

# IBM Proventia Intrusion Prevention System Protection Engine

## Highlights

- **Abwehr von Sicherheitsbedrohungen, bevor sie Ihr Netzwerk beeinträchtigen können**
- **Schutz Ihres Netzwerks und der Geräte in Ihrem Netzwerk, wie z. B. Server, Desktops und Netzwerkinfrastruktur**
- **Schutz der geschäftskritischen Systeme, z. B. VoIP, Datenspeicher, Datenbanken, Serverfarmen und virtualisierte Umgebungen**
- **Schutz von Web-Servern und Webanwendungen, einschließlich Web 2.0-Technologie**
- **Schutz der Endbenutzer vor Angriffsprogrammen, die in scheinbar harmlosen Dokumenten versteckt sind, z. B. in Tabellenkalkulationen, Präsentationen, PDFs und Multimediadateien wie JPEG, GIF, ANI, QuickTime, Flash und ASF**
- **Beibehaltung der Netzwerkbandbreite durch Abwehr von Würmern und Hackerangriffen und Vermeidung einer nicht bestimmungsgemäßen oder unbefugten Nutzung des Netzwerks durch Blockieren von Skype, Instant Messaging und Peer-to-Peer-Filesharing**
- **Vermeidung von Datenverlusten durch besseren Schutz Ihres Netzwerks vor Angriffen und durch die Erkennung und Überwachung der Übertragung vertraulicher Daten über das Netzwerk**

## Sicherheitsbedrohungen stets einen Schritt voraus bleiben – mit der IBM Proventia Intrusion Prevention System Protection Engine

Die IBM Proventia IPS-Technologien (Intrusion Prevention System) wehren Gefahren aus dem Internet ab, bevor diese Ihre Geschäftsabläufe beeinträchtigen können, und schützen alle drei Ebenen Ihres Netzwerks: Kern-, Perimeter- und Remote-Segmente.

Die Grundlage der herausragenden Proventia IPS-Sicherheitstechnologie bildet die Proventia Protection Engine, die präventiven Schutz vor einer Vielzahl verschiedener Gefahren aus dem Internet bietet. Die Proventia Protection Engine basiert auf der jahrelangen Forschung und Entwicklung der IBM Internet Security Systems X-Force auf dem Gebiet der IT-Sicherheit. Die X-Force ist eine weltweit anerkannte, renommierte Forschungsorganisation, die sich auf die proaktive Untersuchung von Sicherheitsbedrohungen und der zugrunde liegenden Software-schwachstellen, die diese auszunutzen versuchen, spezialisiert hat.

Die Proventia Protection Engine kann ganze Kategorien von Angriffen, darunter neue und unbekannte Gefahren, abwehren, ohne dass Updates erforderlich sind. Andere Lösungen versuchen lediglich, geeignete Sicherheitssignaturen für einzelne Angriffsarten zu finden. Doch dieser Prozess ist zu langwierig, um neu entstehende Sicherheitsbedrohungen aufzuhalten, und führt zu einer höheren Fehlalarmquote, sowohl was falsch positive als auch falsch negative Ergebnisse betrifft.

Die Proventia IPS Protection Engine kann Gefahren für Netzwerke der folgenden Kategorien überwachen, erkennen und verhindern:

- *Angriffe auf Anwendungen*
- *Verschleierung von Angriffen durch Verschlüsselung (Attack Obfuscation)*
- *Cross-Site Scripting*
- *Datenlecks*
- *Angriffe auf Datenbanken*
- *DoS- und DDoS-Attacken*
- *Drive-by-Downloads*
- *Sicherheitsbedrohungen durch Insider*
- *Instant Messaging*
- *Schädliche Dokumenttypen*
- *Schädliche Multimediadateien*
- *Malware*
- *Angriffe auf Betriebssysteme*
- *Peer-to-Peer-Netzwerke*
- *Protokolltunnelung*
- *SQL Injection*
- *Angriffe auf Web-Browser*
- *Angriffe auf Web-Server*

Zur Abwehr dieser Angriffe nutzt die Proventia Protection Engine verschiedene Intrusion-Prevention-Technologien, darunter folgende:

- *Portzuordnung*
- *Portverfolgung*
- *Protokollanalyse*
- *Protokolltunnelung*
- *Mustererkennung (Pattern Matching)*
- *IBM Proventia Content Analyzer*
- *Injection Logic Engine*
- *Heuristik*
- *RFC-Konformitätsprüfung*
- *Statistische Analyse*
- *TCP Reassembly*
- *Flow Assembly*

## Die wichtigsten Netzwerkbedrohungen, die durch die Proventia Protection Engine abgewehrt werden

Während wir mit immer neuen Gefahren aus dem Internet konfrontiert werden, dürfen auch ältere Angriffsmethoden nicht außer Acht gelassen werden, und viele Angreifer bauen auf bekannten Methoden unbefugter Zugriffsversuche auf, um nicht erkannt zu werden. Die Proventia Protection Engine ist dafür konzipiert, die folgenden Sicherheitsbedrohungen aus dem Internet abzuwehren:

**Backdoors** – verschaffen einem Angreifer Zugriff auf ein System, indem sie die herkömmliche Prüfung bei der Anmeldung umgehen.



