

Ein Sicherheitskonzept für die IT-Infrastruktur des Fachbereichs Informatik*

Dr. Hans-Joachim Mück
Leiter des Informatik-Rechenzentrums
mueck@informatik.uni-hamburg.de

Michael Krooß
Mitarbeiter im Informatik-Rechenzentrum
krooss@informatik.uni-hamburg.de

Fachbereich Informatik
Universität Hamburg

17. März 2004

Zusammenfassung

Ziel dieses Textes ist es, ein Sicherheitskonzept für die IT-Infrastruktur des Fachbereichs Informatik darzustellen. Dazu werden zunächst die mit dem Sicherheitskonzept verfolgten Ziele und die an das Sicherheitskonzept gestellten Anforderungen aufgeführt. Dann werden die im Rahmen der Forschung und Lehre an die IT-Infrastruktur gestellten Anforderungen an die Funktionalität und daraus folgend die Anforderungen an die Sicherheit aufgezeigt. Anschließend werden die generellen Anforderungen an die Benutzer und an die Administration der IT-Infrastruktur aufgeführt. In den Anhängen dieses Sicherheitskonzepts sind konkretisierte Anforderungen an die Benutzer und Administration enthalten.

*Eine aktuelle Version des Sicherheitskonzepts kann über die Webseiten des Rechenzentrums <http://www.informatik.uni-hamburg.de/RZ/> bezogen werden.

Inhaltsverzeichnis

1	Zweck des Sicherheitskonzepts	3
2	Anforderungen an das Sicherheitskonzept	3
3	Anforderungen an die IT-Infrastruktur	4
3.1	Anforderungen an die Funktionalität	4
3.2	Anforderungen an die Sicherheit	4
4	Anforderungen an Benutzer der IT-Infrastruktur	5
5	Anforderungen an die Administration der IT-Infrastruktur	5
6	Pflege und Wartung des Sicherheitskonzepts	5
Anhänge		7
A	Gefährdungs- und Risikoanalyse	7
B	Benutzungsordnung	10
B.1	Benutzungsbestimmungen für die Benutzung der Rechenanlagen (alte Fassung vom 27. August 1990)	10
C	Betrieb eigener Geräte	12
C.1	Sicherheitsaspekte im öffentlichen Zugangsnetz	12
D	Beschreibung der Sicherheitsmaßnahmen	13

1 Zweck des Sicherheitskonzepts

Zweck dieses Sicherheitskonzepts soll es sein, die Anforderungen an die Funktionalität und die Sicherheit der IT-Infrastruktur des Fachbereichs Informatik explizit aufzuführen. Ferner sollen die hieraus resultierenden Anforderungen an die Benutzer und die Administratoren bestimmt werden. Dadurch sollen diese Personengruppen in die Lage versetzt werden, ihre Rechte und Pflichten bei der Arbeit mit bzw. der Betreuung der IT-Infrastruktur bestimmen zu können.

2 Anforderungen an das Sicherheitskonzept

An das Sicherheitskonzept werden die folgenden Anforderungen gestellt:

- Allgemein und umfassend
Das Sicherheitskonzept soll so allgemein und umfassend gehalten sein, dass es für alle Fachbereichseinheiten des Fachbereichs Informatik gilt (inkl. Verwaltung und Bibliothek).
- Verständlich
Das Sicherheitskonzept soll in einer verständlichen Art und Weise aufgeschrieben werden, so dass sowohl die Benutzer als auch die Administratoren in der Lage sind, einfach zu erkennen, welches Verhalten von ihnen erwartet wird.
- Realistisch
Das Sicherheitskonzept soll den Anforderungen und Möglichkeiten des Fachbereichs gerecht werden. Es sollen keine unnötigen Einschränkungen der Funktionalität erzwungen werden oder Maßnahmen vorgeschlagen werden, die nicht im Rahmen der Möglichkeiten (z.B. finanziell) des Fachbereichs liegen. Das Sicherheitskonzept soll sich am tatsächlichen Vorgehen orientieren. Es soll keine Maßnahmen enthalten, die nicht vollständig durchgesetzt werden.
- Wartbar
Das Sicherheitskonzept soll in einer Weise dokumentiert sein, dass eine Fortschreibung einfach möglich ist.
- Verwendbar
Das Sicherheitskonzept soll in einer Weise aufgeschrieben werden, so dass es von den Betroffenen gelesen wird. Um den von den Betroffenen zu lesenden Anteil möglichst gering zu halten, soll der Aufbau aufgabenbezogen gestaltet werden.

Um den Anforderungen zu entsprechen, ist das Sicherheitskonzept in einen konzeptionellen Teil (Abschnitte 1 bis 6) und Anhänge aufgeteilt. Der konzeptionelle Teil enthält die Anforderungen, die allgemein und beständig sind. Konkrete Anforderungen, die ständig aktuellen Entwicklungen anzupassen sind, sind in Anhängen – unterteilt nach Anforderungen, die die Benutzer bzw. die Administration betreffen – aufgeführt.

3 Anforderungen an die IT-Infrastruktur

Die IT-Infrastruktur des Fachbereichs Informatik soll die Mitarbeiter und Studierenden im Rahmen der Forschung und Lehre unterstützen. Die IT-Infrastruktur stellt für die Mitarbeiter und Studierenden des Fachbereichs Informatik eine unverzichtbare Ressource dar, deren Nicht-Verfügbarkeit zu Einbußen in der Produktivität des Forschens und des Studierens führt.

3.1 Anforderungen an die Funktionalität

Durch die IT-Infrastruktur soll einerseits eine freie Kommunikation und eine übergreifende gemeinsame Nutzung von Ressourcen ermöglicht werden, auf der anderen Seite sollen den Benutzern abgetrennte und geschützte Bereiche für ihre Prozesse und Daten zur Verfügung gestellt werden. Eine an Universitäten oft anzutreffende und in diesem Zusammenhang zu berücksichtigende Eigenheit der IT-Landschaft ist ihre Heterogenität. So werden auch am Fachbereich Informatik sehr unterschiedliche Plattformen und Netzwerkprotokolle genutzt. Für die zukünftige Entwicklung des Benutzerverhaltens und damit der Benutzeranforderungen lässt sich annehmen, dass diese Heterogenität nicht nur erhalten bleibt, sondern durch eine zunehmende Anzahl unterschiedlicher mobiler Endgeräte noch erhöht wird. Für das Rechenzentrum der Informatik ergibt sich als zentraler Dienstleister für die Bereitstellung der notwendigen IT-Infrastruktur hieraus die Anforderung, der steigenden Nachfrage nach Zugangspunkten zu Ressourcen der IT-Infrastruktur, dem steigenden Bedarf an Bandbreite und der Bereitstellung von evtl. aufkommenden neuen Diensten in einem angemessenen Rahmen zu entsprechen.

3.2 Anforderungen an die Sicherheit

Die Komponenten der IT-Infrastruktur sind anfällig gegenüber vielen Arten von Bedrohungen (vgl. Anhang A). Risiken liegen insbesondere im Verlust der Verfügbarkeit, im Missbrauch der Systeme durch autorisierte Benutzer bzw. durch externe Angreifer (z.B. für Angriffe auf Ziele innerhalb und außerhalb der Informatik-Domäne) und im Verlust der Vertraulichkeit bzw. der Integrität von Daten. Aus diesen Risiken können sich als Konsequenz für den Fachbereich und seine Mitglieder der Verlust von Produktivität, Werten und Ansehen, aber auch eine Schädigung Dritter ergeben.

Die Anforderungen an die Sicherheit der IT-Infrastruktur sind die Gewährleistung einer möglichst hohen Verfügbarkeit, eine weitestgehende Unterbindung von Missbrauch und die Wahrung der Vertraulichkeit von Daten. Bei der Durchsetzung der Anforderungen an die Sicherheit sind die Anforderungen an die Funktionalität zu berücksichtigen. Um Sicherheit und damit auch die Funktionalität zu gewährleisten, ist ein angemessenes Verhalten der Benutzer (vgl. Abschnitt 4) und der Administratoren (vgl. Abschnitt 5) notwendig.

4 Anforderungen an Benutzer der IT-Infrastruktur

Alle Benutzer sind verantwortlich für eine effektive, effiziente, ethische und legale Nutzung der IT-Infrastruktur des Fachbereichs. Die Benutzungserlaubnis stellt ein Nutzungsprivileg und kein Nutzungsrecht dar. Sie kann bei Missbrauch entzogen werden. Das Nutzungsprivileg besteht ausschließlich für universitäre Zwecke. Näheres regelt die Benutzungsordnung (vgl. Anhang B).

