BEILAGE 1
zum Mitteilungsblatt
4. Stück - 2007/2008
21.11.2007

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT

IT - Sicherheitsrichtlinie

Kontext/Inhaltsverzeichnis	IT-Sicherheitsrichtlinie der Alpen-Adria Universität Klagenfurt; Basisschutz für alle Universitätsangehörigen
Verantwortliche(r)	Dipl.-Ing. Hermann Maier, DW 9601
Arbeitsgruppe	Mag. Michael Menard, DW 9621 Armin Ploner, DW 9611 Fa. SnT, Mag. Josef Villa, Ing. Roman Gruber
Datum	30. September 2007
Version	1.9
Chronologie	1.0 Ersterstellung, R. Gruber, J.Villa (9.11.2006) 1.3 Komplettierung/Überarbeitung, J. Villa (22.11.2006) 1.5 Endredaktion, Draft, J. Villa (7.12.2006) 1.6 Einarbeitung des Feedback des Präsentationsworkshops (18.12) 1.7 Einarbeitung des Feedback nach letzter Aussendung (13.2.2007) 1.8 Einarbeitung Feedback Datenschutzbeauftragter und Betriebsrat (26.2.2007) 1.9 Final Version (16.3.2007) 2.0 Revised Final Version (Korrekte Schreibweise geschlechtsspezifischer Bezeichnungen; eine Korrektur nach Feedback der Informatikinstitute) 2.1 Verabschiedung im Rektorat (30.10.2007)
Internet	www.uni-klu.ac.at/ORGhandbuch

Inhaltsverzeichnis

1 IT-Sicherheitsrichtlinie der Alpen-Adria-Universität Klagenfurt

1.1 Einleitung

Die Sicherheit von Daten und Transaktionen stellt eine unverzichtbare Grundlage für alle Organisationseinheiten der Universität dar.

Dieses Dokument beschreibt die grundlegenden Richtlinien für die IT-Sicherheit der Universität und hat bindenden Charakter. Im Fällen von unterschiedlicher Interpretation entscheidet das Rektorat.

Die Verantwortung für die Umsetzung und Einhaltung ist Teil der Führungsaufgabe der Führungskräfte der Universität.

Die Grundzüge der IT-Sicherheitsrichtline der Universität sind:

- Die Universität versteht sich als öffentlicher Raum.
- Die IT-Sicherheitsrichtlinie soll eine weitest gehend liberale Nutzung der Infrastruktur innerhalb klar gezogener Grenzen zulassen.
- Die Universität bekennt sich zu den gesetzlichen Verpflichtungen bezüglich des Datenschutzes insbesondere des Datenschutzgesetzes 2000 und zu den dort genannten Prinzipien.
- Die IT-Sicherheitsrichtlinie stellt die Balance zwischen Produktivität und notwendiger sicherheitstechnischer Einschränkung her und versteht sich als Mindeststandard.
- Die Universität ist bestrebt, die Einhaltung von Sicherheitsstandards durch technische Verfahren zu unterstützen, vertraut aber auch auf Unterstützung der Mitarbeiterinnen und Mitarbeiter, dass durch die konsequente Umsetzung dieser Sicherheitsrichtlinien die gesteckten Sicherheitsziele erreicht werden.

1.2 Ziele

Das Ziel dieser Richtlinie ist es,

- Daten und Werte vor unbefugten Zugriffen, Veränderungen und vor Verlust zu schützen.
- den Datenschutz zu verbessern und die gesetzlichen Sicherheitsmaßnahmen zu gewährleisten
- die Kontinuität der Systemnutzung sicherzustellen
- sicherzustellen, dass den Benutzerinnen und Benutzern die Daten, die sie zur Erfüllung ihrer Aufgaben benötigen, in einem sicheren Systemumfeld zur Verfügung gestellt werden
- ein umfassendes Sicherheitsbewusstsein zu entwickeln und danach zu handeln.

1.3 Geltungsbereich

Diese IT-Sicherheitsrichtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter, emeritierte Professorinnen und Professoren, Pensionistinnen und Pensionisten, sowie für Personen, die in einem atypischen Beschäftigungsverhältnis zur Universität stehen, für alle Studierenden und Alumni der Universität sowie für Personen, die in oder für universitätsnahe Organisationen tätig sind und direkt oder indirekt mit dem IT-System der Universität in Berührung kommen. Auftragnehmerinnen/Auftragnehmern sind die jeweils relevanten Punkte durch Vereinbarungen zu überbinden.

