Informationssicherheitsleitlinie

verabschiedet am 27.05.2015 durch das Präsidium der TUHH

Zielsetzung

Die Informationssicherheitsleitlinie (IS-LL) der Technischen Universität Hamburg-Harburg (TUHH) folgt den Vorgaben der IS-LL der Freien und Hansestadt Hamburg (FHH), Beschluss des Hamburger Senats vom 02.04.2013, bezüglich der Schutzziele der

- Verfügbarkeit (Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind),
- Vertraulichkeit (Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind) und
- Integrität (Gewährleistung, dass die Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen überprüfbar sind)

aller vorhandenen Informationen der Hochschule. Sie orientiert sich an BSI-Grundschutz und schreibt die bestehende IT-Sicherheitsleitlinie der TUHH, beschlossen durch den Hochschulsenat der TUHH am 25.02.2004, fort.

Geltungsbereich

Diese Leitlinie gilt für alle angegliederten, sowie eigenständigen Organisationseinheiten, die zur Technischen Universität Hamburg-Harburg (TUHH) gehören oder in deren Netzinfrastruktur integriert sind.
Betroffen sind sowohl digitale Informationen sowie die Geräte, mit denen die Informationen verarbeitet werden, als auch analoge Medien (z.B. Ausdrucke), die ebenfalls schützenswerte Informationen enthalten können.

Zusammenfassung

- Alle Beschäftigten müssen verantwortlich mit den Informationen der TUHH umgehen.
- Die Verantwortung für Informationssicherheit liegt beim Leiter der Organisationseinheit.
- Die dazugehörigen Aufgaben können vom Leiter der Organisationseinheit an einen Mitarbeiter, den Datenverarbeitungsbeauftragten (DVB), delegiert werden.
- Dieser DVB ist Kontakt für den Informationssicherheitsbeauftragen (InSiBe).
- Zentrale Infrastrukturkomponenten werden durch das Rechenzentrum (RZ) betrieben.

1. Motivation

Die Informationstechnik hat sich zu einem der wichtigsten Arbeitsmittel für eine moderne Universität entwickelt. Dabei sind die Möglichkeiten, die eine Vernetzung der Computer untereinander bieten, wie z.B. Mail unverzichtbar und ohne diese Techniken wäre der Auftrag zur Forschung und Lehre für die TUHH kaum erfüllbar.

Leider hat die Vergangenheit gezeigt, dass vernetzte Computersysteme sowohl von innen, d.h. durch Angehörige der TUHH, als auch von außen durch Dritte angreifbar sind und auch missbraucht werden. Ein solcher Missbrauch

- führt zu hohen Kosten bei der Beseitigung von Schäden, weil dadurch die Betroffenen an ihren eigentlichen Aufgaben gehindert und personelle Ressourcen gebunden werden,
- beeinträchtigt oder verhindert die bestimmungsgemäße Nutzung,
- erhöht die Kosten für den Betrieb des Universitäts-Netzwerkes und der Anbindung an das Internet,
- verletzt die Vertraulichkeit von Informationen, die nicht für Dritte bestimmt sind,
- kann gegen geltendes Recht verstoßen und
- schädigt das Ansehen der TUHH in der Öffentlichkeit.

Es gibt auch viele andere Bedrohungen für die Verfügbarkeit der IT-Infrastruktur der TUHH. Dazu zählen höhere Gewalt, organisatorische Mängel, Fehlbedienung, technisches Versagen und vorsätzliche Handlungen wie Diebstahl oder Vandalismus.
Ziel muss es deshalb sein, Missbrauch und Gefahren einzudämmen, damit die Vertraulichkeit und Integrität der Daten und die aufgabengemäße Verfügbarkeit der IT-Systeme gewährleistet sind. Sicherheit kann eine Einschränkung für die Bedienbarkeit und Funktionalität bedeuten, und es muss zwischen den verschiedenen Interessen abgewogen werden. Die Kompromisse, die dabei einzugehen sind, müssen von jedem Nutzer der TUHH-Infrastruktur akzeptiert und mitgetragen werden. Dies gilt auch für Gäste, die nur vorübergehend an der TUHH anwesend sind.

