Ergänzungen zur IT- Sicherheitsrichtlinie der Fachhochschule Wiesbaden

A) Leitfaden zur IT-Sicherheitsrichtlinie der FH Wiesbaden

Version: 1.0

Kontaktadressen, Handlungsanweisungen und Erläuterungen

Überblick

Dieses Dokument beinhaltet eine vom ITSB in Abstimmung mit dem ITC herausgegebene komplette Liste der Kontaktadressen sowie Verfahrensweisen und Erläuterungen zu den in der Sicherheitsrichtlinie behandelten Themen und wird fortlaufend aktualisiert.

In einem separaten Dokument ist ein Musterprotokoll zu finden, das zur Protokollierung bei sicherheitsrelevanten Vorfällen genutzt werden sollte.
Das ausgefüllte Protokoll wird dann bei der Systemadministratorin / beim Systemadministrator des betroffenen Systems aufbewahrt. Eine Kopie davon ist an die IT-Sicherheitsbeauftragte / den IT-Sicherheitsbeauftragten der FH Wiesbaden zu schicken.

Versionen

An dieser Stelle sind Überarbeitungen des Dokuments mit einer kurzen Zusammenfassung der Änderungen vermerkt.
Version: Juli 2007

Kontaktadressen:

Beratung und Hilfe beim Betrieb eines Computers, Probleme mit Viren, Vorbeugung, Antivirensoftware	Tel: 0611/9495-700 E-Mail für FHW Studierende: support@itc.fh-wiesbaden.de E-Mail für Mitarbeiter: service@itc.fh-wiesbaden.de
Netzprobleme	Tel: 0611/9495-700 E-Mail: netzwerk@itc.fh-wiesbaden.de
Probleme mit Crackern Beschwerden wegen Spam-Mail Schwerwiegende Verstöße gegen die Netiquette Schwerwiegende Verstöße gegen das Urheberrecht und/oder lizenzrechtliche Vertragsbestimmungen	Tel: 0611/9495-700 E-Mail: abuse@itc.fh-wiesbaden.de
Bekanntgabe von Änderungen bei der Systemadministration und Auffinden verantwortlicher Systemadministratorinnen und Systemadministratoren, sowie der / des Domainbeauftragten der FH Wiesbaden	E-Mail: netzwerk@itc.fh-wiesbaden.de

SystemadministratorInnen an der FH Wiesbaden:

Name:	Fachbereich, Organisationseinheit
ITC	Verwaltung, Zentrale Einrichtungen
Frank Salffner	Fachbereich Architektur und Bauingenieurwesen
Sonja Tuxhorn	Fachbereich Architektur und Bauingenieurwesen
Carlos Henriques dos Santos	Fachbereich Design Informatik Medien, Studienbereich Informatik
Frank Köhler	Fachbereich Design Informatik Medien, Studienbereich Informatik
Sebastian Rost	Fachbereich Design Informatik Medien, Studienbereich Gestaltung
Stefan Kanitz	Fachbereich Design Informatik Medien, Studienbereich Medienwirtschaft
Jörn Hoffmann	Fachbereich Sozialwesen
Birgit Wiera	Fachbereich Wirtschaft
Kai-Uwe Beetz	Fachbereich Wirtschaft
Armin Leukel	Fachbereich Ingenieurswissenschaften, Studienbereich Maschinenbau
Thomas Pistor	Fachbereich Ingenieurswissenschaften, Studienbereich Maschinenbau
Achim Klippel	Fachbereich Ingenieurswissenschaften, Studienbereich Umwelttechnik und Dienstleistungen
Axel Zuber	Fachbereich Ingenieurswissenschaften, Studienbereich Umwelttechnik und Dienstleistungen
Mathias Blüm	Fachbereich Ingenieurswissenschaften, Studienbereich Informationstechnologie und Elektrotechnik
Henning Wirbs	Fachbereich Ingenieurswissenschaften, Studienbereich Informationstechnologie und Elektrotechnik
Robert Lönarz	Fachbereich Geisenheim
Julian Range	Forschungsanstalt Geisenheim

