

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6
für Linux-Server und -Netzwerke



An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam



7 Intrusion-Detection- und -Prevention-Systeme

Ist Ihre Firewall sicher? Natürlich haben Sie bereits einige Erfahrung in der Konfiguration von Firewalls oder werden dieses Buch aufmerksam lesen, aber sind Sie sicher, dass Sie keinen Fehler machen?

Vielleicht kommt ein potenzieller Angriff auch gar nicht von außen, so dass die Firewall ihn nicht abwehren kann. Viele Angriffe werden von innen ausgeführt. Diese Angriffe müssen die externe Firewall nicht mehr passieren und können daher weder abgewehrt oder protokolliert werden!

Hier helfen Intrusion-Detection- und -Prevention-Systeme. Während ein Intrusion-Detection-System (IDS) keine zusätzliche Sicherheit schafft, sondern nur nach einem Angriff diesen meldet, wehrt ein Intrusion-Prevention-System (IPS) diesen Angriff direkt bei der Erkennung ab. Im Folgenden werde ich Ihnen eine kurze Einführung in die verschiedenen Technologien geben. Weitere Informationen finden Sie in meinem Buch »Intrusion Detection und Prevention mit Snort 2 & Co.« das ebenfalls im Addison-Wesley Verlag erschienen ist.

7.1 Intrusion-Detection-Systeme

Die Intrusion Detection versucht, Einbrüche und Missbrauch zu erkennen und zu melden. Hierzu versuchen die verschiedenen Systeme, sowohl das Netzwerk als auch die Rechner auf Anzeichen eines Angriffs, Einbruchs oder Missbrauchs zu analysieren und im Zweifel einen Alarm auszulösen. Achtung: Die Intrusion Detection verhindert nicht den Einbruch. Sie ist mit einem Feuermelder in einem Haus vergleichbar. Wenn keine Reaktion auf den Feueralarm erfolgt, wird das Haus trotz des Alarms niederbrennen. Für ein erfolgreiches Intrusion-Detection-Konzept ist es erforderlich, dass die Meldungen analysiert und anschließend Reaktionen eingeleitet werden.

Die Intrusion-Detection-Systeme werden allgemein in zwei Gruppen eingeteilt:

- Netzwerkbasierte IDS (NIDS)
- Hostbasierte IDS (HIDS)

Die NIDS beziehen ihre Daten aus dem Netzwerk. Sie analysieren jedes Paket und jede Netzwerkverbindung auf ihre Gültigkeit, auf Angriffsmuster und auf das Vorhandensein von Signaturen bekannter Angriffe. NIDS kämpfen heute vor allem mit zwei Problemen.

1. Die LANs werden immer schneller und transportieren immer mehr Daten. Für die Realisierung dieser LANs wird daher meist eine Paket-Switching-Technologie eingesetzt, die es nicht mehr jedem Rechner im Netzwerk erlaubt, den gesamten Verkehr zu beobachten. Daher müssen NIDS über spezielle Network-Taps oder Spanning-Ports angeschlossen werden. Gleichzeitig sollen die NIDS aber mehrere Systeme, meist ganze Netze, überwachen. Das bedeutet, dass die NIDS heute mit 1-Gbit/s- oder 10-Gbit/s-Verkehr umgehen müssen. Die Anforderungen an die Hardware sind enorm. Meist kann übliche Hardware diese Anforderungen nicht erfüllen und spezielle prozessorunterstützte Netzwerkkarten sind erforderlich.
2. Die wesentlichen Funktionen des NIDS werden immer noch signaturbasiert erreicht. Auch wenn die Signaturen der modernen IDS wie Snort wesentlich besser geworden sind, besteht dennoch die Problematik, dass meist nur für bekannte Angriffe Signaturen existieren. Eine komplette Überprüfung sämtlicher Applikationsprotokolle ist häufig zu aufwändig.

Bei den HIDS gibt es wesentlich mehr Variabilität. Es existieren viele verschiedene Technologien, die ihre Daten von einem Host beziehen und auf unterschiedlichste Weise versuchen, einen Einbruch zu erkennen. Die bekanntesten sind Werkzeuge wie Tripwire, Aide oder Samhain. Hierbei handelt es sich um File Integrity Verifier (auch als System Integrity Assessment bezeichnet). Diese analysieren ein System und melden Änderungen der überwachten Dateien. Sie müssen dann entscheiden, ob die Modifikation der Datei erlaubt war oder ob dies auf eine nicht autorisierte Handlung hinweist. Nachdem Tripwire lange Zeit die am häufigsten eingesetzte Applikation war, kann Samhain seit einigen Jahren eine steigende Zahl an Benutzern vorweisen. Sehr intelligente Funktionen machen es möglich, mit Samhain mehrere Systeme gleichzeitig zentral zu überwachen. Dies ist mit der Open-Source-Variante von Tripwire nicht möglich.

