Ludwig-Uhland-Straße 3, 04435 Schkeuditz

Telefon +49.34204.62598 Fax +49.34204.64490

CSC MANN GmbH
INTERNET INTRANET SECURITY

IDRS - Intrusion Detection and Response System

Ein IDS/IDR überwacht und protokolliert den gesamten Datenverkehr des Netzwerkes in Echtzeit und erlaubt es Unregelmäßigkeiten zu erkennen und abzuwehren. Sowohl an einzelnen Systemen, im internen und externen Netzwerkbereich können Angriffsversuche erkannt und entsprechend behandelt werden.

Auch bei sorgfältig geplanter Absicherung des lokalen Netzwerkes können umfassende Firewallkonzepte unter Ausnutzung entsprechender Lücken in der Konzeption desselben oder der verwendeten Software umgangen werden. Angreifer können so problemlos Zugriff auf lokale Ressourcen erhalten, Informationen manipulieren und vertrauliche Daten einsehen und auch Datenbestände löschen. Die Beschreibung für diese Angriffsversuche ist sehr detailliert im Internet frei nachzulesen. Entsprechende Tools sind ebenfalls im Internet und über die CD der gebräuchlichsten Computerzeitschriften zu bekommen. Zu bedenken ist auch, daß Angriffsversuche häufig auch aus dem lokalen Netzwerk heraus gestartet werden, welche Firewallsysteme - sofern überhaupt möglich - nicht überwachen.

Da Firewallsysteme meist technisch bedingt nur Datenströme für einzelne Verbindungen vergleichen, werden die für Angriffsversuche typischen unterschiedlichen Verbindungen und Dateninhalte nicht erkannt. Auch Contentscanner (Viren- und Mail-Filter) erkennen nur einzelne Datenpakete. Mit einem IDS wird jedoch der Datenverkehr verschiedener Teilnetzwerke und Systeme gemeinsam und gleichzeitig überwacht. Zielgerichtet werden so Störungen (Intrusion) erkannt (Detection) und Reaktionen (Response) herbeiführt.

Wir stellen ein optimal zugeschnittenes System zur Verfügung, das nicht nur als sogenanntes kombiniertes IDS arbeitet - indem es sowohl einzelne Systeme (Host-IDS) und Netzwerksegmente (Netz-IDS) in Summe überwacht – sondern auch die bei den meisten Systemen grundlegend verschiedenen Funktionsweisen – signaturbasierend, anomalieerkennend und protokollanalysierend - eines ID Systems in nahezu idealer Weise miteinander verbindet. Zusätzlich wurde dieses System mit umfangreichen Report- und Reaktionsfunktionen erweitert.

Unser kompetentes Entwicklungsteam wird gemeinsam mit Ihnen Ihre IDRS Lösung umsetzen. Sie erhalten alle notwendigen Leistungen zur Umsetzung und zum Betrieb Ihrer Vorhaben aus einer Hand und benötigen dabei nur einen Ansprechpartner. Unsere IDRS Leistungen im Überblick :

Beratung	-	Analyse des Schutzbedarfes im Netzwerk
	-	Auswahl passender Komponenten
	-	Planung eines IDRS Konzeptes
Lieferung	-	Managementserver
	-	Netzwerk- und Hostsensoren
	-	Zusätzliche Soft- und Hardwarekomponenten
Service	-	Installation von Hard- und Software
	-	Einrichtung und Einweisung
	-	Schulung für Administratoren, Anwender und Kunden
	-	Entwicklung individueller Signaturen und Plugins
Support	-	tägliche Updates für Signaturen
	-	24 Stunden Hotline via Email und Telefon
	-	Updates zur IDRS Software

Unseren Kunden bieten wir umfangreiche Unterstützung und Beratung. Sie werden durch das Support-Team betreut, das per Telefon, Email oder Fax erreichbar ist. Im Rahmen der Anbindung werden technische Unterlagen sowie Benutzerdokumentationen als zusätzliche Unterstützung zur Verfügung gestellt.

Setzen Sie sich mit uns in Verbindung. Wir stellen Ihnen gern einen Gast-Zugang auf unserem Demo-IDRS zur Verfügung, oder vereinbaren Sie mit uns die Leihstellung für eine IDRS Lite-Version.