Auffinden zuständiger Systemadministratorinnen Systemadministratoren: - weltweit: - Europa: - Nordamerika: - Lateinamerika, Karibik - Asien, Pazifik:	 URL: http://www.ripe.net/cgi-bin/whois URL: http://www.arin.net/whois/index.html URL: http://lacnic.net/en/index.html URL: http://www.apnic.net/

Übersichtstabelle - Verstöße

A. Verwendung elektronischer Kommunikation für Attacken gegen Einzelpersonen oder Gruppen von Personen

	Regelverstoß	***Ansprechpartner***
A1	Verbreitung oder In-Umlauf-Bringen von Informationen, die Personen beleidigen oder herabwürdigen (z. B. aufgrund ihrer Hautfarbe, Nationalität, Religion, ihres Geschlechtes, ihrer politischen Gesinnung oder sexuellen Ausrichtung)	Wenden Sie sich direkt an den die **Absenderin** / den **Absender** bzw. die **Verursacherin /** den **Verursacher** der Nachricht. Klären Sie die betreffende Person darüber auf, dass sie gegen die IT-Sicherheitsrichtlinie der FH Wiesbaden verstößt, verlangen Sie gegebenenfalls die Löschung der Daten, sowie die zukünftige Unterlassung derartiger Verstöße. Falls dieses zu keinem Ergebnis führt: Wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de **Hinweis**: Schicken Sie die Beschwerde, wenn möglich, **mit** dem Inhalt der Nachricht **und** immer mit sämtlichen Absenderinformationen (E-Mail-Header) bzw. Adressdaten (WWW, Newsgroup, etc.).
A2	Verbreitung von persönlichen oder anderen schützenswerten Informationen über eine Einzelperson oder eine Gruppe von Personen.	
A3	Mehrfach unerwünschtes Zusenden von Nachrichten.	

Anmerkung: Das unerwünschte und wiederholte Zusenden von Nachrichten sowie das Verbreiten von beleidigenden oder herabwürdigenden Informationen, oder das Verbreiten von unwahren Aussagen über eine Person oder Gruppe von Personen verstoßen gegen gesetzliche Regelungen (u. a. StGB) sowie den im Internet allgemein üblichen Verhaltenskodex (**Netiquette**). Die FH Wiesbaden sieht als intensiver Benutzer des Internets und als große Organisation, deren Angehörige verschiedene Weltanschauungen vertreten, die Notwendigkeit, Regeln für die korrekte Verwendung der elektronischen Kommunikation aufzustellen.

B. Verwendung elektronischer Kommunikation zur Behinderung der Arbeit Dritter

B1	*Regelverstoß*	*Ansprechpartner*
	Behinderung der Arbeit anderer (z. B. durch **"Mailbomben"** und ähnliche Techniken)	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher** der Attacke. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr die Unterlassung der Attacken. Falls dieses zu keinem Ergebnis führt: Wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de **Hinweis**: Schicken Sie die Beschwerde wenn möglich **mit** dem Inhalt der Nachricht **und** immer mit sämtlichen Absenderinformationen (E-Mail-Header).
	Anmerkung: Das Versenden von **Mailbomben** und die Verwendung ähnlicher Techniken erschwert oder macht die Arbeit einer Person unmöglich.	

B2	*Regelverstoß*	*Ansprechpartner*
	Aneignung von Ressourcen über das zugestandene Maß	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher** des Problems. Klären Sie die betreffende Person darüber auf, dass sie gegen die IT Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung. Informieren Sie den zuständigen Systemadministrator von den Vorfällen. Falls dieses zu keinem Ergebnis führt: Wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de
	Anmerkung: Aneignung von Ressourcen über das zugestandene Maß. Dazu zählt eine Benutzung von Ressourcen (z.B. Rechenzeit, Plattenplatz, Drucker, Netzwerk) durch einen Benutzer in einem Maß, das die bei der Vergabe der Zugangsberechtigung zu erwartenden Dimensionen überschreitet und damit andere Benutzer bei der Erfüllung ihrer Aufgaben behindert.	

