

# **Avira SPACE**

- Spam- und Phishingschutz -

Eine Sicherheitsoption für iQ.Suite Wall



## Inhalt

1	Einführung .....	2
2	Avira SPACE – Methoden und Techniken im Detail .....	2
2.1	SPAM-Erkennung.....	2
2.1.1	Fortgeschrittene Text-Analyse .....	2
2.1.2	Analyse bekannter Wörter .....	2
2.1.3	Bayesscher Filter .....	2
2.1.4	Echtzeit-Blacklist .....	3
2.2	Phishing-Erkennung .....	3
2.2.1	Statistische Methoden .....	3
2.2.2	Dynamische Methoden .....	3
3	Über Avira.....	4
4	Über GROUP Business Software .....	5

## 1 Einführung

Avira SPACE (Spam and Phishing Advanced Cross platform Engine) ist eine Erweiterung für die Spamschutz-Lösung iQ.Suite Wall zur Erkennung und Vermeidung von Spam- und Phishing-Mails. Die Spamschutz-Option ist sowohl für die iQ.Suite unter Lotus Notes Domino als auch Microsoft Exchange einsetzbar.

Avira SPACE nutzt verschiedene Methoden und Technologien, um den höchstmöglichen Schutz gegen Spam- und Phishing-Mails zu erreichen:

- Fortgeschrittene Text-Analyse zur Suche nach Mustern, welche häufig in Spam- oder Phishing-Mails auftauchen
- Analyse bekannter Wörter und Erkennung verschleierter Begriffe
- Bayesscher Filter zur Erkennung von Begriffen in Spam- oder Ham-Mails anhand statistischer Methoden
- Online-Abgleich von Spam-Domänen mit Echtzeit-Blacklist-Servern
- Spezielle Phishing-Engine zur Erkennung von Phishing-Mails mittels statistischer und dynamischer Methoden

## 2 Avira SPACE – Methoden und Techniken im Detail

### 2.1 SPAM-Erkennung

#### 2.1.1 Fortgeschrittene Text-Analyse

Die fortgeschrittene Text-Analyse sucht unter den empfangenen E-Mails nach unüblichen Abweichungen, welche normalerweise in Spam-Mails zu finden sind. Diese Anomalien sind Anzeichen dafür, dass versucht wird, den Spamschutz zu umgehen oder den Ursprung der E-Mail zu verbergen. Die Technologie enthält ebenfalls ausführliche Tests, um mögliche Phishing-E-Mails zu entdecken.

#### 2.1.2 Analyse bekannter Wörter

Der Text der E-Mail wird nach verschiedenen verschleierte Inhalten (z.B. Leerzeichen oder Sonderzeichen zwischen Buchstaben) mit Hilfe von regulären Ausdrücken durchsucht. Wenn die E-Mail text/html und text/plain Inhalte enthält, prüft SPACE ob diese identisch zueinander sind oder nicht (sie sollten identisch sein).

#### 2.1.3 Bayesscher Filter

Der Bayessche Filter nutzt eine Kombination aus statistischen Methoden um mögliche Spam-Mails zu entdecken. Diese Technologie basiert auf der Erkenntnis, dass bestimmte Wörter in Spam- oder Ham-Mails gefunden wurden. SPACE ist standardmäßig in der Lage, Spam-, Phishing-Mails sowie Malware zu erkennen.

Wenn andere Methoden eine E-Mail sicher als SPAM oder HAM erkannt haben, lernt sich SPACE unter Nutzung des Bayesschen Filters selbst weiter an. Als Resultat verbessert sich kontinuierlich die Erkennungsrate des Filters – ganz ohne Interaktion des Anwenders.

#### **2.1.4 Echtzeit-Blacklist**

Jede E-Mail enthält die IP-Adresse des Mail-Servers, von dem sie abgeschickt wurde. Avira SPACE nutzt diese IP-Adresse und gleicht sie mit verschiedenen Blacklist-Servern im Internet ab. Wenn diese Domains als bekannte SPAM-IPs gelistet sind, bekommen sie zusätzliche Spam-Punkte zugewiesen.

