Einführung eines Intrusion Prevention/Detection Systems bei der MTU Friedrichshafen GmbH

Diplomarbeit
in der
Fachrichtung
Informationstechnik
an der
Berufsakademie Ravensburg
Außenstelle Friedrichshafen

vorgelegt von
Ingenieurassistent (BA) Johannes Luther
TIT01-2NS
aus Ravensburg

durchgeführt bei
MTU Friedrichshafen GmbH, Abteilung ISI

1. Betreuer und Prüfer: Herr Dipl. Ing. Martin Kromer
2. Prüfer: Herr Prof. Dipl.-Inform. Erwin Fahr

Friedrichshafen, 20. September 2004

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit mit dem Titel

Einführung eines Intrusion Prevention/Detection Systems
bei der
MTU Friedrichshafen GmbH

selbstständig angefertigt, nicht anderweitig zu Prüfungszwecken vorgelegt, keine anderen als die angegebenen Hilfsmittel benutzt und wörtliche sowie sinngemäße Zitate als solche gekennzeichnet zu haben.

Friedrichshafen, den 20. September 2004

Johannes Luther

Kurzzusammenfassung

In den letzten Jahren stieg die Forderung nach weltweiter Datenkommunikation. Heute verfügt nahezu jede Firma, Organisation oder Privatperson über die Möglichkeit, sich mit dem Internet zu verbinden. Neben den vielen Vorteilen, die eine solche Anbindung bietet, verbergen sich auch Gefahren. Mit einer Firewall oder Anti-Virus Lösungen ist zwar ein guter Schutz geboten, jedoch reicht dieser meist nicht aus. Jede Verbindung die eine Firewall zulässt, kann jedoch auch potenziell gefährliche Datenpakete beinhalten. Durch Einbringen bestimmter Schadpakete in den zugelassenen Datenstrom lassen sich Sicherheitslücken im Betriebssystem oder in Anwendungen ausnutzen. Ein Beispiel ist der Wurm „SQL-Slammer“, der sich ohne Benutzerinteraktion, auf ungepatchten SQL-Servern des Herstellers Microsoft festsetzt.

Intrusion Prevention Systeme sollen Computer und Netzwerkkomponenten vor derartigen Angriffen schützen. Dies geschieht durch aktive und zeitnahe Untersuchung von Datenpaketen. So lassen sich schädliche Inhalte erkennen und gegebenenfalls herausfiltern, um das Netzwerk zu schützen. Im Rahmen der Diplomarbeit soll ein solches Intrusion Detection- bzw. Prevention-System in der MTU Friedrichshafen eingeführt werden.

Abstract

The requirement for worldwide data-communication has risen during the last few years. Nowadays nearly every company, organisation or individual has got the possibility to connect to the Internet. Although there are a lot of advantages due to this connection, there are also dangers. A firewall or an anti-virus solution is a good protection, but this is mostly not enough. Each connection, which is allowed by the firewall, could contain potentially harmful data. By dumping harmful packets in the legitimate data stream, security vulnerabilities in applications or the operating system could be exploited. For example the worm Slammer, which infects non-patched sql-servers of the producer Microsoft, without any user-interaction.

Intrusion prevention systems should protect computers and network components against these attacks. By active and realtime-analysis of data-packets, harmful contents can be detected and potentially dropped to protect the network. Such a intrusion prevention system will be established at the MTU Friedrichshafen in the context of this diploma thesis.

Inhaltsverzeichnis

1 Einleitung

1.1 Einführung

Die Bedrohungen aus dem Internet nehmen täglich zu. Nahezu jeden Tag findet sich eine neue Sicherheitslücke in einem Softwareprodukt, oder es taucht ein neues Schadprogramm auf. Innerhalb der letzten drei Jahre hat sich die Anzahl der gemeldeten Vorfälle, hervorgerufen durch Schadprogramme, nahezu versechsfacht (siehe Abbildung 1).

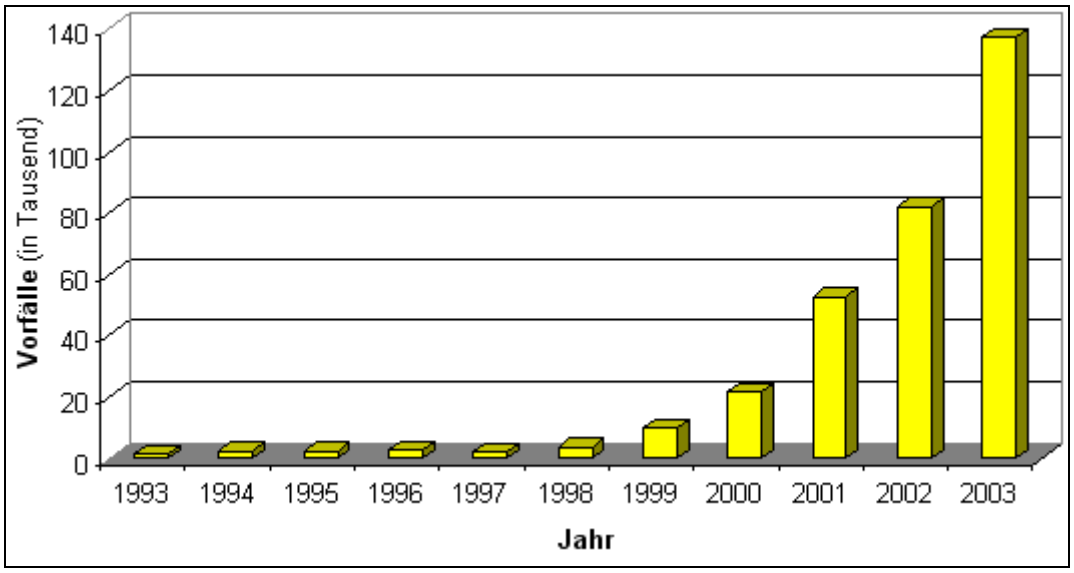


Abbildung 1 - Vorfälle hervorgerufen durch Schadprogramme (Quelle: CERT[1])

Da sich die Angriffsroutinen ständig weiterentwickeln und deren Effektivität steigt, sind neue Werkzeuge notwendig um diese Bedrohungen aus dem Internet abzuwehren. Zu den behandelten Sicherheitsmechanismen zählen u. a. Virenscanner, Firewalls und die, in dieser Arbeit angesprochenen Intrusion Prevention Systeme.

[1] URL: http://www.cert.org (Stand: 02.09.2004)

1.2 Projekteinbettung

Die Forderung nach weltweiter Datenkommunikation nimmt ständig zu. Immer mehr Kommunikationspartner müssen in der Lage sein mit einer Firma auf dem Datenweg zu kommunizieren. In der Regel sind die meisten Unternehmen mit einem permanenten Internetzugang ausgestattet, der im gesamten Netzwerk zur Verfügung steht. Jeder Verbindungsweg in einem Netzwerk bringt jedoch auch Gefahren mit sich. Als Beispiele hierfür sind Viren, Würmer und Cracker zu nennen.
Firewalls verhindern zwar unerlaubte Zugriffe, aber erlaubte Verbindungen können für Angriffe ausgenutzt werden, so dass eine Firewall alleine keinen umfassenden Schutz darstellt. Mit Hilfe eines Intrusion Detection/Prevention Systems lassen sich diese Gefahren weiter reduzieren.

1.3 Zielsetzung

Im Rahmen dieses Projektes ist ein Intrusion Detection/Prevention System bei der MTU Friedrichshafen GmbH einzuführen. Mindestens eine netzwerkbasierende und zwei hostbasierende Instanzen sollen mit Ende der Diplomarbeit installiert und funktionstüchtig sein.
Falls es eine Möglichkeit gibt, das IPS / IDS in ein Laptop Sicherheitskonzept zu integrieren, ist auch dafür eine Empfehlung für einen möglichen Einsatz auszuarbeiten.

2 Grundlagen der Netzwerksicherheit

2.1 Hauptbedrohungen für ein Netzwerk

2.1.1 Viren

„Ein Virus ist ein Programm, das sich replizieren kann, indem es sich an den Code von anderen Programmen anhängt - analog dazu, wie sich biologische Viren reproduzieren[2].“

Seit 1986 besteht die Bedrohung durch Computerviren. Die erste bekannte Virusinfektion verursachte der sog. Brain-Virus[3]. Er verändert den Bootsektor einer 5 1/4“ Diskette, nimmt aber keine Änderungen an der Festplatte vor[4].

Zurzeit existiert eine Vielzahl von Viren, deren Funktionsweise und Zerstörungsgrad sich in einem breiten Spektrum widerspiegelt. Ein Beispiel für einen harmlosen Virus ist Happy99. Dieser generiert ein Feuerwerk auf dem Bildschirm und gibt die Meldung „Happy New Year 1999“ aus[5]. Weitaus gefährlicher sind Viren mit Schadroutinen, die Hardware und Software angreifen können. Ein bekanntes Beispiel für einen zerstörerischen Virus ist CIH, der den gesamten Inhalt des BIOS unbrauchbar macht[6].

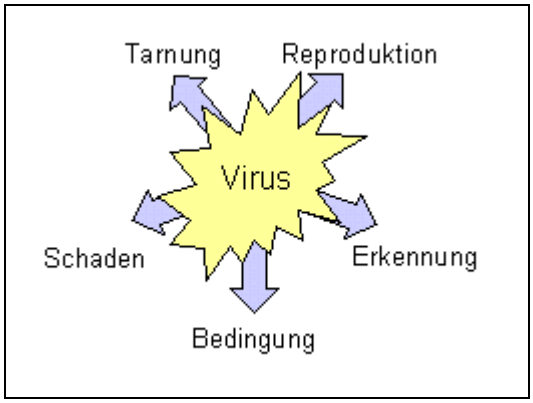


Abbildung 2 - Aufbau eines Virus

[2] Tanenbaum1 - S. 660

[3] Vgl. Hruska, S. 1

[4] Vgl. Sophos, Vireninfo: Brain

[5] Vgl. Oldfield, S. 32

[6] Vgl. ebenda, S. 31

Das hat zur Folge, dass der Rechner ohne einen neuen BIOS Chip nicht mehr funktionstüchtig ist.
Wie aus Abbildung 2 ersichtlich, setzt sich ein Virus aus fünf Teilen zusammen[7].
Im Reproduktionsteil vermehrt sich das Virus. Der Erkennungsteil überprüft, ob das System bereits infiziert ist. Die Auswirkungen für den PC sind im Schadensteil definiert. Hier ist festgelegt, wie sich der Virus in einem infizierten System verhält. Der Bedingungsteil gibt an, unter welchen Umständen, beispielsweise ein Datum, der Virus seine Schadroutine ausführt. Zuletzt kommt der Tarnungsteil des Virus, damit er vom Benutzer oder von der Antivirensoftware schwerer zu entlarven ist.
Die Verbreitungswege von Viren reichen von Datenträgern - wie die Diskette, bis hin zur Übertragung über das Internet via Email. Letzteres ist die gängigste Art der Verbreitung von Computerviren.

2.1.2 Würmer

„Würmer sind in ihrer Wirkung den Viren sehr ähnlich, allerdings benötigen sie keinen „Wirt“, wie z. B. ein Makro oder einen Bootsektor für ihre Verbreitung. Sie erzeugen Kopien von sich selbst und nutzen die Kommunikationskanäle zwischen Computern um sich zu verteilen[8].“

Viele Viren verhalten sich wie Würmer, da sie sich nach einer Infektion selbstständig per Email verbreiten. Andere Würmer sind ohne Interaktion mit dem Benutzer in der Lage ein System zu infizieren. Sie nutzen Sicherheitslücken in Betriebssystemen oder Anwendungssoftware aus, um sich auf anderen Systemen auszubreiten. Bekannte Beispiele sind Lovsan, MSBlaster, SQLSlammer, Sasser und deren Ableger. Variationen dieser Würmer enthalten lediglich verschiedenartige Schadroutinen, die Verbreitungsmethode bleibt jedoch immer dieselbe wie beim Vorgänger. Durch Einsatz des aktuellsten Sicherheitspatches, einer Firewall und einem Intrusion Prevention System kann ein hoher Schutzgrad erreicht werden.

---

[7] Vgl. BSI4, Kap. 1.2. Definitionen und Wirkungsweisen

[8] Vgl. Oldfield, S. 9

Um die Problematik dieser Würmer darzustellen, wird nachfolgend die Verbreitung und Infektion anhand des Wurms Sasser in Abbildung 3 erklärt.

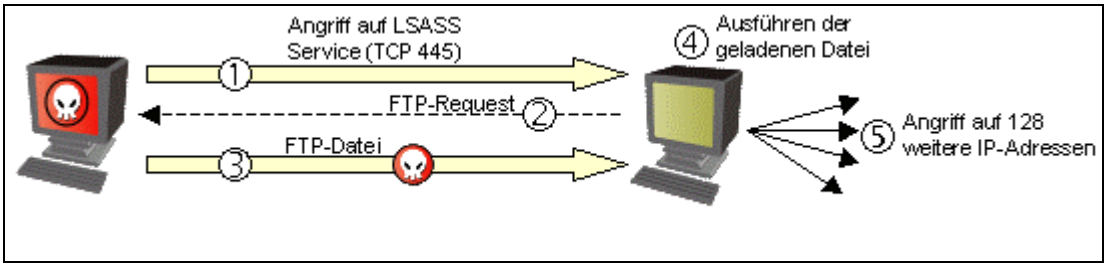


Abbildung 3 - Funktionsweise des Sasser Wurmes

Der Wurm Sasser und seine Variationen breiten sich über eine Sicherheitslücke im Dienst Local Security Authority Subsystem Service (LSASS) aus. Betroffene Betriebssysteme sind Windows 2000 und Windows XP.
Ein infiziertes System generiert zufällig 128 verschiedene IP-Adressen, beispielsweise aus dem lokalen Netzwerk des Clients. Der Wurm (1) spricht jede IP-Adresse auf dem LSASS Service (TCP 445) an und versucht, die Sicherheitslücke im LSASS Service auszunutzen[9]. Ein Pufferüberlauf ermöglicht es auf dem betroffenen System beliebigen Code auszuführen. Das Zielsystem stellt an den Angreifer eine FTP-Anfrage (2), lädt ihm das Schadprogramm (3) und führt es aus (4). Der Kreislauf wiederholt sich, das angegriffene System operiert nun als Angreifer (5).
Die Infektion und Weiterverbreitung dieses Wurmes geschieht automatisch, also ohne Dialog mit dem Benutzer. Ohne zusätzliche Schutzmechanismen wie eine Firewall oder Antivirus, ist die einzige Möglichkeit ein System zu schützen, ein aktuelles Sicherheitsupdate des Betriebssystems einzuspielen oder ein Intrusion Prevention System einzusetzen.

2.1.3 Trojanische Pferde

Ein Trojanisches Pferd erscheint als harmloses Programm. Es enthält Code, der eine unerwartete und unerwünschte Funktionalität ausführt[10]. Einerseits

[9] Sophos - Vireninfo: Sasser-A

[10] vgl. Tanenbaum1, S. 648

ermöglichen es Trojanische Pferde ein Endsystem mit einem Virus zu infizieren. Auf der anderen Seite ist ein harmloses Anwendungsprogramm, welches mit einem Virus infiziert ist, gleichzeitig ein Trojaner[11].
Weitere Arten von Trojanischen Pferden haben eine sog. Backdoor-Routine integriert. Ziel dieser Routinen ist es eine Hintertüre am befallenen PC zu öffnen. So haben u. a. Cracker[12] die Möglichkeit das System über Fernzugriff zu kontrollieren. Das Trojanische Pferd kann auf dem befallenen System alles das tun, was der Benutzer selbst tun kann[13]. Dazu schleust der Angreifer ein Programm in das Zielsystem ein und bringt den Benutzer dazu dieses Programm auszuführen[14]. Moderne Würmer platzieren auch ohne Interaktion einen Trojaner mit Backdoor. Ein Beispiel hierfür ist der Wurm CodeRed-II[15].

In Abbildung 4 ist die Funktionsweise eines Trojanischen Pferdes mit Backdoor-Routine, nach seiner Platzierung auf dem Zielsystem dargestellt.

[11] vgl. Hruska, S. 2

[12] Cracker sind Personen mit Computerfachkenntnissen, die im Gegensatz zu Hackern ihre Fähigkeiten grundsätzlich destruktiv einsetzen.

[13] Vgl. Tanenbaum1, S. 648

[14] Vgl. ebenda, S. 648

[15] Vgl. Sophos - Vireninfo: Troj/CodeRed-II

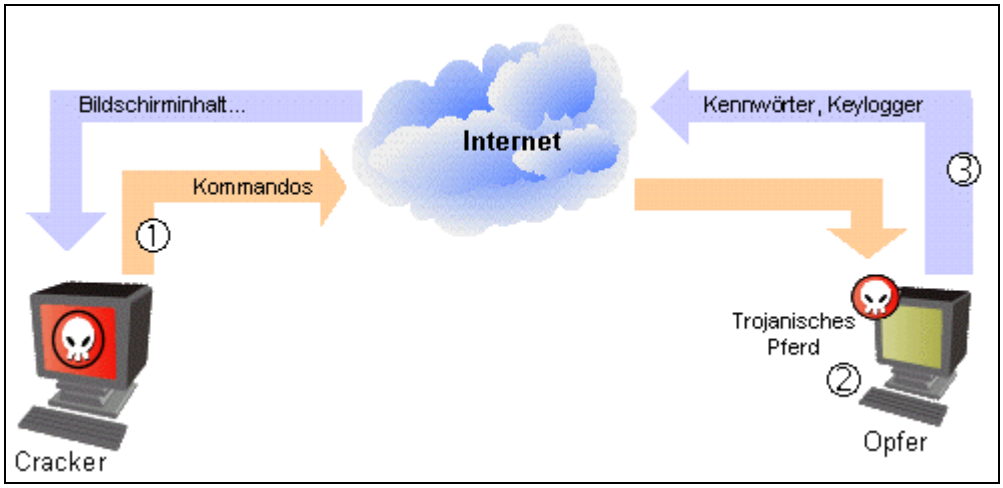


Abbildung 4 - Trojanisches Pferd mit Backdoor-Routine

Der Angreifer kann entsprechend der Implementierung des Trojaners, über die Hintertüre bestimmte Befehle auf dem Zielsystem ausführen. Bei dem Empfang der Befehle schickt das Opfer die entsprechenden Informationen an den Angreifer zurück. Diese Informationen können Aufzeichnungen der Tastatureingaben[16], Kennwörter oder der gesamte Bildschirminhalt sein. Die Variationen sind hier sehr vielfältig. Gesendete Befehle des Angreifers können auch das Verhalten des Zielsystems beeinflussen. Einige Trojaner begnügen sich damit Dialoge auf dem Bildschirm auszugeben oder das CD-Laufwerk zu öffnen[17].

2.1.4 Denial of Service

Eine weitere Bedrohung sind Denial-of-Service-Angriffe (DoS). Diese DoS-Angriffe beeinflussen die Systemverfügbarkeit. Auch jede Netzwerkkomponente ist ein potenzielles Ziel für einen DoS-Angriff, beispielsweise Router oder Firewalls. Zweck eines solchen Angriffes ist es massenhaft Ressourcen zu verbrauchen, beispielsweise durch belegen der CPU oder auffüllen der Platte mit sinnlosen Daten[18]. Weitaus zerstörerischer arbeiten Distributed Denial-of-Service-Angriffe

[16] Sog. Keylogger

[17] Sophos - Vireninfo Troj/CD-Argen

[18] Vgl. Tanenbaum1, S. 660

(DDoS). Diese Attacke ist verteilt über mehrere Rechner, die zu einem bestimmten Zeitpunkt gleichzeitig ein Ziel angreifen, wie in Abbildung 5 dargestellt.

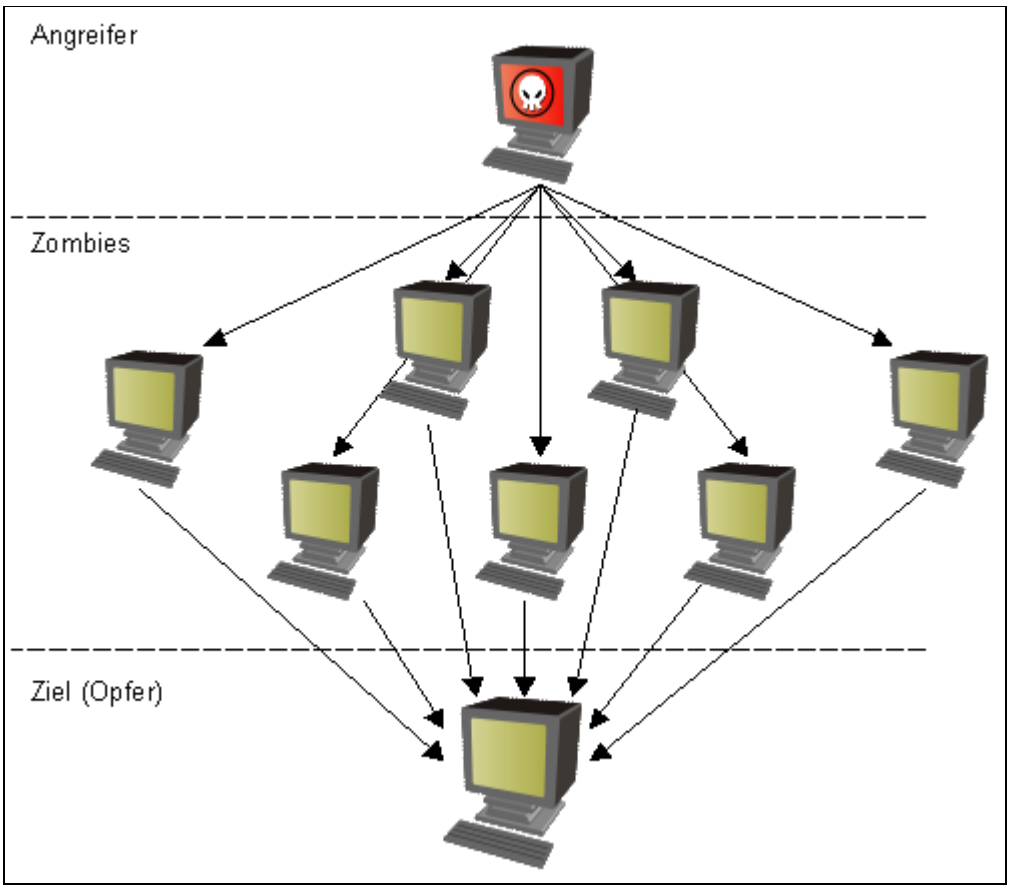


Abbildung 5 - Distributed Denial of Service Angriff

Dass DoS-Angriffe auch wirtschaftlichen Schaden mit sich bringen verdeutlichen die nächsten zwei Beispiele.

Der Wurm „MyDoom“[19] führte im Februar 2004 eine DDoS-Attacke gegen die Webseite der Firma SCO erfolgreich durch. Jeder infizierte Windows-PC mit Verbindung in das Internet flutete den Webserver von SCO mit http GET-Anfragen. Infolge dessen waren die Webserver von SCO über mehrere Stunden nicht erreichbar[20].

[19] Sophos - Vireninfo W32/MyDoom-A

[20] URL: http://www.heise.de/newsticker/meldung/print/44226 (Stand: 20.07.04)

Eine neue Motivation von DDoS-Angriffen ist, über Erpressung an Geld zu kommen. Pünktlich zur Fußball Europameisterschaft 2004 erhielten einige Online-Wettbüros[21] die Aufforderung, einen Betrag über 15.000 USD zu zahlen. Falls nicht, sei die Webseite des Wettbüros über eine längere Zeit nicht erreichbar[22].

Ein Beispiel für eine DoS-Attacke ist der sog. SYN-Flood. Bei einem normalen TCP-Verbindungsaufbau schickt der Sender eine SYN-Anfrage (Synchronize). Der Empfänger antwortet auf diese Anfrage mit einem ACK (Acknowledgement), welches der Sender quittiert. Damit ist eine TCP-Verbindung aufgebaut. Im Fall von SYN-Flooding schickt der Angreifer ein SYN, fälscht aber die Absenderadresse in ein nicht existentes System. Der Empfänger schickt darauf ein ACK zu dem nicht existenten System und bekommt, wie zu erwarten, keine Quittung. Die potenzielle Verbindung befindet sich jetzt beim Empfänger im SYN_RECV (Synchronize Receive) Zustand und verbleibt in einer Verbindungswarteschlange[23]. Nach Ablauf einer voreingestellten Zeit werden die Anfragen in der Warteschlange gelöscht. Falls der Angreifer gefälschte SYN-Pakete in kurzen Abständen schickt, nämlich deutlich kürzer als der Ablauftimer, kann er die Warteschlange komplett auffüllen. Daraus folgt, dass sich keine weiteren, legitimen Verbindungen zu dem Zielsystem aufbauen lassen.

2.1.5 Spyware

Spyware, auch als Adware bezeichnet, ist im Sinne der Verfügbarkeit von Systemen oder Datenintegrität keine Bedrohung für ein Netzwerk. Sie soll aber wegen der Vollständigkeit erwähnt werden.
Nach einer Studie von Earthlink und Webroot[24] ist Spyware mittlerweile auf Desktop-PCs mit Internet-Anschluss fast genauso verbreitet wie Standardsoftware. Viele Softwarepakete enthalten zusätzliche Spyware, die u. a. Informationen über

[21] U.a die Firma Mybet.com

[22] Vgl. c't DoS

[23] Vgl. Anti-Hack, S. 676

[24] Vgl. Earthlink

den Benutzer sammelt. Diese Informationen bekommt ein Spyware-Anbieter geschickt, der die im Computer gezeigte Werbung besser personalisieren kann[25].
In Trojanischen Pferden (Kapitel 2.1.3) ist oft auch ein Spyware-Anteil enthalten, wie z. B. Keylogger oder die Bildschirmbetrachtung. Es gibt Programme, die sich darauf spezialisiert haben, Spyware auf dem Rechner zu entfernen.

2.1.6 Sicherheitslücken und Bugs

Wie in Kapitel 2.1.2 bereits beschrieben, gibt es Würmer, die sich selbstständig in einem Netzwerk, über Sicherheitslücken im Betriebssystem oder Anwendungssoftware verbreiten können. In den meisten Fällen entdecken nicht Cracker Sicherheitslücken, sondern Softwarehersteller oder spezielle Sicherheitsfirmen. Die Hersteller antworten mit einem Patch für die jeweilige Software. Wie in Abbildung 6 zu sehen ist, kann es auch vorkommen, dass ein passender Exploit auch nach Bereitstellung eines Patches, eine Gefahr darstellen kann.

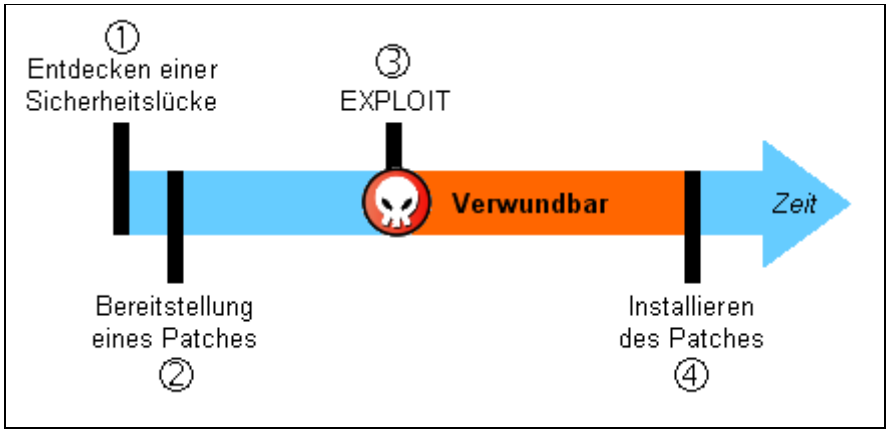


Abbildung 6 - Von der Lücke zum Exploit

Ein Exploit[26] ist ein Programm, welches ein Cracker ausführt, um Schwachstellen in der Systemsicherheit auszunutzen[27]. Im Fall von Sasser (vgl. Kapitel 2.1.2) gab es

[25] Vgl. Hacker's Guide, S. 197

[26] Exploit = englisch: to exploit - ausnutzen

[27] Vgl. Hacker's Guide, S. 91

den Patch[28] für den LSASS Service bereits zwei Wochen bevor Sasser erstmalig aufgetreten ist[29]. Wäre der Patch sofort nach Veröffentlichung installiert worden, hätten diese PCs einen Schutz gegen Angriffe von Sasser gehabt. Jedoch ist es gerade bei großen Firmen schwierig alle Maschinen sofort auf einen aktuellen Patchstand zu bringen. Diesen Vorgang zu automatisieren ist nicht empfehlenswert, da viele Patches einen Neustart des Betriebssystems benötigen. In Hochverfügbarkeitsumgebungen ist dies nicht ohne weiteres zu bewerkstelligen. Darüber hinaus kann man auch nicht sicher sein, ob der neue Patch mit der übrigen Software auf dem Server harmoniert.

2.1.7 Direkte Angriffe durch Personen

Bei den in den vorangegangenen Kapiteln beschriebenen Bedrohungen für ein Netzwerk, sind immer Personen verantwortlich. Die Beweggründe für einen Einbruch in Computersysteme oder dessen absichtliche Beschädigung sind unterschiedlich. Wie in Kapitel 2.1.4 bereits beschrieben, ist ein mögliches Motiv einen wirtschaftlichen Nutzen aus einem Angriff zu erzielen. Des weiteren gibt es auch Personen, welche es als Herausforderung sehen in ein System einzubrechen. In den meisten Fällen ist diese Person hoch qualifiziert und bereit, der Herausforderung eine beträchtliche Menge Zeit zu widmen[30]. Der Volksmund bezeichnet sie als Hacker. Im Internet und in der Literatur gibt es verschiedene Auffassungen zur Definition von Hackern und Crackern. Die am meisten verbreitete Variante lautet: „Ein Hacker ist ein Individuum, das sich in hohem Maße für die geheimnisvollen und verborgenen Arbeitsabläufe von Computerbetriebssystemen interessiert[31].“ Seine Absicht ist jedoch nicht in ein Computersystem einzudringen um dort Schaden anzurichten. Im Gegensatz dazu steht der Ausdruck Cracker.
„Ein Cracker ist eine Person, die in böswilliger Absicht in Rechnersysteme eindringt oder deren Integrität anderweitig beschädigt[32].“ Diese Aktionen haben oft die Zerstörung von Daten, Denial of Service Attacken oder Spionage zur Folge.

---

[28] Vgl. MS-Security1

[29] http://www.heise.de/newsticker/meldung/47037

[30] Vgl. Tanenbaum1, S. 625

[31] Hacker’s Guide, S. 79

[32] Vgl. ebenda

2.2 Netzwerksicherheitssysteme

2.2.1 Firewall

Eine Firewall dient der Kontrolle der Kommunikation zwischen zwei Netzen. Im Regelfall setzt man sie zum Schutz eines Netzes gegen Angriffe aus einem Netz mit einem geringeren Schutzbedarf ein, z. B. bei der Anbindung eines zu schützenden Teilnetzes an ein organisationsumspannendes Netz oder der Anbindung eines Firmennetzes an das Internet[33]. Mit modernen Firewall-Appliances ist es möglich mehr als zwei Netze miteinander zu verbinden. In diesem Fall sind Firewalls gemeint, die auf Paketfilter basieren. Diese Firewalls sind in der Regel Router, die über Funktionen zur Paketfilterung verfügen[34].
Eine Firewall-Policy definiert, welcher Verkehr zwischen den einzelnen Firewall-Segmenten erlaubt oder verboten ist. Da die Firewall auf der Ebene drei und vier im OSI-Schichtenmodell operiert, wird eine Policy anhand der IP-Adresse und des verwendeten Übertragungsprotokolls aufgesetzt (siehe Bsp. Tabelle 1).

Nr.	Quelle (Host/Netz)	Ziel (Host/Netz)	Service	Aktion
1	192.168.1.0 / 24	ANY	tcp/80	accept
2	192.168.1.43	ANY	tcp/21	accept
3	ANY	ANY	ANY	drop

Tabelle 1 - Beispiel einer Firewall Policy

Ein an der Firewall eingehendes Paket wird sequentiell mit der Policy verglichen. Falls das Paket zu einer Regel passt, kommt diese Regel auch zur Anwendung, unabhängig davon welche weiteren Regeln in der Policy definiert sind. In der Fachsprache nennt man diese Vorgehensart First-Match. Im Beispiel aus Tabelle 1 dürfen alle Endgeräte aus dem Netz 192.168.1.0 / 24, den Service http (tcp/80) in das angeschlossene Zielnetz verwenden. Der Host 192.168.1.43 hat zusätzlich die

[33] Vgl. BSI-Grundschutz, S. 194

[34] Vgl. Hacker's Guide, S. 244

Berechtigung den Service FTP (tcp/21) zu nutzen. Alle anderen Pakete verwirft[35] die Firewall.

Die NAT-Funktionalität[36] von Firewalls bietet einen kleinen Schutz für ein internes LAN. Ursprünglich führte man Network Address Translation (NAT) ein, um das Problem des knapper werdenden IPv4-Adressraums (32-Bit) zu lösen. In internen Netzwerken findet deshalb ein privater Adressbereich, der in Tabelle 2 aufgelistet ist, seine Anwendung. Adressen innerhalb dieses Bereichs werden im Internet nicht geroutet. Mit NAT findet eine Übersetzung dieser Adressen in eine oder mehrere öffentliche Adressen statt.

Class	Netz	Anzahl der Hosts
A	10.0.0.0 / 8	16.777.214
B	172.16.0.0 / 12	1.048.574
C	192.168.0.0 / 16	65.534

Tabelle 2 - Private Adressbereiche

Da die internen Adressen im privaten Netzbereich liegen, scheint der gesamte Verkehr hin zum öffentlichen Netz vom NAT-Gerät selbst zu stammen - also von der Firewall. Von außen ist es einem Angreifer nicht möglich Informationen über die interne Topologie zu erhalten[37].

Eine DMZ, wie in Abbildung 7 erklärt, schafft einen abgesicherten Bereich. Falls es einem Angreifer aus dem Internet gelingt einen öffentlichen Server zu kompromittieren, ist das interne LAN weiterhin durch die interne Firewall geschützt. In einer DMZ kommen typischerweise Web-, externer DNS- und Mailserver zum Einsatz.

[35] Fachausdruck: drop (engl.)

[36] RFC 1631 (http://www.ietf.org/rfc/rfc1631.txt?number=1631) - Stand 12.08.2004

[37] Vgl. Hacker's Guide, S. 465

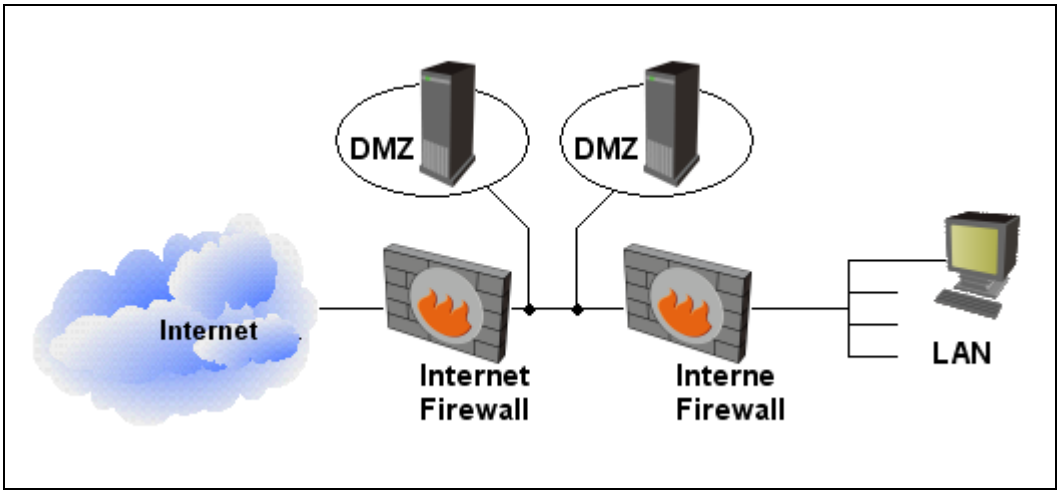


Abbildung 7 - DMZ Konzept

Wie aus Abbildung 7 ersichtlich ist, befindet sich die DMZ zwischen der internen und der externen Firewall, um unberechtigte Zugriffe von außen und innen zu unterbinden. Das DMZ Konzept ist auch mit einer Firewall realisierbar, falls diese die geforderte Menge an Anschlüssen bietet.

Wenn es einem Angreifer gelingt einen Server in der DMZ zu übernehmen, hat er prinzipiell die Möglichkeit, alle Server im selben Netz anzusprechen, selbst wenn diese nicht direkt von außen erreichbar sind. Eine erhöhte Sicherheit ist gewährleistet, falls sich jeder Server in einer eigenständigen DMZ befindet. Für die Kommunikation zweier Server in einer DMZ ist somit ein Router nötig. Diese Funktion deckt die Firewall ab. Ein Angreifer muss folglich die Firewall überwinden, um einen Server in einer anderen DMZ zu erreichen.

Die meisten Firewalls sind nicht transparent. Wie schon zuvor erwähnt, übernehmen sie auch die Rolle eines Routers. Von außen sind die Schnittstellen der Firewall über ihre IP-Adresse ansprechbar. Dadurch sind sie durch DoS-Angriffe (siehe Kapitel 2.1.4) verwundbar[38].

Zudem ist ein Unternehmen durch den Einsatz einer Firewall nicht vollkommen abgesichert. Eine Firewall definiert lediglich, wer für welche Art von Zugriff zugelassen ist. Jedoch ist nicht sichergestellt, ob der zugelassene Verkehr keinen Schaden für das Netzwerk darstellt. Ein Beispiel soll dies verdeutlichen. Auf den Webserver einer Firma darf in der Regel jeder über den Dienst http zugreifen. Falls

[38] Vgl. Hacker's Guide, S. 244

der Webserver eine Sicherheitslücke in der http-Verarbeitung aufweist, ist jeder in der Lage diesen anzugreifen. Die Firewall ist nicht in der Lage einen solchen Angriff zu erkennen, noch ihn zu unterbinden. Der Wurm Nimda nutzt z. B. eine Schwachstelle im IIS (Internet Information Server) aus, um über eine modifizierte http-Get-Anfrage eine infizierte Datei auf den Server zu kopieren[39].

2.2.2 Proxy

Spricht man von einem Proxy, dann ist in den meisten Fällen ein Gateway gemeint. Eine Funktion eines Proxyservers ist, die Kommunikation mit einem anderen Server über verschiedene Protokolle, wie http, ftp oder Telnet[40], herzustellen. Der Web-Proxyserver nimmt beispielsweise http-Anfragen von einem Client entgegen und übersetzt sie in ein anderes Protokoll, wie ftp. Dadurch muss der Browser des Clients nur das Protokoll http beherrschen, kann aber dennoch weitere Dienste nutzen[41].

Nach Abbildung 8 beherrscht der obere Browser das FTP Protokoll und benötigt keinen Proxy-Server. Darunter nutzt ein reiner http-Browser einen Proxyserver, der die FTP-Datenübertragung durchführt.

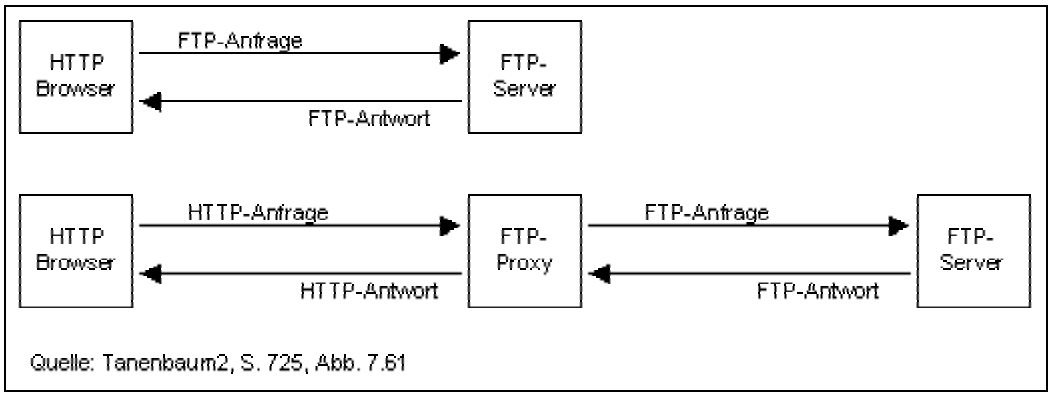


Abbildung 8 - Proxy als Übersetzer

[39] Vgl. Sophos - Vireninfo W32/Nimda-D

[40] Telnet = virtuelles Terminal

[41] Vgl. Tanenbaum2, S. 725f.

Ein Proxyserver kann auch als Sicherheitseinrichtung dienen. Ein Web-Proxyserver legt dabei eine Restriktion auf den Internetzugriff. Jede Kommunikation zum Internet läuft über den Proxyserver, der die eigentliche Anfrage an den entfernten Server schickt[42]. Mit Einbindung einer Verbotsliste, auch Blacklist genannt, lässt der Proxyserver z. B. Anfragen auf Seiten mit gewalttätigen oder pornographischen Inhalten nicht zu. Zur Entlastung der oft teueren Verbindung ins Internet bleiben bereits angefragte Seiten auf dem Proxy zwischengespeichert. Zwischengespeicherte Verbindungen zu einer Seite bedient der Proxyserver dann direkt[43].
Mit Hilfe einer Benutzerliste lässt sich einschränken, welche Personen Anfragen in das Internet schicken dürfen.

Ein Web-Proxyserver soll aus Sicherheitsgründen in einer DMZ stehen. Falls es einem Angreifer gelingt, sich auf eine bestehende TCP-Verbindung zu setzen und diese zu übernehmen[44], kann er ggf. durch eine Sicherheitslücke den Proxyserver übernehmen. Aufgrund der Tatsache, dass der Web-Proxyserver in einer DMZ steht, sitzt der Angreifer dort fest. Im Regelfall dürfen keine Verbindungen, die vom Proxyserver initiiert werden in das interne Netz aufgebaut werden.

2.2.3 Antiviren-Software

„Antiviren-Software erkennt Viren, verweigert den Zugriff auf infizierte Dateien und kann häufig auch Viren entfernen[45]“.

Die meisten Antiviren-Hersteller bieten mittlerweile auch die Erkennung von Trojanern und Würmern an. Um die Schadprogramme zu entlarven, bedienen sie sich verschiedener Techniken. In den meisten Fällen scannt man nach Viren. Diese Methode erkennt Viren, welche zum Zeitpunkt der Herstellung des Scanners bereits existieren. Die Informationen über neue Viren müssen in regelmäßigen Abständen dem Scanner zur Verfügung gestellt werden, um den Schutz zu gewährleisten. Diese Art von Antiviren-Software wird Malware-spezifisch genannt. Virenscanner

[42] Vgl. Tanenbaum2, S.725f.

[43] Vgl. ebenda

[44] Vgl. Anti-Hack, S. 725

[45] Oldfield, S.16

können beim Zugriff auf Dateien zum Einsatz kommen, d. h. sie überprüfen vor dem Zugriff auf eine Datei oder einem anderen infizierbaren Objekt den Inhalt und warnen den Benutzer, falls eine Gefahr davon ausgeht. Bei Bedarf kann auch ein gesamter Scan über eine Auswahl von Objekten, wie eine gesamte Partition, erfolgen[46].

In Emailservern gehören Virenscanner, die Anhänge untersuchen, mittlerweile zur Standardausrüstung. Viele Umgebungen sind sogar so restriktiv, dass Anhänge mit bestimmten Dateiendungen oder verdächtigen Namensstrukturen, im Mailserver sofort geblockt werden. Beispiele dafür sind ausführbare Dateien (*.exe; *.com; *.pif) oder Scripts.
Weitere Ansätze zum Aufspüren von Viren sind über Prüfsummen und heuristische Methoden realisiert. Der Vorteil besteht darin, dass dazu nicht die aktuellsten Virensignaturen nötig sind. Jedoch ist die Anzahl der Fehlalarme größer als bei den Virenscannern. Mit Prüfsummen-Tools lässt sich der Virus erst feststellen, wenn es zu spät ist - also nach der Infektion einer Datei[47].

2.2.4 Anti-Spam-Systeme

Spam ist ein Synonym für Massen-Emails. Diese Müll- und Wurfsendungen in elektronischer Form, die oft kommerzieller Art sind, werden auch Unsolicited Commercial E-Mails (UCE) genannt, was soviel bedeutet wie unaufgeforderte Werbe-Emails[48]. Laut des BSI entstehen durch Spam jährlich Kosten in Milliardenhöhe[49], die einerseits durch den Bandbreitenbedarf von 20-30 %[50] und andererseits durch die Bearbeitung dieser Mails anfallen.
Schutz gegen die Massen-Mails bieten Anti-Spam-Systeme, die z. B. in Mailservern integriert sind. Um zu erkennen ob eine Email Spam ist, wenden Anti-Spam Systeme verschiedene Techniken an. Fast alle Systeme analysieren den Email Header, der Aufschluss über den Absender gibt. Andere Möglichkeiten sind

[46] Vgl. Hacker's Guide, S.404f.
[47] Vgl. Oldfield, S.16f
[48] Vgl. BSI SPAM
[49] Vgl. BSI SPAM1
[50] Vgl. DFN-CERT

Textanalysen über den Betreff und den Inhalt der Email. Dabei werden Übereinstimmungen mit einzelnen Textfragmenten gesucht, die auf einen Werbeinhalt hindeuten. Anti-Spam-Hersteller stellen in den meisten Fällen Blacklisten zur Verfügung, die bekannte Absender von Spam beinhalten.
Anti-Spam-Systeme bieten nicht vollkommenen Schutz gegen Spam, sie filtern aber einen großen Anteil der Email-Spamflut heraus[51].

[51] Vgl. DFN-CERT

3 Intrusion Detection und Prevention Systeme

3.1 Grundlagen

3.1.1 Intrusion Detection Systeme

Intrusion Detection Systeme überwachen aktiv Computersysteme und -netze um Angriffe zu erkennen. Wichtige Randbedingung ist, dass die Erkennung und Alarmierung möglichst zeitnah geschieht[52]. Ein oder mehrere Sensoren erhalten die Daten, beispielsweise IP-Pakete, aus einer Netzwerkverbindung und werten diese aus. Im Gegensatz zu einer Firewall, die Datenpakete nur bis OSI Ebene 4 untersucht, analysiert ein IDS auch die höheren Anwendungsebenen. Dadurch ist es möglich, Angriffe durch Cracker oder Würmer wie Nimda, Blaster oder Sasser zu entdecken.

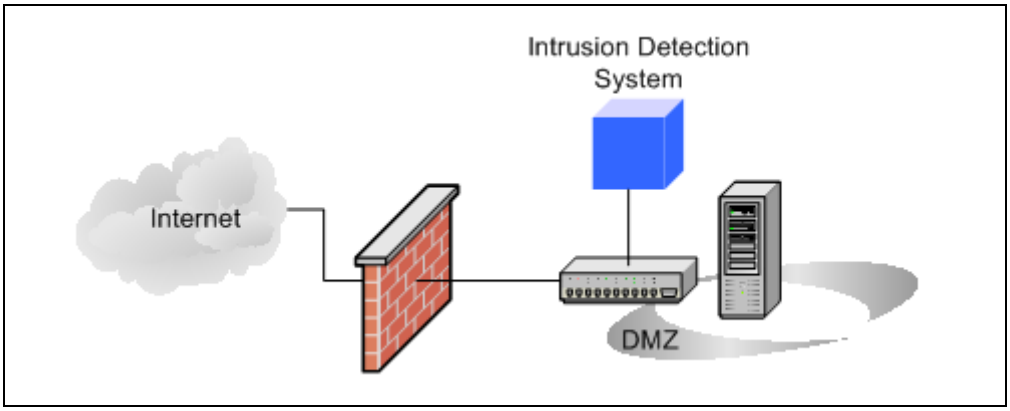


Abbildung 9 - Intrusion Detection System

In Abbildung 9 ist die Überwachung einer DMZ mit Hilfe eines Intrusion Detection Systems dargestellt. Der Anschluss eines IDS erfolgt über ein gespiegeltes Interface. Durch die gespiegelte Schnittstelle[53] erhält das IDS eine Kopie des gesamten Verkehrs zwischen Firewall und DMZ. Der Vorteil dieser Konstruktion ist, dass das IDS für das Netzwerk transparent ist und somit nicht direkt angesprochen werden kann. Ein Angreifer hat keine Möglichkeit die Existenz eines IDS

[52] Vgl. BSI2, S. 5

[53] engl.: SPAN Port

festzustellen. Weiterhin besteht die Möglichkeit mehrere Schnittstellen auf eine zu spiegeln, um dadurch mehrere Segmente zu überwachen. Dabei ist darauf zu achten, dass der Port über eine ausreichende Bandbreite verfügt, um auch bei hoher Last den Verkehr der Switch-Ports vollständig spiegeln zu können[54].
Durch die passive Installation des IDS ist es nicht möglich ein Netzsegment zu schützen. Falls ein Angriff stattfindet, erkennt das System die Bedrohung und alarmiert den Administrator, hat aber keine Schutzmechanismen um den Angriff zu stoppen. Bei erfolgreichem Angriff bleibt dem Administrator nichts weiter übrig, als den Schaden zu begrenzen. Um diese Schwäche auszubessern, verfügen handelsübliche IDS über ein zusätzliches TCP-Reset Interface. Bei einem Angriff schickt dieses Interface ein TCP-Paket mit gesetztem „RST“ (Reset Connection) Flag an den Angreifer zurück. Die Folge ist die Beendigung der TCP-Verbindung. Der TCP-Reset wird aber erst geschickt, nachdem der Angriff bereits sein Ziel erreicht hat. Deswegen ist die Wahrscheinlichkeit sehr hoch, dass einige Angriffspakete bereits ihr Ziel erreicht und Schaden angerichtet haben. Die zweite Schwäche dieser Verteidigung besteht darin, dass Angriffe mit dem verbindungslosen UDP-Protokoll nicht zurücksetzbar sind. Eine weitere Möglichkeit um einen Angriff zu unterbinden ist eine temporäre Änderung im Regelwerk der Firewall[55].

3.1.2 Intrusion Prevention Systeme

Im Gegensatz dazu sind Intrusion Prevention Systeme zum aktiven Schutz von Netzwerken konzipiert. Sie spielen die Rolle eines Gateways im Datenstrom. Sie sind ein erweitertes IDS mit einer zusätzlichen Blockfunktion. In Abbildung 10 ist ein IPS in einem Firewallnetzsegment eingebunden.

[54] Vgl. BSI2, S. 37

[55] Vgl. ebenda, S. 15

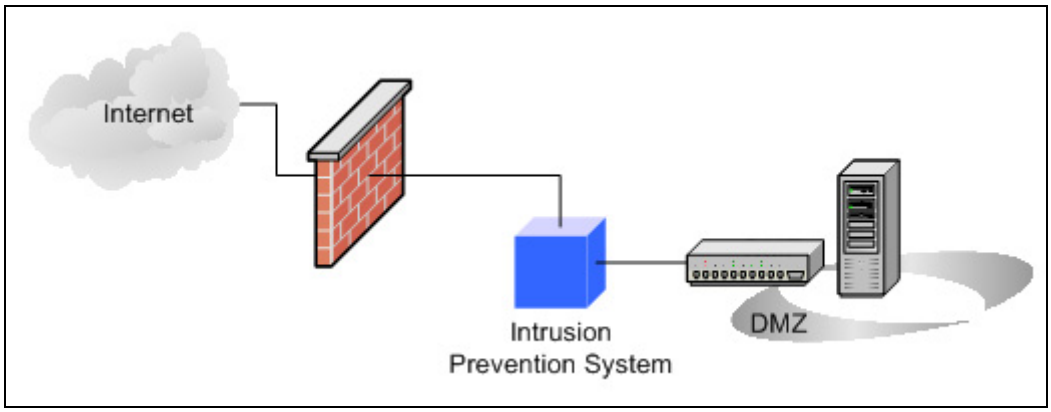


Abbildung 10 - Intrusion Prevention System

Nach der Untersuchung eines eingehenden Datenpakets entscheidet das IPS, ob es zu der ausgehenden Schnittstelle weitergeleitet wird.
Warum man überhaupt IDS einsetzt bzw. eingesetzt hat, ist schnell zu beantworten. Damit ein IPS in der Lage ist richtig zu funktionieren, müssen die Daten mit sehr hoher Geschwindigkeit vom System verarbeitet werden. Dabei darf die Verzögerung des Verkehrs, hervorgerufen durch die Bearbeitung der Pakete, nicht höher sein als bei einem Netzwerkelement wie Router oder Switch. Deswegen müssen IPS eine sehr hohe Systemleistung besitzen. Diese Leistung war bis vor kurzem für einen kommerziellen Erfolg zu kostenintensiv. Da Intrusion Prevention einen Schritt weiter geht als Intrusion Detection und nach Meinung des Autors auch mittlerweile IDS weitestgehend abgelöst hat, wird im weiteren Verlauf der Arbeit nur noch Intrusion Prevention behandelt.

