

## IT-SECURITY

# IDS – Big Brother is helping you

Jede Woche beantworten Sicherheits-  
experten Leserfragen und geben  
Ratschläge, wie sich die Sicherheit in  
einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THU



## Frage: Wie lassen sich unlautere Aktivitäten im Firmennetzwerk erkennen und bekämpfen?

Der Bedarf an Sicherheit im Betriebsnetzwerk steigt von Tag zu Tag, denn beinahe stündlich werden neue Sicherheitslöcher, neue Viren oder neue Würmer bekannt. Firmennetzwerke sind konstant Angriffen von aussen, aber auch von innen ausgesetzt. Ein Intrusion-Detection-System (IDS) ist geeignetes Hilfsmittel, um den Netzwerkverkehr zu analysieren und zu protokollieren.

Bei der Datensammlung werden alle Pakete, die das Netzwerk durchlaufen, gesammelt. So kann das IDS einen Angreifer erkennen während dessen er stattfindet und die nötigen Zweigstellen etwa per E-Mail informieren. Bei der Datenanalyse werden die gesammelten Daten analysiert und aufbereitet. Für die Datenanalyse stehen zwei Techniken zur Verfügung:

Die erste Methode ist die Missbrauchserkennung, welche anhand von Mustern (Patterns) Angriffe erkennt. Bei dieser Methode werden die IP-Pakete mittels eines Fingerprints (Fingerabdruck) analysiert. Denn jeder Angriff be-

inhaltet bestimmte Strings oder TCP-Flags anhand deren der Angriff erkannt werden kann. Diese Fingerprints werden anschliessend mit den im IDS vorhandenen Signaturen verglichen und nach Übereinstimmungen von Mustern (Pattern Matching) gesucht.

Die zweite Technik ist die Anomalieerkennung. Als Anomalie wird eine Abweichung vom normalen Netzwerkverkehr definiert. Bei dieser Technik besteht das Problem, dass eine Anomalie nicht immer au-

## Der wichtigste Aspekt beim IDS ist, dass bei der Visualisierung der Angriff so dargestellt wird, dass er für den Systemadministrator verständlich ist und ihm eine zeitnahe Reaktion ermöglicht.

tomatisch auch eine Gefahr darstellt. Deswegen ist eine präzise Abstimmung der IDS-Konfiguration mit den produktiven, «legalen» Applikationen und Systemen nötig. Aufgrund dieses Prozesses ist die Implementationsphase für diese Technik im Vergleich zur auf Mustererkennung basierenden Methode länger.

Weil ein Intrusion Detection System lediglich alarmiert, ohne selbständig weitere Gegenmassnahmen zu ergreifen,

werden die analysierten Daten in der Ergebnisvisualisierung in geordneter Form und mit unterstützenden Kommentaren aufbereitet. So können beispielsweise Web-Interfaces wie ACID, Prewikka nach der Anzahl von Angriffen sortieren und zugehörige Kommentare finden. Zu den Kommentaren gehören sowohl Informationen zu Attacken, Paketen, Source- und Target-IP-Adressen, CVE-(Common Vulnerability and Exposure) oder BID-Nummer (Securityfocus). Der wichtigste

Aspekt dabei ist, dass bei der Visualisierung der Angriff so dargestellt wird, dass er für den Systemadministrator verständlich ist und ihm eine zeitnahe Reaktion ermöglicht.

Ein IDS ist – kurz gesagt – eine Alarmanlage für das Netzwerk. Falls ein Angriff im System entdeckt oder beispielsweise eine Netzwerkkomponente falsch konfiguriert wird (SNMP-Polling, Broadcasting) schlägt das IDS Alarm und benachrichtigt den Administrator.

Intrusion-Detection-Systeme sind leistungsfähige Werkzeuge der IT-Security und in der Netzwerkumgebung, bedürfen aber viel Wartung und Pflege.

Die Konfiguration eines solchen Instruments muss genauestens abgestimmt sein, da es ansonsten Angriffe nicht erkennt oder aber falsche Alarmer schickt – was im Dauerzustand zu einer Abstumpfung des Reaktionsbewusstseins führt. Aus diesem Grund darf der Betrieb eines IDS nicht auf die leichte Schulter genommen werden, weil es – falsch konfiguriert – eine trügerische Sicherheit vermittelt. Wer sich aber für den Betrieb eines IDS entschliesst und genügend Zeit für die Pflege einplant, der hat im IDS einen wirkungsvollen Gehilfen gegen unlautere Aktivitäten im Netzwerk. ■



**Der Autor**  
Oliver Gruskovnjak ist Consultant und OPST bei der Sicherheitsberaterin Oneconsult, Bern. [www.oneconsult.com](http://www.oneconsult.com)

**Unsere Experten beantworten Ihre Fragen.** Schreiben Sie uns: [it-security@computerworld.ch](mailto:it-security@computerworld.ch)

**Ein Archiv der Helpdeskartikel finden Sie im Internet:**  
[www.computerworld.ch](http://www.computerworld.ch)