Rundschreiben
Nr.: 24/2014

HRK Hochschulrektorenkonferenz
Die Stimme der Hochschulen

Der Präsident

HRK Hochschulrektorenkonferenz, Ahrstraße 39, D-53175 Bonn

An die
Rektorinnen und Rektoren,
Präsidentinnen und Präsidenten
der Mitgliedshochschulen
der Hochschulrektorenkonferenz

Ansprechpartner: Dr. Ulrich Meyer-Doerpinghaus, Teamleiter D1
Kontakt: 0228/887-150, meyer@hrk.de

Zeichen: D1 - 12/2014

IT-Sicherheit an Hochschulen und Forschungseinrichtungen 27.10.2014

Sehr geehrte Damen und Herren,

schon immer sind Ergebnisse wissenschaftlichen Arbeitens entwendet und missbraucht worden. Vor dem Einzug moderner Informations- und Kommunikationstechnologie in den Alltag wissenschaftlichen Arbeitens war hierfür in der Regel noch der physische Diebstahl – meist mit Unterstützung durch „Innentäter" – erforderlich. Durch die Nutzung der vernetzten Informationstechnik ergeben sich indes neue, anders gelagerte Risiken mit hohem Schadenspotential, auf die sich die Wissenschaft einstellen muss. So kommt es zum Beispiel seit geraumer Zeit zu massiven Angriffen ausländischer Nachrichtendienste auf die internen informationstechnischen Systeme wissenschaftlicher Einrichtungen mit allen dort vorhandenen Daten. Dabei sind nicht nur Institute der Hochtechnologie, sondern auch geisteswissenschaftliche Einrichtungen betroffen.

Die in der Allianz der Wissenschaftsorganisationen verbundenen Einrichtungen[1], zu denen auch die Hochschulrektorenkonferenz gehört, haben sich des Themas angenommen und auf der Basis von Vorarbeiten des von der Allianz eingerichteten Arbeitskreises zur IT-Sicherheit in Forschungseinrichtungen (AKIF) ein Grundsatzpapier verabschiedet. Dieses Papier, das ich Ihnen in der Anlage übersende, beschreibt die Bedeutung der IT-Sicherheit an Hochschulen und Forschungseinrichtungen und führt die Grundsätze für eine IT-Sicherheitsstrategie, über die jede wissenschaftliche Einrichtung verfügen sollte, auf.

[1] Die Mitgliedsorganisationen der Allianz sind: Alexander von Humboldt-Stiftung, Deutsche Akademie der Naturforscher Leopoldina – Nationale Akademie der Wissenschaften, Deutsche Forschungsgemeinschaft, Deutscher Akademischer Austauschdienst, Fraunhofer-Gesellschaft, Helmholtz-Gemeinschaft, Hochschulrektorenkonferenz, Leibniz-Gemeinschaft, Max-Planck-Gesellschaft, Wissenschaftsrat

Wenn es gelingt, die in dem Papier formulierten Grundsätze in den Sicherheitsstrategien der Hochschulen und Forschungseinrichtungen flächendeckend zu implementieren und umzusetzen, ist ein wichtiger erster Schritt getan. Jede Sicherheitsstrategie muss jedoch auch mit konkreten, auf die besondere Ausgangssituation einer Einrichtung zugeschnittenen Maßnahmen ausgefüllt werden. Hierzu wird der AKIF in den kommenden Monaten ein Best-Practice-Papier entwickeln, das technische Mindeststandards enthalten und Anregungen für geeignete Maßnahmen geben wird.

Ich hoffe, dass Ihnen das heute übersandte Papier eine erste Hilfestellung für die Weiterentwicklung der IT-Sicherheitsstrategie Ihrer Organisation geben kann.

