IT-SICHERHEIT

Verwundbare Systeme

Mit einer Live-Hacking-Demonstration gaben Studenten der Fachhochschule Hagenberg einen Einblick, wie man in Computersysteme eindringen kann und welche Abwehrmaßnahmen notwendig sind.

Wie verwundbar Computersysteme gegen Angriffe von außen sind, wie man sich vor diesen Angriffen schützen kann und wie wirksam Schutzmaßnahmen im Einzelnen sind, zeigten Studenten des Studiengangs "Computer- und Mediensicherheit" der Fachhochschule Hagenberg, Oberösterreich, am 14., 15. und 20. Jänner 2004. Zielgruppe der Informationsabende in Kooperation mit dem Wirtschaftsförderungsinstitut OÖ waren kleine und mittlere Unternehmen.

Auf Rechner eines Unternehmens, das zuvor sein Einverständnis gegeben hatte, erfolgten von Studenten Attacken mit freien Programmen aus dem Internet. Auf einem Bildschirm konnte mitverfolgt werden, welche Aktionen liefen; auf einer weiteren Projektion, wie die von einem zweiten Studententeam gesteuerten Abwehrsysteme reagieren, welche Warnmeldungen zu denken geben sollten und wie gut die Absiche-rungen waren. Der in der Mitte stehende "Mastermind" erläuterte die jeweiligen Aktionen und Gegenmaßnahmen.

Als "Penetrationstests" erfolgen Attacken von IT-Sicherheitsexperten professionell, um auf Verlangen Computersysteme auf ihre Sicherheit gegen Angriffe von außen zu testen.

In der Phase des "Footprintings" werden Angriffe auf ein System vorbereitet, es wird ein Rechner ausfindig gemacht und dort nach offenen Türen (Ports) gesucht. Ein solcher "Portscan" sollte zu verstärkter Wachsamkeit Anlass geben. Gelingt es dem Angreifer trotzdem, in das System einzudringen, sucht er nach verwundbaren Pfaden, legt einen Trojaner ab, der ihm weitere Zugriffe erlaubt, und stattet sich mit Administratorrechten aus. Damit kann er sich ungehemmt im System bewegen, Daten einsehen, verändern, löschen – der Betroffene kann von Glück reden, wenn lediglich – wie bei der Übung – die Website des Unternehmens und damit dessen Internet-Auftritt verändert wird. Dann stiehlt sich der Angreifer wieder aus dem System.

"Intrusion-Detection-Systeme" erkennen solche Angriffe, eine Firewall blockt sie ab. Allerdings muss die Software aktuell gehalten werden, ebenso wie die zu den Betriebssystemen angebotenen Service-Packete, die erkannte Lücken schließen.

Kurt Hickisch