

# Proaktiver Echtzeit-Schutz mit Intrusion Prevention

Proaktive Sicherheitsmechanismen sind in Zukunft unabdingbar. Unbekannte Angriffe gilt es in Echtzeit zu entdecken und abzuwehren. Es reicht nicht mehr aus, Security-Patches aufzuspielen und Signaturen zu ergänzen. Die Lösung heisst: Intrusion Prevention. *Paul Hasen*



Paul Hasen, dipl. El.-Ing. ETH, ist Verkaufsleiter und Mitglied der Geschäftsleitung bei der bw digitronik ag. Er war 17 Jahre lang in der Software-Entwicklung und Projektleitung tätig und hat international Projekte geleitet. Seit über 10 Jahren befasst er sich als Consultant und Sales Manager mit IT Security.  
[hasen@bwdigitronik.ch](mailto:hasen@bwdigitronik.ch)

Der Bedrohungstrend entwickelt sich in eine eindeutige Richtung: Die Zahl der Sicherheitslücken wächst jährlich. Die Zeit zwischen der Publikation eines Security-Patch und dem ersten Angriff verkürzt sich stetig. Die Geschwindigkeit der Verbreitung von schädlichem Code nimmt rasant zu. Die Folge ist, dass es nicht mehr ausreicht, Security-Patches schnell zu installieren und die Signaturen der Security-Lösungen zu aktualisieren. Um das sogenannte «Window of Vulnerability» zu verkleinern, ist der Einsatz von proaktiven Technologien notwendig. Intrusion-Prevention-Systeme (IPS) wurden entwickelt, um IT-Systeme vor unautorisierten Zugriffen, Schäden und Störungen zu schützen. Neue Netzwerke bieten eine Vielzahl von Diensten an und unterstützen die aktuellsten Kommunikationsstandards. WLANs, Notebooks, Handhelds und internetfähige Handys bereiten IT-Verantwortlichen Kopfzerbrechen. Diese neuen Technologien können dem User die Arbeit erleichtern, öffnen Hackern aber gleichzeitig neue Türen.

## Effiziente Angriffsabwehr

Moderne Intrusion-Prevention-Systeme leisten eine effiziente Angriffsabwehr gegen Bedrohungen wie DoS-Attacken, Buffer-Overflows, Back-Doors, Keyboard-Loggers oder Netzwerkwürmer. Dank der Kombination von verschiedenen Technologien können bekannte und unbekannte Angriffe erfolgreich abgewehrt werden. Die umfassenden Signatur-Datenbanken gewährleisten eine hohe Erkennungsrate für bekannte Bedrohungen. Durch das präzise Scannen von Protokollen können Anomalien im Datenfluss erkannt und neue Attacken gezielt verhindert werden. Informationen im internen Netzwerk werden vor nicht autorisierten Zugriffen geschützt.

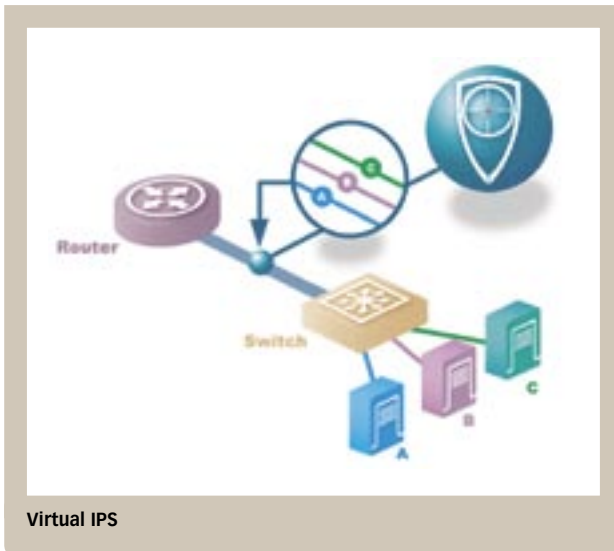
Derzeit gibt es zwei grundlegende Lösungsansätze, mit denen die oben aufgeführten Ziele erreicht werden können: Network-Intru-

sion-Prevention-Systeme (NIPS) und Host-Intrusion-Prevention-Systeme (HIPS). Beide Konzepte bilden eine notwendige Ergänzung zu Firewall und Virenschutz und werden je nach Risikosituation einzeln oder gemeinsam eingesetzt. Angesichts der Dynamik heutiger Bedrohungen gewährleistet eine Kombination aus beiden Ansätzen den grössten Schutz für unternehmenswichtige Daten.