2 Organisatorischer Rahmen

Die Universität richtet die zentrale Funktion eines IT-Security Officers ein, der/die bereichsübergreifend die Implementierung, Kontrolle und Weiterentwicklung der IT-Sicherheit koordiniert und entwickelt.

Dessen Aufgaben sind insbesondere:

- Weiterentwicklung dieser IT-Sicherheitsrichtlinie aufgrund neuer Bedrohungen
- Festlegung und Initiierung von spezifizierenden Dokumenten und Definitionen von Standards zur IT-Sicherheit
- Verantwortliche Mitwirkung an der Realisierung von IT-Sicherheitsmaßnahmen
- Analyse und Bewertung von Informationssicherheitsvorfällen und Ableitung daraus resultierender Maßnahmen
- Definition, Planung und Durchführung von Audits
- Initiativen zur Förderung des Sicherheitsbewusstseins der Mitarbeiterinnen und der Mitarbeiter
- Beratung in sicherheitsrelevanten Fragen

3 Klassifikationen

Die Klassifikation von Daten und Netzwerksegmenten dient der Spezifikation von adäquaten Sicherheitsmaßnahmen in Abhängigkeit von unterschiedlichen Schutzbedürfnissen, Vertraulichkeitsstufen, Bedrohungsszenarios und Schadensauswirkungen.

3.1 Datenklassifizierung

Daten werden in folgenden Klassen zugeteilt:

- *Geheim* – Die Daten stehen unter rechtlichem Geheimhaltungsschutz und unterliegen der Amtsverschwiegenheit.
- *Vertraulich* – Die Daten stehen einem bestimmten Personenkreis zur Verfügung und unterliegen Beschränkungen hinsichtlich Zugriffsrechten, Verarbeitung und Weitergabe.
- *Eingeschränkt* – Daten, die innerhalb einer Organisationseinheit der Universität keinen Beschränkungen unterliegen. Außerhalb dieser Organisationseinheit bestehen jedoch Beschränkungen hinsichtlich Zugriffsrechten, Verarbeitung und Weitergabe.
- *Offen* – alle Daten, die ohne Einschränkungen verwendet werden dürfen.

Die Einordnung von Daten in eine Klasse erfolgt durch Beurteilung der Vertraulichkeit der Daten, des Wertes für die Universität, des Aufwandes für eine Wiederbeschaffung nach Verlust und nach eventuellen gesetzlichen Bestimmungen, die einen besonderen Schutz erfordern.

Die Datenklassifizierung nimmt die jeweilige Organisationseinheit unter methodischer Anleitung des ZID vor.

Werden Daten, die als geheim oder vertraulich eingestuft wurden, an Dritte im Rahmen einer Kooperation oder eines Projektes übergeben bzw. ausgetauscht, so ist mit diesem Partner eine Vertraulichkeitserklärung abzuschliessen, bevor diese Daten übergeben werden. Werden geheime oder vertrauliche Daten auf mobile Datenträger kopiert, sind diese dort verschlüsselt zu speichern.

Datenträger (z.B. Disketten, Festplatten, CDROMs, USB Devices), die ausgeschieden werden, müssen an der zentralen Stelle für Entsorgung abgegeben werden, die für eine ordnungsgemäße Vernichtung der Daten - unabhängig von der Schutzklasse - sorgt.

3.2 Netzwerkinfrastruktur

Die Richtlinien zur Netzwerkinfrastruktur definieren die Voraussetzungen, unter denen Geräte mit dem Netzwerk der Universität verbunden werden dürfen und welche Abstufungen hinsichtlich der Sicherheitsmerkmale bestehen. Diese Regelungen gelten gleichermaßen für kabelgebundene wie auch für drahtlose Netzwerkanbindungen.

Das Netzwerk der Universität wird hinsichtlich der Zugängigkeit von Netzwerkanschlüssen in einen öffentlichen, einen Instituts-/Dienstleistungsbereich und einen internen Verwaltungsbereich unterteilt:

- Als interner Verwaltungsbereich gelten alle Netzwerkanschlüsse in Räumlichkeiten, die Organisationseinheiten der Universitätsleitung und der Universitätsadministration zugeordnet und nicht öffentlich sind.
- Als Instituts- bzw. Dienstleistungsbereich gelten alle Netzwerkanschlüsse in Räumlichkeiten, die Organisationseinheiten der Universität zugeordnet sind, nicht zum internen Verwaltungsbereich zählen und nicht öffentlich sind.
- Als öffentlicher Bereich gelten alle Netzwerkanschlüsse in allgemein zugänglichen Räumlichkeiten (Hörsäle, Seminarraume, Schulungsräume, Sitzungsräume, Aufenthaltsbereiche, Gänge, Stiegenhäuser, Außenbereiche am Campus udgl.)

