Security Policy der TU Wien

Technische Universität Wien
Policy-Sammlung
Begriff: Sicherheit
Name: Security Policy
Autor: Udo Linauer
Organisationseinheit: ZID
Version: 01. September 2002
Überarbeitet von: Georg Gollmann

1. Überblick

Die Technische Universität Wien erwartet von den Benutzern der Computer und der Netze der Technischen Universität Wien verantwortungsbewussten Umgang bei deren Gebrauch. Als Reaktion auf Verstöße gegen die Security Policy oder gegen gesetzliche Bestimmungen sind die Technische Universität Wien und ihre Organisationseinheiten berechtigt, Benutzern Zugangsberechtigungen zeitweise oder auf Dauer zu entziehen, bei Bedarf Daten von Computern der Technischen Universität Wien zu löschen und Computer aus dem Netz zu entfernen. Bei Unklarheiten oder Streitfällen hat der Beauftragte für IT-Sicherheit am ZID, in zweiter Instanz der Leiter des ZID zu entscheiden.

2. Begründung

Die Technische Universität Wien möchte allen Benutzern effizientes und ungestörtes Arbeiten ermöglichen. Daher ist in der Security Policy eine Liste von nicht zulässigen Verhaltensweisen (regelwidrige Benutzung) festgelegt, deren Unterlassung jeder Benutzer einfordern kann, um sich vor Belästigungen und Bedrohungen zu schützen und in Folge die Technische Universität Wien und ihre Organisationseinheiten vor Schäden und rechtlichen Konsequenzen zu bewahren. Um den einwandfreien Betrieb zu gewährleisten werden in der Security Policy Standards für die Sicherheit von Computern, Netzen und Daten festgelegt. Es handelt sich dabei um Mindestanforderungen. Es bleibt demnach den Organisationseinheiten der Technischen Universität Wien überlassen, für bestimmte Bereiche schriftlich strengere Regeln festzulegen.

3. Gültigkeitsbereich

Die Security Policy ist verbindlich für alle Angehörigen der Technischen Universität Wien sowie Personen, denen durch Vereinbarungen die Benutzung von Computern und Netzen der Technischen Universität Wien möglich ist. Darüber hinaus gilt sie als Grundlage für Reaktionen bei Attacken von außerhalb.

4. Versionen

An dieser Stelle sind Überarbeitungen des Dokuments mit einer kurzen Zusammenfassung der Änderungen vermerkt. Die Policy ist alle zwei Jahre auf Aktualität zu überprüfen. Schwer wiegende Veränderungen der verwendeten Technologien oder organisatorischer Art können Überarbeitungen außerhalb dieses Intervalls bedingen.

Version 01.06.2000, Grundfassung, vom Rektor mit Gültigkeit vom 7. 6. 2000 erlassen.
Version 01.09.2002, Formatierung zur besseren Referenzierbarkeit überarbeitet.

5. Einleitung

Der Gebrauch von Computern und Netzen ist für die Angehörigen der Technischen Universität Wien zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtert er viele Tätigkeiten, manche Arbeiten wären gar nicht denkbar ohne den Einsatz von Computern. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer Benutzer verletzen. Die Technische Universität Wien verlangt daher von allen Benutzern sorgfältigen und verantwortungsvollen Umgang beim Gebrauch von Computern und Netzen.

Grundsätzlich bleibt es dem Ermessen jedes einzelnen Benutzers bzw. der Institute und Universitätseinrichtungen der Technischen Universität Wien überlassen, in welcher Art und Weise Computer und Netze verwendet werden. Dieser praktizierte Ansatz, der besagt, dass alles erlaubt ist, was nicht verboten ist, hat sich über die Jahre bewährt und soll beibehalten werden. Die Erfahrung der letzten Jahre hat aber deutlich gemacht, dass es zum Ersten einen allgemein anerkannten Konsens geben muss, welche

regelwidrige Benutzung

nicht akzeptiert wird und wie sie verhindert und geahndet werden kann, und zum Zweiten, welche

Mindeststandards für den Betrieb eines Computers

verbindlich sind. Zweck der Security Policy ist es, die beiden Themenkreise zu formalisieren und allen Benutzern eine einheitliche Grundlage zu bieten, anhand der entschieden werden kann, welche Benutzung konform ist.

Aufgrund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die Security Policy soll das Erkennen von Verstößen beschleunigt werden, um den Schaden für jeden Einzelnen und die Technische Universität Wien gering zu halten. Damit verringert sich auch die Wahrscheinlichkeit, dass Verstöße ohne Konsequenzen bleiben.

Die Technische Universität Wien führt kein generelles Monitoring von Benutzern oder Daten durch und ist darauf angewiesen, dass die Benutzer Mängel entweder auf Institutsebene selbst beheben oder dem ZID melden.

Eine vom ZID herausgegebene komplette Liste der Kontaktadressen sowie Erläuterungen zu den in der Security Policy behandelten Themen ist im Dokument Die Security Policy der TU Wien - HOWTO? zu finden. Dieses Dokument wird laufend am aktuellen Stand gehalten.