2. Zuständigkeiten

Alle Beschäftigten haben die Informationssicherheit durch ihr verantwortliches Handeln zu gewährleisten und die für die Informationssicherheit relevanten Regelwerke (Gesetze, Verordnungen, Richtlinien, personalvertretungsrechtliche Vereinbarungen, organisatorische Regelungen, vertragliche Verpflichtungen u.ä.) einzuhalten.
Den Leitern der Organisationseinheiten obliegt es, mit Anweisungen und Freigaben die spezifischen Anforderungen ihres Bereiches zu regeln und zu verantworten, soweit diese durch zentrale Beschlüsse nicht ausreichend abgedeckt sind (z.B. besondere Vertragsvereinbarungen mit Kooperationspartnern).
Die Informationssicherheit der TUHH liegt als Aufgabe der staatlichen Auftragsverwaltung beim Kanzler, die strategische Ausrichtung der IT beim Chief Information Officer (CIO).

3. Informationssicherheitsbeauftragter (InSiBe)

Der InSiBe koordiniert den übergreifenden Informationssicherheits-Prozess und unterstützt die DVB in ihrer Arbeit. Die Aufgaben des InSiBe sind

1. die Analyse übergreifender, TUHH-weiter Bedrohungen,
2. die Empfehlung und Ausarbeitung von übergreifenden, TUHH-weiten Maßnahmen,
3. die technische Umsetzung der übergreifenden Maßnahmen in Zusammenarbeit mit dem RZ,
4. die Beratung, Information und Weiterbildung der DVB,
5. Entwicklung von Sicherheitskonzepten für die TUHH.

Zur Erfüllung der Aufgaben kann der InSiBe

1. unter Wahrung des Datenschutzes zusammen mit dem DVB Einsicht in IT-Systeme, Netzwerkstruktur und Protokolldateien der Organisationseinheit nehmen oder Informationen verlangen, die eine Beurteilung der Gefährdung ermöglichen,
2. Maßnahmen wie eine Sperrung von Nutzer-Accounts oder eine Netztrennung ergreifen, um Gefahren abzuwehren und Missbrauch zu unterbinden, in gravierenden Fällen wird der CIO informiert,
3. im Rahmen von Maßnahmen unter Beachtung der Datenschutzgesetze den Netzwerkverkehr überwachen, mit dem Ziel Missbrauch und Bedrohungen frühzeitig zu erkennen oder aufzuklären,
4. IT-Systeme und Netze der TUHH auf Sicherheitsprobleme hin überprüfen oder überprüfen lassen,
5. Vertreter verschiedener Organisationseinheiten zur Entwicklung von Sicherheitskonzepten und zur Vorabstimmung neuer Richtlinien einladen.

Der InSiBe erstattet dem CIO zu Beginn jeden Jahres Bericht und informiert den Vorsitzenden des Senatsausschusses IT nachrichtlich. Der InSiBe und dessen Vertreter werden auf Vorschlag des RZ-Leiters vom Präsidium der TUHH beauftragt.

4. Datenverarbeitungsbeauftragte (DVB) der Organisationseinheiten

Die Verantwortung für die Informationssicherheit liegt bei der Leitung der Organisationseinheit. Die operativen Aufgaben können vom DVB, der gegenüber dem RZ von der Leitung benannt wird, übernommen werden. Dabei müssen dem DVB ausreichend Zeit und Ressourcen zur Verfügung gestellt werden, damit dieser den Aufgaben fachgerecht nachkommen kann. Der DVB

1. unterstützt und berät den Leiter fachlich in allen Fragen der Informationssicherheit und informiert diesen über die getroffenen Maßnahmen und sicherheitsrelevanten Vorfälle,
2. ist für alle Anwender der Organisationseinheit erster Ansprechpartner in Fragen der Informationssicherheit und wird dabei vom InSiBe unterstützt,
3. informiert und sensibilisiert alle Anwender der Organisationseinheit für Informationssicherheitsprobleme,
4. achtet auf die technische Umsetzung und Einhaltung von Maßnahmen und Regelungen, die dem Schutz der IT-Systeme dienen (insbesondere auf aktuelle Software-Versionen, sowie auf regelmäßiges Einspielen von Updates und eine in Hinblick auf die IT-Sicherheit angemessene Konfiguration),
5. bildet sich im Rahmen von Schulungen zu aktuellen Themen der Informationssicherheit weiter
6. arbeitet mit dem InSiBe bei der Einschätzung von Risiken, sowie Beurteilungen von Konzepten zusammen und meldet diesem sicherheitsrelevante Vorfälle.

