clearswift
RUAG Cyber Security

Clearswift SECURE Email Gateway

E-Mail ist das primäre Werkzeug für unternehmensübergreifende Zusammenarbeit. Unternehmen müssen deshalb dafür sorgen, dass Inhalte nur gesichert versendet und empfangen werden. Das Clearswift SECURE Email Gateway (SEG) schützt vor dem Verlust kritischer Informationswerte. Es sichert das geistige Eigentum Ihres Unternehmens und unterstützt Sie bei der Einhaltung aktueller gesetzlicher Auflagen und Vorgaben.

Nur durch eine ungehinderte und sichere E-Mail-Kommunikation können Unternehmen heutzutage die Wettbewerbsvorteile erzielen, die aus der Nutzung von Tools für die Online-Zusammenarbeit entstehen können. Die einzigartige Deep Content Inspection von Clearswift macht aus der risikobehafteten E-Mail einen Kommunikationsweg, der auch die Sicherheitsbedürfnisse Ihrer Organisation komplett abdeckt. Das Gateway überprüft E-Mails auf sensible Inhalte und stellt entsprechend der Unternehmensrichtlinien verschiedene Möglichkeiten bereit, wie mit kritischen Mails verfahren werden soll. Unterschiedliche, personenbezogene Regeln werden angewandt. Mit der Funktion Clearswift Adaptive Redaction ist es möglich, lediglich die kritischen Inhalte beim Verschicken oder Empfangen automatisch richtlinienbasiert unkenntlich zu machen, anstatt die komplette E-Mail zu blocken. Somit werden Arbeitsabläufe nicht mehr unterbrochen und die Sicherheit bleibt erhalten.

Schutz vor eingehenden Bedrohungen

Der integrierte Virenschutz von Kaspersky oder Sophos wird alle fünfzehn Minuten aktualisiert. Beide Technologien werden durch Zero-Hour-Schutz-Software und die Ermittlung von Aktivcodes ergänzt. Somit wird sichergestellt, dass das Versenden und Empfangen von Viren oder Schadprogrammen per E-Mail unmöglich ist. Gezielte Angriffe erfolgen in der Regel per E-Mail mit infizierten Office- oder PDF-Dateien. Installieren sich dann solche Exploits auf einem Desktop, werden sie typischerweise mit den Benutzerberechtigungen des Empfängers ausgeführt und erhalten somit möglicherweise Zugriff auf vertrauliche Daten. Deshalb wird zusätzlich zu den Anti-Malware-Funktionen die strukturelle Bereinigung bzw. Beseitigung von Makros, Skripten und Active/X aus E-Mail-Nachrichten, PDF- und Office Dateiformaten angeboten. Das Risiko erfolgreicher Angriffe wird dadurch minimiert.

Hervorragende Spam-Erkennung

Das neue Clearswift SECURE Email Gateway v4.1 wird mit einem neuen Antispam-Modul von Mailshell ausgeliefert. Die DKIM-Unterstützung sorgt für eine weitere Verringerung von Spam-Mails. Mit dem neuen Outlook Spam-Reporter lassen sich Spam-Nachrichten außerdem überwachen, registrieren und beseitigen. Ein mehrstufiger Mechanismus zur Spam-Abwehr mithilfe von IP-Reputation, Greylisting, Signaturen, SPF, RBL, Empfänger-Authentifizierung und Modulen für das maschinelle Lernen (nach der Bayes-Methode) sorgt für eine Erkennungsquote von mehr als 99,9%. Das SEG verringert somit spürbar die Zeit, die Benutzer mit der Verwaltung ihres Posteingangs zubringen und reduziert drastisch die Auswirkungen von Viren und Schadprogrammen, die in Spam-Mails enthalten sein können.

