clearswift
RUAG Cyber Security

Datenblatt: SECURE Web Gateway

Das Internet kann heute als eine Erweiterung der Infrastruktur eines Unternehmens angesehen werden. Die immer häufigere Verwendung von cloud-basierten Diensten wie Salesforce.com oder Office365 sowie die Internetnutzung der Mitarbeiter während der Arbeitszeit zwingt Unternehmen dazu, sicherzustellen, dass die Inhalte und Informationen, die kommuniziert werden, angemessen und freigegeben sind. Der Schutz vor Datenlecks, die zu hohen Strafzahlungen oder einem gravierenden Reputationsverlust führen können, ist zwingend notwendig. Clearswift SECURE Web Gateway (SWG) bietet deshalb eine proaktive, regelbasierte Web-Gateway-Lösung, die aus der risikobehafteten Web-Umgebung eine sichere Ressource macht und die genau auf die Anforderungen Ihres Unternehmens zugeschnitten ist.

Mit den Möglichkeiten von Clearswift zur tief gehenden Inhaltsanalyse (deep-content inspection) steht einer sicheren Kommunikation und damit dem für Unternehmen entscheidenden Wettbewerbsvorsprung nichts mehr im Weg. Das Gateway bietet weitaus mehr, als „nur" Ihr Netzwerk von Viren, unsachgemäßen Inhalten und schädlichen Programmen frei zu halten. Sie haben damit eine individuell einstellbare Kontrolle über die Informationen, auf die online zugegriffen wird bzw. die mit anderen geteilt werden – egal, ob es dabei um Surfen im Internt oder um den unerwünschten Abfluss von sensiblen Daten geht. Mit der Sicherheit, dass die Adaptive-Redaction-Funktionen von Clearswift Inhalte richtlinienbasiert dynamisch anpassen (redigieren), ermöglicht Clearswift SECURE Web Gateway Organisationen, alle Vorteile der unternehmensübergreifenden Web-2.0-Technologien zu nutzen. Anstatt die geschäftskritische Kommunikation zu unterbrechen, werden kritische Inhalte „sicher" gemacht. Die Kommunikation läuft ungehindert weiter, während die proaktive Vorgehensweise von Clearswift den Schutz der vertraulichen Daten sicherstellt.

Schutz vor Datenlecks

Durch die Verwendung der lexikalischen Analyse des SECURE Web Gateway (SWG) kann der versehentliche Abfluss von Daten, eine der größten Herausforderungen heutiger Unternehmen, erkannt und vermieden werden. Selbst die in Metadaten versteckten Informationen können, während des Hochladens von Dateien, entfernt werden. Entweder durch das Durchsuchen der hochzuladenden Dateien nach Schlüsselbegriffen für vertrauliche Daten oder durch die Analyse der Inhalte kann das Datenleck identifiziert und gestoppt werden – gefolgt von den dann notwendigen Konsequenzen.

Zur Einhaltung der gesetzlichen Vorschriften und internen Richtlinien sowie zum Schutz vor Datenlecks, können im SECURE Web Gateway Schlüsselbegriffe hinterlegt werden, die auf vertrauliche Daten hinweisen. Die Schlüsselbegriffe lassen sich aus Standardvorlagen sowie speziellen Wörterbüchern generieren.

Abhängig vom Inhalt können mit der Adaptive-Redaction-Funktion vertrauliche Daten überwacht und ggf. entfernt werden, während die eigentliche Kommunikation – ohne die regelwidrigen Informationen – weitergeführt wird. Dies kann auf Dokumenteigenschaften sowie auf den Änderungsverlauf angewendet werden, wenn dieser möglicherweise vertrauliche Daten enthält.

Deep Content Inspection

Mit der intelligenten Deep Content Inspection (tief gehende Inhaltsanalyse), ist eine sichere Kommunikation über soziale Netzwerke möglich. Die Deep Content Inspection Engine von Clearswift erkennt den Unterschied zwischen einem harmlosen und einem potenziell gefährlichen bzw. unangemessenen Tweet. Die kontextsensitive Suche erkennt vertrauliche Informationen und Bilder und stellt sicher, dass diese nicht ins Internet hochgeladen werden. Die Kombination aus inhalts- und kontext-abhängigen Richtlinien verringert die Zahl der möglichen False-Positives merklich, so dass für eine effiziente Strategie zum Schutz vor Datenverlust weniger Ressourcen aufgewendet werden müssen.