3.1.3 Erkennungsmechanismen

Intrusion Prevention Systeme arbeiten, ähnlich wie eine Antiviren-Software, hauptsächlich mit zwei Erkennungsmechanismen. Das wohl geläufigste Modell ist die Erkennung mit Hilfe von Mustern oder Signaturen. Eine Signatur kann von der einfachen Zeichenanalyse bis hin zur Analyse von komplexen Verhaltensmustern gehen[56]. Beispielsweise ist ein CodeRed-II Wurm dadurch zu identifizieren, dass eine http Get/Post-Anfrage den String „CodeRedII“ enthält und erst nach dem

[56] Vgl. BSI2, S. 11

124sten Zeichen anfängt[57]. Durch unscharfe Signaturen können ähnliche Angriffe, wie Ableger eines Wurmes, mit einer einzigen Signatur erkannt werden[58].
Um die Erkennung eines Angriffes und den Schutz zu garantieren, muss das IDS/IPS immer einen aktuellen Signaturenbestand vorweisen. Das System ist nur in der Lage bekannte Angriffe zu erkennen und abzuwehren. Es ist aber möglich mit der Erkennung durch Signaturen auch unbekannte Exploits zu entlarven. Wie in Kapitel 2.1.6 beschrieben, ist eine Sicherheitslücke in vielen Fällen vor dem Erscheinen des jeweiligen Exploits bekannt. Durch Signaturen die auf Schwachstellen beruhen und nicht auf Exploits, ist ein Schutz auch vor dem ersten Auftreten einer Gefahr möglich. Anhand des CodeRed-II Wurmes wurde oben bereits ein Beispiel für eine exploitbezogene Signatur gezeigt. Eine schwachstellenbasierende Signatur spiegelt die Vorraussetzungen für die Ausnutzung der Sicherheitslücke wider.

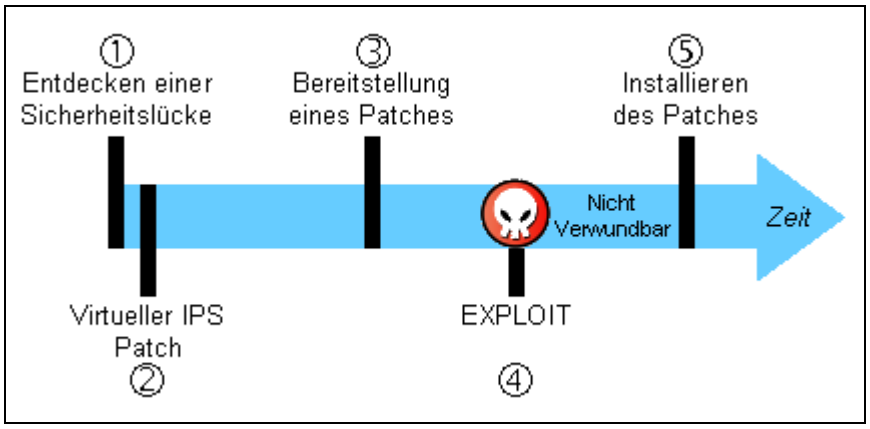


Abbildung 11 - Virtueller Patch

Das Bereitstellen einer schwachstellenbasierenden Signatur kann man mit einem virtuellen Patch für Endsysteme vergleichen. Die Sicherheitslücke besteht zwar weiterhin, aber der Angriff kommt nicht durch das IPS bis zum betroffenen Computer oder Netzwerkkomponente wie in Abbildung 11 dargestellt. Das Patchen eines Betriebssystems oder einer Software entfällt durch dieses Vorgehen nicht, es wird lediglich ein zusätzlicher Zeitpuffer geschaffen.

[57] Vgl. ISS Signature, /HTTP_Code_Red_II.htm

[58] Vgl. BSI2, S. 11

Einen weiteren Ansatz bietet die Anomalieerkennung. Diese Erkennungsart findet im kommerziellen IPS-Bereich keine sehr große Verbreitung, da die Realisierung und Wartung dieser Systeme kompliziert ist. Zudem generieren diese Systeme mehr Fehlalarme als Signatur-Basierende IPS. Die Protokollanalyse ist eines der am häufigsten genutzten Anomalieerkennungsmechanismen. Hier findet ein Vergleich zwischen dem Kommunikationsverkehr und den Protokollspezifikationen statt, da viele Angriffe auf Manipulationen des Netzprotokolls beruhen[59]. Die Anomalieerkennung wendet auch statistische Verfahren an. Dazu muss das IPS das Netzwerk in dem es eingesetzt wird erst einmal kennen lernen. Ein spezieller Trainingsmodus zeichnet zuerst über einen längeren Zeitraum das Normalverhalten des Netzwerks auf[60]. Nach der Lernphase meldet das IPS ein ungewöhnliches Verhalten im Netzwerk, welches vom Normalverhalten erheblich abweicht. Beispiele sind die Anzahl an fehlgeschlagenen Login-Versuchen, Tageszeiten des Zugriffs, Zugriffsdauer und Nutzungshäufigkeit[61]. Dieses Vorgehen hat jedoch Nachteile. Zum einen hat der Administrator die Aufgabe bei jedem Alarm zu entscheiden ob es dem Normalverhalten entspricht oder nicht, zum anderen ist es durch diese Technik nur möglich eine Alarmierung zu realisieren. Einen Schutz vor Bedrohungen kann ein solches System nicht bieten, da zur Feststellung von Anomalien ein Zeitraum analysiert werden muss. Diese Methode eignet sich ausschließlich zur ergänzenden Analyse[62].

3.2 Intrusion Prevention System-Komponenten

3.2.1 Netzsensoren

Netzsensoren (NIPS) suchen im Netzwerkdatenverkehr nach Angriffen. Jeder Verkehr der an der Netzwerkkarte ein- und ausgeht, erfasst ein IPS-Netzsensor. Um einen Schutz zu bieten, arbeiten die Sensoren meist mit Signaturen[63]. Normalerweise bieten Hersteller Netzsensoren als Appliance an. Bei einer

[59] Vgl. BSI2, S.12

[60] Vgl. Hacker's Guide, S.287

[61] Vgl. BSI2, S.12

[62] Vgl. ebenda

[63] Vgl. Hacker's Guide, S. 284

Appliance sind die Hardware und Software vom Hersteller vorgegeben und somit genau auf die Anforderungen an das System angepasst. Dadurch schließen sich Systemfehler durch die Wahl falscher Hardware oder Software nahezu aus.

Eine Netzsensor-Appliance bietet minimal zwei Überwachungsschnittstellen. Auf dem Markt gibt es bereits Lösungen mit mehr als zwei Schnittstellen, zur Überwachung mehrerer Netzsegmente durch eine Appliance. Aufgrund der Forderung nach Transparenz des Sensors, haben die Überwachungsschnittstellen keine IP-Adresse, vergleichbar mit einem Span-Port eines Switches. Dadurch ist es einem Angreifer nicht möglich den Sensor direkt anzusprechen oder seine Existenz festzustellen. Jedes eingehende Paket an einem beliebigen Überwachungsinterface vergleicht der Sensor mit dem Signaturenbestand. Bei einer Übereinstimmung eines schädlichen Paketes mit einer Signatur verwirft der Sensor das Paket und generiert ggf. einen Alarm. Wie in Abbildung 12 dargestellt, setzt man einen Netzsensor typischerweise an einem Übergang von einem sicheren- zu einem unsicheren Netzwerk ein. Für die angeschlossenen Endgeräte verhält sich der Sensor wie ein Netzwerkkabel. Um einen Netzsensor zu installieren bedarf es keines Eingriffs auf den zu überwachenden Endgeräten, er stellt auch keine zusätzliche Belastung für sie dar[64].
Ansprechbar ist der Netzsensor über eine Management-Schnittstelle. Durch diese Schnittstelle kann man die Appliance beispielsweise konfigurieren oder neue Signaturen bzw. Aktualisierungen aufspielen. Der Zugang zum Netzsensor sollte über ein abgesichertes Protokoll wie SSH erfolgen.

[64] Vgl. BSI2, S. 6

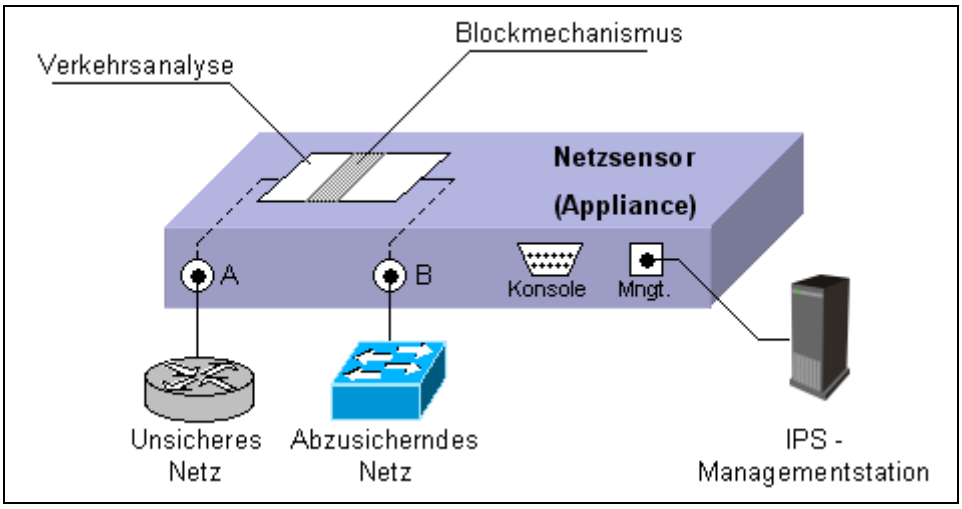


Abbildung 12 - IPS Netzsensor

3.2.2 Hostsensoren

Hostsensoren (HIPS) sind dadurch gekennzeichnet, dass sie Anwendungen auf dem zu überwachenden System sind[65]. Dabei findet eine Überprüfung des gesamten Verkehrs der Netzwerkschnittstellen des Computers, auf dem das IPS installiert ist, statt. Diese Methode findet Anwendung, falls der Schutz nur auf vereinzelten Rechnern gewährleistet sein muss oder Verschlüsselungstechniken eingesetzt werden. Auf jedem zu überwachenden Endgerät muss ein Sensor installiert sein. Vorteil von Sensoren auf Endgeräten ist die Fähigkeit verschlüsselten Verkehr analysieren zu können. Eine Analyse der Übertragung von Datenpaketen durch einen verschlüsselten VPN-Tunnel ist mit einer IPS-Appliance nicht möglich.

[65] Vgl. BSI2, S. 7

Neben dem hostspezifischen Netzverkehr ist ein HIPS auch in der Lage direkt die Anwendungen und das Betriebssystem zu überwachen. Dazu untersucht das HIPS beispielsweise Log-Dateien des Betriebssystems um Anomalien zu erkennen. Folgende Überwachungen sind grundsätzlich möglich[66]:

- Häufig fehlgeschlagene Anmeldeversuche
- Zugriffsverletzungen
- anomale Verhaltensmuster
- Änderungen wichtiger Systemdateien
- Überwachung spezifischer Anwendungen (SQL-Server, Exchange, IIS)

Da HIPS aktive Prozesse auf einem Host sind, belasten sie zusätzlich den Prozessor. Bei CPU-kritischen Systemen, wie. Echtzeitsysteme, kann das HIPS ein störender Faktor sein und deswegen nicht zum Einsatz kommen[67]. Dieses Verhalten kann dazu führen, dass das System durch den Einsatz des HIPS soweit ausgelastet ist und somit kein anderer Prozess genügend CPU-Zeit zugewiesen bekommt. Das entspricht einem Denial-of-Service-Angriff. Ein weiterer Nachteil ergibt sich daraus, dass ein HIPS nicht wie ein NIPS transparent ist, da der Sensor über die IP-Adresse des Hosts ansprechbar ist. Auch gibt es keine Gewährleistung, dass HIPS mit Software von Drittherstellern harmoniert.

3.2.3 Managementstation

Nahezu jedes IPS benötigt eine Managementstation (IPS-Server). Über sie erfolgt die Konfiguration und Kalibrierung des gesamten IPS. Der IPS-Server stellt auch, in Form von GUI oder Kommandozeile, die Schnittstelle zwischen Administrator und IPS zur Verfügung[68].

Angefangen bei der Hauptaufgabe der Managementstation, welche die Verwaltung aller Sensoren ist, stellt sie viele weitere Funktionen zur Verfügung. Auch hier ist die

[66] Vgl. BSI2, S. 7

[67] Vgl. Hacker's Guide, S. 286

[68] Vgl. BSI2, S. 9

Variation zwischen den Herstellern groß. Standardgemäß sollte die Managementstation die nachfolgenden Fähigkeiten besitzen.

Die Policyverwaltung spielt eine wichtige Rolle beim Umgang mit IPS. Die Einsicht oder Änderung des Regelwerks geschieht über die Oberfläche der Managementstation.

Um den Signaturenbestand aktuell zu halten, holt sich der IPS-Server periodisch Updates vom Hersteller und verteilt sie ggf. automatisch an die Sensoren.

Um die Datenhaltung zu optimieren und die Datenmengen, die ein IPS erzeugt zu bewältigen, stellt das Management meist auch eine Datenbankkomponente zur Verfügung. Gerade wenn es um schnelle Zugriffe und um zuverlässige Verwaltung geht ist dies sehr sinnvoll[69]. Im Fall von gängiger SQL-Server-Software, bietet sich dem Administrator durch SQL-Befehle die Möglichkeit an, benutzerdefinierte Auswertungen durchzuführen.

Die letzte wichtige Funktion des Managements ist die Auswertung der Daten. Dies beinhaltet die Anzeige und Aufbereitung der eingehenden Ereignisse, beispielsweise durch Sortierfunktionen und Filtermöglichkeiten. Mit richtiger Einstellung der Filter ist es dem Administrator möglich auf einen Blick die wichtigsten Eigenschaften eines Angriffs zu erkennen oder unwichtige Ereignisse auszublenden (siehe Tabelle 3).

Weiterhin besteht oft die Forderung Management Reports generieren zu können. Die Inhalte dieser Reports sind über einen definierten Zeitraum ermittelte Statistiken und Trends[70].

Prio	Sensor	Time	Tag Name	Source	Target	Block
▲	NIPS1	01.06.04, 13:58:00	CodeRed-II	230.12.6.21	192.168.30.5:80	YES
▲	NIPS3	01.06.04, 15:30:21	CodeRed-II	134.13.65.2	192.168.30.5:80	YES
□	HIPS1	01.06.04, 15:35:32	LoginFail	192.168.3.1	192.168.3.1	-
▼	NIPS1	01.06.04, 16:05:58	Portscan	215.05.24.4	192.168.30.2	NO

Tabelle 3 - Beispiel einer IPS-Auswertung

[69] Vgl. BSI2, S. 9

[70] Vgl. ebenda

3.3 Probleme von Intrusion Prevention Systemen

Trotz der angesprochenen Vorteile von Intrusion Prevention gibt es ebenso Nachteile, die gegen IPS sprechen. Ein IPS spielt eine zweitrangige Rolle bei der Datensicherheit und die Implementierung sollte erst erfolgen, nachdem alle wesentlichen Maßnahmen zur Datensicherheit bereits in Gang gebracht worden sind[71]. Es stellt keine Wunderwaffe im Kampf gegen Angriffe dar.
Des Weiteren basieren die meisten IPS auf Signaturerkennung, die eine ständige Aktualisierung des Systems fordert, um einen effektiven Schutz zu erhalten. Wie bereits in Kapitel 3.1 erwähnt, bietet die Signaturerkennung nur Schutz vor bekannten Angriffen oder Sicherheitslücken[72]. Um dieses Problem zu lösen gibt es die Anomalieerkennung. Mit ihr ist jedoch die Zahl der Fehlalarme beträchtlich höher als bei dem Signaturansatz.
Fehlalarme oder False-positives[73] sind ein weiteres Problem von Intrusion Prevention. Im schlimmsten Fall blocken diese Fehler legitimen Verkehr. Grund ist, dass man gerade bei der Anomalieanalyse, IPS nicht als exakte Wissenschaft interpretieren darf[74]. Es ist schwierig Regeln zu schreiben, die einerseits auch Variationen bekannter Exploits erfassen, andererseits aber definitiv keine benötigten Verbindungen treffen. Deshalb muss man die Regeln auf die spezielle Umgebung anpassen, um die Anzahl der Fehlalarme auf ein erträgliches Maß zu reduzieren[75]. Das Auswerten von Alarmen und das Erkennen von Gefahren benötigt erfahrenes Personal.

Intrusion Prevention Systeme sollen auf den zu schützenden Systemen das Ausnutzen von Sicherheitslücken verhindern. Diese Sicherheitslücken entstehen meist durch Fehler bei der Implementierung des entsprechenden Produktes. Jedoch ist nicht sichergestellt, dass IPS nicht selbst Sicherheitslücken aufweisen. Bewiesen wurde dies im März 2004 durch den Wurm Witty[76]. Dieser verbreitet sich über eine

---

[71] Vgl. Hacker's Guide, S. 283

[72] Vgl. ZDNet Snell

[73] False-positive= eine Bedrohung wird vom System nicht erkannt und darf passieren.

[74] Vgl. NetworkComputing, S. 30

[75] Vgl. HeiseSec

[76] Beschreibung: http://vil.nai.com/vil/content/v_101118.htm (Stand: 24.08.2004)

Sicherheitslücke in den Intrusion Prevention Lösungen der Firma ISS. Ein weiterer Beweis dafür, sich nicht alleine auf eine Sicherheitslösung zu verlassen.

Weiterhin gelten IPS als Erzeuger von Datenmüll. In einem stark frequentierten Netzwerk können sich so mehrere hundert Megabyte Daten pro Tag sammeln. Für einige Firmen besteht die gesetzliche Forderung, diese Daten auch noch Jahre nach der Aufzeichnung aufbewahren zu müssen[77]. Laut dem Sicherheitsexperten Pierre Noel des Consulting Unternehmens TruSecure, schalteten einige Kunden ihr IPS nach ca. zwei Wochen ab, um die anfallenden Datenmengen zu bezwingen[78].

Da IPS Appliances direkt im Netzstrom integriert sind, stellen sie auch eine potenzielle Fehlerquelle für die angeschlossenen Netze oder Endgeräte dar. Falls die Appliance defekt ist oder vom Stromnetz getrennt wird, muss der Datentransfer zwischen den Überwachungsschnittstellen weiterhin garantiert sein. Diese Option nennt man Fail-Open. In vielen Umgebungen ist das Gegenteil der Fall. Im Fehlerfall, sollen alle Pakete zwischen den Schnittstellen verworfen werden (Fail-Close).

3.4 Anforderungen an ein System

Um eine Einführung eines IPS möglichst konkret zu planen, sollte man vor der Anschaffung der nötigen Hardware, eine Anforderungsanalyse durchführen. Dieser Schritt ist nötig um einen passenden Hersteller zu finden, der die Kundenanforderungen am besten erfüllt. Besonders bei den NIPS-Sensoren ist darauf zu achten, dass sie sich in das vorhandene Netzwerk integrieren lassen. Dabei sind folgende Vorüberlegungen besonders wichtig[79]:

- Netzgeschwindigkeit der zu überwachenden Leitung (z. B. 100MBit/s)
- Maximale Verzögerung, die durch die Appliance verursacht wird (Latenz)
- Unterstützung der benötigten Netzprotokolle
- Im Fehlerfall die Fail-Open- oder die Fail-Close-Funktion

[77] Vgl. ZDNet Snell

[78] Vgl. ebenda

[79] Vgl. BSI1, S.67f.

- Verhalten des NIPS-Sensors beim Einspielen der Policy oder von Updates. Möglichkeit den Sensor in einem Simulationsmodus zu betreiben, damit der Verkehr nicht blockiert wird. Diese Funktion ist bei der Einführungsphase eines IPS sehr wichtig, um Auswirkungen auf den Netzverkehr einschätzen zu können
- Art der Erkennung von Angriffen (Signaturen, Anomalie)

Falls Hostsensoren zum Einsatz kommen sollen, ist eine Überprüfung der Verfügbarkeit der HIPS-Software für das entsprechende Betriebssystem nötig. Nicht jeder Anbieter bietet die Überwachungssoftware für jedes Betriebssystem an. Weiterhin ist zu prüfen ob das HIPS nur den hostspezifischen Netzverkehr überwachen muss, oder ob zusätzlich eine Prüfung der Applikationen und des Betriebssystems sinnvoll ist.
Bei Signaturerkennung ist besonders der Support des Herstellers ein ausschlaggebendes Kriterium. Hier sind die Updatezyklen und die Reaktion auf neue Bedrohungen sehr wichtig. Einige Hersteller erlauben das Definieren eigener Signaturen oder das Anpassen bestehender Signaturen. Des Weiteren soll eine detaillierte Beschreibung der einzelnen Signaturen vorliegen, die u. a. beschreibt unter welchen Umständen die Signaturen reagieren.

Ein IPS ist in der Lage verschieden auf Ereignisse und Angriffe zu reagieren. Dazu folgt ein Überblick über die wichtigsten Funktionen[80]:

- Benachrichtigung über Email, SMS oder SNMP
- Unterbrechung der Verbindung (TCP-Reset)
- Blocken des Angriffspaketes
- Aufzeichnen der Angriffspakete (Rohdaten-Log)
- Aufzeichnen der gesamten Kommunikation
- Ausführung von benutzerdefinierten Scripts oder Befehlen
- Automatische Rekonfiguration von Komponenten wie Firewall oder Router
- Aufzeichnung von nutzerspezifischer Aktivität über einen bestimmten Zeitraum

[80] Vgl. BSI1, S. 67f.

Als zusätzliche Aktion ist noch die Attacke gegen den Angreifer zu erwähnen. Diese Methode ist aber eine juristische Gratwanderung. Vor der Aktivierung dieser Funktionen ist auf jeden Fall juristischer Rat einzuholen[81]. Nicht jede Quelle eines Angriffes ist tatsächlich böswillig. Durch Infektionen mit Viren oder Würmer bemerkt ein Benutzer oft nicht, dass er Angriffe gegen ein entferntes System durchführt.

Die Managementstation muss ebenso grundlegende Vorraussetzungen erfüllen. Eine der wichtigsten Funktionen ist das automatische Installieren neuer Signaturen und Updates für die Sensoren. In der Regel muss die Managementstation dazu eine Verbindung zum IPS-Hersteller aufbauen können, um die Updates zu laden. Regelmäßige Updates sind eine Grundvorrausetzung für den Schutz vor neuen Angriffen. Was aber unter Umständen manuell zu geschehen hat ist die Einstellung, wie der Sensor auf neue Ereignisse reagieren soll[82]. Diese Einstellungen geben viele Hersteller bei Signaturupdates nicht vor, um nach dem Update sicherzustellen, dass legitimer Verkehr immer noch als solcher erkannt wird. Es sollte auch einfach möglich sein ein Backup der einzelnen Sensorpolicies, Sensorkonfigurationen und den Managementeinstellungen anfertigen zu können.
Falls IPS-Hersteller mehrere Sensorarten oder Produkte vertreiben, ist es hilfreich, dass die Verwaltung aller Sensoren unter einer gemeinsamen Oberfläche geschieht. Gerade wenn das IPS wächst und in einem Unternehmen viele Sensoren installiert sind, ist eine gemeinsame Managementstation und Oberfläche sehr wichtig.
Für die Sicherheit des Intrusion Prevention Systems, kann die Managementstation auch über eine Benutzer- und Rechteverwaltung verfügen. Damit ist jeder Benutzer in der Lage die Managementkonsole nach seinen Wünschen einzurichten. Zudem ist ein IPS-Administrator in der Lage für verschiedene Nutzer bestimmte Rechte zu vergeben, damit der Zugriff auf das IPS beschränkt und geregelt ist. Damit das Risiko der Manipulation der Managementstation und der Sensoren sinkt, soll die Kommunikation zwischen Sensoren und Management verschlüsselt erfolgen[83]. Wegen des Komforts ist eine GUI-Oberfläche heute üblich. Als Option stellen viele

[81] Vgl. ZDNet Snell

[82] Vgl. BSI2, S. 21

[83] Vgl. BSI1, S. 69

Hersteller zusätzlich einen Zugriff über Kommandozeile auf die Sensoren zur Verfügung.

Die Managementstation stellt in der Regel auch Funktionen zur Auswertung und Reportgenerierung zur Verfügung. Der Umfang hängt wieder stark vom Hersteller ab. Grundlegende Operationen sind beispielsweise:

- Reportgenerierung in verschiedenen Dateiformaten (HTML, PDF, CSV etc.)
- Automatische Reportgenerierung nach Zeitplan
- Benutzerdefinierte Reports und Auswertungen (Filter)
- Umfangreiche Such- und Auswertfunktionen für die Ereignisdatenbank

Viele Hersteller nutzen eine Datenbank für die Speicherung der Ereignisse und der Sensordaten. In der Regel stützen sie sich dabei auf die geläufigen Datenbanksysteme wie IBM DB2, Oracle oder den Microsoft SQL Server. Bei der Wahl eines Herstellers, kann auch das unterstützte Datenbanksystem ein ausschlaggebendes Kriterium sein. Falls ein Unternehmen beispielsweise Oracle einsetzt, bietet es sich an, auch ein IPS mit Oracle-Datenbank einzusetzen. Der Vorteil ist, dass man bereits bestehende Datenbankserver zur Datenhaltung nutzen kann.

