Intrusion Detection Theorie & Wirklichkeit

Vortrag: *Johan Beckers* <jbeckers@iss.net>
WWW: www.iss.net

Bericht: *Dieter Kirchner* <dieter@roko.goe.net>

Johan Beckers von ISS (Internet Security Systems) stellte deren Software *Real Secure 2.5* zum Bereich Intrusion Detection vor. Als erstes Produkt der Firma ISS wurde kurz deren Internetscanner vorgestellt. Bei Real Secure basiert das System auf einem zentralen Managementserver, der mit Agenten auf den Clients verbunden wird. Die Servermanagementsoftware erkennt durch Meldung der Clients etliche verschiedene Angriffe auf den Clients und kann darauf nach unterschiedlichen voreingestellten Prioritäten reagieren. Die Erkennung führt eine Analyse der ankommenden Pakete durch und versucht zu erkennen, ob und welche Form eines Angriffs stattfindet (Pattern-matching). Die Informationen, was ein Angiff ist und was nicht, liest das Programm aus einer Datenbank aus. Bei neuen Angriffsformen wird ein update der Datenbank notwendig. Die Sicherheit durch das Programm wird nicht als maximal eingeschätzt, es soll vor allem Gelegenheitshacker davon abhalten, mit bekannten Tools anzugreifen, da diese sofort erkannt werden. Vorgeführt wurde dies mit dem alten Winnuke. Bei neuem Code auf der Angreiferseite wird das System unter Umständen nicht reagieren. In einer besonders sicheren Variante soll eine Netzwerkkarte ohne IP-Adresse eingeschleift werden, die unsichtbares Kontrollieren des Netzwerks möglich macht. Das Sperren als Reaktion auf einen Angriff wurde nicht empfohlen, da das System wohl nicht mit spoofing klarkommt und ein Angriff unter gefälschter Absendeadresse dazu benutzt werden könnte, einen bestimmten Host für das geschützte Netz unerreichbar zu machen. Intensives Logging der Angriffe soll die Analyse erleichtern und die erreichten Zugriffe dokumentieren. Dazu kommen noch eine Menge kleinerer Tools für bequemes Arbeiten mit der Software.

Das System wird nicht als Ersatz für eine Firewall empfohlen, sondern als Ergänzung, weil 80% der Angriffe aus dem lokalen Netz kommen. Es soll hauptsächlich vor diesen lokalen Angreifern schützen, kann aber auch für die Zugriffskontrolle eingesetzt werden. Durch Editieren von Benutzerprofilen wird es möglich, einzelne Dienste für einzelne Nutzer oder Computer aus einem WindowsNT-Netzwerk zu sperren. Eine Vorführung funktionierte nicht, was auf mangelnde Ressourcen der Real Secure-Installation geschoben wurde :-)) - was wieder einmal demonstriert, wie gut Windows NT doch so funktioniert. Das System könnte selbst angegriffen werden, beispielsweise über fragmentierte Pakete, die den Speicherbedarf des Real Secure-Systems so hoch schrauben, daß das Sicherheitssystem auf Angriffe auf das Netzwerk nicht mehr reagieren kann. Auch andere Verfahren, an diesem Sicherheitspaket vorbeizukommen, dürften nach dieser Präsentation jetzt in Arbeit sein ;-) Das System arbeitet nur mit TCP/IP und benutzt die Ports 901 und 1998. Clients sind auch möglich fur Sun Solaris. UDP wird nicht unterstützt. Der Rechner, auf dem die Software läuft, sollte so schnell wie möglich sein (PentiumII/400 oder schneller) und soviel Speicher wie man auf das Mainboard stecken kann. Das wird sicher die Hardwarehersteller freuen :-), ist aber nötig, um den Managementserver vor Angriffen zu schützen.

Die Software kostet lediglich freundliche 20.000.- DM incl. Updates und Support für das erste Jahr, Kunden sind unter anderem Citybank und US Army (da fühlt man sich doch gleich viel sicherer....). Nach dieser Firmenvorführung beschleicht den geneigten Zuhörer das typische Gefühl bei Windowssoftware zum Thema Sicherheit: Nette Software, mit ordentlich Mausschubserei auch vom Ungeübten zu bedienen, aber irgendwo nicht gerade perfekter Schutz, und das Programm macht unter Umständen selbst Probleme unter Windows oder wird gar selbst zum Sicherheitsloch. Des großen Zulaufs wegen konnte die Veranstaltung nicht wie geplant im Hackcenter stattfinden, sondern wurde auf zwei mitgebrachten Laptops der Firma demonstriert. Ein weiterer Test im Hackcenter wird stattfinden, die Ergebnisse werden nachgereicht :-)