Richtlinien für die kontextsensitive Inhaltsanalyse

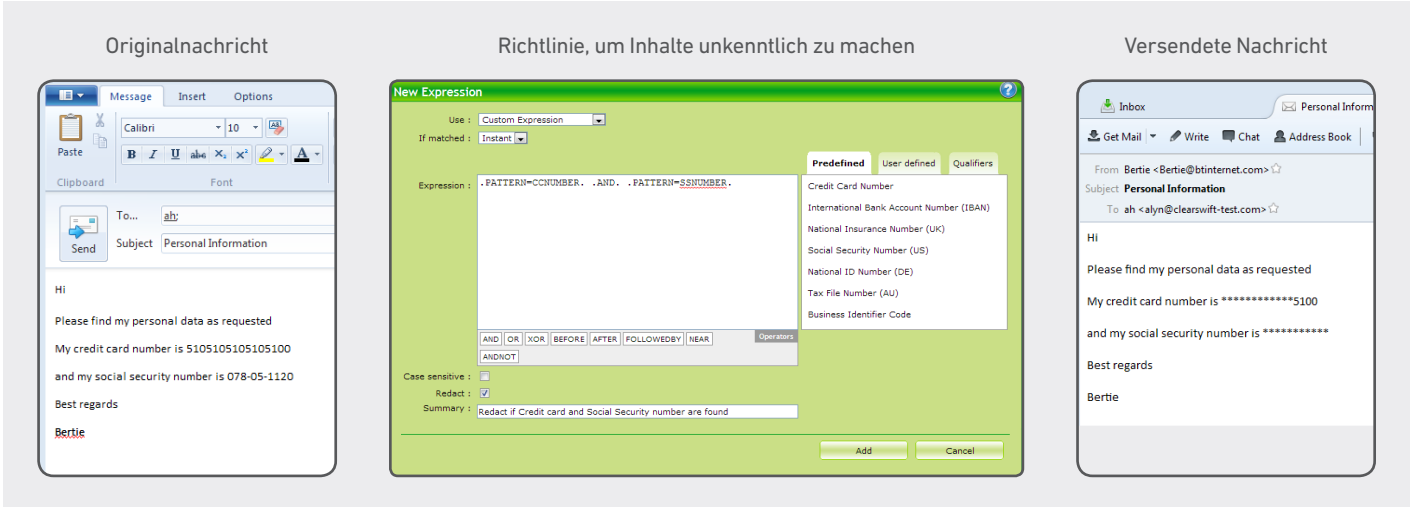
Mit flexiblen Richtlinien und der kontextsensitiven Inhaltsanalyse müssen Sie nicht mehr zwischen frei fließender Kommunikation und inakzeptablen Risiken wählen. Flexible Policies sind für den Einsatz in der Geschäftswelt extrem wichtig. Bei zu restriktiven Richtlinien können die Menschen entweder nicht effektiv arbeiten oder sie versuchen Wege zur Umgehung der Sicherheitsrichtlinien zu finden.

Adaptive Redaction

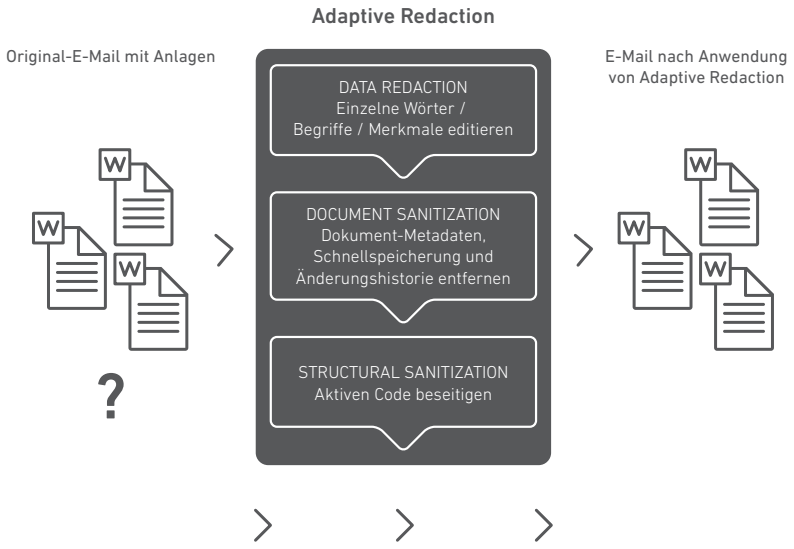
Clearswift Adaptive Redaction verhindert proaktiv, dass sensible Unternehmensinformationen absichtlich oder unabsichtlich innerhalb einer Organisation ausgetauscht bzw. von oder nach außen übermittelt werden. Das besondere an dieser Clearswift-Technologie ist, dass damit Arbeitsabläufe nicht unterbrochen werden, wie es bei Lösungen der Fall ist, die mit

dem herkömmlichen Stopp-and-Block-Ansatz arbeiten. Es werden nur die kritischen Informationen (Kreditkartennummern, Projektnummern, Namen, etc.) unkenntlich gemacht, der Rest der Daten wird ohne Verzögerung zugestellt. Eine reibungslose Zusammenarbeit der Mitarbeiter ist also möglich, ohne die Sicherheit zu vernachlässigen.

Abbildung 1. Clearswift Adaptive Redaction: Data Redaction



Mit der Funktion Document Sanitization lassen sich Änderungsverfolgungen, Dokumenthistorie sowie Schnellspeicherungsdaten mit ggf. heiklen und kritischen Informationen löschen. Dokumenteigenschaften, wie etwa der Autor, die Organisation und der Status, lassen sich komplett entfernen während definierte andere Dokumenteigenschaften beibehalten werden können.



Information Value Protection

Datenverlust gehört heute zu den größten Sorgen von Unternehmen. Ob es um aktuelle Planungen, um Kundendaten oder vertrauliche Mitarbeiterinformationen geht, der Verlust von kritischen Informationen kann den Ruf einer Firma schädigen und sie finanziell ruinieren.

Um zu verhindern, dass kritische Informationen absichtlich oder versehentlich versendet oder empfangen werden, überprüft SECURE Email Gateway anhand vordefinierter Suchmuster die Inhalte von Nachrichten und Anhängen im Kontext zu Benutzern und Benutzergruppen. Dieser Kontext wird durch die Integration des Active Directory durch LDAP bereitgestellt, sodass die Richtlinien für einzelne Benutzer, Benutzergruppen oder für das gesamte Unternehmen (Domänen) erstellt und angewandt werden können.

Diese Suchmuster bestehen aus standardmäßigen Wörtern, Begriffen oder regulären Ausdrücken, die für die Suche nach komplexen alphanumerischen Mustern verwendet werden. Diese Muster werden zum Identifizieren von eindeutigen Informationen eingesetzt wie etwa Kreditkarten, IBAN-Nummern, Sozialversicherungsnummern etc.

Die Begriffe werden mithilfe boolscher Operatoren und Positionsoperatoren kombiniert, um so Regeln wie beispielsweise die folgenden zu erstellen:

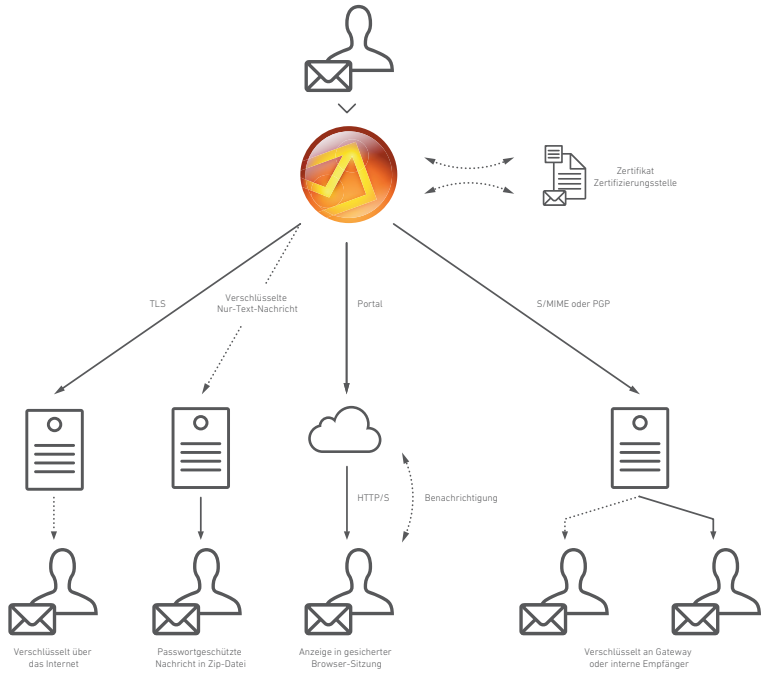
- Vorname. .FOLLOWEDBY=1. .Nachname. .FOLLOWEDBY=1. .Geburtsdatum.
- Vertraulich. .UND. .Projekt.ODER.Material

Compliance (Einhaltung der Regeln)

Das Einhalten rechtlicher Rahmenbedingungen spielt für Unternehmen eine entscheidende Rolle. Um Verantwortliche beim Einhalten der Regeln zu unterstützen, stellt SECURE Email Gateway Standardvorlagen und Schlagwörterlisten mit gängigen Begriffen bereit, die auf eine mögliche Sicherheitsverletzung hinweisen können.

Die Gateways sind mit anpassbaren Verzeichnissen für GLBA, HIPAA, SEC und SOX ausgestattet, um Implementierungszeit zu sparen. Organisationen, die PCI- und PII-Vorschriften einhalten müssen, können eigene Verzeichnisse und die speziellen Merkmale „Kreditkarte" und „Sozialversicherung" einsetzen. Die Standardverzeichnisse sind auch durch Begriffe erweiterbar, die für den jeweiligen Kunden zutreffender sind.

Bestimmte kritische Informationen müssen ausgetauscht werden. Daher ist die E-Mail-Verschlüsselung eine weitere zentrale Funktion des Gateways. Sie gewährleistet, dass Verschlüsselungsregelungen zum Umgang mit vertraulichen, über das Internet versendete Daten, automatisch umgesetzt werden. Das Bundesdatenschutzgesetz (BDSG) schreibt vor, dass das Senden vertraulicher Daten per E-Mail verschlüsselt zu erfolgen hat; für die erforderliche Flexibilität unterstützt SECURE Email Gateway unterschiedliche Verschlüsselungsmechanismen.



E-Mail-Verschlüsselung

Das Email Gateway bietet mit dem Standard TLS und den kostenpflichtigen Optionen, die entweder S/MIME, PGP und Ad-hoc-Verschlüsselung mit passwortgeschützten / AES256-verschlüsselten Dateien oder die portalbasierte Verschlüsselung unterstützen, eine Reihe von Verschlüsselungsmöglichkeiten. Das Gateway versendet vertrauliche Daten sicher, innerhalb von Sekunden und in dem für den Empfänger optimalen Format.

Verwaltung und Reporting

Die Benutzeroberfläche des Gateways ist leistungsstark und leicht zu bedienen. Mit der rollenbasierten Administration, Automatisierung und Wiederverwendung von Richtlinien lässt sich das Erstellen von Regeln, das Verwalten von Verstößen, die Nachverfolgung von Nachrichten und das Erkennen von Trends und Verhaltensmustern schnell und einfach umsetzen. So erhalten Sie wertvolle Einblicke, ohne teure Admin-Ressourcen zu vergeuden.