Ludwig-Uhland-Straße 3, 04435 Schkeuditz

Telefon +49.34204.62598 Fax +49.34204.64490

CSC MANN GmbH
INTERNET INTRANET SECURITY

Die Merkmale unseres IDRS im Überblick

Kombination von host- und netzwerkbasierenden IDRS

Ein **Host-IDS** wird zur Überwachung von Unzulänglichkeiten im Programmablauf, der Benutzeraktivitäten, unberechtigten Zugriffen, u.a.m. auf einem einzelnen System genutzt. Neue Sensoren werden automatisch vom IDS erkannt und integriert. Es werden verschiedene Betriebssysteme für Server und Netzwerkkomponenten unterstützt (Windows, Linux, Solaris, HP-UX, Cisco IOS, Bintec, Lucent, 3COM, u.a.).

Das **Netzwerk-IDS** dient zur Analyse und Protokollierung des Datenstromes in einem Netzwerksegment. Die Anzahl der Sensoren und deren Bandbreite ist nur durch die Kapazität der verwendete Hardware begrenzt. Die Überwachung der Sensorfunktionen sowie deren Steuerung erfolgt automatisch und zentral über den Managementserver.

Verbindung der grundlegenden IDS Methoden signaturbasierend, anomalieerkennend sowie protokollanalysierend

Signaturbasierende Funktionen erkennen aktiv Angriffszenarien auf Grundlage von bekannten und hypothetischen Datenmustern, die in Form von Signaturen verwaltet und mit dem spezifischen Inhalten aus dem Datenstrom verglichen werden. Tägliche Updates der bekannten Signaturen, die Möglichkeit eigene Signaturen zu erstellen, sowie einstellbare Vorfilter erweitern den normalen Leistungsumfang dieser Funktionen erheblich.

Funktionen zur **Anomalieerkennung** vergleichen die Parameter des laufenden Benutzerverhalten im Netzwerk und zeigen Abweichungen von diesem Normalzustand. Die archivierten Datenbestände sind in mehreren Zeitbereichen vergleichbar.

Bei der **Protokollanalyse** wird davon ausgegangen, daß Datenpakete im wesentlichen immer den gleichen Aufbau haben. So kann sehr gezielt und mit hoher Geschwindigkeit nach bestimmten Vorgängen im Datenstrom gesucht werden.

Leistungsfähige Datenbank und optimierte Software

Die **integrierte Datenbank** verwaltet zentral alle Vorfälle, Signaturen und Benutzerdaten. Sie ist **selbstwartend** und paßt sich automatisch dem Umfang des IDRS an. Die Größe des Datenbestandes ist allein durch die verwendete Hardware des Servers begrenzt.

Grundlage für das Betriebsystem der Netzwerksensoren und des Managementserver ist ein angepaßtes Linuxsystem, daß sich durch **hohe Leistungsfähigkeit und stabilen Betrieb** auszeichnet. Optional stehen andere Betriebssystem zur Verfügung.

Ein zentraler Baustein im IDRS ist „Snort“. Diese **extrem leistungsfähige Scan- und Search-Engine** analysiert und protokolliert den Datenstrom der Netzwerksensoren. Die auf der Basis „Open-Source“ entwickelte Software wurde bereits über 60.000 mal installiert.

Spezielle Anpassungen

Optional stehen für verschiedene Anwendungen zusätzliche Module im IDRS zur Verfügung.

Mit dem **ISP-Modul** lassen sich Zugriffsbeschränkungen für verschiedene Benutzergruppen auf Basis von IP-Adressen verwalten. So besteht die Möglichkeit verschiedene, getrennte Netzwerke in einem IDRS gemeinsam zu überwachen und zu managen.

Das **Content-Security-Modul** verschlüsselt den gesamten Dateninhalt der archivierten Ereignisse mit mehrfachen Paßwörtern, so das diese nur nach dem sogenannten „Mehraugen-Prinzip“ geöffnet werden können.

Ludwig-Uhland-Straße 3, 04435 Schkeuditz

Telefon +49.34204.62598 Fax +49.34204.64490

CSC MANN GmbH
INTERNET INTRANET SECURITY

IDRS – Managementserver

Der Managemenserver ist die Zentrale des Systems. Über ein integriertes benutzerfreundliches Webinterface wird das gesamte IDRS kontrolliert, verwaltet, überwacht und ausgewertet. Die enthaltenen selbstwartenden Datenbanken, die Backup-, Steuer- und Absicherungsfunktionen, sowie der integrierte Firewall bieten die Möglichkeit komplexe Vorgänge und Aufgaben zu lösen. Es wird eine optimale Nutzung des Management, der Datenerfassung und Archivierung, der Vorgangsanalyse und Aggregation, Datenanalyse, Reporterstellung und Alarmverarbeitung innerhalb des IDRS ermöglicht.

