IT-Sicherheitsprozess beteiligten Personen einen angemessenen Kenntnisstand über die Gefahren und Gegenmaßnahmen haben. Zu diesem Zweck erstellt das Sicherheitsteam im Rechenzentrum ein zielgruppenorientiertes Schulungskonzept.

Maßnahmen zur Gefahrenabwehr

1. Zur Abwehr akuter schwerwiegender Störungen und Gefahren, die die IT-Sicherheit gefährden, kann das Rechenzentrum temporär
   - Anwender von der Nutzung der IT-Systeme, dem Netzwerk und den IT-Dienstleistungen ausschließen,
   - die Verbindung zu Endgeräten oder Subnetzen unterbrechen.

   Die Maßnahme ist auf den Zeitraum beschränkt, in dem die Störung oder Gefahr vorliegt bzw. der für die Abstellung der Ursache erforderlich ist. Der Endanwender wird umgehend benachrichtigt.
2. Bei schwerwiegenden sicherheitsrelevanten Störungen ist der Rektor der Ruhr-Universität berechtigt, den verursachenden Anwender zeitweise oder auf Dauer von der Nutzung der IT-Systeme, des Netzwerks oder der IT-Dienstleistungen auszuschließen.

Anmerkung

Sämtliche in dieser Leitlinie auftretenden Personen- und Funktionsbezeichnungen sind grundsätzlich gleichwertig in weiblicher und männlicher Form zu verstehen.

Begriffserläuterungen

Informationelles Selbstbestimmungsrecht	Grundrecht des Einzelnen, das ihn vor einem Missbrauch seiner persönlichen Daten schützt: „Jeder hat das Recht, über die Preisgabe und Verwendung seiner Daten selbst zu bestimmen“
Informationstechnologie (IT)	Die Technologie, die sich mit der Verarbeitung von Daten befasst
Integrität	Sicherstellung der Unverfälschtheit und Vollständigkeit von Informationen und IT-Systemen
Internet	TCP/IP basiertes, weltweites Netz von Netzen
Intranet	Organisationsinternes Netzwerk, das die Technik und Protokolle des Internets verwendet (z.B. internes Netz einer Universität)
IT-Sicherheit	Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen und IT-Systemen (Hardware und Software)
IT-Systeme	Arbeitsstationen, Server und Netzwerk
Persönliche Unversehrtheit	Grundrecht des Einzelnen auf körperliche, seelische und geistige Unversehrtheit
TCP/IP	Transmission Control Protocol/Internet Protocol, das gemeinsame Protokoll (Sprache) der Systeme des Internets
Verfügbarkeit	Gewährleistung, dass Informationen und IT-Systeme für berechtigte Benutzer nutzbar sind
Vertraulichkeit	Gewährleistung, dass Informationen ausschließlich Personen zugänglich sind, die dazu berechtigt sind