



... und Sie haben die Sicherheit Ihres Netzwerkes im Griff!

Vernetzung und globale Kommunikation sind Begriffe, die aus unserem Geschäftsleben nicht mehr wegzudenken sind. Die extreme Zunahme der Systemangriffe in den letzten Jahren hat gezeigt, dass Netzwerke und Server trotz Schutz durch Firewalls und Virens Scanner empfindliche Schwachstellen aufweisen. „Nimda“ und „CodeRed“, um hier nur zwei der geläufigsten Vertreter von insgesamt mehreren hundert derzeit bekannten netzwerkbasierenden Angriffen zu nennen, verdeutlichen die Risiken, Gefahren und nicht zuletzt die Kosten, die mit solchen Attacken bzw. der System- und Datenwiederherstellung verbunden sind. Bei einem Großteil der Systeme wird nicht einmal bemerkt, dass sie von Trojanern befallen sind und immer wieder erfolgreich von Hackern angegriffen und erobert werden. Den Unternehmen fehlt zum Großteil ein Instrument zur kontinuierlichen Erkennung, Überprüfung und Rückverfolgung von Angriffen. Dadurch bleiben Systeme weiterhin ungeschützt und der Sicherheitsstatus eines Systems oder Netzwerkes kann nicht verbessert werden.

... aber wir setzen doch bereits Firewalls und Virens Scanner ein ...

Firewalls dienen der Absicherung von Netzwerken. Die Funktion einer Firewall kann mit einem Pfortner verglichen werden, der nur am Übergang zwischen zwei Bereichen vorgegebene Zutrittsregeln umsetzt. Ein „Firewall-Pfortner“ untersucht jedoch nicht die Taschen der für diesen Bereich zugelassenen Personen und wacht auch nicht innerhalb des Gebäudes. So können trotz des Einsatzes von Firewalls über zugelassene Kommunikationskanäle Systeme oft problemlos angegriffen, erobert, manipuliert oder vertrauliche Daten eingesehen werden. Firewalls vergleichen nur einzelne ankommende und abgehende Datenpakete. Da Firewalls keine Angriffssignaturen erkennen, bleiben Netzwerkangriffe durch eine Firewall hindurch unerkannt. Virens Scanner besitzen zwar Virensignaturen, erkennen und untersuchen jedoch nur Dateien. Alle übrigen Pakete und Daten, die über das Netzwerk übertragen werden, können von ihnen nicht erkannt werden.

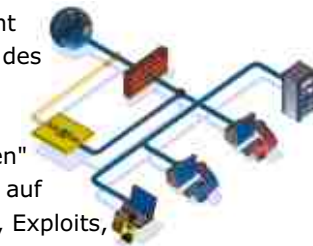


Was leistet das Intrusion Detection System (IDS) PacketAlarm?

Erkennung von Netzwerkangriffen in Echtzeit

Das netzwerkbasierende IDS PacketAlarm überprüft in Echtzeit den gesamten Datenverkehr auf Ihrem Netzwerk. Es können ein oder mehrere so genannter PacketAlarm-Sensoren in verschiedenen Netzwerksegmenten verteilt werden.

Die Sensoren „belauschen“ permanent den gesamten Datenstrom innerhalb des entsprechenden Netzwerksegmentes ohne die Netzwerkperformance zu beeinträchtigen. Alle „vorbeifließenden“ Daten werden analysiert und laufend auf Netzwerkangriffe (z.B. DoS-Attacken, Exploits, Würmer, unerlaubte Zugriffe) untersucht.



Bewährte und leistungsfähige Scan-Engine

PacketAlarm ist eine extrem leistungsfähige IDS. Die Scan-Engine basiert auf dem wohl am häufigsten verwendeten Open-Source-IDS: SNORT. Es existieren bereits ca. 100.000 SNORT Installationen weltweit.

Einfache Installation und Administration

PacketAlarm verbindet die bewährte SNORT-Engine mit einer einfach zu bedienenden browserbasierenden Managementoberfläche. Durch die „Plug 'n' Secure“-Architektur ist PacketAlarm in nur 5 Minuten installiert und einsatzbereit. Bei der Installation wird PacketAlarm über das Display, bzw. Installationsmenue konfiguriert. Nach dem ersten Aufruf der Managementoberfläche startet sich automatisch der Setup-Wizard, mit dem die Konfiguration durch Beantwortung einiger weniger Fragen spielend leicht vollendet wird.

Automatischer Pattern- und Softwareupdate via Internet

Die bereits vorhandene Basis an Angriffssignaturen ist eine der vielfältigsten und detailliertesten überhaupt und umfasst derzeit mehr als 1.600 bekannte Netzwerkangriffe. PacketAlarm lädt auf Wunsch automatisch die aktuell verfügbaren Angriffssignaturen, ScanEngine- und Softwareupdates aus dem Internet herunter. Die neuen Angriffs-Pattern können sofort und ohne Systemneustart in das Regelwerk übernommen werden. Damit befindet sich PacketAlarm stets auf dem neuesten Stand, und dies ohne administrativen Aufwand.

Automatische Alarmierung von Angriffen und Systemhardening

Je nach Konfiguration von PacketAlarm kann auf die Erkennung von verschiedenen Angriffen mit folgenden Methoden reagiert werden:

- Automatische Alarmierung einer oder mehrerer Personen via E-Mail, WinPopUp oder SNMP-Traps
- Automatische sofortige Terminierung (Beendigung) des Angriffsversuches durch PacketAlarm (TCP RST Paket)
- Automatisches „Hardening“ von anderen Systemen beim Auftreten von Angriffen (z.B. Meldung an eine Firewall, um den Angreifer für einige Zeit direkt durch die Firewall zu blockieren.)