Benutzern ist es grundsätzlich gestattet, über private Geräte auf die IT-Infrastruktur des Fachbereichs Informatik zuzugreifen (vgl. Anhang C). In solchen Fällen ist zu beachten, dass die Benutzungsordnung auch bei einem Zugriff über private Geräte gilt. Die Benutzer werden in diesen Fällen als die Administratoren ihrer privaten Geräte angesehen und haben geeignete Maßnahmen zu treffen, damit die Sicherheit der IT-Infrastruktur nicht durch den Anschluss ihrer Geräte gefährdet wird (vgl. den folgenden Abschnitt 5)

5 Anforderungen an die Administration der IT-Infrastruktur

Am Fachbereich Informatik findet keine einheitliche Administration der IT-Infrastruktur statt. Neben den zentral vom Rechenzentrum des Fachbereichs betreuten Geräten werden in den Fachbereichseinheiten Geräte von diesen in Eigenverantwortung betreut und eigene Geräte der Benutzer an die IT-Infrastruktur des Fachbereichs angeschlossen. Die Administratoren haben geeignete Maßnahmen zu treffen, damit von den von ihnen administrierten Geräten keine Gefährdung der IT-Infrastruktur ausgeht. Im Anhang D werden die im Rechenzentrum des Fachbereichs verwendeten Sicherheitsmechanismen zum Schutz der zentral betreuten IT-Infrastruktur beschrieben.

6 Pflege und Wartung des Sicherheitskonzepts

Der konzeptionelle Teil des Sicherheitskonzepts wird vom Fachbereichsrat, die Anhänge des Sicherheitskonzepts von der IT-Kommission des Fachbereichs Informatik beschlossen. Durch die IT-Kommission des Fachbereichs Informatik wird mindestens einmal im Jahr überprüft, ob eine Anpassung des Sicherheitskonzepts notwendig ist.

A Gefährdungs- und Risikoanalyse

Man kann davon ausgehen, dass der Wert der IT-Infrastruktur im Fachbereich Informatik (FB18) als noch höher als in anderen Fachbereichen bzw. Disziplinen einzuschätzen ist, da sie nicht nur ein im Rahmen von Forschung und Lehre eingesetztes Werkzeug, sondern in der Regel auch der Gegenstand der Forschung und der Lehre ist. So muss davon ausgegangen werden, dass Fehler oder Ausfall der IT-Infrastruktur am FB18 vermutlich deutlich höhere Schäden durch Einbußen in der Forschung und Lehre nach sich ziehen würden, als es vielleicht in anderen Fachbereichen der Fall wäre. Dem Schutz der IT-Infrastruktur und seiner Komponenten ist daher eine hohe Aufmerksamkeit zu schenken.

Eine Nutzung der IT-Infrastruktur findet im FB18 insbesondere zur Verarbeitung, Speicherung und Übertragung der im Rahmen der Forschung und Lehre anfallenden Daten und Ergebnisse, zur Kommunikation und zur übergreifenden gemeinsamen Nutzung von Ressourcen statt. Als zu schützende **Werte** der IT-Infrastruktur sind dabei zu betrachten, die am FB18 im Rahmen von Forschung und Lehre, sowie in der Verwaltung dieser genutzten

- Daten, wie personenbezogene Daten, für die eine gesetzliche Schutzpflicht besteht, und die im Rahmen der Forschung und der Lehre anfallenden Ergebnisse und Teilergebnisse.
- Anwendungen, wie Textverarbeitung, Entwicklungswerkzeuge, Compiler, Datenbanken und Clients für Netzwerkdienste, sowie weitere für die Nutzung dieser Anwendungen notwendige Software, wie die Betriebssysteme,
- Dienste, wie der Email-Übertragungsdienst, Dateitransferdienste und andere Datenübertragungsdienste, sowie die zur Nutzung dieser Dienste notwendigen weiteren Dienste, wie z.B. der Domain Name Service (DNS),
- und schließlich die für die Erbringung der Dienste und für das Ablaufen der Software notwendige Hardware, wie die Endgeräte, Server, Peripherie und die Netzwerkinfrastruktur.

Die sich ergebenden **Schutzziele** umfassen die Wahrung der Vertraulichkeit (z.B. bei der Speicherung und Übertragung von personenbezogenen Daten), die Wahrung der Integrität (z.B. bei der Verarbeitung und der Übertragung von Daten) und die Wahrung der Verfügbarkeit (z.B. bei der Speicherung von Daten).