Die Zuständigkeit und Verantwortung für die Netzwerkinfrastruktur liegt grundsätzlich beim ZID.

Im öffentlichen und Instituts-/Dienstleistungsbereich bestehen neben dem ZID weitere technische Administrationen (einzelne Institute, Forschungsgruppen udgl.) Die Verantwortlichen dieser Administrationen haben sicherzustellen, dass dort die Qualität des Sicherheitsniveaus der IT-Sicherheitsrichtlinie nicht unterschritten wird.

Sind öffentliche Netzwerk-Anschlüsse im internen Verwaltungs-, Instituts- oder Dienstleistungsbereich notwendig, so sind diese als „öffentlich“ zu kennzeichnen.

Das Netzwerk der Universität ist in Zonen mit unterschiedlichen Sicherheitsmerkmalen unterteilt. Hinsichtlich der Sicherheitsmerkmale existieren folgende Zonen:

- Zonen mit hoher Sicherheitsstufe – alle Bereiche mit hohem Schutzbedarf, die zwingend mit Schutzmechanismen wie Firewalls, Intrusion Detection Systemen u ä. geschützt sind.
- Zonen mit mittlerer Sicherheitsstufe – geschützte Bereiche aus denen öffentliche Dienste angeboten werden, die durch Firewalls geschützt sind und in die nur definierte Zugriffsprotokolle zulässig sind
- Zonen mit geringer Sicherheitsstufe – alle Bereiche mit geringem Schutzbedarf

Ungeschützte Netzwerkbereiche außerhalb des Netzwerkes der Universität gelten als unsicher und nicht vertrauenswürdig.

Für jede Zone ist mindestens ein befugter Administrationsverantwortlicher/eine befugte Administrationsverantwortliche zu benennen

IP-Adressen und andere Netzwerkkennungen werden grundsätzlich nur vom ZID vergeben. Der ZID kann jedoch für gewisse Teilbereiche die Vergabe an andere Administrationsstellen delegieren. Für IP-Adressen muss nachvollziehbar sein - außer wenn Benutzbarkeitsüberlegungen oder ein übermäßiger technischer Aufwand entgegenstehen - wer oder zumindest welches Gerät zu einer bestimmten Zeit diese IP-Adresse innehatte.

Die Aufnahme und Einführung neuer Dienste und Protokolle am Netzwerk bedarf der Genehmigung des ZID. Jede Form der Störung des regulären Betriebes – dazu zählt auch übermäßige Nutzung von Ressourcen – ist zu vermeiden. Diese Verantwortung trifft jede Benutzerin und jeden Benutzer im Rahmen des von ihr oder ihm wahrgenommenen Aufgabenbereichs.

Der Anschluss und die Inbetriebnahme von funkbasierten Netzwerken (z.B. WLAN Access Point) sind ohne Zustimmung des ZID untersagt.

Das Herstellen von Netzwerkverbindungen außerhalb der dafür vorgesehenen Infrastruktur ist untersagt. Dies betrifft insbesondere Netzverbindungen nach außen, die gleichzeitig mit der

Verbindung in das Netzwerk der Universität bestehen. Netzwerkverbindungen, die Sicherheitszonen überbrücken, sind untersagt.

Vom ZID ist eine Sicherheitsarchitektur einzurichten, damit keine unverschlüsselten direkten Verbindungen aus einer Zone mit geringerer Sicherheitsstufe in eine Zone mit höherer Sicherheitsstufe aufgebaut werden können. Ausgenommen sind nur jene, die zur Bereitstellung der Dienste und Funktionen notwendig sind.

Verschlüsselte Netzwerkverbindungen (z.B. Virtual Private Networks, VPN) aus und in das Netzwerk der Universität und andere Topologie verändernde Verbindungen (z.B definitionsfremde Verwendung von TCP-Ports) sind in besonderem Maße sicherheitsrelevant. Deshalb ist es zwingend erforderlich, dass vor Inbetriebnahme solcher Verbindungen die Zustimmung des ZID bezüglich des geplanten Verfahrens eingeholt wird.

3.2.1 Öffentlicher Bereich

Der öffentliche Bereich ist als Kommunikationsraum mit den geringsten Sicherheitsmaßnahmen konzipiert und dient in erster Linie der Kommunikation im Bereich der Lehre, im Internet, für Informationsterminals, Selbstbedienungsstationen u. ä.

Der Anschluss von Fremdgeräten darf nur an als aktiv gekennzeichneten Netzwerkanschlüssen vorgenommen werden. Angeschlossene Systeme (Kioske) dürfen nicht vom Netzwerk entfernt und der Anschluss anderweitig verwendet werden.

Aus dem öffentlichen Bereich dürfen ausnahmslos keine unverschlüsselten Netzwerkverbindungen in Zonen mit hoher Sicherheitsstufe aufgebaut werden können.

Die Kommunikation erfolgt grundsätzlich nur nach erfolgreicher Authentifizierung. Ausnahmen sind Informationsterminals oder Recherche-Systeme in den Lesesälen der Bibliothek.

3.2.2 Instituts- und Dienstleistungsbereich

Der Instituts- und Dienstleistungsbereich dient in erster Linie als Kommunikationsbereich zu Forschungs-, Lehr- und Informationszwecken.

Alle Anschlüsse des Instituts- und Dienstleistungsbereichs dürfen nicht der Zone mit geringer Sicherheitsstufe angehören.

Werden von einzelnen Organisationseinheiten eigene IT-Administrationen eingerichtet, dann liegt die Sicherheit der angeschlossenen Systeme in der Verantwortung des Leiters/der Leiterin der betroffenen Organisationseinheit. Unabhängig davon gilt auch in diesem Fall die IT-Sicherheitsrichtlinie. Ausnahmen müssen über die Bestimmungen zum Verfahren für eine Ausnahmeregelung (Kapitel 10) durchgeführt werden.

3.2.3 Interner Verwaltungsbereich

Der Anschluss von nicht zertifizierten Geräten (siehe Kapitel 4) im internen Verwaltungsbereich ist untersagt. Alle Geräte müssen vollständig den ZID Vorgaben entsprechen.

Alle Anschlüsse des internen Verwaltungsbereiches müssen der Zone mit hoher Sicherheit angehören.

Für den optimalen Schutz der Daten muss im internen Verwaltungsbereich eine 2-Faktor Authentifizierung zum Einsatz[1] kommen.

[1] Die Einführung einer 2-Faktor Authentifizierung befindet sich noch in der Planungs- und Evaluierungsphase durch den ZID. Eine 2-Faktor Authentifizierung erfolgt durch eine Chipkarte mit PIN und ersetzt das Verfahren mit Username und Password.

Im internen Verwaltungsbereich darf nur zentral bereitgestellte Software installiert und verwendet werden.

4 Richtlinien für Endbenutzer/Endbenutzerinnen und Endgeräte

Es ist die Aufgabe des ZID, die entsprechenden Beschaffungsvorgänge für Hardware und Lizenzen unter dem Gesichtspunkt einer Standardisierung vorzubereiten und die jeweils festgelegten Komponenten dieser Standardkonfigurationen im Intranet zu veröffentlichen. Der interne Verwaltungsbereich und die Instituts- und Dienstleistungsbereiche sind verpflichtet, diese Geräte-Standardisierung umzusetzen.

Die installierten Schutzmaßnahmen am Endgerät dürfen weder deaktiviert noch in ihrer Wirkung eingeschränkt werden. Insbesondere ist der Virenschutz aktuell zu halten.

Automatisierte Verfahren zur Aktualisierung und Verteilung von sicherheitsrelevanten Aktualisierungen von Software, insbesondere Komponenten des Betriebssystems, dürfen weder behindert, abgebrochen noch deaktiviert werden. Abbrüche bedingt durch eine Fehlersituation sind als Störungen zu qualifizieren und es ist das vorgesehene Verfahren der Störungsmeldung einzuleiten.

Erkennbare sicherheitsrelevante Einstellungen insbesondere im Betriebssystem, Internetbrowser, Mail-Client, Virenschutz, Bildschirmsperre und Firewalls dürfen nicht verändert werden.

