

cirosec warnt vor Angriffen auf Applikationsebene

In 80 Prozent aller Webserver kann eingebrochen werden

HEILBRONN, 25. Juni 2003 – cirosec, der IT-Sicherheitspezialist in Deutschland, warnt vor den Gefahren durch Angriffe auf Applikationsebene. Marktbeobachtungen zufolge ist es möglich, in 80 Prozent aller Webserver einzubrechen und von dort weiter in interne Systeme wie Datenbanken oder SAP-Systeme zu gelangen. Auf diese Weise kann der Angreifer Daten manipulieren, löschen oder auch stehlen und dadurch sowohl einen großen materiellen als auch immateriellen Schaden verursachen.

Die große Gefahr, die von Angriffen auf Applikationsebene ausgeht, liegt laut Stefan Strobel, Geschäftsführer von cirosec, in den technischen IT-Sicherheitskonzepten der letzten zehn Jahre begründet. „Firmen haben sich vor allem auf die Absicherung der Netzwerk Grenzen konzentriert. Firewalls aus dynamischen Filtern, Proxies, Virenschannern und URL-Filter wurden am Internet-Zugang aufgebaut.“, so Strobel weiter. „Zu einer Zeit, in der laut Gartner bereits 75% aller Angriffe auf Applikationsebene stattfinden, sind diese Mechanismen einfach nicht mehr ausreichend, um sich erfolgreich gegen Hackerangriffe zu schützen.“

Je weiter der technische Fortschritt nach E-Business-Kommunikation verlangte, umso mehr Anwendungen wurden den Partnern über eine Web-Schnittstelle angeboten und umso mehr Systeme bei Kunden und Lieferanten mussten möglichst direkt miteinander kommunizieren. Da man bestimmte Protokolle für verschiedene Anwendungen freischaltete, bekamen die Firewalls immer mehr Löcher und die erreichbaren Applikationen entwickelten sich zu beliebten Objekten von Hackern.

Mit Hilfe erlaubter Protokolle wie http können Hacker durch SQL-Injection beispielsweise unbemerkt durch Firewalls hindurch in Webserver und in die dahinter liegenden Datenbanken eindringen. Selbst bei Web-Portalen, die durch starke Authentisierung geschützt werden, ist es einem Angreifer häufig durch Cross-Site-Scripting möglich, die Cookies und damit die Benutzersession eines berechtigten Benutzers zu stehlen. Auf diese Weise kann er sich als legitimer Nutzer am Portal anmelden.

Mittlerweile gibt es moderne Technologien, die Angriffe auf Applikationsebene verhindern können. Sie lernen teilweise automatisch die benötigten URLs jeder Applikation, die erlaubten Wertebereiche und Längen von Eingabewerten und bauen daraus eine Policy auf, gegen die jeder http-Request geprüft wird. Zusätzlich überwachen sie den Status der Benutzersessions.

Diese Technologien arbeiten in der Regel als Reverse-Proxies, die man vor den Webserver schaltet und die im Gegensatz zu klassischen Reverse-Proxies nicht nur die http-Protokollebene betrachten, sondern die semantische Integrität jeder URL oder jedes einzelnen Eingabefeldes in jeder Benutzermaske auf seine jeweiligen Beschränkungen hin prüfen. Moderne Angriffe wie SQL-Injection, Parameter Tampering, Hidden Manipulation und viele andere Angriffe auf Web-Applikationen werden damit verhindert.