Diesen Schutzziele wird durch das Auftreten von Vorfällen entgegengewirkt. Vorfälle entstehen durch das Aufeinandertreffen von Verwundbarkeiten und Bedrohungen. Die eingesetzte IT-Infrastruktur birgt viele **Verwundbarkeiten**, die teilweise der eingesetzten Technik inhärent zugrunde liegen, teilweise aber auch durch die Einsatzumgebung, die Administration oder die Nutzung verursacht werden. Zu diesen Verwundbarkeiten gehören

- Fehler beim Entwurf (z.B. Nicht-Berücksichtigung von Anforderungen) oder der Konstruktion (z.B. keine Überprüfung von Eingabewerten),

- Unangemessenheit von Schutzmechanismen bedingt durch den Einsatz in Umgebungen oder für Zwecke, die beim Entwurf nicht vorgesehen waren (vgl. z.B. das Internet Protocol (IP), das in der Version 4 keine Mechanismen für Authentizität oder Integrität vorsieht, aber trotzdem in sensiblen Bereichen eingesetzt wird),
- Sicherheitslücken bedingt durch Fehler oder Versäumnisse bei der Administration, wie z.B. die Bereitstellung (Nicht-Deaktivierung) von nicht benötigten Diensten oder das einmalige Einrichten eines Systems ohne regelmäßiges Einspielen von Patches und ohne Durchführung von anderen Anpassungen an geänderte Anforderungen,
- Sicherheitslücken entstehend durch Fehlverhalten bei der Nutzung, wie z.B. durch das Abschalten von Sicherheitsfeatures aus Performancegründen und die Nutzung (und daraus folgend die Bereitstellung) von inhärent unsicheren Diensten (z.B. Klartextübertragung von Passwörtern bei telnet, rsh, usw.),
- die einfache Möglichkeit große Werte zu entwenden, wie z.B. das oft einfach mögliche Kopieren von Software oder Daten bzw. der Diebstahl von nicht sehr großer oder schwerer aber wertvoller Hardware (insbesondere CPUs oder Speicherbausteine),
- Anfälligkeit gegen Umwelteinflüsse, wie Temperatur, Staub, Wasser, Schwankungen in der Stromversorgung usw.

Bedrohungen können ausgehen von autorisierten Benutzern, die Systeme missbrauchen, von externen Angreifern, Malware jeglicher Form, höherer Gewalt (z.B. Ausfall von Hard- oder Software, Eintritt von Wasser oder Ausbruch von Feuer) und Fehler in der Nutzung und in der Administration (z.B. Eingabe nicht akzeptierter Werte, versehentliches Löschen von Daten).

Unter **Risiko** wird in diesem Zusammenhang oft die Auftrittswahrscheinlichkeit von Vorfällen verknüpft mit dem zu erwartenden Ausmaß der Schäden verstanden. Als Schäden sind hier nicht nur einfach quantifizierbare Schäden z.B. durch Ersatzbeschaffungen, sondern insbesondere auch nicht einfach zu quantifizierende Schäden, wie Einbußen in der Produktivität durch die eingeschränkte Verfügbarkeit der IT-Infrastruktur oder Schädigung des Ansehens, zu berücksichtigen. Am FB18 bestehen einerseits Risiken durch die mögliche Notwendigkeit von Ersatzbeschaffungen, z.B. nach Ausfall oder Diebstahl. Andererseits bestehen aber auch nicht einfach zu quantifizierende Risiken durch Einbußen in der Produktivität, z.B. nach temporären oder dauerhaften Ausfall von dezentralen oder zentralen Komponenten der IT-Infrastruktur, sowie durch eine Schädigung des Ansehens, z.B. beim Missbrauch der IT-Infrastruktur des FB18 bei Angriffen auf Dritte, bei der nicht gewollten Offenlegung sensibler Daten und bei der Nicht-Einhaltung von Fristen.

Damit das Gesamtausmaß der Schäden am FB18 möglichst gering gehalten wird, ist es notwendig, die Verwundbarkeiten der IT-Infrastruktur, die den Schutzzielen entgegenwirken, auf ein akzeptables Maß zu verringern. Eine Einschränkung der Verwundbarkeiten kann grundsätzlich durch eine Einschränkung des Leistungsumfangs (z.B. der bereitgestellten Dienste) oder durch den Einsatz von Schutzmaßnahmen erfolgen. Eine Einschränkung

des Leistungsumfangs ist in dem hier betrachteten universitären Umfeld im Allgemeinen nicht angebracht. Wohl aber können gewisse Leistungen durch andere mit einem geringeren Risiko ersetzt werden. Dies trifft z.B. auf verschiedene Dienste zu, bei denen eine Übertragung des Passworts grundsätzlich im Klartext erfolgt (vgl. telnet, rsh, pop3, imap). Diese können oft ohne großen Aufwand durch gleichwertige Dienste ersetzt werden, bei denen eine Verschlüsselung der übertragenen Daten oder zumindestens der übertragenen Passworte erfolgt. Der Einsatz von Schutzmaßnahmen am FB18 wird im Anhang D des Sicherheitskonzepts beschrieben.