3.5 Produkte

Zum Zeitpunkt der Produktuntersuchung für diese Arbeit, gab es nur wenige Hersteller von Intrusion Prevention Systemen.
Da das Netzwerk der MTU Friedrichshafen hauptsächlich aus Geräten der Firma Cisco und Enterasys besteht, boten sich diese Hersteller an.
Cisco bietet IDS Erweiterungskarten für einige Router und Switche an. Jedoch ist die Lösung von Cisco ein Intrusion Detection System und deshalb nur in der Lage Angriffe zu erkennen. Das Gleiche gilt für das Produkt „Dragon“ von Enterasys. Hier bietet der Hersteller eine eigenständige IDS-Appliance an. Dieses Produkt beschränkt sich auch auf die Erkennung und nicht auf die Abwehr.

Nach einem Test der NSS-Group[84] haben einige IPS sehr gut abgeschnitten. In diesem Test sind u.a. auch Funktionen getestet, welche in den Anforderungen nach Kapitel 3.4 bereits festgelegt wurden. Folgende Intrusion Prevention Produkte sind im NSS-Report vertreten:

- ISS Proventia G200 Revision A
- NetScreen-IDP 500 V3.0
- Network Associates McAfee IntruShield 4000 V1.8
- TippingPoint UnityOne-1200 V1.4
- Top Layer Attack Mitigator IPS 2400 V2.1

Die getesteten Produkte sind Network IPS-Sensoren. HIPS-Produkte sind nicht Gegenstand dieses Tests.

Um Interfaces zu sparen, werden bei der MTU verschiedene DMZ über VLANs abgebildet, die zur Firewall hin in einem 802.1q Trunk zusammengefasst sind. Aufgrund dieser Forderung konnten sich für einen potenziellen Einsatz nur die ISS Proventia G200 und der McAfee Intrushield 4000 qualifizieren. Der Intrushield bietet sogar die Möglichkeit für jedes VLAN in einem Trunk eine eigene Policy zu definieren.

Bestandteil dieses Projektes ist die Einführung einer netzbasierenden und zweier hostbasierenden IPS-Instanzen. Aufgrund dieser Vorraussetzung und der Forderung, dass sich HIPS und NIPS unter einer gemeinsamen Managementoberfläche verwalten lassen müssen, konnte sich der NAI Intrushield nicht für einen Einsatz bei der MTU qualifizieren. HIPS und NIPS sind bei NAI grundlegend verschiedene Produkte, welche sich einerseits von den Signaturen und vom Support, andererseits vom Management unterscheiden.
Deshalb fiel die Wahl auf die Proventia G200 von ISS. Diese Appliance kommt als NIPS zum Einsatz. Das HIPS-Produkt von ISS ist der Realsecure Server Sensor für die Betriebssysteme Windows 2000/2003 Server, Linux und Solaris. Der Realsecure Desktop Protector kommt auf Clients mit modernen Windows Betriebssystemen

[84] Vgl. NSS Report IPS

zum Einsatz. Alle ISS-Produkte sind über die Managementoberfläche Siteprotector konfigurierbar.
Eine tiefergehende Analyse folgt im Anhang: Anforderungsanalyse.

4 Vorbereitungen

4.1 Rechtliche Aspekte

Ein IPS sammelt Daten, die in vielen Fällen personenbezogen sind. Dies bedeutet, dass es möglich ist, eine Zuordnung von Personen zu durchgeführten Aktivitäten herzustellen. Je nach Konfiguration des IPS lassen sich dadurch z. B. fehlgeschlagene Loginversuche, Zugriffsverletzungen oder sogar Angriffe aufzeichnen[85]. IPS können sie auch legitime Vorgänge wie Emails oder Internetverkehr erfassen. Bei angepasster Policy ist beispielsweise die Erfassung und Protokollierung jeder http-Get-Aktivität möglich. Vorraussetzung dafür ist eine unverschlüsselte Übertragung der Daten. Einen Beispielauszug für legitime Benutzerdaten und Aktionen zeigt Tabelle 4.

Prio	Time	Tag Name	Source	Target / Data	User
▼	15.07.04, 08:21:45	http-GET	192.168.2.6	www.technik.ba-ravensburg.de/neu/	Max
▼	15.07.04, 08:30:54	http-GET	192.168.2.6	www.bild.de/bild.jpg	Max
▼	15.07.04, 08:30:55	eMail_Dat	192.168.2.9	215.56.42.14 / Sehr geehrte Damen u [...]	Gerd
▼	15.07.04, 09:20:28	http_login	192.168.2.9	www.gmx.de / Login: Mustermax; PW: test	Gerd

Tabelle 4 - Auszug aus Verkehrserfassung

Der Grad der Aufzeichnung von personenbezogenen Daten hängt stark von den Einstellungen der Policy des IPS[86] und dessen Standort ab.

Um den Arbeitnehmer zu schützen gibt es rechtliche Vorgaben beim Erheben von personenbezogenen Daten. Im Bundesdatenschutzgesetz (BDSG)[87] sind die meisten dieser Vorgaben festgehalten. Besonders zu beachten ist, dass es IPS-Administratoren untersagt ist personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Alle aufgezeichneten Daten unterliegen dem Datenschutz.

[85] Vgl. BSI3, S. 3

[86] Vgl. ebenda

[87] Link: www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm (Stand: 30.08.2004)

Beim Einsatz eines IPS sind besonders folgende Paragraphen des BDSG relevant[88]:

- §14 (2): Das Speichern, Verändern oder Nutzen [...] ist [...] zulässig, wenn es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten [...] erforderlich ist.
- §14 (4), §31: Personenbezogene Daten, die ausschließlich [...] zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage genutzt werden, dürfen nur für diesen Zweck verwendet werden.

Wenn sich die Sammlung personenbezogener Daten nicht vermeiden lässt, sind die betroffenen Mitarbeiter über das System und dessen Einsatzzweck zu informieren. Besonders der Betriebs- oder Personalrat ist in den Prozess der Einführung des IPS einzubinden. Generell gilt aber, dass die Auswertung der Daten nur zur Gewährleistung des ordnungsgemäßen Betriebs von DV-Anlagen erfolgt. Der Umfang der Datenerhebung muss sich auf das Erkennen von Angriffen, Angriffsversuchen und Sicherheitsverletzungen beschränken.
Die Mitarbeiter die mit den IPS arbeiten und berechtigt sind die gesammelten Daten einzusehen, sind auf das Datenschutzgesetz zu verpflichten[89].

4.2 Einsatzort von IPS Sensoren

4.2.1 Einsatz in der Firewallumgebung

Um den Standort eines Sensors in der Firewallumgebung optimal bestimmen zu können, ist die Kenntnis über die prinzipiell erlaubten Verbindungen nötig. Ein Intrusion Prevention System macht nur dort Sinn, wo die Firewall Lücken offen lässt. Um mit einem Sensor einen möglichst großen Bereich abzudecken ist es auch möglich, einen NIPS-Sensor vor die externe Firewall zu setzen (Position 1 in Abbildung 13). An diesem Standort kann der gesamte Verkehr am Netzübergang mitprotokolliert werden und deshalb ist die Platzierung an dieser Stelle grundsätzlich sinnvoll. Durch Einsatz eines NIPS-Sensors an Position eins lassen sich mehrere DMZ überwachen. Trotz dieser Vorteile ist der Einsatz an dieser Position nicht empfehlenswert. Je mehr Filterkomponenten zwischen dem unsicheren Netzwerk,

[88] Vgl. BSI3, S. 4f.

[89] Vgl. ebenda, S. 7

wie dem Internet und dem internen Netz vorhanden sind, desto geringer ist die zu erwartende Angriffslast[90]. Ohne eine Filterkomponente ist also die Angriffslast an Position 1 am höchsten. Das führt zu hohen Datenmengen, die das IPS sammelt. In Kapitel 3.3 ist die Problematik bereits angesprochen, dass IPS große Datenmengen erzeugen. Zwangsläufig wird die Speicherkapazität des gesamten IPS in kürzester Zeit überschritten[91]. Des Weiteren steigt auch die Anzahl der Fehlalarme die ein Sensor generiert.
Sinnvoller ist es einen NIPS hinter die erste Filterinstanz zu installieren.

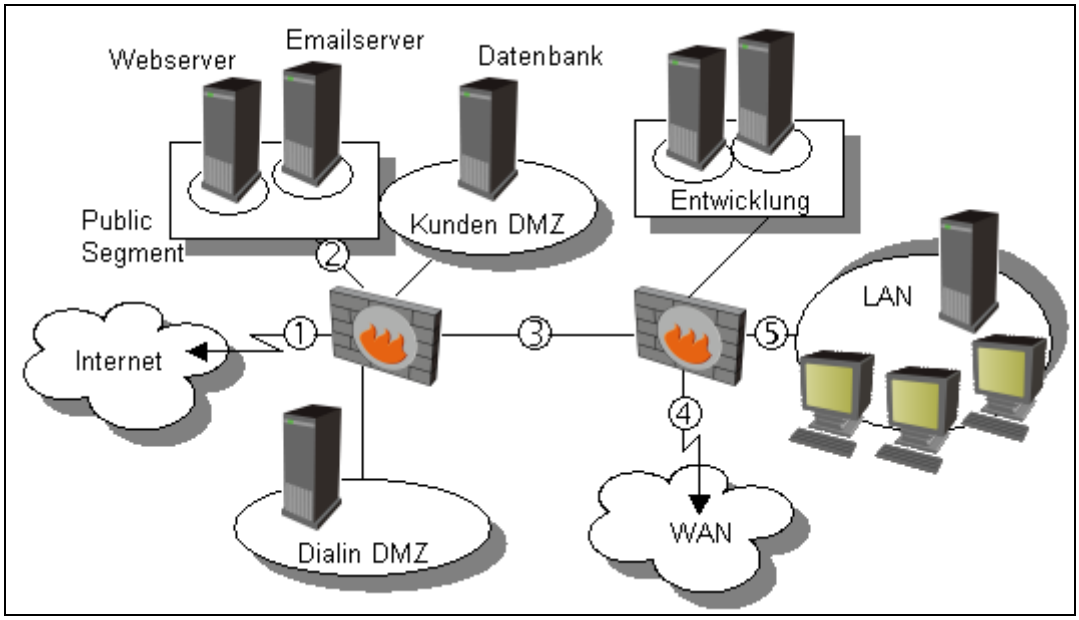


Abbildung 13 - Beispielplatzierungen in der Firewallumgebung

Um zu entscheiden an welchem Firewallsegment oder DMZ-Server der Einsatz eines IPS sinnvoll ist, kann man auf folgende Fragestellungen zurückgreifen:

Wer (Benutzergruppen, IP-Bereiche, einzelne Hosts) hat Zugriff auf
Was (Server, Clients, Netzwerkkomponenten) und
Wie (Protokoll, Service) darf dieser Zugriff erfolgen.

[90] Vgl. BSI1, S. 59
[91] Vgl. ebenda

Anhand dieser Fragestellungen lässt sich eine Priorisierung der einzelnen DMZ oder Firewallsegmente festlegen. Ein Server welcher von innen oder von außen nur von einer kleinen Benutzergruppe mit einem exotischen Service ansprechbar ist, ist weitaus weniger Gefahren ausgesetzt als ein öffentlich zugänglicher Web-, Mail- oder DNS-Server. Zur Bestimmung des Sensorstandorts sind Kenntnisse über die zugelassene Kommunikation zu den einzelnen DMZ nötig. Diese Informationen lassen sich aus der Firewall-Policy in Erfahrung bringen. Durch eine Aufstellung der potenziellen Einsatzorte nach Servern und dessen Zugriff, kann man feststellen welches Segment die meisten öffentlichen Zugriffe zulässt. Ein Beispiel dieser Aufstellung ist in Tabelle 5 dargestellt.

Segment	Server	Zugriff von	Service
Public	Web	Any	http, https
	Email	Any	smtp, pop3, imap, http
Kunden	Datenbank	Kunden	tcp/3520, sql_port
	Datenbank	Dial-In Clients	sql_port
Entwicklung	Fileserver	LAN_Entwickler	File Transfer Protocol
	Fileserver	Dial-In Clients	File Transfer Protocol
WAN	Domain Ctrl.	Aussenstellen	LDAP, Kerberos
	Fileserver	Ausst. China	CIFS, FTP

Tabelle 5 - Zugriffe auf Firewallsegmente

Wie anhand der Aufstellung zu erkennen ist, bietet das Public-Segment die meisten Zugriffsmöglichkeiten. Als Hauptkriterium für die Auswahl des Standortes gilt, wer für den Zugriff zugelassen ist. Alle Benutzer aus dem Internet oder dem internen LAN haben die Berechtigung auf Web- und Email-Server zuzugreifen. Über die zugelassenen Protokolle (http, https) sind Angriffe aus dem Internet möglich. Ein Beispiel ist der bereits angesprochene Wurm CodeRed-II, der eine Sicherheitslücke im IIS ausnutzt. Die Entscheidung des Standortes anhand der zugelassenen Services (wie http) ist zwar wegen bestehenden Gefahren wichtig, jedoch zweitrangig, da jederzeit neue Bedrohungen durch neue Lücken entstehen können. Es besteht keine Garantie, dass sichere Anwendungen auch zukünftig sicher bleiben werden. Es sollte jedoch beachtet werden, dass das NIPS in Segmenten zum Einsatz kommt, in denen es in der Lage ist den Verkehr zu analysieren. In

einem Segment, welches durch die Firewall nur verschlüsselten Protokollen erreichbar ist, macht ein NIPS keinen Sinn.
Die Wahl für die erste NIPS Sensorinstanz fällt in diesem Fall auf die Verbindung zwischen der externen Firewall und dem Public-Segment, also Position zwei.
Falls in einem Segment die Überwachung nur für Server stattfinden soll und dort wenige Server stehen, bietet sich auch die Installation mehrerer HIPS-Sensoren an. Diese sind in der Lage verschlüsselten Verkehr, wie https zu analysieren. Oft ist diese Softwarelösung auch preiswerter als eine NIPS-Appliance. Bei der Überwachung einer DMZ mit vielen verschiedenen Endgeräten, bietet sich eine NIPS-Appliance an. Zu beachten ist auch, dass meistens nicht für jedes System ein HIPS-Sensor zur Verfügung steht. Die Unterstützung von HIPS-Sensoren ist nicht für jedes Betriebssystem oder Netzkomponente garantiert oder möglich. An vielen Servern in Hochverfügbarkeitsumgebungen wird auch die Installation zusätzlicher Dienste vermieden, um die Systemstabilität zu gewährleisten.

Bei Positionierung des Sensors an die Position 3 ist man in der Lage, den gesamten Verkehr aus dem internen Netz in das Internet zu überwachen. Diese Position ermöglicht beispielsweise das Aufdecken von Spyware. Obwohl es nicht Aufgabe eines IPS ist, kann auch die Untersuchung verdächtiger Email-Anhänge oder Scripts von der NIPS-Appliance erfolgen. Bei dieser Platzierung entsteht auch ein Problem bezüglich der Email-Kommunikation. Emails an Empfänger außerhalb des eigenen Netzwerks müssen die Appliance passieren. Mit einem Sensor ist es prinzipiell möglich, eine personenbezogene Überwachung über die Emails herzustellen. Wie in Kapitel 4.1 beschrieben, bedeutet dies einen Konflikt mit dem BDSG. Normales „Surfverhalten“, beispielsweise http-Zugriffe, ist im Zusammenhang mit dem Datenschutz meist nicht relevant. Üblicherweise erfolgen aus dem internen Netz die Webzugriffe über einen Proxy, der bei jeder Web-Kommunikation entweder die Quelle oder das Ziel der Kommunikation darstellt. Ein Personenbezug lässt sich dadurch nur in Kombination mit der Webproxy-Logdatei herstellen. Ein Sensor an der Position 3 stellt zudem auch einen Schutz für die Entwickler DMZ dar. Die gesamte externe Kommunikation, wie aus dem Dial-In-Segment, wird somit überwacht.

Falls ein Unternehmen weitere Außenstellen über WAN angeschlossen hat, ist die Platzierung an Position 4 prinzipiell sinnvoll und wichtig. Beispiele für WAN-Verbindungen sind Frame-Relay, ATM oder MPLS. Meist haben diese Außenstellen auch mit einigen Diensten Zugriff auf DMZ-Bereiche oder auf Server im internen LAN. Deshalb soll auch ein Schutz am Übergang zu Weitverkehrsnetzen erfolgen.

Eine weitere Möglichkeit um den Standort der NIPS-Sensoren zu ermitteln ist das Durchführen von Simulationen. Bei dieser Vorgehensweise werden die Sensoren an den potenziellen Standorten getestet. Der Verkehr wird an den einzelnen Positionen lediglich mitgelauscht. Deshalb genügt es die Sensoren passiv an einen gespiegelten Port zu installieren. Dadurch ist eine einfache Installation während des laufenden Betriebes möglich, ohne die zu überwachende Leitung trennen zu müssen. Natürlich sind auch während der Simulationen die Datenschutz-bestimmungen zu beachten. Es besteht auch nicht die Gefahr legitimen Verkehr zu blocken, da sich das IPS wie ein Intrusion Detection System verhält. Die an einem Standort über einen Zeitraum gesammelten Daten helfen bei der Entscheidung des Standortes. Ein Netzsegment, das während der Simulationen Ziel häufiger Attacken ist, sollte bevorzugt mit einem NIPS ausgestattet werden. Bei den Simulationen sollte das Regelwerk des IPS-Sensors keinen Beschränkungen unterliegen. Dadurch nehmen zwar die Anzahl der Fehlalarme und die gesammelte Datenmenge zu, jedoch erhält man einen Überblick über die laufende Kommunikation des betroffenen Netzsegments. Diese Methode dient als Ergänzung zu der Untersuchung des Standortes mit den Firewallregeln. Es gibt keinerlei Garantie, dass Standorte die während der Simulationen keinen Attacken ausgesetzt waren, auch in Zukunft sicher sind. Es besteht immer die Gefahr, dass für die Software eines aus heutiger Sicht sicheren Servers, eine Sicherheitslücke auftaucht.

4.2.2 Einsatz im internen Netzwerk

Nicht nur an Übergängen zu unsicheren Netzwerken finden Angriffe statt. Es ist durchaus möglich, dass Angriffe auch vom internen Netzwerk ausgehen. Besonders mobile Clients, stellen eine Bedrohung für das Netzwerk dar. Im internen Netz sind die Endgeräte durch die Firewall und den aktuellen Virenscanner weitgehend geschützt. Meist haben Sie auch keine direkte Internetanbindung. Falls diese

Endgeräte direkt an ein unsicheres Netzwerk angeschlossen werden, beispielsweise über ein Modem oder eine ISDN-Verbindung, ist die Infektionsgefahr deutlich höher. Diese unsichere Anbindung kann bei Dienstreisen, Homeoffices oder längeren Auslandsaufenthalten zustande kommen. Virenscanner sind zwar ein Grundschutz vor Internetwürmern, jedoch kann bei langsamen Verbindungen der Download der aktuellen Virensignaturen unter Umständen sehr lange dauern. Falls der Download eines aktuellen Signaturupdates 30 Minuten dauern sollte, ist der Client für diesen Zeitraum nicht immun gegen neue Bedrohungen, deren Muster erst in dem neuen Signaturpaket enthalten sind. Es kann auch vorkommen, dass die Mitarbeiter vergessen die Signaturen zu aktualisieren, für diesen Vorgang nicht ausreichend geschult sind oder keine Zeit dafür haben. Das Spektrum an Möglichkeiten ist in diesem Fall groß. Wieder angeschlossen am Firmennetzwerk ist der Wurm auf dem infizierten Laptop, beispielsweise MSBlaster, sofort auf der Suche nach angreifbaren Hosts und kann sich so verbreiten. Dieser Fall ist nur ein Beispiel für mögliche Bedrohungen aus dem internen Netz.

Weitere Gefahrenquellen können nicht-mobile Endgeräte sein, welche nicht regelmäßig gepatcht werden, mit keinem Anti-Virenprogramm ausgestattet sind oder die Firewall umgehen, wie Modems. Dies trifft beispielsweise auf Echtzeitsysteme zu, die u. U. mit Sicherheitssoftware nicht ordnungsgemäß arbeiten.

Des Weiteren besteht auch die Gefahr eines direkten Angriffs durch einen Mitarbeiter.

Im internen Netzwerk ist die Platzierung von Sensoren in der Regel aufwändiger. Der erste Grund ist, dass interne Netzwerke oft hochverfügbar sind, d. h. es gibt redundante Verbindungen zu wichtigen Komponenten. Des Weiteren geht der Trend in Richtung Gigabit-LAN im internen Netz[92]. Aus diesem Grund müssen auch NIPS-Sensoren diese Bandbreite unterstützen. IPS Hersteller beginnen erst mit der Auslieferung von Sensoren mit einer Leistung von einem Gigabit Voll-Duplex. Deshalb sind diese Sensoren noch nicht häufig am Markt vertreten bzw. liegen im Preis deutlich über Fast-Ethernet Sensoren.

Ein Beispiel für die Architektur eines internen Netzes ist in Abbildung 14 dargestellt.

[92] Vgl. Heise News: http://www.heise.de/newsticker/meldung/print/48587 (Stand: 31.08.04)

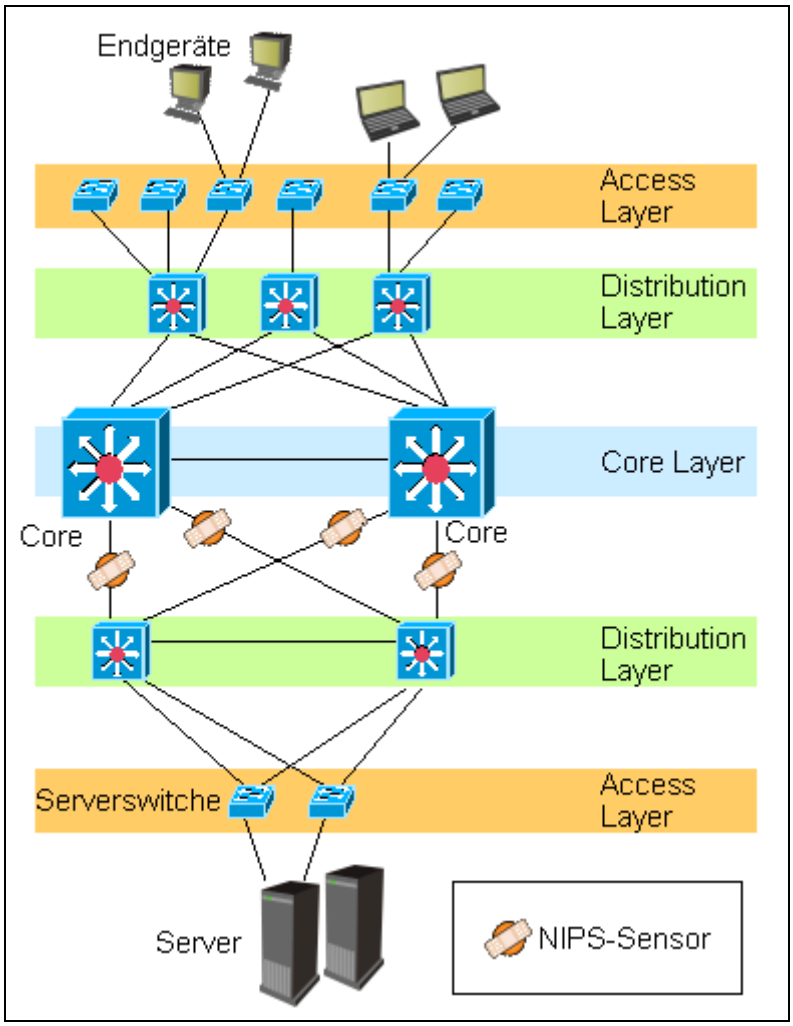


Abbildung 14 - Sensoren im internen Netz

Alle Endgeräte wie Workstations, Laptops und Drucker sind an den Endgeräte-switchen der Access-Layer angeschlossen. Unter der Annahme, dass die redundanten Verbindungen gleichzeitig aktiv sind und die Leitungen einen automatischen Lastenausgleich bieten, benötigt man für jede Verbindung einen NIPS-Sensor. Dies ist mit zusätzlichen Kosten verbunden, da die Sensoren ebenso redundant ausgelegt sein müssen. Im Netzwerk aus Abbildung 14 bieten sich die Leitungen von den Cores zu der Server-Distribution Layer an, um die internen Server vor Zugriffen der Clients zu schützen. Der Grund ist einerseits, dass der gesamte Verkehr zwischen Clients und Servern analysiert werden kann, andererseits die Anzahl der nötigen Sensoren geringer ist, als beispielsweise zwischen der Core und Endgeräte-Distribution Layer.

Mit der Positionierung der Sensoren in das interne Netzwerk ist es möglich personenbezogene Daten zu protokollieren. Gespeicherte Daten von Internetzugriffen und Emails können in direkte Verbindung mit einem Mitarbeiter gebracht werden. Dieser Einsatz steht im Konflikt mit dem BDSG. Vor dem IPS-Einsatz im internen Netz ist juristischer Rat einzuholen[93].

