

GeNUDetect 2.2 spürt unbekannte Hacker-Angriffe auf

Intrusion Detection & Prevention System mit Anomalie-Erkennung erweitert

Kirchheim bei München, 27. September 2005. Hacker sind verhaltensauffällig – dies macht sich das neue Release von GeNUDetect zu Nutze. Der IT-Security-Spezialist GeNUA hat das Intrusion Detection & Prevention System mit der Anomalie-Erkennung erweitert: Ungewöhnliche Bewegungen im Netzwerk werden aufgespürt, um auch bisher unbekannte Hacker- und Wurm-Attacken umgehend zu enttarnen. So können rechtzeitig Abwehrmaßnahmen ergriffen werden, bevor durch die neuen Angriffsvarianten Schaden entsteht. Bei GeNUDetect 2.2 ergänzt die Anomalie-Erkennung die bewährte Signatur-basierte Fahndung nach bekannten Angriffsmustern.

Die exakte Anomalie-Erkennung ist das Ergebnis ausgefeilter Statistik. Dazu beobachtet GeNUDetect nach der Installation zunächst über mehrere Tage den Datenverkehr des zu schützenden Netzwerks. Zulässiger Datenaustausch, regelmäßige Schwankungen und langfristige Trends werden analysiert und ein charakteristisches Muster berechnet. Anhand dieses Profils überwacht GeNUDetect den fortlaufenden Netzwerk-Betrieb. Wenn jetzt eine deutliche Anomalie festgestellt wird, liegt mit Sicherheit eine ungewollte Netzwerk-Aktivität vor - ein Hacker-Angriff, eine Wurm-Attacke oder auch eine fehlerhafte System-Konfiguration -, die sofort an den Administrator gemeldet wird.

Neue Angriffsvarianten sind besonders auffällig

Das entscheidende Merkmal der Anomalie-Erkennung ist, dass auch unbekannte Angriffsvarianten aufgespürt werden. Denn gerade neue Methoden erzeugen im Netz ungewohnte Bewegungen – also auffällige Anomalien. Hier liegt der Vorteil gegenüber der Signatur-Erkennung, die ausschließlich auf bekannte Gefahren reagieren kann. Dafür nennt das Signatur-Verfahren wiederum erkannte Angriffe direkt beim Namen, so dass umgehend bewährte Abwehrmaßnahmen ergriffen werden können. Beide Verfahren bieten Vorteile und sind im Intrusion Detection & Prevention System GeNUDetect 2.2 kombiniert.

Trennschärfe wird kontinuierlich verfeinert

Anomalie-Erkennung kann mit geringem Administrationsaufwand betrieben werden. Nach der Installation verfeinert GeNUDetect automatisch anhand der ständigen Datenanalysen seine Trennschärfe. So wird nach einer Lernphase auch bei geringen Anomalien zuverlässig zwischen erlaubten und gefährlichen Aktivitäten unterschieden. Für die exakte Analyse des Datenverkehrs sind Sensoren mit Dual CPUs und vier GB Speicher erforderlich, die an sensiblen Stellen des Netzwerks installiert werden.

Über GeNUA

GeNUA, Gesellschaft für Netzwerk- und Unix-Administration, ist ein Spezialist für IT-Sicherheit. Das Leistungsspektrum umfasst hochwertige Sicherheitslösungen mit Firewalls, Intrusion Detection & Prevention Systemen, VPN-Appliances sowie ein umfangreiches Dienstleistungs- und Beratungsangebot. Mit dem System GeNUGate bietet das Unternehmen die einzige Firewall, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem internationalen Standard ITSEC in der Stufe E3 hoch zertifiziert ist. Kunden in über 30 Ländern setzen auf die Erfahrung und Lösungen des 1992 gegründeten Unternehmens, das am Firmensitz in Kirchheim bei München 70 Mitarbeiter beschäftigt.

Weitere Informationen:

GeNUA, Gesellschaft für Netzwerk- und Unix-Administration mbH
Dietmar Bruhns
Domagkstr. 7
85551 Kirchheim
Tel.: 089/ 99 19 50 -169
Fax: 089/ 99 19 50 -999
dietmar.bruhns@genua.de
www.genua.de