

Der Wandel von Intrusion Detection zu Intrusion Prevention

Was steckt wirklich hinter dem Schlagwort IPS

Jedes Jahr hat seine Schlagwörter und seine dazugehörigen Abkürzungen. Auch auf die IT-Sicherheitsbranche trifft dies zu. Eines dieser Schlagwörter, das in 2003 besonders oft verwendet wird, ist sicherlich Intrusion Prevention als Nachfolge von Intrusion Detection. Dementsprechend spricht man von IPS oder auch IDP (Intrusion Detection Protection). Was sich genau hinter IPS verbirgt, sieht jedoch fast jeder Hersteller anders. Völlig unterschiedliche Technologien nehmen die Bezeichnung IPS für sich in Anspruch. Darunter sind klassische netzwerkbasierte Intrusion-Detection-Produkte, die bei einem erkannten Angriff automatisch versuchen, den Angriff zu blockieren ebenso wie Web-Applikations-Filter, die Angriffe auf Applikationsebene durch eine Analyse aller Web-Seiten, Formulare, Links und Benutzer-Eingaben in http-Übertragungen verhindern wollen. Dieser Artikel versucht, die verschiedenen Technologien, die sich mit der Bezeichnung Intrusion Prevention schmücken, vorzustellen und einzuordnen.

Nähert man sich dem Begriff Intrusion Prevention von der reinen wörtlichen Bedeutung, so handelt es sich um Produkte oder Technologien, die das Ziel haben, einen Angriff zu verhindern. Diese grundsätzliche Idee ist nicht unbedingt neu. Schon Firewall-Systeme haben ja den Zweck, Angriffe zu verhindern, indem Kommunikations-Verbindungen auf diejenigen IP-Adressen und Ports beschränkt sind, die unbedingt benötigt werden. Dennoch nennt derzeit keiner der großen Firewall-Hersteller seine Produkte Intrusion Prevention. Nach dem derzeit üblichen Verständnis im IT-Sicherheits-Markt sind Intrusion Prevention Systeme nämlich gerade keine Firewalls, sondern Produkte, die komplementär dazu Angriffe verhindern können.

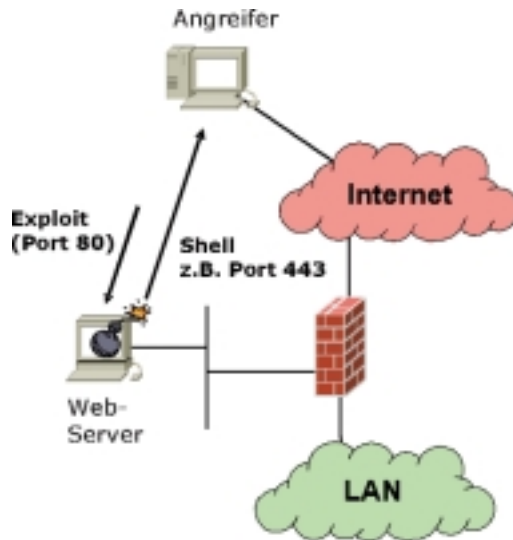
Eine sehr verbreitete Interpretation des IPS-Begriffs sind Intrusion Detection Systeme, die wie bisher auch schon Angriffe anhand von Mustern oder Protokoll-Abweichungen im Datenverkehr erkennen und als Reaktion auf den Angriff versuchen, diesen zu blockieren. Für diese Blockade kommen vor allem drei Techniken zum Einsatz:

- Beenden einer TCP-Session durch Reset-Pakete
- Blockade weiterer Kommunikation von der Quelladresse des Angriffs durch Einfügen temporärer Regeln in Firewall-Systeme
- Verwerfen der Pakete eines erkannten Angriffs in einem Inline-System, das den Datenverkehr als Gateway transportieren muss.