4.3 Management

Wie bereits in Kapitel 3.2.3 beschrieben, spielt die Managementstation die zentrale Funktion in einem Intrusion Prevention System. Deswegen ist die richtige Positionierung der Managementstation im Netzwerk ebenfalls wichtig. Vorraussetzung ist, dass die Managementkonsole jederzeit Zugriff zu Signatur-Updates hat. Diese können in der Regel von Servern des IPS-Herstellers bezogen werden. Des Weiteren müssen alle Sensoren die Möglichkeit haben mit der Managementstation in ständigem Kontakt zu stehen.
Um der Managementstation zu gestatten sich aktuelle Signaturen vom Hersteller zu laden, gibt es zwei Möglichkeiten. Ein Weg ist dem Server ein Benutzerkonto einzurichten, welches ihm gestattet, sich über den Web-Proxyserver zum Internet zu verbinden. Wichtig dabei ist, dass die Managementsoftware eine Verbindung über einen Proxyserver zulässt. Zudem ist darauf zu achten, dass das Kennwort des IPS-Benutzerkontos nicht ablaufen kann, bzw. dessen Änderung bei Ablauf nicht vergessen wird. Mit einem abgelaufenen Kennwort ist der Managementserver nicht in der Lage, sich beim Proxy zu authentifizieren und so Updates des Herstellers zu beziehen.
Ein anderer Weg ist, den Managementserver an der Firewall freizuschalten. Diese Firewallregel kann sehr restriktiv eingerichtet werden. Vorraussetzung ist die Kenntnis über die IP-Adresse des Herstellers und die Dienste, welche für das Update nötig sind.

Eine Vorbereitung für die Kommunikation zwischen Management und Sensoren muss auch geschehen. NIPS-Appliances bieten für den Management-Anschluss eine separate Netzwerk-Schnittstelle. Wenn das NIPS in einer DMZ installiert ist,

[93] Vgl. BSI1, S. 61

muss der Anschluss des NIPS-Managementinterface auch in einer DMZ angeschlossen werden. Eine Verbindung der Management-Schnittstelle des NIPS zu einem Switch im internen Netz würde eine Umgehung der Firewall und somit ein Sicherheitsrisiko bedeuten. Diese Situation ist in Abbildung 15 dargestellt.

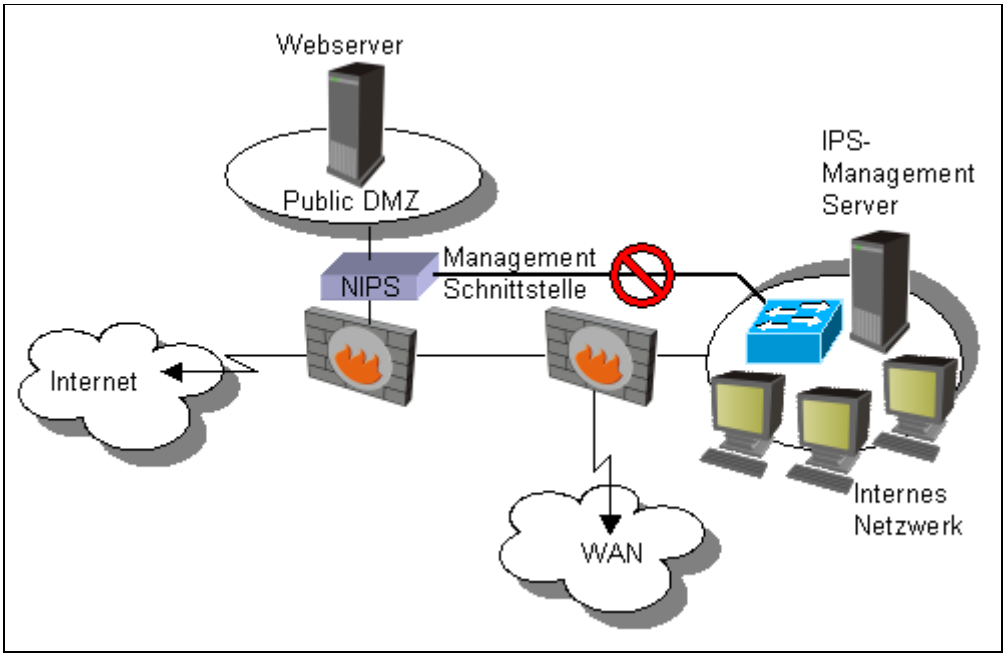


Abbildung 15 - Umgehen der Firewall durch das Management

Falls es einem Angreifer gelingt, eine Sicherheitslücke im IPS auszunutzen und den NIPS-Sensor zu übernehmen, könnte er ggf. durch die Managementschnittstelle, an der Firewall vorbei und so auf das interne LAN zugreifen. Deswegen muss die Managementschnittstelle des NIPS auch in einem DMZ angeschlossen sein. Damit das funktioniert, müssen an der internen Firewall zusätzliche Regeln definiert werden, die den Verkehr zwischen Sensor und Management zulassen. Die dabei genutzten Dienste sind meist in der IPS-Dokumentation beschrieben.
Weiterhin ist für Intrusion-Response eine Kommunikation zwischen Managementstation und anderen internen IT-Systemen nötig[94]. Intrusion-Response bewirkt eine Benachrichtigung des IPS-Administrators bei bestimmten Ereignissen. Dienste sind beispielsweise Email-Server, SNMP-Server oder ein SMS- bzw. Pagergateway. Konsolen bzw. die GUI der Managementkonsole müssen auch erreichbar sein.

[94] Vgl. BSI1, S. 21

Einige Beispiele für den Zugriff auf das Management des IPS sind eine webbasierende Oberfläche, eine direkte Remote-Verbindung auf dem Management-Server oder eine eigenständige Anwendung, welche mit dem Server kommuniziert. Falls der Managementserver und die Clients im internen LAN stehen, ist diese Bedingung in der Regel erfüllt. Wenn externe Zugriffe auf die Managementstation nötig sind oder sich der Managementserver in einer DMZ befindet, müssen die benötigten Dienste an der Firewall freigeschaltet sein.

4.4 Policypolitik

Entscheidend für die Effektivität des IPS ist die Kalibrierung der Signaturen. Je sorgfältiger die Anpassung der Policy eines IPS-Sensors erfolgt, desto höher ist der Erkennungsgrad und umso niedriger die Anzahl der Fehlalarme. Die meisten IPS-Anbieter bieten zwar schon eine recht passable Basiseinstellung Out-of-the-box an, dennoch bringt eine Kalibrierung des IPS einige Vorteile für den Betrieb. Falls die Leistungsfähigkeit des eingesetzten IPS von der Anzahl der aktivierten Signaturen abhängt, muss ohnehin auf einen ausgewählten Signaturenbestand geachtet werden.

Grundsätzlich kann jede Signatur deaktiviert werden, welche nachweislich ein unschädliches Ereignis erkennt und auch nicht relevant für Auswertungszwecke ist. Beispiel einer solchen Signatur kann eine Telnet-Verbindung oder ein einfaches http-get sein. Es gibt Signaturen die Angriffe erkennen, welche nicht zur eingesetzten IT-Umgebung passen. Wenn ein Unternehmen nur UNIX-Systeme betreibt, können sämtliche Windows-spezifischen Angriffssignaturen deaktiviert werden[95]. Für die Sicherheit des Systems ist es nicht relevant, ob diese Signaturen aktiv sind oder nicht. Jedoch stören diese scheinbar unnützen Signaturen oft den Betrieb nicht. Es können sich sogar Vorteile ergeben, wenn Signaturen aktiv sind, welche Ereignisse erkennen, die normalerweise nicht in einer Umgebung auftauchen dürften. Das Protokollieren eines Windows-spezifischen Protokolls in einer homogenen UNIX-Umgebung, ist ein Indiz für eine Fehlkonfiguration im System oder einem verdächtigen Server. Beispiel hierfür ist ein unerlaubter Zugriff in den Serverraum um dort einen Server zu installieren, welcher Firmendaten aufzeichnet und ggf. an Dritte weitersendet.

[95] Vgl. BSI1, S. 31

Zudem ist es wichtig vorsichtig mit der Festlegung von Alarmen umzugehen. Alarmierte Ereignisse, welche sich nach näherer Untersuchung als ungefährlich entpuppen, stumpfen die Sensibilität des IPS-Betreuungspersonals schnell ab. Das führt erstens zur Nicht-Akzeptanz des IPS als relevantes Instrument zur Erkennung von Sicherheitsverletzungen[96], zweitens besteht die Gefahr, dass tatsächliche Angriffe nicht frühzeitig als solche erkannt werden.

Ebenfalls soll jede Signatur aktiviert werden, welche auf ein schadenverursachendes Ereignis hinweist[97]. Meistens sind diese Signaturen bereits vom Hersteller aktiviert, um auch bei einem automatischen Update geschützt zu sein. Ereignisse sollen auch nur dann vom IPS geblockt werden wenn ausgeschlossen ist, dass diese Signatur auch bei ungefährlichen Verkehr triggert. Im produktiven Betrieb muss das Blocken des legitimen Verkehrs ausgeschlossen sein.

Für eine genaue Anpassung der Signaturen des Sensors, können zusätzliche Simulationen stattfinden. Viele Sensoren bieten dazu die Möglichkeit sie in einem Simulationsmodus oder als IDS passiv an einem Spiegelport zu betreiben. In diesem Modus ist ausgeschlossen, dass legitimer Verkehr blockiert wird. Nach dem Aufzeichnen und Auswerten der Sensordaten über einen längeren Zeitraum, können somit Signaturen identifiziert werden, welche häufige Fehlarme auslösen oder fälschlicherweise legitimen Verkehr blockieren.

4.5 Tests der Sensoren

Für Tests am IPS welche die Verfügbarkeit des Netzwerks beeinträchtigen können oder ggf. sogar die Systemsicherheit gefährden, empfiehlt sich eine Testumgebung, welche keine Verbindung zum Produktivnetz hat. Ein Beispiel für den Aufbau einer Testumgebung ist in der Abbildung Anhang 2 - Testumfeld angegeben.
Das IPS auf der Basis von Angriffserkennung zu testen ist schwierig, da Angriffe meist nicht simulierbar sind. Viren, Würmer oder Exploits sind nicht öffentlich

[96] Vgl. BSI1, S. 32

[97] Vgl. ebenda, S. 30

zugänglich und die meisten Sicherheitshersteller stellen diese auch für Testzwecke nicht zur Verfügung. Das Sicherheitsrisiko ist in diesem Fall zu hoch.

Informative bzw. benutzerdefinierte Signaturen sollten jedoch stichprobenartig untersucht werden. Bei der MTU wurden Signaturen getestet, welche auf http-get, Email-Aktivität oder Remote Desktop Events, wie VNC reagieren. Um eine Signatur auszulösen, welche auf beispielsweise auf fehlgeschlagene Virtual Network Computing (VNC) Logins reagiert, genügt es sich auf einen VNC Server zu verbinden und ein falsches Verbindungskennwort einzugeben. Vorraussetzung ist, dass die VNC Verbindung über ein überwachtes Segment geht.
Weiterhin ist die Verwendung von benutzerdefinierten Signaturen eine Möglichkeit um die Funktion des Sensors zu testen. Ein Beispiel ist in Tabelle 6 dargestellt.

Signaturname	**Quelle**	**Ziel**	**Service**
Ping_Test	192.168.0.22 / 32	192.168.5.0/24	ICMP Request
	Reaktion		
	Alarm auf Konsole, Blocken, Email, SNMP		

Tabelle 6 - Beispiel einer benutzerdefinierte Signatur

In diesem Beispiel werden alle Ping Anfragen vom Host 192.168.0.22 an das Netz 192.168.5.0 / 24 alarmiert und blockiert. Außerdem wird eine Email an den IPS-Administrator geschickt und ein SNMP-Trap ausgelöst. Mit benutzerdefinierten Signaturtests ist der IPS-Administrator nicht an die Vorgaben und Randbedingungen eines IPS Herstellers gebunden, sondern kann die Testfälle und die Reaktionen selbst gestalten.

Das Verhalten eines NIPS im Bezug auf Verfügbarkeit, Systemleistung und das Verhalten im Fehlerfall muss ebenfalls getestet werden. Dieses Wissen ist vor produktiver Inbetriebnahme unbedingt notwendig um in einem Fehlerfall schnell reagieren zu können.
Zu Untersuchen ist das Verhalten bei Ausfall der Stromversorgung der NIPS-Appliance. Besonders zu beachten ist die Zeit welche benötigt wird um ggf. die Sensorports in den Fail-Open State umzuschalten (vgl. Kapitel 3.3). Ebenso ist die Zeit wichtig, welche benötigt wird um das System wieder aktiv zu setzen. Im

Regelfall darf der Netzverkehr zwischen den Sensorports nicht beeinträchtigt werden.
Im Fall der G200 NIPS Appliance von ISS, fällt die Verbindung zwischen den Sensorports für ca. drei Sekunden aus, bevor die Schnittstellen kurzgeschlossen werden. Bei fehlender Stromversorgung entspricht die Topologie zwischen den Sensorports der eines gekreuzten Kabels. Im Betriebszustand erkennt die G200 selbstständig den angeschlossenen Endgerätetyp und passt automatisch die Topologie zwischen den Sensorports an.

Weiterhin ist das Verhalten der Appliance während Updates oder Regelveränderungen wichtig. Während dieser Vorgänge darf es zu keinen Verbindungsunterbrechungen zwischen den Überwachungsschnittstellen kommen. Im Produktivbetrieb muss jederzeit auf die Policy zugreifbar sein um evtl. Änderungen durchzuführen, ohne den Verkehr zu beeinträchtigen.

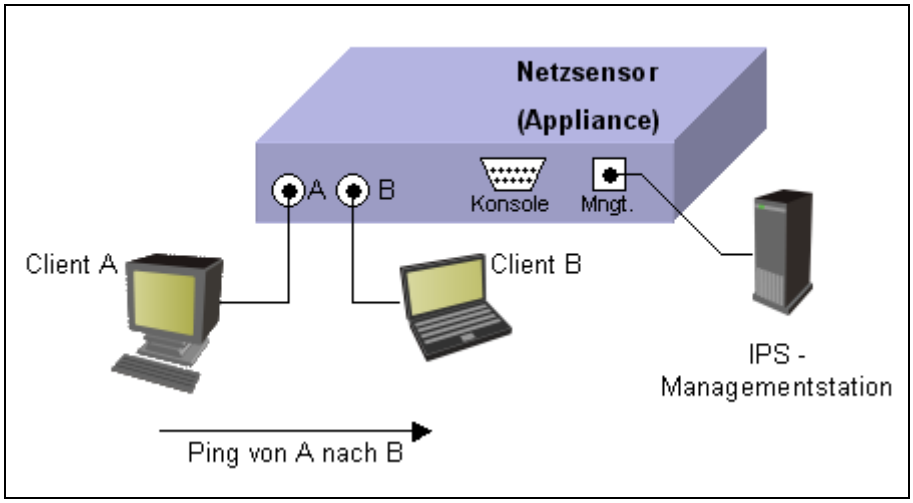


Abbildung 16 - Test des NIPS

In Abbildung 16 ist ein minimaler Testaufbau dargestellt. Um die Funktion der Appliance prüfen zu können reichen Ping-Tests in der Regel aus. Prinzipiell sollten Tests über alle Einstellmöglichkeiten des Sensors stattfinden und dessen Reaktion darauf. Es muss unbedingt sichergestellt sein, dass die Verbindung zwischen den Schnittstellen A und B aufrechterhalten bleibt.

Die G200 von ISS hat diese Forderung im Auslieferungszustand nicht erfüllt. Bei Änderungen der Eigenschaften oder der Policy des Sensors, kam es zwischen den Interfaces zu Ausfällen von bis zu zehn Sekunden. Erst nach der Installation eines zusätzlichen Herstellerupdates hält die Appliance die Verbindung aufrecht.

In Kapitel 3.2.2 wurde die Problematik der HIPS im Bezug auf die Penetration angesprochen. Dieses Verhalten konnte durch Tests bestätigt werden. Zum Testen wurde ein System mit installierten HIPS mit dem Programm „pjam“ angegriffen. Dieses Programm sendet in sehr kurzen Abständen kleine Datenpakete auf einem zufälligen Zielport. Da das HIPS jedes Datenpaket aufzeichnen und analysieren muss, benötigt es 100% der CPU. Kein anderer Prozess bekommt CPU-Zeit zugewiesen. Dasselbe Resultat wurde bei dem gleichen Test ohne HIPS ermittelt, wenn stattdessen ein Netzwerkmonitor auf dem System gestartet wurde. Bei einem Angriff durch „pjam“ benötigt der Netzwerkmonitor beim Aufzeichnen der Pakete ebenfalls 100% der CPU.

4.6 Laptop Sicherheit durch Desktop Protection

Mobile Endgeräte wie Laptops sind aus Sicht der Netzwerksicherheit kritisch. Wie in Kapitel 4.2.2 beschrieben, sind sie außerhalb der Firmenumgebung meist angreifbar. Falls zusätzlich die Verbindungsgeschwindigkeit sehr langsam ist, kann ein Update von Virensignaturen eine längere Zeit in Anspruch nehmen.
Dazu ein Rechenbeispiel mit folgenden Annahmen.
Ein aktuelles Signaturenupdate weist eine Größe von 3 Megabyte auf und das mobile Endgerät verfügt über eine langsame Modemverbindung mit einer Übertragungsgeschwindigkeit von 9600 Baud.

$$9600\,Baud = 1200\,\frac{Byte}{s}$$
$$3MB = 3072kByte = 3145728\,Byte$$

$$Übertragungszeit = \frac{Datenmenge}{Übertragungsgeschwindigkeit}$$

$$t = \frac{3145728\,Byte}{1200\,Byte}\,s = 2621s \approx 43\,\text{min}$$

Selbst bei einer optimalen Verbindung dauert die Übertragung der Virensignaturen länger als 43 Minuten. Ein Zeitfenster für diesen Vorgang zu finden ist in manchen Geschäftsbereichen schwierig. Es findet kein Update statt, somit ist der Laptop angreifbar. Wieder am internen Firmennetzwerk angeschlossen, hat ein auf dem Laptop vorhandenes Schadprogramm die Möglichkeit, sich im Netzwerk zu verbreiten.

Im Rahmen dieser Arbeit ist zu untersuchen, ob durch Einsatz eines HIPS auf mobilen Endgeräten die Sicherheit erhöht werden kann. Intrusion Prevention stellt eine Ergänzung bisheriger Schutzmechanismen dar und soll nur auf Systemen arbeiten, welche bereits einen gewissen Schutz aufweisen. Dieser Schutz ist nicht gewährleistet, falls die Virensignaturen nicht aktuell sind. Des Weiteren arbeiten Intrusion Prevention Systeme ebenfalls mit Signaturen, die in regelmäßigen Abständen zu aktualisieren sind. Obwohl mit Virtual Patching auch die Möglichkeit der Erkennung unbekannter Bedrohungen besteht, ist ein stets aktueller Signaturenbestand trotzdem Voraussetzung für einen umfassenden Schutz. Deshalb eignet sich ein HIPS auf mobilen Endgeräten mit langsamen Netzverbindungen nicht. Genau wie bei einem Virenscanner müssen regelmäßige Updates durchgeführt werden.

Mit einer NIPS Appliance kann die Gefahr ausgehend von mobilen Hosts jedoch reduziert werden. Durch Schaffung eines eigenständigen VLANs für mobile Hosts, welches durch ein NIPS mit dem nächsten Router verbunden wird, kann ein Schutz für das interne LAN hergestellt werden. Ein weiterer Ansatz sind Quarantänezonen, welche von einigen Switchherstellern unterstützt werden. Diese Lösung zielt genau auf die oben genannte Problematik ab.

5 Installation des Intrusion Prevention Systems

5.1 Standortbestimmung und Testinstallationen

In Kapitel 4.2.1 sind Methoden genannt um in einer Firewallumgebung den Standort eines NIPS zu bestimmen. Durch diese Vorgehensweise können mehrere mögliche Positionen ermittelt werden. Eine zusätzliche Testinstallation ist in den betroffenen Netzwerksegmenten meist nötig um Ereignisse des IPS aufzuzeichnen und um eine Vorhersage über das Verhalten im produktiven Betrieb fällen zu können. Da es sich hier nur um Testinstallationen handelt und ausschließlich Auswertungen durchgeführt werden, muss der NIPS-Sensor nicht zwingend in die zu überwachende Leitung integriert sein. Es genügt die passive IDS-Installation am Spiegelport eines Switches um den Installationsaufwand zu verringern, wie in Abbildung 9 gezeigt.
Bei Testläufen empfiehlt es sich nicht mit einem eingeschränkten Regelwerk des IPS zu arbeiten. Die Aufzeichnung aller Ereignisse ist sehr wichtig, um feststellen zu können, welcher Verkehr überhaupt über das zu überwachende Segment fließt. Durch ein vollständig aktiviertes Regelwerk steigt zwar die Anzahl der Fehlalarme und nichtrelevanten Meldungen, dennoch kann man mit dieser Kenntnis im Falle einer produktiven Inbetriebnahme, die Policy besser auf das jeweilige Segment anpassen. Da die Installation einer Teststellung meist nicht sehr lange angeschlossen ist, spielt in den meisten Fällen die Kapazität der Ereignisdatenbank keine Rolle.

Aus der Analyse des Firewallregelwerks haben sich bei der MTU Friedrichshafen zwei Standorte zum Testen ergeben. Eine Positionierung des Sensors im Extranet-Segment und in der Verbindung zwischen interner und externer Firewall.
Besonders der Extranet-Webserver ist durch Angriffe aus dem Internet bedroht. Auf diesen Webserver hat jeder über den http-Port 80 Zugriff aus dem Internet. Zudem sind auf diesem und weiteren Servern im Extranet-Segment sensible und unternehmenskritische Daten gespeichert. In Abbildung 17 ist die Installation des Sensors im Extranet-Segment dargestellt. Die Dauer der Installation in diesem Segment war auf drei Tage festgelegt.

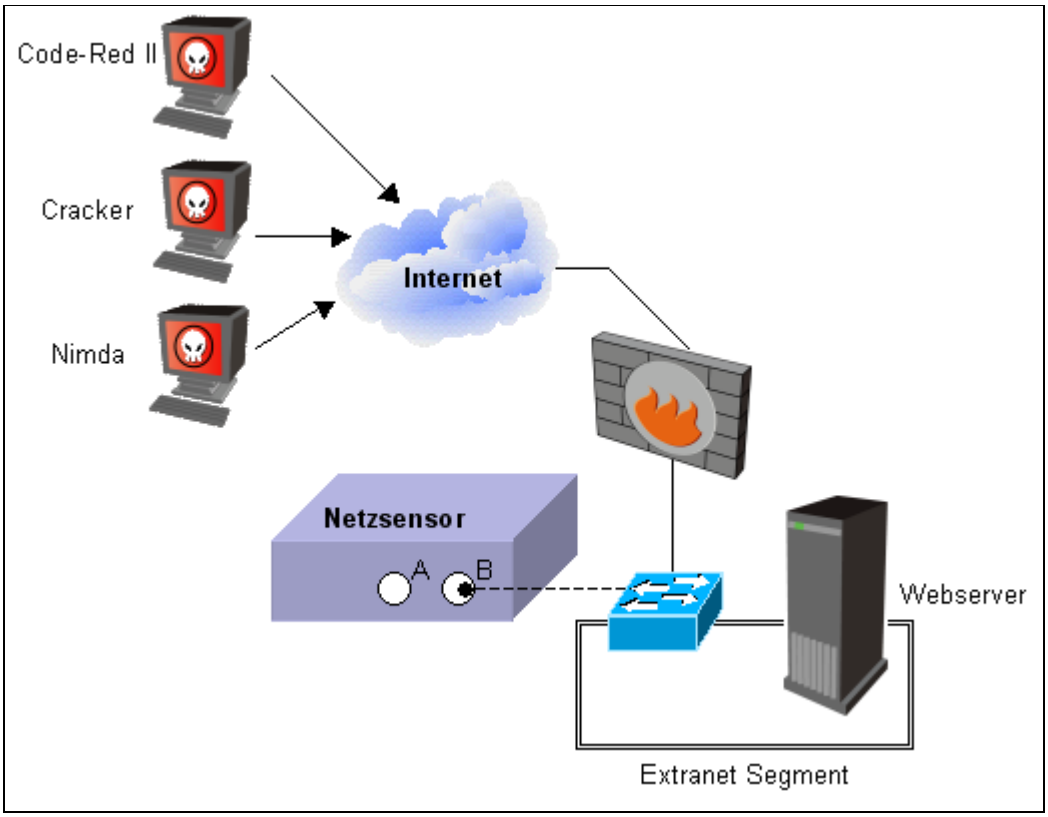


Abbildung 17 - Test im Extranet-Segment

Besonders auffällig sind in diesem Segment die Angriffe durch den Wurm CodeRed-II. Dieser Wurm greift eine Sicherheitslücke im Microsoft IIS an, um den Server zu infizieren. Zugriffsversuche durch Cracker wurden ebenfalls festgestellt. In den meisten Fällen versuchen sie über eine durch den CodeRed-II geöffnete Hintertüre auf den Server zuzugreifen. Die Übergabe von Parametern in einer URL erlaubt das Ausführen beliebiger Kommandos auf dem Webserver.

Weiterhin wurde die Appliance in die Verbindung zwischen interner und externer Firewall installiert. Über dieses Segment läuft beispielsweise der gesamte Verkehr aus dem internen Netzwerk in das Internet. Ankommende und abgehende Emails gehen ebenfalls über diese Verbindung. Besonders auffällig in diesem Segment sind http-Anfragen an Webseiten. Ohne Justierung an der Policy wird jedes http-Get-Ereignis und jede Email aufgezeichnet. Der Datenschutz ist hierbei wiederum zu beachten. Eine Personalisierung des http-Webverkehrs ist nicht möglich, da entweder der Absender oder der Empfänger einer http-Verbindung immer der

Proxyserver ist. Um einen Personenbezug herstellen zu können sind Daten aus dem Proxyserver nötig.
Aufgrund der Tatsache, dass der gesamte Webverkehr aufgezeichnet wird, ist ein Nachweis für Spyware-Aktivität im internen Netzwerk möglich. Spyware arbeitet meist auf dem http-Port, um die gesammelten Daten zu versenden. Mit den richtigen Signaturen ist es möglich diesen Verkehr nachzuweisen und zu unterbinden. Bei der Testinstallation der MTU konnte tatsächlich Spyware im internen Netzwerk nachgewiesen werden. Hier handelte es sich um das Programm Gator/Claria, welches personalisierte Werbung zur Verfügung stellt. In diesem Fall ist der Schaden bzw. die Gefahr welche von Spyware ausgeht minimal, jedoch gibt es ebenfalls Spyware welche unternehmenskritische bzw. geheime Daten ausspäht und versendet. Selbst das Sammeln von Email-Adressen kann sich im Bezug auf Spam sehr negativ auf ein Unternehmen auswirken.

