

# Status und Zukunft von Intrusion Prevention Systemen (IPS)

Mathias Füglistaler, Daniel Lys  
Telekommunikation und Informatik  
mfueglistaler@bluewin.ch, lys.da@gmx.net

## 1. Abstract

Bisherige Sicherheitskonzepte basieren auf einer Firewall und einem Antivirenprogramm. Jedoch können diese Massnahmen bei weitem nicht mehr alle Gefahren abwehren. Die Angriffe werden immer komplexer und effektiver. Eine Firewall kann wohl ein Grossteil der Angriffe von Aussen abwehren, jedoch können Angriffe innerhalb des Netzwerkes so nicht verhindert werden. Auch werden Angriffe so getarnt, dass sie eine Firewall nicht mehr als solche erkennen und abwehren kann.

Um den neuen Gefahren entgegen zu treten braucht es neue, intelligente Abwehrmechanismen. Genau hier setzen die Intrusion Prevention Systeme ein. Sie sind eine Weiterentwicklung von Intrusion Detection Systemen und können Angriffe jeglicher Art abwehren.

Damit ein IPS funktionieren kann, müssen verschiedene Komponenten zusammenspielen. Normalizer, Service Scanner, Detection Engine und Traffic Shaper bilden dabei die Grundpfeiler. Das Zusammenspiel dieser Komponenten erlaubt es den Datenverkehr zu analysieren und entsprechende Massnahmen zu ergreifen, wenn ein Angriff erkannt wird. Da IPS sowohl Hostbasiert als auch Netzbasiert eingesetzt werden, können auch Angriffe aus dem eigenen Netzwerk effektiv erkannt werden.

Die Zukunft von IPS ist noch sehr ungewiss. Es gibt immer noch diverse Punkte, die zuerst abgeklärt werden müssen. Klar ist, dass die IPS mehr untereinander kommunizieren werden. Um den Ansprüchen gerecht zu werden, müssen auch die Hardware sowie die eingesetzten Algorithmen noch stark verbessert werden.

## 2. Body of Paper

### Einleitung:

Die ersten Rechnernetze wurden vorwiegend von Universitäten und Grossfirmen genutzt, um Informationen auszutauschen und Ressourcen gemeinsam zu nutzen. Durch die rasante Verbreitung des Internets sind immer mehr Leute miteinander vernetzt. Auch wird das Internet nicht mehr nur zum einfachen Informationsaustausch genutzt. Banktransaktionen, Steuererklärungen und

andere sensible Daten bahnen sich ihren Weg durch die Datenautobahn. Unter diesen Aspekten spielt die Sicherheit eine zunehmend wichtigere Rolle.

Eine Privatperson muss sich nicht speziell mit der Sicherheit seines eigenen Netzes auseinandersetzen. Anders ein Sicherheitsbeauftragter in einem grossen Unternehmen. Dieser kann an seine psychischen und physischen Grenzen stossen. Die Angreifer sind meistens intelligent, gut ausgerüstet und haben die entsprechende Zeit für einen Angriff. Auch geht hervor, dass die Angriffe nicht immer vom Internet her kommen, sondern viel häufiger vom eigenen Netz, beispielsweise von frustrierten Mitarbeitern. Vom Internet dringen meistens Viren und Würmer ins eigene Netz. Aus diesem Grund ist es wichtig ein System zu haben, das die „guten“ Bits von den „bösen“ Bits trennt.

Die Netzsicherheit kann in drei verschiedene Bereiche unterteilt werden: Authentifizierung, Integrität und Geheimhaltung. Authentifizierung verlangt, dass sich ein gegenüber zuerst ausweisen muss, bevor man miteinander kommuniziert. Die Integrität stellt sicher, dass Daten nicht verfälscht wurden. Geheimhaltung soll den unerlaubten Zugriff auf Daten oder Dienste verhindern. Alle diese Aspekte müssen bei der Planung eines Netzwerkes berücksichtigt werden.

### Gefahrenpotenzial

Die einzelnen PCs sind heute meist zu Netzwerken zusammen geschlossen. Dies ergibt viele Vorteile, wie gemeinsam genutzte Kapazität oder zentraler Speicherplatz für die Daten. Heutzutage sind die meisten Netzwerke über das Internet miteinander verbunden. Dies bringt jedoch gravierende Nachteile mit sich. Immer mehr Cyberkriminelle machen zwielichtige Geschäfte über das Internet. Diese können durch Lücken in der Software in ein Netzwerk eindringen oder durch das unbedachte ausführen einer Datei von einem Netzwerkteilnehmer eine Hintertür in das System einbauen.

Betrachten wir zuerst ein Heimnetzwerk. Dieses Netzwerk ist in der Regel klein und wird nicht ständig überwacht. Meistens werden nur ein Antivirenprodukt und eine Firewall eingesetzt. Damit ist ein Heimnetzwerk ausreichend geschützt.

Wenn wir jedoch grössere Netzwerke, wie Firmennetzwerke betrachten, kommt noch eine zusätzliche Gefahrenquelle hinzu. Nämlich ein Angriff von Innen. Diese Gefahr können wir bei den meisten Heimnetzwerken ausschliessen. Bei einer Firma ist diese Gefahr jedoch nicht zu unterschätzen. Selbst der Einsatz einer Firewall kann dies nicht verhindern. Eine Firewall nützt nichts, solange der Verkehr nicht über diese Firewall geleitet wird. Interner Verkehr muss nicht über die Firewall und kann somit eine Gefahrenquelle darstellen.

Ein kleines Beispiel hierzu. Ein Mitarbeiter fühlt sich ungerecht behandelt oder es ist ihm gekündigt worden. Der Mitarbeiter kann dies entweder akzeptieren oder er wird sich wehren. Er kann sich zum Beispiel an der Firma rächen, indem er Informationen oder gar Betriebsgeheimnisse kopiert und anschliessend der Konkurrenz zur Verfügung stellt. Dies kann nicht durch eine Firewall verhindert werden.

Eine Firewall bietet nur Schutz gegen Attacken von Aussen. Firewalls besitzen einige gravierende Nachteile. Eine Firewall hält den Port für jeden und jedes Programm offen oder hält diese geschlossen. Das heisst, wenn ein Angreifer einen offenen Port gefunden hat, kann dieser, ohne dass es die Firewall merkt, in ein Netzwerk eindringen und Schaden anrichten. Erfolgt ein Angriff, kann höchstens noch ein Antivirenprodukt Abhilfe schaffen.

Antivirenprodukte erkennen zurzeit die meisten Viren und Würmer, oft auch Spyware. Doch sind diese Produkte nur in der Lage, die beschriebene Malware korrekt zu erkennen, wenn es eine entsprechende Signatur dafür gibt. Die Heuristik in den Antivirenprodukten versuchen gegen die noch unbekanntes Gefahren zu schützen. Jedoch können Antivirenprodukte nicht erkennen ob sich eine Person auf einem System einloggen darf oder nicht.

### Die Antwort

Um die ungelösten Probleme (Person x darf sich auf einem System einloggen oder nicht, Angriffe von Innen und Aussen zu erkennen gegebenenfalls sogar abzuwehren) in den Griff zu bekommen, wurden sogenannte IDS (Intrusion Detection Systeme) also Einbrucherkennungssysteme entwickelt. Das Wort „Erkennung“ heisst, es wird erst etwas erkannt, sobald dies passiert. Im schlimmsten Fall ist zu diesem Zeitpunkt der Einbruch bereits in vollem Gange und kann eventuell gar nicht mehr oder nur noch sehr schwierig abgewehrt werden.

IPS (Intrusion Prevention System) also Einbruchverhinderungssysteme, sind eine Weiterentwicklung von IDS und sollten das gerade beschriebene Problem von der Erkennung lösen. Sie versuchen automatisch einen Angriff abzuwehren. Oftmals können Angriffe so verhindert werden, bevor sie überhaupt Schaden anrichten.

### IPS

Ein funktionsfähiges IPS besteht aus verschiedenen Komponenten. Normalizer, Service Scanner, Detection Engine und Traffic Shaper bilden die Grundpfeiler. Diese Komponenten sind bereits heute standardmässig in IDS integriert. Der **Normalizer** dient dazu, den Datenstrom zu normalisieren. Dazu gehören Verfahren wie das Defragmentieren des Verkehrs, Überprüfung der IP-Header Checksumme und Filterungen anhand von Access-Control-Listen (ACL).

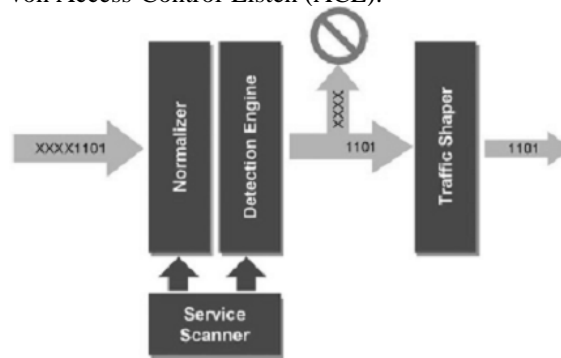


Abbildung 1: Komponenten eines IPS

Um möglichst alle Angriffe zu erkennen und abzuwehren, sollte sich das IPS wie das Zielsystem selbst verhalten. Dazu wird der **Service-Scanner** eingesetzt. Dieser stellt dem Normalizer und der Detection Engine wertvolle Informationen zur Verfügung. Diese Informationen benötigt der Normalizer um den Datenstrom richtig zu defragmentieren. Die **Detection Engine** entscheidet anschliessend anhand der defragmentierten Daten, ob es sich um einen Angriff handelt oder nicht. Wird ein Angriff erkannt, entscheidet ebenfalls die Detection Engine, ob das Zielsystem überhaupt verwundet werden kann. Besteht eine potenzielle Gefahr für das Zielsystem, verhindert das System das Weiterleiten des Datenverkehrs.

Der **Traffic Shaper** erfüllt zwei Hauptaufgaben, die Protokollklassifizierung und das Flow Management. Die Klassifizierung nach den Protokollen ist bereits heutzutage Standard. In Zukunft werden die Entscheidungen anhand der

verwendeten Applikationen des Benutzers getroffen.

Um die Effizienz eines IPS zu steigern, kommen verschiedene Methoden zum Einsatz. Damit wird eine minimale **False-Positive-Rate** angestrebt. Darunter werden das Verhältnis erkannter harmloser Angriffe oder gar irrtümlich blockierter Datenverkehr verstanden. Um solchen Fehlalarmen zuvor zu kommen, müssen verschiedene Analyse- und Ermittlungsverfahren gezielt eingesetzt werden. Dazu werden verschiedene Techniken zur Protokollidentifikation und -erkennung sowie Methoden zur Analyse des Datenverkehrs eingesetzt.

#### *Protokollidentifikation und -erkennung*

**Portzuordnung:** Das Hypertext Transfer Protokoll (http) belegt beispielsweise den Port 80. Verwendet ein anderes Protokoll diesen Port, erkennt das IPS sofort diese Abweichung und blockiert den Zugriffsversuch.

Mittels **Heuristischer Methoden** wird der gesamte Netzwerkverkehr ständig auf eindeutige Verhaltensmuster untersucht.

Meistens wird zusammen mit heuristischen Methoden das **Port Following** eingesetzt. Damit lassen sich bereits identifizierte Verbindungen überwachen. Dies ist ein wesentlicher Vorteil, da einige Anwendungen einen bestimmten Port zur Verbindungskontrolle und ein zufälliger Port für die Datenübertragung verwenden. Die ausgehandelten Ports werden vom Port-Following zu einer Gruppe zusammengefasst. Der gesamte Verkehr kann so auf schädlichen Code untersucht werden.

Hacker verschleiern oft ihre Angriffe, indem sie Datenpakete in andere Datenpakete verpacken. Um diese Angriffe zu erkennen, wird das sogenannte **Protocol Tunneling** angewendet. Damit lassen sich die getunnelten Protokolle erkennen.

