

Anmeldung eines Servers mit Internetdiensten

Seite 1

An die
Zentraleinrichtung für Datenverarbeitung (ZEDAT)
Firewall-Konfiguration



– durch Fach –

In der Verantwortung für einen sicheren Betrieb des Campusnetzes der Freien Universität Berlin hat es sich als notwendig erwiesen, zentrale Maßnahmen zum Schutz des Netzes und der angeschlossenen Rechner vor Angriffen aus dem Internet zu ergreifen.

Rechner im FU-Campusnetz sind immer wieder zu Ziele von Angriffen aus dem Internet. Die Angriffe nutzen zumeist Sicherheitslücken in Programmen, die Internetdienste wie WWW, FTP oder Telnet erbringen. Betroffen hiervon sind alle Betriebssysteme. Erfolgreiche Angriffe führen in der Regel dazu, dass die betroffenen Rechner von den Angreifern zu weiteren Missbräuchen benutzt werden. Diese Form des Missbrauchs führt zu folgenden Problemen:

- mögliche Ausspähung oder Zerstörung von Daten
- erhebliche Belastung der betroffenen Rechner
- zusätzlicher Datenverkehr im Campusnetz und ins Internet
- Angriffe auf fremde Rechner aus dem FU-Netz heraus
- zahlreiche Beschwerden aus aller Welt
- Mehraufwand für Rechner- und Netz-Administratoren
- möglicher Konnektivitätsverlust (Sperrung von FU-Netzen durch externe Opfer)
- Imageverlust der Freien Universität Berlin.

Die Angreifbarkeit von Rechnersystemen besteht häufig darin, dass die zur Erbringung von Internetdiensten eingesetzte Software – die sogenannten Daemonen – öffentlich publizierte Programmier- oder Konfigurationsfehler enthält, die von Angreifern systematisch gesucht und zum Einbruch in solche Systeme genutzt werden. Leider zeigt die Erfahrung, dass nicht alle Rechner im Campusnetz mit der Sorgfalt und Schnelligkeit gepflegt werden (z.B. durch Einspielen entsprechender Patches), wie dies für einen sicheren Betrieb im Internet erforderlich wäre. Außerdem stehen nicht für alle Probleme zeitnah Software-Patches zur Verfügung. Darüber hinaus ist festzustellen, dass zunehmend unerfahrene Anwender Rechner in Betrieb nehmen, auf denen unbeabsichtigt und unbemerkt Serverdienste angeboten werden, weil das verwendete Betriebssystem entsprechend vorkonfiguriert ist.

Zum Schutz der Rechner im Campusnetz sind die besonders gefährdeten Internetdienste (FTP, Mail/SMTP, Telnet, WWW/HTTP) für alle von außen eingehenden Verbindungen in das Campusnetz von der ZEDAT gesperrt. Die ZEDAT weist entsprechende Anfragen vergleichbar einem Firewall am zentralen Eingangsrouten der Freien Universität Berlin für alle Zielrechner in den Netzen 160.45.*.* und 130.133.*.* ab. Darüber hinaus können auch auf Routern im Campusnetz die entsprechenden Verbindungen zwischen Subnetzen unterbunden sein. Die genannten Dienste können also nur im eigenen Subnetz uneingeschränkt angeboten werden. Die von FU-Systemen (als Clients) ausgehenden Verbindungen zu Diensten außerhalb der FU Berlin sind von dieser Sperr-Maßnahme in keinem Fall betroffen.

Ausgenommen von der Sperrung der Verbindungen zu den Diensten werden auf Antrag nur diejenigen Serversysteme im Campusnetz der FU, die für den jeweiligen Bereich Dienste über das eigene Subnetz hinaus oder nach außen öffentlich anbieten müssen und für die der ZEDAT mit umseitigem Formular zuständige Administratoren als Ansprechpartner benannt werden. Diese Administratoren müssen über hinreichende Kenntnisse verfügen und die von ihnen betreuten Systeme nach den „Regeln der Kunst“ durch geeignete Konfiguration und Software-Pflege sicher betreiben. Die ZEDAT empfiehlt, die Zahl der Rechner, die öffentliche Dienste anbieten, auf ein Minimum zu beschränken.

Weitergehende Fragen zur beschriebenen Sicherheitsmaßnahme richten Sie bitte per E-Mail an die Adresse

Firewall@ZEDAT.FU-Berlin.DE

Anmeldung eines Servers mit Internetdiensten

Seite 2

Hiermit bitten wir, folgenden Server im Campusnetz der Freien Universität Berlin zur Erbringung von öffentlichen Internetdiensten zu registrieren und die entsprechenden Dienst-Ports in FU-Routern freizuschalten. Wir versichern, den Server durch geeignete Maßnahmen so gut wie möglich vor Einbrüchen aus dem Netz zu schützen.

Antragstellende Einrichtung	
FB / ZI / ZE / übergreifende Einrichtung	_____
Wissenschaftliche Einrichtung / Institut	_____
Abteilung / Arbeitsgruppe	_____
Server	
Hostname im DNS	_____
IP-Nummer	_____ Betriebssystem/Version _____
Freizuschaltende Dienste (Zugriff über Standard-Ports)	
Freizuschaltende Dienste bitte ankreuzen	
<input type="radio"/> FTP	<input checked="" type="checkbox"/> Anonyme Datei-Ablage (ohne Passwort) wird nicht gestattet
<input type="radio"/> Mail/SMTP	<input checked="" type="checkbox"/> Mail-Relaying wird verhindert
<input type="radio"/> Telnet	<input checked="" type="checkbox"/> Anonymes Login (ohne Passwort) wird nicht gestattet
<input type="radio"/> WWW/HTTP	
Verantwortlicher Administrator, zugleich Ansprechpartner für die ZEDAT	
Vorname _____	Name _____
Dienstanschrift _____	
Telefon _____	Mobiltelefon _____
E-Mail _____	Telefax _____
Datum _____	Unterschrift _____
Vertreter des Administrators	
Vorname _____	Name _____
Dienstanschrift _____	
Telefon _____	Mobiltelefon _____
E-Mail _____	Telefax _____
Einverständniserklärung des Leiters der Einrichtung	
Mit der Freischaltung des oben genannten Servers für die öffentlich zu erbringenden Internetdienste bin ich einverstanden.	
Vorname _____	Name _____
Funktion _____	
Datum, Dienstsiegel _____	Unterschrift _____