Intrusion Detection

Schutz vor virtuellen Einbrechern

Was passiert in Ihrem Netzwerk? Wissen Sie über alle Aktivitäten Bescheid? In Anbetracht des riesigen Datenaufkommens ist dies von Hand nicht mehr zu bewältigen. Intrusion Detection Systeme, kurz IDS genannt, untersuchen alle Datenpakete auf Manipulationen und geben bei Veränderungen Alarm.

Autor: Andreas Wisler

Was ist ein IDS?
IDS steht für Intrusion Detection System. Ein IDS überwacht und protokolliert den gesamten Datenverkehr des Netzwerkes in Echtzeit und erlaubt es, Unregelmässigkeiten zu erkennen und abzuwehren. Es unterstützt somit eine Firewall, welche nicht zwischen „Gut“ und „Böse“ unterscheiden kann, sondern Datenpakete anhand des Zielportes und eventuell der Ziel-IP passieren lässt. Angreifer können so problemlos Zugriff auf lokale Ressourcen erhalten, Informationen manipulieren und vertrauliche Daten einsehen und auch Datenbestände löschen. Zu bedenken gilt auch, dass Angriffsversuche häufig auch aus dem lokalen Netzwerk heraus gestartet werden, welches Firewallsysteme nicht überwachen.

Arten des IDS

Zum Einsatz gelangen hauptsächlich zwei Arten von IDS-Systemen: auf dem Client (Host IDS) oder im Netzwerk (Network IDS).

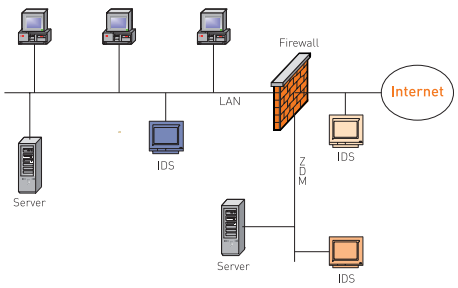
Host IDS (HIDS)

Bei dieser Art des IDS werden auf jedem Host Agents installiert. Diese Agents überprüfen Event-Logs, kritische System-Daten, unautorisierte Zugriffe oder suspekte Daten. Immer wenn etwas nicht in das Schema passt, wird ein Alarm generiert. Zum Beispiel kann ein HIDS die erfolgten Login-Zugriffe überwachen und zu viele falsche Passwort-Eingaben aufzeichnen. Ein anderer Mechanismus ist, den Status eines Systems und der Daten zu überwachen, meistens über einen Snapshot-Mechanismus. Will ein Angreifer oder ein Trojanisches Pferd Veränderungen an dem System erreichen, schlägt das HIDS Alarm.

Network IDS (NIDS)

Diese Systeme beobachten den Netz-Verkehr in Echtzeit um DoS-Attacken („Denial of Service“ Attacke, Versuch, einen Server zu viele Anfragen zu überlasten) oder gefährliche Inhalte zu analysieren, bevor das Ziel erreicht wird. Das wird durch den Vergleich mit einer Datenbank erreicht (Signaturen-Datenbank). Diese Datenbank wird in regelmässigen Abständen gepflegt und erweitert. Wird ein verdächtiger Netz-Verkehr erkannt, kann sowohl ein Alarm gegeben als auch die Verbindung unterbrochen werden. Die meisten heute bekannten Systeme arbeiten im „promiscuous mode”. Das bedeutet, dass alle Pakete eines Segmentes interpretiert werden, egal ob Sie für die IDS-Maschine bestimmt sind oder nicht. Das heisst allerdings auch, dass speziell bei höherer Bandbreite eine erhebliche Anzahl Frames von der IDS-Maschine interpretiert werden müssen.

Viele Angriffe können auch erst erkannt werden, wenn eine Serie von Paketen zum Ziel gelangt ist. Um diese Attacken zu erkennen, müssen diese Pakete von der IDS-Maschine zwischengespeichert werden.



