International Working Group
on Data Protection
in Telecommunications

3. September 2003

Arbeitspapier zu Intrusion Detection Systemen (IDS)[1]

– angenommen auf der 34. Sitzung der Arbeitsgruppe, 2.-3. September 2003, Berlin –

- Übersetzung -

Was ist ein IDS?

Intrusion Detection ist der Prozess des Erkennens unberechtigter Nutzung von Systemen und Netzen unter Nutzung spezieller Software und/oder Hardware.

Ein IDS eröffnet die Möglichkeit, in Echtzeit Netzwerk- und Systemaktivitäten zu beobachten, unberechtigte Aktivitäten zu identifizieren und nahezu in Echtzeit darauf zu reagieren. IDS-Produkte bieten auch die Möglichkeit, gegenwärtige Aktivitäten vor dem Hintergrund vergangener Aktivitäten zu analysieren, um Trends und Probleme in größeren Zeiträumen zu erkennen.

Zweck und Vorteile von IDS

Der primäre Zweck der Durchführung von Intrusion Detection ist, Konsequenzen unentdeckten Eindringens verhindern zu helfen. Die Implementierung eines Programms wirksamer Sicherheitskontrollen ist ein effektiver Ausgangspunkt dafür, die unterstützende Sicherheitsinfrastruktur zu schaffen. Die Fähigkeit, einen Eindringversuch oder seine Vorbereitung in Echtzeit zu erkennen, ist ein wichtiger Aspekt von Intrusion Detection. Das Wissen, wann eine Attacke stattfindet, und die Fähigkeit, unmittelbar zu handeln, erhöhen die Wahrscheinlichkeit signifikant, Eindringversuche erfolgreich zu beenden und zu ihrer Quelle zurückzuverfolgen. Echtzeit-Erkennung hängt von der Existenz eines Überwachungssystems ab, das im Hintergrund angesiedelt ist und alle Aktivitäten einschließlich der angeschlossenen Geräte überwacht. Das Überwachungssystem muss in der Lage sein, verschiedene Ereignisse zu interpretieren und tatsächliche Attacken zu diagnostizieren.

Die meisten traditionellen IDS arbeiten entweder nach einem netzwerk- oder einem rechnerbasierten Ansatz zur Identifizierung von und zum Schutz gegen Attacken[2]. In beiden Fällen suchen IDS nach „Signaturen“ von Attacken,spezifischen Mustern, die normalerweise auf böswillige Absichten oder verdächtige Aktivitäten schließen lassen. Ein wirklich effektives IDS wird beide Methoden anwenden.

[1] Dt.: etwa „Einbruchs-Erkennungssysteme“
[2] Siehe den technischen Anhang für weitere Informationen.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

Datenschutzprobleme

Da IDS viele Verkehrs- oder Ereignisdaten sammeln und aufzeichnen, die sicherlich auch personenbezogene Daten enthalten, dürften die Datenschutzbedenken auf der Hand liegen.

In diesem Zusammenhang hält es die Arbeitsgruppe für notwendig, die Aufmerksamkeit aller Verantwortlichen für die Entwicklung von IDS auf die folgenden Punkte zu lenken: Die Erkennung und Abwehr von Einbrüchen erfordert bei der Suche nach Angriffs-„Signaturen“ oder spezifischen Mustern, die normalerweise auf böswillige oder verdächtige Absichten hindeuten, die Analyse des Netzverkehrs und von Protokollierungsdaten von Betriebssystemen.

Die gesammelten Netzwerkverkehrs- oder Ereignisdaten können personenbezogene Daten enthalten, d. h. Daten, die einer bestimmten Person zugeordnet werden können. Die Geräte- oder IP-Adresse kann ein Beispiel eines solchen Datums sein. Daher könnte Intrusion Detection als ein Instrument zur Überwachung von Nutzern und ihrem Verhalten genutzt werden. Wenn Intrusion Detection genutzt werden soll, um „interne“ Eindringlinge, d. h. Mitarbeiter einer Organisation, zu erkennen, müssen die Auswirklungen bedacht werden.