6. Regelwidrige Benutzung

Die in der Security Policy festgelegten Regelverstöße sind thematisch in vier Bereiche gegliedert (siehe die ausführliche Beschreibung in tabellarischer Form im Dokument Die Security Policy der TU Wien - HOWTO?)

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

A1) Verbreitung oder In-Umlauf-Bringen von Informationen, die Herabwürdigungen oder Beleidigungen von Personen aufgrund ihrer Hautfarbe, Nationalität, Religion, ihres Geschlechtes, ihrer politischen Gesinnung oder sexuellen Ausrichtung beinhalten.

A2) Verbreitung von persönlichen oder anderen schützenswerten Informationen über eine Einzelperson oder eine Gruppe von Personen.

A3) Wiederholtes und unerwünschtes Zusenden von Nachrichten.

B. Verwendung elektronischer Kommunikation zur Behinderung der Arbeit Dritter

B1) Behinderung der Arbeit anderer durch Mailbomben und ähnliche Techniken.

B2) Aneignung von Ressourcen über das zugestandene Maß.

B3) Versenden von elektronischen Massensendungen (Spam E-Mails). Ausnahme: Verbreitung von dienstlichen Mitteilungen in Analogie zur Hauspost.

B4) Weitersenden oder In-Umlauf-Bringen von elektronischen Kettenbriefen.

B5) Manipulation von elektronischen Daten.

B6) Zugriff auf Daten Dritter ohne deren explizite Erlaubnis.

C. Vergehen gegen Lizenzvereinbarungen oder andere Vertragsbestimmungen

C1) Kopieren und Verbreiten auf Computer der TU Wien bzw. der Transport über Netze der TU Wien von urheberrechtlich geschütztem Material im Widerspruch zu Lizenzvereinbarungen oder anderen Vertragsbestimmungen.

C2) Weitergabe von Zugangsberechtigungen, entgeltlich oder unentgeltlich, an Dritte, außer wenn diese durch Vereinbarungen abgedeckt ist.

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

D1) Portscans (Automatisiertes Ausforschen von Servern und Services). Ausnahme: Sicherheitstests nach Absprache mit dem Systemadministrator.

D2) Unerlaubte Aneignung von Ressourcen oder der Versuch einer solchen Aneignung (Hacken). Ausnahme: Sicherheitstests nach Absprache mit dem Systemadministrator. (**Meldepflicht von Verstößen an den ZID !**)

D3) Beschädigung oder Störung von elektronischen Diensten (Denial of service attacks). (**Meldepflicht von Verstößen an den ZID !**)

D4) Verbreitung oder In-Umlauf-Bringen von Virenprogrammen, Computer worms, Trojanischen Pferden oder anderen schädlichen Programmen.

D5) Ausspähen von Passwörtern oder auch der Versuch des Ausspähens (z.B. Passwort Sniffer).

D6) Manipulation oder Fälschung von Mailheaders, elektronischer Verzeichnisse oder anderer elektronischer Information, insbesondere Vorgabe einer falschen Identität (auch IP-Spoofing etc.).
Ausnahme: Verwendung von Network Address Translation (NAT) oder ähnlicher Technologien beim Einsatz einer Firewall.

D7) Ausnützung von erkannten Sicherheitsmängeln bzw. administrativen Mängeln.

7. Anforderungen für den Betrieb eines Computers

Um den ordnungsgemäßen Betrieb eines Computers oder einer aktiven Netzkomponente zu gewährleisten, müssen zumindest folgende Punkte erfüllt sein.

1. Fachgerechte Installation
2. Installation notwendiger Patches, vor allem von Security-Patches
3. Durchführen notwendiger Upgrades
4. Regelmäßige Änderung von Passwörtern. Wahl sicherer Passwörter oder stärkerer Authentifizierungsmethoden (z.B. Public Key). Regelmäßige Überprüfung der existierenden Accounts auf Aktualität (zumindest am Semesterende).
5. Unverzügliche Bekanntgabe an den ZID von Personaländerungen bei der Systemadministration.
6. Womöglich die Bereitstellung eines sicheren Logins ohne Klartextpasswörter (bei Fernwartung verpflichtend).

Ad 1.-4.)
Bei nicht entsprechender Wartung kann ein Computer den Betrieb von Teilen des TUNET gefährden (z.B. Hacker, Mail relaying). Beratung und Hilfestellung leistet der ZID, Abteilung Standardsoftware.

Ad 5.)
Der ZID stellt mit der TUNET-Datenbank und dem zugehörigen Webinterface ein einfach zu bedienendes Werkzeug zur

Bekanntgabe von Änderungen bei der Systemadministration und zum Auffinden verantwortlicher Systemadministratoren zur Verfügung. Personaländerungen müssen per E-Mail an den ZID, Abteilung Kommunikation bekannt gegeben werden.

Die Kenntnis des Systemadministrators ist wichtig, weil bei Attacken (z.B. Hacker) die schnelle Kontaktaufnahme unumgänglich ist. Außerdem können gewisse Services wie z.B. die Sicherheitsüberprüfung eines Computers nur auf Anfrage des Systemadministrators bzw. des Institutsvorstandes oder des Leiters einer Universitätseinrichtung geleistet werden.

Systemadministratoren können sich bei Fragen zum Betrieb eines Computers an den ZID, Abteilung Standardsoftware wenden, bei Fragen zu aktiven Netzkomponenten an die Abteilung Kommunikation.

Falls einem Benutzer eines Computers Sicherheitsmängel auffallen, ist er verpflichtet, den Systemadministrator davon zu informieren und ihn zur Behebung derselben aufzufordern.

8. Konsequenzen bei Nichteinhaltung der Policy

Die meisten Verstöße resultieren erfahrungsgemäß aus Unkenntnis der Security Policy oder technischer Unzulänglichkeit. In solchen Fällen wird es ausreichen, wenn der Verursacher über den Verstoß gegen die Security Policy der TU Wien aufgeklärt und die Unterlassung weiterer Verstöße gefordert wird. Bei Verstößen gegen die Netiquette oder gegen Lizenzvereinbarungen muss gegebenenfalls die Löschung von Daten von Servern verlangt werden. Wenn anzunehmen ist, dass erkannte Verstöße auch andere Institute, Universitätseinrichtungen oder Organisationen (auch außerhalb der TU Wien) betreffen könnten, sind die betreffenden Systemadministratoren und eventuell auch der ZID zu informieren (z.B. Sperre eines Benutzers, der auch über Zugangsberechtigungen auf anderen Computern verfügt).

Falls die direkte Aufforderung ohne Erfolg bleibt oder die Identität des Verursachers nicht festgestellt werden kann, ist der ZID in die Lösung des Problems miteinzubeziehen. Der Kontakt mit dem ZID sollte am besten über die dafür vorgesehene E-Mail-Adresse hergestellt werden (siehe Dokument Die Security Policy der TU Wien - HOWTO?). Neben der Beschreibung des Problems sollte immer explizit angeführt werden, gegen welchen Punkt der Security Policy verstoßen wurde. Bei Uneinigkeit über die Richtigkeit der Beschwerde entscheidet der **Beauftragte für IT-Sicherheit**, in zweiter Instanz der **Leiter des ZID**.

Maßnahmen durch den ZID

1. Der ZID wird den **Netz- oder Systemadministrator** des Computers (Netzes), von dem die Attacken ausgehen, auffordern, Regelverstöße zu unterbinden, gegebenenfalls die Zugangsberechtigung des Verursachers zu sperren sowie bei Verstößen gegen die Netiquette oder gegen Lizenzvereinbarungen die betreffenden Informationen von Servern zu löschen.

2. Ist der Systemadministrator des betreffenden Computers nicht erreichbar oder nicht imstande bzw. nicht bereit, solche Verstöße zu verhindern, so ist der ZID verpflichtet, den **Institutsvorstand** bzw. den **Leiter der Universitätseinrichtung** von den Missständen zu informieren und ihn zur Behebung derselben aufzufordern.

3. Bleibt auch die Maßnahme in Punkt 2. ohne Erfolg, so ist der ZID verpflichtet, den betreffenden Computer aus dem Netz zu entfernen bzw. die betreffenden Services zu sperren.

4. Wenn die Umstände es verlangen (**Gefahr in Verzug**), können Sperren vom ZID auch ohne Rücksprache mit den Systemadministratoren vollzogen werden. Der ZID ist in solchen Fällen verpflichtet, die betroffenen Systemadministratoren und den Institutsvorstand bzw. den Leiter der Universitätseinrichtung **unmittelbar** über die getroffenen Maßnahmen zu informieren.

5. Zusätzlich kann vom Verursacher die schriftliche Zurkenntnisnahme der Policy verlangt werden (Musterprotokoll im Dokument Die Security Policy der TU Wien - HOWTO?).

9. Definitionen

aktive Netzkomponente	Router, Switch etc.
Benutzer	Endbenutzer

elektronische Kommunikation	Verwendung von Computern, Netzen (TUNET, Telefon etc.) und deren Services.
Netze	Alle Kommunikationsnetze (z.B. TUNET, Telefonnetz)
Service	Jedes Service, das vom ZID zur Verfügung gestellt oder weitergeleitet wird.
Systemadministrator	In der TUNET-Datenbank als technische Kontaktperson eingetragene, für den ordnungsgemäßen Betrieb eines Computers oder einer Netzkomponente verantwortliche Person.
TUNET	Netz-, Kommunikations- und Rechnerinfrastruktur für die Informations- und Datenverarbeitung.
TU Wien	Technische Universität Wien mit ihren Organisationseinheiten und eventuell angegliederten Forschungsinstituten und interuniversitären Einrichtungen.
Verwendung	Anwendung eines vom ZID zur Verfügung gestellten Services sowie der Kommunikationseinrichtungen (z.B. Leitungen, Geräte) des ZID (egal ob betrieben, gemietet oder in dessen Eigentum), der vom ZID betriebenen oder gewarteten Software und aller Informationen, die verfügbar gemacht werden.
ZID	Zentraler Informatikdienst