Deep Content Inspection

Besonders wichtig für eine präzise und damit zuverlässige Ermittlung des tatsächlichen Dateityps ist die Deep Content Inspection von Clearswift, bei der die Dateien anhand ihrer Signatur und nicht an der Datei-Endung erkannt werden. Komprimierte Dateiarchive werden geöffnet und der Inhalt in Echtzeit analysiert. Eine rekursive Zerlegung erlaubt es, eingebettete Objekte mehrere Ebenen tief zu analysieren und den Inhalt umfassend zu überprüfen. So wird sichergestellt ist, dass keine Daten unbemerkt nach außen oder in das Unternehmen hinein gelangen.

Flexible Implementierung

Sie wählen selbst, auf welcher Plattform Sie Clearswift SECURE Email Gateway implementieren möchten. Die Lösung ist entweder als vorinstallierte Hardware-Appliance, als Software-Image auf eigener Hardware oder virtualisiert in einer VMWare-/HyperV-Umgebung erhältlich. Clearswift SECURE Email Gateway kann auch als Cloud-Lösung eingesetzt werden, die Ihnen absolute Flexibilität hinsichtlich der Anforderungen Ihres Unternehmens bietet.

Über Clearswift

Weltweit vertrauen Unternehmen auf die Lösungen von Clearswift, wenn es darum geht, ihre geschäftskritischen Informationen wirksam zu schützen. Damit sichern sie ihre interne und externe Zusammenarbeit und können sich so auf ihr Tagesgeschäft konzentrieren.

Clearswifts Lösungen für Information Value Protection (IVP) basieren auf einer innovativen Deep Content Inspection Engine. Mit der einzigartigen Adaptive-Redaction-Technologie kann eine IVP-Lösung ganz unkompliziert implementiert und im Unternehmen die Grundlage für eine durchgängige Information-Governance-Strategie geschaffen werden. Das Resultat ist eine 100%-ige Transparenz der Informationen zu jeder Zeit.

Als globales Unternehmen unterhält Clearswift Standorte in Deutschland und anderen europäischen Ländern, Australien, Japan und den USA.

Clearswift verfügt ferner über ein Netzwerk von mehr als 900 Vertriebspartnern weltweit.

Weitere Informationen finden Sie unter **www.clearswift.de**

UK – Globaler Hauptsitz
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Vertrieb: +44 (0) 118 903 8700
Technischer Support: +44 (0) 118 903 8200
E.Mail: info@clearswift.com

Australien
Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street, North Sydney
New South Wales, 2060
Australia

Tel: +61 2 9424 1200
Technischer Support: +61 2 9424 1210
E.Mail: info@clearswift.com.au

Deutschland
Clearswift GmbH
Im Mediapark 8
D-50670 Köln
Deutschland

Tel: +49 (0) 221 8282 9888
Technischer Support: +49 (0)800 1800556
E.Mail: info@clearswift.de

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technischer Support: 0800 100 0006
E.Mail: info.jp@clearswift.com

USA
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technischer Support: +1 856 359 2170
E.Mail: info@us.clearswift.com