## Network-Intrusion-Prevention-Systeme

Network-Intrusion-Prevention-Systeme werden in dem zu schützenden Netzwerksegment installiert. Sämtliche Daten müssen das NIPS passieren und werden genau gescannt. Die präzise NIPS nutzen verschiedene Technologien, um einen hohen Grad von Verlässlichkeit bei der Erkennung von Angriffen zu erreichen. Extreme Genauigkeit und hohe Leistungsfähigkeit sind für die Effizienz eines IPS entscheidend. Einerseits ist es notwendig, dass der zulässige Datenverkehr bei der Überprüfung nicht verzögert oder unterbrochen wird. Andererseits muss die Fehlerkennung minimiert werden, damit sie den zulässigen Datenstrom nicht behindert. Mit NIPS kann der Datenverkehr von einem Kontrollpunkt aus überwacht werden. Das System ist flexibel und leicht skalierbar. Ein Sensor wird transparent als Knoten in das bestehende Netzwerk integriert. Dadurch entfallen grössere Kosten bei der Installation. NIPS ist plattformunabhängig. Damit können auch unübliche Betriebssysteme oder nicht computerbasierte Systeme im Netzwerk geschützt werden. Einzelne NIPS bieten zusätzlich Schutz vor verschlüsselten Angriffen. Eingehende SSL-Pakete werden entschlüsselt, um eine vollständige Datenüberprüfung zu gewährleisten. Mit der genauen Überwachung des Datenstroms verhindert NIPS Angriffe schon im Netzwerk, bevor sie auf einzelne Hosts gelangen können.

Neue Intrusion-Prevention-Systeme unterstützen Virtual IPS (VIPS). Die sogenann-



Virtual IPS

te Virtualisierung stellt einen bedeutenden Fortschritt dar. Dank dieser Funktion kann ein physikalischer Netzwerk-Sensor in mehrere logische Geräte aufgeteilt werden. So kann ein Administrator einzelne virtuelle Policies für verschiedene Netzwerksegmente erstellen. Mit der Integration von VIPS in die Hardwarearchitektur ist ein Höchstmass an Leistung gewährleistet. Selbst wenn alle Signaturen und Features aktiviert sind, wird mit modernster Technologie auch bei 1000 Virtual IPS Policies ein Durchsatz von mehreren GBit/s unterstützt.

### Schwachstellen in Protokollen

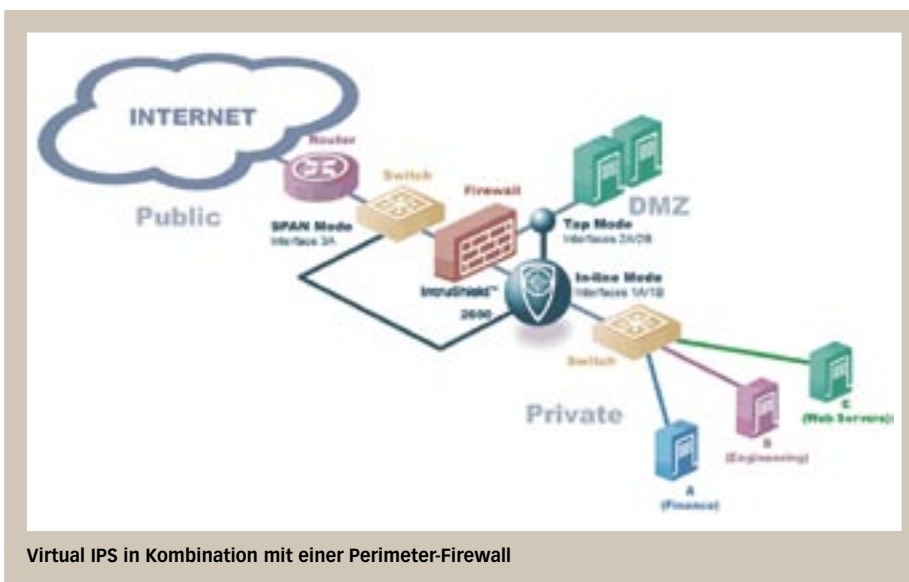
Interessant wird die Anwendung von Virtual IPS in Kombination mit einer Perimeter-Firewall. IPS-Geräte enthalten meistens auch Firewall-Funktionen. So können NIPS in Netzwerken sowohl als IPS wie auch als