Drei Prinzipien, die die Herausforderung für den Datenschutz darstellen, sollten beim Einsatz von Intrusion Detection berücksichtigt werden:

?? Intrusion Detection muss dem Zweck der Datensicherheit oder des Systemschutzes dienen,

?? die Speicherung der Daten (Netzwerk-Pakete, Audit-Logs) muss dem Schutzzweck angemessen sein,

?? eine Festlegung (policy), die die Anforderungen an den Schutz personenbezogener Daten abdeckt, die in IDS gespeichert werden, sollte entwickelt und angewandt werden.

Der erste Aspekt betrifft die Vereinbarkeit der Überwachung des Verhaltens von Nutzern/Beschäftigten mit Zielen der Intrusion Detection.

Der zweite Aspekt betont, dass nur solche Daten gesammelt und analysiert werden sollten, die zur Erkennung von Attacken erforderlich sind. Nach dem Vergleich von Ereignisdaten mit Angriffs-„Signaturen“ des IDS sollten Daten, die nicht länger benötigt werden oder für die kein Hinweis auf einen Angriff bestand, gelöscht werden; die relevanten Daten, die auf einen Angriff hindeuten, sollten in sicherer Weise gespeichert werden. Allerdings kann die Löschung der Daten unter bestimmten Umständen nicht angemessen sein; Ereignisdaten könnten für eine spätere Untersuchung archiviert werden müssen, z. B. zum Zwecke der Rückverfolgung zum Angreifer oder für die spätere forensische Analyse. Einige Daten mögen zunächst unbedenklich erscheinen. Nach weiterer Analyse könnte sich herausstellen, dass sie mit einer Attacke zusammenhängen. Die Korrelation mit später erhobenen Daten könnte auch den Zusammenhang mit einer Attacke beweisen. In jedem Fall und aus verschiedenen Gründen einschließlich des Datenschutzes sollten die Daten umfassend gegen unberechtigte Zugriffe geschützt werden. Die getroffenen Maßnahmen sollten mit der Sicherheitspolitik der Organisation im Einklang stehen.

Der dritte Punkt bedeutet, dass die Vertraulichkeit personenbezogener Daten geschützt und im Einklang mit der generellen Datenschutzpolitik einer Organisation oder mit Rechtsvorschriften, die auf sensible personenbezogene Daten anzuwenden sind, praktiziert werden muss.

Gegenwärtig existieren nur sehr wenige spezielle gesetzliche und regulatorische Anforderungen im Zusammenhang mit Intrusion Detection. Es wird erwartet, dass Gesetze oder Regelungen sich herausbilden, die für einen adäquaten Schutz der Privatsphäre von Individuen sorgen und gleichzeitig

IDS und damit zusammenhängenden Aufzeichnungen über Ereignisse erlauben, hinreichend viele Daten zu speichern und zu nutzen, um potentiell schädliche Einbrüche zu erkennen. Bereits jetzt enthalten einige nationale Regelungen das Kriterium der Angemessenheit und der Zweckbestimmung der Nutzung personenbezogener Daten. Einige Länder verfügen über Regelungen hinsichtlich des Schutzes personenbezogener Daten von Arbeitnehmern und von Rechten der Arbeitnehmer, am Schutz ihrer personenbezogenen Daten mitzuwirken. Zusätzlich können verschiedene nationale Regelungen und Verträge über grenzüberschreitende Datenflüsse Intrusion Detection und Datenschutz beeinflussen.

Einige nationale Gesetze und Regelungen verlangen, dass, falls die Überwachung von Aktivitäten von Einzelpersonen stattfindet, z. B. durch Ereignisaufzeichnung und IDS -spezifische Sensoren oder Überwachungsagenten, Arbeitnehmer und Vertragsnehmer in besonderer Weise darüber informiert werden und dies bestätigt haben müssen, bevor solche Maßnahmen ergriffen werden. Dies könnte in der Form unterschriebener arbeitsvertraglicher Regelungen oder einem gesonderten Schreiben oder jeglichem anderen Weg erfolgen, der im Einklang mit der nationalen Gesetzgebung steht.

Die Grundbegriffe dieser Erwägungen, die den Datenschutz betreffen, sind bereits von einigen Datenschutzbehörden formuliert[3] und insbesondere in dem geänderten Entwurfstext des folgenden Entwurfs für einen Standard integriert worden:

?? ISO/IEC WD 18043, „Richtlinien für die Herstellung, den Betrieb und die Verwaltung von Intrusion-Detection-Systemen (IDS)“.

