

MIMESweeper™ for Exchange

Preisgekrönte Policy-basierte Content Security-Lösung für interne Email

Interne Email hat sich vom einfachen Nachrichtensystem zur zentralen Plattform für die schnelle und systematische Verteilung von Dokumenten und Dateien innerhalb des Unternehmens entwickelt. Parallel zur internen Email ist jedoch auch die Anfälligkeit der Unternehmen für eine Vielzahl unterschiedlicher Gefahren gestiegen. Die absichtliche oder zufällige Verbreitung ungeeigneter Inhalte und Dateianhänge per Email innerhalb des Unternehmens ist eine ernstzunehmende Gefahr. Die Studie „2004 Information Security Breaches Survey“ des britischen Department of Trade and Industry (Industrie- und Handelskammer) hat gezeigt, dass etwa ein Drittel aller Sicherheitsprobleme ihren Ursprung im Unternehmen haben.

MIMESweeper for Exchange

Mit MIMESweeper for Exchange können sich Unternehmen gegen digitale Gefahren der internen Email-Kommunikation umfassend schützen. Die gleichen Gefahren, die am SMTP-Gateway an der Grenze zum Unternehmen abgewehrt werden können (z.B. Virenbefall, Konfrontation mit oder Verbreitung von Nachrichten mit anstößigen Formulierungen oder anderen ungeeigneten Inhalten, Preisgabe vertraulicher Informationen, Verlust von Netzwerkbandbreite und Speicherplatz), können auch innerhalb des Unternehmens entstehen, wenn Mitarbeiter Witze, MP3-Dateien oder diskriminierende Nachrichten versenden. Ein anderes Risiko ist die Übertragung von Viren auf Unternehmenssysteme durch mitgebrachte Datenträger oder die Notebooks der Mitarbeiter. Diese Gefahren können von MIMESweeper for Exchange auch innerhalb des Unternehmens ohne Ausnahme erkannt und gelöscht werden.

MIMESweeper for Exchange besteht aus den folgenden Komponenten:

- Preisgekrönte MIMESweeper Content-Analyse-Technologie
- Report Center (Web-basiert)
- REMOTEmanager
- Personal Message Manager (PMM)
- Spam-Filterlösung

Die Gefahr kommt von innen: Überwachung des Gateway reicht nicht

Obwohl viele Gefahren außerhalb der Unternehmensnetzwerke entstehen, kann eine am SMTP-Gateway installierte Sicherheitslösung Netzwerk und Geschäftsprozesse nicht vor Risiken schützen, die innerhalb des Unternehmens entstehen, zum Beispiel Haftungsrisiken durch falsches Benutzerverhalten oder Sabotageakte.

Zudem müssen Unternehmen damit rechnen, dass Viren oder illegale bzw. unerwünschte Inhalte am Gateway vorbei in das Netzwerk gelangen – zum Beispiel über Web-basierte Email oder mobile Speichermedien und Rechner, die zeitweise außerhalb des Unternehmens benutzt werden – und dann über das interne Email-System an andere Benutzer verteilt werden.

Eine andere Gefahr ist die in vielen Unternehmen geplante oder bereits vollzogene Einführung eines Web-basierten Zugangs zu Outlook.

Die Kernpunkte:

Sabotage: Viren, Trojaner, Würmer und andere bösartige Programme können auch durch interne Emails verbreitet werden. Da der Großteil der internen Nachrichten in Unternehmen heute in elektronischer Form übertragen wird, ist gleichzeitig die Gefahr für Angriffe auf diese Daten gestiegen.

Produktivitätsverlust: Durch die Entwicklung von Email zum bevorzugten Kommunikationsmittel der Geschäftswelt ist das Gesamtaufkommen von Email exponentiell gestiegen. Im Durchschnitt werden an Empfänger innerhalb des Unternehmens acht Mal mehr Emails versendet als an externe Empfänger. Daraus folgt nicht nur ein erhöhter Zeitaufwand für das Sortieren des Nachrichteneingangs, sondern auch der Missbrauch interner Emails für das Versenden von Witzen und anderen geschäftlich nicht relevanten Inhalten.