Sicherheit im Zugriff

Der Zugriff auf das System und damit auf den Managementserver erfolgt über einen separaten unabhängigen Netzwerkanschluß. Die **integrierte Sessionverwaltung** regelt den gleichzeitigen und mit SSL verschlüsselten Zugriff der Benutzer (auf verschieden Ebenen über Timeout-, Paßwort- und Absenderüberprüfungen) auf den Managementserver.

Zentrales Systemmanagement

Die Webschnittstelle bietet eine umfangreiche und **leistungsstarke Oberfläche** mit einer **einfachen Menüstruktur**. Über Sie werden im **zentralen Management** die Benutzer des IDRS und deren Zugriffsberechtigungen, die Steuerung und Überwachung der Sensoren, die Verwaltung und die Updates der Signaturen sowie die Konfiguration der Reports und Reaktionen vorgenommen. Zur Optimierung der Benutzerführung wurden eine **Online-Hilfefunktion** und eine **Cachefunktion für Grafiken** integriert.

wartungsfreie Datenbanken und Echtzeitverarbeitung

Über eine **lokale Wissensdatenbank** werden Angriffsmuster, Programmfehler und regelwidrige Anwendungen in Form vom Signaturen gespeichert, die **tägliche aktualisiert** werden. Zusätzlich wird das Erstellen eigener Signaturen und die Verwaltung sogenannter Vor-Prozessoren unterstützt. Die Verwaltung dieser und deren Verteilung auf den Sensoren läßt sich zentral steuern. Die von den Sensoren gescannten Vorfälle werden in **Echtzeit** erfaßt, in Beziehung gebracht, ausgewertet und in der Datenbank archiviert. Somit lassen sich diese im Bedarfsfall auch über einen größeren Zeitraum rekonstruieren.

Integrierte Reportfunktionen

Um die verschiedenen Ereignisse und Systeme in übersichtliche und logische Verbindungen zu bringen, sind zahlreiche **frei konfigurierbare Reportfunktionen integriert.** Es stehen verschiedene, auch **graphisch unterstützte Auflösungsebenen** zur Verfügung. Die Konfiguration der Reportfunktionen erlaubt die Verwendung nahezu aller möglichen Parameter, wie z.B. Signaturen, Sensoren oder IP-Adressen, die bezogen für verschiedene Zeiträume genutzt werden können.

Frei konfigurierbare Reaktionen

Zur Analyse der gespeicherten Vorfälle stehen neben dem passiven Modus auch **aktive, individuell einstellbare Reaktionen** (Response) zur Verfügung. Dazu gehören neben dem typischen Versand von Nachrichten auch Echtzeit-Eingriffe in den Datenverkehr, um beispielsweise den Datenverkehr auf einem Firewall für bestimmte Adressen und/oder Ports zu sperren. Der Zugriff auf Anwendungen kann unterbunden werden oder auch komplette Netzwerksegmente können abgetrennt werden. **Typische Anwendungen** für aktive Reaktionen sind der Versand von Email und SMS, die Erweiterung der Filtersätze für Firewallsysteme und andere Netzwerkkomponenten (z.B. Linux, Checkpoint, BSD, Cisco, Lucent, Bintec).
In den Report- und Reaktionsfunktionen sind **zusätzliche Tools** eingebunden, aus denen tiefergehende Detailabfragen zu verschiedenen Vorfällen direkt nutzbar sind. Dazu gehören zum Beispiel Verweise auf die Webseiten der verschiedenen Referenzserver, Abfragen der Whois-Datenbanken und einfache Netzwerktests (z.B. DNS, Ping, Traceroute).

IDRS - Netzwerksensoren

Mit den Netzwerksensoren steht ein extrem effizientes und hochprofessionelles System zur Verfügung, mit dessen Überwachungstechnik die Datenströme des Netzwerkes analysiert und überprüft werden können. Grundlage für diesen Sensortyp ist hauptsächlich die weltweit marktführende Search- und Scan-Engine auf „Snort“ Basis.

LAN und WAN Anwendung

Eine Kopplung mehrerer Netzwerksensoren ist möglich. Durch sie ist es auch möglich **größere Netzwerke leicht und abgesichert zu überwachen**. Problemlos können auch entferntere und räumlich getrennte Netzwerksegmente integriert und kontrolliert werden.

Angepaßte Hard- und Software

Die Netzwerksensoren basieren im Betriebsystem auf einem schlanken und angepaßten Linuxsystem. Die verwendete Hardware ist speziell optimiert. Für diese stehen umfangreiche Support- und Serviceoptionen zur Verfügung. Die sehr leistungsfähigen Sensoren genügen somit **höchsten Ansprüchen in der Performance**.

Optimaler Schutz

Durch die **vorinstallierte Konfiguration** der Sensoren sind diese gegen Angriffe auf System-Ebene selbst resistent. Angriffe auf die Search- und Scan-Engine selbst werden durch Umordnung der fragmentierten Pakete und Datenströme sowie laufende Updates umgangen.

Steuerung und Wartung

Die Steuerung des/der Netzwerksensoren erfolgt ebenso zentral über den Managementserver wie die Verteilung und Konfiguration der Signaturen. Updates der Signaturen erfolgen während des Betriebes; ohne einen Neustart – und somit Datenverlust - des Systems. Zusätzlich steht eine Option zur Verfügung die neue Konfigurationsparameter unabhängig vom eigentlichen Sensor selbst auf Ihre Lauffähigkeit hin überprüfen kann. Damit sind die Netzwerksensoren selbst vollständig **wartungsfrei**.

Zusätzliche Optionen

Außer der eigentlichen Überprüfung des Datenstromes nach Signaturen stehen verschiedene Vor-Pozessoren im Netzwerksensor zur Verfügung. Diese führen komplexe Stateful Protokollanalysen durch, um Unregelmäßigkeiten wie DoS-Attacks, ARP-Spoofing, Stack-Fingerprinting und Portscans frühzeitig zu erkennen und zu protokollieren.

Minimierte Fehlalarme und Lastprobleme

Durch die **fortlaufenden Updates der Signaturen** während des Betriebes, den vom Benutzer angelegten Signaturen und vor allem durch eine individuelle Verwaltung jedes einzelnen Sensor selbst ist ein optimaler Betrieb gesichert, der Fehlalarme auf ein Minimum begrenzt.
Seit der Version 2.x der „Snort“ Software wird auch eines der größten Probleme bei Netzwerksensoren ausgeschlossen. Bei hohem Datenverkehr – und damit verbundener hoher Last – können verschiedene Sensoren diesen meist nicht mehr vollständig überwachen und protokollieren. Die neue Version umgeht diesen Engpaß durch **optimierte Suchroutinen,** einer **Richtungserkennung des Datenverkehrs** und damit angepaßter Geschwindigkeit.

Statistik und Auswertung

Über den Managementserver stehen **detaillierte Auswertungen** zum Last- und Scanverhalten der Sensoren selbst - mit verschiedenen Einzelwerten und graphisch aufbereitet - zur Verfügung. Die Ergebnisse der Überprüfungen der Datenströme werden auf dem Managementserver in Echtzeit gespeichert und lassen sich über Report- und Reaktionsfunktionen verarbeiten.

Unsere Angebote

1) Leihstellung

- Planung, Lieferung und Betrieb einer IDRS Demoversion

2) IDRS Lite-Version

- geeignet für System mit einem Datendurchsatz bis ca.1 TB pro Monat
- Integriertes System, auf Basis eines Servers
- Management, ohne Userverwaltung
- Netzwerksensor mit Fastethernet Anschluß

3) Managementserver

- integrierte Userverwaltung
- optional weitere Module

3.1) Typ „Medium“
- für Netzwerke mit bis zu 5 Netzwerksensoren und mittlerem Datenaufkommen

3.2) Typ „Big“
- für Netzwerke ab 5 Netzwerksensoren und größerem Datenaufkommen

4) Netzwerksensor

4.1) Typ „Medium“
- 1 Anschluß Netzwerk 100 MB (Fastethernet)

4.2) Typ „Dual“
- 2 Anschlüsse 100 MB (Fastethernet)

4.4) Typ „Big“
- 1 Anschluß 1GB (Gigaethernet)

5) Hostsensoren

5.1) Betriebsystem Linuxsystem
- Einrichtung Hostsensor auf einem Linuxsystem

5.2) Hostsensor Unix
- Einrichtung Hostsensor auf einem Unixsystem

5.3) Hostsensor Windows
- Lizenz Software
- Einrichtung Hostsensor unter Windows

6) Support und Service

- Updates von Signaturen (täglich)
- Updates der Software (Managementserver und Sensoren)
- Support via Email und Telefon

7) Zusätzliche Module

7.1) „ISP“ Modul
- getrennte Zugriffsberechtigung für User (auf Basis IP-Adressen)

7.2) „ME“ Modul
- Zugriff auf Detailinformationen nur nach dem sogenannten „Mehraugenprinzip“