So kann die Firewall am Gateway keine versuchte Buffer-Overflow-Angriffe erkennen, die über Port 80 gestartet wird. Für sie handelt es sich um normalen Datenverkehr. Erst durch die Aktivierung der Firewall-Funktionen im IPS kann auch der Netzwerkkern erfolgreich überwacht werden. Sobald ein NIPS verdächtigen Verkehr feststellt, kann es das betreffende Paket sofort löschen und den Rest des Datenflusses blockieren oder markieren. Auf diese Weise wird verhindert, dass bösartiger Datenverkehr in das geschützte Netzwerk eindringen kann. Intrusion-Prevention-Systeme werden häufig zwischen Subnetzen installiert. So kann man mit VIPS den verschiedenen Subnetzen unterschiedliche Sicherheitsrichtlinien zuweisen. Dies gewährleistet eine regelbasierte und spezifische Überwachung des Datenstroms.

Firewall eingesetzt werden. Damit wird der interne Datenverkehr umfassend geschützt. Perimeter-Firewalls blockieren verdächtige Datenpakete am Gateway. Das Problem ist, dass viele Bedrohungen die Schwachstellen in Protokollen ausnutzen, die von Firewalls durchgelassen werden müssen. Dieser Vorgang dient häufig als Sprungbrett für weitere Angriffe auf interne Server.

### «Last Line of Defense»

Ein Host IPS (HIPS) ist eine Software, die auf einzelnen Systemen wie Servern, Workstations oder Notebooks installiert wird. Der Datenverkehr des Hosts wird genau kontrolliert und das Verhalten von Anwendungen und Betriebssystem permanent überprüft. Sobald eine Bedrohung vom HIPS entdeckt wird, kann die Attacke entweder auf Netzwerkschnittstellen-Ebene blockiert werden oder Anfragen an Anwendungen oder Betriebssystem werden gestoppt. So werden etwa Buffer-Overflow-Angriffe erfolgreich abgewehrt. Die Ausführung bösartiger Programme, die sich im Speicher einnisten wollen, wird unterbunden. Versuche, Back-Doors über Anwendungen wie den Internet Explorer zu installieren, werden systematisch abgeblockt. Der vom IE ausgegebene Befehl, eine Datei zu schreiben, wird abgefangen und abgelehnt. Mobile Systeme sind mit HIPS auch ausserhalb des Firmennetzwerks vor Bedrohungen abgesichert. Denn gerade Notebooks werden häufig für Attacken missbraucht. Lokale Angriffe werden vom HIPS so vereitelt, dass die Programmausführung von Datenträgern aus nicht zugelassen wird. Hostbasierte Lösungen bieten zusätzlich Schutz vor verschlüsselten Angriffen. Dabei wird der Datenfluss überprüft, nachdem er auf dem Host-System entschlüsselt wurde. Ein HIPS bildet die sogenannte «Last Line of Defense» im Netzwerk. Angriffe, die andere Sicherheits-Tools umgangen haben, können vom HIPS effizient abgewehrt werden. Eine aktuelle Anwendung ist der Einsatz auf NT4-Servern. Microsoft hat auf Januar 2005 das «End of Support» von NT4 angekündigt. Mit der Installation von HIPS kann deren Lebensdauer verlängert werden, ohne dass die Sicherheit stark eingeschränkt wird.



Virtual IPS in Kombination mit einer Perimeter-Firewall

### Fazit

Zusammenfassend lässt sich sagen, dass der Einsatz von IPS-Technologie eine notwendige Methode darstellt, Netzwerkumgebungen vor den hoch entwickelten Bedrohungen effektiv zu schützen. Kein Unternehmen kann es sich heutzutage leisten, seine Netzwerke und Systeme ohne Firewall und Virenschutz zu betreiben. IPS ist die logische Ergänzung zu herkömmlichen Sicherheitssystemen und wurde entwickelt, um einen proaktiven Echtzeitschutz zu gewährleisten. Unternehmen, die für ihre Sicherheit sorgen wollen, greifen schnell zu dieser neuen Technologie, um mit den rasanten Veränderungen Schritt zu halten. ■