Die folgende Grafik stellt alle drei Varianten schematisch dar:



Die Probleme dieser Interpretation von Intrusion Prevention sind vielfältig. Angriffe, die mit Hilfe von automatisierten Exploit-Werkzeugen durchgeführt werden, sind meist in wenigen IP-Paketen enthalten und wirken sehr schnell. Das IDS/IPS kann den Angriff erst erkennen, wenn das Angriffsmuster schon auf dem Weg zum Opfer ist. Ein Reset-Paket, das vom IDS- bzw. IPS-System verschickt wird, kommt daher in vielen Fällen erst dann beim Täter oder Opfer an, wenn die erkannte Phase des Angriffs bereits beendet ist. Darauf folgende Schritte des Angreifers werden häufig über eigene Verbindungen erfolgen, die vom IDS/IPS nicht dem ursprünglich erkannten Angriff zugeordnet werden können. Die Effektivität einer Angriffsverhinderung über das Versenden von Reset-Paketen ist daher bei musterbasierten Systemen fragwürdig.



Auch das Einfügen temporärer Regeln in eine Firewall benötigt Zeit. Eine Sekunde oder auch zwei vergehen dabei je nach Firewall-Typ und Auslastung durchaus und in dieser Zeit kann ein automatisierter Angriff bereits abgeschlossen sein und als Ergebnis eine neue Verbindung mit interaktiver Eingabemöglichkeit zum Angreifer zurück aufgebaut haben.

Ein weiteres Problem der gerade beschriebenen Art von IPS-Systemen ist die Anfälligkeit für Denial-of-Service-Angriffe. Dabei wird das Prinzip des IPS selbst für einen Angriff missbraucht. Ein Angreifer täuscht Angriffe von verschiedenen wichtigen Partnern des Opfers vor. Daraufhin fügt das IDS/IPS temporäre Regeln in die Firewall ein, die sämtliche Kommunikation von den Quelladressen der vermeintlichen Angreifer blockieren. Damit kann das Opfer nicht mehr mit seinen wichtigen Partnern oder Kunden kommunizieren. Die vom Intrusion Prevention System erkannten Angriffe sind dabei nur Mittel zum Zweck für den eigentlichen DoS-Angriff. Es wäre allerdings technisch möglich, diesem Problem zu begegnen. Wenn das IPS vor dem Eingriff in die Kommunikation sämtliche TCP-Verbindungen überwachen würde, könnte es anhand der ausgetauschten Sequenznummern erkennen, ob die Quelladresse eines Angriffs offensichtlich gespoofed ist. Diese Methode funktioniert zwar nicht bei statusloser Kommunikation mit UDP, aber die meisten Angriffe werden ohnehin in TCP transportiert. In der Praxis unterstützen heute die wenigsten IDS- oder IPS-Systeme eine solche Verifikation der Quelladressen. Grund dafür sind vor allem die großen Datenmengen und der weitere Performance-Verlust eines ohnehin unter großer Belastung stehenden musterbasierten IDS/IPS.

Aber auch im normalen Betrieb wird ein Intrusion Prevention System, das auf der Erkennung von Angriffsmustern basiert, Probleme bereiten. Grund dafür sind die unvermeidbaren Fehlalarme, die schon bei einem klassischen, netzwerkbasieren IDS viel Arbeit verursachen. Diese Fehlalarme, auch „Falsch-Positiv-Alarme“ genannt, sind in einer reinen IDS-Umgebung nur lästige Hinweise, bei denen eines der Angriffsmuster in normalem

ungefährlichem Datenverkehr vorkommt und deshalb ein Alarm erzeugt wird, der überflüssig ist. In einer Intrusion Prevention Umgebung dagegen hat die Blockier-Reaktion des IPS auf einen Fehlalarm schlimme Folgen, da die Kommunikation unschuldiger Personen blockiert wird, falls das IPS innerhalb der Kommunikation fälschlicherweise glaubt, einen Angriff zu erkennen. In der Praxis werden solche Systeme deshalb während einer Testphase meist sehr schnell wieder außer Betrieb genommen.

