

Handbuch zu Intrusion Detection and Prevention Systemen (IDPS)

Guide to Intrusion Detection and Prevention Systems (IDPS)

Laurent Weber

Hausarbeit zum Seminar in IT-Sicherheit

Betreuer: Prof. Dr. Ing. Alfred Scheerhorn

Luxemburg, 25.05.2008

Inhaltsverzeichnis

1) Was ist Intrusion Detection?	4
2) Unterschied zwischen IDS und IPS?	4
3) Was kann ein Intrusion Detection und Prevention System(IDPS)?	4
4) Wichtige Funktionen eines IDPS	4
5) Technologien eines IDPS	5
5.1) Signature-Based Detection.....	5
5.2) Anomaly-Based Detection.....	6
5.3) Stateful Protokoll Analysis.....	6
5.4) Typen von IDPS Technologies.....	7
6) IDPS Technologien	7
6.1) Typisch Komponente.....	8
6.2) Netzwerk Architektur.....	8
6.3.1) Information Ansammlungsfähigkeiten.....	8
6.3.2) Logging Einsatzmöglichkeiten.....	8
6.3.3) Detektion Einsatzmöglichkeiten.....	8
6.3.3.1) Grenzwerte (Threshold).....	8
6.3.3.2) Blacklists und Whitelists.....	8
6.3.3.3) Alarmeigenschaften.....	8
6.3.3.4) Code Einsicht und Modifikation.....	8
7) Management	9
7.1) Aufsetzen eines IDPS.....	9
7.1.1) Komponente Testen und Aufstellen.....	9
7.1.2) Sichern der IDPS Komponente.....	9
7.1.3) Administration und Instandhaltung.....	9
7.1.4) Laufende Instandhaltung.....	9
7.1.5) Updates empfangen und aufspielen.....	9
8) IDPS Typen	10
8.1) Netzwerk basierte IDPS (Network-Based IDPS).....	10
8.2) Kabellose IDPS (Wireless IDPS).....	11
8.3) Netzwerkverhalten Analyse (Network bahaviour analysis).....	12
8.4) Computerbasierte IDPS(Host-based IDPS).....	13
9) Benutzung und Integration multipler IDPS	14
10) IDPS Produktauswahl	15

1) Was ist Intrusion Detection?

Intrusion Detection ist die Eigenschaft zu erkennen, was auf einem Computer oder in einem Netzwerk vorgeht, und diese Vorgänge so zu analysieren, dass man anhand dieser, mögliche Attacken, die den Regelungen eines Unternehmens nicht entsprechen, erkennt. Diese können zum Beispiel Malware sein, aber auch von Benutzer aus dem internen Netz stammen, oder von Angreifer aus dem Internet.

2) Wo ist der Unterschied zwischen einem Intrusion Detection System (IDS) und einem Intrusion Prevention System (IPS)?

Ein IDS ist eine Software, die die Aktionen unbefugter Software oder Nutzern, erkennt. Ein IPS, hingegen, hat die Fähigkeit selbst ein solches Eindringen sofort zu bemerken und die Fähigkeit Versuche zu starten, Tätigkeiten dieser Eindringlinge zu stoppen.

3) Was kann ein Intrusion Detection und Prevention System (IDPS)?

Bei IDPS wird der Schwerpunkt auf das Erkennen von Gefahren gelegt. So kann ein IDPS zum Beispiel erkennen, wenn ein Angreifer ein System erfolgreich kompromittiert hat, indem er eine Sicherheitslücke des Systems ausgenutzt hat. Das IDPS kann auch dem Administrator Bescheid geben, dass dies passiert ist und auch genaue Informationen zur Vorgehensweise des Angreifers liefern, so dass der Administrator zusätzliche Sicherheitsmaßnahmen einsetzen kann, um die Schäden so gering wie möglich zu halten.

Viele IDPS können so ähnlich wie eine Firewall konfiguriert werden, so dass sie Netzwerkprotokolle erkennen können, die gegen die Vorschriften des Unternehmens gehen. Weitere IDPS können auch Datei-Transfers überwachen, und jene erkennen, die suspekt sind, zum Beispiel Transfers von großen Datenbanken auf Laptops.

IDPS können auch Aufklärungsaktivitäten erkennen, wie zum Beispiel Portscans durch Worms oder andere Werkzeuge. Diese Aufklärungsaufgaben deuten darauf hin, dass ein Angriff unmittelbar bevor steht.

Solche Aufklärungsaufgaben können von einem IDPS gestoppt werden und ein Administrator davon in Kenntnis gesetzt werden.

Viele IDPS besitzen auch die Fähigkeit zu zeigen, wenn etwas schlecht oder doppelt konfiguriert wurde, zum Beispiel, durch eine schlecht konfigurierte Firewall.

Ein IDPS kann Sicherheitsprobleme ausfindig machen, und diese auch dokumentieren, so dass ein Administrator gleich genauestes Bescheid weiß über die möglichen Sicherheitslücken des Systems.

Mit einem IDPS kann man leicht Personen ausfindig machen, die gegen die allgemeinen Regelungen des Unternehmens verstoßen.

4) Wichtige Funktionen eines IDPS

Die wichtigsten Funktionen eines IDPS sind das Aufschreiben (loggen) der Ereignisse des Netzwerks sowie die Benachrichtigung des Sicherheitsadministrators über wichtige oder gefährliche Ereignisse. Dies kann auf viele verschiedene Art und Weisen geschehen, im Regelfall kann diese Benachrichtigung konfiguriert werden. Der für Sicherheit zuständige Administrator kann sich dann, lokal oder von außerhalb (falls zugelassen), ins IDPS einloggen und da nachprüfen was genau passiert ist.

Viele IDPS schreiben auch Berichte über ihre Überwachungen, dies ermöglicht es dem Administrator eine Art Zusammenfassung zu erhalten.

Eine große Anzahl an IDPS können auch den Sicherheitslevel des Systems hoch schrauben, falls eine Gefahr entdeckt wurde. Dies könnte zum Beispiel sein, dass, falls etwas Suspektes in einer Sitzung erkannt wurde, diese Sitzung genauer protokolliert wird.

Ein IPS besitzt folgende Fähigkeiten, beim Versuch eines Angriffs, diesen zu verhindern:

Das IPS kann die Netzwerkverbindung oder die Benutzersitzung, die für den Angriff benutzt wird, trennen. Der Zugang von einer IP, einem Benutzerkonto oder anderer Attribute des Angreifers, zum angegriffenem Ziel kann verhindert werden. Traffic jeder Art, der zu dem angegriffenen Ziel, geht kann ganz unterbunden werden.

Ein IPS kann die Sicherheitsumgebung, die er benutzt modifizieren. Dies kann man sich, beispielsweise, in einer Umkonfiguration eines Netzwerkadapters vorstellen, so, zum Beispiel, das Umstellen einer Firewall, oder eines Routers, damit der Angreifer nicht mehr an sein Angriffsziel kommt. Andere IPS können sogar Patches aufspielen, wenn sie merken, dass es auf einem Host Sicherheitslücken gibt, die nicht gepatcht sind, es aber sein sollten.