Zur Erfüllung der Aufgaben kann der DVB

1. unter Wahrung des Datenschutzes in Abstimmung mit dem verantwortlichen Leiter IT-Systeme und Netze in der Organisationseinheit auf Sicherheitsprobleme hin überprüfen,
2. unter Wahrung des Datenschutzes zusammen mit den betroffenen System-Administratoren oder Nutzern Einsicht in IT-Systeme, Netzwerkstruktur und Protokolldateien der Organisationseinheit nehmen oder Informationen verlangen, die eine Beurteilung der Gefährdung ermöglichen,
3. in Absprache mit dem verantwortlichen Leiter Maßnahmen ergreifen, um Gefahren abzuwehren und Missbrauch zu unterbinden.

Bei der Benennung des DVB ist besonders auf eine personelle Kontinuität zu achten. Eine Organisationseinheit ohne einen DVB darf keine eigenen IT-Dienste (z.B. Web-Server) betreiben, bei denen die IT-Infrastruktur der TUHH genutzt wird. Die erforderlichen IT-Kompetenzen richten sich nach der betriebenen IT-Infrastruktur.

5. Datenverarbeitungsbeauftragte eigenständiger Organisationseinheiten

Organisationseinheiten wie z.B. der Allgemeine Studierendenausschuss (AStA) oder andere Forschungseinrichtungen sind juristisch eigene Personen und nicht unmittelbar der Weisung des Präsidiums der TUHH unterstellt, obwohl sie gänzlich oder zumindest teilweise in die Infrastruktur der TUHH integriert und durch diese mit IT-Dienstleistungen versorgt sind. Auch diese eigenständigen Organisationseinheiten müssen einen DVB und mindestens einen Vertreter gegenüber dem InSiBe benennen, der die Bereiche innerhalb der TUHH Infrastruktur vertritt.
Sollte eine Zusammenarbeit mit den eigenständigen Organisationseinheiten bei Sicherheitsvorfällen nicht möglich sein und eine akute Gefährdung der Infrastruktur bestehen, so werden die Organisationseinheiten zum Schutz der übrigen Teilnehmer temporär getrennt, bis die Probleme behoben oder ein Konsens mit dem Präsidium über die weitere Kooperation hergestellt wurde.
Für den DVB der eigenständigen Organisationseinheit gelten dieselben Aufgaben und Kompetenzen wie für die übrigen DVB, auch hier ist auf personelle Kontinuität zu achten.

6. Rechenzentrum (RZ)

Das RZ ist mit dem sicheren, operativen Betrieb der zentralen Infrastruktur der TUHH beauftragt. Insbesondere liegt die Hoheit des LAN, des Funknetzes sowie der Netzübergänge in Fremdnetze (z.B. Internet) im RZ. Andere Organisationseinheiten können gekapselte Teilnetze betreiben. Eine Verbindung in andere Netze oder eine konkurrierende Funknetz-Struktur erfordert jedoch eine schriftliche Abstimmung mit dem RZ, da hierdurch die Sicherheit und die Qualität der übrigen Teilnehmer betroffen sein kann.
Das RZ trifft geeignete Maßnahmen, um TUHH fremde Personen (etwa bei Kongressen, Raumvermietung an Externe) nur auf nötige Dienste (z.B. Internet-Zugang) zu beschränken. Das RZ setzt Maßnahmen (wie Beschränkungen von Ports / Protokollen) nach Empfehlung des InSiBe um.

7. Schlussbemerkung

Sicherheitsmaßnahmen müssen formuliert, kommuniziert, realisiert, überwacht und fortentwickelt werden. Letztendlich liegt dies immer in der Verantwortung des Präsidiums bzw. der Leitung der Organisationseinheit, auch wenn die faktische Zuarbeit durch den InSiBe und die DVB erfolgt.
Sofern einzelne Maßnahmen oder Regelungen einen gravierenden Einfluss auf die Arbeitsabläufe haben, sollten diese der Leitung zur abschließenden Entscheidung vorgelegt werden. Ausnahmen von solchen bindenden Maßnahmen und Regelungen bedürfen der schriftlichen Zustimmung.