HELPDESK

Einbrüche erkennen und verhindern

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

ILLUSTRATION: CW/THÜ

Frage: Welche Leistungsmerkmale zeichnen ein modernes Intrusion-Detection-System aus?

Das primäre Entscheidungskriterium betrifft den Einsatzzweck des Intrusion-Detection-Systems (IDS): Soll es nur zur Identifizierung und Analyse von Einbrüchen dienen oder auch aktive Abwehr von digitalen Einbrüchen ermöglichen? Für ersteres reicht ein herkömmliches IDS. Gilt es jedoch digitalen Einbrüchen mit Gegenmassnahmen zu begegnen, ist der Einsatz eines Intrusion Prevention Systems (IPS) angebracht. Kombinierte Intrusion-Detection-/Prevention-Systeme (IDP) dienen sowohl als technische Einbruchsalarmierungs- sowie als Eindämmungssysteme für die IT-Landschaft.

Ein weiteres Entscheidungskriterium bildet das Lizenzierungsmodell. Es gibt sowohl kommerzielle wie auch nicht-kommerzielle (Open Source) IDS. Wie sich ein Unternehmen entscheidet, hängt dabei oft davon ab, wie viel Know-how- und Betriebs-Ressourcen im Unternehmen zur Verfügung gestellt werden sollen oder können. In den letzten drei Jahren sind bei der Weiterentwicklung von IDS in den Bereichen Integrationsfähigkeit, Betriebseffizienz sowie Performance bedeutende Fortschritte erzielt worden. IDP-Systeme haben sich von eindimensionalen Netzwerk-basierten- (NIDP) und Host-basierten IDP (HIDP) zu Multi-Layer-IDP, auch als hybride IDP bezeichnet, weiter entwickelt. Hybride IDP verfolgen einen integralen Ansatz. Sie bieten Schnittstellen, um bestehende Security-Infrastrukturen wie beispielsweise Monitoring Tools, Log Analyzer und Security Scanner zu integrieren. Durch die Aggregation verschiedener Security Datenquellen bezüglich der OSI-Netzwerklayer 1 bis 7 wird der Erkennungsgrad von sicherheitsrelevanten technischen Vorfällen (Security Incidents) und die Einleitung präventiver Massnahmen maximiert.

«Das Betriebskonzept ist ausschlaggebend für den erfolgreichen Einsatz eines IDS.»

Ein intuitiv gestaltetes Webinterface, welches das zentrale Management der gesamten IDS-Infrastruktur ermöglicht, erlaubt effizientes Arbeiten, was sich positiv auf die Betriebskosten auswirkt. Fortschrittliche Monitoring-, Analyse- und Reporting-Tools ermöglichen die effiziente Kontrolle des aktuellen Sicherheitsstatus. Ein gutes IDP-Frontend sollte präzises Filter- und Regelmanagement ermöglichen, welches die konsequente Anpassung des IPD an die bestehende IT-Landschaft vereinfacht. Ausserdem sollten Incident-Response-Werkzeuge integriert sein, um das IDP-Team bei Alarmen und Sicherheitsvorfällen möglichst effizient zu unterstützen.

Ein IDP-System sollte ausgesprochen skalierbar sein und die individuellen Bedürfnisse und Anforderungen erfüllen. Besonders geeignet sind verteilte, modulare Architekturen, welche es ermöglichen, so viele Sensoren wie benötigt hierarchisch angeordnet einzusetzen und effizient zu managen. So kann das IDS bei Bedarf elegant ausgebaut werden und mit dem Unternehmen wachsen.

Zu guter Letzt sollte die IDP-Infrastruktur den sogenannten Active-active-Failover-Support bieten und katastrophenresistent sein um auch bei gravierenden Sicherheitsvorfällen die Datenintegrität weiterhin zu gewährleisten.

Es darf nicht vergessen werden, dass das Betriebskonzept für den erfolgreichen Einsatz eines IDS ausschlaggebend ist, da sich der Betrieb zu einem wesentlichen Kostentreiber entwickeln kann. Ein IDS bedarf intensiver Betreuung durch ein Spezialistenteam. Die IDS-Alarme müssen regelmässig analysiert und die IT-Infrastruktur gemäss diesen Erkenntnissen rekursiv gehärtet werden. Alarm- und Reaktionsmuster (Signaturen) sind regelmässig zu hinterfragen und allenfalls zu aktualisieren, um mit den Security Entwicklungen Schritt zu halten (IDS Tuning). Denn ein IDS ist nur so gut, wie das Team, welches es betreut. ■

Der Autor
Nicolas Mayencourt ist Direktionsmitglied von Isecom und Dream-lab Technologies, Bern, www.isecom.org.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch