Max Weber Stiftung

Deutsche Geisteswissenschaftliche Institute im Ausland

IT-Sicherheitsleitlinie

(Stiftungsratsbeschluss vom 16.11.2012)

1. Einleitung

Die Max Weber Stiftung fördert die Forschung mit Schwerpunkten auf den Gebieten der Geistes-, Sozial- und Kulturwissenschaften. Sie forscht dezentral; ihre derzeit zehn Institute sind in ihrer wissenschaftlichen Arbeit unabhängig. Mit ihren weltweit tätigen Instituten leistet die Max Weber Stiftung einen wesentlichen Beitrag zur Verständigung und Vernetzung zwischen Deutschland und den Gastländern bzw. -regionen. Indem sie sowohl den Dialog der Fachkulturen fördert als auch wissenschaftliche und nicht-wissenschaftliche Beschäftigte aus verschiedenen Ländern mit unterschiedlichen kulturellen Hintergründen zusammenbringt, verstärkt sie die Internationalisierung der Forschung in den Geistes-, Sozial- und Kulturwissenschaften.

Die Max Weber Stiftung bekennt sich zur IT-Sicherheit und ihrer Sicherstellung.

Inhalte der Sicherheitsleitlinie

Im Folgenden wird die Basis für ein IT-Sicherheitskonzept und daraus folgender Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik dargestellt.

IT-Sicherheitsziele und Maßnahmen orientieren sich an den Empfehlungen der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), soweit sie für Forschungseinrichtungen und ihre Verwaltung relevant sind.

Insbesondere:

- Anwenderinnen und Anwender haben ein Grundverständnis für Belange der IT-Sicherheit
- IT-Systeme werden in einer sicheren Umgebung betrieben
- Informationen (Systeme, Daten, etc.) werden adäquat vor unberechtigten Zugriffen geschützt
- IT-Systeme werden vor schädlicher Software (sog. "Malware") geschützt

- IT-Systeme werden auf einem adäquaten Versionsstand gehalten
- Die administrative Arbeit auf IT-Systemen wird sicher und nachvollziehbar gestaltet
- Informationen werden ihrer Kritikalität entsprechend angemessen sicher verarbeitet
- IT-Systeme werden durch kompetentes Personal langfristig betreut
- Die Wirksamkeit der Schutzmaßnahmen wird regelmäßig überprüft und dokumentiert
- IT-Sicherheitszwischenfälle werden dokumentiert und kommuniziert

IT-Sicherheit umfasst die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und Anwendungen. In allen drei Hinsichten sind technische Systeme bedroht (Technische Ausfälle, Möglichkeiten der Manipulation und des Vertraulichkeitsverlustes). Gegen diese Bedrohungen sind geeignete Maßnahmen zu ergreifen.

Aufgrund der Bedeutung der Informations- und Kommunikationstechnik überwacht der Stiftungsrat die Realisierung und Einhaltung der IT-Sicherheit durch die Geschäftsführung und die Leitung der Institute. IT-Sicherheit hat einen sich wiederholenden Prozesscharakter. Beteiligte am Sicherheitsprozess sind alle Personen, die die Instituts-IT nutzen können (z. B. Institutsangehörige, Praktikanten, Gäste, externe Dienstleister, Institutsleitung).

2. Bedeutung der Informations- und Kommunikationstechnik

Die Informations- und Kommunikationstechnik ist von zentraler Bedeutung für die Aufgabenerfüllung der Institute. Das Spektrum der IT-Anwendungen in den Instituten umfasst den Betrieb von Anlagen, wissenschaftliche Anwendungen, die Arbeit der Verwaltung sowie der zentralen Dienste und die Kommunikation mit externen Partnern und Auftraggebern. Je nach Anwendungsgebiet sind die Auswirkungen von Störungen oder Ausfällen in den verschiedenen Anwendungsgebieten von unterschiedlicher Tragweite.

3. IT-Sicherheitsziele

Die Sicherheitsziele Vertraulichkeit, Verfügbarkeit, Integrität dienen dazu, die Arbeitsfähigkeit der Institute sicherzustellen. Die Institute können weitere Sicherheitsziele definieren. Lösungen zur Erreichung von Sicherheitszielen sollen das Restrisiko verkleinern, müssen angemessen und wirtschaftlich vertretbar sein, sie müssen deutschen Standards entsprechen und – sofern diese strenger sind – auch den Standards der Gastländer.

3.1. Verfügbarkeit der Informations- und Kommunikationstechnik

Technische Systeme (Hard-, Software und Daten) besitzen eine begrenzte Verfügbarkeit. Dabei ist organisatorisch festzulegen, welche Ausfallzeiten akzeptabel und unter dem Ge-

sichtspunkt der Wirtschaftlichkeit vertretbar sind. In Abhängigkeit dieser Forderungen 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.

3.2. Integrität von Daten

Unbefugte oder unbemerkte Veränderungen von Daten sollen ausgeschlossen sein, sei es durch Personen 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 Integrität von Daten zu erhalten.