Verschiedene IPS haben die Fähigkeit den „bösen“ Inhalt eines Angriffs herauszufiltern und ihn durch harmlose Daten zu ersetzen. Ein Beispiel wäre ein IPS das, eine, mit einem Virus verseuchte, E-Mail weiterleitet, nachdem der Anhang entfernt wurde. Ähnliches könnte mit einem Proxy erreicht werden, der die Pakete beim Eingang ins Netz des Unternehmens normalisiert. Dabei wird das Paket anders gepackt, und die Headerinformationen ignoriert. Dies führt dazu, dass einige Angriffe nicht mehr funktionsfähig sind.

Wichtig zu wissen ist, dass ein IDPS nicht notgedrungen immer Recht hat. Falsche negative sowie falsche positive Ergebnisse können immer dabei sein. Es ist nahezu unmöglich alle falschen positiven Ergebnisse auszuschließen.

Das Anpassen der Konfiguration eines IDPS um seine Erkennungsrate zu steigern wird auch noch Tunen genannt.

Viele Unternehmen wählen die Option, die falschen negativen Ergebnisse durch Tuning herunter zu schrauben, allerdings wird dadurch die Anzahl an falschen positiven Ergebnissen größer. Dies heißt, dass mehr suspekten Ereignisse auffallen, die im Grunde ganz harmlos sind. Natürlich werden aber auch mehr böse Inhalte gefunden, das Ganze zu unterschieden wird nur immer komplizierter.

Die meisten IDPS Technologien bieten auch Mittel die Evasionstechniken erkennen können. Ein Evasionsangriff ist ein Angriff, bei dem der Angreifer das Format oder das Timing seiner „bösen“ Aktivität so modifiziert, dass das IDPS es nicht versteht, der angesprochene Dienst des Angriffsziel jedoch schon.

5) Technologien eines IDPS

Die meisten IDPS nutzen mehrere Technologien, entweder getrennt oder ineinander integriert, damit die Erkennungsrate steigt.

Es gibt mehrere Technologien die eingesetzt werden:

5.1) Signature-Based Detection

Eine Signatur ist ein Ausfallmuster, das zu einer bestimmten Bedrohung passt. Eine Signatur basierte Erkennung vergleicht einfach die überwachten Ereignisse mit den, in einer Liste eingetragenen, bekannten, Signaturen von Schädlingen. Beispiele, wo sich eine Signatur basierte Erkennungstechnologie als erfolgreich erweisen würde, wären: Ein Versuch sich über Telnet als root einzuloggen, was gegen die Sicherheitsvorschriften des Unternehmens geht. Das Empfangen einer E-Mail mit dem Betreff: „Free Software!“ und als Anhang eine Datei die „freeSoftware.exe“ heißt, was den Eigenschaften eines bekannten Schadprogrammes entspricht.

Es werden aber auch Systemlogfiles analysiert, so würde ein Wert von 645, der bedeutet, dass die Systemauditierung ausgeschaltet wurde, einer Signatur basierten Technologie auffallen.

Man merkt also schnell, dass eine Signatur basierte Erkennung nur die „bösen“ Ereignisse erkennt, die auf einer Liste stehen, das heißt, neue Schädlinge oder Angriffe werden nicht durch eine solche Technologie gebremst. So reicht es, dass der Angreifer nur Kleinigkeiten ändert um diese Sicherheitsmaßnahme zu umgehen. Zum Beispiel: Eine E-Mail mit dem Betreff: „Free Software!“ und als Anhang eine Datei namens „freeSoftware.exe“ hat, was den Eigenschaften eines bekannten Schadprogrammes entspricht, würde nicht erkannt werden wenn der Angreifer den Anhang „freeSoftware23.exe“ nennen würde.

Signatur basierte Erkennungsdienste sind die einfachsten Überwachungsmethoden, die es gibt. Sie vergleichen einfach die Ereignisse des Momentes (zum Beispiel ein Paket oder eine Logfile) per Stringvergleich mit einer Liste bekannter Schädlinge. Sie verstehen also nicht wie das Netzwerk aufgebaut ist oder wie es funktioniert.

5.2) Anomaly-Based Detection

Anomalie basierte Erkennung vergleicht eine, als normal, eingestufte Netzwerkaktivität mit der überwachten Aktivität um Abweichungen festzustellen. Ein IDPS das Anomalie basierte Erkennungstechnologien einsetzt besitzt Profile für Benutzer, Hosts, Netzwerk-Verbindungen oder Applikationen, die als normal gelten.

Man kann sich die Vorgehensweise folgenderweise vorstellen: Man hat ein Profil von der Netzwerkaktivität eines Webservers. Dieser benutzt 13% der Bandbreite an „normalem“ Arbeitstagen. Wenn er, auf einmal, signifikant mehr verbraucht, wird der Administrator benachrichtigt. So ein Profil kann man für alles mögliche erstellen, E-mails, die ein Benutzer verschickt, falsche Loginversuche, Prozessorleistung...

Ein großer Pluspunkte dieser Technologie ist, dass sie sehr effektiv ist, wenn es darum geht vorher unbekannte Gefahren zu erkennen. Wenn, zum Beispiel, ein Rechner des Netzes von einer Malware befallen ist, könnte diese viel Prozessorleistung benötigen und somit das Profil des Rechners in puncto Prozessorleistung sprengen und so den Administrator auf sie aufmerksam machen. Die Malware könnte aber auch große Massen an Mails verschicken, oder viele Netzwerkverbindungen erstellen, alle diese Aktionen würden den Rahmen des normal Profiles sprengen und so Aufmerksamkeit erregen.

Das „normale“ Profil wird über Tage/Wochen erstellt. Es gibt statische und dynamische Profile.

Statische Profile bleiben unverändert, bis man dem IDPS sagt, er solle einen neuen generieren.

Dynamische Profile passen sich den neuen Ereignissen die ganze Zeit an.

Statische Profile müssen also immer wieder angepasst werden, da sich das Netzwerk über die Zeit ändert. Dynamische Profile nicht, da sie dynamisch mitwachsen. Allerdings ist hier das Risiko von Evasion viel höher. So könnte ein Angreifer über lange Zeit nur sehr wenig Aktivität generieren, sodass der IDPS meint es sei ein neues Netzwerkereignis und ihn in die Liste mitaufnimmt. Man muss auch acht geben keine böse Aktivitäten bei der ersten Profilerstellung mit einzubinden.

5.3) Stateful Protocol Analysis

Bei einer Stateful Protocol Analyse vergleicht man standard Protokoll-Aktivitäten für jedes Protokoll mit den überwachten Protokollen und versucht Abweichungen zu erkennen.

Stateful Protocol Analyse basiert auf den Standardprotokollen, und deren Definition aus den RFCs.

Das „stateful“ im Namen der Technologie bedeutet, dass die IDPS fähig ist zu verstehen und den Status des Netzwerks zu verfolgen.

Es gibt verschiedenen Stusse in denen der Benutzer verschiedene Aktivitäten machen darf, bei andern jedoch wird er als suspekt eingestuft. So, zum Beispiel bei einer FTP-Session, wenn der Benutzer nicht eingeloggt ist, befindet er sich in einem bestimmten Status, nennen

wir ihn, Logoff-Status. Da darf der Benutzer nur ein paar Befehle ausführen, sich einloggen oder help aufrufen. Ist der Benutzer nun eingeloggt, dann darf er weitere Befehle ausführen und befindet sich in einem andern Status, dem Login-Status. Versucht der Benutzer nun im Logoff-Status Befehle des Logins-Status auszuführen, so wird er als suspekt eingestuft. Dies gilt auch für Befehle die hierarchisch angeordnet sind, wenn der Benutzer einen Befehl ausführt, der von einem anderen Befehl stattfinden muss, dieser aber noch nicht ausgeführt wurde, so merkt das IDPS das. Die Stateful Protokoll Analysis erkennt auch auffälliges Benehmen des Benutzers, so zum Beispiel, wenn er wiederholt den gleichen Befehl eingibt, oder Parameter, die 1000 Zeichen haben statt dem üblichen Durchschnitt von 20, benutzt. Wenn da auch noch Binärcode enthalten ist, dann wird das Benehmen als sehr suspekt eingestuft.

Die Analyse der Protokolle ist an den RFC angelehnt, diese Protokollmodelle berücksichtigen auch Variationen in den einzelnen Protokoll-Implementationen. Protokolle werden selten genau so benutzt wie vorgesehen, die Dokumentationen sind oft nicht so genau und auch die Verkäufer setzten proprietäre Teile hinzu. Proprietäre Protokolle werden oft nicht bis ins Detail öffentlich vorgestellt, so dass es schwer ist, für ein IDPS, diese zu analysieren. Des weiteren muss man IDPS, die solche Technologien einsetzen, immer upgedatet halten, da die Protokolle sich oft ändern, oder weiterentwickelt werden.

Ein Nachteil dieser Technologie ist, dass es sehr ressourcenintensiv ist, da sie Analyse relativ komplex ist, und man muss auf jede Session achten egal wie viele simultan laufen. Des weiteren ist es unmöglich Attacken welche den Protokoll-Standards entsprechen anhand dieser Technik zu erkennen. So können DoS (Denial of service) Attacken weiterhin erfolgreich durchgeführt werden.

5.4) Typen von IDPS Technologien

Es gibt hauptsächlich 4 Typen von IDPS Technologien:

Netzwerkbasierte: Die Aktivität im Netzwerk für verschiedene Segmente oder Adapter des Netzwerkes werden überwacht und analysiert. Hierbei wird versucht suspekta Aktivität ausfindig zu machen.

Kabellos: Die kabellose Aktivität wird überwacht und analysiert um suspekta Handlungen ausfindig zu machen. Hierbei wird das Protokoll selbst auch noch mit überwacht.

Network Behaviour Analysis (NBA): Diese Technologie analysiert die Netzwerkaktivität um Gefahren zu entlarven, die ungewohnte Aktivität hervorrufen, wie zum Beispiel DoS-Attacken, Scanning, und verschiedene Arten von Malware.

Host-Based: Diese Technologie überwacht die Eigenschaften eines einzelnen Systems und überwacht die Aktivitäten dieses Hosts um suspekta Aktivität zu erkennen.

Verschiedene IDPS Technologien sind weiter ausgereift als andere, da sie schon länger benutzt werden. So sind netzwerkbasierte und host-basierte IDPS schon seit über 10 Jahren kommerziell zu haben.

6) IDPS Technologien

6.1) Typische Komponenten

Sensors oder Agent: Sensoren und Agenten überwachen und analysieren die Netzwerkaktivität. Sensoren überwachen das Netzwerk, Agenten befassen sich mehr mit dem Host-System.

Management Server: Der Management Server ist ein zentraler Baustein, der die Informationen der Sensoren und Agenten entgegen nimmt und diese managt. Um die Korrelation kümmert sich dieser Management Server ebenfalls. Korrelation wird das Phänomen genannt, das den Management Server dazu bringt alle Aktionen einer IP zusammenzufügen.

Database Server: Auf dem Database Server werden die Informationen der Agent und Sensoren gespeichert sowie die der Management Server.

Konsole: Nur dem Administrator zugängliche Konsolen ermöglichen das IDPS zu konfigurieren, oder die Überwachung anzuschauen und zu analysieren.

6.2) Netzwerk Architektur

IDPS können über das normale Netzwerk einer Firma verbunden werden, oder aber, es kann ein spezielles Netzwerk für Sicherheit eingerichtet werden, dieses wird dann Management Network genannt. Falls so ein Netzwerk benutzt wird, dann hat jeder Sensor oder Agent einen zusätzlichen Netzwerkadapter. Das ist dann das Management Interface, dieses verbindet dann mit dem Management Netzwerk. Traffic kann dann nicht vom Standard Netzwerk in das Management Netzwerk gelangen. Des weiteren ist der Management Server, der Database Server und die Konsole nur an diesem Management Netzwerk angeschlossen. So kann ein Angreifer diese nicht erreichen und es ist immer gewährleistet, dass das Management Netzwerk genug Bandbreite hat, sogar im Falle einer DoS Attacke. Man muss allerdings einen weiteren Kostenaufwand betreiben um so ein Management Netzwerk aufzusetzen. Alternativ könnte man für das Management Netzwerk ein VLAN einrichten, was allerdings dann die oben genannte Vorteile, z.B. garantierte Bandbreite nicht bietet.

6.3) Sicherheit Einsatzmöglichkeiten

6.3.1) Informationsansammlungsfähigkeiten

Verschiedene IDPS können Sammlungen von Informationen über Hosts oder Netzwerk Aktivität erstellen, zum Beispiel das Betriebssystem ausfindig machen, Applikationen die laufen ausfindig machen(durch port scans) sowie Netzwerkeigenschaften feststellen..

6.3.2) Logging Einsatzmöglichkeiten

IDPS loggen im Normalfall alles, was mit Detektion zu tun hat. Durch diese Informationen kann der Administrator dann die Bedrohung bestätigen oder die Ereignisse, die in der IDPS mit den andern Logs zusammenzuführen, zwecks Analyse.

6.3.3) Detektionseinsatzmöglichkeiten

6.3.3.1) Grenzwerte (Threshold)

Ein Threshold ist ein Wert, der die Grenzen für normales und abnormales Benehmen setzt. Thresholds setzen normalerweise einen maximalen Wert, wie, zum Beispiel, 60 Loginversuche in 60 Sekunden.

6.3.3.2) Blacklists und Whitelists

Eine Blacklist enthält alles Mögliche (Hosts, Ports, URLs, Filenamen, usw.) das zuvor als suspekt eingestuft wurde. Anhand solcher Listen erkennt und blockt das IDPS die Aktivität, die den Kriterien dieser Liste entsprechen. Verschiedene IDPS erzeugen dynamische Blacklists, zum Beispiel, auf die IP des Angreifers bezogen.

Whitelists sind der genaue Gegenteil, Einträge in einer Whitelist haben freundliche Intentionen. Whitelists werden oft benutzt um falschen Positiven aus dem Weg zu gehen. Beide Listen werden in Signature based detections und stateful protocol analysis benutzt.

6.3.3.3) Alarmerigenschaften

Der Administrator kann jeden Alarm-Typ selber konfigurieren, an oder aus, Priorität, was geloggt und welche Prävention benutzt werden soll.

6.3.3.4) Code Einsicht und Modifikation

Verschiedene IDPS erlauben es dem Administrator den Code einzusehen und ihn zu editieren, um, zum Beispiel, weiteren Code einzufügen, um etwa weitere Präventionsmechanismen einzubauen. Falscher oder fehlerhafter Code könnte aber auch die ganze IDPS unbrauchbar machen.

7) Management

7.1) Aufsetzen eines IDPS

Sehr genau sollte überlegt werden wo man die Agenten und Sensoren installieren will. Wie wichtig sollte die Zuverlässigkeit und Belastbarkeit des ganzen Systems sein? Werden mehrere Sensoren, zur Überwachung der gleichen Aktivität benötigt, falls einer ausfällt? Wo werden die Komponenten (Database Server, Management Server,...) platziert und wie viele von jeder Sorte werden benötigt? Mit welchem anderen System muss das IDPS interferieren? Wird ein Management Netzwerk benutzt oder nicht? Was muss noch alles im aktuellen Netzwerk geändert werden?

7.1.1) Komponente Testen und Aufstellen

Zuerst sollte man das IDPS in einem Testumfeld testen, danach erst in einem produktiven Umfeld benutzen. Am Anfang nur einige Sensoren einschalten und diese dann genauestens überprüfen und tunen, damit keine false positives mehr drin sind. Nach und nach sollte dann das ganze IDPS einsatzbereit sein.

7.1.2) Sichern der IDPS Komponente

Das sichern von IDPS Komponenten ist sehr wichtig, da IDPS sehr gerne angegriffen werden. Ein IDPS überwacht nicht nur die gesamte Aktivität im Netzwerk, es erstellt auch sehr viele interessante Informationen über die Netzwerkinfrastruktur, was für einen Angreifer sicherlich sehr interessant ist. Als Tipps werden vorgeschlagen, so wenig wie möglich, als Administrator auf der IDPS eingeloggt zu sein, und Firewalls so zu konfigurieren, dass ein Angreifer nicht auf das IDPS zugreifen kann. Die Kommunikation im IDPS soll geschützt sein, entweder durch ein separates Netzwerk (Management Netzwerk) oder ein VPN oder durch Benutzung einer geprüften Verschlüsselung, TLS zum Beispiel.

7.1.3) Administration und Instandhaltung

Die meisten IDPS lassen sich bequem per GUI administrieren, diese heißt Konsole. Sie ermöglicht es den Administratoren das System zu warten (neue Sensoren zu aktivieren beispielsweise) und auch Überwachungslogs zu lesen und zu managen. Die Administration des IDPS kann aufgeteilt werden, durch das Anlegen von Benutzern, die nur die Berechtigung haben verschiedene Sensoren zu überwachen oder für diese Reports zu generieren. Viele IDPS bieten auch eine Shellschnittstelle für die Kommunikation an, so kann man, zum Beispiel, per SSH auf eine solche IDPS zugreifen, egal wo man sich gerade befindet.

7.1.4) Laufende Instandhaltung

Der Administrator muss drauf achten, dass die IDPS Komponenten selber als sicher gelten. Regelmäßiges testen, ob das IDPS funktionsfähig ist, ist ebenfalls angeraten. Die Vulnerabilities Liste muss regelmäßig upgedatet werden und man muss sich über die aktuellen Sicherheitslücken in IDPS, OS und benutzter Software informieren.

7.1.5) Updates empfangen und aufspielen

Es gibt 2 Typen von Updates: Signaturen Updates, und Software Updates. Software Updates halten das System aktuell, stopfen Sicherheitslücken und fügen neuen Funktionalitäten hinzu. Signaturen Updates, hingegen, erhöhen die Fähigkeit des IDPS aktuelle Schädlinge und Attacken zu erkennen.

Die Integrität der Software Updates ist sehr wichtig, so sollte man auf jeden Fall, vor dem Installieren, die selber generierte Checksumme mit der vom Verkäufer gelieferten vergleichen.

8) IDPS Typen

8.1) Netzwerk basierte IDPS (Network-Based IDPS)

Ein auf Netzwerk basierendes IDPS überwacht die Aktivität in einem bestimmten Netzwerkteil oder analysiert das Netzwerk, Transport und Applikationsprotokoll um suspekte Aktivität ausfindig zu machen. Netzwerk basierte IDPS sind den andern IDPS Technologien sehr ähnlich unterscheiden sich jedoch durch die Art der Sensoren. Diese überwachen die Netzwerkaktivität an einem oder mehreren Netzwerksegmenten. In Sachen Sensoren muss man folgende unterscheiden: Application-based Sensoren, die aus Hardware Sensoren und Software Sensoren bestehen, und Software-only Sensoren, welche auf Hosts, die verschiedenen Spezifikationen gerecht werden, installiert werden können.

Unternehmen sollten ein Management Netzwerk anlegen, und wenn sie sich entscheiden kein separates, Hardware getrenntes, Netzwerk einzurichten, dann wenigstens ein VPN, zum Beschützen des IDPS und dessen Kommunikation. Neben der Wahl des angebrachten Management Netzwerk, sollen die Administratoren auch überlegen, und entscheiden, wo sie IDPS Sensoren einsetzen wollen. Diese Sensoren kann man in 2 verschiedenen Moden betreiben: Inline Sensoren, werden so angebracht dass der Netzwerktraffic durch sie hindurchgeht, passive Sensoren, hingegen, werden so eingesetzt, dass sie eine Kopie des aktuellen Netzwerktraffics analysieren. Als Faustregel kann man sich merken, dass man Inline Sensoren dann einsetzt, wenn Präventionsmethoden eingesetzt werden und passive Sensoren falls dies nicht der Fall ist.

Netzwerk basierte IDPS bieten eine große Anzahl an Sicherheitseinsatzmöglichkeiten, so können solche IDPS Informationen über die sich im Netz befindenden Hosts ausfindig machen, wie, zum Beispiel, welches Betriebssystem sie einsetzen, welche Applikationen und Versionsnummer auf ihnen laufen. Des weiteren können Netzwerk basierte IDPS über die Entdeckungen im Netzwerk Buch führen (loggen). So ist auch Pakete Abfangen eine Fähigkeit die die meisten IDPS beherrschen.

Netzwerk basierte IDPS bieten oft sehr fortgeschrittene Entdeckungsfähigkeiten. Meistens werden diese durch eine Mischung aus Signature-based, stateful protocol analysis erreicht. Damit werden dann sehr tiefe Analysen von alltäglichen Protokollen betrieben.

Unternehmen sollten auf jedenfalls auf Netzwerk basierende IDPS einsetzen, die solche Kombinationen von Detektion Fähigkeiten besitzen, da durch eine solche Kombination die Entdeckungsrate von Schädlingen jeder Art extrem gesteigert wird.

Des weiteren sollten Unternehmen Netzwerk basierte IDPS benutzen, die mit den gängigen Evasionstechniken (verschleierte Attacken in kryptischer Form) umgehen können, was wiederum die Entdeckungskapazität steigert.

Man soll sich auch über die Grenzen eines Netzwerk-basierten IDPS bewusst sein. So kann ein Netzwerk basiertes IDPS, zum Beispiel, keine Attacken entdecken, die mit verschlüsselter Kommunikation durchgeführt werden. So sollte man denn, also am besten, die Segmente der Übertragungsrouten überwachen, in der die Daten schon entschlüsselt sind, das heißt vor der Verschlüsselung, oder nach der Entschlüsselung. Alternativ könnte man auch, um dieser Gefahr aus dem Weg zu gehen, Host-based IDPS, zum Überwachen der Endpunkte, einsetzen.

Wenn sehr viel Traffic herrscht, sind Netzwerk-based IDPS oft nicht mehr fähig den ganzen Traffic zu überwachen. So sollten Unternehmen bewusst solche Sensoren aussuchen, die schon sehr viel Aktivität zugleich vertragen, und dann das System noch so konfigurieren, dass, wenn der Sensor zu viel Aktivität erkennt, er entweder verschiedene Typen an Traffic ungefiltert durchlässt, oder aber die Pakete die eine geringe Priorität haben einfach weglässt um die Aktivität zu senken. Allgemein kann man sagen, dass Netzwerk-based IDPS am meisten durch Attacken gefährdet sind, die viel Netzwerk Traffic einsetzen. Um solchen Attacken zu widerstehen, sollten Unternehmen sich was ausdenken, um einem Einzelnen zu verbieten zu viel Traffic zu erzeugen, dazu gibt es ebenfalls IDPS Produkte.

Auf keinen Fall sollten Sensoren, die den Traffic überwachen, mit IP Adressen ausgestattet sein, da man sie sonst ansteuern könnte. Sensoren, die dem IDPS Management dienen, sollten

jedoch eine IP Adresse haben. Passive und Inline Sensoren bieten verschiedene Präventionsfähigkeiten. So können viele passive Sensoren, zum Beispiel, versuchen eine TCP Session zu beenden, indem sie sie reseten, jedoch mit der Einschränkung, dass dies nur bei TCP geht, bei UDP, beispielsweise, würde das nicht klappen. Inline Sensoren besitzen mehrere Fähigkeiten zur Prävention, sie können inline Firewalling betreiben, die Bandbreite verkleinern, die Umstände ändern wenn suspekter Inhalt entdeckt wird. Alle diese Möglichkeiten sind, je nach Situation, mehr oder weniger wirksam. Inline sowie passive Sensoren können andere Netzwerksicherheitsbausteine umkonfigurieren und so größeren Schutz bieten. Software von Dritten kann auch von beiden ausgeführt werden, diese könnte dann, zum Beispiel, weitere Präventionsaktionen vornehmen.

8.2) Kabellose IDPS (Wireless IDPS)

Ein kabelloses IDPS überwacht den kabellosen Netzwerk Traffic und analysiert die kabellosen Netzwerkprotokolle um suspekte Aktivitäten ausfindig zu machen. Die Komponenten eines kabellosen IDPS sind die gleichen, wie die eines Kabelnetzwerkes, nur die strategische Platzierung spielt eine Rolle. So hat ein kabelloses IDPS auch Konsolen, Datenbank Server, Management Server, und Sensoren. Im Gegensatz zu einem Kabelnetzwerk IDPS, kann ein kabelloses IDPS nicht den ganzen Traffic des Netzwerks überwachen, da nicht alle Chanel zur gleichen Zeit überwacht werden können. Wichtig ist hierbei, dass, je länger ein Chanel überwacht wird, desto größer ist die Wahrscheinlichkeit, dass der Sensor einen Angriff, der auf einem andern Chanel ausgeübt wird, verpassen wird. Deswegen ändern Sensoren ständig den Chanel, den sie überwachen. So können sie jeden Chanel ein paar mal in der Sekunde überwachen.

Solch einen kabellosen Sensor kann man in verschiedenen Formen antreffen. So gibt es “dedizierte Sensoren”, die entweder fest oder mobil angetroffen werden können. Diese gehen den typischen IDPS Funktionen nach, geben den Netzwerktraffic jedoch nicht von Ausgangsort zum Ziel weiter, sie kümmern sich nur um das Analysieren. Andere Sensoren sind an Access-Points oder an Wireless-switches gebunden. Da sich dedizierte Sensoren auf die Entdeckung von suspekter Aktivität konzentrieren können und den Traffic nicht weiter leiten müssen, haben diese stärkere Erkennungsfähigkeiten als die andern Sensoren, die an Switches oder AP gebunden sind. Jedoch sind dedizierte Sensoren sowohl in der Anschaffung als in der Installation und der Wartung teurer. Gebundene Sensoren können an bereits existierender Hardware angebracht werden, entgegen den dedizierten Sensoren, die neue Hardware- und Software-Anschaffung verlangen. Firmen sollten also hier auch wieder einen Kosten/Risiko Vergleich anstellen, und dann über die benötigte Hardware entscheiden.

Die einzelnen, kabellosen IDPS sollten durch ein Kabelnetzwerk miteinander verbunden sein, da man eine strikte Trennung zwischen Kabel- und kabellosem Netzwerk machen soll. Ein Management Netzwerk oder ein Standard Netzwerk sollte für ein kabelloses IDPS reichen. Einen fundamentalen Unterschied zwischen Kabel- und kabellosem IDPS ist die Auswahl der Plätze, wo man die Sensoren anbringen soll. Wenn das Unternehmen WLAN benutzt, dann sollten die Sensoren so angebracht werden, dass sie die Reichweite dieses WLANs überwachen. Alternativ kann man auch Sensoren da anbringen, wo keine Netzwerkaktivität stattfinden soll, oder aber auch auf Chanel, die das Unternehmen nicht benutzt. Man sollte ebenfalls auf die Plätze acht geben, wo man die Sensoren anbringt, denn zu leichte physische Zugänglichkeit, könnte einen Angreifer dazu bringen das Teil einfach abzubauen oder zu beschädigen. Manche Sensoren-Hersteller tarnen ihre Sensoren deswegen zum Beispiel in AP. Die Reichweite der Sensoren sowie die Kabelnetzwerkanbindungs-Möglichkeiten und die Kosten sollten beim Erwerben solcher Sensoren in Betracht gezogen werden.