#### *Datenverkehrsanalyse*

Die Datenverkehrsanalyse lässt sich in mehrere Methoden unterteilen. Die **Protokollanalyse** überprüft die einzelnen Protokolle auf ihr Standardverhalten und stellt Abweichungen fest. Somit können selbst Angriffe erkannt werden, die eine Schwachstelle ausnützen, die noch nicht bekannt ist.

Der **RFC Compliance Check** überprüft, ob die verwendeten Protokollen den Vorgaben der Internet Engineering Task Force (IETF) und deren

herausgegeben Request for Comments (RFC) entspricht.

Oftmals werden Schadprogramme von Hackern auf verschiedene Datenpakete aufgeteilt. Diese Fragmentierung macht es herkömmlichen Analysesystemen fast unmöglich den Angriff zu erkennen. Mit dem **TCP Reassembly** Verfahren lassen sich die fragmentierten Angriffscodes wieder zusammensetzen. Damit lassen sich die versteckten Angriffe erkennen und es können Gegenmassnahmen ergriffen werden.

Ähnlich wie beim TCP Reassembly Verfahren werden auch beim **Flow Assembly/ Simulation** die Datenpakete zusammengesetzt. Jedoch kann der gesamte Datenverkehr einer Verbindung ermittelt werden und so eine genaue Analyse durchgeführt werden.

Bei der **statischen Schwellenwertanalyse** wird ein Schwellenwert (Baseline) ermittelt und bei Abweichungen sofort Alarm geschlagen. Der Schwellenwert wird ermittelt, indem über einen gewissen Zeitraum der Netzverkehr überwacht wird. Erfolgt bei der Ermittlung des Schwellenwertes bereits Angriffe, werden diese als normale Auslastung aufgefasst. Spätere Attacken können dann vom System nicht als solche erkannt werden.

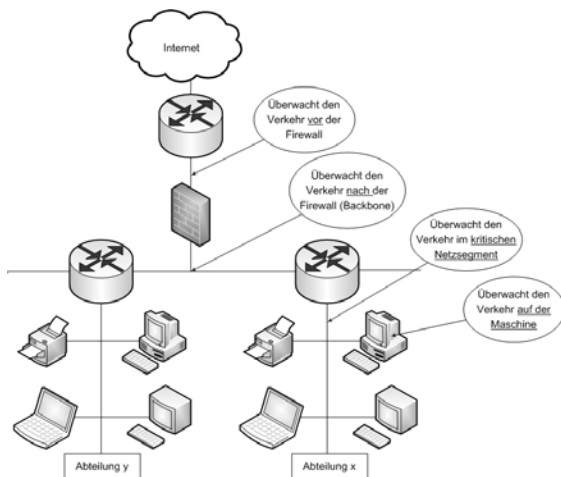
Die populärste Analysemethode ist das **Pattern Matching**. Hier werden die Datenpakete auf bestimmte Zeichenfolgen hin überprüft und mit einer Datenbank verglichen. In der Datenbank befinden sich Signaturen von bösartigen Zeichenfolgen. Mit dieser Methode lassen sich nur bekannte Attacken identifizieren. Neuer Schadcode muss zuerst erkannt und in der Datenbank gespeichert werden. Diese Methode wird bereits bei den Antivirenprogrammen erfolgreich eingesetzt.

Ein IPS kann auf zwei verschiedene Arten implementiert werden.

Netzbasiert: Hier wird der Verkehr auf dem zu überwachendem Netzbereich gescannt.

Hostbasiert: Hier wird der Verkehr auf dem zu überwachendem Host gescannt.

Keine der beiden Varianten ist perfekt. Jede hat ihre Stärken und Schwächen. Das untenstehende Bild zeigt die verschiedenen Positionen von möglichen IPS Sensoren.



**Abbildung 2: Position der IPS**

### Zukunftsvisionen

In Zukunft werden sowohl host- wie auch netzbasierte IPS eingesetzt. Damit wird eine möglichst grosse Sicherheit erreicht. Dabei werden die einzelnen IPS untereinander kommunizieren und sich austauschen. Somit lassen sich auch Angriffe von einem Insider aus dem eigenen Netz detektieren und abwehren.

Durch den immer grösser werdenden Netzverkehr und die grösseren Bandbreiten muss ein IPS sehr grosse Datenmengen in extrem kurzer Zeit überwachen. Um dies zu erreichen, reicht es nicht aus, leistungsfähigere Hardware einzusetzen. Auch die Mechanismen und Algorithmen müssen effizienter werden. Dabei wird eine false-positive-Rate von Null angestrebt. Ein Ausfall von Ressourcen aufgrund eines Fehlalarms wird nicht mehr geduldet. Man geht lieber das Risiko ein, einen Angreifer zu übersehen. Ähnlich wird es heutzutage schon bei den Antiviren-Programmen gehandhabt. Mittels Pattern-Matching werden die Schädlinge identifiziert und verbannt. Genau so wird es auch bei den IPS angewendet werden. Mittels Updatefunktionen werden laufend die aktuellen Patches eingespielt. Ob es jemals möglich sein wird, ein lernfähiges IPS zu entwickeln, das selbständig Angriffssequenzen erkennt und abblockt, ist eher unwahrscheinlich.

Nicht nur technisch werden sich die IPS weiter entwickeln. Auch im Marketing-Segment müssen Anstrengungen unternommen werden. Die Akzeptanz und zwangsläufig auch die Verbreitung von IPS sind heutzutage eher spärlich. Um dies zu verbessern, müssen sich die aktuellen IPS erst bewähren. Sie müssen beweisen, dass sie eine Anschaffung wert sind, wenn nicht sogar unentbehrlich sind bei der ganzen Flut von Angriffen. Das ganze Management eines solchen

Systems und vor allem auch die Visualisierung werden sich stark verbessern.

Bevor der Siegeszug der IPS voran schreiten kann, müssen auch rechtliche und moralische Fragen geklärt werden. Darf eine Firma den gesamten Netzverkehr seiner Mitarbeiter durchsuchen? Was darf die Firma sehen und was nicht? Dürfen aufgrund der Log-Dateien Mitarbeitern gekündigt werden? Diese und viele andere Fragen müssen zuerst noch geklärt werden und werden in Zukunft für die einte oder andere Schlagzeile sorgen.

### 3. Quellenverzeichnis

- [Bart04] Barth, Wolfgang: Das Firewall-Buch. Grundlagen, Aufbau und Betrieb sicherer Netzwerke mit Linux. 3, aktualisierte und erweiterte Auflage. Poing: Nicolaus Millin Verlag GmbH, 2004
- [Strob03] Strobel, Stefan: Firewalls und IT-Sicherheit. Grundlagen und Praxis sicherer Netze: IP-Filter, Content Security, PKI, Intrusion Detection und Applikationssicherheit. 3, aktualisierte und erweiterte Auflage. Heidelberg: dpunkt.verlag GmbH, 2003
- [FrGu05] Fritsch, Jörg / Gundel Steffen: Firewalls im Unternehmensinsatz. Grundlagen, Betrieb und Produkte. 2, überarbeitete und aktualisierte Auflage. Heidelberg: dpunkt.verlag GmbH, 2005
- [Kret07] Kretschmer, Michael (2007): „Die Türsteher: Intrusion-Prevention-Systeme“. URL: [http://www.securitymanager.de/magazin/artikel\\_1518\\_intrusion\\_prevention\\_systeme\\_ips.html](http://www.securitymanager.de/magazin/artikel_1518_intrusion_prevention_systeme_ips.html) [Stand 22.02.2008]
- [TrBu] Reto Trinkler, Reto Burkhalter : „Gefragt ist aktive Intrusion Prevention“ URL: [http://www.basis06.com/media/pdf/article\\_netzguide.pdf](http://www.basis06.com/media/pdf/article_netzguide.pdf) [Stand 30.04.2008]
- [Wes05] Wespi, Andreas: Intrusion Detection. Vorlesung "Network Security" IBM Zurich Research Laboratory (2005)

### 4. Abbildungsverzeichnis:

- Abbildung 1: übernommen aus [TrBu]
- Abbildung 2: selbst erstellt