Andere HIDS überwachen die Anzahl der Prozesse, die angemeldeten Benutzer oder den Speicherverbrauch und melden hier ungewöhnliche Zustände. Systeme wie Logwatch oder Logsurfer analysieren die Protokolldateien und erkennen unbekannte Meldungen, die sie anschließend melden. Der Administrator muss nun wieder entscheiden, ob die Meldung harmlos ist oder auf einen Einbruch hinweist.

Da das Thema dieses Buches der Aufbau von Firewalls ist und von mir zum Thema Intrusion Detection bereits ein Buch im Addison-Wesley Verlag (»Intrusion Detection und Prevention mit Snort 2 & Co.«, ISBN 3-8273-2134-4) erschienen ist, möchte ich für weitere Informationen auf diesen Titel verweisen.



Achtung

Bei allem Hype um Intrusion-Detection-Systeme sollten Sie nie vergessen, dass ein Intrusion-Detection-System nie gute Systemadministration, gutes Patchmanagement und eine gute Firewall ersetzen kann. Außerdem vereinfacht ein IDS nicht die weitere Administration, sondern erhöht den Aufwand, da die Meldungen des IDS analysiert und ausgewertet werden müssen. Denken Sie an den Feuermelder, den niemand hört!

7.2 Intrusion-Prevention-Systeme

Im Juni 2003 erklärte die Beratungsfirma Gartner, dass IDS bis zum Jahr 2005 überflüssig werden würden. Dies führte zu viel Verwirrung bei den führenden Anbietern von IDS und ihren potenziellen Kunden. Gartners Schlüsselaussage war, dass Firmen in Zukunft mehr Geld in ihre Firewalls investieren würden, um Angriffe abzuwehren, anstatt in IDS, um die erfolgreichen Einbrüche zu melden.

Diese Aussage weist eine gewisse Logik auf. Jedoch existierten kaum Firewalls, die die Angriffe abwehren können, die ein Intrusion-Detection-System erkennen kann. Die Hersteller von IDS sahen hier ein neues Geschäftsfeld. Die Intrusion Prevention war geboren.

Ein Network-Intrusion-Prevention-System (NIPS) ist die aktive und intelligente Kombination aus Firewall und IDS. Dabei wird der Verkehr von der Firewall gefiltert, und bestimmte Protokolle werden zusätzlich von dem IDS analysiert. Sobald das IDS einen Angriff erkennt, erlaubt die Firewall nicht die Weiterleitung des Netzwerkpakets. Jeder namhafte Hersteller hat seit einigen Jahren NIPS-Produkte in seinem Portfolio.

Genauso haben die Anbieter von HIDS die Entwicklung von Host-Intrusion-Prevention-Systemen begonnen. Diese erkennen zum Beispiel den Versuch einer Dateimodifikation und verhindern diesen direkt. Zusätzlich kann der betroffene Benutzer gleichzeitig abgemeldet werden, können erneute Anmeldungen unterbunden werden oder ähnliche Maßnahmen von dem HIPS eingeleitet werden.

Ein HIPS kann Prozesse beenden oder dafür sorgen, dass ein Prozess immer läuft. Sobald ein bestimmter Prozess versucht, andere unautorisierte Prozesse zu starten (zum Beispiel eine Shell), kann der Prozessaufruf unterbunden werden oder sogar der Elternprozess beendet werden.

Die größte Schwäche dieser IPS sind falsch-positive Angriffserkennungen. Während dies bei einem IDS ärgerlich ist und mit Fine-Tuning recht gut in den Griff zu bekommen ist, ist dies bei einem IPS unverzeihlich. Die Netzwerkverbindung oder der Zugriff auf eine Datei werden effektiv unterbunden. Falls gerade wichtige, nicht wiederherstellbare Daten transportiert oder gespeichert werden sollen, kann ein IPS hohe Verluste erzeugen.

Wenn die Intrusion-Prevention-Systeme in Zukunft zielsicherer werden und die Gefahr falsch-positiver Erkennung zurückgeht, stellen sie eine sinnvolle Ergänzung einer Firewall dar. Wenn Sie heute bereits mit derartigen Systemen experimentieren möchten, empfehle ich Ihnen mein Buch »Intrusion Detection und Prevention mit Snort 2 & Co.« aus dem Addison-Wesley Verlag.