Richtlinienbasierte Web-Sicherheit

Die intuitive und leistungsstarke Benutzerschnittstelle bietet eine einfache Aufgabenverwaltung, mit der Fehler vermieden und Betriebskosten gesenkt werden können. Die flexiblen und einfach zu konfigurierenden Richtlinien (Policies) des Gateways bieten sehr umfangreiche Reporting- und Audit-Funktionen.

Flexible Kontrollen für Web 2.0-Richtlinien

Clearswift vereinfacht die Erstellung von Richtlinien (Policies) für die bekanntesten sozialen Medien, indem es Policies für Facebook, LinkedIn, Twitter und YouTube vordefiniert. Damit können unterschiedliche Richtlinien für unterschiedliche Abteilungen aufgesetzt werden. Jeder dieser Pfade enthält vordefinierte Inhaltsregeln, so dass zur jeweiligen Webseite passende Policies erstellt werden können. Das bedeutet natürlich auch, dass Mitarbeiter die sozialen Medien frei verwenden und für den Benefit Ihres Unternehmens nutzen können. Über die detaillierten Reporting- und Audit-Funktionen kann analysiert werden, wie die Informationen im Unternehmensnetzwerk genutzt werden. Mit diesen Erkenntnissen können sich Organisationen effektiv vor eingehenden Bedrohungen schützen, Datenlecks verhindern und einen produktiven Einsatz Ihrer Netzwerk-Ressourcen sicher stellen.

Sollten Sie Datenlecks über Facebook, Webmail oder ähnliche Seiten befürchten, können Sie den Zugriff darauf zwar erlauben, den Datenfluss nach draußen aber durch Richtlinien zur Überprüfung und Bereinigung kontrollieren oder verhindern. YouTube enthält möglicherweise unsachgemäße Inhalte – deshalb können Sie die Nutzung auf zulässige Videos beschränken. Die granular einstellbaren Richtlinien des Clearswift SECURE Web Gateway helfen Ihnen, Datenverluste und Rechtsstreitigkeiten zu vermeiden, Reputationsrisiken zu entschärfen und die Einhaltung gesetzlicher Vorgaben zu sichern.

Vordefinierte reguläre Ausdrücke für PII (Personally Identifiable Information) und PCI (Payment Card Industry)

- Nationale Versicherungs- und ID-Nummern
- Kreditkartennummern
- Sozialversicherungsnummern
- International Bank Account Number (IBAN)

Anpassbare Compliance-Wörterbücher

- Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Securities and Equities Commission (SEC) and Sarbanes Oxley (SOX)

Kontextbezogene Policies für Facebook und andere Web-2.0-Seiten

- Schutz vor eingehenden Bedrohungen
- Verhindern von Datenlecks, die durch Kommunikation nach außen entstehen.
- Spezielle Facebook-Regeln

Diese intuitive und leistungsstarke Benutzerschnittstelle bietet eine einfache Aufgabenverwaltung, die Fehler vermeidet und Betriebskosten senkt.

Schutz vor eingehenden Bedrohungen

Das SECURE Web Gateway enthält Anti-Virus-, Anti-Malware- und Anti-Spyware-Schutz von Kaspersky oder Sophos, die sich automatisch updaten und so den aktuellsten Schutz gewährleisten.

Diese Technologien werden durch die MIMEsweeper Content Inspection Engine noch weiter verbessert, die das Herunterladen verdächtiger Scripts, ausführbarer Malware und anderer gefährlicher Inhalte verhindert. Mehr noch: Aktive Inhalte können in Dokumenten und HTML-Code erkannt und auf Wunsch entfernt werden.

Texte in Web-Inhalten können durchsucht, entsprechend dem Kontext oder der Kommunikationsrichtung analysiert und anschließend einer Richtlinie folgend behandelt werden.

- **URL:** Unsachgemäße Recherchen verhindern oder diese mit Benachrichtigung z.B. der Personalabteilung erlauben.
- **Dokumente:** Hochladen vertraulicher Daten auf Web-2.0-Seiten oder über Webmail verhindern.
- **Web-Seiten:** Seiten mit anstößigen Inhalten blockieren.
- **HTTP-Header:** Veraltete und nicht zulässige Browser-Versionen werden blockiert.

Erweiterte URL-Filterung

Die Clearswift-URL-Datenbank enthält 84 Kategorien und wird täglich aktualisiert. Sie deckt Millionen von URLs und Milliarden von einzelnen Webseiten ab. Außerdem enthält sie eine weitere, stündlich aktualisierte Datenbank mit Malware- und Phishing-Signaturen.

Kategorisierung in Echtzeit

Diese Funktion findet neue fragwürdige Sites, Remote Proxies, Pornografie und Hacking, die täglich neu auftauchen können. Die Kategorisierung in Echtzeit ist darauf ausgelegt, die Charakteristika solcher Seiten zu erkennen und den Zugriff darauf zu verhindern.

Surfzeit und Quoten-Policies

Ausgereifte Richtlinien erlauben sowohl die Festlegung von Uhrzeiten als auch von Gesamtzeiten pro Tag, die ein User beim Surfen in einer bestimmten Kategorie verbringen darf.

Flexible Einsatzoptionen

Sie entscheiden, wie Sie das Clearswift SECURE Web Gateway kaufen und einsetzen. Es ist entweder als vorinstallierte Hardware Appliance, als Software-Image, das auf unterschiedlichen Hardware-Plattformen installiert werden kann oder in virtualisierter Form in einer VMware-Umgebung verfügbar.

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

Clearswift hat seinen Firmensitz in Großbritannien und unterhält weitere Standorte in Europa, im Raum Asien-Pazifik und den USA. Clearswift hat ein Netzwerk mit mehr als 900 Vertriebspartnern weltweit.

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

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17
40 Mount Street
North Sydney
New South Wales, 2060
AUSTRALIA

Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1210
Email: info@clearswift.com.au

Deutschland
Clearswift GmbH
Im Mediapark 8
D-50670 Köln
Deutschland

Tel: +49 (0) 221 8282 9888
Technical Support: +49 (0)800 1800556
Email: 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
Technical Support: 0800 100 0006
Email: info.jp@clearswift.com

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

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

clearswift
RUAG Cyber Security

Feature	Benefit
Richtlinien	
Flexible und granulare Richtlinienkontrollen	Einfaches Definieren von Richtlinien um die Verwendung von Web 2.0 zu ermöglichen. Gleichzeitige Risikominimierung
Richtlinien für Facebook, LinkedIn, Twitter und YouTube.	Erlauben Sie den Zugriff auf Web 2.0-Sites aber nur auf richtlinienkonforme Inhalte und Funktionen.
Zeit und Kontingente für die Zugriffsrechte pro Nutzer.	Definieren Sie zur Zugriffsbegrenzung Uhrzeiten oder Nutzungskontingente für bestimmte Websites.
Policies getrennt für Inbound und Outbound	Unterbinden Sie das Hochladen bestimmter Dateitypen wie etwa Tabellenkalkulationen, erlauben Sie jedoch deren Herunterladen.
„Info"-Seiten zum genehmigten Zugriff	„Info-Seiten" machen klar, dass das Surfen auf bestimmten Seiten überwacht wird und den Firmenrichtlinien unterliegt.
Hygiene	
Bi-direktionales Virus- und Anti-Malware-Scanning	Hindert bekannte und unbekannte Malware daran, in das Unternehmensnetzwerk einzudringen
Bi-direktionales Anti-Spyware-Scanning	Stoppt Spyware, Adware, Key-Logger und Spyware Call-Homes sowie infizierte Rechner.
URL-Filter-Datenbank mit 84 Kategorien	Verhindert Zugriff auf unsachgemäße Webseiten und liefert Kontext für Websurf-Reports.
Malware-, Phishing- und Spyware-Kategorien	Verhindert den Zugriff auf bekannte, hochriskante URLs und Sites (Stündliche Updates)
Echtzeit-Kategorisierung	Verhindert den Zugang zu neuen oder unkategorisierten Sites mit unerwünschten Inhalten.
Contentabhängige Analyse bis zu 50 Ebenen tief	Verhindert das Herunterladen von .exe-Dateien (einschließlich ActiveX), auch wenn diese in anderen Dateitypen oder komprimierten Dateien eingebettet sind.
Structural Sanitization (Strukturelle Bereinigung)	Entfernung aller aktiven Inhalte wie Makros und Scripte aus Dokumenten oder HTML-Dateien.
Inhaltsanalyse (Content Inspection)	
MIMEsweeper – Identifikation „binärer Dateitypen	Genaue, signatur-basierte Identifikation mit der Möglichkeit, eigene Dateisignaturen zu definieren
Komplette HTTPS-Untersuchung und -Analyse	Einblick in verschlüsselten Datenverkehr zur Verhinderung von Malware und Sicherheitslücken
Lexikalische Analyse und reguläre Ausdrücke	Durchsuchen von Kommunikationsdaten nach Stichwörtern und Wortkombinationen aus einfachen Ausdrücken oder nach komplexen Datenmustern aus regulären Ausdrücken, Bool`schen Operatoren und regionalen Suchbegriffen. Erstellung von Tokens für komplexe Suchprofile, zur Verringerung von False-Positives und zum Vergleich mit strukturierten Datenquellen.
Adaptive Redaction	Automatisches Bereinigen oder Unkenntlich-Machen von Texten nach typischen vordefinierten Stichwörtern oder Tokens. Entfernen unerwünschter oder vertraulicher Datei-Verlaufsinformationen wie z. B. spezifischer (schädlicher) Dateieigenschaften. Erkennung aktiver Inhalte und Entfernen von deren Spuren.
Vordefinierte Templates für vertrauliche Daten	Identifikation von Kreditkarten-, Bankkonto-, Sozialversicherungs- und persönlichen ID-Nummern sowie ähnlichen Nummernfolgen.
Compliance-Wörterbücher	Mehrsprachige Wörterbücher für obszöne Ausdrücke sowie bearbeitbare Compliance-Wörterbücher wie z.B. GLBA, HIPAA, SEC, SOX, PCI und PII zur Verringerung von Terminologierisiken und Reputationsverlusten.
Management und Reporting	
Intuitive, web-basierte Oberfläche	Bequeme Verwendung ohne Notwendigkeit zum Lernen komplexer Syntax oder Linux-Befehle.
Vordefinierte, benutzerdefinierbare Reports	Bequeme Modifikation, Ausführung und gemeinsame Nutzung graphischer Reports mit intuitivem Drill-Down.
Zeitgesteuertes Reporting	Ermöglicht einmalige Erstellung und vielfache Ausführung von Reports sowie ihre Verteilung per E-Mail.
konsolidiertes Reporting über mehrere Gateways	Konsolidiertes Reporting von Benutzeraktivitäten zur bequemeren Analyse und gemeinsame Nutzung von Verwaltungsdaten.
„Active Directory (AD)"- und LDAP-Integration	Volle nutzerbasierte Kontrolle für flexibles Richtlinien- und Audit-Reporting nach Gruppen oder Einzelpersonen.
Planmäßiges Spyware-Reporting	Bessere Kontrolle von Spyware mit Identifikation der Endgeräte, die eine Aktion am Gerät erfordern.
SNMP-, SMTP- und SYSLOG-Alarmierung	SNMP- bzw. SMTP-Management-Benachrichtigungen erleichtern die Nutzung von Datenzentren während der Nachtzeiten sowie die automatische Konsolidierung von LOG-Dateien per SYSLOG.
SECURE HTTP Caching Proxy	Bereitstellung entweder als vorinstallierte Hardware-Appliance, als Software-Image oder in virtualisierter Form auf VMware.