CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Clearswift Information Governance

Information Governance und Adaptive Redaction

Inhalt

Zusammenfassung

Information Governance ist ein weitreichender Begriff. Es geht dabei um Richtlinien und Prozesse für die effiziente Verwaltung und Überwachung der Informationen eines Unternehmens im Rahmen der Erfüllung der gesetzlichen Vorgaben. Im Mittelpunkt steht das Bedürfnis, die im Unternehmen vorhandenen Informationen zu verstehen, um diese entsprechend zu schützen. Bisher bestand dieser Schutz aus Data Loss Prevention-Lösungen (DLP). Diese Lösungen basieren auf Content Inspection und nutzen Richtlinien um zu entscheiden, ob eine Information das Unternehmen verlassen darf oder nicht – ein Schwarz/Weiß-Ansatz der Informationen stoppt oder sperrt.

Adaptive Redaction ist DLP der nächsten Generation und ermöglicht die automatische Anpassung von Inhalten basierend auf Richtlinien. So wird die Unternehmenskommunikation nach außen gewährleistet, ohne dass kritische Informationen abfließen können.

Adaptive Redaction ist in die Clearswift-Technologie integriert und als lizensierbare Option erhältlich.

Einleitung

Die Clearswift SECURE Information Governance Platform (SIGP) erzeugt ein System für die Überwachung und Verwaltung von Informationen, während diese innerhalb eines Unternehmens oder über dessen Grenzen hinaus versendet werden. Sie basiert auf den SECURE Gateway-Produkten und verfügt über ein zugehöriges SDK, das die Integration von Anwendungen und Lösungen von Drittanbietern ermöglicht.

Dieses White Paper beschreibt die neuen Funktionen in der aktuellen Version der SECURE Gateways – Adaptive Redaction. Adaptive Redaction basiert wie alle Produkte von Clearswift auf der Deep Content Inspection-Technology.

Deep Content Inspection

Clearswift ist seit über zehn Jahren führend im Bereich Deep Content Inspection (DCI). Im Gegensatz zu seinen Wettbewerbern verfügt Clearswift über die Technologie, Informationen aus Dateien selbst zu extrahieren, anstatt sich hierfür auf Komponenten von Drittanbietern zu verlassen. Dadurch bietet sich die einzigartige Möglichkeit, nicht nur den Text aus einer Datei zu extrahieren, sondern auch Informationen aus der Datei zu entfernen oder zu ersetzen und eine geänderte Datei zu erzeugen. Diese integrierte DCI-Technologie macht Adaptive Redaction erst möglich.

Die DCI Engine ist der Kern der führenden Produkte von Clearswift, den SECURE Gateways.

Clearswift SECURE Gateways

Die Clearswift SECURE Gateways haben sich seit mehr als zehn Jahren weltweit bei einer Vielzahl großer und kleiner Unternehmen bewährt. Es gibt drei verschiedene Gateways für E-Mail, Web und Dateiübertragung. Diese können als Appliance, in einer virtuellen Maschine oder als einfache Software installiert werden. Die Gateways bieten eine für alle IT-Umgebungen passende Implementierung.

Auch wenn Adaptive Redaction eine wichtige Information Governance-Funktion ist, der Erwerb des Clearswift SECURE Information Governance Server (SIGS) ist nicht unbedingt erforderlich. Adaptive Redaction wird in den Gateways implementiert und ist so mit allen Gateway-Produkten verfügbar.

Adaptive Redaction

Adaptive Redaction (AR) ist ein Überbegriff für alle Methoden zur Änderung der Informationen in einer Datei.

Es gibt vier verschieden Methoden für AR:

- Text-Redaction
- Document Sanitization
- Structural Sanitization
- Verschlüsselung

Bei der Untersuchung eines Dokuments werden alle Aspekte dieses Dokuments erfasst, so dass ein richtlinien-basiertes Entfernen von sensiblen Informationen und Ersetzen durch Platzhalter, zum Beispiel durch „X“ möglich ist. Danach wird das Dokument erneut zusammengefügt.
Für besonders sicherheitsbewusste Unternehmen: Sensible Informationen können aus dem neuen Dokument entfernt werden, d. h. sie werden nicht nur versteckt und verbleiben in den Eigenschaften oder in einem Kommentar.

Text-Redaction

Text-Redaction oder Textredaktion bezeichnet das Entfernen von Informationen aus einer Datei oder Webseite. Dies kann ein einzelnes Wort oder ein Ausdruck sein, aber auch ein komplexer Token wie eine Kreditkartennummer. Die Redaktion von Text, insbesondere in gedruckten Dokumenten, wird häufig als „Schwärzen“ bezeichnet.

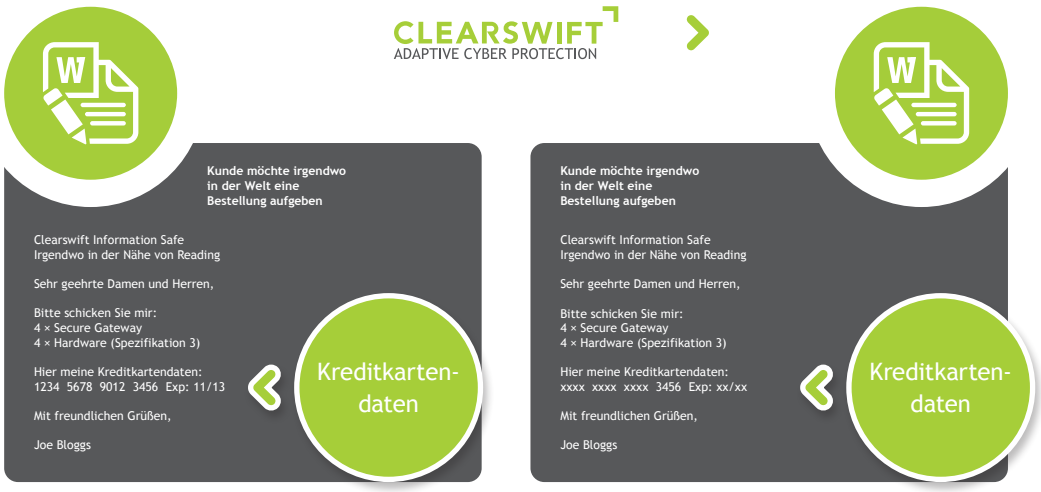

Abbildung 1: Textredaktion, Entfernen sensibler Informationen

Fallbeispiel (ausgehend):

Einfaches Ersetzen sensibler Wörter oder Ausdrücke, z. B. Wörter des M&A Code.

Fallbeispiel (ausgehend):

Ersetzen von Tokens wie Ausweisnummer oder Sozialversicherungsnummer.
In diesem Fall wurde eine Kreditkartennummer ersetzt, die Nummer kann bis auf die letzten vier Stellen durch „X“ ersetzt werden.

Fallbeispiel (eingehend):

Soziale Netzwerke mit Unternehmensseiten, die auf Grund von Obszönitäten in Kommentaren gesperrt werden, können dank der automatischen Redaction anstößiger Wörter sicher betrachtet werden.

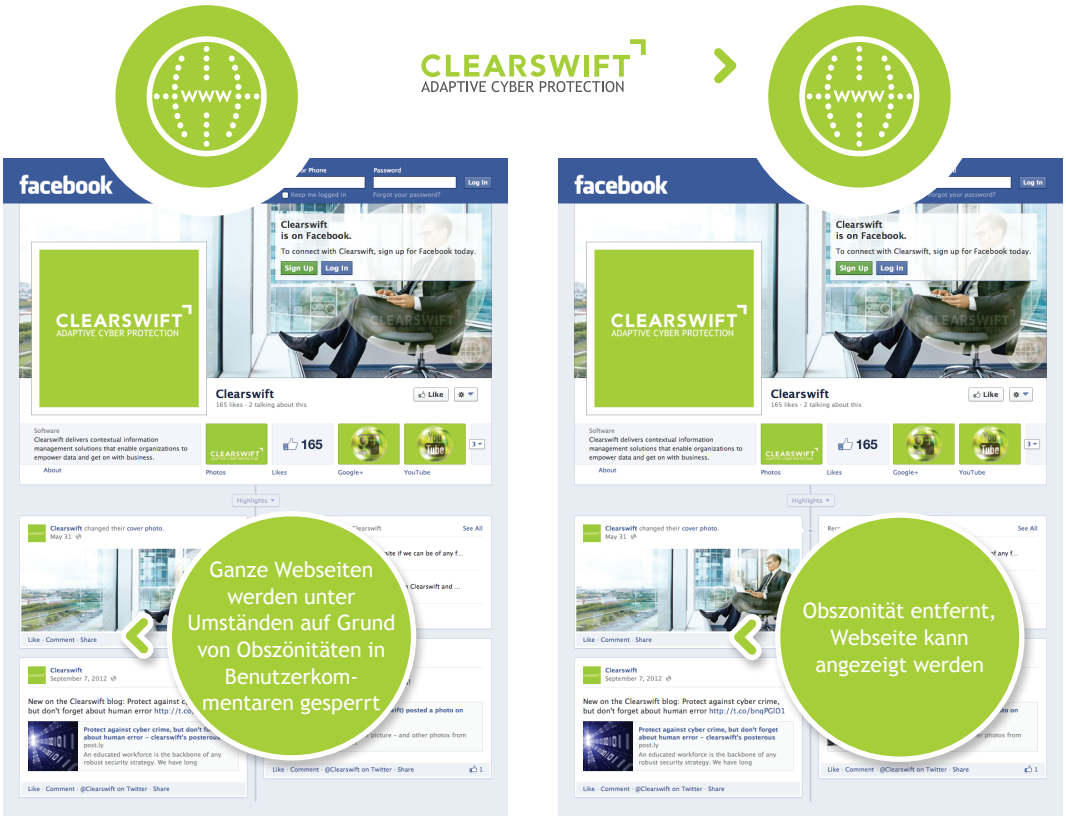

Abbildung 2: Textredaktion zum Entfernen von Obszönitäten auf Webseiten

Data Loss Prevention der nächsten Generation

Aus Sicht der Data Loss Prevention (DLP) stellt Adaptive Redaction eine sichere Alternative zum „Stoppen und Sperren“ herkömmlicher Lösungen dar. Durch das automatische Entfernen von sensiblen Informationen, die zu einem Sperren der Informationsübertragung durch die DLP-Richtlinie führen, können die verbleibenden Informationen gesendet werden und einer reibungslosen Kommunikation steht nichts im Weg.

Fallbeispiel (eingehend):

Entfernen eingehender Kreditkartennummern. Vielen Unternehmen bereitet der Empfang von Kreditkartennummern Kopfzerbrechen. Text-Redaction stellt sicher, dass eine evtl. gesendete Kreditkartennummer nicht empfangen wird, und beseitigt so das Problem der Verwaltung der Nummer und des zugehörigen Dokuments.

Folgende Formate werden für die Text-Redaction unterstützt: Word/Excel/PowerPoint (Microsoft Office ab 2007), PDF, RTF, HTML und Textdateien.

Document Sanitization

Standardmäßige Office-Dokumente wie MS Office und PDF enthalten „unsichtbare“ Elemente mit Informationen wie Metadaten der Dokumenteigenschaften und Revisionsverlauf. Diese könnten für ein Unternehmen kompromittierend sein, wenn ein Dokument an ein externes Unternehmen geschickt wird. Neben den standardmäßigen Eigenschaften bieten viele Anwendungen auch die Möglichkeit, benutzerdefinierte Eigenschaften mit zusätzlichen Informationen zu erstellen, die beim Verlassen des Unternehmens ebenfalls zu Problemen führen können.

Auch wenn einige Anwendungen eine Möglichkeit zum Entfernen von Metadaten und Revisionsverlauf bieten, ist dies ein manueller Vorgang, der die Bedrohung nicht effektiv eliminiert. Der Benutzer muss immer daran denken, die Informationen aktiv zu entfernen. Aufgrund einer Vielzahl bekannt gewordener Fälle, in denen Empfänger durch Untersuchen der versteckten Daten zusätzliche Informationen aufdecken konnten, ist es in vielen Branchen, insbesondere im öffentlichen Sektor mittlerweile Pflicht, diese sensiblen Informationen zu entfernen. Dies ist zwar gesetzlich vorgeschrieben, wurde in der Vergangenheit aber auf Grund des Fehlens automatisierter Tools nicht immer so umgesetzt.

Document Sanitization bezeichnet das automatische, richtlinien-basierte Entfernen der Metadaten und des Revisionsverlaufs. Damit wird die Gefahr versehentlicher Datenlecks verringert und den neuen Richtlinien zur Information Governance Rechnung getragen, die im Zusammenhang mit dem Entfernen „versteckter“ Informationen aus Dokumenten, die nach außerhalb des Unternehmens verschickt werden, erfüllt werden müssen.

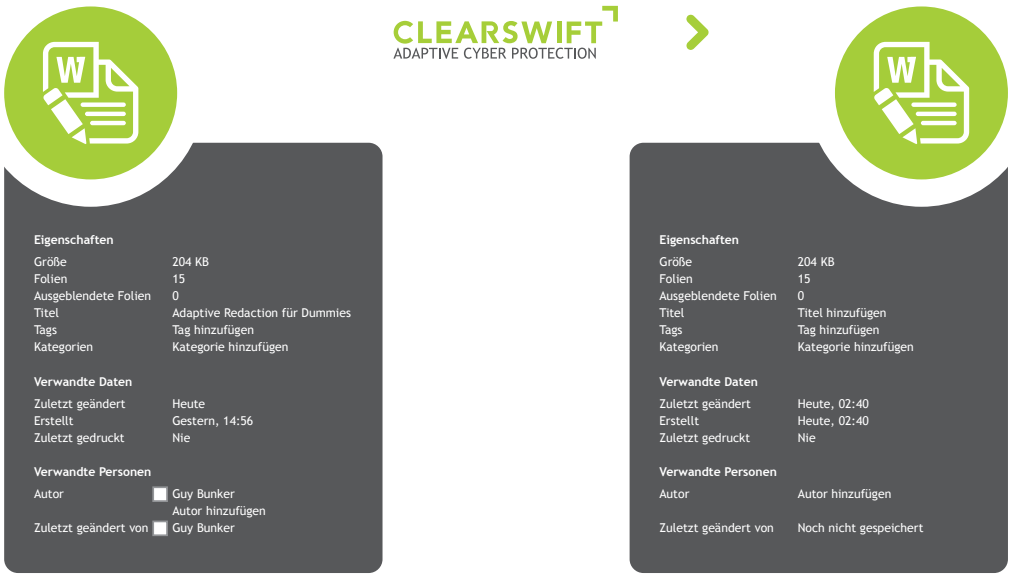

Abbildung 3: Document Sanitization, Entfernen von Metadaten

Word-Dokumente können auch während der Lebensdauer des Dokuments mit der Funktion „Änderungen verfolgen“ erstellte Revisionen enthalten. PDF-Dateien bieten eine Option zum Schnellspeichern, bei der ebenfalls der Revisionsverlauf im Dokument verbleibt. Dieser Verlauf ist oft blamabel für ein Unternehmen, falls beim Veröffentlichen des Dokuments veraltete Inhalte aufgerufen werden können. Bei den Daten handelt es sich häufig um Preise oder andere, nicht zur Veröffentlichung taugliche Inhalte.

Fallbeispiel (ausgehend):

Entfernen aller Metadaten, so dass unternehmensspezifische Informationen wie z.B. Namen von Autoren oder interne Abteilungs- bzw. Projektbezeichnungen das Unternehmen nicht verlassen.

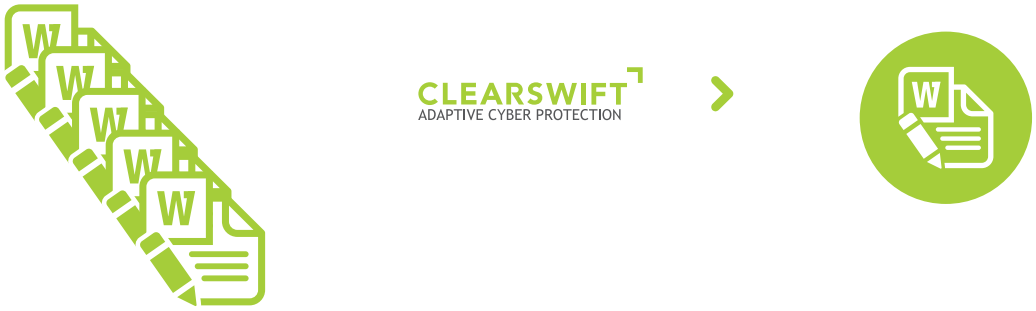

Abbildung 4: Document Sanitization, Entfernen von Versionsinformationen

Unternehmen, die diese Informationen entfernen möchten, setzen für das Bereinigen eine Anwendung von Drittanbietern ein oder verlassen sich auf die in Office-Produkten integrierten Funktionen. Dies kann zwar wirksam sein, ist jedoch ein benutzergesteuerter Prozess und kann deshalb vergessen oder innerhalb des Unternehmens inkonsistent gehandhabt werden. Mit der Implementierung auf einem serverseitigen Gerät ist die konstante Einhaltung der Richtlinie gewährleistet und es ist keine zusätzliche Schulung für Desktop-Anwendungen erforderlich.

Fallbeispiel (ausgehend):

Entfernen aller Versionsinformationen aus ausgehenden Angebotsdokumenten, so dass keine alten Versionen mit unter Umständen abweichenden Angaben aus anderen Angeboten oder deutlich anderen Preisen herausgegeben werden.

Folgende Funktionen werden unterstützt:

- Entfernen aller oder ausgewählter Gruppen der Dokumenteigenschaften, einschließlich benutzerdefinierter und sogar „unerwarteter “ (oder fehlerhafter) Eigenschaften in der falschen Eigenschaftsgruppe.
- Entfernen aller verfolgten Änderungen oder Daten der Schnellspeicherung aus Word- und PDF-Dateien.

Folgende Formate werden für die Daten-Sanitization unterstützt: Word/Excel/PowerPoint (Microsoft Office ab 2007), PDF und HTML.

Structural Sanitization

Auf Grund der ständig wachsenden Gefahr von Malware in häufig verwendeten Dateiformaten wurden die Gateways nicht nur erweitert, um aktive Inhalte zu erkennen, sondern es wurde auch eine Option hinzugefügt, mit der alle aktiven Inhalte aus dem ursprünglichen Format entfernt werden können.

Abbildung 5: Structural Sanitization zum Entfernen aktiver Inhalte aus Dokumenten

Die strukturelle Sanitization unterstützt das Erkennen und Entfernen verschiedener Typen aktiver Inhalte aus verschiedensten Dateitypen. VBA-Makros in Microsoft Office-Dokumenten, PowerPoint-Dateien und Tabellenkalkulationen werden erkannt und entfernt. Bei HTML-Dokumenten und bei Anhängen werden JavaScript-, VB Script- und ActiveX-Inhalte entfernt. Bei PDF-Dokumenten können sowohl JavaScript- als auch ActiveX-Komponenten entfernt werden.

Fallbeispiel (eingehend):

Entfernen aller aktiven Inhalte aus per E-Mail oder über das Internet erhaltenen Dateien, um die Gefahr einer Malware-Infizierung zu verringern.

Strukturelle Überprüfung (Structural Validation)

Adaptive Redaction bezeichnet auch die Möglichkeit, die Dateistruktur zu überprüfen. Eine heutzutag oft gesehene Methode für einen Malware-Angriff oder um Daten aus einem Unternehmen abzuziehen, ist das Anhängen der Informationen an das Dateiende. Für eine Vielzahl von Dateitypen kann eine Überprüfung durchgeführt werden, um sicherzustellen, dass das nicht der Fall ist. Dies wird als strukturelle Überprüfung bezeichnet. Werden zusätzliche Informationen gefunden, kann der Inhalt entsprechend der Unternehmensrichtlinien gesperrt werden.

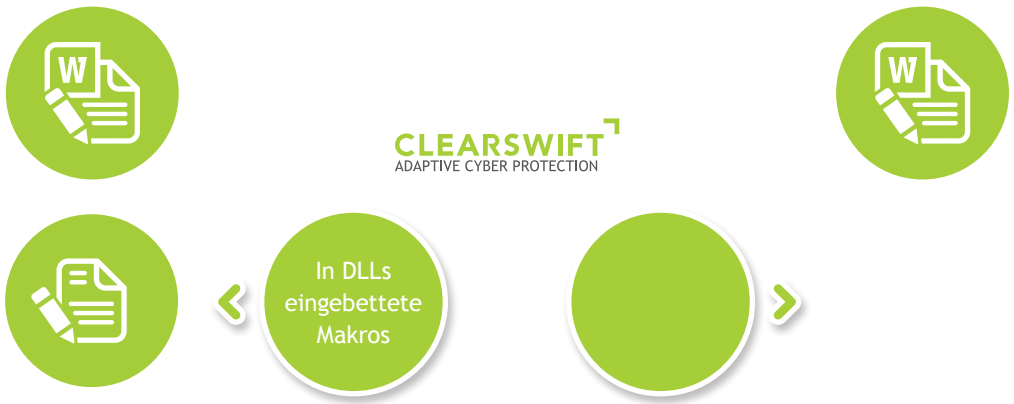

Abbildung 6: Structural Sanitization, Entfernen von in Dokumenten versteckten Informationen

Für die strukturelle Überprüfung unterstützt werden Microsoft Office-Dokumente (alle Versionen) und Open Office-Dokumente sowie eine Vielzahl weiterer Formate.

Verschlüsselung

Verschlüsselung ist bereits seit mehreren Jahren eine lizenzierbare Option unserer Gateways, und es werden mehrere voll automatisierte, richtlinien-basierte Verschlüsselungsmethoden unterstützt:

- S/MIME / PGP – erfordert unter Umständen einen Schlüssel oder ein Plug-In
- Ad-hoc-Verschlüsselung mit Kennwort (Windows)
- Ad-hoc-Verschlüsselung mit Kennwort (AES) – erfordert die Installation eines ZIP-Pakets für die AES-Unterstützung.

Abbildung 7: Richtlinien-basierte Verschlüsselung von Dokumenten

Die Verschlüsselungsfunktion fällt unter die Kategorie Adaptive Redaction, da die Form der Informationen automatisch auf dem Weg zum Empfänger geändert (verschlüsselt) wird. Der Inhalt der Informationen wird aber nicht entfernt oder geändert, nur die Datei wird geändert.

Hinweis: TLS (Transport Layer Security) wird im Email Gateway standardmäßig unterstützt, dies ist jedoch keine Änderung der Form der Informationen, sondern es wird ein verschlüsselter Kommunikationskanal genutzt

Fallbeispiel:

Sichere Übertragung von Informationen außerhalb des Unternehmens.

Warum Adaptive Redaction?

„Adaptive“ bei Adaptive Redaction beschreibt die Tatsache, dass alle durchgeführten Aktionen richtlinien-basiert angepasst werden können. Eine Richtlinie kann für alle Anwender gelten, beispielsweise das Entfernen von Metadaten, kann aber auch individuell unterschiedlich definiert sein. Auf eine an zwei Empfänger gesendete E-Mail mit Anhang können also zwei verschiedene Methoden der Adaptive Redaction angewendet werden. Ein Empfänger erhält beispielsweise den ganzen Inhalt einer Datei, jedoch verschlüsselt, während der andere eine Datei erhält, bei der mit Hilfe von Adaptive Redaction Teile der Informationen entfernt wurden.

Abbildung 8: Adaptive Redaction bietet verschiedene Ansichten derselben Informationen abhängig vom Empfänger

Die wirtschaftliche Seite von Information Governance

Adaptive Redaction ist eine innovative, neue Technologie. Heutzutage wird jedoch mehr als nur eine Technologie um der Technologie Willen benötigt – es müssen wirtschaftliche Vorteile erkennbar sein. In diesem Fall ist dies Information Governance. Information Governance, oder IG, bezeichnet die Evolution von Informationssicherheit[1], die alle Aspekte im Zusammenhang mit Unternehmensinformationen umfasst. Bei vielen modernen Unternehmen ist eine Lücke zwischen dem Verständnis der Bedeutung ihrer Informationen und deren Schutz erkennbar. Ohne Verständnis der Informationstypen in einem Unternehmen sind diese nur äußerst schwer zu überwachen, zu verwalten und zu kontrollieren. Eine umfassende IG-Strategie beginnt bei den Informationen – um welche Informationen handelt es sich, und was ist deren Bedeutung. Der nächste Schritt bei der Klassifizierung der Informationen beginnt mit der Überlegung, wie diese geschützt werden. Bevor ein wirksamer Schutz eingerichtet werden kann, muss bestimmt werden, „wo" die Informationen vorgehalten werden, z.B. in einem Datenzentrum, auf einem Smartphone, oder überall.

IG verfolgt einen umfassenden Ansatz und berücksichtigt die Lebensdauer der Informationen sowie Mitarbeiter, Prozesse und Disziplinen, die die Informationen nutzen. Compliance, ob Einhaltung gesetzlicher Vorgaben oder von Richtlinien, ist eine wichtige Komponente. Es gibt eine Vielzahl gesetzlicher Vorschriften, deren Hauptziel es jedoch immer ist, sicherzustellen, dass unternehmenskritische Informationen sicher sind. Wir sehen heute einen Wandel. Es sind nicht mehr nur Informationen wie Kreditkarten- und Bankdetails in Verbindung mit persönlichen Daten zu schützen, sondern auch geistiges Eigentum sowie weitere vertrauliche Unternehmens-informationen. Im Zentrum der IG stehen das Verstehen der Informationen und Kommunikationsströme sowie der ultimative Schutz der Informationen. Auf Grund der ständigen Veränderung von Geschäftsmethoden ist dies eine immer komplexer werdende Herausforderung. Egal ob vermehrte Zusammenarbeit, „Bring Your Own Device" (BYOD) oder die Nutzung Cloud-basierter Services, stets werden Informationen aus der Kontrolle eines Unternehmens nach außen gegeben. Data Loss Prevention-Lösungen (DLP) bieten zwar eine Möglichkeit zu verhindern, dass unangemessene Inhalte das Unternehmen verlassen, sie stehen aber meist auch dem täglichen Geschäftsablauf im Weg. Mit Adaptive Redaction entfällt diese Einschränkung, da sensible Informationen automatisch basierend auf Richtlinien entfernt werden und so ein reibungsloser Geschäftsablauf garantiert ist.

Zusammenfassung

In unserer durch vermehrte Zusammenarbeit und soziale Medien geprägten Welt, bedeutet eine Verzögerung der Kommunikation eine Verzögerung Ihres Geschäfts. Clearswift Adaptive Redaction ist eine neuartige Lösung für ein altbekanntes Problem – Verhindern, dass versteckte oder vertrauliche Informationen versehentlich das Unternehmen verlassen. Adaptive Redaction bietet auch eine Möglichkeit, das Problem des herkömmlichen Ansatzes „Stoppen und Sperren" einer Data Loss Prevention-Lösung zu umgehen und Inhalte, die nicht den Unternehmensrichtlinien entsprechen, automatisch zu entfernen. Nicht zuletzt bietet sie die Möglichkeit, potenziell schädliche aktive Inhalte aus Dokumenten zu entfernen, bevor ein Benutzer diese öffnet.

Adaptive Redaction von Clearswift umfasst eine Reihe separat lizenzierbarer Optionen für den Clearswift SECURE Email Gateway und den Clearswift SECURE Web Gateway, Schlüsselkomponenten der Information Governance-Strategie eines Unternehmens.

[1] Information Governance ist abgeleitet von „Data Protection", was sich zu „Information Security" und dann zu „Information Assurance" entwickelt hat, bevor es schließlich als „Information Governance" bezeichnet wurde.

Über Clearswift

Clearswift ist ein Anbieter von Lösungen für Informationssicherheit. Weltweit vertrauen mehrere Tausend Kunden auf unsere adaptiven Cyber-Lösungen zum Schutz ihrer unternehmenskritischen Daten vor internen und externen Bedrohungen.

Basierend auf einer innovativen Deep Content Inspection Engine und verwaltet und gesteuert durch ein vollintegriertes Richtlinienportal unterstützen die Lösungen von Clearswift eine umfassende Information Governance-Strategie und so die einfache und problemlose Verwaltung und den Schutz der Daten.

Als globales Unternehmen unterhält Clearswift Standorte in Europa, Australien, Japan und den USA.

Clearswift hat ein Partnernetzwerk mit mehr als 900 Vertriebspartnern weltweit.

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

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

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
Email: info@clearswift.com

Australia

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
Email: info@clearswift.com.au

Deutschland

Clearswift GmbH
Landsberger Straße 302
80687 München
Deutschland

Tel: +49 (0)89 904 05 206
Technischer 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
Technischer Support:
0066 33 812 501
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
Tel (Toll Free): +1 888-937-7938
Technischer Support:
+1 856 359 2170
Email: info@us.clearswift.com