Security-Policy der BOKU

Die Security-Policy regelt die Grundlagen für die Sicherheit des IT-Betriebs an der BOKU.

Hier finden Sie die derzeit formell gültige, aus dem Jahr 2001 stammende Version. Eine neue Version ist für die nähere Zukunft geplant.

Zielgruppe der Dokumentation:	Mitarbeiter/innen, Forscher/innen, Studierende
Anfragen:	hotline@boku.ac.at

Inhaltsverzeichnis

Security Policy der BOKU

Dienstanweisung des Rektors nach Anhörung des Universitätskollegiums am 12. Dezember 2001

1 Überblick

Die Universität für Bodenkultur Wien (BOKU) erwartet von den Benutzern der Computer und der Netze der BOKU verantwortungsbewussten Umgang bei deren Gebrauch. Als Reaktion auf Verstöße gegen die Security Policy oder gegen gesetzliche Bestimmungen sind die BOKU und ihre Organisationseinheiten berechtigt, Benutzern Zugangsberechtigungen zeitweise oder auf Dauer zu entziehen, bei Bedarf Daten von Computern der BOKU zu löschen und Computer aus dem Netz zu entfernen. Bei Unklarheiten oder Streitfällen hat der Direktor der BOKU-IT zu entscheiden.

2 Begründung

Die BOKU 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 BOKU 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 BOKU überlassen, für bestimmte Bereiche schriftlich "strengere" Regeln festzulegen.

3 Gültigkeitsbereich

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

Die rechtlichen Grundlagen dafür sind die Betriebs- und Benutzungsordnung der BOKU-IT und die einschlägigen Gesetze.

4 Einleitung

Der Gebrauch von Computern und Netzen ist für die Angehörigen der BOKU 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 BOKU verlangt daher von allen Benutzern sorgfältigen und verantwortungsvollen Umgang beim Gebrauch von Computern und Netzen.

- 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 derer 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 BOKU gering zu halten. Damit verringert sich auch die Wahrscheinlichkeit, dass Verstöße ohne Konsequenzen bleiben.

Die BOKU führt kein generelles Monitoring von Benutzern oder Daten durch und ist darauf angewiesen, dass die Benutzer Mängel entweder auf Institutsebene selbst beheben oder der BOKU-IT melden.

Eine von der BOKU-IT herausgegebene Liste der Kontaktadressen sowie Erläuterungen zu den in der Security Policy behandelten Themen sind in den Security-Web-Pages der BOKU-IT zu finden. Diese Informationen werden von der BOKU-IT laufend am aktuellen Stand gehalten.

Die in der Security Policy festgelegten Regelverstöße sind thematisch in vier Bereiche gegliedert

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 BOKU bzw. der Transport über Netze der BOKU 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 im eigenen Verantwortungsbereich oder durch die BOKU-IT.

D2) Unerlaubte Aneignung von Ressourcen oder der Versuch einer solchen Aneignung (Hacken). Ausnahme: Sicherheitstests im eigenen Verantwortungsbereich oder durch die BOKU-IT. (Meldepflicht von Verstößen an die BOKU-IT!)

D3) Beschädigung oder Störung von elektronischen Diensten (Denial of service attacks). (Meldepflicht von Verstößen an die BOKU-IT!)

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 (Passwort Sniffer).

5 Anforderungen für den Betrieb eines Computers oder einer Netzkomponente

Vor der Inbetriebnahme eines Computers, auf dem **Server**-Dienste laufen, oder einer aktiven Netzkomponente, sowie **vor** jeder Inbetriebnahme von neuen oder zusätzlichen Server-Diensten oder aktiven Netzkomponenten, muss dies bei der BOKU-IT beantragt werden und die Bewilligung der BOKU-IT abgewartet werden. Die BOKU-IT hat diese Bewilligung zu erteilen, wenn

a) dieses Netz-Service in der vorgesehenen Form technisch sinnvoll ist und

b) keine Gefahr für die IT-Sicherheit der BOKU darstellt, und wenn

c) der BOKU-IT bekannt gegeben wird, welche Person als Systemadministrator für den Betrieb und die Sicherheit dieses Servers bzw. dieser Netzkomponente zuständig ist und wie diese Person oder ihr Stellvertreter von der BOKU-IT bei Bedarf kurzfristig erreicht werden kann.

Ad a) Um unnötige Sicherheitsrisiken zu vermeiden, sollen so weit wie möglich dezentrale Server- und Netz-Dienste vermieden und stattdessen die von der BOKU-IT betriebenen und abgesicherten zentralen Server und Netzkomponenten verwendet werden.

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 die BOKU-IT 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 BokuNet gefährden (z.B. Hacker, Mail relaying). Beratung und Hilfestellung leistet die BOKU-IT.