B Benutzungsordnung

Zur Zeit sind am Fachbereich Informatik die „Benutzungsbestimmungen für die Benutzung der Rechenanlagen“ in der Fassung vom 27. August 1990 gültig (vgl. Anhang B.1). Auf Ebene der Universität wird unter der Federführung des Regionalen Rechenzentrums ein Entwurf für eine einheitliche Benutzungsordnung diskutiert. Diese soll den aktuell bestehenden Anforderungen gerecht werden (vgl. „Entwurf einer Muster-Benutzungsordnung für Universitätsrechenzentren und sonstige wissenschaftliche Forschungseinrichtungen im Deutschen Forschungsnetz“¹). Sobald dieser Entwurf verabschiedet wurde, sollen die bisher geltenden Benutzungsbestimmungen durch die Benutzungsordnung ersetzt werden.

B.1 Benutzungsbestimmungen für die Benutzung der Rechenanlagen (alte Fassung vom 27. August 1990)

1. Aufgrund der Mitarbeit in Projekten erhält die Benutzerin / der Benutzer (im folgenden B genannt) auf Antrag seiner Projektleiter eine Benutzungserlaubnis (in Form einer Benutzerkennung) für die Arbeit auf den im Projekt vorgesehenen Rechnern.

Studierende erhalten in einem vereinfachten Verfahren eine Benutzungserlaubnis für Übungen in kleinem Umfang sowie für persönlichen E-Mail-Zugang.

Die Benutzungserlaubnis gilt nur für den beantragenden Benutzer und nur für Arbeiten im Rahmen der jeweiligen Projekte. Die Nutzung der Rechner für private und kommerzielle Zwecke ist ausdrücklich ausgeschlossen. Die Projektleiter oder die Anlagenbetreiber können die Benutzungserlaubnis aus wichtigen Gründen jederzeit zurückziehen. Die Benutzerkennung gilt ausschließlich für den Benutzer, dieser hat dafür Sorge zu tragen, daß die Benutzerkennung nicht von anderen benutzt werden kann (insbesondere durch sorgfältige Wahl, Geheimhalten und regelmäßige Änderung des Paßwortes.

Wenn B bekannt wird oder der Verdacht besteht, daß die Benutzerkennung mißbräuchlich von anderen verwendet worden ist bzw. das Paßwort bekannt geworden ist, so hat er dies sofort den Anlagenbetreibern zu melden und unverzüglich das Paßwort zu ändern.

Die Benutzung spezieller Ressourcen (z.B. Benutzung von E-Mail oder File-Transfer außerhalb des Fachbereichs) über den von den Projektleitern beantragten Rahmen hinaus ist nur mit besonderer Genehmigung der Systembetreiber zulässig.

Den Anordnungen der Systembetreiber und der Projektleiter hinsichtlich der Benutzung der Anlagen ist Folge zu leisten.

2. B verpflichtet sich, die Rechte von urheberrechtlich bzw. vertraglich geschützter Software zu wahren. Insbesondere sind das Kopieren, die Mitnahme und/oder Weitergabe von Software oder Dokumentation verboten, sofern dies nicht explizit erlaubt (z.B. Public Domain-Programme) oder für die Projektarbeit erforderlich ist. In jedem Fall sind dabei aber die gesetzlichen und lizenzrechtlichen Bestimmungen einzuhalten. Nach Ablauf der Benutzungserlaubnis hat B unaufgefordert alle o.g. geschützte Software und Dokumentation, die noch

¹<http://www.dfn.de/index.jsp?path=/beratung-weiterbildung/rechtimdfn/archiv/musterbenutzungsordnung/>

in seinen Besitz ist, an die Projektleiter zurückzugeben und ggf. angefertigte Kopien davon zu vernichten, sofern das Einbehalten der Software oder Dokumentation nicht explizit (z.B. durch die Projektleiter oder die Autoren) erlaubt ist.

Sofern B Zugang zu spezieller, nicht allgemein zugänglicher Software gewährt wird, ist er bei seiner Arbeit verpflichtet, darauf zu achten, daß auf die Software nicht von Unbefugten zugegriffen werden kann.

