DuD
Datenschutz und Datensicherheit

Intrusion Detection Systeme (IDS)

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Grenzen von Firewalls

Die Entwicklung von *Intrusion Detection Systems* (IDS, „Eindringungs-Erkennungs-Systeme") wurde durch verschiedene prinzipielle und praktische Grenzen von Firewall-Systemen motiviert:

- So schützen Firewalls die Systeme eines „inneren" Netzes nur gegen Angriffe von „außen", nicht aber vor internen Angreifern. Statistiken über Angriffe auf Rechnersysteme betonen jedoch immer wieder den großen Anteil von „Innentätern".[1]
- In heutigen Unternehmensnetzen ist ein Internet-Zugang nur noch in den seltensten Fällen ausschließlich über die Firewall des Unternehmens möglich: Modems, ISDN-Karten und vor allem mobile Systeme erlauben oft einen unkontrollierten und ungefilterten Zugang ins Internet.
- Konfigurationsfehler in einer Firewall-Architektur können insbesondere in komplexen Netzarchitekturen nicht ausgeschlossen werden und einem Angreifer das Eindringen über die Firewall ermöglichen.
- Werden Firewalls nicht direkt am System sondern durch Fernzugriff administriert, existiert ein Nutzeraccount auf der Firewall – und damit ein sehr sensibler Angriffspunkt.
- Firewalls sind eine statische Schutzmaßnahme. Neue Angriffsmethoden und unentdeckte Fehler im Betriebssystem des Firewall-Rechners können Angreifern auch bei korrekter Konfiguration ein Eindringen ermöglichen.

Ziel eines IDS ist es, mögliche Angriffspunkte, stattgefundene Angriffsversuche oder sogar durchgeführte Attacken auf ein internes Netz zu entdecken. Intrusion Detection Systeme können daher Firewalls nicht ersetzen, wohl aber die Sicherheitsinfrastruktur eines Netzes ergänzen.

Funktionen eines IDS

Zentrale Funktionen eines IDS sind die folgenden Mechanismen:

- Regelmäßige Überprüfung der Konfiguration der Sicherheitskomponenten (insbesondere Firewalls) durch Analyse der Konfigurationsdateien (passiv) oder sogenannte „Port-Scans" und Angriffssimulationen (aktiv).
- Prüfung der Versionsstände der Software und Betriebssysteme von Sicherheitskomponenten, ggf. Installation von Bug-Fixes oder Updates, die bekannte Probleme beseitigen.
- Auswertung der oft großen und unübersichtlichen Log-Dateien von Sicherheitssystemen sowie verständliche Interpretation der protokollierten Ereignisse.
- Feststellung von Modifikationen wichtiger Dateien (z. B. Konfigurationen) zentraler Sicherheitskomponenten durch die Verwendung kryptographischer Integritätschecksummen.
- Erkennung typischer bekannter „Angreifermuster" durch die Korrelation und Analyse bestimmter Netzaktivitäten.
- Feststellung extrem ungewöhnlicher Netzaktivitäten („Anomalien"), die auf einen Angriffsversuch hindeuten könnten.
- Auslösung von Alarmen bei Angriffserkennung (E-Mail, Sys-/Event-Logs, Alarmsignal).
- Aktive Gegenmaßnahmen bei erkanntem Angriffsversuch durch Konfigurationsänderungen der Firewall (z. B. Filterung der vom Angreifer verwendeten IP-Adresse).
- Reaktion auf Angriffsversuche, ggf. mit irreführenden Antwortpaketen, um Informationen über den Angreifer zu gewinnen.
- Möglicherweise Identifikation der IP-Adresse der Maschine, von der ein Angriff versucht wurde.

Einige IDS-Lösungen erlauben auch die zentrale Administration unterschiedlicher Sicherheitskomponenten eines Netzes über eine benutzerfreundliche Oberfläche.

IDS-Komponenten, die den Netz-Verkehr analysieren („Sensoren"), sind für ein angreifendes System nicht „sichtbar" und können daher nicht ohne weiteres selbst Opfer eines Angriffs werden.

Grenzen von IDS

Ausgereifte Intrusion Detection Systeme sind seit etwa fünf Jahren verfügbar und werden ständig weiterentwickelt. Da sie auf aktuelle Kenntnisse neuer Angriffsmethoden angewiesen sind, ist ein IDS nur so gut wie die Wissensbasis, auf der es beruht.

Bei der Auswahl eines IDS sind neben dem Funktionsumfang, der von System zu System stark variieren kann, vor allem auch die Leistungsfähigkeit zu berücksichtigen:

- ID-Systeme sind grundsätzlich in der Anzahl der TCP/IP-Verbindungen, die sie gleichzeitig analysieren können, beschränkt, da für jede Analyse erhebliche Speichermengen benötigt werden.
- Die fehlerfreie Online-Analyse des Netzverkehrs ist natürlicherweise in der Übertragungsbandbreite bei hoher Netzlast (Performance) begrenzt. So kommen zwar die meisten ID-Systeme mit großen IP-Paketen in 100 Mbit-Netzen zurecht; sind die Pakete aber sehr klein (< 100 Byte), geraten einige Systeme an ihre Grenzen.

Da Zahl und Qualität der im Internet verfügbaren Programme und Hilfsmittel zur Durchführung von Angriffen ständig wächst, werden insbesondere in Sicherheitsinfrastrukturen großer Netzumgebungen Intrusion Detection Systeme zukünftig zweifellos eine immer wichtigere Rolle spielen.

[1] Ob dies auf die inzwischen große Verbreitung von stabilen Firewall-Lösungen oder auf der unvollständigen Erfassung externer Angriffe beruht, sei hier offengelassen.