Mobile Systeme, die in ungeschützten Bereichen außerhalb der Universität eingesetzt werden und die im internen Verwaltungs- oder Instituts-/Dienstleistungsbereich zum Einsatz kommen, bedürfen einer mindestens einmal pro Jahr durchzuführenden Sicherheitskontrolle (Zertifizierung) durch den ZID bzw. durch andere Prüfungsstellen nach Vorgaben des ZID. Die Verantwortung für die Durchführung dieser Überprüfung liegt beim Benutzer/bei der Benutzerin des Systems.

Die Standortveränderung von Endgeräten, das Öffnen und selbstständige Verändern der Hardware durch den Endbenutzer/die Endbenutzerin ist nicht gestattet. Diese Tätigkeiten dürfen ausschließlich durch befugtes, qualifiziertes IT-Personal durchgeführt werden.

Bei Verlust oder Diebstahl eines Endgerätes ist der/die Vorgesetzte zu informieren, eine polizeiliche Meldung vorzunehmen und die zentrale Inventarisierungsstelle zu informieren.

Bei Abwesenheit vom Computerarbeitsplatz, muss ein unberechtigter Zugriff auf Daten durch eine automatische Bildschirmsperre verhindert werden (z.B. passwortgeschützter Bildschirmschoner).

Benutzer und Benutzerinnen sind verpflichtet, qualitätsvolle Passwörter zu wählen. Die Weitergabe von persönlichen Passwörtern ist grundsätzlich untersagt.

Der Versuch, Zugriff auf Daten zu erhalten, für die keine Berechtigung besteht, ist verboten.

Bei Beendigung des Dienstverhältnisses sind die im Eigentum der Universität stehenden Endgeräte, Softwarelizenzen, Zugangsberechtigungen und Abonnement-Passwörter an den jeweiligen Vorgesetzten/die jeweilige Vorgesetzte zu retournieren.

5 Richtlinien für Administratoren/Administratorinnen und Serversysteme

5.1 Identity Management

Benutzer-/Benutzerinnenkonten sind mit den gespeicherten Daten zur Person (Personalführung, Studierenden- und Alumni-Evidenz) zu verknüpfen und daraus Zugriffsrechte und Laufzeiten abzuleiten. Ist dies nicht möglich, dürfen Benutzer-/Benutzerinnenkonten nur befristet eingerichtet werden. Es ist sicherzustellen, dass Benutzer-/Benutzerinnenkonten nach Ausscheiden bzw. Austritt der Person stillgelegt werden. Die Löschung erfolgt innerhalb eines Jahres nach Stilllegung

Für Veranstaltungen, Gaststudierende, Gastdozentinnen/Gastdozenten, können befristet Sammelbenutzer-/benutzerinnenkonten eingerichtet werden, zu denen mehrere Personen Zugang

haben können. Solche Konten dürfen keinen Zugriff auf und keine Speicherung von Daten vornehmen, die den Datenklassen geheim, vertraulich oder eingeschränkt angehören.

Die Zugangsdaten zu Benutzer-/Benutzerinnenkonten von Administratoren und Administratorinnen müssen zumindest einer zweiten fachkundigen Person bekannt sein.

Systempasswörter müssen so gewählt werden, dass deren Identifizierung unter Berücksichtigung der aktuellen Technologie nicht mit vertretbarem Ausmaß möglich ist.

Für Benutzer/Benutzerinnen-Passwörter sind entsprechend dem Schutzbedarf Mindeststandards festzulegen.

Diese Bestimmungen gelten für alle Systeme der Universität, welche über eine Benutzer-/Benutzerinnenverwaltung verfügen. Notwendige Ausnahmen bedürfen des Verfahrens der Ausnahmeregelung nach Punkt 10.

5.2 Vergabe von Zugriffsrechten

Zugriffsrechte sind vom jeweiligen Identity Management für Benutzer bzw. Benutzerinnen grundsätzlich so einzustellen, dass nur auf jene Daten Zugriff besteht, die der Benutzer/die Benutzerin für seine/ihre Tätigkeit im Rahmen seiner/ihrer Aufgaben benötigt.

Die Vergabe von Zugriffsrechten basiert auf Personengruppen spezifischen Standardrechten, die von der jeweiligen Benutzer-/Benutzerinnenverwaltung festzulegen sind. Darüber hinaus gehende Rechte bedürfen der Autorisierung durch den/die für die Daten, die IT-Anwendung oder den Zugriff Verantwortlichen/Verantwortliche. Autorisierungen sind nachweislich (z.B. per Mail) zu beauftragen.

