Sicherheitsgruppen im Hochschuldatennetz

Arbeitskreis IT-Sicherheit an der UniBwM

Gültig ab: 22.07.2009

Datum	Bemerkung
07.02.2009	Erstfassung
04.03.2009	Überarbeitung
22.07.2009	Zustimmung durch HL

Zielgruppe: Systemverantwortliche, Subnetzverantwortliche

Thematik: Hochschuldatennetz (HDN), Firewall

Zusammenfassung: Bisher sind Arbeitsplatzrechner und Server gemischt in gemeinsamen Subnetzen untergebracht. Das Schutzniveau ist bei vielen dieser Netze unzureichend. Dieses Dokument beschreibt die Mechanismen, mit denen künftig die Teile des Hochschuldatennetzes noch besser geschützt werden.

Inhaltsverzeichnis

1 Einführendes Beispiel

Familie Schlau ist der modernen Kommunikationstechnik sehr aufgeschlossen. Vater, Mutter und die beiden Kinder teilen sich drei Notebooks, einen Netzdrucker, einen kleinen Fileserver und den über einen DSL-Router realisierten Internet-Anschluss. Zusätzlich hat sich Familie Schlau bei einem Internet-Hoster eine Webpage www.familie-schlau.de eingerichtet und nutzt auch passende Email-Adressen wie z.B. sabine@familie-schlau.de. Da Tochter Sabine zur Zeit zum Studium im Ausland weilt, nutzt sie meist das Webmail-Angebot des Provider unter webmail.familie-schlau.de. Die Kommunikationsweise der Familie Schlau ist der Kommunikation im Hochschuldatennetz durchaus ähnlich:

- Die Notebooks und Netzdrucker sollen nur untereinander kommunizieren. Der Rest der Welt soll nicht darauf zugreifen können.
- Die persönlichen Dokumente bleiben intern auf dem Fileserver, so dass sie alle Familienmitglieder ansehen können, aber der Rest der Welt keinen Zugriff darauf hat.
- Auf den Webseiten kann Mutter Schlau ihr Erdbeerkuchenrezept der ganzen Welt bekannt machen.
- Nachbarfamilie Ungeschickt hat auf Ihren Computern eine Wurminfektion. Da der DSL-Router keine Verbindungen von außen auf das Heimnetz von Familie Schlau zulässt, bedeutet dies keine Gefahr für die IT-Systeme der Familie Schlau.

2 Gruppenmodell

Im Netz der UniBwM gibt es Clientrechner und Server. Clientrechner bieten in der Regel keine Dienste über das Netz an. Server bieten ihre Dienste nur für eine bestimmte Nutzergruppe (z.B. Studenten, Mitglieder einer Arbeitsgruppe, eines Instituts oder einer Fakultät) innerhalb des Hochschuldatennetzes. Andere Server bieten Dienste für alle Personen im Hochschuldatennetz an. Wieder andere Server bieten ihre Dienste weltweit an.

Um unerwünschte Zugriffe zu verhindern kann man Dienste mit einem Authentifizierungsschutz versehen, der nur der gewünschten Gruppe den Zugriff ermöglicht. Zudem kann man mit Firewallregeln sicherstellen, dass bestimmte Systeme von anderen aus gar nicht erreicht und damit nicht angegriffen werden können. Im Gruppenmodell der UniBwM werden nachfolgend aufgeführte Gruppen mit folgenden Merkmalen unterschieden:

2.1 Studenten

Studenten sind in Wohngebäuden untergebracht. Innerhalb der Wohngebäude kann auf andere Rechner zugegriffen werden. Um Infektionen zu stoppen ist der Zugriff auf Studentenrechner in anderen Gebäuden unterbunden. Studentenrechner sind von anderen Gruppen aus nicht erreichbar.

2.2 Institute

Auch durch Institute ist der Zugriff nur auf andere Rechner im gleichen Subnetz möglich. Zugriff auf andere Institutsrechner (z.B. zwecks Zusammenarbeit) kann auf Antrag ermöglicht werden.

2.3 Server Weltweit

Die Institute bieten einige Dienste weltweit an wie z.B. Webserver. Diese Server sind besonders gefährdet. Damit eventuell erfolgreiche Angriffe auf diese Server nicht Client-Rechner bedrohen, wird die Gruppe der weltweit erreichbaren Server von anderen Rechner geschützt betrieben und bildet somit eine eigene Gruppe. Weltweit verfügbare Server werden durch den AK IT-Sicherheit genehmigt. Grundlage dafür ist ein durch den Beirat IKIS genehmigtes Rechner- und Betriebskonzept.

2.4 Server Campus

Nicht alle Dienste müssen weltweit verfügbar sein. Server, die nur universitätsintern Dienste anbieten (= Server Campus), werden ebenfalls in eine eigene Gruppe gepackt und vor anderen Rechnern geschützt.

2.5 Internet

In der Gruppe Internet befinden sich alle Client- und Server-Rechner, die nicht Teil des Hochschuldatennetzes sind. Diese Rechner haben nur auf die Server in der Gruppe Server Weltweit Zugriff.

2.6 Studentische Server

Die Netze der Wohnbereiche sind voreinander geschützt (vgl. 2.1). Um trotzdem gemeinsam auf studiumsrelevanten Datenbeständen arbeiten zu können, wird eine Gruppe Studentische Server gebildet, die nur aus den Studentischen Wohnbereichen erreichbar ist. Studentische Server werden durch den CSO-RZ o.V.i.A. genehmigt.

2.7 Tabellarische Übersicht

Von-Nach	Studenten	Institute	Server Weltweit	Server Campus	StudServer	Internet
Studenten	eigenes Netz		erlaubt	erlaubt	erlaubt	erlaubt
Institute		eigenes Netz	erlaubt	erlaubt		erlaubt
Server Weltweit						erlaubt
Server Campus						erlaubt
StudServer				erlaubt		erlaubt
Internet			erlaubt			erlaubt

2.8 Verwaltung und Militärischer Bereich

Verwaltung und Militärischer Bereich sind stärker abgeschottet als die anderen Gruppen. Die detaillierte Umsetzung regelt der CSO-RZ o.V.i.A. nach technischen Erfordernissen.

2.9 Abkürzungsverzeichnis

AK Arbeitskreis

CSO Chief Security Officer

DSL Digital Subscriber Line

HDN Hochschuldatennetz

IKIS Informations- und Kommunikations-Infrastruktur

IT Informationstechnik

o.V.i.A. oder Vertretung im Amt

RZ Rechenzentrum

UniBwM Universität der Bundeswehr München