Probleme beim Einsatz von IDS

Der Einsatz von IDS erfordert genaues Planen, zum Beispiel bei der Frage, welche Angriffsziele geschützt werden sollen. Signaturen für den Einsatz von Windows müssen in einer UNIX Umgebung nicht zwingend aktiviert werden. Der Einsatz von so genannten Port-Scannern oder anderen Tools gibt Auskunft darüber, welche Systeme potentielle Ziele sind. Je nachdem, wie diese Ergebnisse ausfallen und welche Bedrohungsszenarien erkannt werden, wird sich auch die einzusetzende IDS Soft- oder Hardware herauskristallisieren. Speziell für NIDS gilt es nicht nur eine Paket-für-Paket-Analyse zu betreiben, sondern auch Serien von Paketen zu beobachten. Fragmentierte Pakete müssen erst wieder zusammengesetzt werden, bevor sie ihr wahres Erscheinungsbild zeigen. Das erfordert grosse und schnelle Puffer wie auch leistungsfähige Maschinen. In rein geswitchten Architekturen gilt es, einen Port so zu konfigurieren, dass alle Pakete dort ausgegeben werden. Ansonsten wird nicht der gesamte Netzwerkverkehr überwacht.

Analyseverfahren

Bei den Analyseverfahren haben sich in den letzten Jahren drei Richtungen herauskristallisiert. Die älteste Methode, Einbrüche festzustellen, ist Misuse Detection. Bei diesem Verfahren wird ein Mustervergleich (Pattern Matching) vorgenommen. Die Daten der Event-Box werden mit Angriffsmustern (Attack Signatures) aus einer Datenbank verglichen. Ist dieser Vergleich positiv, dann wurde eine Verletzung der Security Policy erkannt, und es wird entsprechend reagiert. Im kommerziellen sowie im nichtkommerziellen Bereich ist Misuse Detection immer noch das am häufigsten benutzte Verfahren. Es ist

Kostenloses IDS

Snort ist seit Jahren das beliebteste IDS System auf Open Source Basis. Es bietet die Möglichkeit, den Netzwerkverkehr umfassend zu überwachen. Dies geschieht mit einer Anomaly Detection. Die Regeln können kostenlos heruntergeladen werden. Zur einfachen Auswertung empfiehlt sich das ebenfalls kostenlose ACID.
www.snort.org

einfach zu realisieren und anzuwenden und nicht sehr anfällig für falsche Alarme (False Positives). Der grosse Nachteil dieses Verfahrens ist, dass es nur bekannte Angriffe erkennt, was zur Folge hat, dass neue Angriffe, die sich noch nicht in der Signatur-Datenbank befinden, keinen Alarm auslösen (False Negatives) und somit unbemerkt bleiben.

Um dieses Defizit auszugleichen, wurde ein neuer Weg eingeschlagen und Anomaly Detection entwickelt. Anomaly Detection geht davon aus, dass alles, was nicht zur Menge des „normalen" Verhaltens gehört, ein Angriff sein muss. Diese Methode hat gegenüber Misuse Detection den Vorteil, dass sie es ermöglicht, neue Angriffe zu erkennen, da sie ein abnormales Verhalten darstellen. Zudem muss keine Datenbank mit Angriffsmustern aktualisiert und gepflegt werden. Nachteilig wirkt sich aus, dass zuerst das „normale" Verhalten eines Netzes oder Computersystems erlernt werden muss. Weitere Verfahren heissen Burglar Alarm, Passive Traps, oder Strict Anomaly Detection. Sie kombinieren die beiden Verfahren. Die guten Pakete werden in einer Datenbank abgelegt und können so schnell wieder ausgelesen werden.

IDS – Auch für Ihr Netzwerk?

Die Auswertung der anfallenden Daten ist nicht einfach und sehr zeitaufwendig. Zu Beginn ist mit vielen False Positives zu rechnen. Dies ist ein Grund dafür, dass viele IDS-Konzepte nach kurzer Zeit wieder fallengelassen werden. Es lohnt sich aber auf jeden Fall hier Zeit zu investieren und die Sonden korrekt zu konfigurieren. Sobald diese einmal sauber eingestellt sind, kann das Netzwerk umfassend und sicher überwacht und damit tiefgehend geschützt werden. ◆

Zum Autor

Andreas Wisler (Tel. 052 320 91 20), Dipl. Ing. FH, CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produkteneutralen IT Sicherheitsüberprüfungen und -beratungen auseinander setzt. System Hardening rundet das Portfolio ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) herunter geladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.