DHBW
Duale Hochschule
Baden-Württemberg
Ravensburg

Informationen zur Sperrung von Port 25 (SMTP)

Port 25 – was ist das?

Verbindungen zu Port 25 dienen der Kommunikation zwischen Mailservern per "Simple Mail Transfer Protocol" (SMTP) und sind insofern primär auch nur zwischen Mailservern notwendig. Endkunden nutzen immer nur den Mailserver Ihres Providers, dieser verbindet sich dann über den Port 25 mit anderen Servern.

Seit dem Aufkommen von Mailprogrammen auf PCs wird SMTP aber auch für den Versand von E-Mail vom PC zum ausgehenden Mailserver eingesetzt. Seit einigen Jahren ist dafür zwar ein anderer Port vorgesehen (587 statt 25), aber die meisten Mailprogramme sind standardmäßig noch auf Port 25 voreingestellt, obwohl zumindest die großen Mail-Provider auch Port 587 unterstützen.

Wozu dient die Sperrung?

Die Sperrung im gesamten BelWue-Netz in dient dem Zweck, schlecht gepflegte Rechner auf den Campi mit installierter Mailserver-Software daran zu hindern, als "Relais" für den Versand von unverlangter Werbe-Mail ("Spam") von außerhalb nach außerhalb zu fungieren. Inzwischen sind offene Relais-Mailer allerdings nicht mehr die Hauptquelle von dubiosen E-Mails, da einerseits die meisten Einrichtungen Maßnahmen gegen solche Quellen ergriffen haben, die verbliebenen andererseits in öffentlichen schwarzen Listen aufgeführt sind. Diese werden von den meisten Mailserver-Betreibern verwendet, um E-Mail von diesen Systemen zu blockieren.

Deshalb gibt es seit einiger Zeit eine Allianz zwischen Viren/Wurm-Programmierern und den Versendern von Spam-Mail. Der Großteil der Würmer der letzten Monate verfügt über ausgefeilte Funktionen zur Fernsteuerung des befallenen PCs. Dazu ist auch kein direkter Zugriff von außen auf den PC erforderlich (der z.B. durch die bestehende Sperrung aller eingehenden Verbindungen oder durch Firewalls unterbunden wird), sondern die PCs melden sich selbst über unverdächtige Kanäle (IRC, HTTP, DNS) bei einem steuernden Rechner irgendwo auf der Welt an und holen sich aktiv die für sie vorgesehenen Kommandos. Alle mit demselben Steuerrechner verbundenen PCs bilden ein "Zombie-Netzwerk", das zu beliebigen Aktionen genutzt werden kann. Die Hauptanwendungen liegen in "Distributed Denial-of- Service"-Angriffen (DDOS); also in Angriffen von möglichst vielen verteilten Rechnern auf ein System, mit dem Ziel dieses lahmzulegen. Die zweite Hauptanwendung ist der Versand von Spam-Mails über einen eingebauten "Mini-Mailserver", der keinen weiteren Mailserver benötigt und sich direkt mit den Zielmailern verbindet. Mittlerweile sind diese gekaperten Systeme die Hauptquelle von Spam-Mails geworden. Besonders beliebt sind dabei permanent laufende Rechner, z.B. zu Hause an DSL-Anschlüssen oder eben in Universitäten (beliebt wegen der guten Netzanbindung).

Die Portsperre verhindert nun den Missbrauch der befallenen Rechner für den Versand von Spam nach außen, sowie gleichzeitig die Weiterverbreitung der Würmer per E-Mail an Ziele außerhalb der Universität, und damit die wichtigsten negativen Auswirkungen. DDOS-Angriffe (s.o.) können damit nicht verhindert werden, ebenso bleiben die Rechner fernsteuerbar (mit allen Folgen, z.B. Mitschneiden von Tastendrücken, Diebstahl oder Zerstörung/Modifikation von sensitiven Daten, etc.). Deshalb sollte diese Ankündigung keineswegs so verstanden werden, dass infizierte Rechner nunmehr gefahrlos weiterbetrieben werden können.

Lösung

Versuchen Sie Ihr Mailprogramm auf Port 587 zu konfigurieren. Oder fragen Sie Ihren Mail-Provider nach weiteren alternativen Einstellungen.