Bei Wechsel des Aufgabengebietes ist vom jeweiligen/von der jeweiligen Vorgesetzten eine Meldung an die Benutzer-/Benutzerinnenverwaltung vorzunehmen.

Eine Überprüfung der Notwendigkeit von Zugriffsrechten und Benutzer-/Benutzerinnenkonten muss im Auditplan einmal im Jahr vorgesehen sein.

5.3 Systemmanagement

Für Systemmanagementaufgaben sind sichere Prozeduren und sichere Kommunikationsprotokolle einzusetzen. Die Systemmanagement-Tätigkeiten müssen den einzelnen Administratoren/ Administratorinnen eindeutig zuordenbar sein. Die Einrichtung und Nutzung von Sammel-IDs oder Gruppenzertifikaten ist nicht zulässig.

Die Tätigkeit des Systemmanagements sollte, wenn technisch möglich, protokolliert werden.

Die Betriebs- und Anwendungssoftware von Serversystemen ist - wenn keine technischen Gründe entgegenstehen - auf dem jeweils aktuellen Sicherheitsstand zu halten.

Alle Serversysteme sind so zu konfigurieren, dass nur die notwendigen Dienste aktiviert sind, und Verbindungen nur zwischen ausdrücklich erlaubten Systemen aufbaubar sind.

Die Betriebsdaten sind zumindest so lange aufzubewahren, dass sie für ein Audit gemäß Auditplan zur Verfügung stehen.

6 Datensicherung und Wiederherstellung

Daten der Klassen geheim und vertraulich müssen auf zentral bereitgestellten Datenspeichern gespeichert werden.

Dazu sind in Datensicherungsplänen die Sicherungsintervalle, die Sicherungsmethode, die Art der Datenträger und die Generationenverwaltung festzulegen. Diese Pläne haben auch die Archivierung mit Sicherstellung eventueller Behaltefristen einzubeziehen.

Jeder Datensicherungsplan hat einen Datensicherungsverantwortlichen/ eine Datensicherungs-verantwortliche und einen Stellvertreter/eine Stellvertreterin festzulegen.

Werden Daten mehrerer Datenklassen über einen Datensicherungsplan gesichert, dann sind für den ganzen Plan die Sicherheitsbestimmungen der höchsten Klasse anzuwenden.

Bei Rücksicherungen muss der Zielort der Datenrücksicherung über die gleichen Zugriffsrechte verfügen wie die Originaldaten. Insbesondere dürfen Daten nicht auf allgemein zugängliche Verzeichnisse zurückgesichert werden, um eine Vermehrung von Zugriffsrechten zu unterbinden.

Bei Bedarf sollten zum Schutz von Daten und zur Sicherung der Systemverfügbarkeit Datenreplikationen und Systemredundanz in Ausfallrechenzentren ausgelagert werden.

7 Umgang mit Sicherheitsvorfällen

Sicherheitsrelevante Vorkommnisse oder Sicherheitsmängel sind von allen Personen, die in den Geltungsbereich dieser IT-Sicherheitsrichtlinie fallen, umgehend dem Helpdesk des ZID oder dem /der Vorgesetzten zu melden. Über schwerwiegende Sicherheitsvorfälle ist der IT-Security Officer zu informieren.

Handlungsabläufe für die Behandlung von Sicherheitsvorfällen sind so auszurichten, dass zuerst die Sicherheit, dann die Verfügbarkeit und zuletzt die Beweis- und Ursachensicherung berücksichtigt werden.

Zur Vorbeugung bzw. Einschränkung der möglichen Folgeschäden eines Sicherheitsvorfalles müssen die Logfiles auf den Servern und auf der Firewall in regelmäßigen Abständen durch die jeweiligen Administratoren/Administratorinnen auf Anomalien überprüft werden.

Bei Gefahr im Verzug ist die zuständige Systemadministration berechtigt, Services und Zugänge zu Systemen und Netzwerksegmenten zu sperren, bis die Bedrohung bzw. Behinderung beseitigt ist.

8 Audit und Revision

Um die Einhaltung und somit die Wirksamkeit der bestehenden Bestimmungen und Schutzmaßnahmen zu überprüfen, werden in regelmäßigen Abständen Audits durchgeführt.

Der IT-Security Officer erstellt einen Auditplan mit Beschreibung des Ziels, der Methoden, der betroffenen Bereiche, der von der Leitung des ZID zu genehmigen ist.

Audits müssen im Vorfeld angekündigt werden.

Über die Ergebnisse der Auditpunkte erfolgt eine Protokollierung, aufgrund der in Absprache mit den betroffenen Bereichen Maßnahmen zur Verbesserung der Sicherheitssituation festzulegen sind.

9 Maßnahmen bei Nichteinhaltung

Ein Verstoß liegt dann vor, wenn die einschlägigen Gesetze oder Bestimmungen dieser IT-Sicherheitsrichtlinie nicht eingehalten werden. Regelwidriges Verhalten ist insbesondere die Verwendung von IT-Einrichtungen

- für Angriffe auf und Behinderung oder Störung von Einzelpersonen oder Personengruppen
- zur Behinderung der Arbeit Dritter z.B. durch übermäßige Inanspruchnahme von Systemressourcen.
- für Attacken gegen Computer, das Netzwerk oder die Services, die darauf erbracht werden.
- mit Verletzung von Lizenz- oder anderer vertraglichen Bestimmungen

Erfahrungsgemäß resultiert die Mehrzahl der Verstöße aus Unkenntnis. In diesem Fall erfolgt eine Aufklärung durch den Vorgesetzten/die Vorgesetzte bzw. bei Studierenden durch den Helpdesk des ZID, verbunden mit der Aufforderung, diese Verstöße zukünftig zu unterlassen. Bei lizenzrechtlichen Vergehen kann der IT-Security Officer eine Löschung verlangen.

Bei wiederholten oder schweren Verstößen gegen die IT-Sicherheitsrichtlinie erfolgt vom IT-Security Officer eine schriftliche Sachverhaltsdarstellung an den Vorgesetzten/die Vorgesetzte. bzw. bei Studierenden kann ein befristeter Entzug der Benützungsbewilligung erfolgen.

10 Regelungen bei Ausnahmen

Wenn Bestimmungen dieser IT-Sicherheitsrichtlinie nicht umgesetzt werden können, dann kann eine Ausnahmeregelung festgelegt werden. Dazu ist vom jeweils Verantwortlichen/von der jeweils Verantwortlichen unter Angabe des Anlasses, des Zwecks, der Methoden und Auswirkungen für einen eingeschränkten Benutzer-/Benutzerinnenkreis eine zeitlich befristete Ausnahme beim ZID zu beantragen. Der ZID hat dazu eine Stellungnahme abzugeben. Im Falle einer Ablehnung durch den ZID entscheidet das Rektorat. Eine Verlängerung der Ausnahmeregelung erfolgt mittels neuer Beantragung.

11 Sicherheits-Detailregelungen

Es liegt in der Verantwortung des IT-Security Officers, zur Erreichung der Sicherheitsziele von einzelnen Sicherheits-Richtlinien vertiefende Dokumente oder die genaue Beschreibung von Standards in Zusammenarbeit mit den verantwortlichen Organisationseinheiten zu erstellen.

Die Leitung des ZID prüft die Detailregelung auf Übereinstimmung mit der IT- Sicherheitsrichtlinie.

12 Verfahren für Änderungen der IT-Sicherheitsrichtlinie

Die Weiterentwicklung dieser IT-Sicherheitsrichtlinie liegt im Verantwortungsbereich des IT-Security Officers, dem dadurch auch die Verwaltung der Versionen obliegt.

Der IT-Security Officer bewertet eingebrachte und eigene Änderungsvorschläge auf deren Relevanz für die IT-Sicherheitsrichtlinie, die aus veränderten Bedrohungsszenarien, Topologien, Prozessen und Erkenntnisse aus Sicherheitsvorfällen resultieren.

13 Inkrafttreten, Änderungen

Die gegenständliche Richtlinie sowie jede Änderung der Richtlinie tritt mit dem auf die Kundmachung im Mitteilungsblatt der Alpen-Adria-Universität Klagenfurt folgenden Tag in Kraft.

14 Glossar

Audit

Als Audit (von lat. "Anhörung") werden allgemein Untersuchungsverfahren bezeichnet, die dazu dienen, Prozessabläufe hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten. Im Bereich der IT-Sicherheit geht es also darum, zu überprüfen, ob die Sicherheitsziele erreicht werden und wo Schwachstellen und Verbesserungsmöglichkeiten bestehen.