B3	*Regelverstoß*	*Ansprechpartner*
	Versenden von elektronischen Massensendungen (**Spam E-Mails**). (Ausnahme: Verbreitung von dienstlichen Mitteilungen in Analogie zur Hauspost.)	**Achtung: die Absenderadresse sind in den meisten Fällen gefälscht!** Bei **Spam**-Mails, die **aus der FHW heraus** verschickt wurden, wenden Sie sich direkt an den

		Absender der Nachricht. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung Falls dieses zu keinem Ergebnis führt: Wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de **Hinweis**: Schicken Sie die Beschwerde wenn möglich **mit** dem Inhalt der Nachricht **und** immer mit sämtlichen Absenderinformationen (E-Mail-Header). Bei **Spam**-Mails, die **von außerhalb der FHW** verschickt wurden, ist i. A. keine Verfolgung möglich. **Löschen Sie daher diese Mails !**
	Anmerkung: Das Versenden von **elektronischen Massensendungen** (z. B. **Spam E-Mails**), insbesondere zu kommerziellen Zwecken, wird von den meisten Benutzern als störend empfunden und ist nicht gestattet. Erlaubt sind allerdings Ankündigungen von internen Veranstaltungen, das Versenden von Verordnungen etc. in Analogie zum Versand durch die Hauspost. Das Führen von Mailing-Listen, in die sich Adressaten selbst eintragen können, ist ebenfalls gestattet.	

B4	***Regelverstoß***	***Ansprechpartner***
	Weitersenden oder In-Umlauf-Bringen von elektronischen **Kettenbriefen**.	Wenden Sie sich direkt an die **Absenderin** / den **Absender** der Nachricht. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung. Falls dieses zu keinem Ergebnis führt, wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de **Hinweis**: Schicken Sie die Beschwerde wenn möglich **mit** dem Inhalt der Nachricht **und** immer mit sämtlichen Absenderinformationen (E-Mail-Header).
	Anmerkung: Elektronische Kettenbriefe sind meistens harmlos und mehr oder weniger informativ. Sie verursachen aber Kosten (z. B. Telefongebühren) und werden manchmal mit dem Ziel verschickt, bestimmte Mailserver (z. B. einer Konkurrenzfirma) zu blockieren. In Einzelfällen kann es auch zur Blockade von Teilen des Internets kommen. Aus diesem Grund ist das Weitersenden oder In-Umlauf-Bringen von elektronischen Kettenbriefen verboten. Seien Sie sich bewusst, dass Benachrichtigungen über Sicherheitsprobleme von Softwareherstellern so gut wie nie über E-Mail erfolgen, auf keinen Fall werden Sie darin aber aufgefordert, diese Informationen weiterzuleiten. Auch Organisationen, die sich mit Netz- und Computersicherheit oder der Virenproblematik beschäftigen, versenden Benachrichtigungen nur auf Anforderung. Sollten Sie also eine E-Mail mit der Aufforderung erhalten, den Inhalt an möglichst viele Bekannte weiterzuschicken, können Sie davon ausgehen, dass es sich um einen elektronischen Kettenbrief handelt.	

B5	*Regelverstoß*	*Ansprechpartner*
	Unberechtigte Manipulation von elektronischen Daten anderer.	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher**. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung. Informieren Sie den Systemadministrator von den Vorfällen. Sollte keine eigenständige Lösung des Problems möglich sein, wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de.

Anmerkung: Unberechtigte Manipulation von elektronischen Daten.
Dazu zählt die Veränderung, Verfälschung etc. von elektronischen Daten ohne vorhergehende Zustimmung der Besitzerin / des Besitzers.

Falls Sie die Manipulation von Dokumenten bemerken oder davon informiert werden, führen Sie folgende Schritte durch:

1. Als BenutzerIn

- Wenn Sie Manipulationen Ihrer eigenen Dokumente bemerken, überprüfen Sie zuallererst, ob die Besitzrechte (permissions) richtig gesetzt sind, und ändern Sie sofort Ihr Passwort.
- Sollten Sie keine Anhaltspunkte dafür finden, wie es zur Manipulation Ihrer Dokumente kommen konnte, wenden Sie sich an den zuständigen Systemadministrator.
- Sind Sie der Meinung, die Verursacherin / den Verursacher der Manipulation zu kennen, so teilen Sie Ihren Verdacht dem zuständigen Systemadministrator mit.
- Wenn es sich um Daten Dritter handelt, informieren Sie die Besitzerin / den Besitzer der Daten und die zuständige Systemadministratorin / den zuständigen Systemadministrator von Ihren Beobachtungen.