3.3. Vertraulichkeit von Daten

Die Institute verarbeiten unterschiedlichste vertrauliche Informationen. 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 Arbeitsplatzcomputern und auf den Übertragungswegen ergriffen werden, die einen möglichst effektiven Zugriffsschutz bewirken.

3.4. Einhaltung gesetzlicher Auflagen

Die Institute haben eine Vielzahl gesetzlicher Auflagen wie Datenschutz, Arbeitssicherheit, etc. zu erfüllen. IT-Systeme und die dazu erlassenen organisatorischen Regelungen müssen so ausgelegt sein, dass die deutschen gesetzlichen Bestimmungen - und, sollten diese strenger sein, auch die des Gastlandes - eingehalten werden.

4. Aufgabenzuordnung

- Die Gesamtverantwortung für die institutsübergreifende IT-Sicherheit liegt bei dem Geschäftsführer der Stiftung, sofern die Geschäftsstelle in das entsprechende Verfahren involviert ist,
- bei Fachverfahren und den dazugehörigen IT-Verfahren, die in den Instituten durchgeführt werden, beim Direktor des jeweiligen Institutes; bei Verfahren, an denen mehrere Institute beteiligt sind, benennen die Institute einen gesamtverantwortlichen Direktor

Geschäftsführer und Direktoren werden auf diese Verantwortlichkeit hingewiesen, bevor sie ihre Ämter annehmen.

Der Stiftungsrat bestellt auf Vorschlag des Geschäftsführers einen IT-Sicherheitskoordinator der Stiftung und stellt ihm die erforderlichen Ressourcen und Befugnisse zur Verfügung. Die Aufgaben des IT-Sicherheitskoordinators sind:

- Beratung des Stiftungsrates und des Geschäftsführers
- Erstellung und Pflege eines Sicherheitskonzepts der Stiftung auf der Basis der einzelnen Sicherheitskonzepte der Institute
- die Analyse übergreifender Bedrohungen,
- die Empfehlung und Ausarbeitung von übergreifenden Maßnahmen,
- die Empfehlung technischer Maßnahmen zur Sicherung übergreifender Aufgaben,
- die Beratung, Information und Weiterbildung der IT-Sicherheitsbeauftragten
- Vertretung der Stiftung in externen Gremien.

Zur Aufgabenerfüllung kann der IT-Sicherheitskoordinator

- unter Wahrung des Datenschutzes und der lokalen Dienstvereinbarungen zusammen mit dem zuständigen IT-Sicherheitsbeauftragten (s.u.) Einsicht in IT-Systeme, Netzwerkstruktur und Protokolldateien eines Arbeitsbereiches oder seiner Einrichtung nehmen oder Informationen verlangen, die eine Beurteilung der Gefährdung ermöglichen. Bei Interessenkonflikten zwischen IT-Administration und IT-Sicherheitsbeauftragung kann der IT-Sicherheitskoordinator vom Institutsdirektor Einsichtnahme verlangen,
- auf die Ergreifung geeigneter Maßnahmen zur Gefahrenabwehr und Verhinderung von Missbrauch dringen. In gravierenden Fällen wird der Stiftungsrat informiert,
- im Rahmen von Maßnahmen unter Beachtung der Datenschutzgesetze und der Dienstvereinbarungen den Netzwerkverkehr überwachen, mit dem Ziel Missbrauch und Bedrohungen frühzeitig zu erkennen oder aufzuklären,
- sich in besonderen Fällen mit den Sprechern des Arbeitskreises MWS-IT in Verbindung setzen

Der Stiftungsrat beauftragt die Direktoren mit der Sicherstellung der IT-Sicherheit. Die Direktoren gewährleisten, dass die in dieser IT-Sicherheitsleitlinie benannten Ziele umgesetzt werden. Sie sorgen dafür, dass angemessene IT-Sicherheitsmaßnahmen realisiert, fortentwickelt und überwacht werden. Dazu wird an jedem Institut vom Direktor ein lokaler IT-Sicherheitsbeauftragter bestimmt. Die Sachkunde des IT-Sicherheitsbeauftragten muß dem Direktor geeignet nachgewiesen werden. Die Institutsleitung stellt dem IT-Sicherheitsbeauftragten die nötige Unterstützung und Ressourcen zur Erfüllung seiner Aufgaben zur Verfügung. Der IT-Sicherheitsbeauftragte