### **2.2 Phishing-Erkennung**

#### **2.2.1 Statistische Methoden**

Diese Methoden kombinieren verschiedene Verfahren, in denen entschieden wird, ob eine bestimmte E-Mail eine Phishing-Mail ist. Basis der Erkennung ist eine bekannte Domain oder der Name im Absender-Feld des E-Mail Headers.

Hier ein Beispiel: Wenn eine E-Mail vom Absender security@paypal.com eintrifft und einen gefälschten Link auf eine andere Domain oder einen verdächtigen Text (wie z.B. „Klicken Sie hier um Ihren Account zu aktivieren“) enthält, markiert die Lösung die E-Mail als mögliche Phishing-Mail.

#### **2.2.2 Dynamische Methoden**

Die zwei folgenden Methoden nutzen dieselben Daten um eine Entscheidung zu treffen, jedoch mit zwei unterschiedlichen Algorithmen. Avira SPACE analysiert die E-Mail und extrahiert bestimmte Informationen, um ein charakteristisches Profil der Nachricht zu erstellen. Derzeit werden mehr als 40 Elemente berücksichtigt. Diese Informationen werden benötigt, um zu entscheiden, ob eine E-Mail vertrauenswürdig ist oder nicht. Im Hintergrund erfolgt dabei die eigentliche Analyse: der Algorithmus verwendet die Informationen über die charakteristischen Elemente und lernt, diese auf eine neue Art zu kombinieren, um Spam-Mails zu erkennen.

##### *Entscheidungsbaum*

Der Entscheidungsbaum (eine Methode aus der Stochastik und Entscheidungstheorie) ist in der Lage, eine Klassifizierung des Erkennungsvektors in 4 verschiedene Kategorien vorzunehmen: normal, echte Mail, mögliche Phishing-Mail und definitive Phishing-Mail.

##### *Phishing-Punkte*

Diese Methode nutzt eine Punktemethode und addiert Phishing-Punkte zu einer Gesamtpunktzahl, abhängig vom Erkennungsvektor. Wenn die Summe der Phishing-Punkte eine bestimmte Grenze überschreitet, wird die Mail als Phishing-Mail markiert.

### 3 Über Avira

Avira ist ein weltweit führender Hersteller von IT-Sicherheitslösungen für den professionellen und privaten Gebrauch. Das Unternehmen gehört mit mehr als zwanzigjähriger Erfahrung zu den Pionieren in diesem Bereich. Als Gründungsmitglied des Vereins „IT Security made in Germany“ (ITSMIG e.V.) garantiert Avira, ausschließlich IT-Sicherheitsprodukte ohne die Möglichkeit zur Datenspionage anzubieten.

Der deutsche IT-Sicherheitsexperte hat seinen Hauptsitz in Tettng am Bodensee und unterhält weltweit mehrere Unternehmensstandorte. Avira beschäftigt rund 300 Personen und leistet bei Millionen von Privatanwendern mit dem kostenlosen Virenschutz Avira AntiVir Personal einen signifikanten Sicherheitsbeitrag.

Zu den nationalen und internationalen Kunden zählen neben namhaften börsennotierten Unternehmen auch viele kleine und mittelständische Betriebe sowie Bildungseinrichtungen und öffentliche Auftraggeber. Neben dem Schutz der virtuellen Umgebung kümmert sich Avira durch Fördern der Auerbach Stiftung um mehr Sicherheit in der realen Welt. Die Auerbach Stiftung des Firmengründers unterstützt gemeinnützige und soziale Vorhaben sowie Kunst, Kultur und Wissenschaft.

## 4 Über GROUP Business Software

GROUP Business Software ist der führende Anbieter von IBM Lotus-basierten Lösungen und Dienstleistungen in den Bereichen E-Mail-Management und -Archivierung, Cloud Computing, CRM, Corporate Compliance und Administration. Die GROUP-Geschäftsbereiche bieten weltweit "Collaborative Business Solutions", welche Unternehmen und Anwender in ihrer täglichen Arbeit unterstützen und Geschäftsprozesse vereinfachen helfen.

Während Wettbewerber im Markt nur einen Ausschnitt der Anforderungen heutiger „Collaborative Business Solutions“ abdecken, bietet der GROUP-Konzern umfassende aufeinander abgestimmte Lösungen, die alle Bereiche der Zusammenarbeit erfassen. Durch Integration von GROUP-Technologien in die Geschäftsprozesse erreichen Organisationen und Unternehmen ihre Ziele leichter, schneller und effizienter.

### Kompetenzen

**Zentral:** GROUP-Lösungen machen die Verwaltung und Steuerung geschäftskritischer Prozesse an zentraler Stelle möglich und entlasten sowohl die Administration als auch Endanwender in Ihrer täglichen Arbeit. Die unternehmensweite Einbeziehung der Aktivitäten aller Nutzer geschieht serverseitig und kann auf diese Weise über eine zentrale Oberfläche gesteuert werden.

**Unkompliziert:** GROUP-Lösungen zeichnen sich durch eine hohe Benutzerfreundlichkeit und einzigartige Effizienz aus. Die serverbasierten Lösungen reduzieren Aufwand und Interaktion seitens der Anwender auf ein absolutes Minimum. Gleichzeitig tragen intelligente Automatismen zur Steigerung der Produktivität und Wirtschaftlichkeit bei.

**Konform:** Zentral definierte Prozesse gewährleisten die Einhaltung von unternehmenseigenen Policies und gesetzlichen Vorgaben. Intuitive Konfigurationsmöglichkeiten erlauben es, die eingesetzten Lösungen flexibel an die Anforderungen des Marktes, des Unternehmens oder neuer Gesetze anzupassen.

### Kunden

Die GROUP Business Software AG ist in Europa und den USA vertreten. Weltweit vertrauen Unternehmen die Sicherheit, Organisation und Effizienz ihrer Systeme den Lösungen des GROUP-Konzerns an. Zu den Kunden des Konzerns zählen neben mehr als drei Viertel der Sparkassen und Volksbanken in Deutschland weltweit namhafte Unternehmen, wie die Deutsche Bank, Ernst & Young, Honda, Heineken, Allianz und Miele.

Weitere Informationen und [www.gbs.com](http://www.gbs.com)

© 2010 GROUP Business Software AG

Die Produktbeschreibungen haben lediglich allgemeinen und beschreibenden Charakter. Sie verstehen sich weder als Zusicherung bestimmter Eigenschaften noch als Gewährleistungs- oder Garantieerklärung. Spezifikationen und Design unserer Produkte können ohne vorherige Bekanntgabe jederzeit geändert werden, insbesondere, um dem technischen Fortschritt Rechnung zu tragen. Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der GROUP Business Software AG zum Zeitpunkt der Veröffentlichung dar. Da GROUP Business Software AG auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens der GROUP Business Software AG dar und GROUP kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren. Dieses Dokument dient nur zu Informationszwecken. Die GROUP Business Software AG schließt für dieses Dokument jede Gewährleistung aus, sei sie ausdrücklich oder konkludent. Dies umfasst auch Qualität, Ausführung, Handelsüblichkeit oder Eignung für einen bestimmten Zweck. Alle in diesem Dokument aufgeführten Produkt- oder Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

#### European Headquarters

##### **GROUP Business Software AG**

MesseTurm  
60308 Frankfurt / Germany  
Phone: +49 69 789 8819-0  
Fax: +49 69 789 8819-99

#### North American Headquarters

##### **GROUP Business Software Corporation**

40 Wall Street, 33rd Floor  
New York, NY 10005 / USA  
Phone: +1 212 995-2900  
Fax: +1 212 995-2206

#### Email Main Office

##### **GROUP Business Software AG**

Ottostrasse 4  
76227 Karlsruhe / Germany  
Phone: +49 721 4901-0  
Fax: +49 721 4901-199

#### UK Office

##### **GROUP Business Software (UK) Ltd.**

3 More London Riverside  
London SE1 2RE / UK  
Phone: +44 207 206 0001

[info@de.gbs.com](mailto:info@de.gbs.com)  
[www.gbs.com](http://www.gbs.com)

 GROUP