3. Die Verarbeitung personenbezogener Daten (nach dem Bundesdatenschutzgesetz und dem Hamburger Datenschutzgesetz) ist im allgemeinen nicht zulässig und bedarf der Anmeldung und Genehmigung durch die Systembetreiber.
4. Die Systembetreiber sind bemüht, einen möglichst störungsfreien Betrieb der Anlagen zu gewährleisten. B hat aber keinen Anspruch auf die Benutzung der Anlagen oder auf deren störungsfreien Betrieb. Insbesondere kann einzelnen Benutzergruppen zu bestimmten Zeiten der Zugang zu den Anlagen untersagt werden.

Die Systembetreiber oder Projektleiter können unter keinen Umständen für den Verlust von Daten oder daraus resultierende Schäden verantwortlich gemacht werden.

5. Die rechtliche Unwirksamkeit einzelner Teile dieser Bestimmungen berührt die Gültigkeit der übrigen Bestimmungen nicht.

C Betrieb eigener Geräte

Um Mitarbeitern und Studierenden die Möglichkeit zu bieten, auch ihre privaten Notebooks/Rechner auf dem Stelling Campus für die Nutzung zu universitären Zwecken an das Fachbereichs-Datennetz anbinden zu können, wird vom Rechenzentrum des Fachbereichs Informatik (FB18-RZ) derzeit ein sog. öffentliches Zugangsnetz aufgebaut, welches sowohl aus Wireless-Access-Points als auch aus Festnetz-Anschlussplätzen bestehen wird. Der Aufbau erfolgt in Kooperation mit dem Regionalen Rechenzentrums (RRZ) der Universität, von dem zur Zeit ein Zugangsnetz für die anderen Einrichtungen der Universität aufgebaut wird. Das auf dem Stelling Gelände betriebene öffentliche Zugangsnetz kann im Testbetrieb von allen Studierenden und Mitarbeitern mit einer gültigen Benutzerkennung des FB18-RZ oder des RRZ genutzt werden. Die im Antrag auf Erteilung einer Benutzungserlaubnis akzeptierten Benutzungsbestimmungen behalten auch im öffentlichen Zugangsnetz ausdrücklich ihre Gültigkeit!

Zur Zeit wird am Fachbereich Informatik außerdem die Praxis geduldet, dass Mitarbeiter ihre Geräte unkontrolliert an das interne Fachbereichs-Netz anschließen. Bei Übernahme des öffentlichen Zugangsnetzes in den Regelbetrieb soll diese Praxis unterbunden werden.

C.1 Sicherheitsaspekte im öffentlichen Zugangsnetz

Die Anmeldung erfolgt zunächst in dem öffentlichen Netz und wird nach Überprüfung einer gültigen Benutzerkennung über eine Firewall in das Fachbereichsnetz geschaltet. Da die Funktionalität dieses Verfahrens (ssh-Anmeldung an Firewall) zur Zeit auf eine Auswahl gesicherter Dienste eingeschränkt ist, wird auch das Anbinden über einen VPN-Tunnel angeboten. Die beiden Verfahren unterscheiden sich damit in folgendem:

- SSH-Anmeldung an Firewall: ssh/scp/http/https/ftp/imaps/pop3s, Printserver für die Druckerqueues d105_hp und d116_hp.
- VPN-Tunnel mit PPTP bzw. L2TP über IPSec: volle Funktionalität im Fachbereichsnetz, der Durchsatz ist aber stark abhängig von Verschlüsselungsleistung des Clients.

Es muss ausdrücklich darauf hingewiesen werden, dass insbesondere im Wireless-Bereich bekanntermaßen die Möglichkeiten für einen aus Sicht des einzelnen Benutzers sicheren Betrieb sehr begrenzt sind. Um sowohl einen Schutz gegen das Abhören der übertragenen Daten als auch gegen gezielte Angriffe aus dem Zugangsnetz auf den eigenen Rechner sicherstellen zu können, sind unbedingt entsprechende Maßnahmen durch den Benutzer selbst vorzunehmen! Es wird daher dringend empfohlen, eine persönliche Firewall mit möglichst restriktiven Einstellungen auf dem Notebook zu nutzen! Für den Zugang zum Fachbereichsnetz und damit zum Internet ist die Nutzung von zusätzlicher Verschlüsselung (ssh/ssl-Applikationen bzw. VPN) vorgesehen.

D Beschreibung der Sicherheitsmaßnahmen

Nur für den internen Gebrauch