Wegen der sensiblen Daten auf dem Extranet-Webserver, soll dieser auch durch ein NIPS geschützt werden. Um den Schutz zu erhöhen, wurde zeitgleich zum NIPS ein Inbound-Proxyserver installiert. Die Kommunikation zum Extranet-Webserver geht über den Proxyserver im Gateway-Segment.

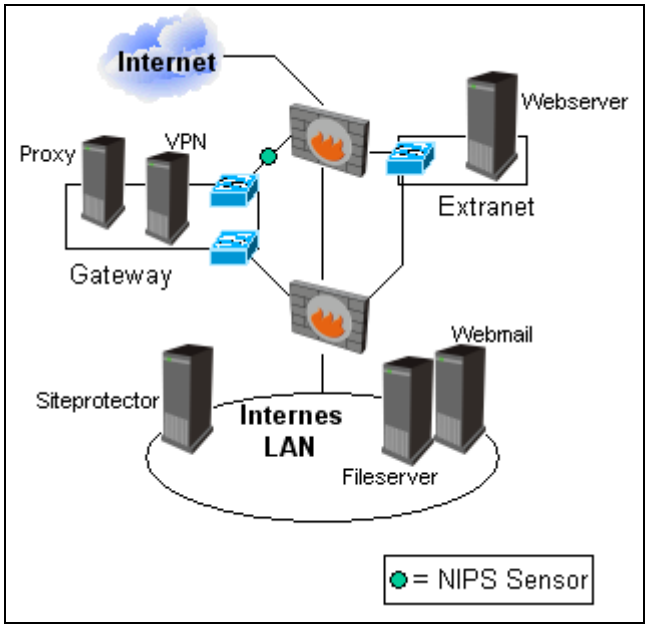


Abbildung 18 - NIPS im Produktivnetz der MTU

Dieser sog. Inbound-Proxyserver nimmt alle Verbindungen an, die für den Webserver im Extranet gedacht sind und leitet diese weiter. Gleichzeitig übernimmt er auch die Rolle des Proxies für den internen Webmail Server. Über Webmail ist es möglich über einen http-Browser auf sein Postfach zuzugreifen.
Deshalb macht es Sinn das NIPS nicht direkt vor das Extranet-Segment zu installieren, sondern vor den Inbound-Proxyserver im Gateway-Segment, wie in Abbildung 18 dargestellt. Dadurch erreicht man nicht nur einen Schutz des Webservers, sondern auch einen Schutz des internen Webmail-Servers. Ebenfalls wird der Proxyserver selbst geschützt, da es nicht ausgeschlossen werden kann, dass er selbst angreifbar ist.
An diesem Standort ergibt sich ein zusätzlicher Nutzen in Bezug auf die Virtual Private Network-Verbindungen. Der verschlüsselte VPN-Tunnel kann auf dem Hinweg zum VPN-Server durch das NIPS nicht analysiert werden. Da der verschlüsselte Tunnel aber beim VPN-Server terminiert und ab diesem Zeitpunkt auch unverschlüsselt ist, besteht die Möglichkeit den Weg des Verkehrs zur externen Firewall hin zu analysieren und einen Schutz zu garantieren. Die externe Firewall ist das Default-Gateway für den VPN-Server und somit immer erste Anlaufstelle für die Datenpakete.

Die HIPS Sensoren kommen auf zwei Netzwerkmanagement-Servern zum Einsatz. Ein Server übernimmt das Management der Cisco Netzwerkkomponenten der andere Server führt SNMP-Anfragen bei verschiedenen Endgeräten durch. Diese Server sind im produktiven Einsatz, müssen jedoch nicht hochverfügbar sein. Es gibt zwei Gründe für die Installation auf diesen Servern. Wie bereits in Kapitel 3.2.2 erwähnt, ist nicht gewährleistet, dass HIPS uneingeschränkt mit dem Betriebssystem und anderen Anwendungen harmonieren. Um das Verhalten der HIPS zu untersuchen und über einen längeren Zeitraum zu protokollieren, werden diese auf einem Windows 2000 und einem Windows 2003 Server installiert.
Der zweite Grund für den Einsatz auf den beiden Servern ist die Zugehörigkeit zu verschiedenen Netzbereichen. Beide Server gehören zu unterschiedlichen Netzwerkbereichen und übernehmen deshalb die Rolle eines sog. Honeypots, um Angriffe auf dem internen Netzwerk zu erkennen. Falls automatisierte Attacken ausgehend von einem Wurm sämtliche Adressen eines Netzbereiches untersuchen,

ist das HIPS auch ein potenzielles Ziel. Falls der Sensor angegriffen wird, hat man Auskunft über die Quelle und kann Aktionen starten um die Infektion zu bereinigen.
Die Hostsensoren haben sich über einen Zeitraum von zwei Monaten nicht negativ auf das Verhalten der Server ausgewirkt und können zukünftig auf kritischeren und stärker gefährdeten Systemen eingesetzt werden.

5.2 Aufnahme des Normalzustandes und Einstellung der Policy

Damit das IPS optimal arbeiten kann muss die Policy zuerst angepasst werden. Die Einstellung des Systems soll soweit optimiert werden, dass einerseits soviel Informationen über Angriffe und außergewöhnliche Netzwerkaktivität wie möglich aufgezeichnet, andererseits so wenig Fehlalarme und nicht relevante Ereignisse wie möglich angezeigt werden. Die Relevanz der Ereignisse hängt vom Normalverhalten der einzelnen Netzwerkkomponenten ab. Diese Ereignisse belegen viel Speicherplatz in der Ereignisdatenbank und lenken von informativen Events ab (vgl. Kapitel 4.4).

Um diesen Zustand zu erreichen ist eine Voreinstellung der einzelnen Sensoren nötig. Für wenig erfahrene Benutzer bieten IPS-Hersteller meistens auch Policyvorlagen an, welche relativ hohe Erkennungsraten bei wenigen Fehlalarmen vorweisen. Um jedoch die maximale Informationsgewinnung zu erzielen, sollte prinzipiell jede Signatur in der Policy aktiv sein, um die danach ermittelten überflüssigen Signaturen schrittweise zu deaktivieren. Die Anzahl der Signaturen eines IPS-Produktes ist sehr hoch. Deshalb kennen die wenigsten Administratoren den gesamten Signaturbestand bzw. wissen nicht unter welchen Umständen eine Signatur triggert. Zumal kommen wegen der Updates ständig neue Signaturen zum Bestand dazu. Der Signaturbestand von ISS beläuft sich im Auslieferungszustand alleine auf mehr als 5.000 Signaturen.
Es besteht bei einer gut verwalteten Signaturdatenbank dennoch die Möglichkeit ohne vorherige Tests und Probeläufe im Vorfeld einige Signaturen zu deaktivieren. Ein Beispiel ist eine Signatur die bei einem http-Get anzieht. Gerade in Segmenten über welche Webtraffic transportiert wird, löst diese Signatur ein Auffüllen der Ereignisdatenbank mit unwichtigen Ereignissen aus. In Umgebungen, welche mit DHCP arbeiten, wäre eine Signatur unsinnig, die auf DHCP-Anfragen triggert. Die Deaktivierung dieser Signaturen hängt stark vom Einsatzort des Sensors ab. In

manchen Umgebungen macht es durchaus Sinn Signaturen welche auf DHCP-Anfragen triggern zu aktiveren, falls dort kein DHCP verwendet wird.
Nachdem das Regelwerk für den neuen Sensor nach den Empfehlungen angepasst wurde, kann der Sensor nun im Netzsegment betrieben werden. Hier empfiehlt sich zuerst der Betrieb im Simulationsmodus, um ggf. keinen legitimen Verkehr zu blockieren.
Besonders Ereignisse welche vom Hersteller nicht als Bedrohung eingestuft sind und sofort nach Aktivierung des Sensors gemeldet werden, weisen auf Normalverhalten im Netzwerk hin. Dies könnte beispielsweise wieder eine Signatur sein welche auf ein http-get reagiert. Eine Deaktivierung dieser Signaturen ist nötig, um den Speicherplatz der Datenbank nicht in kürzester Zeit auszuschöpfen. Eine etwas elegantere Methode ist die Definition von Filtern in den Signaturen. Dazu das Beispiel aus Tabelle 7.

Prio	Time	Tag Name	Source	Target	Community
▼	15.07.04, 08:21:45	SNMP_Get	192.168.2.6	192.168.5.6	public
▼	15.07.04, 08:22:54	SNMP_Get	192.168.2.6	192.168.1.1	public
▼	15.07.04, 08:23:55	SNMP_Get	192.168.2.6	192.168.9.6	public
▼	15.07.04, 09:24:28	SNMP_Get	192.168.2.6	192.168.8.9	public

Tabelle 7 - Filter für Signaturen

Die Signatur SNMP_Get schreibt die Ereignisdatenbank voll. Ungefähr jede Minute kommt ein neuer Eintrag hinzu. Das bedeutet 1440 Ereignisse pro Tag, die Platz in der Datenbank beanspruchen. Der IPS-Administrator möchte jedoch nicht die SNMP_Get-Signatur deaktivieren um ungewöhnliches Verhalten der Netzwerk-geräte durch das IPS analysieren zu können. Wie aus der Spalte „Source“ zu erkennen ist, gehen die SNMP-Get-Anfragen immer von derselben Quelle aus, also höchstwahrscheinlich vom SNMP-Server im Netzwerk. Durch definieren von Signaturfiltern bzw. Ausnahmeregelungen kann man das IPS dazu bewegen prinzipiell die SNMP_Get-Signatur weiterhin zu benutzen, jedoch nur wenn sie nicht in ein bestimmtes Muster passt. Im Beispiel oben könnte der Filter so definiert sein, dass alle SNMP_Get-Ereignisse angezeigt werden, außer die Quelle des Ereignisses ist der SNMP-Server. Durch diese Methode lässt sich das Regelwerk eines Sensors optimal anpassen, jedoch bedeutet dies einen deutlich höheren Administrationsaufwand.

Die Policy für die IPS Sensoren der MTU wurde von Default-Policies des Herstellers abgeleitet. Die Default-Policy von ISS aktiviert alle Angriffe, wovon einige nach Empfehlung von ISS geblockt werden. Die informativen Ereignisse, die Audit-Events genannt werden, sind in der Standardeinstellung deaktiviert. Da der Informationsgewinn so hoch wie möglich sein soll, wurden alle Audit-Events manuell aktiviert. Ereignisse wie http-get wurden durch grobe Durchsuchung der Policy anschließend deaktiviert.
Nach Zuweisung der angepassten Policy an die Sensoren wurden bereits nach einigen Minuten Logging-intensive Ereignisse erkannt. Nach Prüfung ob diese Ereignisse legitim sind und keine nennenswerten Informationen über die Netzwerkaktivität offenbaren, wurden diese deaktiviert. Beispiel sind VRRP-Multicasts, die jede Sekunde ein Ereignis erzeugten. Durch setzen von Filterregeln konnten informative Signaturen, welche regelmäßig viele Datensätze in der Datenbank erzeugten, dennoch aktiviert bleiben. Natürlich ist das Anpassen der Policy ein kontinuierlicher Prozess.

5.3 Policy im Bezug auf automatische Updates

Damit das IPS einen Schutz bieten kann, muss zu jeder Zeit ein aktueller Signaturenbestand vorliegen. Die Managementstation hat die Aufgabe diese Updates vom Hersteller zu beziehen, um sie anschließend auf die Sensoren zu verteilen. Dieser Vorgang sollte möglichst vollautomatisch erfolgen. Dadurch ergeben sich einerseits für den Benutzer, andererseits auch für den Hersteller Probleme. Der Hersteller muss die Reaktionen des IPS auf die neuen Signaturen festlegen, beispielsweise ein Blockieren der Datenpakete. Des Weiteren muss sich der Hersteller entscheiden ob Signaturen, welche bei informativen Ereignissen triggern, überhaupt zu aktivieren sind. Im schlimmsten Falle sind diese Auslöser für Fehlalarme in einem Netzwerk verantwortlich und schreiben die Ereignisdatenbank voll.
Als Nutzer eines IPS ist man somit auf die Vorgaben des Herstellers angewiesen, der einerseits den größten Schutz bieten will, andererseits keine Fehlalarme oder das Blockieren legitimen Verkehrs auslösen will.
Als IPS-Administrator empfiehlt sich deshalb in regelmäßigen Abständen die Signaturen von Hand einzustellen. Beispielsweise wenn ein neuer Signaturen-

bestand vom Hersteller vorliegt. Denkbar ist eine Lösung, dass automatisch alle Signaturen welche auf einen schwerwiegenden Angriff hindeuten, automatisch aktiv sind und Angriffspakete auch blockieren. Informative Ereignisse sollten bei einem automatischen Update manuell nachgezogen werden.
Viele Hersteller bieten eine Benachrichtigung über Email, Pager oder SMS an, falls neue Signaturen auf den Sensoren verteilt wurden.

Die Installation von Updates zu Softwareversionen der Sensoren oder der Managementstation, sollten unter keinen Umständen automatisch geschehen. Diese Aktion sollte manuell erfolgen, da der Sensor ggf. neu durchstarten muss, mit der Folge einer Verbindungsunterbrechung. Ein IPS-Administrator sollte sich hier an die Release-Notes der neuen Version halten.

5.4 Wartung der Datenbank

Die Komponente des IPS, auf die das höchste Augenmerk bezüglich der Wartung gelegt wird, ist die Ereignis-Datenbank. Besonders der Speicherplatz spielt hier eine Rolle. Damit die Datenbank nicht innerhalb kürzester Zeit den gesamten Speicherplatz in Anspruch nimmt, unterstützen einige IPS-Produkte eine automatische Datenbankbereinigung, beispielsweise alle Ereignisse mit niedriger Priorität, die älter als drei Monate sind. Benötigt man die Ereignisdaten länger, empfiehlt sich ein Backup der Datensätze auf Band oder eine automatische Auslagerung der alten Datensätze auf einen Fileserver. Die Archivierung vergangener Ereignisse kann auch in Form von Managementreports erfolgen.
Bei der MTU wird einmal pro Woche die Datenbank nach alten Events durchsucht. Dabei werden die Indizes automatisch defragmentiert um die Leistung der Suche innerhalb der Datenbank zu erhöhen. Außerdem werden ab einem Schwellwert von 70% des Datenbank-Speicherplatzes alte Ereignisse gelöscht.
Egal welche Möglichkeit gewählt wird, sollte auf jeden Fall dafür gesorgt werden, dass der IPS-Datenbank genügend Speicherplatz zur Verfügung steht.

5.5 Reporting und Zuständigkeiten

Um einen Überblick über aufgetretene Ereignisse zu erhalten, empfiehlt sich die automatische Generierung von Managementreports. Hersteller von IPS bieten

verschiedene Auswertfunktionen und grafische Visualisierungen der Ereignisse an. ISS bietet im Siteprotector die Möglichkeit diese Reports in HTML, PDF oder Comma Seperated Values (CSV) zu erstellen. In diesen Reports sind typischerweise nicht alle Details eines Angriffes hinterlegt. Vielmehr stellen sie einen einfachen Überblick über die aufgetretenen Ereignisse dar, zusammengefasst über die ausgelösten Signaturen. Ein Auszug eines Monatsreports ist im Anhang beigefügt.

Detaillierte Reports sind oft nicht durchführbar, da die Menge der gesammelten Daten sehr hoch ist. Ein genauer Report schlüsselt jedes Ereignis mindestens in die exakte Uhrzeit, den Angreifer, das Ziel und die Schadroutine auf. Ein Beispiel für die Informationen, welche nur durch Auslösung einer einzigen Signatur gesammelt werden, wird in Abbildung 19 gezeigt.

Event Details Name	Event Details Value
Date/Time	2004-09-05 03:23:52 CEST
Tag Name	HTTP _Code_Red_II
Alert Name	HTTP _Code_Red_II
Severity	High
Observance Type	Intrusion Detection
Combined Event Count	1
Cleared Flag	FALSCH
Target IP Address	212.2.67.38
Target Object Name	80
Target Object Type	Target Port
Target Service	http
Source IP Address	219.231.165.36
SourcePort Name	4923
Sensor DNS Name	df0004.mtu-friedrichshafen.com
Sensor IP Address	53.130.9.70
Sensor Name	fn_df0004
Attributes Name	**Attributes Value**
:adapter	A;B
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u685
:arg	8%ucbd3%u7801%
:URL	/default.ida
:vlan	802
algorithm-id	2004602
DROP	ConnectionWithReset
DYNAMICBLOCK	BlockWorm|100|3600
EventsNotBlocked	4
InlineApplianceMode	Inline Simulation

Abbildung 19 - Auszug eines detaillierten Ereignisses

Das in Abbildung 19 dargestellte Ereignis spiegelt einen Code-Red-II Angriff wieder. Im oberen Teil der Tabelle werden allgemeine Fakten wie Uhrzeit, Quelle, Ziel, Service und Angriff angezeigt. Im unteren Teil sind die angriffsspezifischen Daten aufgelistet und die Reaktion des Sensors auf diesen Angriff.

Aufgrund der Tatsache, dass ein Intrusion Prevention System Ereignisse verschiedenster Art protokolliert und ggf. alarmiert, darf nur geschultes IPS-Personal Zugang zu Auswert- und Überwachungsfunktionen besitzen. Die Vorgänge, Alarmklassen und die Signaturen sind sehr komplex. Deshalb ist es nicht sinnvoll eine Überwachungskonsole dem First-Level Support zur Verfügung zu stellen. Es macht jedoch durchaus Sinn, ein einheitliches Betriebshandbuch für alle IPS-Administratoren zu verfassen, in dem die generellen firmen- und einsatzabhängigen Vorgänge beschrieben sind. Das MTU IPS-Betriebshandbuch ist im Anhang beigefügt.

5.6 Erfolgreiche Angriffe und Eskalation

Ein IPS bietet wie jede Sicherheitskomponente keinen uneingeschränkten Schutz. Es kann durchaus vorkommen, dass Angriffe von einem IPS nicht erkannt werden und ggf. in das Netzwerk eindringen. Das Resultat ist die Infektion von Servern, Clients oder sogar Netzwerkkomponenten.
Einen erfolgreichen Angriff erkennt man natürlich erst wenn es zu spät ist und eventuell auch bereits Schaden dadurch entstanden ist. In diesem Fall ist es besonders wichtig die betroffenen Systeme schnellstmöglich durch aktuelle Antiviren-Software oder Herstellerpatches zu bereinigen um eine weitere Ausbreitung der Infektion zu verhindern. Im Extremfall kann dies auch eine Trennung der befallenen Systeme vom Netzwerk bedeuten, bis sie vollständig bereinigt sind. Gleichzeitig muss der Infektionsweg analysiert und unterbrochen werden um erneute Infektionen zu verhindern. Falls es sich um einen ungesicherten Zugang handelt, ist zu ermitteln ob sich der Zugang durch Sicherheitssysteme wie IPS absichern lässt.

Falls der Angriff ein IPS System überwunden hat bzw. nicht erkannt wurde, muss eine Untersuchung erfolgen ob die entsprechenden Signaturen bereits auf dem IPS System verteilt wurden oder ob der Hersteller sie bereits zur Verfügung gestellt hat.

Wenn der Hersteller für den spezifischen Angriff keine Signaturen zur Verfügung stellt, müssen benutzerdefinierte Signaturen erstellt werden, die den Angriff erkennen und abwehren.

6 Fazit

6.1 Zusammenfassung

Im Rahmen dieser Arbeit zeigte sich, dass sich Intrusion Prevention Systeme sehr gut als zusätzlicher Schutz für Netzwerke anbieten, da Anti-Virus- und Firewallsysteme nicht alle Bedrohungen erkennen und abwehren können. Besonders Server in einer Firewallumgebung, die von einer großen Benutzergruppe erreicht werden können, sind besonders gefährdet und erhalten durch ein IPS einen erweiterten Schutz.

Durch die Unterstützung von Trunking und dem gemeinsamen Management aller IPS-Sensoren ist die Wahl des Herstellers bei der MTU auf Internet Security Systems gefallen. Eine NIPS G200-Appliance wird im Gateway-Segment eingesetzt, um den Extranet-Webserver, den Inbound-Proxyserver und den internen Webmailserver zu schützen. Zusätzlich ist eine Überwachung von VPN-Verbindungen möglich welche in das interne Netzwerk geleitet werden. Die HIPS-Sensoren von ISS sind auf zwei Netzwerkmanagement Servern mit Windows 2000 und Windows 2003 installiert. Diese Sensoren sollen zukünftig auf Systemen Einsatz finden auf denen unter anderem verschlüsselter Verkehr analysiert werden muss. Eine IPS-Lösung für MTU Laptops konnte nicht empfohlen werden, da ein HIPS genauso wie ein Virenscanner auf Signaturen angewiesen ist. Auf Dienstreisen ist eine ausreichend schnelle Internetverbindung für den Signaturendownload meist nicht verfügbar.

Für die Verwaltung und Monitoring eines IPS ist geschultes Fachpersonal notwendig, da durch vielfältige Signaturen die Alarme eine hohe Komplexität aufweisen können.

6.2 Ausblick

Um einen flächendeckenden Schutz zu erreichen, empfiehlt sich das IPS-Konzept auszuweiten. Viele Segmente in der Firewallumgebung und im internen Netzwerk sind noch immer prinzipiell angreifbar und somit verwundbar. Der Einsatz eines NIPS in der externen Extranet-Verbindung, der Verbindung zwischen der internen und externen Firewall, des WAN-Segments und diverser DMZ ist durchaus sinnvoll. Einige Workstations bzw. mobile Endgeräte im internen Netz, welche aus

Kompatibiltätsgründen nicht über einen Virenscanner verfügen, können zum besseren Schutz in ein separates VLAN umgezogen werden, dessen Verbindung zum nächsten Router über ein NIPS erfolgt. Vereinzelte Server welche für die Speicherung von sensiblen Daten genutzt werden oder eine wichtige Rolle im Netzwerk übernehmen, sind über HIPS zu schützen.