Mit freundlichen Grüßen

Professor Dr. Horst Hippler

Allianz der
Wissenschaftsorganisationen

Alexander von Humboldt-Stiftung
Deutsche Forschungsgemeinschaft
Fraunhofer-Gesellschaft
Hochschulrektorenkonferenz
Leibniz-Gemeinschaft
Deutsche Akademie der Naturforscher Leopoldina – Nationale Akademie der Wissenschaften
Deutscher Akademischer Austauschdienst
Helmholtz-Gemeinschaft
Max-Planck-Gesellschaft
Wissenschaftsrat

Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen

Für die Arbeit an wissenschaftlichen Einrichtungen sind Dienstleistungen der Informations- und Kommunikationstechnik (IKT bzw. IT) von zunehmender Bedeutung. Damit nimmt auch die Abhängigkeit von der Funktionstüchtigkeit einer IKT stetig zu. Gleichzeitig bedarf es für hochwertiges wissenschaftliches Arbeiten in Forschung und Lehre einer angemessenen Informations- und IT-Sicherheit. Es ist daher unerlässlich, umfassende Schutzmaßnahmen zu ergreifen. Hierfür sollte nach Auffassung der in der Allianz der Wissenschaftsorganisationen verbundenen Einrichtungen jede wissenschaftliche Einrichtung eine grundlegenden IT-Sicherheitsstrategie formulieren, verabschieden und auf Leitungsebene verankern, die die Basis für ein IT-Sicherheitskonzept und daraus folgende Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik darstellt.

1. Bedeutung der IKT

Die Informations- und Kommunikationstechnik ist von zentraler Bedeutung für die Aufgabenerfüllung wissenschaftlicher Einrichtungen. Das Spektrum der IT-Anwendungen umfasst den Betrieb von Anlagen, die Durchführung von Versuchen und Experimenten, wissenschaftliche Anwendungen und Simulationen, die Lehre, die Arbeit der Verwaltung sowie der Zentralen Dienste und die Kommunikation mit externen Partnern und Auftraggebern. Die Bedeutung der Informationstechnik für die unterschiedlichen Anwendungsgebiete ist unterschiedlich hoch. Dementsprechend sind die Auswirkungen von Störungen oder Ausfällen in den verschiedenen Anwendungsgebieten von unterschiedlicher Tragweite. Datenverlust an Unautorisierte kann zu finanziellen Einbußen und Reputationsbeschädigungen führen und dem muss vorgebeugt werden. Die immer häufiger von Zuwendungsgebern geforderten Sicherheitsnachweise können auf Basis der IT-Sicherheitsstrategie leichter erbracht werden.

2. Eckpfeiler der IKT-Sicherheitsstrategie

Grundlegende Voraussetzung für Informationssicherheit ist ein Risikomanagement auf Basis einer Klassifizierung der Daten, Anwendungen und Netzwerkinfrastruktur hinsichtlich der Anforderungen an Verfügbarkeit, Vertraulichkeit und Unversehrtheit. Insbesondere die „Kronjuwelen“ der Forschungstätigkeit müssen identifiziert und besonders geschützt werden.

2.1 Umfang der IT-Sicherheit

IT-Sicherheit umfasst die Verfügbarkeit, Vertraulichkeit und Unversehrtheit von Daten und Anwendungen.

Verfügbarkeit der Informations- und Kommunikationstechnik

Technische Systeme[1] besitzen eine begrenzte Verfügbarkeit. Dabei ist organisatorisch festzulegen, welche Ausfallzeiten akzeptabel und unter dem Gesichtspunkt der Wirtschaftlichkeit vertretbar sind. In Abhängigkeit hiervon sind geeignete Maßnahmen zu ergreifen, die in den akzeptierten zeitlichen Grenzen einen Wiederanlauf ermöglichen. Daten sind in mehrstufigen Verfahren so zu sichern, dass nach menschlichem Ermessen ein grundsätzlicher Verlust ausgeschlossen werden kann.

