

10

entscheidende Schritte zur E-Mail-Sicherheit

Ein Best-Practice-Leitfaden
von Clearswift



Einleitung

E-Mail - so einfach, so wichtig

Moderne Geschäftsabläufe sind zunehmend auf E-Mail-Verkehr angewiesen. Organisationen, die mit E-Mails arbeiten, stellen sich folgende Fragen:

Wie können wir massenweise Spam kontrollieren, ohne dass eine geschäftliche E-Mail darin verloren geht?

Wie verhindern wir, uns über E-Mails mit Viren zu infizieren?

Wie schützen wir unsere E-Mails auf ihrem Weg zum Empfänger vor fremdem Zugriff?

Wie verhindern wir, dass vertrauliche Informationen unser Netzwerk verlassen oder in unbefugte Hände gelangen?

Können wir Phishing-Attacken aufdecken und stoppen?

Wie verhindern wir einen Image-Schaden durch Missbrauch oder Fehlverhalten von Mitarbeitern?

Wie verhindern wir, dass unzulässige Inhalte im Unternehmen kursieren oder veröffentlicht werden?

In Anbetracht dieser Gefahren ist es schon erstaunlich, dass Organisationen E-Mails überhaupt zulassen. Andererseits - versuchen Sie einmal, einen Tag ohne E-Mails auszukommen - es ist fast unmöglich.

Ihre Sicherheitslösung sollte Sie in die Lage versetzen, unbesorgt und ungehindert über das Internet zu kommunizieren. Dieser kurze Leitfaden hilft Ihnen dabei, Freiheit und Sicherheit bei der E-Mail-Kommunikation in ein angemessenes Gleichgewicht zu bringen.

Wenn man einige fundamentale Grundsätze beachtet, kann man E-Mails innerhalb und aus dem Unternehmen verschicken ohne Risiken einzugehen. Gleichzeitig können schädliche Elemente wie z. B. Viren-, Spam-, Spyware-, Trojaner-, Phishing- und DoS-Attacken (denial-of-service), der Verlust sensibler Daten und der Austausch von unerlaubtem, anstößigem oder beleidigendem Material verhindert werden.

Die Verursacher dieser Bedrohungen sind zunehmend raffinierter und verfügen auch über die finanziellen Mittel, sich weiter zu entwickeln. Den einzig wahren Schutz bietet die aufmerksame Anwendung von Richtlinien, Technologien und Verfahren zur Sicherung von E-Mails.



1

Definieren Sie eine solide E-Mail-Richtlinie und kommunizieren Sie sie

Nicht Ihre Server verschicken E-Mails, sondern Menschen. Deshalb ist es wichtig, dass jeder in Ihrem Unternehmen sich im Klaren darüber ist, was beim Umgang mit E-Mails zu beachten ist.

Wir haben die Erfahrung gemacht, dass das Verhältnis zwischen der Zeit, die ein Unternehmen auf die Definition, Kommunikation und Durchsetzung seiner E-Mail-Richtlinie verwendet, und der Summe, die es für die Bearbeitung von Problemen und Schäden durch mangelhaftes Management von E-Mails ausgibt, umgekehrt proportional ist.

Eine gute Richtlinie sieht folgendermaßen aus:

- **Eindeutig** - klar verständlich mit minimalem Interpretationsspielraum
- **Realistisch** - basiert auf der Einbeziehung aller Aspekte des Geschäftsalltags, um sich Ihrer Arbeitsweise anzupassen
- **Granular** - berücksichtigt, dass verschiedene Anwender, Abteilungen und Standorte unterschiedlich mit E-Mails umgehen (und gleichzeitig eine gemeinsame Basis besteht)
- **Flexibel** - ist in der Lage, sich mit Ihrem Unternehmen zu ändern
- **Aktuell** - deckt alle neuen Bedrohungen ab und setzt kontinuierlich Feedback aus dem Unternehmen um
- **Sichtbar** - eine effiziente Richtlinie findet man bei Einführungen, auf Anschlagtafeln, in Mitarbeiter-Leitfäden, in internen Newslettern usw.

Erzählen Sie den Mitarbeitern nicht nur von der Richtlinie, informieren Sie auch darüber, dass sie mithilfe von Filtertechnologien umgesetzt wird. Dies kann die Anzahl der Verstöße verringern.

CLEARSWIFT SECURE Email Gateway enthält MIMESweeper, unsere bekannte Technologie zur Content-Analyse und -Filterung. Legen Sie die Regeln fest - und lassen Sie sie von MIMESweeper umsetzen.

2

Machen Sie sich die Gefahren klar

Wenn die E-Mail-Sicherheitsstrategie Ihres Unternehmens nicht die komplette folgende Liste von Bedrohungen abdeckt, weist Ihr Unternehmen Sicherheitslücken auf:

- Viren
- Trojaner und Bots
- Spam- und Phishing-Attacken
- Spyware (inklusive "Call-home"-Aktivitäten)
- DoS-Attacken (Denial-of-Service)
- Verlust vertraulicher Daten
- Propaganda-E-Mails und pornografische E-Mails
- Verbotenes Material und gestohlene Dateien
- Richtlinienverstöße

Eine Sicherheitslösung, die nur eine dieser Bedrohungen außer Acht lässt, ist keine Lösung. Mit Clearswift-Produkten konsolidieren Sie alle genannten Bereiche und können anhand Ihrer Richtlinien festlegen, wie Sie auf jede dieser Bedrohungen reagieren möchten. Tauchen neue Bedrohungen auf, passt sich Ihre Clearswift-Lösung schnell und problemlos an - ohne Hintertüren.

3

Sorgen Sie für einen nachhaltigen Schutz

Eine E-Mail-Sicherheitsstrategie, die sowohl die IT-Abteilung als auch die E-Mail-Administratoren überlastet, wird letztlich nicht funktionieren und bindet zu viele Ressourcen.

Ein nachhaltiger Ansatz sieht wie folgt aus:

- **Technologiesteuert** - unterstützt durch stabile Tools zur Filterung und Analyse des Datenverkehrs
- **Integriert** - eine Lösung, die von einer einzigen Schnittstelle aus auf alle Bedrohungen reagiert und verwaltet werden kann
- **Online verwaltet** - Zugang für Administratoren über jeden beliebigen Browser
- **Gemeinsame Verantwortung** - Anwender verwalten ihre eigenen Quarantänelisten und befugte Abteilungen helfen bei wichtigen Richtlinienverstößen
- **Automatisch aktualisiert** - alle Updates und Patches sollten automatisiert erfolgen
- **Leicht zu installieren, zu überprüfen und zu verwalten** - sowie ein umfassendes Reporting, um Transparenz und Nachverfolgung zu ermöglichen

Stellen Sie Ihre Sicherheitslösung auf die Probe. Wenn die genannten Aspekte nicht umgesetzt werden können, lassen sich Effizienz und Komfort der Lösung noch optimieren.

Die Clearswift-Technologie vereint die besten Schutzmechanismen in einer einzigen, online verwalteten Plattform mit zentralen Richtlinien, rollenbasierter Verwaltung und automatischen Updates. Einfacher geht es nicht.

4

Schützen Sie Ihren gesamten Datenverkehr

Die besten Sicherheitsmechanismen für ein- und ausgehende E-Mails einzusetzen nützt nichts, wenn die Nutzung von Webmail übersehen und ungeschützt bleibt.

Durch die Kombination von Clearswift SECURE Web Gateway mit CLEARSWIFT SECURE Email Gateway können Unternehmen ihren gesamten Nachrichtenverkehr sichern. Es können Richtlinien von einer gemeinsamen Management-Oberfläche aus erstellt werden, die die gleichen Regeln und Privilegien sowohl für E-Mail (SMTP) als auch für Webmail (HTTP/s) festlegen. So sparen Sie Zeit und gewährleisten Einheitlichkeit auf all Ihren Plattformen.



5

Wählen Sie die für Sie richtige Installationsform aus

Am besten können Sie selbst entscheiden, welche Bereitstellungsvariante optimal für Ihr Unternehmen geeignet ist. Kleinere Organisationen zum Beispiel ziehen möglicherweise eine Hardware-Paketlösung oder eine Installation auf ihrer eigenen bereits vorhandenen Hardware vor. Größere Unternehmen entscheiden sich häufig für eine Kombination aus physischen und virtuellen Servern, um ein ausgeglichenes Verhältnis von Leistung und Ausfallsicherheit zu schaffen.

Clearswift SECURE Email Gateway bietet eine Reihe von Bereitstellungsoptionen:

Dell-Hardwarepaket

Clearswift verwendet die neuesten Server-Plattformen von Dell, um Ihr Netzwerk zuverlässig zu schützen. Mit der Unterstützung eines weltweit führenden Anbieters können Sie beruhigt in die Zukunft blicken.

Eigene Hardware

Clearswift ist bewusst, dass Organisationen gegebenenfalls Hardware von einem bestimmten Anbieter bevorzugen. Clearswift hat seine Software deshalb auf einer Reihe von Hardware-Plattformen von Anbietern wie z. B. HP und IBM getestet und stellt Ihnen eine Hardwarekompatibilitätsliste zur Verfügung. Damit gibt Clearswift seinen Kunden die Freiheit, Systeme ganz auf ihre jeweiligen Bedürfnisse zuzuschneiden.

VMware / Hyper-V

Clearswifts Lösungen zur Informationssicherheit können in virtuellen Umgebungen eingesetzt werden, um Hardwarekosten, Platzbedarf und Stromverbrauch zu reduzieren. Mit Lösungen von Clearswift können Kunden physische und virtuelle Appliances nach Belieben miteinander kombinieren und so die Vorteile beider Bereiche ausnutzen.

6

Schließen Sie das Zero-Day-Fenster

Antivirus- und Anti-Spyware-Lösungen bieten hervorragenden Schutz vor bekannten Bedrohungen. Was aber hält einen brandneuen Virus davon ab, in Ihr Netzwerk einzudringen, bevor Sie Sicherheitslücken überhaupt ermittelt haben?

Das Zero-Day-Fenster ist eine der offensichtlichsten Schwachstellen bei den E-Mail-Strategien vieler Unternehmen, und es gibt nur einen Weg, dagegen anzugehen: Content-Filterung anhand intelligenter Richtlinien.

Neben bewährten Filtern, die neue Malware aufdecken, analysiert die Content-Filterungstechnologie von Clearswift SECURE Email Gateway Nachrichten und Anhänge, zerlegt sie in ihre Einzelteile und bestimmt die Charakteristika des Inhalts. Per Richtlinie können Sie dann entscheiden, was mit verdächtigen Inhalten passieren soll: blocken, parken, umleiten, löschen, melden oder eine Kombination aus diesen Verfahren. Hauptsache ist, Sie lassen verdächtige oder unbekannte Inhalte nicht einfach durchkommen!

CLEARSWIFT SECURE Email Gateway ist um die MIMESweeper Engine zur Content-Filterung herum aufgebaut. Jede Nachricht wird in ihre Einzelteile zerlegt, gemäß der jeweiligen Richtlinie analysiert und entsprechend behandelt.

7

Sichern Sie Ihren Schutz für die Zukunft

Die Bedrohungen für Ihr Unternehmen verändern sich kontinuierlich. Sie möchten sicherlich nicht in Technologien investieren, die bereits veraltet sind, wenn die nächste schlechte Nachricht eintrifft. Rechtzeitige und einfache Upgrade-Pfade sind deshalb unabdingbar.

Eine wichtige Komponente Ihrer E-Mail-Sicherheitslösung ist die Content und Policy Engine. Um produktiv und effizient arbeiten zu können, muss sie Ihnen ermöglichen, problemlos neue Regeln, Profile und Prozesse hinzuzufügen, um auf neue Bedrohungen oder Veränderungen in Ihrem Unternehmen zu reagieren.

Clearswift SECURE Email Gateway aktualisiert dynamisch seine Antivirus- und Spam-Konfiguration. Updates erfolgen voll automatisch während Upgrades zwar automatisch bereitgestellt werden, es dem Administrator aber ermöglichen, den Zeitpunkt für die Installation selbst zu wählen. Als Vorreiter im Bereich Richtlinien-basierter Content Security ist Clearswift auch heute noch führend in der Branche, insbesondere weil wir fortlaufend auf das Auftauchen neuer Bedrohungen reagieren.

8

Erfassen Sie Datenverkehr und Nutzungsverhalten

Sie können nicht sichern, was Sie nicht sehen. Analysieren Sie Nutzungsverhalten und Performance-Probleme aller E-Mails anhand von Reports, so dass Sie schnell reagieren können.

Reports können Aufschluss geben über die größten Absender und Empfänger von E-Mails sowie häufig verwendete Dateitypen und -größen.

Andere Reports schlüsseln E-Mail-Mengen und Datentypen nach Standort, Abteilung, Server oder Gateway auf.

Diese Informationen können sich bei der Ermittlung von Problembereichen als äußerst nützlich erweisen und es Ihnen ermöglichen, Richtlinien zu optimieren und Ressourcen entsprechend neu zu verteilen.

Anhänge zu blocken, die eine bestimmte Größe überschreiten, kann ebenfalls zum Schutz Ihrer Speicherplatz- und Bandbreitenressourcen beitragen. Legen Sie in Ihrer Richtlinie fest, dass übergroße Anhänge gesondert von der E-Mail behandelt - zum Beispiel geparkt und über Nacht gesendet - werden. Ein Protokoll über Richtlinienverstöße wird Ihnen in jedem Fall helfen, auf alle Probleme zu reagieren.

Alle Lösungen von Clearswift enthalten umfassende webbasierte Reporting- und Analysefunktionen, die helfen, den gesamten Datenverkehr zu verstehen und zu steuern sowie Gefahren vorzeitig zu erkennen. Sie können Termine festlegen, an denen Reports automatisch an Ihren Posteingang versendet werden.



9

Sichern Sie Ihre Daten

Die zunehmende Online-Vernetzung von Unternehmen erhöht auch das Risiko, dass vertrauliche Informationen von Unbefugten gelesen werden. Es ist von entscheidender Bedeutung, E-Mails zu verschlüsseln, um Nachrichten geschützt an Externe versenden zu können. Das Problem ist, dass viele Verschlüsselungslösungen dabei Verfahren einsetzen, die sowohl kompliziert als auch teuer sind.

Clearswift SECURE Email Gateway geht neue Wege: Es bietet eine benutzerfreundliche, auf Richtlinien basierende Verschlüsselung an, die einfach und erschwinglich ist. E-Mails werden zentral und ohne Interaktion der Benutzer ver- und entschlüsselt, vollautomatisch nach Ihrer vorab einmalig definierten Richtlinie. Verschlüsselter Inhalt kann entschlüsselt und auf Gefahren gescannt werden. Dabei werden Standards wie S/MIME und Open PGP unterstützt. Durch die Ad Hoc Encryption können Sie sogar mit Kommunikationspartnern verschlüsselt kommunizieren, die selbst noch keine Verschlüsselungstechnologie einsetzen. So stellt Clearswift SECURE Email Gateway sicher, dass Nachrichten sicher, zuverlässig und richtliniengemäß ankommen.

10

Beachten Sie rechtliche Vorgaben und Branchen-Standards

Für viele Unternehmen oder Branchen gelten besondere Vorschriften und Empfehlungen bezüglich Ihrer IT-Sicherheit.

Obwohl einige Verstöße nicht mehr als eine Verwarnung nach sich ziehen, sollte man unbedingt wissen, dass einige Regierungsbehörden befugt sind, Geldstrafen zu verhängen oder andere Konsequenzen zu ziehen. Mit anderen Worten: Wenn Sie sich nicht an die Regeln halten, könnte dies einen finanziellen und einen Image-Schaden für Ihr Unternehmen mit sich bringen.

Wenn Sie mit Clearswift SECURE Email Gateway Richtlinien definieren und durchsetzen, leisten Sie für Ihr Unternehmen einen entscheidenden Beitrag zur Compliance.

Kontakt zu Clearswift

UK - Internationale Zentrale
Clearswift Limited
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA
UK
Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Vertrieb: +44 118 903-8700
Technischer Support: +44 118 903-8200
Email: info@clearswift.com

Australien
Clearswift
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIEN
Tel : +61 2 9424 1200
Fax : +61 2 9424 1201
Email: info@clearswift.com.au

Deutschland
Clearswift GmbH
Amsinckstraße 67
20097 Hamburg
DEUTSCHLAND
Tel : +49 40 23 999-0
Fax : +49 40 23 999-100
Email: info@clearswift.de

Japan
Clearswift K.K.
7F Hanai Bldg.
1-2-9 Shibakouen,
Minato-ku, Tokyo
105-0011
JAPAN
Tel : +81 (3)5777 2248
Fax : +81 (3)5777 2249
Email: info.jp@clearswift.co.jp

Spanien
Clearswift España S.L.
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón
Madrid
SPANIEN
Tel : +34 91 7901219 / +34 91 7901220
Fax : +34 91 7901112
Email: info.es@clearswift.com

USA
Clearswift Corporation
161 Gaither Drive
Centerpointe
Suite 101
Mt. Laurel, NJ 08054
USA
Tel : +1 856-359-2360
Fax : +1 856-359-2361
Email: info@us.clearswift.com

Zusammenfassung

Schutz und automatisierte Steuerung von Unternehmensinhalten

Die genannten 10 Schritte fassen eine einfache Best-Practice-Strategie für E-Mail-Sicherheit zusammen.

Die Technologien zum Schutz vor auftretenden Bedrohungen mögen sich ändern, die Grundlagen bleiben jedoch bestehen:

- Definieren und fördern Sie eine eindeutige E-Mail-Richtlinie.
- Setzen Sie sie mit der richtigen Technologie um.
- Halten Sie es einfach.

Clearswift ist seit mehr als 20 Jahren im Bereich Content Security tätig. Das Unternehmen hat solide Technologien zum Schutz Ihrer Informationen im Online-Datenverkehr entwickelt und zukunftsweisende Standards gesetzt.

Sprechen Sie mit uns darüber, wie Sie Ihre Informationssicherheit vereinfachen können, oder besuchen Sie www.clearswift.de um einen Einblick in unsere Lösungen zu bekommen.

Über Clearswift

Clearswift vereinfacht Content Security

Clearswift ist Anbieter von Lösungen für Informationssicherheit und kann auf viele Innovationen zurückblicken. Wir erkennen nicht nur Dateitypen, sondern verstehen Inhalte und wie Menschen arbeiten und kommunizieren. Die content-sensitiven, Richtlinien-basierten Lösungen von Clearswift werden weltweit von 17.000 Organisationen genutzt und ermöglichen es diesen, ohne Zugeständnisse Daten sowie die E-Mail- und Internet-Sicherheit über alle Gateways hinweg und in alle Richtungen zu verwalten und zu schützen.

Innovationen von Clearswift verfügen über viele Funktionen, die in der Sicherheitsbranche mittlerweile gang und gäbe sind, z. B. Image Scanning, Richtlinien-basierte Verschlüsselung und Nachrichtenverfolgung auf Benutzerebene. Durch die Bereitstellung von einsatzbereiten virtuellen Appliances auf den ESX- und ESXi-Plattformen von VMware ist Clearswift unverändert führend in der Branche. Die Appliances verfügen über effiziente und erprobte content-sensitive Richtlinien, die unsere Kunden und deren Mitarbeiter gleichermaßen schützen.

Wir sind der Ansicht, dass die IT-Sicherheitsbranche sich weiterentwickeln muss, um eine bessere Kommunikation und Zusammenarbeit von Organisationen in der vernetzten Welt zu fördern, anstatt Kommunikation zu beschränken. Die content-sensitiven Lösungen von Clearswift passen sich an die Anforderungen des Geschäftslebens an und fördern die Produktivität.

Clearswifts einheitliche Lösungen für Internet- und E-Mail-Sicherheit räumen schlichtweg mit Angst und Negativität auf und ermöglichen es Unternehmen, ihre Geschäfte ohne Beeinträchtigung der Sicherheit zu führen.