Abkürzungsverzeichnis

ATM	Asynchronous Transfer Mode
BDSG	Bundesdatenschutzgesetz
BIOS	Basic Input Output System
BSI	Bundesanstalt für Sicherheit in der Informationstechnik
CD	Compact Disc
CPU	Central Processing Unit
CSV	Comma Separated Values
DDos	Distributed Denial of Service
DMZ	Demilitarisierte Zone
DoS	Denial of Service
DV	Datenverarbeitung
FTP	File Transfer Protocol
ggf.	gegebenenfalls
GUI	Graphical User Interface
HIPS	Host Intrusion Prevention System
HTML	HyperText Markup Language
http	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IIS	Internet Information Server
IP	Internet Protocol
IPS	Intrusion Prevention System
ISS	Internet Security Systems
LAN	Local Area Network
LSASS	Local Security Authority Subsystem Service
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NIPS	Network Intrusion Prevention System
OSI	Open Systems Interconnection
PC	Personal Computer
PDF	Portable Document Format
RFC	Request for Comments
SMS	Short Message System

SNMP	Simple Network Management Protocol
sog.	so genannte
SSH	Secure Shell
TCP	Transmission Control Protocol
u. a.	unter anderem
UDP	User Datagram Protocol
USD	US Dollar
vgl.	vergleiche
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
z. B.	zum Beispiel

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[Anti-Hack] George Kurtz, Stuart McClure, Joel Scambray
Das Anti-Hacker-Buch
mitp-Vlg., 2002 - 3. Auflage

[BSI Grundschutz] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
IT-Grundschutzhandbuch - 5.EL
Bundesanzeiger-Verlag 2003
URL: http://www.bsi.de/gshb/deutsch/download/GSHB2003.pdf
Stand: 10.08.2004

[BSI Spam] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
BSI für Bürger - SPAM
URL: http://www.bsi-fuer-buerger.de/abzocker/05_06.htm
Stand: 16.08.2004

[BSI Spam1] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
Informationen zu Spam
URL: http://www.bsi.bund.de/av/Spam.htm
Stand: 16.08.2004

[BSI1] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
Leitfaden zur Einführung von Intrusion-Detection-Systemen.
URL: http://www.bsi.de/literat/studien/ids02/dokumente/Leitfadenv10.pdf
Stand: 15.07.2004

[BSI2] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
Intrusion Detection Grundlagen
URL: http://www.bsi.de/literat/studien/ids02/dokumente/Grundlagenv10.pdf
Stand: 15.07.2004

[BSI3] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
Rechtliche Aspekte beim Einsatz von IDS
URL: http://www.bsi.de/literat/studien/ids02/dokumente/Rechtv10.pdf
Stand: 15.07.2004

[BSI4] Bundesanstalt für Sicherheit in der Informationstechnik (BSI)
Informationen zu Computer-Viren
URL: http://www.bsi.de/av/virbro/kap1/kap1_2.htm
Stand: 11.07.2004

[c't DoS] Patrick Brauch
Artikel „Geld oder Netz“
In: c't - Ausgabe Nr.14/2004

[DFN-CERT] Zentrum für sichere Netzdienste GmbH
Technische Maßnahmen gegen Spam
URL: http://www.cert.dfn.de/infoserv/dib/dib-9901.html
Stand: 16.08.2004

[Earthlink] Andreas Wilkens
Earthlink and Webroot track the growth of spyware
URL: http://www.earthlink.net/about/press/pr_spyAudit/
Stand: 05.08.2004

[Hacker's Guide] Anonymous
Hacker's Guide - Sicherheit im Internet und im lokalen Netz
Markt+Technik Verlag 2003

[HeiseSec] Jürgen Schmidt
Artikel „Besser vorbeugen - Intrusion Prevention soll Angriffe abwehren“
URL: http://www.heise.de/security/artikel/print/42557
Stand: 24.08.2004

[Hruska] Jan Hruska
Computer-Viren erkennen und abwehren
Prentice-Hall International Inc., London 1991

[ISS Signature] Internet Security Systems
Signature Database
URL: http://www.iss.net/security_center/reference/vuln/*Signaturname*
Stand: 19.08.2004

[MS-Security1] Microsoft Deutschland
Microsoft Security Bulletin MS04-011
URL: http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/bulletinMS04-011.htm
Stand: 05.08.2004

[NetworkComputing] Michael Piontek
Artikel „Intrusion-Prevention-Scanner - Meilenstein oder Marketing“
in: Network Computing - Augabe Nr. 18/2003

[NSS Report IPS] The NSS Group
IPS Group Test (Edition 1)
URL: http://www.nss.co.uk/ips/edition1/index.htm
Stand: 27.08.2004

[Oldfield] Paul Oldfield
Von Viren, Würmern und Trojanern
Sophos Vlg., Nieder-Olm 2001

[Siemens Lexikon] Siemens AG
Das Siemens Online Lexikon
URL: http://www.siemens.de/
index.jsp?sdc_p=pICNGo1174233fcl0smnt4u0
Stand: 12.08.2004

[Sophos] Sophos Virendatenbank
URL: http://www.sophos.de
Stand: 12.07.2004

[Tanenbaum1] Andrew S. Tanenbaum
Moderne Betriebssysteme
Parson Studium 2002 - 2., überarbeitete Auflage

[Tanenbaum2] Andrew S. Tanenbaum
Computernetzwerke
Parson Studium 2000 - 3., revidierte Auflage

[ZDNet Braue] David Braue
Artikel „Intrusion Detecton-Systeme: im eigenen Netz gefangen?“
URL: http://www.zdnet.de/enterprise/print_this.htm?pid=39117883-20000006c
Stand: 24.08.2004

[ZDNet Snell] Markus Snell
Artikel „Intrusion-Detection-Systeme: eine Einführung“
URL: http://www.zdnet.de/enterprise/print_this.htm?pid=20000452-20000006c
Stand: 24.08.2004

Anhang

Inhaltsverzeichnis

Anforderungsanalyse

		ISS	NAI
M[98]	Leistung 100 Mbit Vollduplex	x	x
M	Netztyp: Ethernet	x	x
M	In-Line (Intrusion Prevention)	x	x
M	Appliance	x	x
M	Geringe Latency (ca. 100us)	x	x
M	802.1q Unterstützung	x	x (16 VLANs)
M	Bei Ausfall/Fehler durchschalten	x	x
M	Updates einspielen ohne den Netzverkehr zu beeinträchtigen	x	x
M	Virtual Patching (im Gegensatz zu Network AV)	x	0
S[99]	Aufbereitung von Paketen und Protokoll-Inkonsistenzen	x	x
		100 %	90 %

Hostsensoren (auch Client)			
M	Windows 2000 / 2003 (Server)	x | 0	x | 0
M	Überwachung des hostspezifischen Netzverkehrs	X	x
M	Überwachung der Registry und BS-spezifischen Daten	X	x
S	Client (Laptop) Sensoren	X	x
		100 %	100 %

Kalibrierung und Skalierbarkeit			
M	Definition von eigenen Signaturen	x	0
M	Änderung bestehender Signaturen	x	0
M	Unterschiedliche Alarmklassen	x	x
S	Detaillierte und nachvollziehbare Doku der Signaturen	x	0
		100 %	25 %

Intrusion Response			
M	Alarm per Email und SNMP	x	x
M	Unterbrechen von Verbindungen	x	x
M	Rohdaten-Log (Evidence Logging)	x	x
S	Ausführung nutzerfreundlicher Kommandos / Skripts	x	x
		100 %	100 %

[98] Muß-Kriterium

[99] Soll-Kriterium

Management und Auswertfunktionen			
M	Automatisches Einspielen von Updates (Signaturen, Patches)	x	x
M	Backup von Policies und Signaturen	x	x
M	Umfangreiche Such- und Auswertfunktionen	x	x
M	GUI-basierende Administrationsoberfläche	x	x
M	System muss Sensorausfälle erkennen.	x	x
M	Reset von Sensoren -> System automatisch erkennen	x	x
M	Zentrales Management für alle Sensortypen	x	0
S	Detaillierte Datenbank zur Anngriffsbeschreibung ...	x	0
S	Benutzer- und Rechteverwaltung des IDS	x	0
S	Datenhaltung	MS SQL	MySQL
S	System muss Client Sensoren mit Laptoplösung anbieten	x	0
		100 %	50 %
	GESAMTWERTUNG	**100 %**	**73 %**

Tests

Topologie zwischen den Sensorinterfaces der G200

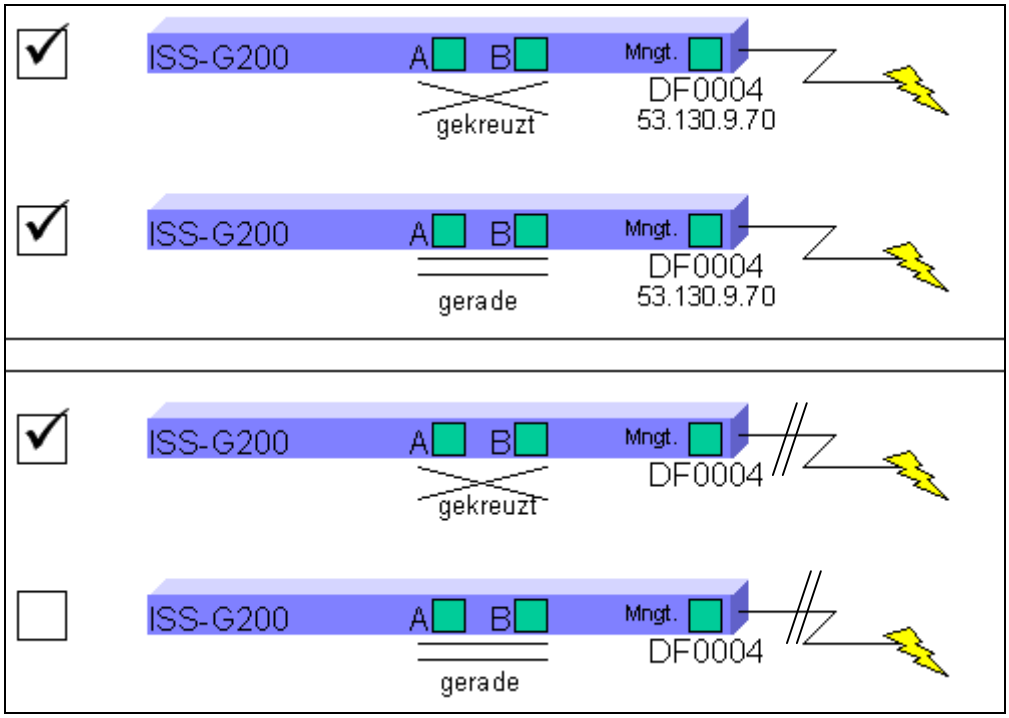


Abbildung Anhang 1 - Verbindung zwischen Interfaces A und B

Durchführung:

Testen der Verbindung zwischen Interface A und B wenn

a) Stromversorgung der Appliance vorhanden

b) Stromversorgung der Appliance unterbrochen

Die Ermittlung der Topologie zwischen den Sensorports wird mit einem Netzwerk-Kabeltester durchgeführt

Ergebnis:

Im Betriebszustand erkennt die Appliance die angeschlossenen Geräte selbst und schaltet automatisch die Sensorports, damit eine Verbindung möglich ist.

Bei Stromausfall, ziehen die Relais der Appliance an und kreuzen die Verbindung zwischen den Interfaces.

Aufbau der Testumgebung

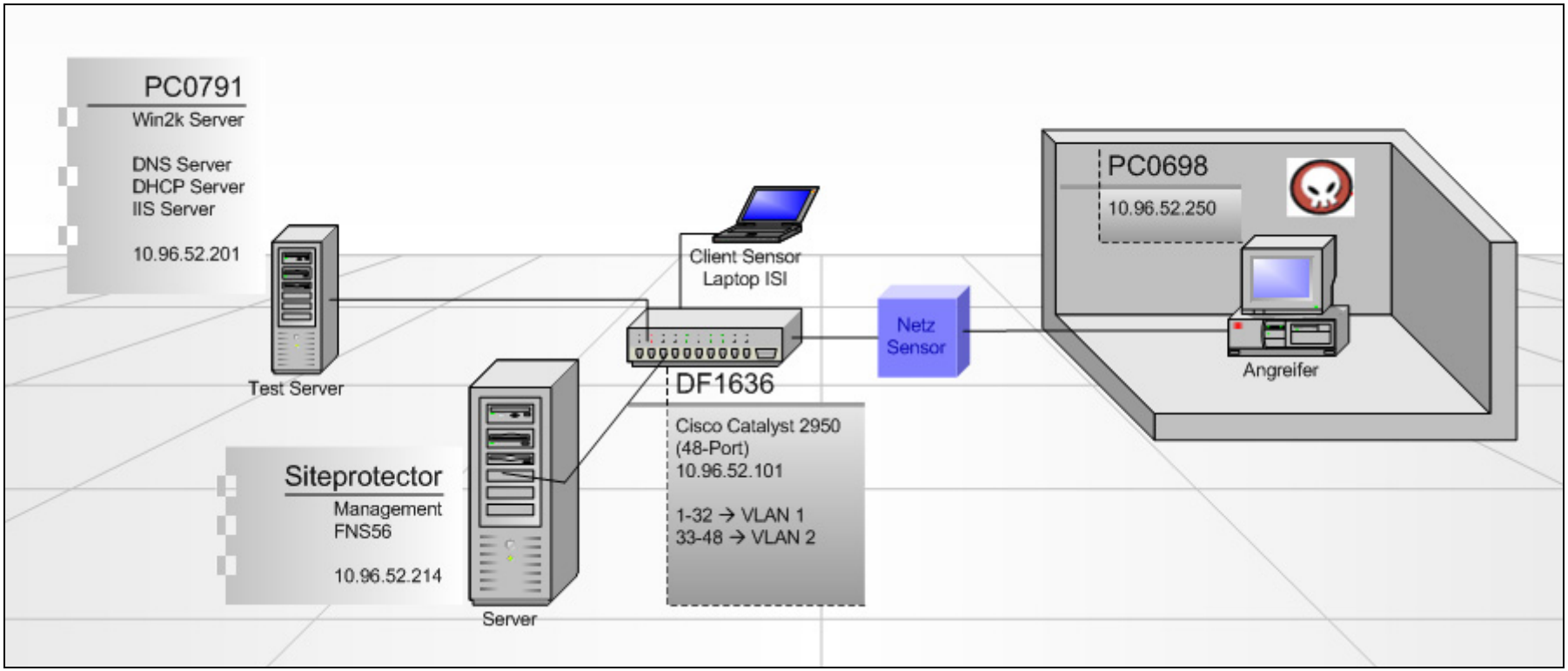


Abbildung Anhang 2 - Testumfeld

Auszug der Ereignisse des Monats August 04

FILTERS:

Time BETWEEN (2004-07-31 22:00:00 GMT, 2004-08-31 06:00:00 GMT)

To find Vulnerability information go to:

http://www.iss.net/security_center/reference/vuln/[vulnerability name].htm

Report Generated: Fri Sep 10 08:43:42 CEST 2004

Severity	Tag Name	Event Count	Source Count	Target Count	Sensor Name
High	HTTP_IIS_Unicode_Wide_Encoding	256	23	6	fn_df0004
High	SMB_NT_Transact_Bo	180	2	2	fn_df0004
High	HTTP_Windows_Executable	86	11	5	fn_df0004
High	HTTP_IIS_Unicode_Encoding	31	1	1	fn_df0004
High	SSL2_Master_Key_Overflow	29	12	5	fn_df0004
High	SSL_PCT1_Overflow	19	3	6	fn_df0004
High	HTTP_DotDot	8	2	2	fn_df0004
High	HTTP_Code_Red_II	7	7	4	fn_df0004
High	HTTP_ActiveX	2	2	2	fn_df0004
High	HTTP_Nimda_Worm	2	1	1	fn_df0004
High	SQL_PasswordArray_Overflow	1	1	1	fn_df0004
High	Startup_of_important_programs	1	1	1	fn_lan_srv_fns41
Med	SNMP_Activity	442	20	9	fn_df0004
Med	SNMP_Community	442	20	9	fn_df0004
Med	HTTP_URL_Name_Very_Long	147	45	5	fn_df0004
Med	TCP_Port_Scan	99	2	1	fn_lan_srv_fns4
Med	TCP_Port_Scan	93	1	1	fn_lan_srv_fns41
Med	HTTP_IIS_Double_Eval_Evasion	64	11	5	fn_df0004

Med	HTTP_repeated_character	50	2	2	fn_df0004
Med	SMB_Winreg_File	30	1	2	fn_df0004
Med	Nachi_Ping_Protection	29	27	2	fn_df0004
Med	HTTP_IIS_UTF8_Evasion	29	3	2	fn_df0004
Med	SMB_Filename_Overflow	16	1	1	fn_df0004
Med	FSP_Detected	15	6	3	fn_df0004
Med	Ping_Sweep	15	1	4	fn_lan_srv_fns41
Med	SNMP_Set	9	1	3	fn_lan_srv_fns41
Med	Ping_Sweep	8	8	1	fn_df0004
Med	FSP_Write_File	8	2	2	fn_df0004
Med	HTTP_Connect_Proxy_Bypass_SMTP	6	2	4	fn_df0004
Med	TCP_Port_Scan	4	2	2	fn_df0004
Med	HTTP_IIS_Percent_Evasion	2	1	1	fn_df0004
Med	Smurf_Attack	1	1	1	fn_lan_srv_fns41
Med	SNMP_Counter64	1	1	1	fn_lan_srv_fns41
Med	FSP_Read_File	1	1	1	fn_df0004
Low	Synthesized_Network_Attack_Flood	158	1	4	fn_lan_srv_fns41
Low	Netbios_Session_Request	117	20	7	fn_df0004
Low	Netbios_Session_Rejected	108	1	15	fn_df0004
Low	HTTP_Authentication	81	1	1	fn_lan_srv_fns4
Low	SMB_Malformed	36	3	2	fn_lan_srv_fns41
Low	SMB_Malformed	36	1	1	fn_lan_srv_fns4
Low	HTTP_Authentication	22	4	5	fn_df0004
Low	TCP_Service_Sweep	16	2	3	fn_df0004
Low	SMB_Auth_Failed	15	1	1	fn_lan_srv_fns4
Low	SNMP_RMON_Collections	12	1	4	fn_lan_srv_fns41

Low	Echo_Reply_Without_Request	10	1	1	fn_df0004
Low	Netbios_Session_Granted	9	6	5	fn_df0004
Low	Ping_Flood	6	2	3	fn_df0004
Low	Failed_login-bad_username_or_password	5	1	1	fn_lan_srv_fns41
Low	SMB_Executable_Access	4	1	1	fn_lan_srv_fns4
Low	Failed_login-bad_username_or_password	4	1	1	fn_lan_srv_fns4
Low	MSRPC_Share_Enum_Sweep	2	1	1	fn_lan_srv_fns4
Low	IIS_Reveal_Address	1	1	1	fn_df0004
Low	Email_ServerID	1	1	1	fn_lan_srv_fns41

Betriebshandbuch „ISS Proventia und Siteprotector“

1. Siteprotector Login

Es gibt 3 Möglichkeiten sich mit dem ISS Siteprotector zu verbinden:

- Installation der Siteprotector Konsole auf dem Client:
  Über den Internet Explorer eine Verbindung zu: https://fns56:3994 herstellen.
  Mit Klick auf den Menüpunkt „Siteprotector Deployment Manager“, kommt man auf den Siteprotector Installationsmanager.
  Über „Install Additional SiteProtector Console“ lädt man sich das Installationspaket für die Konsole.
  Wichtig: Die Konsole ist ein auf JAVA-basierendes Programm. Eine aktuelle JAVA (JRE) Version ist erforderlich (mindestens 1.4.2).

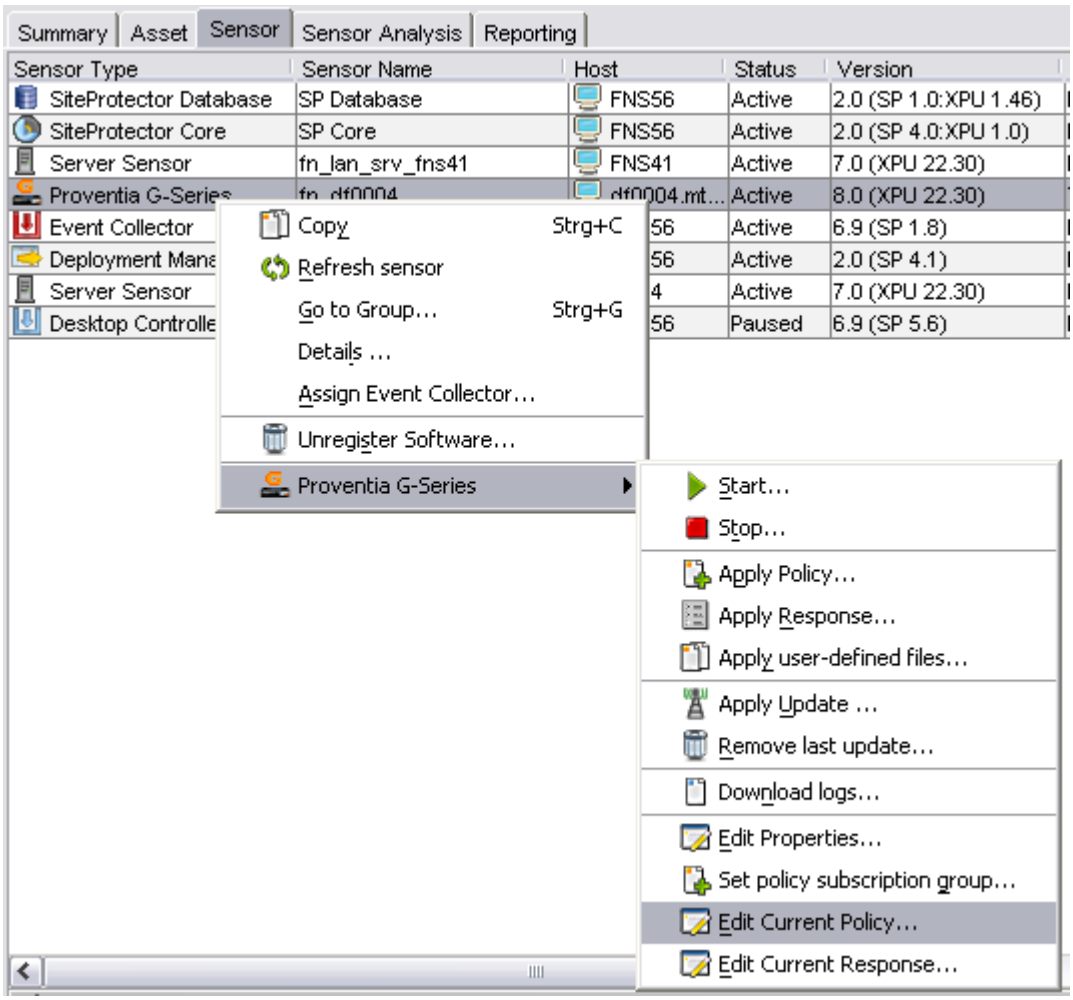
- Zugriff auf die Weboberfläche
  Über den Internet Explorer eine Verbindung zu: https://fns56:3994 herstellen.
  Mit „SiteProtector Web Access“ kommt man zur Oberfläche.
  Wichtig: Der Zugriff ist unabhängig von Berechtigungen schreibgeschützt. Es können keine Daten, Einstellungen oder Policies verändert werden.

- Remote Desktop Connection oder VNC
  Über dem MS RDP oder dem VNC Viewer kann man sich auf den Managementserver verbinden (FNS56). Das Betriebssystem ist Windows 2003 Server.
  Auf dem Desktop der Verknüpfung „Console“ folgen.

2. Zugriffsberechtigungen

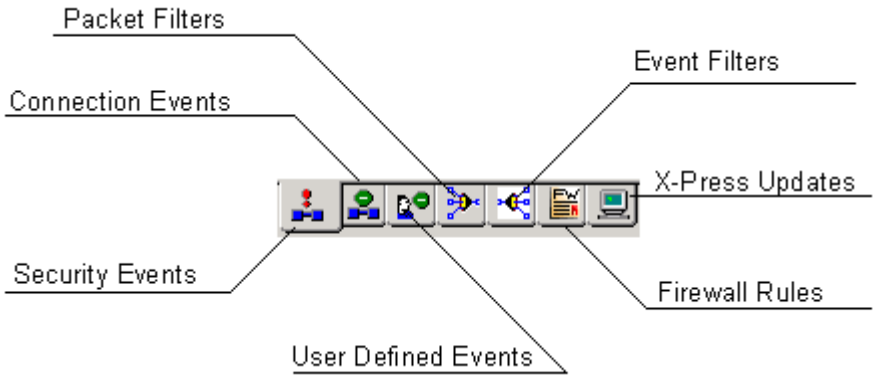
Der Zugriff auf den Siteprotector ist über eine Gruppenmitgliedschaft auf dem Managementserver realisiert. Mitglieder der lokalen Gruppe „RSSP-Administrator“ haben Zugriff auf den Siteprotector.

3. Manuelle Änderung der Policy einzelner Sensoren



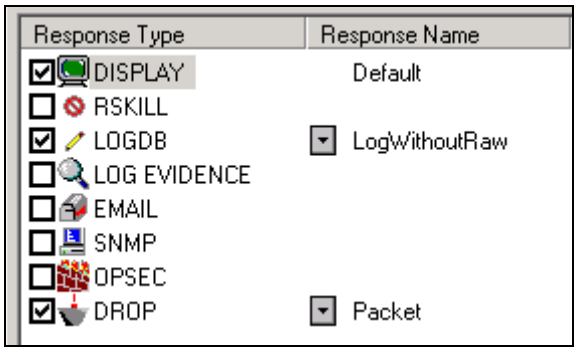
Die Policy kann auf Serversensoren, Netzsensoren und Desktop Sensoren verändert werden. Alternativ können unter dem Menüpunkt „Sensor → Manage → Policy“ alle Policies angezeigt oder verändert werden.

Die Toolbar der Netzsensoren in den Policy Einstellungen:



- Security Events

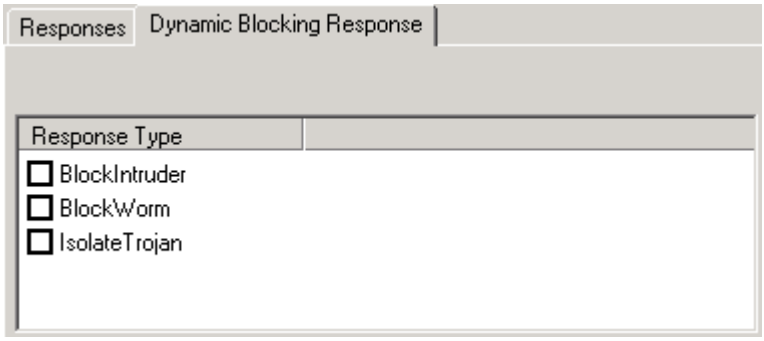
Der Signaturbestand ist unterteilt in *Attacks* - also konkrete Attacken und in *Audits* welche auf keine Attacken hindeuten, sondern rein informativ sind.
Aktivierte Signaturen sind mit einem Häckchen markiert. Auf getriggerte Signaturen wird ja nach Einstellung unterschiedlich reagiert. Hier sind die Einstellungen:



- **Display** = Funktioniert nur in Kombination mit LogDB. Das Ereignis wird auf der Konsole ausgegeben.
- **RSKill** = Falls das TCP-Reset Interface angeschlossen ist, wird ein TCP-Reset an den Angreifer zurück geschickt.
- **LogDB** = Ereignis wird in die Datenbank geloggt.
  - LogWithoutRaw = Keine Pakete werden mitgeloggt.
  - LogWithRaw = Alle mit dem Ereignis zusammenhängenden Pakete werden gespeichert.
- **Log Evidence** = Speicherung des Pakets, welches das Event ausgelöst hat.
- **EMail** = Benachrichtigung über EMail.
- **SNMP** = SNMP-Trap an SNMP-Manager senden.

- **OPSEC** = Dynamisches Anpassen des Firewall Ruleset (nicht empfehlenswert).
- **Drop** = Verfügbar falls der Sensor im Inline Modus arbeitet. Folgende Einstellungen sind möglich:
  - ConnectionWithReset = Alle Pakete der Verbindung werden geblockt. Ein TCP Reset wird außerdem ausgelöst
  - Paket = Alle Pakete der Verbindung werden geblockt.
  - Connection = Das Paket welches der Auslöser ist, wird geblockt.

„Dynamic Blocking“ ist eine Erweitung der Blockierfunktion.



- **BlockIntruder** = Alle Verbindungen vom Angreifer zum Ziel werden für eine gewisse Zeitspanne (Default: 3600s) geblockt.
- **BlockWorm** = Alle Verbindungen welche vom Angreifer mit dem Angriffsdienst kommen, werden für eine Zeitspanne geblockt. Das Ziel ist dabei nicht relevant.
- **IsolateTrojan** = Isoliert schädlichen Code, der in scheinbar harmlosen Code platziert ist.

- Connection Events

Definition eigener Signaturen, welche auf einer Verbindung beruht. Die Verbindung ist mit den Parametern Protokoll, Quelle, Ziel und Service definiert.

- User Defined Events

Definition eigener Signaturen, welche auf dem Inhalt eines Pakets beruhen. Beispiel könnte die Alarmierung jedes SMNP-Pakets sein, welches einen bestimmten Community String enthält.

- Packet Filters

Die Filterung von Ereignissen in Abhängigkeit von Verbindungsparametern Protokoll, Quelle, Ziel, Service. Gefilterte Pakete durchlaufen die Policy (Security Events und X-Press Updates) nicht mehr.

- Event Filters

Die Filterung von Ereignissen in Abhängigkeit von Quell-Adresse/Service, Ziel-Adresse/Service und der Signaturbezeichnung. Gefilterte Pakete durchlaufen die Policy (Security Events und X-Press Updates) nicht mehr.