Hohe IT-Kosten: Vor dem Hintergrund einer verschärften Kostenkontrolle ist es zwingend notwendig, den Anstieg der IT-Kosten durch ausufernden Email-Gebrauch zu verhindern. Ohne Filter- und Analysefunktionalität kann das Unternehmen nicht sicherstellen, dass die großen Datenmengen, die im Netzwerk bewegt werden, für die Geschäftsprozesse notwendig und nützlich sind.

Haftungsrisiken: Für das Unternehmen beinhaltet die Verbreitung anstößiger oder unerwünschter Inhalte, urheberrechtlich geschützter Dateien und vertraulicher Unternehmensinformationen durch Mitarbeiter das Risiko der rechtlichen Haftung und des Imageverlusts. Denn öffentlich geführte Prozesse können eine irreparable Rufschädigung für das Unternehmen sein.

Gesetzeskonformität: Unternehmen müssen ihre internen Abläufe immer wieder an neue Gesetze und Bestimmungen anpassen. Da die Unternehmen heute zunehmend dafür verantwortlich sind, wie Informationen gespeichert, verwendet und verteilt werden, ist eine sachgemäße Verwaltung und Kontrolle der Daten eine Grundvoraussetzung.

Produkt-Highlights:

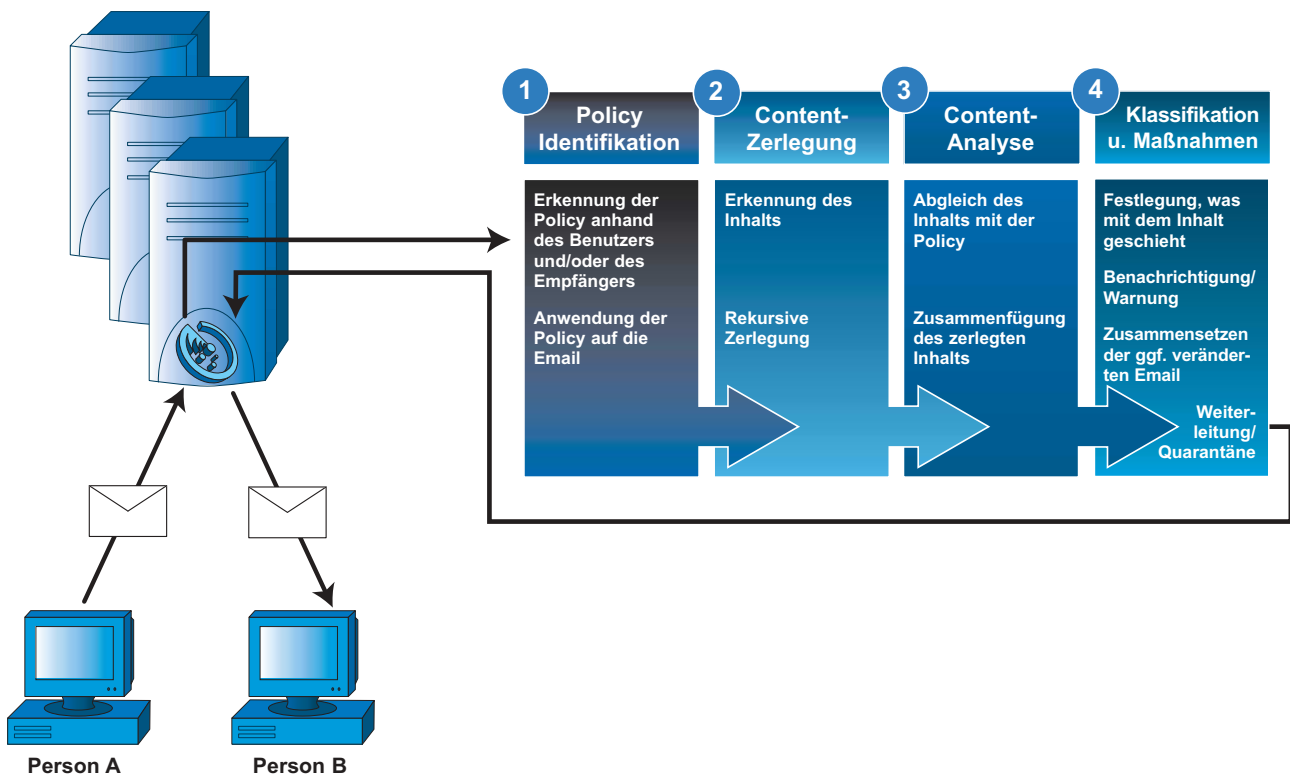
- Weltweite #1 für Email Content Security
- Verhindert die Verbreitung digitaler Gefahren per interner Email
- Verhindert die Verbreitung von Viren und unangemessenen Inhalten
- Web-basiertes Report Center ermöglicht unternehmensweiten Zugriff
- REMOTEmanager für flexible Systemadministration

Auch hier sind interne Email-Systeme offen für Gefahren, weil ein- und ausgehende Daten keinerlei Berührung mit der SMTP-Überwachung haben.

Auch die vorsätzliche oder versehentliche Weitergabe von vertraulichen Informationen aus Personal-, Vertriebs-, Rechts- oder Entwicklungsabteilungen an unberechtigte Benutzer birgt Gefahren, die insbesondere aufgrund neuer Gesetze (wie dem europäischen Datenschutzgesetz) berücksichtigt werden müssen. Die veränderte Rechtslage zwingt Unternehmen dazu, die Einhaltung entsprechender Richtlinien umfassend zu überwachen, damit sensible Daten weder absichtlich noch unabsichtlich per Email an unautorisierte Mitarbeiter verschickt werden. So ist zum Beispiel im Personalsektor die Übermittlung von persönlichen Daten aus Personalakten, wie zum Beispiel Gehaltseinstufungen oder Informationen über Disziplinarmaßnahmen (Abmahnungen etc.), an unbefugte Personen untersagt.

Wie es funktioniert

Das Exchange-Intercept-Modul fängt alle an den Exchange Server gerichteten Emails ab und leitet sie zur Prüfung an MIMESweeper weiter.

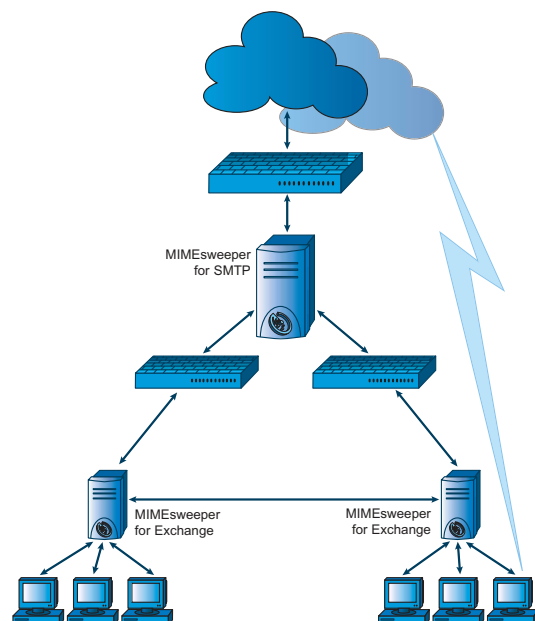


Flexible Implementierung

MIMESweeper for Exchange kann auf zahlreichen verschiedenen Systemarchitekturen und zusammen mit anderen MIMESweeper-Produkten eingesetzt werden. Die Art der Implementierung hängt von der Größe und Komplexität der jeweiligen internen Email-Infrastruktur ab.

Der Einsatz von MIMESweeper for Exchange auf mehreren Microsoft-Exchange-Servern verhindert die Verbreitung von Gefahren zwischen Anwendern innerhalb einer Organisation. MIMESweeper for SMTP als Bestandteil einer Sicherheitslösung für externe Gefahren schützt vor Bedrohungen wie Spam und externen Denial-of-Service-Attacken und verhindert dadurch, dass interne Netzwerkkressourcen durch unangemessene Inhalte von außen beeinträchtigt werden.

In Unternehmen mit verschiedenen Niederlassungen kann MIMESweeper for Exchange so eingerichtet werden, dass jede einzelne Niederlassung eine eigene Sicherheitsrichtlinie für die interne Kommunikation definiert oder regionale Variationen der Unternehmensrichtlinien implementiert.



Umfassende Sicherheit

MIMESweeper for Exchange liefert Antworten auf drängende Sicherheitsfragen. Diese Lösung kombiniert die technologische Überlegenheit der Clearswift MIMESweeper Content-Analyse mit leistungsstarken Managementfunktionen und schützt Unternehmen zuverlässig gegen unterschiedlichste digitale Bedrohungen – heute und in Zukunft. Zusätzlich lässt sich der Email-Server mit einem wesentlich geringeren Aufwand an Zeit und Ressourcen verwalten.

MIMESweeper for Exchange ermöglicht die Implementierung von Content-Sicherheitsrichtlinien (Policies) für Microsoft-Exchange-Server 2000/2003. Alle an den Exchange-Server gerichteten Nachrichten werden abgefangen, geprüft und nach den Richtlinien des Unternehmens bearbeitet. Diese Funktionen werden beim Austausch von Nachrichten der lokalen Benutzer über den Exchange-Server auf eingehende und ausgehende Nachrichten angewendet.

Content Security Total

Angesichts der anhaltenden Zunahme der Email- und Internetnutzung müssen Unternehmen heute lückenlose Sicherheitsrichtlinien implementieren. Fehler oder Störungen können verheerende Verluste nach sich ziehen. Die Mehrzahl der Unternehmen hat die Notwendigkeit der Nutzung von Sicherheitstechnologien erkannt und mit der Implementierung von Sicherheitstools für alle Gateways und Protokolle begonnen, die auf verschiedenen Ebenen ansetzen und einander ergänzen. Die einzelnen Komponenten sollten jedoch in ein mehrstufiges Sicherheitsmodell integriert werden, damit eine umfassende Sicherheit gewährleistet wird.

Die Sicherheitsstrategie von Clearswift sieht die Einrichtung eines mindestens drei Ebenen umfassenden Abwehrsystems am SMTP-Gateway vor, damit alle Arten digitaler Gefahren erfasst werden:

Eingangsebene

- **Firewall** – regelt den Datenverkehr, um unberechtigtes Eindringen in das Netzwerk zu verhindern.
- **Anti-Viren-Tool** – filtert Viren heraus, erkennt aber nur bekannte Virentypen.

Basis-Sicherheitsebene

- **Adress-Lookup** – verhindert den Zugriff auf Daten, die gemäß einer Datenbank mit Blacklist-Adressen als Bedrohung für die Unternehmenssicherheit angesehen werden.

Komplett-Sicherheitsebene

- **Content-Analyse** – scannt Inhalte in Echtzeit entsprechend der jeweiligen Policy und erlaubt bzw. verbietet Zugriffe in Abhängigkeit von den Resultaten der Analyse von Dateitypen, Bildern und eingebetteten Codes.

Umfassender Schutz beinhaltet die Analyse und Bewertung der Daten in den Emails nach den Vorgaben der Sicherheitsrichtlinie eines Unternehmens und der Absender-Empfänger-Beziehung. Emails können aufgrund von Kriterien wie Dateityp, Text- oder Bildinhalt blockiert werden.

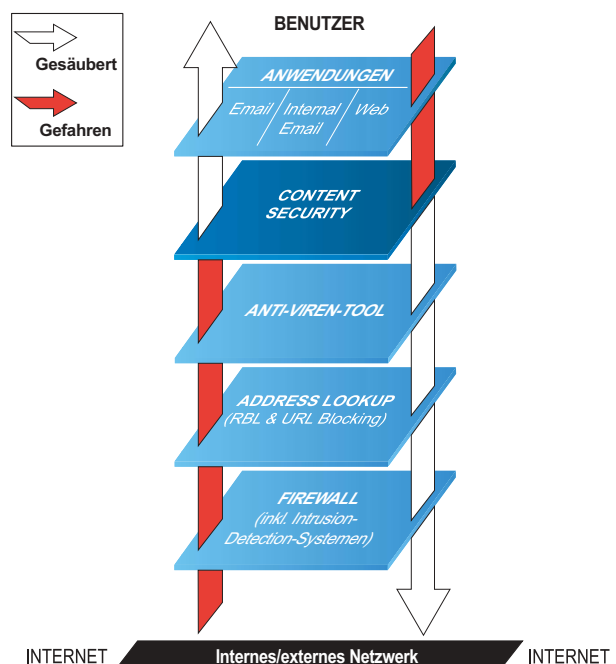
Ein Unternehmen, das sich auf oberflächlichen Schutz verlässt, muss in Kauf nehmen, dass viele Risiken des elektronischen Datenverkehrs bestehen bleiben und keine systematische Kontrolle der Einhaltung von Normen und Gesetzesvorschriften gegeben ist.

Komfortable Administration

Die Systemverwaltung durch Administratoren kann viel Zeit in Anspruch nehmen. MIMESweeper for Exchange vereinfacht und beschleunigt das Sicherheitsmanagement für interne Emails in hohem Maße.

REMOTEmanager ist ein Web-basiertes Verwaltungs- und Administrationsmodul, das die umfangreichen Funktionen von MIMESweeper für Systemadministratoren erweitert. Über diese Verwaltungskonsolle können Administrationsaufgaben standort-unabhängig über das Internet und zudem durch mehrere Zugriffsberechtigte parallel ausgeführt werden.

Das in MIMESweeper enthaltene Report Center gibt einen Überblick über sämtliche Parameter und erleichtert dadurch Management, Kapazitätsplanung und Entscheidungen hinsichtlich der Sicherheitsrichtlinien. Die Informationen können auf unterschiedliche Weise in vordefinierten grafischen Formaten dargestellt werden, um die Entscheidungsfindung durch fundierte Informationen zu vereinfachen.



MIMesweeper™ for Exchange

Sicherheit durch Einführung einer E-Policy

Mit MIMesweeper for Exchange können Unternehmen ihre E-Policy (Sicherheitsrichtlinie) schriftlich definieren und innerhalb eines klar umgrenzten Rahmens implementieren. Nachdem diese E-Policy definiert ist und alle Beschäftigten des Unternehmens darüber aufgeklärt wurden, was unter einem akzeptablen Benutzerverhalten im Zusammenhang mit Email zu verstehen ist, kann das Unternehmen die Richtlinien mit Hilfe der installierten Technologie einheitlich durchsetzen.

Der komfortable und intuitiv zu bedienende Policy-Manager von MIMesweeper for Exchange ermöglicht die Anwendung unterschiedlicher Richtlinien für verschiedene Anwender, sowohl für Einzelne als auch für Gruppen. E-Policy-Wizards begleiten den Administrator Schritt für Schritt bei der Definition und Implementierung unternehmensgerechter Sicherheitsrichtlinien.

Technische Voraussetzungen

- Windows 2000 Server (SP4 oder höher) oder Windows Server 2003
- Microsoft Exchange 2000 Server (SP3 oder höher) oder Exchange Server 2003 (SP1 oder höher)
- Mindestempfehlung: Pentium™ III, 800 MHz, oder gleichwertig
- 1 GB freier Speicherplatz auf NTFS-Partition für die Installation
- 1 GB freier Speicherplatz im Verzeichnis/Temp
- 512 MB Arbeitsspeicher

Was spricht für Clearswift?

Clearswift ist weltweit die #1 in Content Security. Wir sorgen für sichere Inhalte und schützen gegen digitale Angriffe. Mit unseren Produkten lassen sich Policies zur Produktivitätssteigerung, IT-Kostensenkung und Gestaltung einer sicheren Geschäftsumgebung umsetzen. Bei wachsender Anwenderbasis bietet Clearswift 15.000 Kunden und 20 Millionen Nutzern weltweit Schutz und unbeschwertes Arbeiten.

Kontakt Clearswift

Deutschland

Amsinckstraße 67, 20097 Hamburg
Tel. +49 40 23 999 0 | Fax: +49 40 23 999 100

USA

15500 SE 30th Place, Suite 200,
Bellevue, Washington, 98007
Tel. +1 425 460 6000 | Fax: +1 425 460 6185

Großbritannien

1310 Waterside, Arlington Business Park, Theale,
Reading, Berkshire, RG7 4SA
Tel. +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Australien

Ground Floor, 165 Walker Street, North Sydney,
New South Wales, 2060
Tel. +61 2 9424 1200 | Fax: +61 2 9424 1201

Schweden

Frösundaviks allé 15, 4tr, SE-169 70 Solna
Tel. +46 8 50 90 40 78 | Fax: +46 8 655 26 10

Japan

Eisho Takanawadai Bldg 6F, 2-11-8, Minato-ku Shiroganedai
Tokyo-to, 108-0071
Tel. +81 (3) 5423 8171 | Fax: +81 (3) 5423 1274

MAILsweeper™ Business Suite

IMAGEmanager™

SECRETsweeper™

MIMesweeper™ for Web

URL Filter

Reporting

MIMesweeper™ for Exchange

MIMesweeper™ for Domino

e-Sweeper™