clearswift
RUAG Cyber Security

Funktion	Vorteil
Flexible Richtlinien	
Granulare Richtlinienkontrolle	Leicht zu definieren mit selbsterklärenden Regeln, die effektive Nutzung zulassen und gleichzeitig das Risiko minimieren.
Directory-Integration	Regelmäßiges Erfassen von E-Mail-Adressen für Sender und Empfänger aus dem Active Directory.
Flexible Richtlinien	Aufsetzen von Workflows für kritische E-Mails, die das Überprüfen und Freigeben der Nachrichten durch einen Vorgesetzten ermöglichen.
Eingehende Bedrohungen	
Bi-direktionales Viren- und Malware-Scanning *	Hindert bekannte und unbekannte Malware am Eindringen und Verlassen des Netzwerks durch den Einsatz von bis zu zwei Antivirus-Engines (Sophos und/oder Kaspersky)
Zero-Hour-Schutz-Software	Das Ermitteln und Blockieren neuartiger Virenangriffe, bevor die Virensignaturen verfügbar sind, mindert das Risiko neuer Bedrohungen durch Malware.
Mehrstufige Antispam-Lösung	Mehrere Spam-Module bieten einen ganzheitlichen Ansatz bei der Spam-Ermittlung und erkennen mehr als 99,9% der Spam-Mails bei einer False-Positives-Rate von 1 in 300.000.
Structural Sanitization	Aktive Codes, wie etwa Makros, Skripte und Active/X in Nachrichten und Anlagen werden in Microsoft Office-, Open Office- und PDF-Dateien erkannt UND entfernt. Somit können diese automatisiert sicher ausgeliefert werden.
Überprüfung von Bildern und Grafiken	Bilder und Grafiken werden analysiert und gegebenenfalls in Quarantäne gestellt.
Schutz vor Datenverlust	
Identifikation von Binärdateitypen	Genaue Identifikation auf Basis vorhandener Signaturen sowie die Möglichkeit, eigene Dateisignaturen zu definieren.
Adaptive Redaction*	Data Redaction: Sensible Wörter und Begriffe in Nachrichten und Anlagen werden unkenntlich gemacht. Document Sanitization: Dokumenteigenschaften, Änderungshistorie und Schnellspeicherungsdaten werden beseitigt.
Lexikalische Analyse und reguläre Ausdrücke	Durchsuchen der Dateiinhalte nach Schlüsselwörtern und Phrasen unter Verwendung regulärer Ausdrücke um sensible Daten zu identifizieren.
Vordefinierte Vorlagen für sensible Daten	Einfache Identifizierung und Ermittelung von standardisierten Informationsmerkmalen, einschließlich Kreditkarten-, Konto- sowie Sozialversicherungs- und Krankenversicherungsnummern. Benutzerdefinierte Tokens lassen sich leicht erstellen.
Workflow-Regeln	Für ausgehende Nachrichten kann erzwungen werden, dass jeweils eine Kopie an den Vorgesetzten gesendet wird. Bei einem Richtlinienverstoß können Nachrichten vom Line-Manager verwaltet werden. Diese Nachrichten können um eine definierte Zeit x verzögert verschickt werden. So können sie bei Bedarf von einem Vorgesetzten gelöscht werden.
Compliance (Einhaltung der Richtlinien)	
Compliance-Verzeichnisse	Mit anpassbaren Verzeichnissen für GLBA, HIPAA, SEC und SOX, um Implementierungszeit zu sparen. Eigene Verzeichnisse für PCI- und PII-Vorschriften, um das Risiko eines Reputationsverlustes zu reduzieren.
Integrierte Verschlüsselung	TLS wird als Standard Verschlüsselung bereitgestellt, einschließlich der optionalen Methoden S/MIME, PGP und Ad-hoc-Verschlüsselung*, damit Nachrichten sicher versendet werden können.
Portalbasierte Verschlüsselung*	Web-basierte E-Mail-Verschlüsselung, die das Versenden verschlüsselter Nachrichten an Empfänger ohne Verschlüsselungslösung ermöglicht.
Unterstützung der Off-Box-Archivierung	Verwendung von Relay-to und BCC, um alle oder einen Teil der Nachrichten an lokale oder cloud-basierte Archivierungslösungen umzuleiten.
Management	
Intuitives, web-basiertes Interface	Einfache Verwendung, keine Linux-Kenntnisse erforderlich.
Über mehrere Gateways konsolidiertes Reporting	Konsolidiertes Reporting zur Analyse und Auswertung.
Nachrichtenverfolgung über Multi-Gateway	Überblick über Herkunft, Verarbeitungsweise und Versand von Nachrichten über mehrere Gateways. Umfassende Exportfunktionen, die manuell oder automatisiert ausführbar sind.
Zentralisierte SYSLOG-, SNMP-, SMTP-Warnungen	Konsolidierung in einem zentralen SIEM oder Verwendung von SNMP- oder SMTP-Management-Alerts bei der Implementierung von Rechenzentren mit „Lights-Out".

*Kostenoption