IT-Sicherheitspolitik in der FhG

Dipl.-Math. Wilfried Gericke
IT-Verantwortlicher

IT-Sicherheitspolitik in der FhG

Motivation

IT-Sicherheitsziele

Verantwortlichkeit

Maßnahmen und Umsetzung

Motivation(1)

Die Fraunhofer-Gesellschaft und ihre Institute sind zur Erfüllung ihrer Geschäftsprozesse, und um mit nationalen und internationalen Kunden und Partnern zusammenarbeiten zu können, auf die Verfügbarkeit moderner Informations- und Kommunikationstechnik angewiesen.

Es bestehen gesetzliche Bestimmungen und vertragliche Verpflichtungen gegenüber Vertragspartnern.

Durch die wachsende Zahl der IT-Anwendungen, die zunehmende Vernetzung von IT-Systemen und das Zusammenwachsen unterschiedlicher Kommunikationsdienste ergeben sich für eine wachsende Zahl potentieller Angreifer ständig neue technische Möglichkeiten, welche die Sicherheit der IT-Systeme und Daten der Fraunhofer-Gesellschaft beeinträchtigen könnten.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Motivation(2)

Vorstand, Institutsleiter, Zentrale und Mitarbeiter der Fraunhofer-Gesellschaft unternehmen daher alle erforderlichen Schritte, um die Verfügbarkeit, Funktionsfähigkeit und Sicherheit der IT-Systeme an allen Fraunhofer-Standorten zu gewährleisten.

Die Fraunhofer-Gesellschaft nutzt dazu insbesondere das interne Know-How zu Fragen der IT-Sicherheit.

Die Schutzmaßnahmen umfassen sowohl technische und organisatorische Vorkehrungen als auch für alle Mitarbeiter der Fraunhofer-Gesellschaft verbindliche Regeln und Vorgaben.

Die Fraunhofer-Gesellschaft strebt stets solche IT-Sicherheits-Lösungen an, die sich durch einen sinnvollen Kompromiss zwischen Sicherheitsanforderungen und Bedienkomfort/Zugriffsgeschwindigkeit auszeichnen.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

IT-Sicherheitsziele (1)

Die Fraunhofer-Gesellschaft schützt ihre Interessen und ihr Ansehen in der Öffentlichkeit durch die Sicherung ihrer Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit für Kooperationspartner und Kunden. Dies gilt auch und gerade in Bezug auf die IT-basierten Arbeits- und Kommunikationsmittel.

Zu den IT-Sicherheitszielen der Fraunhofer-Gesellschaft zählen:

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

IT-Sicherheitsziele (2)

- Gewährleistung die Verfügbarkeit der IT-Systeme, Programme und Daten
- Schutz der Integrität der IT-Systeme, Programme und Daten
- Verhinderung des Missbrauch der IT-Systeme, Programme und Daten (zweckwidrige Nutzung, Nutzung durch Unbefugte), sowohl aus Gründen des Selbstschutzes als auch zum Schutze Dritter
- vertrauliche Informationen sollen unabhängig von der Art ihrer Aufzeichnung derart behandelt werden, dass ihre Vertraulichkeit jederzeit sichergestellt ist
- Sicherstellung der Integrität, Funktionsfähigkeit und Vertraulichkeit von Arbeitsergebnissen und Produkten und von Projektdaten
- strikte Einhaltung der einschlägigen Gesetze und sonstiger rechtlicher Bestimmungen zur IT
- Wahrung der Persönlichkeitsrechte der Fraunhofer-Mitarbeiter

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(1)

Aufgrund der dezentralen IT-Strukturen der Fraunhofer-Gesellschaft kommt den Fraunhofer-Instituten eine wichtige Rolle bei der Erreichung der IT-Sicherheitsziele zu.

Fraunhofer-Vorstand und Zentrale leiten, koordinieren und unterstützen die Institute bei ihren IT-Sicherheitsaktivitäten.

Ein Arbeitskreis IT-Sicherheit initiiert und lenkt in Absprache mit dem Vorstand die IT-Sicherheitsmaßnahmen in der Fraunhofer-Gesellschaft.