Die Sicherheitsfähigkeiten eine kabellosen IDPS sind weit gefächert. Die meisten können von überwachten Netzwerknutzern Informationen sammeln, und die Geschehnisse genau loggen. Ein kabelloses IDPS kann Angriffe, falsch konfigurierte sowie Missbräuche der WLAN Protokolle ausfindig machen. Unternehmen sollten IDPS Produkte auswählen, die nicht zugelas-

sene oder schlecht gesicherte WLANs, ungewohnte Aktivität, Netzwerkscanner, DaS Angriffe, sowie Man-in-the-middle Attacken entlarven. Anhand von triangulation, kann man, mit einem guten IDPS, den genauen Standpunkt, von dem der Angriff übers WLAN erfolgt, ausfindig machen. Triangulation beruht darauf, dass man, durch die Kenntnis der Stärke des WLAN-Signals eines gegebenen WLAN Adapter zu verschiedenen Sensoren, den genauen Standpunkt eben dieses Adapters ausfindig machen kann.

Allgemein kann man sagen, dass kabellose IDPS ein wenig getunt und konfiguriert werden müssen, damit sie ihre Erkennungsrate steigern. Die meiste Arbeit steckt darin, einzustellen welches WLAN, AP oder STA erlaubt sind und diese in die kabellose IDPS einzutragen. Natürlich muss diese Konfiguration immer upgedatet sein, um sicher zu gehen, dass sie immer noch der Situation im Netzwerk angepasst ist. Wichtige Änderungen der physischen Infrastruktur des Unternehmens sollte dem Administrator auch mitgeteilt werden und in das IDPS eingetragen werden, da dies notwendig ist zur Lokalisierung der Angreifer im Wlan. Ebenso wichtig ist es, die Planung der neuen Sensoren in den neuen Teilen des Unternehmens sorgsam anzugehen.

Prinzipiell haben kabellose IDPS sehr robuste Entdeckungsfähigkeiten. Allerdings gibt es auch Begrenzungen. So können kabellose IDPS zum Beispiel keine passiven Sniffer im Netzwerk ausfindig machen. Nach einer solchen Attacke kann der WLAN Traffic bequem offline ausgewertet werden. Machtlos ist ein kabelloses IDPS auch gegen Evasionstechniken, zum Beispiel solche die die scanning Attitüde des Produktes kennen, und so immer auf dem Channel arbeiten wo gerade nicht gescannt wird. Bei DoS Attacken und physischen Angriffen muss das IDPS sich meistens auch geschlagen geben.

8.3) Netzwerkverhaltens Analyse (Network behaviour analysis)

Ein Netzwerkverhaltens-Analyse (NBA) System analysiert entweder den Netzwerk Traffic oder Statistiken der Netzwerkaktivität, um, dadurch, außergewöhnliche Aktivitäten festzustellen. NBA verfügen über Sensoren und Konsolen, manche Hersteller solcher Produkte bieten aber auch Management Server an. Die Sensoren sind denen von den Netzwerk basierten IDPS sehr ähnlich, da sie ebenfalls Pakete sniffen können und meistens auf einem oder mehreren Netzsegmenten ausgerichtet sind. Andere NBA Sensoren überwachen den Netzwerktraffic nicht in direktem Weg, sondern halten sich an die Netzwerkaktivitäts-Informationen, die sie von Routern und anderen Netzwerk-Bausteinen kriegen.

Eine weitere Gemeinsamkeit zwischen Netzwerkbasierten IDPS und NBA sind die Anbindungsmethoden, die benutzt werden um die Sensoren ans Netzwerk zu hängen. Man muss wissen, dass die meisten Netzwerksensoren nur über einen passiven Modus verfügen. Die Sensoren, die das Netzwerk über direktem Wege überwachen, sollten auf strategisch gut ausgewählten Stellen, wie zum Beispiel Netzwerkübergänge oder DMZ, angebracht werden. Inline Sensoren sollten innerhalb des Netzwerkes betrieben werden, aber vor der Firewall, sodass sie dieser Schutz, gegen die auf sie ausgerichteten Angriffe, bieten kann.

Die NBA Produkte bieten eine Vielzahl an Sicherheitsfähigkeiten. Sie können zum Beispiel detaillierte Informationen über die überwachten Hosts ausfindig machen und auch konstant die Netzwerkaktivität überwachen. Wenn eine suspekte Aktivität entdeckt wird, loggt das NBA System alles was in irgendeiner Form zu der Aktion in Verbindung stehen könnte. NBA besitzen die Fähigkeit eine Vielzahl an Attacken ausfindig zu machen, wie zum Beispiel DoS Attacken, Scannings, die durchgeführt werden, aber auch Worms oder unerwünschte Services die angeboten werden. Zusammenfassend könnte man also festhalten, dass ein NBA darauf ausgerichtet ist Angriffe, welche viel Traffic in kurzer Zeit im Netzwerk verursachen, ausfindig zu machen. Verschiedene NBA besitzen auch die Fähigkeit eine Serie von beobachteten Ereignissen wiederherstellen, damit sich die Herkunft des Angriffes leichter feststellen lässt. NBA benötigen wenig Tuning an der Konfiguration. Das einzige was zu tun ist, ist die Firewall Konfiguration upzudaten. Ein paar IDPS bieten auch die Möglichkeit ihre Signaturen minimal manuell anzupassen, was den Vorteil bietet, dass sie so ausgerichtet werden können,

dass die Inline Sensoren danach Signaturen ausfindig machen und blocken, die die Firewall so nicht erkannt hätte. Administratoren müssten sich auch drum kümmern, dass neue Hosts und Services in diese NBA mit eingebunden werden. Im Normalfall gibt es für diese Aktion keine Automatisierung, da eine Verbindung zwischen Management System und NBA nicht gegeben ist.

Wie jede Technologie hat auch die NBA Technologie ihre Grenzen. So spielt die Dauer bis ein Angriff entdeckt wird eine sehr wichtige Rolle. Dies liegt an den Quellen von denen die NBA ihre Netzwerkinformationen her kriegt. Wenn der Informationsfluss zuerst auf einem Router oder anderen Netzwerkbausteinen aufgeschrieben wird und dann zur Auswertung zum NBA geschickt wird, braucht das seine Zeit. Diese Übertragung findet von minütlich bis hin zu ein paar mal in der Stunde statt, so dass schnelle Attacken bereits das System übernommen oder stark geschädigt haben können, ehe die NBA es erst bemerkt. Dieses Problem kann anhand von Sensoren, die ihre eigene „Paketfänger“ und Analyse haben, behoben werden. Jedoch ist dies sehr ressourcenintensiv. Des weiteren kann ein Sensor der mit einer Logdatei vom Netzwerkfluss konfrontiert wird, mehrere Netzwerke gleichzeitig analysieren. Ein Sensor, der sofort das geschehen im Netzwerk analysiert, hingegen, kann nur ein paar Netzwerke auf einmal überwachen. Das Unternehmen muss also in Betracht ziehen, dass, wenn es den Traffic exklusiv mit Sensoren, die ihre eigene Analysewerkbank mitbringen, überwachen will, dies viel treuerer wird, als wenn sie einen Sensor den Netzwerkfluss überwachen lässt.