- unterstützt und berät den Direktor fachlich in allen Fragen der IT-Sicherheit und informiert diesen über die getroffenen Maßnahmen und sicherheitsrelevante Vorfälle,
- ist für alle Anwender des Institutes erster Ansprechpartner in Fragen der IT-Sicherheit,
- erstellt und pflegt das IT-Sicherheitskonzept des Institutes
- informiert und sensibilisiert alle Anwender des Institutes für IT-Sicherheitsprobleme,
- achtet darauf, dass die IT-Administration vermeidbare Sicherheitsprobleme in der Software auf den eingesetzten IT-Systemen durch regelmäßiges Einspielen von Updates, Patches oder neuerer Software-Versionen beseitigt und die Software in Hinblick auf die IT-Sicherheit angemessen konfiguriert ist,
- kann unter Wahrung des Datenschutzes in Abstimmung mit dem verantwortlichen Bereichsleiter IT-Systeme und Netze im Institut auf Sicherheitsprobleme hin überprüfen,
- kann zur Aufgabenerfüllung und unter Wahrung des Datenschutzes und der Dienstvereinbarungen zusammen mit den betroffenen lokalen IT-Managern oder Nutzern Einsicht in IT-Systeme, Netzwerkstruktur und Protokolldateien des Institutes nehmen oder Informationen verlangen, die eine Beurteilung der Gefährdungslage ermöglichen,
- kann zur Aufgabenerfüllung in Absprache mit dem verantwortlichen Bereichsleiter Maßnahmen ergreifen, um Gefahren abzuwehren und Missbrauch zu unterbinden,
- achtet auf die Einhaltung von Maßnahmen und Regelungen, die dem Schutz der IT-Systeme dienen,
- arbeitet mit dem zentralen IT-Sicherheitskoordinator zusammen und meldet diesem sicherheitsrelevante Vorfälle.

Damit alle Beteiligten die nötigen Informationen und Mitwirkungsmöglichkeiten bei der Einführung oder Veränderung von IT-basierten Verfahren haben, schaffen die Institute Strukturen, in denen der Direktor als Verantwortlicher, der Verwaltungsleiter, der IT-Sicherheitsbeauftragte, der Leiter der IT-Abteilung bzw. der IT-Administrator und entsprechend der Fachanwendung der Leiter der jeweiligen Fachabteilung gemeinsam planen. Die Arbeit der örtlichen IT-Sicherheitsbeauftragten wird unterstützt und koordiniert durch den IT-Sicherheitskoordinator.

Die Regeln, die sich aus den IT-Sicherheitsmaßnahmen ergeben, sind für die Leitung und alle anderen Nutzer der IT-Infrastruktur der Institute, insbesondere die Beschäftigten verbindlich. Die Nutzer müssen sich auf die Einhaltung der Regeln verpflichten. Jeder Benutzer der Informations- und Kommunikationstechnik ist für die Sicherheit und den Schutz der Daten in seinem Verantwortungsbereich verantwortlich. Alle Angehörigen der Institute sind verpflich-

tet, bei der Erfüllung der Aufgabe „IT-Sicherheit" kooperativ und verantwortungsbewusst mitzuwirken. Externe Dienstleister und Auftragnehmer im IT-Bereich sind in den Sicherheitsprozess einzubeziehen, bei Aufnahme der Vertragsbeziehung werden sie über die Anforderungen der IT-Sicherheit in der Max Weber Stiftung bzw. dem Institut informiert. Das Institut mißt die IT-Sicherheit der externen Dienstleistungen mit denselben Maßstäben wie die eigene IT-Sicherheit.

5. Sicherheitskonzept und IT-Maßnahmenkatalog

Die Institute sorgen für die Erstellung und Pflege ihrer IT-Sicherheitskonzepte und die Umsetzung des IT-Maßnahmenkatalogs. Der IT-Sicherheitskoordinator unterstützt dies und wird von den Instituten bei der Erstellung und Initiierung ihrer lokalen Sicherheitskonzepte und Sicherheitsprozesse informiert.

Der IT-Einsatz in den Instituten wird in IT-Verfahren zusammengefasst, die IT-Verfahren werden dokumentiert und beschrieben und im Hinblick auf ihren Schutzbedarf analysiert. Für alle Verfahren wird schriftlich eine Ansprechpartnerin bzw. ein Ansprechpartner benannt.

Es wird ein Basisschutz definiert, der in allen Bereichen umgesetzt werden muss. Ist ein Basisschutz nicht ausreichend, wird anhand von Risikoanalysen bestimmt, welchen Gefährdungen die IT-Verfahren im Hinblick auf die Schutzziele ausgesetzt sind. Auf dieser Grundlage wird das notwendige Schutzniveau für die Informationen ermittelt.

Das Schutzniveau ist regelmäßig, mindestens einmal pro Jahr auf seine Wirksamkeit, Angemessenheit und Konformität mit dem Regelwerk zur IT-Sicherheit zu prüfen.

Abweichungen und Änderungen von Sicherheitskonzept und IT-Maßnahmenkatalog sind zu dokumentieren.

Der IT-Sicherheitskoordinator führt die nötigen Schritte eines Sicherheitsbeauftragten im Sicherheitsprozess für institutsübergreifende Verfahren (wie z. B. Personalaktenführung, Buchungssoftware) durch, an denen die Geschäftsstelle beteiligt ist. Verantwortlich und entscheidend ist hier der Geschäftsführer.

Aus den Sicherheitskonzepten der Institute und dem für die stiftungsweiten Verfahren erstellt der IT-Sicherheitskoordinator das Gesamt-IT-Sicherheitskonzept, das dem Stiftungsrat vorgelegt wird. Das Sicherheitskonzept besteht aus einem Teil für stiftungsübergreifende Verfahren und Teilkonzepten der Institute, dabei stellt der IT-Sicherheitskoordinator die Vergleichbarkeit der Teilkonzepte her.