Vorstand, Institutsleiter und jeder Benutzer und Administrator der IT-Infrastruktur der Fraunhofer-Gesellschaft trägt durch sein Verhalten zur Gewährleistung der Gesamt- IT-Sicherheit in der Fraunhofer-Gesellschaft bei.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(2)

Der **Vorstand**,

in herausgehobener Position der **Chief Information Officer (CIO) der Fraunhofer-Gesellschaft,** trägt die Gesamtverantwortung für die IT-Sicherheit.

Er initiiert und koordiniert zusammen mit der Zentrale die entsprechenden Aktivitäten und sorgt für die nötige Priorität und Aufmerksamkeit für Fragen der IT-Sicherheit.

Die **Institutsleiter**

schaffen die erforderlichen Rahmenbedingungen, um der IT-Sicherheit in ihrem Zuständigkeitsbereich den erforderlichen Stellenwert zu geben und die notwendigen Ressourcen für die Erreichung der Sicherheitsziele zur Verfügung zu stellen.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(3)

Die **IT-Verantwortlichen**, bzw. die **IT-Sicherheitsbeauftragten**

der Institute legen diejenigen Maßnahmen fest, die aus ihrer Sicht zur Verbesserung und Erhaltung der IT-Sicherheit in ihrem jeweiligen Wirkungsbereich ergriffen werden müssen;

sie reagieren außerdem eigenverantwortlich bei Verstößen gegen oder die Nichtbeachtung von IT-Sicherheitsvorgaben.

Die **IT- Manager bzw. die Administratoren**

setzen die notwendigen technischen und organisatorischen Sicherheitsmaßnahmen nach Vorgabe der IT-Verantwortlichen, bzw. der IT-Sicherheitsbeauftragten um.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(4)

Jeder **Projektleiter**

sorgt für den Schutz von Projektergebnissen und Kundendaten und stimmt sich zu speziellen Erfordernissen der IT-Sicherheit mit dem IT-Verantwortlichen, bzw. IT-Sicherheitsbeauftragten ab.

Jeder **Nutzer der Fraunhofer IT-Infrastruktur**,

insbesondere aber der **Fraunhofer-Mitarbeiter,** achtet auf die konsequente Anwendung der bekannt gemachten, individuell zur Verfügung stehenden IT-Sicherheits-Maßnahmen und – Mechanismen.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(5)

Das **Netzzentrum (NOC)** der Fraunhofer-Gesellschaft dient in Form eines Kompetenz-zentrums als fachliche und beratende Ansprechstelle bei IT-Sicherheitsvorfällen

Die **Zentrale** ergreift geeignete Sicherheitsmaßnahmen und unterstützt die Institute und Serviceanbieter bei ihren Sicherheitsanstrengungen.

Der **Arbeitskreis IT-Sicherheit** der IT-Verantwortlichen der Fraunhofer-Gesellschaft initiiert in Absprache mit dem Vorstand verbindliche Vorgaben in Bezug auf IT-Sicherheits-maßnahmen

Seite 11

DECUS Symposium 2004

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(5)

Ansprechpartner innerhalb der Fraunhofer-Gesellschaft

CIO (Chief Information Officer), Prof. Dr. Dennis Tsichritzis (Mitglied des Vorstandes)

Hauptabteilungsleiter Wissens- und Kommunikationsmanagement

IT-Sicherheitskoordinator

Datenschutzbeauftragter

Netzzentrum (NOC) beim IITB

Kompetenzzentrum LAN-Management

IT-Verantwortliche der Institute

Seite 12

DECUS Symposium 2004

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Verantwortlichkeit(5)

Ansprechpartner außerhalb der Fraunhofer-Gesellschaft

DFN-CERT (Computer-Notfallteam des deutschen Forschungsnetzes)

BSI-CERT (CERT-Bund, Computer-Notfallteam des Bundes, vor allem für Behörden)

