iQ.Suite Watchdog

- Zentraler Virenschutz -

Intelligenter serverbasierter Virenschutz und Datei-Blocking durch Fingerprint-Technologie

Expertise matters

Inhalt

1 Zusammenfassung

Ausgelöst durch die in den vergangenen Jahren stattgefundenen weltweiten Virenattacken in immer neuen Varianten ist die Bedrohung bestehender Computersysteme durch Dateiviren, Trojaner und E-Mail-Würmer allgemein gegenwärtig. Die aufgrund von Viren nicht zur Verfügung stehenden Mail-Server, Netzwerke und Clients verursachen immense Kosten und können nicht zuletzt erhebliche Imageschäden für das jeweilige Unternehmen zur Folge haben.

Dieses Whitepaper zeigt, wie sich Unternehmen umfassend und zuverlässig vor den Gefahren durch bekannte und neu im Umlauf befindliche Viren schützen können.

2 Einführung

E-Mail und Messaging sind mittlerweile das wichtigste Kommunikationswerkzeug der Unternehmenswelt. Viele Geschäftsprozesse werden ganz oder teilweise mit Hilfe elektronischer Post abgewickelt und ein Ende des E-Mail-Booms ist nicht in Sicht.

Bei den per E-Mail abgewickelten Geschäftsprozessen sind zunächst vier Bereiche zu unterscheiden:

Anbahnung:

- Herstellung des ersten Kundenkontaktes
- Direkt E-Mail-Marketing
- Kontaktaufnahme zu Lieferanten

Verhandlung:

- Austausch der Anforderungen, Produktinformationen, Preise, etc.

Kundenbindung:

- Aktuelle Information über Produkte, Dienstleistungen, etc.
- Supportleistungen

Unternehmensinterne Prozesse:

- Workflows wie z.B. Urlaubsantrag, Beschaffung, Neue Mitarbeiter, etc.

Für alle Bereiche gilt: Die Verfügbarkeit der Kommunikationsinfrastruktur ist von existenzieller Bedeutung. Viele Unternehmensbereiche arbeiten so intensiv mit dem Medium E-Mail, dass ein Ausfall des Mailsystems einen völligen Arbeitsstopp zur Folge hat, was immense zusätzliche Kosten verursacht.

Eine der Hauptursachen für den Ausfall von E-Mail-Systemen sind dabei Computerviren.

3 Computerviren

Ein Computervirus ist ein Schadprogramm (Malware), das in der Lage ist, Kopien von sich selbst zu erzeugen und so andere Programme infizieren kann. Wie bei „echten“ Viren gibt es auch auf dem Computer eine Inkubationszeit. Bei Erreichen oder Durchführung eines bestimmten Ereignisses wird das Virus aktiv. Dabei führt das Virenprogramm die, sehr häufig Schaden verursachenden, Anweisungen des Programms aus.

3.1 Arten von Viren

3.1.1 Dateiviren

Die so genannten Dateiviren hängen sich vorwiegend an .COM- und .EXE-Dateien an. Die Infektion erfolgt beim Laden der Dateien, also durch Aufruf des Programms. Bei den Bootsektorviren wird der Bootsektor (dort liegt das Programm, welches das Laden des Betriebssystems veranlasst) innerhalb der Datenträger befallen. Die Übertragung geschieht durch infizierte Disketten, weshalb die Verbreitung dieser Viren Wochen und Monate dauert. Dateiviren waren bis in die 90er Jahre hinein die vorherrschenden Vertreter der Gattung Computervirus.

3.1.2 Makroviren

Seit Anfang der 90er Jahre existieren die Makroviren. Einer der Gründe für die regelrechte Schwemme von Makroviren, die bis zur Jahrtausendwende eine sehr verbreitete Form der Viren darstellten, ist die Tatsache, dass die Herstellung von Makroviren vergleichsweise einfach ist. In jedes der weit verbreiteten Office-Pakete ist heute eine Programmiersprache integriert. Mit Hilfe dieser Programmiersprache (hauptsächlich Visual BASIC for Applications – VBA) lassen sich Makroviren erstellen und beispielsweise in Word- oder Excel-Dokumente integrieren. Einmal per E-Mail verteilt, verbreiten sich diese Viren innerhalb von Minuten weltweit. Allerdings sind Makroviren weltweit stark rückläufig.

3.1.3 Trojaner

Ein Trojaner (von „Trojanisches Pferd“) ist ein nach außen hin harmlos erscheinendes Programm, das aber im Hintergrund eine Schadensroutine abarbeitet. Ein Beispiel dafür ist ein Programm, das einen LoginPrompt anzeigt, worauf der nichts ahnende Benutzer Username und Passwort eingibt; der Trojaner schickt dieses per E-Mail anderswohin, gibt “Login incorrect“ aus und übergibt an das reguläre Login. Trojaner kopieren sich nicht selbst und verbreiten sich daher nicht so schnell wie Viren. In der heutzutage häufigen Kombination mit Viren sind Trojaner jedoch sehr gefährlich, da Viren Trojaner herunterladen können, die Tastaturfolgen speichern oder Daten stehlen. Trojaner werden auch dazu benutzt, einen Computer mit einem Virus zu infizieren. Ein so genannter Backdoor-Trojaner

ermöglicht es einem Angreifer, sich mit dem befallenen Computer zu verbinden und ihn für seine eigenen Zwecke zu missbrauchen.

3.1.4 Skriptviren

Skriptviren, basierend auf Visual Basic Skript (VBS), verbreiten sich mit rasanter Geschwindigkeit. Diese seit einigen Jahren „in freier Wildbahn“ existierende Klasse von Viren hat sich innerhalb kürzester Zeit einen Spitzenplatz in der Virenhitliste gesichert.

Das bekannteste Beispiel dieser Klasse dürfte der Virus VBS/Loveletter (auch VBS/Love oder VBS/ILoveYou genannt) sein. Diese Viren sind extrem einfach zu programmieren und zu verbreiten. Sie lassen sich z.B. in E-Mail-Nachrichtentexte einfügen. In manchen E-Mail-Clients werden die schädlichen Skripte ausgeführt, sobald die E-Mail über eine Vorschau angesehen oder nur der Text gelesen wird.

3.1.5 Würmer

Ein Wurm ist ein Schadprogramm, das sich von Computer zu Computer via Netzwerk selbsttätig weiter verbreitet. Die „Absicht“ der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen. Würmer – einmal auf den Weg gebracht – vermehren sich selbsttätig, um sich rasend schnell innerhalb eines Firmennetzwerks oder über das Internet zu verbreiten. Internetwürmer nutzen Sicherheitslücken im Betriebssystem und „springen“ durch sie zwischen vernetzten Computern hin und her. Würmer können bei der Selbstverbreitung (sie kopieren sich selbst) ein hohes Maß an Internetverkehr erzeugen, so dass die Kommunikation verlangsamt wird oder Computer abstürzen. So benutzen sie beispielsweise die E-Mail-Funktionen eines Rechners, um sich an beliebige Internetadressen zu versenden. Neben ihrer Fähigkeit zur schnellen autonomen Verbreitung haben Würmer eine Ladung, das eigentliche Schadprogramm, das sich wie ein herkömmlicher Virus innerhalb des befallenen PCs aktiviert. Würmer machen mittlerweile fast 100% der im Umlauf befindlichen Computerviren aus.

3.2 Kosten durch E-Mail-Attacken

Die Kosten durch Malware sind enorm. Mittlerweile hat praktisch jedes Unternehmen bereits eine Virusattacke erleiden müssen. Dabei sind direkte Schäden, die beispielsweise durch die Zerstörung von Daten entstehen, leichter einzuschätzen als Ausfälle, die durch die Behinderung der Unternehmenskommunikation entstehen.

Neben dem Verlust von Daten und der Nicht-Verfügbarkeit von PCs sind es vor allem die Kosten aufgrund Produktivitätsverlusts und von korrupten Dateien, welche die größten Schäden anrichten.

3.3 Auf welchem Weg gelangen Viren in Unternehmen?

Die heute aktuellen Wurmviren verbreiten sich zu fast 100% über E-Mail-Anhänge. Auf die Vorsicht der Mitarbeiter, einen E-Mail-Anhang nicht zu öffnen, kann man sich nicht verlassen, zumal die Viren in der Regel mit gefälschten Absendern in Umlauf gebracht werden.

4 Virenschutz = Virenschutz?

Die alarmierende Zunahme der Virenattacken hat dazu geführt, dass fast alle Unternehmen Antivirus-Produkte einsetzen. Vergleichen wir den Desktop-Virenschutz mit einem serverbasierten Virenschutz.

4.1 Desktop Antivirenschutz

4.1.1 Unzureichender Schutz

Noch immer setzen viele Unternehmen Antivirus Produkte auf den PCs der Mitarbeiter ein. Die Schutzwirkung für Viren, die über Disketten verteilt werden, ist hier recht hoch. Wir haben jedoch gesehen, dass heute fast 100% aller Computerviren per E-Mail verteilt werden.

Bei den durch E-Mail verbreiteten Viren stellt der Benutzer-PC das letzte Glied in der Kette dar und ist insbesondere bei Skriptviren auch das am meisten gefährdete Glied, da diese Viren in aller Regel Features des E-Mail-Clients verwenden, um ihre Schadfunktionen auszuführen. Der clientbasierte Virenscanner auf dem Benutzer-PC schützt hier nur unzureichend oder gar nicht.

4.1.2 Aufwand für Softwarepflege

Nur ständig aktualisierte Antivirus-Software bietet Schutz vor neuen Virenattacken. Aufgrund ständig neuer Viren verkürzen sich die Update-Intervalle für Programme und vor allem für die Antivirus-Muster ständig. Für Desktop-basierte Virenscanner heißt dies, dass jedes Update der Antivirus-Software auf allen PCs des Unternehmens verteilt werden muss. Auch wenn hier Login-gesteuerte Mechanismen genutzt werden, so ist eine zentrale Administration und Pflege nur schwer möglich, kontrollierbar und mit zusätzlichen Kosten und Aufwand verbunden.

4.1.3 Belastung der Infrastruktur

Gerade bei Virusattacken durch neu entdeckte Viren stellt die Softwareverteilung ein Problem dar.

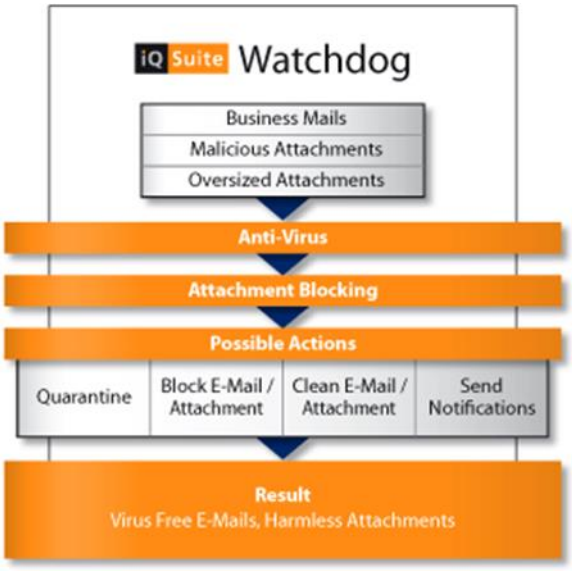
Massive Attacken belasten die Netzwerk-Infrastrukturen so sehr, dass trotz einer vorhandenen aktualisierten Virenmusterdatei eine Verteilung dieser Dateien auf alle Desktops nahezu unmöglich ist.

4.2 Unternehmensweiter serverbasierter Virenschutz

Ein serverbasierter Antivirusschutz mit iQ.Suite Watchdog bietet dem Unternehmen viele Vorteile.

4.2.1 Zentrale Administration

iQ.Suite Watchdog kann auf den bereits vorhandenen E-Mail-Servern genutzt werden. Die Anschaffung eines dedizierten Servers ist nicht erforderlich. Watchdog ist über eine einheitliche Benutzeroberfläche zentral administrierbar. Aufgrund der serverbasierten Arbeitsweise ist eine unternehmensweite Softwareverteilung auf Benutzer-PCs nicht erforderlich. Dementsprechend müssen auch keine aktualisierten Virenmusterdateien verteilt werden. Dadurch reduziert sich der Aufwand für Administration und Wartung erheblich. Darüber hinaus verbessert dies die Reaktionsgeschwindigkeit bei Virenattacken mit neuen Viren.



4.2.2 Erst schützen, dann speichern

iQ.Suite Watchdog prüft und reinigt E-Mails, bevor diese auf den E-Mail-Servern gespeichert werden können. Eine Infizierung des E-Mail-Servers ist dadurch von vornherein ausgeschlossen. Alle E-Mails kommen bereits virenfrei bei den Benutzern an.

4.2.3 Kostengünstiger Schutz

iQ.Suite Watchdog reduziert die Kosten für Implementierung und Management einer unternehmensweiten Virenschutzlösung. Die aufwändige Pflege clientbasierter Software ist nicht erforderlich.

4.2.4 Schutz von Datenbanken und Öffentlichen Ordnern

Nicht nur ein- und ausgehende E-Mails können Viren enthalten, sondern auch andere elektronische Dokumente. Diese Dokumente können ebenfalls auf IBM Notes/Domino und MS Exchange Servern abgelegt werden.

iQ.Suite Watchdog schützt nicht nur den E-Mail-Verkehr, sondern auch die Zugriffe auf IBM Notes/Domino Datenbanken und Öffentliche Ordner in Microsoft Exchange. Dies verbessert den Schutz der E-Mail- und Messaging-Infrastruktur erheblich.

4.2.5 Höchste Zuverlässigkeit durch gleichzeitigen Einsatz verschiedener Virenscanner

Bisherige Virenattacken haben immer wieder gezeigt, dass eingesetzte Virenscanner unterschiedliche Erkennungsraten besitzen und die Reaktionszeiten auf neue Viren variieren.

In iQ.Suite Watchdog sind verschiedene Virenscanner, wie z.B. von Avira oder Sophos, integrierbar. Zusätzlich unterstützt Watchdog alle gängigen Virenscanner der unterschiedlichsten Hersteller.

iQ.Suite Watchdog bietet außerdem die Möglichkeit, alle unterstützten Virenscanner parallel zu nutzen. Die Zuverlässigkeit des Virenschutzes wird hierdurch immens gesteigert.

4.2.6 Investitionsschutz

Die Partnerschaften mit den führenden Herstellern von Virenscannern ermöglichen iQ.Suite Watchdog Benutzern, die bereits im Unternehmen vorhandenen Virenscanner zu integrieren und die erweiterten Möglichkeiten von Watchdog zu nutzen. Sollte ein Unternehmen zukünftig weitere oder andere Virenscanner einsetzen wollen, können diese problemlos in Watchdog integriert werden.

4.2.7 Flexibilität

Die Verlagerung der Antivirusprüfung von den Clients auf den Server ermöglicht die Nutzung von regelbasierten Schutzmechanismen. „Regelbasiert“ bedeutet zunächst einmal, dass eine Anzahl von „Wenn-Dann“ Bedingungen definiert wird. Wobei sowohl das „Wenn“ mehrere Bedingungen enthalten kann, als auch das „Dann“ mehrere auszuführende Aktionen beinhalten darf.

Wenn...,	dann...
eine E-Mail an abc@xyz.com gesendet wird	prüfe nach Viren mit Virenscanner 1 und 2
eine E-Mail von *@test.com empfangen wird	prüfe nach Viren mit Virenscanner 3 und 4

4.2.8 Intelligente Dateianhangskontrolle

iQ.Suite Watchdog erkennt nicht nur Viren, Würmer, etc., sondern bietet auch die Möglichkeit, Einschränkungen für die Dateianhänge anhand unterschiedlichster Kriterien zu erstellen.

4.2.9 Einschränkungen anhand der Dateiendung

Ein Beispiel für eine Einschränkung anhand einer Dateiendung betrifft die Skriptviren (siehe Punkt 3.1.4 Skriptviren). Skriptviren sind in der Regel Visual Basic Skript (vbs) Dateien. Dateianhänge mit einer Endung wie z.B. vbs können mit iQ.Suite Watchdog anhand des Namens zuverlässig erkannt und geblockt werden.

4.2.10 Einschränkungen anhand von Fingerprints

Viele Dateitypen besitzen ein eindeutiges binäres Muster (genannt Fingerprint), anhand dessen die Identifikation eines Dateityps möglich ist.

Dieser Fingerprint ermöglicht es, auch dann den ursprünglichen Dateityp festzustellen, wenn eine Datei beispielsweise von „execute.exe“ in „execute.txt“ umbenannt wurde.

Watchdog erkennt eine Vielzahl von Dateitypen anhand eindeutiger Fingerprints, die dadurch geblockt werden können. Dieses Feature verbessert wesentlich die Sicherheit bei der Dateierkennung. Der Manipulation von Dateien wird damit ein Riegel vorgeschoben.

4.2.11 Einschränkungen anhand der Größe und Anzahl von Anhängen

E-Mail-Anhänge können auch dann zu einer Gefahr für die Infrastruktur werden, wenn diese auf Grund ihrer Anzahl oder Größe Netzwerkbandbreiten und Serverkapazitäten blockieren.

Mit iQ.Suite Watchdog ist es möglich, mit folgenden Einschränkungen E-Mails zu blocken:

- Anzahl der Anhänge pro E-Mail
- Maximale Größe eines Anhangs pro E-Mail
- Maximale Größe aller Anhänge pro E-Mail

4.2.12 Serverbasierte Inhaltsprüfung verschlüsselter E-Mails

Für eine umfassende, serverbasierte Sicherheit des E-Mail-Verkehrs ist Antivirenschutz allein nicht ausreichend. In vielen Unternehmen spielt beispielsweise auch die Verschlüsselung von E-Mails eine große Rolle. Hierbei ist folgendes zu beachten:

Clientbasierte Verschlüsselung verhindert umfassende E-Mail-Inhaltssicherheit

Der Grund: Eine verschlüsselte Mail kann von Antiviren-Programmen und anderen E-Mail-Sicherheitsprogrammen auf den Mail-Servern nicht geschützt werden, denn die gesamte Mail ist für diese Programme nicht lesbar, so dass alle Schutzmechanismen, die auf den Mail-Servern implementiert sind, nicht greifen. Dies ist eine prekäre Situation. Haben sich doch die meisten Unternehmen aus gutem Grund dazu entschlossen, E-Mail-Sicherheitsanwendungen zentral auf den Servern zu betreiben, da dadurch die Administration in vielerlei Hinsicht wesentlich erleichtert wird. Die clientbasierte Verschlüsselung widerspricht damit der Notwendigkeit, E-Mail-Infrastrukturen und die entsprechenden Sicherheitsmechanismen zentral und unternehmensweit einheitlich zu implementieren und zu administrieren.

Mit iQ.Suite Watchdog in Verbindung mit iQ.Suite Crypt Pro bietet sich die Möglichkeit, auch den verschlüsselten E-Mail-Verkehr auf Viren und unerwünschte Dateitypen zu untersuchen. Dies gilt sowohl für ein- als auch für ausgehende E-Mails.

5 Einsatzszenarien

5.1 Zuverlässiger Virenschutz

Nach erfolgreicher Implementierung einer E-Mail-Infrastruktur in einem Unternehmen wird die Kommunikation mit Kunden und Lieferanten mehr und mehr auf elektronischem Wege durchgeführt. Dabei zeigte sich, dass der aktuell genutzte Desktop-Virenscanner nicht für ausreichende Sicherheit sorgen konnte. Immer wieder gelangen Viren auf die Desktops und verursachen dort Schäden.

Um die E-Mail-Kommunikation umfassend zu schützen, werden nun geeignete Antivirus-Lösungen eruiert.

5.1.1 Anforderungen

1. Da sich die Pflege der clientbasierten Antiviruslösung als problematisch herausgestellt hat, ist eine serverbasierte Lösung erwünscht. Hierdurch sollen der Aufwand für die Verteilung und Pflege der Antivirussoftware reduziert werden.
2. Das Unternehmen möchte eine Antivirus-Lösung, die sie nicht von dem Hersteller eines Virenscanners abhängig macht. Daher muss das gewünschte Produkt mehrere Virenscanner unterstützen.
3. Die Vergangenheit hat gezeigt, dass ein Virenscanner nicht alle bekannten Viren erkennt, daher sollen mehrere Virenscanner parallel zum Einsatz kommen. Dies erhöht die Sicherheit und Zuverlässigkeit. Allerdings sollen nur Mails, die aus dem Internet empfangen werden, von mehreren Virenscannern geprüft werden, für den internen Mailverkehr wird nur ein Virenscanner verwendet.
4. Um sowohl ein- und ausgehende Mails als auch den internen Mailverkehr zu schützen, ist eine Lösung erforderlich, die auf allen E-Mail-Servern läuft.

5. Für einen umfassenden Schutz sollen nicht nur ein- und ausgehenden E-Mails nach Viren untersucht werden, sondern auch die auf den E-Mail-Servern genutzten Datenbanken. Zusätzlich zum Echtzeit-Schutz sollen einmal pro Nacht um 01:00 Uhr alle Datenbanken durchsucht werden.
6. Parallel zur Einführung des E-Mail-Virenschutzes ist die Implementierung einer serverbasierten Lösung für Verschlüsselung geplant.
7. Die Antiviruslösung muss sich also so in das gesamte E-Mail-Sicherheitskonzept integrieren lassen, dass auch verschlüsselte E-Mails serverbasiert geschützt werden können.

5.1.2 Lösungsansätze

1. Zunächst wird festgelegt, welche Virenscanner zum Einsatz kommen sollen.
2. Die gewünschten Virenscanner werden gemeinsam mit iQ.Suite Watchdog auf allen E-Mail-Servern des Unternehmens installiert.
3. Über das serverbasierte Regelwerk der iQ.Suite werden die erforderlichen Regeln für das Scannen von eingehenden, ausgehenden und internen Mails definiert.

Wenn...,	dann...
eine E-Mail vom Internet empfangen wird	durchsuche diese Mail mit Virenscanner A und Virenscanner B
eine E-Mail ins Internet gesendet wird	durchsuche diese Mail mit Virenscanner A
eine E-Mail vom Intranet empfangen wird	durchsuche diese Mail mit Virenscanner B
etc.	etc.

4. Der Schutz der gewünschten Datenbanken auf den E-Mail-Servern wird ebenfalls über das serverbasierte Regelwerk aktiviert.

Wenn...,	dann...
ein Objekt in die Datenbank geschrieben werden soll	durchsuche dieses Objekt mit Virenscanner A und Virenscanner B
die Uhrzeit 01:00 Uhr erreicht ist	durchsuche alle Datenbanken mit Virenscanner A

5. Die definierten Regeln werden automatisch auf alle gewünschten E-Mail-Server verteilt.
6. Um nun auch die serverbasierte Verschlüsselung zu gewährleisten, wird mit iQ.Suite Crypt Pro das Verschlüsselungsmodul implementiert.

5.2 Unterbinden unerwünschter Dateitypen

1. Mit der Einführung einer E-Mail-Infrastruktur und der Verlagerung der Kommunikation von Brief und Fax auf das Medium E-Mail wächst auch täglich das Mailvolumen. Eine Analyse hat gezeigt, dass vor allem die Anzahl der empfangenen und gesendeten Audiodateien wie beispielsweise MP3 und WMA, aber auch Video-Dateien rapide zugenommen haben. Diese Dateien belasten nicht nur die Netzwerkbandbreite, sondern auch die Ressourcen der E-Mail-Server.
2. Darüber hinaus kann man davon ausgehen, dass diese Dateien keine geschäftsrelevanten Informationen enthalten, also eher die Mitarbeiter von ihren eigentlichen Aufgaben abhalten.
3. Um Infrastrukturressourcen zu schonen, sollen auch übergroße Mails nur in Teilbereichen des Unternehmens gesendet und/oder empfangen werden können.
4. Daher hat sich die Geschäftsleitung entschlossen, eine Lösung zu implementieren, die für diese Probleme Abhilfe schafft.

5.2.1 Anforderungen

1. Die Dateitypen, die von der Geschäftsleitung als unerwünscht definiert werden, sollen geblockt werden können.
2. Die unerwünschten Dateitypen sollen unterschiedlich behandelt werden können. D.h., ein Teil der Dateien soll zentral in eine Quarantäne gestellt werden können, andere Dateien sollen sofort gelöscht werden können.
3. Für bestimmte Abteilungen im Unternehmen soll es weiterhin möglich sein, Bilddateien erhalten und versenden zu können.
4. Mails ab einer bestimmten Größe sollen geblockt werden können. Hierfür soll es für eingehende/ausgehende und interne Mails unterschiedliche Grenzen geben können.
5. Um die Verbreitung von Skriptviren zu verhindern, sollen Visual Basic-Skript- und Javaskript-Dateien geblockt werden.
6. Das Unternehmen möchte eine höchstmögliche Sicherheit gewährleisten. Daher muss das gewünschte Produkt die ursprünglichen Dateitypen auch dann erkennen können, wenn ein Dateityp umbenannt wurde. D.h., eine „abc.VBS“ Datei muss auch dann erkannt werden, wenn diese in „abc.TXT“ umbenannt wurde.
7. Die Lösung muss Möglichkeiten bieten, über ein zentrales Regelwerk schnell und einfach Veränderungen in den Sicherheitsrichtlinien vornehmen zu können.

5.2.2 Lösungsansätze

1. Definition der unerwünschten Dateitypen:
   a. .AVI, .MPG,.MP3,.WMA, WAV, .GIF, .JPG, .BMP, .TIF, sollen generell geblockt werden
2. Definition der gewünschten Aktionen:
   a. .TIF, .AVI, .MPG, .MP3, .WMA, .WAV werden sofort gelöscht .GIF, .JPG, .BMP werden in Quarantäne gestellt
3. Abteilung Marketing darf weiterhin .GIF, .JPG, .BMP und. TIF senden und empfangen
4. Maximale Größe eingehender Anhänge 4 MB
5. Maximale Größe ausgehender Anhänge 2 MB
6. Maximale Größe im internen Mailverkehr 10 MB
7. .VBS und .JS Dateien werden geblockt
8. Installation von iQ.Suite Watchdog auf den E-Mail-Servern
9. Einrichtung des Regelwerks

Regelwerk:

Wenn...,	dann...
eine E-Mail Anhänge vom Typ GIF, .JPG, .BMP beinhaltet	Betroffene Anhänge aus Mail löschen und Dateien auf E-Mail-Server in Quarantäne stellen. Benachrichtigung an Sender/Empfänger und Administrator
eine E-Mail Anhänge vom Typ .TIF, .AVI, .MPG, .MP3, .WMA, .WAV beinhaltet	Betroffene Anhänge aus Mail löschen und Benachrichtigung an Sender/Empfänger und Administrator
eine E-Mail Anhänge vom Typ GIF, .JPG, .BMP,.TIF beinhaltet und von oder an Abteilung Marketing gesendet wird	Benachrichtigung an Datenschutzbeauftragten
Eingehender Anhang aus Internet > 4 MB	Anhang in Quarantäne stellen
Ausgehender Anhang ins Internet > 2 MB	Anhang in Quarantäne stellen, Benachrichtigung an Absender
Eingehender Anhang aus Intranet > 10 MB	Anhang in Quarantäne stellen
Ausgehender Anhang ins Intranet > 10 MB	Anhang in Quarantäne stellen, Benachrichtigung an Absender
Anhang mit Typ .JS oder .VBS	Anhang in Quarantäne stellen, Administrator benachrichtigen

6 iQ.Suite Watchdog auf einen Blick

Highlights

- Integrierbare Virenscanner
- Effiziente E-Mail- und Datenbankprüfung

  Alle eingehenden, ausgehenden und internen E-Mails sowie alle Datenbanken werden gezielt auf Viren überprüft und in Echtzeit bearbeitet.
- Intelligente Anhangkontrolle

  Dateimusterprüfung und -sperrung verhindern das Eindringen und Versenden von Nachrichten mit manipulierten, unerwünschten oder bösartigen Dateianhängen.
- Flexibles Regelwerk

  Durch den Einsatz eines intelligenten, frei definierbaren Regelwerks zur gezielten Prüfung von E-Mails und Applikationsdatenbanken bietet iQ.Suite Watchdog höchste Flexibilität und Sicherheit. Aktuelle Regelsätze gehören bereits zum Lieferumfang.
- Maximaler Virenschutz

  Die gleichzeitige Verwendung von Virenscannern und Packern verschiedener Hersteller bietet maximalen Schutz auch vor neuesten oder rekursiv verpackten Viren.
- Integrierte und zentrale Administration

  Die vollständige Integration in die Server-Plattform garantiert einfache Administration.

Features

- Sichere Dateimusterprüfung und –sperrung anhand von Größe und Typ, erkennt und blockt auch manipulierte Dateien
- Konfigurierbare Regeln für alle Prüf- und Schutzfunktionen
- Rekursive Virenprüfung aller E-Mails und Dateianhänge in Echtzeit, ereignis- und zeitgesteuert
- Vollständige Unterstützung von Mail.box (IBM Domino) und Storage Groups und Multiplen Datenbanken (Microsoft Exchange)
- Rekursive Prüfung der Datenbanken in Echtzeit, ereignis- und zeitgesteuert
- Vollständige Prüfung auf manipulierte Notes-Designelemente/Outlook Elemente in E-Mails und Datenbanken
- Automatische Erkennung von neuen Postfächern und Applikationsdatenbanken bzw. Öffentlichen Ordnern
- Gleichzeitige Verwendung von Virenscannern und Packern verschiedener Hersteller
- Unterstützung automatischer Updates für Virensignaturen, Regelsätze und Dateimuster
- Detaillierte Protokollfunktionen und Statistik
- Konfigurierbare Meldungen an Absender, Empfänger und Administrator
- Optimiertes Multiprozessing und Multithreading auch für Partitioned Server und Cluster (IBM Domino)
- Skalierbare Architektur
- Einfache Erweiterung mit weiteren iQ.Suite Produkten

Über GBS

GROUP Business Software ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die IBM und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Weitere Informationen unter www.gbs.com