- Firewall Rules

Definition eigener Firewall-Rules im bestimmten Verkehr zu blockieren. Diese Funktion wird nicht genutzt, da die MTU eine seperate Firewall Appliance nutzt.

- X-Press Updates

Dasselbe wie „Security Events“. Hier sind die neuen Signaturen hinterlegt, welche nach X-Press Update Version gruppiert sind. Diese Signaturen werden bei einem neuen Siteprotector Release in den Karteireiter „Security Events“ integriert.

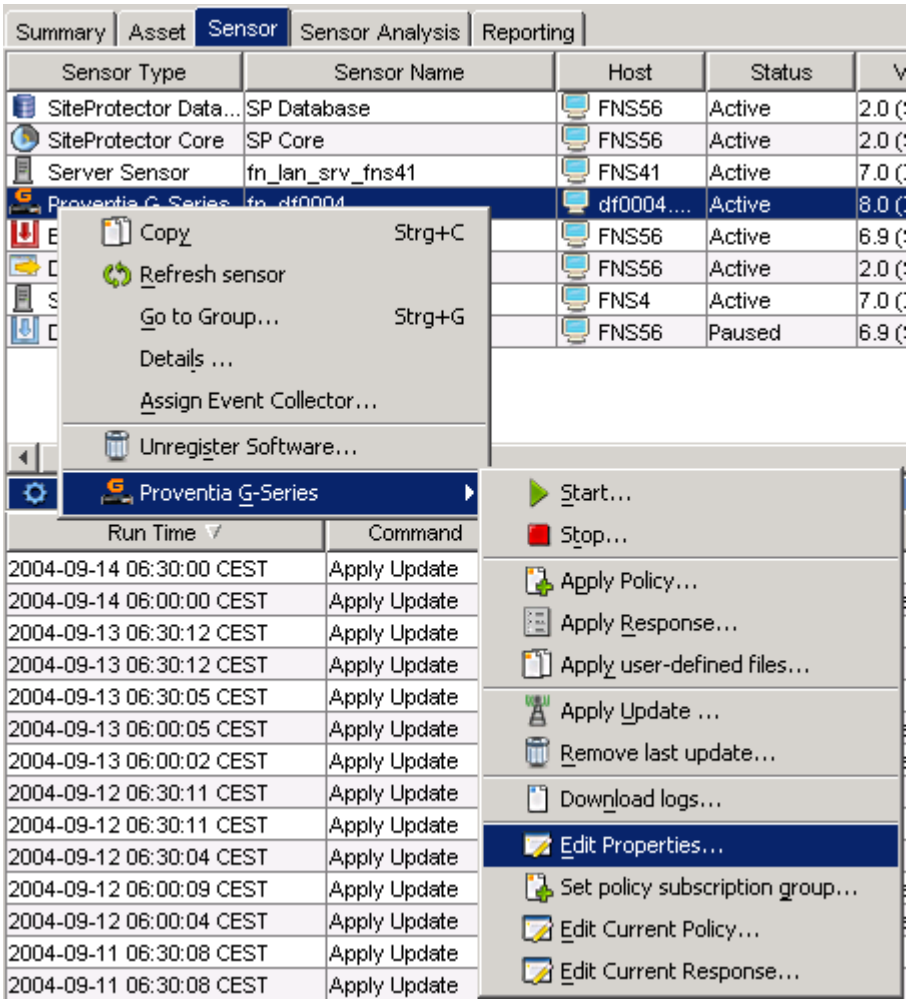
Wichtig: Bei Änderungen der Policy sind diese in dem entsprechenden Exel Formular auf dem Laufwerk „G:\ISI\NETZ\Intrusion Prevention System\Policy“ zu dokumentieren.

4. Simulation- und Protection Modus

Im Simulationsmodus blockt der Sensor unter keinen Umständen Pakete. Im Inline-Protection Modus können Pakete nach den Vorgaben in der Policy blockiert werden. Um den Sensor in den Modus „Simulation“ oder „Protection“ zu setzten, sind folgende Aktionen durchzuführen:

Siteprotector - Karteireiter „**Sensor“**.

Rechter Mausklick auf den Sensor → Edit Properties.



Im Fenster mit den Sensoreigenschaften kann in der Combobox „Inline Appliance Mode“ entweder „Inline Simulation“ oder „Inline Protection“ eingestellt werden. Mit Klick auf „O.K.“ werden wie Änderungen sofort aktiv.

5. X-Press Updates

Der Siteprotector holt sich vom Hersteller ISS in regelmäßigen Abständen neue Signaturen für die Sensoren. Der Managementserver nimmt alle zwei Stunden Kontakt mit ISS auf. Das Intervall und die Quelle der Signaturchecks ist in den Eigenschaften des „Siteprotector Cores“ einzustellen.

Sensor Tab: Rechter Mausklick auf „Siteprotector Core“ → „Edit Properties“

Jeden Tag zwischen 6:00 und 6:30 verteilt der Siteprotector die Updates auf die Sensoren. In der Policy sind diese neuen Signaturen unter dem Karteireiter „X-Press Updates“ aufgelistet.

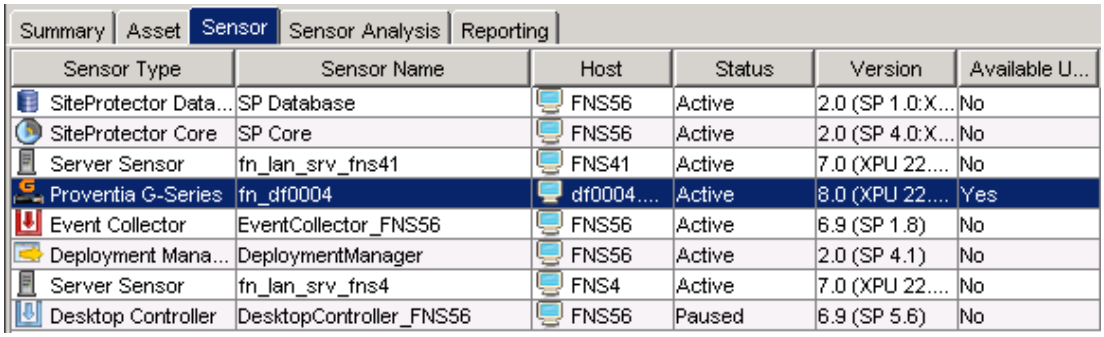
Die Signaturen sind deaktiviert und müssen manuell aktiviert werden. Es muss anhand der Beschreibungen selbstständig eine Entscheidung getroffen werden, ob ein Ereignis blockiert wird oder nicht. Um einen Schutz zu erreichen genügt das Markieren des Feldes „Drop“ mit der Einstellung „ConnectionWithReset“.

Die Empfehlungen von ISS welche Signaturen aktiv sind und die Reaktion auf die Signaturen können in der Default Policy „Attack Blocker_inline“ nachgeschlagen werden. Änderungen an der Policy der Sensoren sind im Exel Formblatt einzutragen. Siehe auch 3. Manuelle Änderung der Policy einzelner Sensoren. Der Policyeditor kann einfach geschlossen werden. Durch einen Dialog speichert der SP die Policy und verteilt sie auf den Sensoren.

6. Updates der Sensoren und des Management

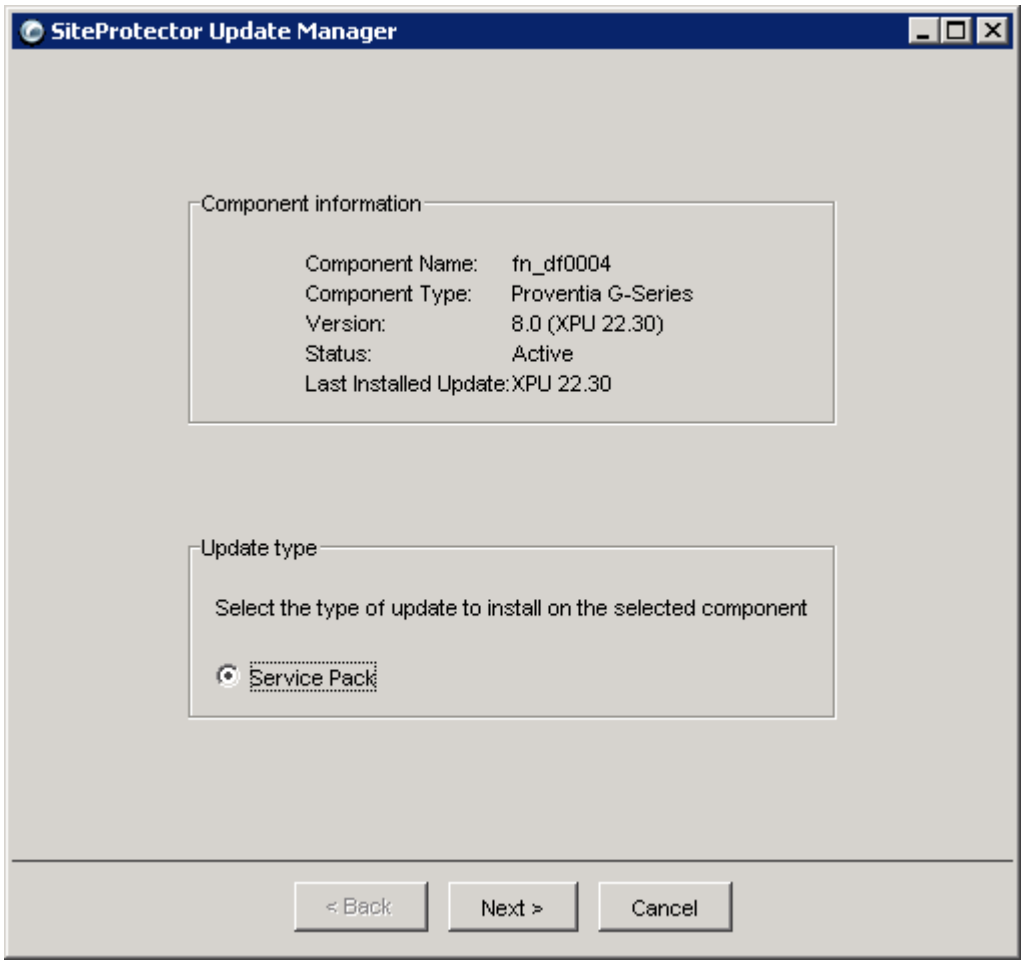
Versionsupdates der Sensoren und der Managementstation werden nicht automatisch durchgeführt. Die Installation der neuen Pakete erfolgt manuell. Diese Updates sind nicht sehr zeitkritisch.

Um zu erkennen ob Updates für einen Sensor verfügbar sind, genügt ein Blick auf den Karteireiter „Sensor“ im Siteprotector unter der Spalte „Avaiable Update“.

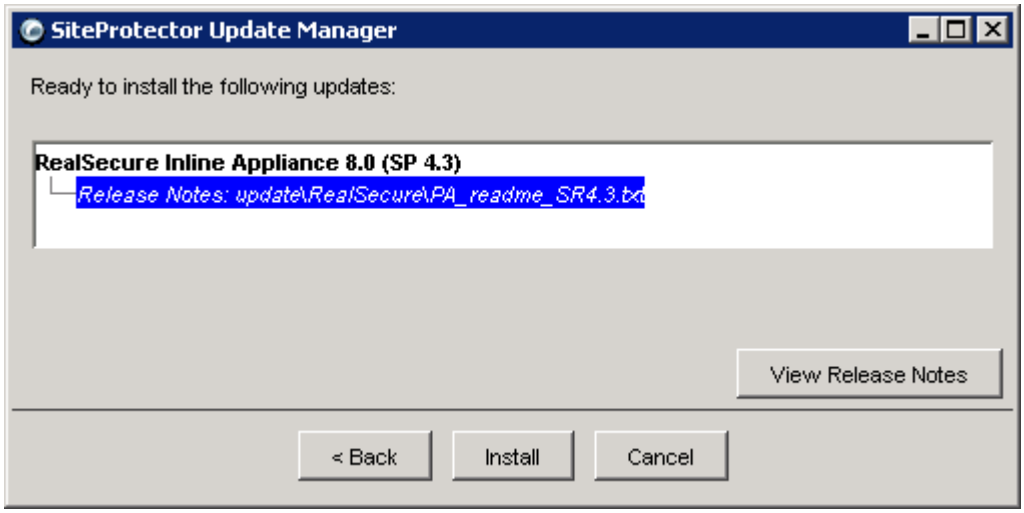


Sensor Type	Sensor Name	Host	Status	Version	Available U...
SiteProtector Data...	SP Database	FNS56	Active	2.0 (SP 1.0:X...	No
SiteProtector Core	SP Core	FNS56	Active	2.0 (SP 4.0:X...	No
Server Sensor	fn_lan_srv_fns41	FNS41	Active	7.0 (XPU 22....	No
Proventia G-Series	fn_df0004	df0004....	Active	8.0 (XPU 22....	Yes
Event Collector	EventCollector_FNS56	FNS56	Active	6.9 (SP 1.8)	No
Deployment Mana...	DeploymentManager	FNS56	Active	2.0 (SP 4.1)	No
Server Sensor	fn_lan_srv_fns4	FNS4	Active	7.0 (XPU 22....	No
Desktop Controller	DesktopController_FNS56	FNS56	Paused	6.9 (SP 5.6)	No

In diesem Beispiel ist für den Sensor „fn_df0004“ ein Update verfügbar.
Installiert wird das Update über einen Rechtsklick auf den Sensor → Proventia G-Series → Apply Update. Falls die Installation sofort erfolgen soll, bestätigt man das folgende Fester mit Klick auf „OK“. Im folgenden Fenster werden Informationen über den Sensor und den Updatetyp angegeben.

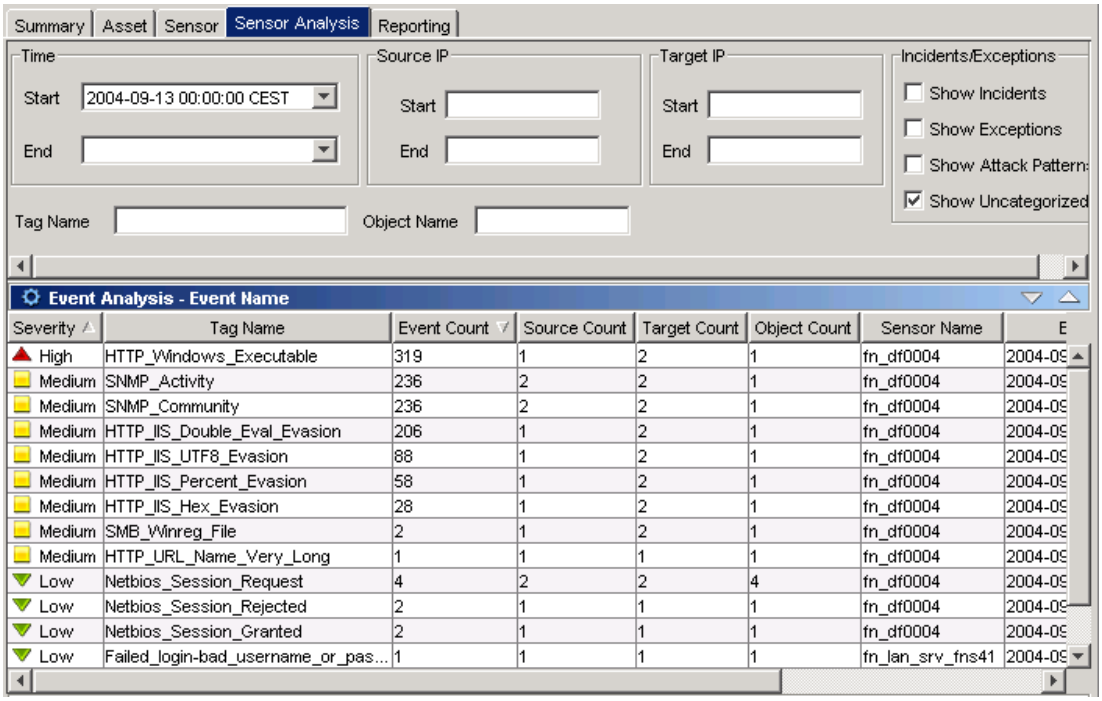


Falls mehrere Updates verfügbar sind (auch X-Press), sind neben „Service Release“ weitere Punkte angegeben.
Mit „Next“ kommt man auf das Fenster mit der EULA (End User License Agreement), welches mit Next bestätigt wird.



Das nächste Fenster ist das letzte vor der Installation. Mit Klick auf den Button „Install“ wird das Update durchgeführt. Es müssen auf jeden Fall die Release Notes (Button „Release Notes“) beachtet werden, welche den Updates beiliegen. Hier ist u.a. beschrieben, wie sich der Sensor nach dem Update verhält und ob das Update ggf. Ausfälle zwischen den Monitorports auslöst.

7. Logging



Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Sensor Name	E
High	HTTP_Windows_Executable	319	1	2	1	fn_df0004	2004-09
Medium	SNMP_Activity	236	2	2	1	fn_df0004	2004-09
Medium	SNMP_Community	236	2	2	1	fn_df0004	2004-09
Medium	HTTP_IIS_Double_Eval_Evasion	206	1	2	1	fn_df0004	2004-09
Medium	HTTP_IIS_UTF8_Evasion	88	1	2	1	fn_df0004	2004-09
Medium	HTTP_IIS_Percent_Evasion	58	1	2	1	fn_df0004	2004-09
Medium	HTTP_IIS_Hex_Evasion	28	1	2	1	fn_df0004	2004-09
Medium	SMB_Winreg_File	2	1	2	1	fn_df0004	2004-09
Medium	HTTP_URL_Name_Very_Long	1	1	1	1	fn_df0004	2004-09
Low	Netbios_Session_Request	4	2	2	4	fn_df0004	2004-09
Low	Netbios_Session_Rejected	2	1	1	1	fn_df0004	2004-09
Low	Netbios_Session_Granted	2	1	1	1	fn_df0004	2004-09
Low	Failed_login-bad_username_or_pas...	1	1	1	1	fn_lan_srv_fns41	2004-09

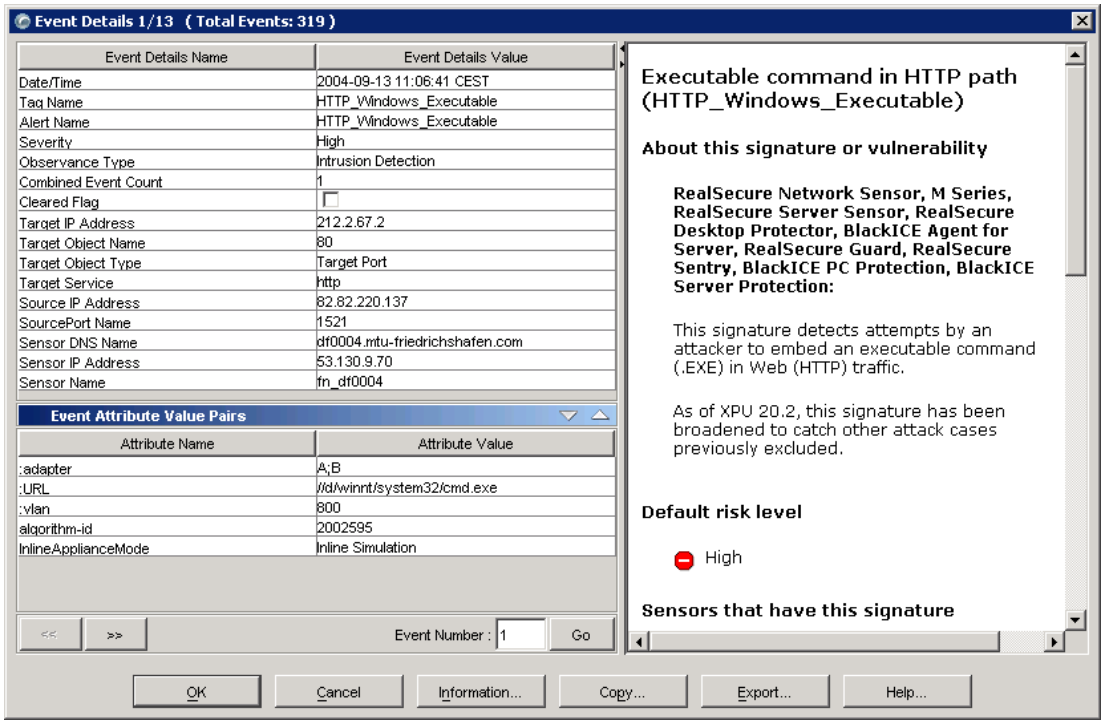
Unter dem Reiter „Sensor Analysis“ sind die aufgezeichneten Events aufgelistet, die zu den ausgewählten Sensoren der „Enterprise Groups“ gehören. Standardmäßig ist die Ansicht „Event Analysis - Event Name“ geladen um einen Überblick über die laufenden Events zu erhalten.
Um die Events automatisch alle 60 Sekunden zu aktualisieren muss der Knopf  Aktiv sein.

Die Sortierung ist absteigend nach Priorität und Anzahl der Ereignisse. Standardmäßig werden die Ereignisse des laufenden Tages angezeigt.
Um die Events nach Quelle und Ziel zu filtern, können in den Textboxen die Adressbereiche eingetragen werden. Um einzelne Events genauer analysieren gibt es zwei weitere Ansichten:

1. Auswählen der Analyseansicht „Event Analysis - Details“

oder rechter Mausklick auf das Ereignis → „What are the Event Details?“ um die Details des ausgewählten Ereignisses zu erhalten.

2. Recher Mausklick auf das gewünschte Ereignis → „View Event Details“



In dieser Ansicht ist jedes einzelne Event einer Signatur aufgeschlüsselt. Im Fenster rechts wird die jeweilige Signaturbeschreibung angezeigt.

Erweiterte Filter- und Auswertmöglichkeiten erhält man mit Klick auf das „Advanced“ Symbol 
oder mit Auswählen von „Analysis → Configure → Add/Remove Data Columns“ in der Hauptmenüleiste.
Ob ein Ereignis geblockt wurde, kann aus der detaillierten Ansicht entnommen werden. Hier wird ausdrücklich erwähnt, falls eine Blockierung stattgefunden hat.

Einzelne Ereignisse können prinzipiell mit der Entf Taste gelöscht werden.
Achtung: Vor Drücken der Entf Taste muss sichergestellt sein, dass auch ein Ereignis im Fenster „Event Analysis“ ausgewählt ist. Falls der Fokus auf einem Element in der Gruppenanzeige „Enterprise Groups“ liegt, kann mit der Taste Entf eine ganze Gruppe Sensoren gelöscht werden!

Alle Filter die auf der Anzeige liegen können mit der Taste F7 aufgehoben werden.

8. Automatische Jobs

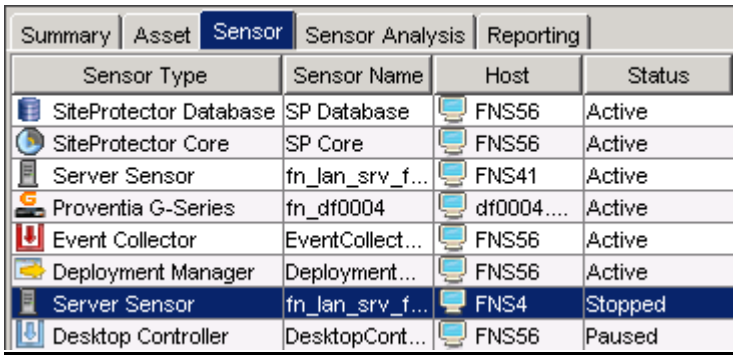
Auf der FNS56 laufen folgende automatische Aktionen:

Wochentag	Uhrzeit	Aktion	Script
Mo - Su	01:00	Sichern der Analyseansichten nach D:\Backup\analysis	Scripts\Backup_Analysis.bat
Mo - Su	01:10	Sichern der Eigenschaften und Policies der Sensoren und SP Komponenten nach D:\Backup\Policy_Properties	Scripts\Backup_Pol_Prop.bat
Mo - Su	06:00	X-Press Updates der Netzsensoren	--
Mo - Su	06:30	X-Press Updates der Serversensoren	--
Mo - Su	06:45	Testen der Netzsensoren	Scripts\NetworkSensor_Test.bat
Mo - Su	07:00	Testen der Hostsensoren	Scripts\ServerSensor_Test.bat

Falls zusätzliche Jobs hinzugefügt werden, sind diese in „D:\Informational\Dayly Tasks.txt“ zu vermerken.

9. Troubleshooting

Status der Sensoren



Die Sensoren können auf der Registrierkarte „Sensor“ verschiedene Stati annehmen.

Im Normalzustand ist der Status **Active**, der darauf hinweist, dass der Sensor ordungsgemäß arbeitet. Mit Rechtsklick auf den Sensor → Start/Stop kann der Sensor aktiviert oder deaktiviert werden.

- Active = Sensor arbeitet ordungsgemäß.
- Stopped = Sensor ist deaktiviert. Aktivierung mit Rechtsklick auf „Sensor → Start“.
- Paused = Sensor/Komponente wird im Moment nicht benötigt und ist nicht Aktiv (bsp.: Desktop Controller).
- Processing = Der Sensor verarbeitet gerade ein Update oder einen Job.
- Error = Ein Fehler ist aufgetreten. Rechtsklick auf „Sensor → Details“ um den Fehler zu analysieren.

10. Assets

Assets sind Geräte, welche anhand der IP-Adresse im Siteprotector erfasst sind. Um einen Sensor zum SP hinzufügen zu können, muss das dazugehörige Gerät zuerst als Asset im Siteprotector definiert sein. Assets können manuell durch eine IP-Adresse oder ein Netz definiert werden.

Hosts im Active Directory werden automatisch hinzugefügt (Enterprise Group: DC=com) und in regelmäßigen Abständen aktualisiert.

CD

Inhalt:

- Diplomarbeit im DOC (Microsoft Word 2000) und im PDF Dateiformat
- Präsentation der Diplomarbeit (Microsoft Powerpoint)
- Abbildungen welche für die Diplomarbeit erstellt wurden
- Beispielreports

CD-ROM entfällt
in diesem Exemplar