2. Als SystemadministratorIn

- Falls Sie davon informiert wurden, überprüfen Sie die Angaben auf deren Richtigkeit.
- Führen Sie eine umfassende Sicherheitsüberprüfung Ihres Computers durch.
- Falls Sie den Verursacher der Manipulation ausfindig machen konnten, sperren Sie dessen Zugangsberechtigung.

Falls keine Zugangsberechtigung vergeben wurde, handelt es sich auch um eine unerlaubte Aneignung von Zugangsberechtigungen (**siehe D2**).

B6	*Regelverstoß*	*Ansprechpartner*
	Zugriff auf Daten Dritter ohne deren Erlaubnis.	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher**. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung.

		Informieren Sie den Systemadministrator von den Vorfällen. Sollte keine eigenständige Lösung des Problems möglich sein, wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de

Anmerkung: Zugriff auf Daten Dritter ohne deren Erlaubnis.
Nicht nur die Manipulation fremder Daten, auch der unbefugte Zugriff (Lesen, Kopieren etc.) ist unzulässig. Ausnahmen davon sind z. B. das Anlegen von Sicherungen u. ä. durch den Systemadministrator und das Löschen von Daten, wenn dies technisch unumgänglich ist (z. B. temporäre Daten) oder durch die Sicherheitsrichtlinie ausdrücklich verlangt wird.

C. Vergehen gegen Lizenzvereinbarungen oder andere vertraglichen Bestimmungen

C1	*Regelverstoß*	*Ansprechpartner*
	Die Nutzung, das Kopieren und Verbreiten von urheberrechtlich geschütztem Material im Widerspruch zu Lizenzvereinbarungen oder anderen Vertragsbestimmungen auf Computern der FH Wiesbaden bzw. der Transport über das Netz der FH Wiesbaden.	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher**. Klären Sie die betreffende Person darüber auf, dass diese gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, verlangen Sie ggf. die **sofortige** Löschung der Daten, sowie die zukünftige Unterlassung derartiger Verstöße. Falls dieses zu keinem Ergebnis führt, wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de

Anmerkung:

Falls Sie Vergehen bemerken oder davon informiert werden, führen Sie folgende Schritte durch:

1. Als Benutzerin / Benutzer

- Kontaktieren Sie die Besitzerin / den Besitzer der Daten und klären Sie, ob es rechtliche Implikationen gibt.
- Wenden Sie sich an die zuständige Systemadministrator / den zuständigen Systemadministrator.

2. Als Systemadministratorin / Systemadministrator

- Falls Sie davon informiert wurden, überprüfen Sie die Angaben auf deren Richtigkeit.
- Falls die Verursacherin / der Verursacher nicht zur Unterlassung bereit ist, ergreifen Sie geeignete Maßnahmen, die den Zugriff zu diesen Daten unterbinden.

C2	*Regelverstoß*	*Ansprechpartner*
	Verletzung des Urheberrechts durch Verfälschung elektronischer Dokumente.	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher**. Klären Sie die betreffende Person darüber auf, dass diese gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr die Kenntnisnahme der Sicherheitsrichtlinie. Es muss sichergestellt werden, dass das Dokument wieder in den ursprünglichen Zustand gebracht wird. Eine Benachrichtigung des ITC sollte **in jedem Fall** erfolgen, auch dann schon, wenn der Verursacher sein Tun korrigiert und keine weiteren direkten Maßnahmen erforderlich sind.

Anmerkung:

Falls Sie Vergehen bemerken oder davon informiert werden, führen Sie folgende Schritte durch:

1. Als Benutzerin / Benutzer

- Kontaktieren Sie die Besitzerin / den Besitzer der Daten, bzw. das ITC oder die IT-Sicherheitsbeauftragte / den IT Sicherheitsbeauftragten und klären Sie, ob es rechtliche Implikationen gibt.
- Wenden Sie sich an die zuständige Systemadministratorin / den zuständigen Systemadministrator.