Authentifizierung

Authentifizierung, auch Authentisierung bezeichnet den Nachweis eines Kommunikationspartners/einer -partnerin, dass er/sie tatsächlich derjenige/diejenige ist, der er/sie vorgibt zu sein. Die einfachste Form der Authentifizierung ist die der Eingabe von Benutzer-/Benutzerinnenkennung und Password. Unter starker Authentifizierung versteht man die Kombination von zwei Authentifizierungstechniken, wie Chipkarte und Geheimnummer. Daher wird dies auch häufig als Zwei-Faktor-Authentifizierung bezeichnet.

Firewall

Eine Firewall, auch Sicherheitsgateway genannt, ist eine Netzwerk-Sicherheitskomponente bestehend aus Hard- und Software, die Netzwerkverkehr anhand eines definierten Firewall-Regelwerks zulässt oder verbietet. Das Ziel einer Firewall ist es, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauens-Stufen abzusichern. Ein typischer Einsatzzweck ist es, den Übergang zwischen einem lokalen Netzwerk (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren.

Identity-Management

Als Identitätsmanagement wird der zielgerichtete und bewusste Umgang mit Identität, Anonymität bezeichnet. Durch das Internet hat die Frage von bewusstem Umgang mit Identität und Anonymität eine neue und zuvor nicht gekannte Komplexitätsstufe erreicht. Identity-Management befasst sich vornehmlich mit der Verwaltung von Identitäten d.h. mit Benutzer-/Benutzerinnendaten, die einzelnen Personen zugeordnet sind und deren Identitäten bestimmen.

IP-Adresse

Eine IP-Adresse (Internet-Protocol-Adresse) ist eine Nummer, die die Adressierung von Rechnern und anderen Geräten im Internet erlaubt. Technisch gesehen ist die IP-Adresse eine 32-stellige Binärzahl und wird in Form von 4 Zahlengruppen angegeben (z.B. 143.205.64.1).

Der Mensch merkt sich jedoch leichter sprechende Namen. Deshalb ist im Internet ein Dienst eingerichtet, der Internetnamen in IP-Adressen auflöst, so dass in den meisten Fällen die Angabe von Namen statt numerischer Kennungen zulässig ist. So wird beispielsweise der Internetname des Web-Servers der Universität www.uni-klu.ac.at aufgelöst in 143.205.180.80.

Password-Qualität

Die Sicherheit eines Kennwortes hängt vor allem davon ab, dass dieses geheim bleibt. Um dies zu gewährleisten sollte ein Password eine Struktur haben, die es erschwert, dass es durch spezielle Vergleichssoftware mit Wörterbüchern oder anderen Textvorlagen ermittelt werden kann. Merkmale für eine qualitätsvolle Password-Struktur sind z.B. Passwordlänge von zumindest 8 Zeichen, Enthaltensein von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, keine Namen und Namensteile, keine Ähnlichkeit mit dem Usernamen und bei Änderung keinen Bezug zu den Vorgänger-Passwörtern.

TCP-Port

Das Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets. **Ports** (englisch für *Anschlüsse*) sind Adresskomponenten, die in Netzwerkprotokollen eingesetzt werden, um Datensegmente den richtigen Programmen und Diensten zuzuordnen. Die **Internet Assigned Numbers Authority** (**IANA**) ist eine Organisation, die unter anderem die Vergabe von Ports, den sog. Well Known Ports regelt. Firewall-Regeln basieren vielfach auf den IANA Well Known Ports.

Virtual Private Network (VPN)

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner/-partnerinnen sicher authentifiziert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

WLAN AccessPoint

Mit WLAN (Wireless Local Area Network) wird ein System räumlich begrenzter Rechnerverbünde (WLAN Zellen) bezeichnet, in denen die Kommunikation durch Funkübertragung erfolgt. Die einzelnen Rechner einer WLAN Zelle kommunizieren miteinander über einen zentralen Zugangspunkt (Access Point). Dieser Access Point stellt auch den Übergang zum kabelgebundenen Anteil eines Netzwerkes dar. Access Points werden so angeordnet, dass mehrere Zellen einen räumlich überdeckenden Bereich ergeben, in dem mobile Computer von Zelle zu Zelle wandern können, ohne die Netzwerkverbindung zu verlieren.