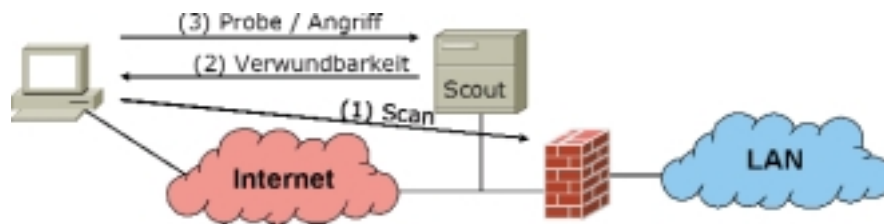
Die Reaktion der Hersteller und Berater auf dieses Problem ist gelegentlich das Feintuning der Erkennungsmuster und Regeln. Dabei versucht ein Berater, die Empfindlichkeit der Erkennung optimal einzustellen. Die entscheidende Frage ist, wo dieses Optimum liegt. Bei einem reinen IDS wird man einen Mittelweg suchen, bei dem weniger Fehlalarme auftreten, aber dennoch kritische Angriffe erkannt werden. Eine gewisse Menge von Fehlalarmen wird dabei aber bleiben. Bei einem IPS mit automatischer Blockade kann man sich diese Fehlalarme aber nicht leisten. Ein IPS, das „nur“ zehn Fehlalarme pro Tag erzeugt, bedeutet wahrscheinlich auch, dass sich zehnmal Anwender oder Manager beschweren, weil die Netzwerk-Infrastruktur nicht funktioniert. Um ein solches IPS dennoch betreiben zu können, muss sich das System auf die Erkennung der wenigen, eindeutig identifizierbaren Angriffe beschränken.

Ganz andere Eigenschaften haben Intrusion Prevention Systeme, die nicht auf der Technologie klassischer, netzwerkbasierter Intrusion Detection Systeme aufbauen. Dazu gehören Systeme, die auf den Servern oder Arbeitsplätzen das Verhalten ablaufender Prozessen überwachen und anhand einer Policy beschränken oder aber netzwerkbasierte Systeme, die mit dem Angreifer interagieren, um seine Intention herauszufinden.

Die Identifikation von Angreifern durch Nachweis ihrer Intention, ist eine Idee, die von der Firma ForeScout erstmalig in einem Produkt umgesetzt wurde. Der so genannte ActiveScout versucht erst gar nicht viele tausend Muster von potentiellen Angriffen zu erkennen, denn der musterbasierte Ansatz ist neben seinen Problemen mit Fehlalarmen auch ein dauerhafter Wettlauf gegen die Hacker, den man nie gewinnen kann. Jede neue Angriffsmethode muss zunächst bekannt werden, um dann in einem Muster abgebildet werden zu können. Da täglich neue Verwundbarkeiten von Systemen bekannt werden und Hacker ständig neue Werkzeuge entwickeln, um diese Verwundbarkeiten auszunutzen, muss ein musterbasiertes IDS ständig aktualisiert werden. Zwischen dem Erscheinen eines neuen Angriffs, der Verfügbarkeit eines Updates und dem tatsächlichen Einspielen der Updates auf allen Sensoren entsteht ein Zeitfenster, in dem man schutzlos ist. ForeScout geht deshalb einen anderen Weg. Nahezu alle tatsächlich durchgeführten Angriffe haben eine Gemeinsamkeit im Vorgehen des Angreifers. Dieses Vorgehen ist meist in mehrere Phasen gegliedert. Die erste Phase dient der Informationsgewinnung, die zweite dem Angriff über das Netz und weitere Phasen der Ausweitung seiner Rechte und dem Verwischen seiner Spuren. Zunächst wird ein Angreifer also nach Verwundbarkeiten suchen und erst wenn er weiß, wo er angreifen kann, wird er den ersten Angriffsversuch starten.

Die Methoden, die in der ersten Phase des Angriffs zur Informationsgewinnung verwendet werden, sind überschaubar und relativ einfach zu erkennen. Im Gegensatz zu über 4.000 verschiedenen Mustern, die ein klassisches, netzwerkbasiertes Intrusion Detection System kennt, um Angriffe zu identifizieren, ist es in der frühen Phase ausreichend, 15 bis 20 verschiedene Methoden der Informationsgewinnung zu erkennen. Selbstverständlich reicht das Sammeln von Informationen nicht aus, um auf einen tatsächlichen Angriff zu schließen. Forescout beantwortet deshalb diese Informations-Sammel-Zugriffe mit vorgetäuschten Schwachstellen auf vorgetäuschten Systemen. Mit geschickten dynamischen und lernfähigen Mechanismen wird der potentielle Angreifer in die Irre geführt. Er kann nicht zwischen möglicherweise tatsächlich vorhandenen Schwachstellen und vorgetäuschten Schwachstellen auf Servern, die es gar nicht gibt, unterscheiden. Sobald er jedoch versucht, eine vorgetäuschte Schwachstelle auszunutzen, ist er entlarvt. Es ist jetzt sicher,