Im Hinblick auf die gegenwärtigen Entwicklungen im Zusammenhang mit der Stardardisierung unterstützt die Arbeitsgruppe in vollem Umfang die Integration der oben genannten Erwägungen in alle internationalen, regionalen und nationalen Standards, die die oben erwähnten Angelegenheiten des Datenschutzes betreffen.

[3] Die belgische Datenschutzbehörde ist in dieser Hinsicht besonders aktiv gewesen.

Technischer Anhang

Prinzipielle Typen von IDS

Rechner-basierte IDS

Rechner-basierte Intrusion Detection begann in den frühen 80er Jahren, bevor Netzwerke so vorherrschten und so komplex und miteinander verbunden waren, wie sie es heute sind. In dieser einfachen Umgebung war es eine gängige Praxis, Protokolldateien nach verdächtigen Aktivitäten zu durchsuchen.

Rechner-basierte IDS nutzen nach wie vor Protokolldaten, tun dies aber stärker automatisiert und haben sich zu durchdachteren und reaktionsschnellen Erkennungstechniken entwickelt. Rechnerbasierte IDS überwachen typischerweise Systeme, Ereignisse und Protokolldateien. Wenn eine dieser Dateien verändert wird, vergleicht das IDS den neuen Eintrag mit Angriffs-„Signaturen“, um Übereinstimmungen herauszufinden. In diesem Fall antwortet das System mit der Alarmierung von Systemverwaltern und anderen Hinweisen auf Handlungsbedarf. Es überwacht Dateien im System im Hinblick auf Veränderungen. Der primäre Zweck Rechner-basierter IDS besteht in der Überwachung von Systemen hinsichtlich einzelner Dateiveränderungen.

Rechner-basierte IDS sind um andere Technologien erweitert worden. Bei einer gängigen Methode zur Erkennung von Einbrüchen werden wichtige Systemdateien und ausführbare Dateien durch Checksummen in regelmäßigen Abständen auf unerwartete Veränderungen überprüft. Die Reaktionszeit hängt direkt von der Frequenz der Kontrollinterwalle ab. Schließlich überwachen einige Produkte Port-Aktivitäten und alarmieren Administratoren, wenn auf bestimmte Ports zugegriffen wird. Diese Art der Kennung integriert ein grundlegendes Maß Netzwerk-basierter Intrusion Detection in die Rechner-basierte Umgebung.

Netzwerk-basierte IDS

Netzwerk-basierte IDS nutzen „rohe“ Netzwerkpakete als Datenquelle. Typischerweise benutzen Netzwerk-basierte IDS Adapter, die im „Promiscuous Mode“ angewandt werden, zur Überwachung und Analyse des Netzwerkverkehrs in Echtzeit. Der „Promiscuous Mode“ macht es für einen Angreifer extrem schwer, die Überwachungsmaßnahme zu erkennen und zu lokalisieren.

Die Funktionalität zur Angriffserkennung benutzt drei gebräuchliche Techniken, um die Signatur einer Attacke zu erkennen:

?? Statistische Erkennung von Anomalien

Im Anomalieerkennungs-Modell erkennt das IDS ein Eindringen, indem es nach Aktivitäten sucht, die von dem normalen Verhalten eines Nutzers oder eines Systems abweichen. Anomalie-basierte IDS erkennen Grundregeln normalen Verhaltens durch Profilbildung für einzelne Nutzer oder Netzwerkverbindungen und durch die Überwachung von Aktivitäten, die davon abweichen.

?? Muster-, Befehls- oder Byte-Code-Vergleich

Die Mehrzahl der kommerziellen Produkte basiert auf Verkehrsanalysen, in denen nach dokumentierten Mustern von Angriffen gesucht wird. Dies bedeutet, dass das IDS programmiert wird, jede bekannte Exploit-Technik zu identifizieren. Dies kann so einfach wie ein Vergleich von Mustern ausgestaltet sein. Das klassische Beispiel besteht darin, jedes Muster in einem

Netzwerksegment nach einem definierten Aktivitätsmuster zu durchsuchen, das auf einen Versuch hinweist, auf ein gefährdetes Skript auf einem Webserver zuzugreifen. Einige IDS bauen auf großen Datenbanken auf, die Tausende solcher Muster enthalten. Das IDS überwacht jedes Paket auf der Suche nach Paketen, die eines dieser definierten Muster enthalten.

?? Zusammenschau mit weniger gravierenden Vorfällen