Ad 5.) Personaländerungen, die den Systemadmistrator oder dessen Stellvertreter betreffen, müssen per E-Mail an die BOKU-IT bekannt gegeben werden. Die Kenntnis des Systemadministrators ist wichtig, weil bei Attacken (z.B. Hacker) die schnelle Kontaktaufnahme unumgänglich ist.

Systemadministratoren können sich bei Fragen zum Betrieb eines Computers an die BOKU-IT wenden.

Falls der Server oder die Netzkomponente nicht von der BOKU-IT bewilligt wurde oder falls die für den sicheren Betrieb eines Servers bzw. Netz-Dienstes notwendigen Punkte nicht mehr vollständig erfüllt werden oder werden können, müssen unverzüglich alle Server-Dienste **abgedreht** oder der Computer bzw. die Netzkomponente komplett **vom Netz genommen** werden.

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

6 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 BOKU 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 BOKU) betreffen könnten, sind die betreffenden Systemadministratoren und die BOKU-IT 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 die BOKU-IT in die Lösung des Problems einzubeziehen. Der

Kontakt mit der BOKU-IT sollte am besten über die dafür vorgesehene E-Mail-Adresse hergestellt werden (siehe die Security-Web-Pages der BOKU-IT). 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 **Direktor der BOKU-IT**.

Maßnahmen durch die BOKU-IT

1. Die BOKU-IT 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 oder gegen Gesetze - 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 die BOKU-IT verpflichtet, den **Institutsvorstand** bzw. den **Leiter** der Universitätseinrichtung von den Missständen zu informieren und ihn zur Behebung derselben aufzufordern.

3. Bleibt auch diese Maßnahme ohne Erfolg, so ist die BOKU-IT verpflichtet, den betreffenden Rechner aus dem Netz zu entfernen bzw. die betreffenden Services zu sperren. Falls die BOKU-IT keinen Zugriff auf den einzelnen Rechner erhält, kann er statt dessen den gesamten Netzteil, in dem sich der den Netzbetrieb störende Computer befindet, vom Netz abklemmen.

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

5. Zusätzlich kann vom Verursacher die schriftliche Zurkenntnisnahme der Policy verlangt werden.

7 Definitionen

aktive Netzkomponente	Router, Switch, Access Point etc.
Benutzer	Endbenutzer
BOKU	Die Universität für Bodenkultur mit ihren Organisationseinheiten und eventuell angegliederten Forschungsinstituten und interuniversitären Einrichtungen.
BokuNet	Netz-, Kommunikations- und Rechnerinfrastruktur für die Informations- und Datenverarbeitung innerhalb der BOKU.
elektronische Kommunikation	Verwendung von Computern, Netzen (BokuNet, Internet) und deren Services.
Netze	Alle Kommunikationsnetze (z.B. BokuNet, Modem-Anschlüsse, Internet)
Server	Jede Computer-Anwendung, die von anderen Computern innerhalb oder außerhalb der BOKU angesprochen werden kann. Dazu zählen z.B. Web-Server, Mail-Server, FTP-Server und dergleichen. File-Sharing Freigaben zählen nur dann dazu, wenn sie einen Zugriff von außerhalb des BokuNet ermöglichen. Nicht dazu zählen reine Client-Anwendungen wie Web-Browser (Netscape), Mail-Clients (Pegasus Mail) und dergleichen.
Service	Jedes Service, das von der BOKU-IT zur Verfügung gestellt oder weitergeleitet wird.
Systemadministrator	Für den ordnungsgemäßen Betrieb eines Computers oder einer Netzkomponente verantwortliche Person.
Verwendung	Anwendung eines von der BOKU-IT zur Verfügung gestellten Services sowie der Kommunikationseinrichtungen (z.B. Leitungen, Geräte) der BOKU-IT (egal ob betrieben, gemietet oder in dessen Eigentum), der von der BOKU-IT betriebenen oder gewarteten Software und aller Informationen, die verfügbar gemacht werden.
BOKU-IT	Informatikdienst der BOKU

Historie

Letzte Änderung: 23. Jänner 2020

Die **aktuelle Version** dieser Dokumentation finden Sie auf den Serviceseiten der BOKU-IT unter:
http://short.boku.ac.at/it-guidelines

Dokument		**Security-Policy**	SecurityPolicy_DE_V.1.0.1_2014-02-20.docx
Quelldokument		BOKU	---
Aktualisierungs-datum/ Autor	**Version**	**Änderungen**	
2014-02-20 (HP/ZID)	1.0.0.	Originaltext aus dem Jahr 2001	
2020-01-23 (AST/BOKU-IT)	1.0.1	Umbenennung ZID in BOKU-IT	