Bundesdatenschutzbeauftragter

Bayerisches Staatsministerium des Innern

Regulierungbehörde für Telekommunikation und Post (RegTP)

Fraunhofer INT Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(1)

Zur Gewährleistung der IT-Sicherheit in der Fraunhofer-Gesellschaft im Sinne der oben genannten Sicherheitsziele werden von allen Fraunhofer-Einrichtungen mindestens die nachfolgend beschriebenen Maßnahmen ergriffen:

- Organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der IT-Sicherheit in jeder Einrichtung (lokaler IT-Sicherheitsprozess)
- Bereitstellung der technischen und personellen Ressourcen für die IT-Sicherheit, angemessene Einbettung in die Strukturen und die Hierarchie der Fraunhofer-Einrichtung
- Priorisierung der notwendigen IT-Sicherheitsmaßnahmen und deren Umsetzung;
- Information, Schulung und Betreuung der Nutzer im Umgang mit den IT-Systemen und ihren Sicherheitsmechanismen (Benennen kompetenter Ansprechpartner für Fragen und Probleme; Bereitstellen geeigneter Dokumentation);

Fraunhofer INT Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(2)

• Berücksichtigung der IT-Sicherheits-Erfordernisse in der Zusammenarbeit mit Partnern bzw. externen Dienstleistern; wo erforderlich Abschluss vertraglicher Vereinbarungen

• Regelmäßig wiederholte Bestandsaufnahme und Analyse der Sicherheitsaktivitäten und -mechanismen, sowie Überprüfen der Einhaltung von Sicherheitsmaßnahmen

• Regelmäßige Überarbeitung der Dokumentation der Sicherheitsmaßnahmen

• Festlegung von Konsequenzen bei Verstößen gegen IT-Sicherheitsregelungen und unzureichenden Vorkehrungen (Behebung der Schwachstellen, Vermeidung wiederholter Verstöße)

• Organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der IT-Sicherheit in der Fraunhofer-Gesellschaft (Globalsteuerung des IT-Sicherheitsprozesses), sowie Bereitstellung der dafür erforderlichen technischen und personellen Ressourcen

Fraunhofer INT Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(3)

- Definition, Weiterentwicklung und Pflege einer Benutzungsordnung mit den Mindestanforderungen für alle Nutzer, die über die IT-Infrastruktur der Fraunhofer-Gesellschaft Aufgaben im Auftrag der Fraunhofer-Gesellschaft bearbeiten.
- Erstellung, Weiterentwicklung und Pflege eines IT-Sicherheitshandbuchs als Handlungshilfe für die Institutsleiter, das Führungspersonal, die IT-Verantwortlichen und die IT-Sicherheitsbeauftragten in den Instituten und der Zentrale.
- Prüfung der Umsetzung und Einhaltung der Sicherheitsvorgaben in den Instituten (Audit), Festlegung von Konsequenzen bei Verstößen gegen IT-Sicherheitsregelungen und unzureichenden Vorkehrungen.

Fraunhofer INT Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(4)

Um Doppelarbeiten vermeiden und gleichzeitig - bei optimierten Kosten und möglichst geringem lokalem Aufwand - Fraunhofer-weite Mindeststandards einhalten zu können, sollen die Institute bei der Umsetzung der Policy-Vorgaben durch die Beschreibung einer standardisierten Vorgehensweise bei der Durchführung von IT-Risikoanalysen unterstützt werden.

Der rote Faden für eine solche Vorgehensweise ist das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
http://www.bsi.de/gshb/deutsch/menue.htm

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung; IT-Grundschutzhandbuch (1)

Was ist das IT-Grundschutzhandbuch ?

Im IT-Grundschutzhandbuch werden Standardsicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.

Um den sehr heterogenen Bereich der IT einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt das IT-Grundschutzhandbuch das Baukastenprinzip. Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wider, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung; IT-Grundschutzhandbuch (2)

Diese Gefährdungslage bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren. Die Gefährdungslage wird zur Sensibilisierung angeführt.

