

# Teil IV

## Einsatz in einem Unternehmensnetzwerk



Beim Einsatz von Intrusion-Detection-Systemen in größeren Unternehmensnetzwerken sind häufig Aspekte zu berücksichtigen, die über die bereits besprochenen Funktionen hinausgehen. So nimmt in einem derartigen Netzwerk die Anzahl der zu überwachenden Rechner und der Netzwerke stark zu. Diese Überwachung und ihre Administration wird dadurch sehr aufwändig und zeitintensiv. In einigen Fällen mag sie mit den besprochenen Ansätzen nicht mehr akzeptabel zu lösen sein.

Diese Umgebungen verlangen häufig zentrale Administrations- und Überwachungsmethoden. Der Sicherheitsbeauftragte kann nicht sämtliche von allen Tripwire-Installationen versandten E-Mails täglich lesen und die Snort-Protokolle manuell untersuchen. Die Analyse der

weiteren Protokolle auf zahllosen Rechnern wirft häufig ungeahnte Probleme auf und bei der Korrelation der protokollierten Ereignisse stellt sich oft heraus, dass die Uhren der unterschiedlichen Systeme unterschiedlich falsch gehen. Eine Korrelation der Protokollmeldungen unterschiedlicher Systeme ist daher häufig vollkommen unmöglich.

Dieser Teil versucht verschiedene Techniken an einem hypothetischen Beispielszenario vorzustellen, die eine Lösung dieser Probleme darstellen können. Hierbei werden die zentrale Administration und die Auswertung von Tripwire-Installationen, die Konfiguration von mehreren Snort-Sensoren und ihre zentrale Protokollierung in eine Datenbank, die Implementation eines zentralen Protokollservers und der Einsatz von Zeitsynchronisationssystemen besprochen. Den Abschluss bildet dann die Installation und Implementation von grafischen webasierten Administrations- und Überwachungsanwendungen für Ereignisse im Netzwerk.

Als hypothetisches Beispiel soll das Netzwerk der imaginären Firma nohup.info dienen. Diese Firma besteht aus einer Zentrale mit drei Filialen. Diese Filialen sind mit der Zentrale über ein VPN verbunden und besitzen eigene Zugänge zum Internet. Diese Zugänge werden über einen Squid-Proxy in ihrer demilitarisierten Zone (DMZ) realisiert. Das Netzwerk der Zentrale verfügt ebenfalls über eine Netzwerkverbindung. Über diese Netzwerkverbindung werden zusätzlich Dienste im Internet bereitgestellt. Die entsprechenden Rechner, die diese Dienste zur Verfügung stellen, befinden sich ebenfalls in einer demilitarisierten Zone (DMZ). Dort werden ein Webserver, ein E-Mail-Server und ein DNS-Server für den Zugriff aus dem Internet angeboten. Der Zugriff der Mitarbeiter auf das Internet erfolgt ebenfalls über einen Proxy. Intern befinden sich in dem Netzwerk der Zentrale weiterhin ein E-Mail-Server, ein Samba-Datei- und Druckserver und ein OpenLDAP-Server für die Authentifizierung. Die entsprechenden Paketfilter auf den in der Abbildung als Firewall bezeichneten Systemen wurden entsprechend so konfiguriert, dass die gewünschte Kommunikation erfolgen kann.