8.4) Computerbasierte IDPS (Host-based IDPS)

Auf Hosts bezogene IDPS überwachen die typischen Merkmale der einzelnen Hosts und überprüfen, ob die Ereignisse dieser Hosts in irgendeiner Form suspekt sind. Host-based IDPS überwachen, beispielsweise, die Netzwerkschnittstellen, Kabelnetzwerk- wie auch kabellose Netzwerkadapter. Die laufenden Prozesse, wie auch die Systems Logfiles, helfen dem Host-based IDPS suspekten Aktivität festzustellen. Als sehr hilfreich erweisen sich auch die Zugangsberechtigungen, sowie der Zugriff auf verschiedene Dateien, die für den Host wichtig sind. So fallen einem IDPS, das auf einen Host ausgerichtet ist, auch Konfigurationsänderungen auf. Die Überwachungssoftware solcher IDPS sind auch noch als Agenten (Agents) bekannt. Diese Agenten werden auf das zu überwachende System installiert. Jeder dieser Agenten konzentriert sich exklusiv auf ein Host. Überwachung und Prävention, falls aktiviert, sind die Aufgaben dieser Agenten. Agenten übertragen Daten zum Management Server. Im üblichen Fall überwacht ein Agent einen Server, Desktop-PC, Laptop oder aber auch einen Application Service.

Im üblichen Fall benötigen Host-based IDPS kein spezielles Management Netzwerk, da sie über das normale Netzwerk miteinander kommunizieren. Die Netzwerktopologie, die solche Host-based IDPS benötigen, ist also relativ einfach. Das Einsatzgebiet solcher Host-based IDPS befindet sich auf kritischen Hosts, die man von außen erreichen kann, oder aber auch, auf Server die empfindliche Daten beinhalten. Da es aber Agenten für die meisten Betriebssysteme gibt, können sich Unternehmen auch überlegen ein solches IDPS auf alle Rechner des Unternehmens zu installieren. Jedoch sollten Unternehmen bei der Auswahl ihrer Agenten verschiedene Eigenschaften beachten. So wäre es, zum Beispiel, unnötig Aktivitäten zu überwachen, die bereits von anderen IDPS überwacht werden. Sie sollten auch die Anschaffungskosten, sowie die Wartung und das Auswerten dieser Agenten in Betracht ziehen. Es sollte auch überprüft werden welche Betriebssysteme unterstützt werden und was für eine Netzwerkinfrastruktur für die Kommunikation benötigt wird.

Die meisten IDPS Agenten benutzen so genannte “shims”, zur Überwachung der Hosts. Shims sind code layer, die zwischen die bereits existierenden Code Layer gepackt werden, und somit die interne Architektur des Systems ändern. Allerdings gibt es auch IDPS, die ohne shims arbeiten. Ihre Entdeckungsrate ist jedoch schwächer, und die Überwachung wird eingeschränkt. Die Prävention wird ohne shims auch fast ganz unmöglich gemacht.

Die Sicherheitsfähigkeiten eines Host-IDPS sind ebenfalls sehr vielfältig. Im Normalfall loggt so eine Technologie sehr intensiv, falls eine suspekta Aktivität bemerkt wird. Die Enttarnungstechniken, die eingesetzt werden sind sehr vielfältig und beinhalten Codeanalyse, Netzwerk-Aktivitäts-Analyse, Netzwerktraffic Filterung, Überwachung der System Files, Auswertung von Logs und die Überwachung der Netzwerkkonfiguration. Produkte, die mehrere Entdeckungstechniken benutzen, sollten im Normalfall fähig sein mehr Gefahren zu erkennen, als IDPS die nur eine Technik anwenden. Denn jede Technik überwacht das System anders. Um das passende Produkt auszuwählen, sollten Unternehmen überlegen welche Eigenschaften der Hosts überwacht werden sollten.

Im Regelfall brauchen Host-based IDPS sehr viel Tuning und Konfigurationsaufwand. Das kommt davon, dass zum Beispiel viele Host-based IDPSysteme darauf beruhen, dass sie das Host-System observieren und, daraus eine Richtlinie für das zu erwartende Benehmen des Systems aufbauen. Andere benötigen strenge und genaue Regelrichtlinien, so dass sie genau wissen, welche Applikation sich wie zu benehmen hat. Administratoren müssen dafür sorgen, dass wenn ein neuer Dienst zum Beispiel freigeschaltet wird, dieser auch im host-based IDPS freigeschaltet wird.

Die Grenzen eines solchen IDPS sind ebenfalls eng bemessen. Verschiedene Techniken testen zum Beispiel nur in regelmäßigen Abständen (Minuten/Stunden) die Files oder Dienste, die sie überwachen. Auch wenn sie dann den Schädling entdecken, kann dieser in dieser Zeit schon weitere Systeme angegriffen oder auf dem aktuellen System starke Schäden angerichtet haben. Viele Host-based IDPS geben auch ihre Entdeckungslogs an den Management Server weiter, der sie ein paar mal in der Stunde entgegen nimmt, was wiederum einen schnellen Eingriff unmöglich macht. Durch die Agenten, die auf den Host laufen, wird auch deren Performance eingeschränkt. Aufpassen muss man auch bei der Installation der Agenten, dass sie keine Konflikte zu den bereits existierenden Sicherheitsmaßnahmen (Firewall, VPN-Clients) des Hosts erzeugen. Das Reboot des Hosts wird auch bei Upgrades und Konfigurationsänderungen nötig.

Host-based IDPS bieten eine Vielzahl an Präventionsmöglichkeiten. Diese variieren allerdings je nach benutzter Entdeckungstechnik. So kann man festhalten, dass ein Host-based IDPS der Code Analyse benutzt, das Ausführen von Code verhindern kann. Dies ist eine sehr effektive Art und Weise, bekannte und unbekannt, Attacken zu erkennen und zu stoppen. Eine Netzwerktraffic Analyse kann hereinkommenden und ausgehenden Traffic stoppen, egal auf welchem Layer die Attacke geführt wird. Das kann auch die Benutzung von unerlaubten Protokollen oder Applikationen unterbinden. Das Netzwerktraffickingfiltern arbeitet wie eine Firewall, stoppt die Dienste, die nicht zugelassen sind, und lässt die erlaubten Dienste durch. Die Überwachung der Filesysteme kann Files davor schützen gelesen, modifiziert, ersetzt oder gelöscht zu werden. Das kann Malware davon abhalten sich auf dem Host auszubreiten, aber auch andere Attacken, die das Filesystem betreffen, können damit gestoppt werden. Weitere Host-based IDPS können keine Prävention, da sie nur feststellen, dass etwas nicht stimmt, nachdem sich der Schädling eingenistet hat.

Weitere Sicherheitsvorkehrungen werden von verschiedenen IDPS angeboten. Sie können zum Beispiel mobile Speichermedien daran hindern, sich ins System einzubinden, um so den Diebstahl sensibler Daten, oder auch das Einspeisen von Schädlingen verhindern oder etwa die audiovisuelle Peripherie überwachen.