dass er nicht nur Informationen sammelt oder nur zufällig auf eine falsche Adresse zugegriffen hat. Durch den Zusammenhang seines Verhaltens - dem gezielten Suchen nach Schwachstellen und dem darauf folgenden Angriffsversuch - ist die Intention des Angreifers bekannt und er kann ausgesperrt werden.



Dieses Prinzip erinnert in Teilen an bereits existierende Honey-Pot-Systeme. Im Gegensatz zu diesen wird ein Einbruch jedoch nicht zugelassen, sondern nur Schwachstellen vorgetäuscht. Sobald ein potentieller Angreifer tatsächlich versucht auf die Schwachstellen zuzugreifen, wird er blockiert.

Diese Methode der Erkennung der Intention eines Angreifers impliziert einige interessante Aspekte:

- Durch die Erkennung der Intention eines potentiellen Angreifers kann er ausgesperrt werden, bevor er überhaupt gefährliche Daten an ein Opfer schicken kann. Die üblichen Methoden, wie das Einfügen temporärer Firewall-Regeln, können bei rechtzeitiger Reaktion noch funktionieren.
- Das IPS kann sich auf die Überwachung von Zugriffen auf vorgetäuschte Verwundbarkeiten beschränken. Es müssen nicht alle anderen Datenströme mitverfolgt werden. Deshalb ist die Performance weit weniger kritisch als bei einem musterbasierten IDS und die oben beschriebene Verifikation von Quelladressen lässt sich durchführen.
- Da das System nicht auf der Erkennung bekannter Muster basiert, müssen auch nicht ständig neue Muster aktualisiert werden.
- Die Intentions-Erkennung liefert keine falschen Alarme, da tatsächlich eine Interaktion zwischen dem Angreifer und dem IPS stattfindet, die sich nur mit sehr viel Phantasie als ungewollt oder zufällig begründen lässt.
- Da es keine falschen Alarme mehr gibt, können sinnvolle statistische Auswertungen aus den erkannten Angriffen erzeugt werden.

Dieses Funktionsprinzip löst selbstverständlich auch nicht alle Sicherheitsprobleme der heutigen Zeit. Ein fiktiver Angreifer, der genau weiß, wohin er will und auf jedes Auskundschaften verzichtet, würde von dem oben beschriebenen System nicht erkannt. Gleiches gilt für Würmer wie den SQL-Slammer, die anstelle einer Informationsgewinnung in einem einzigen Paket schon den vollständigen Angriff an zufällige Adressen verschicken. Dennoch ist das Prinzip der Intentionserkennung von ForeScout, die als erster Hersteller dieses implementiert haben, ein sehr interessantes neues Feature. Es wird sicherlich in den nächsten Jahren von anderen Herstellern nachgebaut werden, denn es ergänzt andere Sicherheitssysteme um einen wichtigen Punkt: die Erkennung und Abwehr neuer Angriffstechniken, für die es bei klassischen Intrusion Detection Systemen noch keine Vergleichsmuster gibt. Dabei ist es unerheblich, ob der Angreifer eine reale Person oder ein Wurm-Programm ist. Außerdem sind die Betriebskosten einer solchen Lösung im Vergleich zu einer klassischen IDS-Lösung verschwindend gering.

Im Bereich der Web-Applikationen gibt es ebenso wie bei hostbasierten Systemen den Begriff der Intrusion Prevention. Näheres dazu erfahren Sie im zweiten Teil dieses Artikels.

Autor: Stefan Strobel, Geschäftsführer der Firma cirosec und Autor diverser Fachbücher, die in mehreren Sprachen erschienen sind.