**Botnets** – sind Gruppen manipulierter Computer, die von einem Botnet-Betreiber gesteuert werden und für diesen bestimmte Aufgaben ausführen – in der Regel in böswilliger Absicht, z. B. zur Verbreitung von Spam und/oder Malware.



**Clientseitige Angriffe** – nutzen Sicherheitslücken im Web-Browser aus, um Drive-by-Downloads und verdächtige Browser-Verschleierungen zu installieren.



**Cross-Site Scripting (XSS)** – nutzt webbasierte Sicherheitslücken aus, um Schadcode in einen anscheinend legitimen Link einzubetten, der auf dem Computer eines Benutzers ausgeführt werden kann – in der Regel, um Daten zu stehlen.



**Distributed Denial of Service (DDoS)** – nutzt eine große Zahl von manipulierten Systemen, um ein einzelnes Ziel mit einer Flut von Nachrichten anzugreifen und das Zielsystem so lahmzulegen.



**Insider-Angriffe** – können Viren, Würmer und Trojaner in ein Netzwerk einschleusen oder versuchen, vertrauliche Daten zu stehlen.



**Instant Messaging** – kann verwendet werden, um Trojaner, Viren und sonstige Malware in ein Netzwerk einzuschleusen.



**Schädliche E-Mail** – wird häufig für Spyware und Phishing verwendet, um Benutzer auf schädliche Websites zu locken und dann Malware in das Netzwerk einzuschleusen.



**Peer-to-Peer-Netzwerke (P2P)** – ermöglichen die Übertragung von Dateien, die mit Viren und Trojanern infiziert sind, die Denial-of-Service-Angriffe ausführen und Daten beschädigen sollen.



**Protokolltunnelung** – platziert schädliche Daten für gewöhnlich innerhalb eines Protokolls einer höheren Ebene, sodass sie Netzwerksegmente passieren können, in denen Protokolle einer niedrigeren Ebene blockiert werden könnten.



**Reconnaissance** – bezeichnet eine Gruppe von Sicherheitsbedrohungen, die dazu dienen, Informationen auszuspionieren. Dazu gehören Brute-Force-Angriffe, Enumeration, das Erraten von Kennwörtern und Port-Scans.



**Rootkits** – sind eine Gruppe von Tools oder Programmen, die Hackern Administratorrechte oder Rootzugriff auf ein Netzwerk oder System verschaffen.



**Schadinhalte** – bezeichnet schädlichen Multimedia- und Shellcode, der in Dokumente eingebettet ist.



**SQL Injection** – ist eine Methode, bei der schädlicher SQL-Code „huckepack“ auf gewollten Befehlen durch die dynamische logische Ebene einer Webanwendung eingeschleust wird, um die Anwendung dazu zu veranlassen, Datenbankzugriff zu gewähren.



**Trojaner** – verstecken gefährlichen Code in scheinbar harmlosen Programmen oder Daten.



**Würmer** – sind Viren, die sich selbst replizieren, indem sie sich selbst als E-Mail-Anhang oder Teil einer Nachricht neu versenden.



## Mehrschichtige Intrusion-Prevention-Technologien in der Proventia Protection Engine

Die Proventia Protection Engine kombiniert verschiedene Technologien zur Bekämpfung von Sicherheitsrisiken, die gemeinsam Gefahren aus dem Internet abwehren. Sie nutzt die folgenden Methoden zur Abwehr von Angriffen:

**IBM Proventia Content Analyzer** – prüft und blockiert unverschlüsselte Daten in Ihrem Netzwerk mittels vordefinierter, speziell angepasster Signaturen. Diese Technologie bietet die Möglichkeit, nach Mischdateien zu suchen und Mischdokumente zu prüfen, darunter Microsoft Office-Dokumente, PDFs und Zip-Dateien – über zehn unterschiedliche Protokolle.

**Portzuordnung** – Intrusion-Prevention-Systeme sollten nicht davon ausgehen, dass eine bestimmte Art von Datenverkehr an einem bestimmten TCP/IP-Port auftaucht. Wenn sie es doch tun und die Art des Datenverkehrs zu dem angenommenen Port passt und daher passieren darf, können Angreifer Zugriff erlangen. Proventia prüft sämtlichen Datenverkehr, unabhängig vom Port, für den er bestimmt ist.

**Portverfolgung** – verfolgt Kommunikationssitzungen, um sicherzustellen, dass der ursprünglich zur Herstellung einer Verbindung verwendete Port der einzige verwendete Port ist. Dadurch werden Hacker, die sich Zugriff auf einen offenen Port mit authentischen Identifikationsdaten verschaffen, daran gehindert, eine Verbindung zu einem anderen offenen Port herzustellen, um unbemerkt Daten zu übertragen. Die Proventia-Technologie für die Portverfolgung verhindert zusammen mit anderen Technologien Datendiebstahl.

**Injection Logic Engine** – erkennt mittels heuristischer Verfahren böswillige Einschleusversuche, z. B. SQL Injection und die Einschleusung von Shellbefehlen, und schützt vor aktuellen und künftigen Schwachstellen, ohne dass Signaturupdates erforderlich sind.