Aufzeichnung und Anzeige der Paketinhalte eines Angriffs

Stellt ein PacketAlarm-Sensor einen Angriff fest, so wird dieser automatisch aufgezeichnet. Dadurch können Netzwerkangriffe auch im Nachhinein problemlos nachvollzogen und die Herkunft einer Attacke ausfindig gemacht werden.

Einfache Erstellung von individuellen Signaturen

PacketAlarm bietet die Möglichkeit, einfach und schnell eigene Signaturen über die Managementoberfläche zu erstellen. Die Regeln können über den Regel-Editor auch in Kombination z.B. nach Source- oder Destination-Adresse, Ports, Pakettyp, Paketgröße oder Inhalt (z.B. Schlüsselwörter, Text oder Hexadezimalzahl) und Häufigkeit des Auftretens innerhalb einer definierten Zeitspanne erstellt werden. Damit können Sie nach Ihren individuellen Wünschen bestimmte Verbindungen alarmieren, terminieren oder auf andere Weise reagieren.

Kommunikation mit zentralen Managementsystemen

Über die integrierte SNMP-Schnittstelle kann PacketAlarm problemlos in zentrale Managementschnittstellen wie HP OpenView oder Tivoli eingebunden werden.

Optimales Monitoring und Autoreporting

PacketAlarm ermöglicht einen vollständigen Überblick über die Vorfälle im Netzwerk. Eine komfortable Abfrage- und Anzeigeoption listet innerhalb eines frei definierbaren Zeitraums die Vorfälle nach unterschiedlichen Kategorien auf. So können die Angriffe nach den befallenen Systemen oder nach ihrer Gefährlichkeit (High, Medium, Low, Info) sortiert dargestellt werden. Möglich ist auch eine Aufstellung nach angegriffenen Systemen. Die Auto-Report-Funktion fasst die wichtigsten Angriffe und Regelverstöße je nach Konfiguration täglich, wöchentlich oder monatlich in einem übersichtlichen E-Mail-Report zusammen.



Nehmen Sie Kontakt mit uns auf:



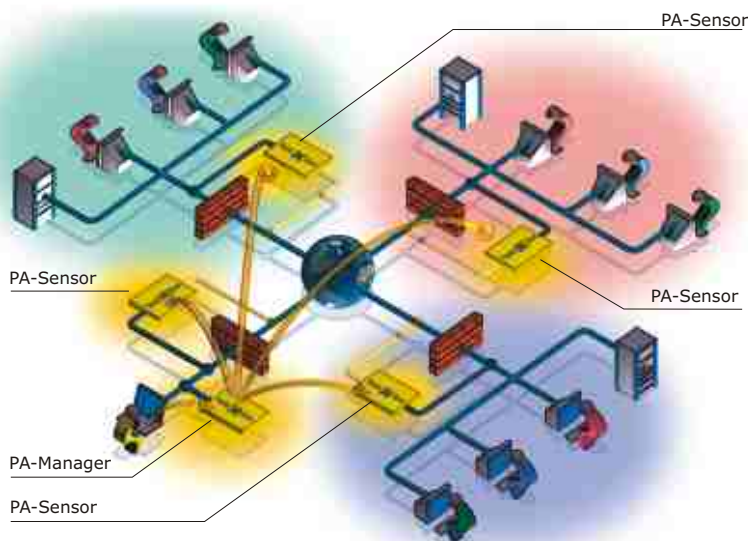
Höchste Performance

Durch die sehr schnelle und optimierte Scan-Engine, und die Verwendung eines extrem schlanken und gehärteten Linux-Kernels erreicht PacketAlarm Spitzenwerte in Sachen Geschwindigkeit.

Zentrales Management durch Sensor/Manager Architektur

Über die integrierte Sensor/Manager Architektur können auch große Infrastrukturen spielend überwacht werden. Einzelne Sensoren können über die gesamte Infrastruktur verteilt und mit einem Manager zentral konfiguriert, administriert und überwacht werden. Der Manager übernimmt den Download der neuesten Patterns und verteilt sie auf die angemeldeten Sensoren. Diese können nicht nur lokal, sondern auch via Internet oder VPNs in Zweigniederlassungen mit zentralen Managern kommunizieren. Damit erhalten Sie einen gesamtheitlichen Überblick über den aktuellen Status Ihrer globalen Infrastruktur.

PacketAlarm kann bei der Erstkonfiguration einfach als Sensor, Manager oder Sensor und Manager auf einem System konfiguriert werden. Dadurch wird in kleineren bis mittleren Infrastrukturen nur ein PacketAlarm System benötigt.



Sicheres Management

PacketAlarm unterstützt standardmäßig zwei Netzwerkinterfaces. Das Sniffing-Interface wird an das zu überwachende Netzwerksegment angeschlossen und besitzt keine eigene IP-Adresse (Stealth-Modus). Dadurch ist PacketAlarm selbst nicht angreifbar. Das Management-Interface kann einfach in einem z.B. durch eine Firewall geschützten Segment platziert werden. Zusätzlich kann über die PacketAlarm Managementkonsole der Managementzugriff auf bestimmte IP-Adressen beschränkt werden. Die Kommunikation zwischen Browser und Manager, sowie zwischen Manager und Sensor ist mittels Verschlüsselung geschützt.

Verfügbare Versionen:

- 🔗 PacketAlarm Appliance mit 10/100 Netzwerkinterface (1HE)
- 🔗 PacketAlarm Appliance mit Gigabit Netzwerkinterface (2HE)
- 🔗 PacketAlarm Softwareversion 100
- 🔗 PacketAlarm Softwareversion 250