9) Benutzung und Integration multipler IDPS

Die vier Primären IDPS Technologien nutzen alle fundamental verschiedene Art und Weisen mit der sie an Informationen kommen, wie sie die Gefahren deuten und das System vor ihnen schützen.

Die einzelnen Technologien bieten verschiedenen Schutz, sind sozusagen auf einem Gebiet spezialisiert. So sollten sich Unternehmen überlegen, welche IDPS Systeme sie nutzen wollen. Mehrere IDPS Technologien einzusetzen ist ratsam. Meistens kann ein robustes IDPS

System nicht mit nur einem IDPS erreicht werden, es sollten schon verschiedene IDPS in Kombination eingesetzt werden. Oft reicht ein Netzwerk-basierendes IDPS mit einem Host-based IDPS um sich zu schützen. Eine oft unterschätzte Gefahr ist das kabellose Netzwerk, das, sollte das Unternehmen über ein solches verfügen, unbedingt überwacht werden soll. NBA Technologien werden eingesetzt, falls das Unternehmen DoS-Attacken oder Würmern vorbeugen will, da diese Technologie für diesen Angriffstyp sehr gut geeignet ist.

Falls das Unternehmen beschließt verschiedene IDPS Technologien einzusetzen, oder sogar eine Vielzahl an IDPS Produkten der gleichen Technologie, sollte sie auch überlegen, ob diese Produkte in irgendeiner Weise miteinander integriert sind. Direkte Integration hat man oft, wenn man mehrere Produkte des gleichen Herstellers nimmt. Oft verfügen diese dann über eine Konsole, mit der man das gesamte Paket an IDPS verwalten kann. Andere Produkte können Information für andere Systeme freigeben, so dass die Analyse schneller abläuft. Eine begrenzt Form der Integration wäre wenn ein IDPS Produkt Daten an ein anderes IDPS Produkt weiter gibt. So könnte, beispielsweise, ein semantikbasiertes IDPS Informationen über ein Netzwerktraffik an einen NBA Sensor weitergeben.

Oft wird ein Security Information und Event Management (SIEM) benutzt um eine indirekte IDPS Integration zu erlangen. Diese Software verknüpft die verschiedenen Logs und gleicht sie ab, sodass suspekte Aktivität erkannt wird und Alarm gegeben werden kann.

Als Alternative zu einem SIEM könnte man ein Framework einsetzen, welches die verschiedenen IDPS Logs annehmen und verarbeiten kann. Syslogs sind sehr flexibel und daher gut dazu geeignet. Sie verfügen über verschiedene Felder, in die die IDPS ihre Informationen platzieren können, das Format ist dabei gleichgültig. Andererseits wird jedoch dadurch die Analyse dieser Logs für den zuständigen Administrator komplizierter. In der Tat, jedes IDPS Produkt kann dann sein eigenes Format benutzen, so dass das Auswerten nur mühsam vor sich geht. Automatisierte Loganalyser müssen ebenfalls alle Formate kennen, damit sie die Chance haben die Gefahren zu erkennen. Im Regelfall kann man sagen, dass dieses zentralisierten Syslogs über zu wenig Analysefähigkeiten verfügen um eine ausreichende Erkennung und Prävention zu bieten.

Zusätzlich können Unternehmen weitere Technologien einsetzen die, je nachdem, vielleicht, einige IDPS Fähigkeiten besitzen, die IDPS selbst aber in keiner Weise ersetzen. So könnte ein Unternehmen Forensik Analyse Applikationen, sowie Anti-Malware, Firewalls und Router einsetzen.

10) IDPS Produktauswahl

Vor der Auswahl eines IDPS Produktes sollten sich Unternehmen zuerst genauestens überlegen, was für Produkte ihren Ansprüche gerecht werden. Die verschiedenen verfahren, die solche IDPS benutzen, sowie die Fähigkeiten, die sie haben, sind grundverschieden. So muss sich jedes Unternehmen seine eigene, an ihre Bedürfnisse angepasste, IDPS zusammensuchen. Ein Unternehmen muss zuerst die Netzwerktopologie sowie das gesamte System verstehen, um zu wissen welches IDPS es einsetzen kann, denn dieses IDPS sollte mit den bereits existierenden Komponenten kompatibel sein und sollte auch die Fähigkeit besitzen das Netzwerk erfolgreich zu überwachen.

Dieses Wissen wird ebenfalls benötigt um den Aufbau des IDPS zu planen. Nachdem die Netzwerktopologie verstanden wurde, sollten die Ziele des IDPS in Betracht gezogen werden. Hierbei sollten die bereits existierenden Regelungen des Unternehmens vor der Auswahl des Produktes beachtet werden.

Zusätzlich sollten neben den allgemeinen Anforderungen auch spezifischere Anforderungen analysiert werden, so etwa die Sicherheitsfähigkeiten des Systems. Dazu zählt, unter anderem, Informationen Sammeln, Loggen, Prävention und Detektion. Überaus wichtig ist auch die Performance des Systems, hierbei muss man auf Design, Implementation, Training und Wartung des Systems achten, sowie auch auf die Dokumentation und den Beistand in Problemfäl-

len. Natürlich spielen auch die Kosten des Systems, seien es die Anschaffungskosten oder die Wartungskosten, eine wesentliche Rolle.

Diese Kriterien können Unternehmen nutzen um sich ein eigenes Profil anzulegen, wie sie IDPS einsetzen wollen. Sie sollten dann auch, wie oben erwähnt, die bereits existierenden Sicherheitsregelungen nicht außer Acht lassen, wie auch die aktuelle und zukünftige Infrastruktur des Netzwerkes zu berücksichtigen sind.

Nachdem die Anforderungen analysiert wurden, müssen sich Unternehmen glaubwürdige Informationsquellen suchen, um die Bewertung verschiedener Produkte zu vergleichen. Gewöhnliche Informationen sind die Leistung in Laborbedingungen, wie auch in real-world tests, aber auch die Informationen, die der Hersteller ausgibt, und die Bewertung von Dritten (zum Beispiel Unternehmen die mit der besagten IDPS Erfahrungen gemacht haben).

Ein IDPS vollkommen zu testen ist meistens unmöglich. Daher gibt es Tests, die nur eine limitierte Auswertung eines IDPS erlauben. Diese Auswertung hilft vielen Unternehmen sich ein Bild über den täglichen Gebrauch und die Sicherheitsmöglichkeiten zu machen, sowie zu erfahren, wie sich die IDPS Technologien untereinander verhalten. Bei der Auswahl ihrer Produkte sollten sich Unternehmen an mehreren Quellen orientieren. Die Herkunft der Daten sollte auf jedenfalls immer geprüft werden und suspekten Quellen lieber keine Achtung geschenkt werden.

Beim Testen der IDPS sollten Unternehmen Wert drauf legen, das zu testen, was für sie am besten geeignet ist, und sich von Tests, welche die Arbeitsfähigkeit des Unternehmens gefährden könnten, fernhalten.