**Protokollanalyse** – untersucht den Datenverkehr im Netzwerk, um abweichendes Verhalten zu erkennen, das nicht den akzeptierten Normen entspricht, und kann Protokolle bis zu Layer 2 des OSI-Modells decodieren. Durch die Protokollanalyse kann Proventia von der Norm abweichendes Verhalten erkennen, ohne auf Signaturen angewiesen zu sein.

**Protokolltunnelung** – wird manchmal in Verbindung mit der Portzuordnung verwendet. Proventia erkennt und verhindert die Protokolltunnelung, um schädliche und/oder vertrauliche Daten zu finden, die in Protokollen einer höheren Ebene eingebettet sind und so möglicherweise Netzwerksegmente passieren können, in denen Protokolle einer niedrigeren Ebene blockiert werden. Die Protokolltunnelung hindert Hacker daran, Firewalls zu umgehen, um Netzwerkzugriff zu erlangen, ohne Verdacht zu erregen. Sie verhindert außerdem, dass sowohl Insider als auch Hacker von außerhalb Tunnel einrichten und nutzen können, um Daten aus einem Unternehmen zu schmuggeln.

**Stateful Pattern Matching (zustandsbasierte Mustererkennung)** – verwendet hoch entwickelte Algorithmen, um Angriffsmuster zu erkennen – allerdings nur in bestimmten Teilen des Datenverkehrs, in denen tatsächlich ein Angriff stattfinden könnte. Dadurch lässt sich die Zahl falsch positiver Ergebnisse deutlich reduzieren. Proventia nutzt Stateful Pattern Matching in Verbindung mit heuristischen Verfahren, um neue Sicherheitsbedrohungen abzuwehren, die ihre Muster verändern, um nicht erkannt zu werden.

**Heuristik** – erkennt und stoppt Schadcode auf der Basis von dessen Verhalten, anstatt eine bestimmte Angriffssignatur oder ein bestimmtes Angriffsmuster zu vergleichen. Die Heuristik kann neu entstehende Sicherheitsbedrohungen abwehren, die geringfügige Aspekte ihrer Signaturen verändern, um herkömmliche IPS-Lösungen zu umgehen.

**RFC-Konformitätsprüfung** – vergleicht den Datenverkehr mit RFC-Standards für die Netzwerkkommunikation zwischen Hosts und zwischen Anwendungen und dem Netzwerk-Stack. Entspricht der Datenverkehr diesen Standards nicht, wird er von Proventia blockiert.

**Statistische Analyse** – erstellt über einen bestimmten Zeitraum Vergleichsdaten (eine „Baseline“) von Netzwerkaktivitäten und vergleicht dann konstant die aktuelle Aktivität mit der Baseline, um Abweichungen zu erkennen und zu verhindern. Proventia nutzt die statistische Analyse zur Abwehr von Angriffen, ohne den Datenaustausch im Netzwerk zum Erliegen zu bringen.

**TCP Reassembly** – stellt Netzwerkpakete neu zusammen und untersucht sie auf mögliche Sicherheitsrisiken.

**Flow Assembly** – analysiert die gesamte Netzwerkverbindung – nicht nur die einzelnen Pakete –, um schädlichen Datenverkehr zu blockieren, der möglicherweise in den Kommunikationsstrom eingeschleust wurde, um eine offene Verbindung auszunutzen. Flow Assembly ergänzt TCP Reassembly, da es den Datenverkehr auf einer höheren Ebene analysiert, um komplexe Sicherheitsbedrohungen abzuwehren.

### **Der Vorteil der Proventia Protection Engine – Mehrschichtiger Schutz durch Kombination unterschiedlicher Intrusion-Prevention-Technologien**

Die Protection Engine der Proventia IPS-Technologien ist das Ergebnis kontinuierlicher Forschung auf dem Gebiet von Schwachstellen und Angriffsmethoden. Da ständig neue Sicherheitsbedrohungen entstehen und ältere Exploits nie wirklich ausgemerzt werden, verstärkt IBM ISS die Proventia Protection Engine laufend mit Technologien, die ganze Kategorien von neuen und alten Sicherheitsrisiken bekämpfen.

### **Weitere Informationen**

Wenn Sie mehr über die Proventia IPS-Technologien und präventiven Schutz erfahren möchten, besuchen Sie

**[ibm.com/services/de/iss](https://ibm.com/services/de/iss)**



IBM Deutschland GmbH  
Pascalstrasse 100  
70569 Stuttgart  
**ibm.com/de**

IBM Österreich  
Obere Donaustrasse 95  
1020 Wien  
**ibm.com/at**

IBM Schweiz  
Vulkanstrasse 106  
8010 Zürich  
**ibm.com/ch**

Die IBM Homepage finden Sie unter:

**ibm.com**

IBM, das IBM Logo, ibm.com, Proventia und X-Force sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Weitere Unternehmens-, Produkt- oder Service-namen können Marken anderer Hersteller sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2009  
Alle Rechte vorbehalten.