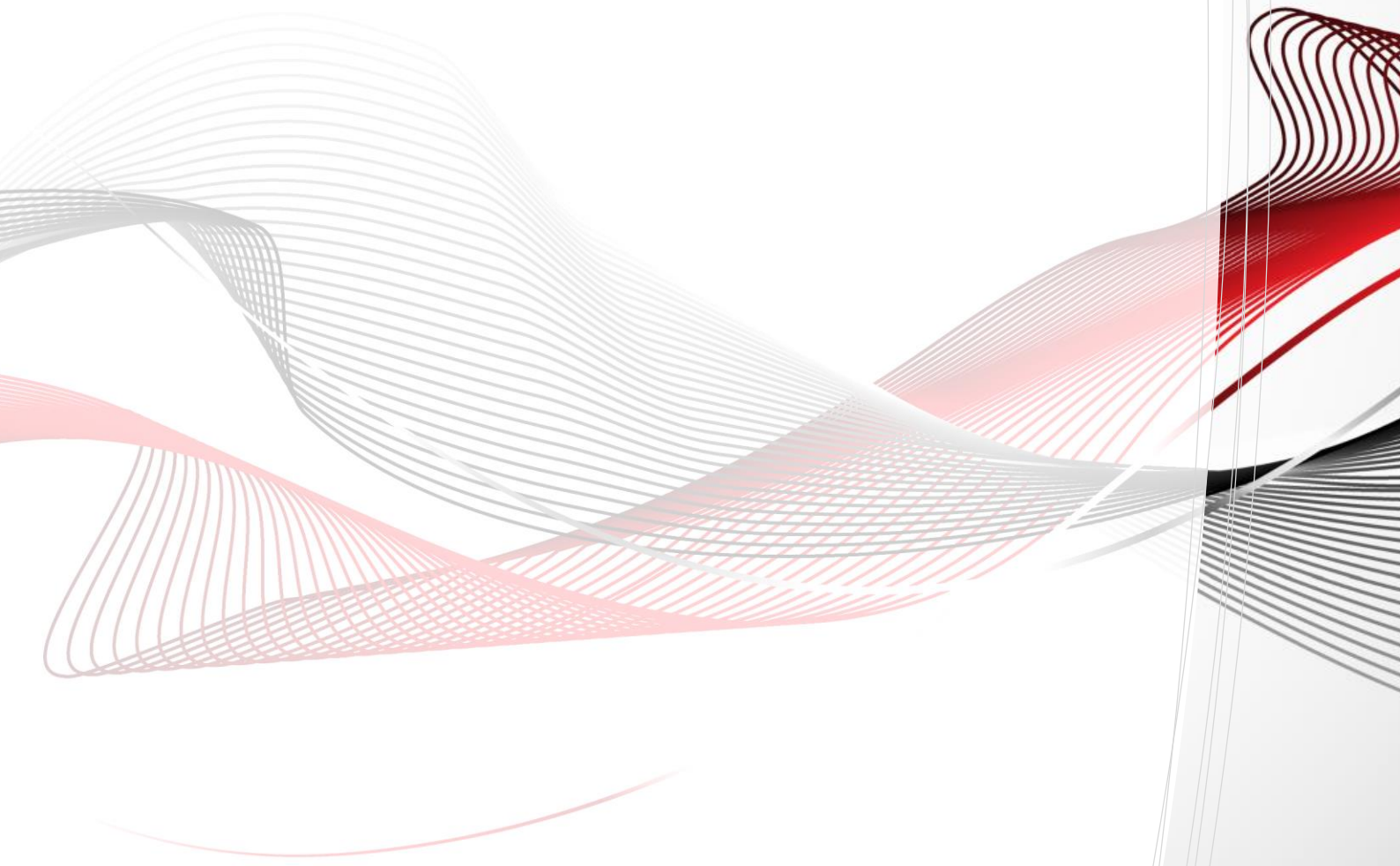
COI Solutions for DOCUMENTS

COI-BusinessFlow
Intrusion Detection

Business White Paper



1 Zusammenfassung

Die Sicherung der Unternehmensdaten und -informationen hat in jedem Unternehmen höchste Priorität. Durch den heute oftmals weltweiten Zugriff auf Unternehmensdaten aus unterschiedlichen Umgebungen und Netzwerken heraus, steigen die Anforderungen an die Datensicherheit beständig.

Folgende Fragen stehen bei der Sicherheit der Datennutzung im Vordergrund:

- Wie können Daten gegen den Zugriff Dritter geschützt werden?
- Wie lassen sich Informationen, neben den Berechtigungsmechanismen, systemweit durchgängig bis in die Administration inhaltlich schützen?
- Wie wird die dezentrale Datennutzung vor Datenmissbrauch geschützt?
- Wie können Datennutzungsabweichungen erkannt und Schutzmechanismen entsprechend aktiviert werden?

Die COI GmbH bietet in COI-BusinessFlow zwei neue Sicherheitsmodule, welche den Schutz der Daten gewährleisten und die Antwort auf die oben genannten Fragen geben.

- COI-BusinessFlow Verschlüsselung auf der Basis AES256 (siehe separates Business White Paper)
- COI-BusinessFlow Intrusion Detection

2 Einführung

Anmerkung: Die nachfolgenden Informationen des Kapitels Einführung und Problemlösung basieren auf der BSI-Richtlinie[1] für Intrusion-Detection-Systeme und führen allgemein in das Thema ein.

Intrusion-Detection-Systeme (kurz IDS) können dazu dienen, die aus den erhöhten Kommunikationsanforderungen und der verringerten Schutzwirkung der Firewall-Systeme resultierenden, zusätzlichen Risiken wieder zu vermindern. IDS erlauben die Überwachung des Netzverkehrs, der Systeme und Anwendungen auf Angriffe und Sicherheitsverletzungen. Die zeitnahe Erkennung von Angriffen, angriffsvorbereitenden Aktivitäten und Sicherheitsverletzungen bildet dabei die Voraussetzung dafür, Schäden zu verhindern, zu begrenzen oder zumindest zeitnah zu beheben. Hierdurch lassen sich die Verfügbarkeit und Integrität von Systemen, Anwendungen und auf diesen basierender Dienste erhöhen.

Dies setzt jedoch voraus, dass die Auswirkungen erkannter Angriffe zeitnah untersucht werden und auf diese angemessen reagiert wird. IDS können zwar grundsätzlich auch automatisch Gegenmaßnahmen einleiten, in den meisten Fällen kann auf eine manuelle Prüfung der Auswirkungen des Angriffs aber nicht verzichtet werden. Dies liegt darin begründet, dass IDS einerseits nicht frei von Fehlalarmen sind und andererseits die Auswirkungen des Angriffs nur begrenzt durch das IDS erfasst werden können.

Über die eigentliche Erkennung und Meldung von Angriffen hinaus bieten IDS Funktionen zur Auswertung aufgezeichneter Ereignisse. Diese können zur Visualisierung der Angriffslast, zur Ermittlung von Angriffskontexten und ggf. zur Rückverfolgung von Angreifern dienen. In vielen Fällen ermöglicht das Erkennen von Verhaltensweisen, die erst durch den IDS-Einsatz sichtbar werden, auch die Verbesserung von Systemkonfigurationen.

2.1 Intrusion Detection Definition

Als Intrusion-Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion-Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.

Intrusion-Detection ist als Prozess zu verstehen und bedarf einer geeigneten organisatorischen Einbindung sowie der technischen Unterstützung durch geeignete Werkzeuge.

2.2 Unterstützende Werkzeuge

Intrusion-Detection bedarf einer technischen Grundlage, um überhaupt Ereignisse aufnehmen und sie dann nach interessierenden Kriterien bewerten zu können. Eine werkzeugbasierte Unterstützung kann zur Generierung von Ereignissen, zur Filterung von Ereignissen, zur Auswertung und Alarmierung sowie zur Archivierung der gefundenen Ergebnisse erfolgen.

Ob und in welcher Form Werkzeuge den Intrusion-Detection-Prozess unterstützen können, hängt im Einzelfall vom organisatorischen und technischen Einsatzumfeld,

[1] BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, Bonn

insbesondere auch vom Überwachungsziel ab. Einfache Werkzeuge, z. B. zur Generierung und zum Vergleich von Checksummen ausgewählter Dateien oder zum Vergleich von Zeichenketten bei der Analyse von Logdateien, können hierzu ebenso nützlich sein wie komplexe Werkzeuge zur Überwachung des Netzverkehrs.

Ein wirksames Intrusion-Detection bedarf daher einer angepassten und zusammenpassenden Auswahl geeigneter Hilfsmittel.

2.3 Intrusion-Detection-System

Als Intrusion-Detection-System wird eine Zusammenstellung von Werkzeugen bezeichnet, die den gesamten Intrusion-Detection-Prozess von der Ereigniserkennung über die Auswertung bis hin zur Eskalation und Dokumentation von Ereignissen unterstützen. IDS können jedoch auch aus Einzelkomponenten zusammengesetzt werden. Auswahl und Zusammenstellung des IDS richten sich dabei nach den individuellen technischen und organisatorischen Gegebenheiten und Anforderungen.

3 Problemlösung

Derzeit werden von fast allen Anbietern kommerzieller IDS Analysemethoden angewendet, die auf der Erkennung von Angriffsmustern oder auf Protokollanalyse beruhen. Zusätzlich bieten fast alle IDS die Möglichkeit zur manuellen statistischen Anomalieerkennung auf der Basis vom IDS erzeugter Reporte und Angriffsstatistiken. Die automatische statistische Anomalieerkennung ist im Gegensatz dazu kaum in marktverfügbare Produkte integriert und fast ausschließlich im wissenschaftlichen Bereich anzutreffen. Auch die Relevanz von IDS, deren Angriffserkennung auf Basis künstlicher Intelligenz erfolgt, beschränkt sich auf den wissenschaftlichen Bereich.

Die Anomalieerkennung auf Basis von Honeypots ist ein am Markt verfügbares Analyseverfahren. Honeypots werden von einigen Herstellern angeboten und sind auch im Open-Source-Bereich erhältlich. Eine automatische sensorübergreifende Korrelation von Ereignisdaten bieten nur wenige der marktverfügbaren IDS. Möglichkeiten zur manuellen Korrelation sind jedoch in der Regel gegeben.

3.1 Erkennen von Angriffsmustern

Als Signaturen werden im IDS-Kontext Muster bzw. Ereignisse bezeichnet, die auf einen bekannten Angriff oder ein missbräuchliches Systemverhalten hinweisen. Signaturen reichen dabei von einfacher Zeichenerkennung in Daten ("pattern matching") bis hin zu komplexen Verhaltensmustern. So erlauben sie auch die Erkennung fehlerhafter Verhaltensweisen des Systems oder einzelner Nutzer (z. B. drei Login-Fehlversuche innerhalb von 5 Minuten).

Bei signaturgestützten IDS erfolgt die Definition des zu erkennenden Angriffs auf der Basis definierter Angriffsmuster. Das IDS alarmiert, sobald ein solches Muster zutrifft. Die meisten verfügbaren IDS gestatten das Anpassen oder Neuerstellen von Signaturen durch eine einfache Skriptsprache.

Vorteil dieser Methode ist die leichte Verständlichkeit des Vorgehens. Nachteilig ist, dass praktisch alle Angriffe (in sämtlichen Modifikationen) aufgezählt werden müssen, damit sie erkannt werden können. Zwar können ähnliche Angriffe durch dieselbe Signatur erkannt werden, wenn die Signatur entsprechend "unscharf" definiert ist. Hierdurch erhöht sich jedoch auch die Fehlalarmrate (false positives) des IDS und mit ihr der personelle Aufwand zur Analyse der IDS-Meldungen.

3.2 Anomalieanalyse

Als Anomalieanalyse werden Auswertungsmethoden bezeichnet, bei denen die Abweichung des Systems von seinem Normalverhalten erkannt und gemeldet wird.

3.3 Korrelation von Ereignisdaten

Die Auswertungslogik kann basieren auf Ereignissen und Daten von

- einem Sensor,
- mehreren Sensoren gleicher Art oder
- mehreren Sensoren unterschiedlicher Arten.

Die Berücksichtigung mehrerer, nicht zeitgleicher Ereignisse oder Ereignisse unterschiedlicher Sensoren durch die Auswertungslogik wird als Korrelation bezeichnet. Die Korrelation kann mit der Signaturanalyse und Anomalieanalyse kombiniert sein.

Die Korrelation von sensorübergreifenden oder langfristigen Ereignissen erfolgt in der Regel intuitiv, kann jedoch durch IDS unterstützt werden, z. B. in Form von regelmäßigen Reports.

Nicht alle am Markt erhältliche IDS-Produkte weisen automatische Korrelationsmöglichkeiten auf. Dagegen wird eine manuelle Korrelation typischerweise durch die Möglichkeit unterstützt, auf Basis der in der Ereignisdatenbank gespeicherten Daten nach verschiedenen Kriterien zu filtern (Report-Funktionen).

Voraussetzung ist hierfür eine möglichst umfangreiche Speicherung der Ereignisdaten und Kontextinformation, da zunächst belanglos erscheinende Daten bei einer Langfrist-Analyse nachträglich an Bedeutung gewinnen können (z. B. Portscans mit einem Port pro Tag oder netzübergreifendes Scanning desselben Ports).

Die Anforderung nach umfangreicher Aufzeichnung verdächtiger Ereignisse konkurriert mit Anforderungen an den Datenschutz. Deshalb ist zu klären, welche Daten für welchen Zeitraum gespeichert werden dürfen. Ereignisdaten können im Allgemeinen auch pseudonymisiert zur Erkennung von Angriffen beitragen. Eine Pseudonymisierung der Ereignisdaten bei der Speicherung wird jedoch von marktverfügbaren IDS-Produkten in der Regel nicht unterstützt.

Die Korrelation wird in der Praxis derzeit hauptsächlich dadurch erschwert, dass einerseits ungeeignete Datenbanksysteme zur Speicherung der Ereignisdaten eingesetzt werden und andererseits aufgrund fehlender Standardisierung eine Korrelation über Sensoren verschiedener Hersteller hinweg nicht von den IDS unterstützt wird. Manuelle Korrelationen sind zwar möglich, jedoch sehr zeitaufwändig und damit kostenintensiv.

3.4 Intrusion-Response-Funktionen

Als Reaktion auf erkannte Ereignisse können verschiedene Aktionen ausgelöst werden, von der Dokumentation des Ereignisses, über die Alarmierung bis zur automatischen Aktivierung von Gegenmaßnahmen. Die von einem IDS automatisch eingeleiteten Maßnahmen werden als Intrusion-Response bezeichnet.

- Dokumentation
- Alarmierung
- Automatische Einleitung von Gegenmaßnahmen

4 Intrusion Detection mit COI-BusinessFlow

Als ECM-Plattform mit den Standardfunktionsbereichen Archivierung und Dokumentenmanagement steht die Sicherheit der verwalteten Daten an erster Stelle. Revisionssichere Archivierung ermöglicht zwar die über Jahre hinweg unveränderbare Speicherung von Unternehmensdokumenten und -informationen, in Verbindung mit dem Modul Intrusion Detection in COI-BusinessFlow erhalten die Daten aber einen zusätzlichen Schutz. In Kombination mit der umfangreichen Rechte- & Rollentechnologie der COI-Plattform werden Informationen durchgängig gegen unberechtigte Nutzung Dritter geschützt. Dabei haben die Aspekte der Datensicherheit und des Datenschutzes höchste Priorität.

Durch den Einsatz der Erweiterungskomponente COI-Intrusion Detection, die auf der COI-Betriebssystemüberwachung (COI-Monitoring Tool) aufbaut, wird die gesamte COI-ECM-Plattform auf Basis einer Vielzahl standardisierter Sensoren überwacht. In Verbindung mit unterschiedlich definierbaren Aktionsmustern kann die ECM-Plattform im Falle einer Bedrohung entsprechende Schutzaktionen auslösen.

4.1 Beschreibung

Das IDS ist nach dem Modell "Sensor – Analyse – Reaktion" konzipiert:

Sensoren sind alle im System befindlichen Protokollierungsmechanismen. Analyse und Reaktion werden über ein Framework realisiert, das die Bearbeitung unabhängig voneinander konfigurierter Prüfobjekte („Analyse“) mit Alarmierungen und Folgeaktionen („Reaktion“) erlaubt. Dieses Framework ist mit einigen vordefinierten Prüffunktionen bestückt und kann durch die Implementierung weiterer Prüffunktionen erweitert werden.

Aufbau und Funktionsweise des IDS orientieren sich an dem bereits vorhandenen Tool Monitoring, welches zur Betriebsüberwachung eingesetzt wird.

4.2 Funktionsübersicht

- Überwachen, Erkennen und Melden von verdächtigen Benutzeraktivitäten
- Sensoren sammeln Dateninformationen. Diese liefern die Rohdaten an die Analysekomponenten. Diese entscheiden, ob ein unerlaubter Eingriff vorliegt und leiten die Ergebnisse an die Reaktionskomponente. Die Reaktionskomponente benachrichtigt entsprechend den Administrator. Diese Komponente basiert auf dem Modul Betriebsüberwachung. Standardmäßig wird eine Reihe von Modulen ausgeliefert (weitere Module können projektspezifisch implementiert werden).

- Sensoren-Module:
  - Benutzer-Aktionen (Liste der Benutzeraktionen pro Zeitraum, z. B. der Benutzer hat zwei Dokumente bearbeitet, und zehn exportiert)
  - Update-Server Aktionen (Liste der Gets/Puts/ …)
- Analyse-Module:
  - Benutzer-Aktionen,
  - Update-Server-Aktionen
- Reaktion-Module:
  - Administrator per E-Mail benachrichtigen,
  - Benutzer mit Eingriffsverdacht ausloggen,
  - Benutzer mit Eingriffsverdacht deaktivieren.

5 Resümee

Mit der Integration der Verschlüsselungstechnologie AES256 (siehe COI-Business-WhitePaper Verschlüsselung) und der Erweiterung COI-Intrusion Detection ermöglicht COI-BusinessFlow, zusätzlich zum Leistungsumfang der unveränderbaren und revisionssicheren Datenarchivierung, einen umfassenden Daten- und Dokumentschutz. COI-Intrusion Detection schützt die Daten durch Analyse und Überwachung des Systems und Auslösen von Schutzmechanismen, abhängig von den gemeldeten Ergebnissen der aktiven Sensoren.

Dies trägt zu einem wesentlichen Schutz des Unternehmenswissens und der in der ECM-Umgebung abgelegten Daten und Informationen bei. Der Sicherheitsstandard des COI-BusinessFlow wurde durch die Entwicklung der COI-Intrusion Detection Komponente und der ebenfalls neuen Verschlüsselungsfunktionen der AES256-Technologie umfangreich ausgebaut.

COI Solutions for DOCUMENTS

COI-BusinessFlow -

die moderne ECM-Plattform aus dem Hause COI.

Ihr Vorteil: Einzigartige Integrationsfähigkeit,
umfassende Prozessoptimierung und
übergreifendes Informationsmanagement.
Mit diesen innovativen Lösungen werden Visionen von morgen
schon heute Realität.

COI – Consulting für Office und Information Management GmbH
Am Weichselgarten 23 – 91058 Erlangen
Telefon: +49 (0)9131 / 9399 0 - Telefax: +49 (0)9131 / 9399 4959
E-Mail: info@coi.de
Web: www.coi.de