2. Als Systemadministratorin / Systemadministrator

- Falls Sie davon informiert wurden, überprüfen Sie die Angaben auf deren Richtigkeit.
- Kontaktieren Sie die Besitzerin / den Besitzer der Daten und klären Sie, ob es rechtliche Implikationen gibt.
  Falls der Urheber dazu nicht bereit ist, ergreifen Sie geeignete Maßnahmen, die den Zugriff zu diesen Daten unterbinden.

C3	*Regelverstoß*	*Ansprechpartner*
	Weitergabe von **Zugangsberechtigungen** an Dritte. (Accounts und Passwörter)	Wenden Sie sich direkt an die **Urheberin** / den **Urheber**. Klären Sie die betreffende Person darüber auf, dass diese gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr die Kenntnisnahme der Sicherheitsrichtlinie. Falls dieses zu keinem Ergebnis führt, wenden Sie sich an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de

	Anmerkung: Weitergabe von Zugangsberechtigungen an Dritte, außer wenn diese durch Vereinbarungen abgedeckt ist. Die Erteilung von Zugangsberechtigungen ist an vertragliche Bestimmungen gebunden. (siehe dazu auch IT Benutzungsordnung der FH Wiesbaden unter http://www.fh-wiesbaden.de/irc/ordnungen/). Eine undokumentierte Weitergabe von Zugangsberechtigungen verletzt diese Vertragsbestimmungen und erschwert außerdem die Analyse bei sicherheitsrelevanten Vorfällen. Falls Sie Vergehen bemerken oder davon informiert werden, führen Sie folgende Schritte durch: **- Als Benutzerin / Benutzer** • Informieren Sie Ihre Systemadministratorin / Ihren Systemadministrator. **- Als Systemadministratorin / Systemadministrator** • Sperren Sie den Zugang bis die Person über den Verstoß gegen die Sicherheitsrichtlinie aufgeklärt wurde. • Sollte ein Computer ohne Genehmigung im lokalen Netz der FH Wiesbaden betrieben werden, entfernen Sie ihn aus dem Netz und informieren Sie das ITC.

D. Verwendung elektronischer Kommunikation für Attacken gegen Computer, das Netz oder Services, die darauf erbracht werden

D1	***Regelverstoß***	***Ansprechpartner***
	Systematisches Ausforschen von Servern und Services (z.B. **"Portscans"**). Ausnahme: Sicherheitstests nach Absprache mit dem Systemadministrator.	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher** des Problems. Klären Sie die betreffende Person darüber auf, dass sie gegen die IT-Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr eine schriftliche Kenntnisnahme. **und** Meldung an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de Fügen Sie der E-Mail die relevanten Auszüge aus Ihren Log-Dateien bei.
	Anmerkung: Systematisches Ausforschen von Servern und Services (z. B. **"Portscans"**). Ausnahme: Sicherheitstests nach Absprache mit der Systemadministratorin / dem Systemadministrator. Portscans sind oft ein erster Schritt einer Attacke durch Cracker, bei der Informationen über Topologie und Services eines Netzes gesammelt werden.	

<table>
<tr><th></th><th>Regelverstoß</th><th>Ansprechpartner</th></tr>
<tr><td>D2</td><td>Unerlaubte Aneignung von Zugangsberechtigungen oder der Versuch einer solchen Aneignung (z. B. Cracken).</td><td rowspan="2">Wenden Sie sich direkt an die Systemadministratorin / den Systemadministrator des Computers (Netzes), von dem aus die Attacken stammen. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr die Verhinderung solcher Attacken.

und

Meldung an den ITC unter der E-Mail: abuse@itc.fh-wiesbaden.de

Fügen Sie der E-Mail die relevanten Auszüge aus Ihren Log-Dateien bei.</td></tr>
<tr><td>D3</td><td>Beschädigung oder Störung von elektronischen Diensten
(z.B. "Denial of service attacks").</td></tr>
<tr><td></td><td colspan="2">Unerlaubte Aneignung von Zugangsberechtigungen oder der Versuch einer solchen Aneignung (z. B. "Cracken") und so genannte "Denial-of-Service-Attacken" (DoS) zählen zu den schwerwiegendsten Verstößen gegen die Sicherheitsrichtlinie.
Im Rahmen eines erfolgreichen Hackerangriffs wird gegen mehrere Regeln verstoßen. Dazu zählen der unerlaubte Zugriff auf fremde Daten, die Aneignung von Ressourcen und sehr oft auch die Verwendung der angeeigneten Ressourcen (Computer) für Angriffe auf weitere Computer. Der Angreifer verfügt über ein Standbein im lokalen Netz der FH Wiesbaden und erhält damit implizit Zugriff auf Daten, die diesem nicht zustehen.
Da die Punkte D2) und D3) eine besonders große Gefahr für das FH-Netz darstellen, müssen bei Verstößen sowohl die zuständige Systemadministratorin / der zuständige Systemadministrator als auch der Beauftragte für IT-Sicherheit bzw. den Leiter des ITC informiert werden.</td></tr>
</table>

D4	*Regelverstoß*	*Ansprechpartner*
	Vorsätzliche Verbreitung oder In-Umlauf-Bringen von schädlichen Programmen (z.B. **Viren**, "**Computer-Würmer**", "**Trojanische Pferde**").	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher** des Problems. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr eine schriftliche Kenntnisnahme. **und** Meldung an den **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de Fügen Sie der E-Mail die relevanten Auszüge aus Ihren Log-Dateien bei.
	Verbreitung oder In-Umlauf-Bringen von schädlichen Programmen (z.B. **Viren**programmen, "**Computerwürmer**", "**Trojanischen Pferden"**). Die genannten Programme bergen folgende Gefahren: 1. Datenbeschädigung 2. Zugriff für Unbefugte 3. Schädigung Dritter durch schnelle Ausbreitung 4. Imageverlust durch 1. bis 3. Diese Programme werden nicht durch einen gezielten Angriff gefährlich, sondern verbreiten sich quasi automatisch. Das ITC bietet eine entsprechende **Anti-Virus-Software** im Rahmen einer für FH-Angehörige kostenlosen Campuslizenz an. Informationen erhalten Sie im Web: URL: http://www.fh-wiesbaden.de/itc/	

D5	*Regelverstoß*	*Ansprechpartner*
	Ausspähen von Passwörtern oder auch der Versuch des Ausspähens (z.B. **"Passwort Sniffer"**)	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher** des Problems. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung. **und** Meldung an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de

D6	*Regelverstoß*	*Ansprechpartner*
	Unberechtigte Manipulation oder Fälschung von Identitätsinformationen (z.B. "Mailheader", elektronischer Verzeichnisse, **"IP-Spoofing"**, etc.).	Wenden Sie sich direkt an die **Verursacherin** / den **Verursacher** des Problems. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie die Unterlassung. **und** Meldung an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de
	Anmerkungen: Die Vorgabe einer falschen Identität verstößt gegen die Sicherheitsrichtlinie der FH Wiesbaden. Die Verwendung von Pseudonymen und die Wahl der Anonymität gelten nicht als Fälschung der Identität.	

D7	*Regelverstoß*	*Ansprechpartner*
	Ausnutzung erkannter Sicherheitsmängel bzw. administrativer Mängeln.	Wenden Sie sich direkt an den an die **Verursacherin** / den **Verursacher** des Problems. Klären Sie die betreffende Person darüber auf, dass sie gegen die Sicherheitsrichtlinie der FH Wiesbaden verstößt, und verlangen Sie von ihr eine schriftliche Kenntnisnahme. **und** Meldung an das **ITC** unter der E-Mail: abuse@itc.fh-wiesbaden.de
	Anmerkungen: Falls Ihnen als Benutzerin / Benutzer eines Computers Sicherheitsmängel auffallen, sind Sie verpflichtet, den Systemadministrator davon zu informieren und ihn zur Behebung derselben aufzufordern.	

Anmerkungen:

Die FH Wiesbaden dankt den Kollegen der HRZ der Technischen Universität Darmstadt und dessen Leiter für die Genehmigung die IT- Sicherheitsrichtlinie der TU Darmstadt als Basis der IT-Sicherheitsrichtlinie der FH-Wiesbaden verwenden zu dürfen.