Mit Hilfe des IT-Grundschutzhandbuchs lassen sich IT-Sicherheitskonzepte einfach und arbeitsökonomisch realisieren. Wegen der Innovationsschübe und Versionswechsel im IT-Bereich ist das IT-Grundschutzhandbuch auf leichte Erweiterbarkeit und Aktualisierbarkeit ausgerichtet. Daher ist es durch Bausteine und Kataloge modular aufgebaut und als Lose-Blatt-Sammlung erweiterungsfähig. Das BSI überarbeitet und aktualisiert regelmäßig die bestehenden Bausteine, um die Empfehlungen auf dem Stand der Technik zu halten. Darüber hinaus wird das bestehende Werk regelmäßig um weitere Bausteine erweitert.

Seite 19

DECUS Symposium 2004

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(5)

Die Entwicklung des IT-Sicherheitskonzepts nach dem IT-Grundschutzhandbuch des BSI:

IT-Strukturanalyse

Schutzbedarfsfeststellung

IT-Grundschutzanalyse (Bausteine)

Ergänzende Sicherheitsanalyse

Realisierungsplanung

Seite 20

DECUS Symposium 2004

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(6)

Wichtige und bindende Dokumentationen und Handbücher zur IT-Sicherheit in der Fraunhofer-Gesellschaft sind:

IT-Rahmenplan

IT-Sicherheitshandbuch

IT-Gesamtbetriebsvereinbarungen

Rechtsvorschriften

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(7)

IT-Rahmenplan

Bestandsaufnahme der IT-Infrastruktur der Fraunhofer-Gesellschaft. Um den Instituten später die Übernahme dieses IT-Rahmenplans bei der Erstellung eines eigenen IT-Rahmenplans zu ermöglichen, erfolgt zunächst eine Art Definition der zu betrachtenden IT-Infrastruktur. Aufbauend auf diese Definition können die Institute dann in Anlehnung an oder Ergänzung institutsspezifische Informationen bereitstellen. Dies reduziert den Aufwand bei der Erstellung der Instituts-IT-Rahmenpläne erheblich und führt zu einer weit-gehenden Vergleichbarkeit der Instituts-IT-Rahmenpläne

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(8)

IT-Sicherheitshandbuch

Das IT-Sicherheitshandbuch ist das Kerndokument der IT-Sicherheit in der Fraunhofer-Gesellschaft. Es wendet sich vor allem an die Leiter, IT-Manager und IT-Administratoren der Fraunhofer-Gesellschaft, regelt Verantwortlichkeiten und enthält vorgaben für die Planung und Umsetzung von IT-Sicherheitsmaßnahmen.

Es soll auch dazu motivieren, IT-Sicherheit als eine wichtige Management- bzw. IT-Administrationsaufgabe zu begreifen.

Es enthält auch eine Nutzerordnung. Dieses Dokument regelt den Umgang mit den IT-Systemen und –Diensten der Fraunhofer-Gesellschaft und die Rechte und Pflichten der Nutzer.

Alle Nutzer von IT-Systemen in der FhG sind zur Einhaltung der Regeln dieser Benutzerordnung verpflichtet.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(9)

Gesamtbetriebsvereinbarungen

- SIGMA
- Dokumentenmanagementsystem DMS
- Nutzung von Internet-Diensten in der FhG
- E-Learning
- Video-Konferenzsystemen
- Einsatz von Mobiltelephonen
- Einsatz von Projekt-Management-System (PMS)

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Maßnahmen und Umsetzung(10)

IT-Rechtsvorschriften

Eine Zusammenfassung von wichtigen Gesetzen wurde von der Arbeitsgruppe IT-Sicherheit der IT-Manager der FhG zusammengestellt.

Eine detaillierte Übersicht zu wichtigen Gesetzen und Verordnungen zum IT-Bereich finden Sie unter
http://www.lrz-muenchen.de/~rgerling/gesetze/index.html

Hinweise zum Datenschutz finden Sie auch unter

http://www.bfd.bund.de/technik/DS-KAP/35.htm

Adresse der Datenschutzbeauftragten von NRW: http://www.ldi.nrw.de/

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen