clearswift
by HelpSystems

DATENBLATT *(Cybersicherheit)*

Verschlüsselung mit Secure Email Gateway

Eine Komponente der Clearswift Adaptive Redaction-Technologie: Information Governance der nächsten Generation im Einsatz.

Was ist Verschlüsselung?

Verschlüsselung, die bidirektionale Umwandlung von offenem Inhalt in kryptographierten Inhalt, ist das absolut leistungsstärkste Sicherheitstool, das einem Administrator zu Verfügung steht. Verschlüsselung alleine erfüllt zwei der drei Sicherheitsgrundsätze („CIA“) und ermöglicht den dritten. Sie garantiert die Vertraulichkeit (Confi dentiality) von Unternehmensdaten, stellt die Integrität (Integrity) von Unternehmensdaten sicher und ermöglicht durch eine sichere Speicherung die Verfügbarkeit (Availability) der Unternehmensdaten. Bei korrekter Verwendung gibt es für Angreifer keine Möglichkeit, eine moderne Verschlüsselung zu knacken. Verschlüsselung ist ein grundlegender Bestandteil des Data Loss Prevention (DLP) Toolkit.

Die Bedeutung von Verschlüsselung

Verschlüsselung garantiert die Sicherheit von Unternehmensdaten auch, wenn ein System verletzt wird und sogar wenn Daten gestohlen werden.

Verschlüsselung ist zudem für die Erfüllung einer ständig steigenden Anzahl rechtlicher und regulatorischer Vorschriften zum Schutz personenbezogener Daten erforderlich. In vielen dieser Vorschriften ist festgehalten, dass verlorene Daten nicht als verloren gelten – egal wer im Besitz der Daten ist – wenn diese verschlüsselt sind.

Verschlüsselung bietet also Sicherheit für das Unternehmen und gewährleistet die Einhaltung der Rechtsvorschriften.

Die Bedeutung automatischer Verschlüsselung

Verschlüsselung hat einen großen Nachteil: sie ist oft zu schwierig zu implementieren oder zu kompliziert in der Anwendung.

Nur eine vollautomatische Verschlüsselung – wie sie mit dem Secure Email Gateway möglich ist – bietet die Voraussetzungen für eine vertrauenswürdige, umfassende, konsistente und kosteneffiziente Datenverschlüsselung.

Die Clearswift Gateway-Verschlüsselungsfunktion

SECURE Email Gateway sichert Daten am Ausgangspunkt entsprechend der vorgegebenen Richtlinie.
Alle sensiblen Daten können automatisch verschlüsselt werden, sobald diese nach außerhalb des

Unternehmenssystems versendet werden, egal ob als E-Mail oder als Inhalt eines Anhangs.

Die intelligente Verschlüsselungsrichtlinie kann auf Absender, Empfänger, Betreff, Inhalt, Nachrichtentext, Typ des Anhangs, Inhalt des Anhangs oder Attributen des Nachrichtenheaders basieren. Wörterbücher mit PII-Daten wie Nummern von Bankkarten, Sozialversicherungsnummern, Vorlagen für IBAN-Codes usw. sind integriert, um die Einhaltung der Rechtsvorschriften zu gewährleisten. Bei Erkennung einer Vorlage wird der Inhalt verschlüsselt.

Verschlüsselungsoptionen

Secure Email Gateway bietet eine Vielzahl verschiedener Verschlüsselungsverfahren, so dass der Anwender die für ihn am besten geeignete Methode auswählen kann. TLS ist Standard und geeignet, wenn eine Verschlüsselung nur zwischen dem eigenen und anderen bekannten Unternehmen erforderlich ist.

Portalbasierte Verschlüsselung ist eine Option, falls eine allgemeinere sichere Kommunikation mit Unternehmen erforderlich ist, die entweder andere oder keine Verschlüsselungsverfahren einsetzen. Hierbei wird ein gehostetes Verschlüsselungsportal verwendet, das als „Pick-up Center“ dient.

Eine weitere Option ist die Verwendung der PGP- und S/MIMEVerschlüsselung mit öffentlichen Schlüsseln, falls eine stärkere Verschlüsselung erforderlich ist. Dies kann für die Kommunikation zwischen Empfängern mit standardmäßigen E-Mail Clients wie Outlook, Outlook Express und Notes verwendet werden und ermöglicht die Erstellung richtlinienbasierter Verbindungen zwischen Gateways oder von Gateways zu Empfängern.

Adaptive Redaction

Verschlüsselung ist eine Funktion der Clearswift Adaptive Redaction-Technologie. Adaptive Redaction ist das intelligente Entfernen oder Ändern von Informationen in einem Dokument, um sicherzustellen, dass der Inhalt die Informationssicherheitsrichtlinien des Unternehmens erfüllt. Die Kombination aus automatischem Entfernen versteckter Inhalte (Sanitization) und dem Entfernen sensibler Inhalte (Redaction) ermöglicht Data Loss Prevention- und Information Governance-Lösungen der nächsten Generation.

Falls keine vollständige Verschlüsselung erforderlich ist, aber einige Inhalte dennoch versteckt werden sollen, kann alternativ eine der anderen Clearswift Adaptive Redaction-Funktionen verwendet werden. Dabei wird nicht das gesamte Dokument verschlüsselt, sondern sensible Inhalte werden vor dem Versenden nach außerhalb des Unternehmens entfernt.

Siehe die anderen Clearswift Adaptive Redaction-Datenblätter für weitere Details.

Verschlüsselung – Zusammenfassung

Verschlüsselung ist ein leistungsstarkes Tool sowohl für die Unternehmenssicherheit als auch für die Einhaltung der Rechtsvorschriften. Secure Email Gateway bietet eine Vielzahl von Optionen für alle Verschlüsselungsanforderungen sowie eine automatische, richtlinienbasierte, transparente Verschlüsselung über das gesamte Unternehmen.

Die neue FIPS-Option

Bei der Installation des Email Gateways existiert eine Option zur Einrichtung im FIPS (Federal Information Processing Standards) Modus. Die Aktivierung des FIPS Modus stellt sicher, dass alle verwendeten Verschlüsselungsarten mit den Normen der USRegierungsbehörden kompatibel sind. Damit dies geschehen kann, werden die Optionen zur Ad-hocund PGP-Verschlüsselung deaktiviert und von der Benutzeroberfl äche entfernt.

clearswift
by HelpSystems

www.clearswift.de

Über HelpSystems

HelpSystems ist ein Softwareunternehmen, in dem die Menschen an erster Stelle stehen. Getreu unserem Motto Build a Better IT TM unterstützen wir außergewöhnliche Unternehmen bei ihrer Arbeit. Unsere ganzheitliche Produktsuite aus Sicherheits- und Automatisierungslösungen schafft eine einfachere, intelligentere und leistungsstarke IT. Kunden in über 100 Ländern und in den unterschiedlichsten Branchen vertrauen auf HelpSystems. Erfahren Sie mehr unter www.helpsystems.com/de.