Unversehrtheit von Daten

Unbefugte oder unbemerkte Veränderungen von Daten sollen ausgeschlossen sein, sei es durch Personen, Schadsoftware oder technische Fehler. Es wird erwartet, dass Daten weder irrtümlich noch mutwillig manipuliert werden. Je nach Anwendung sind deshalb geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Unversehrtheit von Daten zu erhalten.

Vertraulichkeit von Daten / Schutz vor unberechtigtem Zugriff

In wissenschaftlichen Einrichtungen werden unterschiedlichste vertrauliche Informationen verarbeitet. Da nicht ausgeschlossen ist, dass auf die Daten unberechtigt zugegriffen wird, müssen geeignete technische, organisatorische und personelle Maßnahmen in den Anwendungen, dem IT-Netz, den Servern, den Arbeitsplatzcomputern und auf den Übertragungswegen ergriffen werden, die einen möglichst effektiven Zugriffsschutz bewirken.

2.2 Proaktive Maßnahmen

Grundlegend für die Abwehr von Angriffen sind proaktive Maßnahmen, die ermöglichen, dass Angriffe zeitnah erkannt und unterbunden werden können. Dazu gehören besonders die Verwendung von Verschlüsselung, eine ausreichende Protokollierung und Auswertung sowie das Filtern des Datenverkehrs nach gefährlichen Inhalten. Durch geeignete Aufbewahrungsfristen für Protokolldateien und betriebliche Regelungen zur Auswertung ist dabei ein Ausgleich zwischen Datenschutz, Mitbestimmung und IT-Sicherheitsinteressen zu finden.

2.3 Aufgabenzuordnung und Rahmenbedingungen

Die Gesamtverantwortung für die IT-Sicherheit liegt bei der Leitung der wissenschaftlichen Einrichtung. Die IT-Sicherheit ist für die Einrichtung ein wesentliches strategisches Ziel.

Die Leitung der wissenschaftlichen Einrichtung bestellt eine/n IT-Sicherheitsbeauftragte/n und stellt ihm/ihr die erforderlichen Ressourcen und Befugnisse zur Verfügung.

Der oder die IT-Sicherheitsbeauftragte ist dafür zuständig, dass die in der IT-Sicherheitsstrategie benannten Ziele in der Einrichtung umgesetzt werden. Er oder sie sorgt dafür, dass angemessene IT-Sicherheitsmaßnahmen im Rahmen eines IT-Sicherheitskonzepts und IT-Maßnahmenkatalogs unter Beachtung der Anforderungen aus Forschung und Lehre realisiert, fortentwickelt und überwacht werden.

[1] Darunter wird Hard-, Software und Daten verstanden

Sich hieraus ergebende Regeln sind für alle Nutzer der IT-Infrastruktur der wissenschaftlichen Einrichtung, insbesondere für die Beschäftigten, verbindlich.

Jeder Benutzer der Informations- und Kommunikationstechnik ist für die Sicherheit und den Schutz der Daten in seinem Verantwortungsbereich verantwortlich. Alle Angehörigen der Einrichtung sind verpflichtet, bei der Erfüllung der Aufgabe „IT-Sicherheit“ kooperativ und verantwortungsbewusst mitzuwirken.

Lösungen zur Erreichung von Sicherheitszielen sollen das Restrisiko verkleinern, müssen angemessen und wirtschaftlich vertretbar sein. Der Aufwand für die IT-Sicherheitsmaßnahmen ist in Relation zu dem erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen.

Bei dauernd wechselnden Gefährdungen ist die Aufrechterhaltung der IT-Sicherheit eine permanente Aufgabe. Dieses erfordert personelle und finanzielle Mittel und die Mitwirkung jedes Einzelnen.

Um Gefahren wirksam abzuwehren, muss ein vertrauensvoller, systematischer Informationsaustausch zwischen den Einrichtungen auf der einen Seite und den zuständigen Behörden auf der anderen Seite etabliert werden. Nur so kann ein Lagebild für die Forschungslandschaft erstellt und bewertet werden.