Data Leakage Prevention (DLP)

- Schutz der ausgehenden E-Mail-Kommunikation -

Expertise matters

Inhalt

1 Die unterschätzte Gefahr

Wer an E-Mail Sicherheit denkt, verbindet damit häufig nur Viren- und Spamschutz. Generell liegt in vielen Unternehmen der Fokus auf der eingehenden Kommunikation. Risiken, die bei unkontrollierter Kommunikation von innen nach außen lauern, werden nur selten wahrgenommen.

Die Praxis zeigt aber, dass gerade der Verlust von sensiblen Informationen, das arglose Versenden von personenbezogenen Daten und die Missachtung von Vorschriften, beispielsweise zum Schutz von Kundendaten, immer größere Probleme bereitet. Data Leakage Prevention (DLP) hat sich in diesem Umfeld zum Schlüsselbegriff entwickelt und prägt zunehmend die Entscheidungen in modernen Unternehmen. DLP ist dabei ein Kernthema bei datenschutzbezogenen Überlegungen und der Absicherung des eigenen Know-hows.

Bezogen auf die E-Mail-Kommunikation bedeutet dies, den E-Mail-Verkehr aus Prozesssicht zu betrachten. Es gilt Gefahren rechtzeitig zu erkennen, um pro-aktiv eingreifen zu können.

2 Maßnahmen für eine sichere, ausgehende Kommunikation

Mit der iQ.Suite steht eine Lösung zur Verfügung, die den gesamten E-Mail-Verkehr – eingehend wie ausgehend – auf vielfältige Weise schützt. Dabei werden sämtliche Aspekte aus betrieblicher wie auch rechtlicher Sicht berücksichtigt und in einem umfassenden Gesamtprozess abgebildet. Dieser durchgängige Ansatz vermeidet Bruchstellen in der E-Mail-Kommunikation und ermöglicht es überhaupt erst, eine zielgerichtete DLP-Strategie zu definieren und umzusetzen.

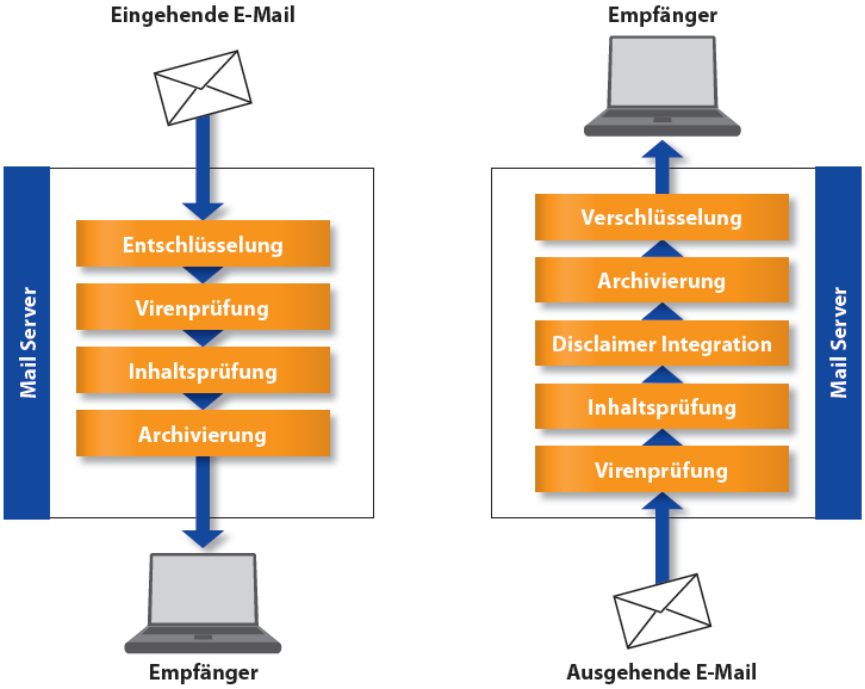

Abbildung 1: Kontrolle eigehender und ausgehender E-Mails

2.1 Kontrolle ausgehender Dateianhänge

Regelmäßig enthalten Dateianhänge sensible Informationen und Unternehmenswissen – seien es Angebote, Verträge oder beispielsweise Spezifikationen. Nicht immer ist der unkontrollierte Versand dieser Daten gewollt.

An dieser Stelle setzt die iQ.Suite mit einer auf elektronischen „Fingerprints“ basierenden Technologie an. Damit können Dateiformate unabhängig von ihrer Benennung zuverlässig erkannt werden. Derzeit werden out-of-the-Box über 300 Formate analysiert. Weitere Dateiformate lassen sich leicht hinzufügen. Damit bildet diese Technologie einen wichtigen Lösungsbaustein beim Schutz vertraulicher Daten.

2.1.1 Beispiel: Schutz von Konstruktionszeichnungen

Konstruktionszeichnungen enthalten oftmals wichtige technische Neuerungen oder auch patentrelevante Informationen. Sie spielen beispielsweise in der Automobil- oder Luftfahrtindustrie eine bedeutende Rolle. Die zugrundeliegenden Dateiformate (z.B. aus AutoCAD, CATIA, Pro/Engineer etc.) werden durch die iQ.Suite erkannt und entsprechend der organisatorischen Richtlinien verarbeitet. Diese Verarbeitung kann auf unterschiedliche Weise erfolgen und lässt sich an die individuellen Bedürfnisse des Unternehmens anpassen.

Hier einige Beispiele:

- Blocken dieser Dateiformate für alle ausgehenden E-Mails
- Definition von Ausnahmen für dedizierte Kommunikationskanäle
- Statistik über Häufigkeit der erkannten Restriktionen
- Report über erkannte Restriktionen an Dritte (z.B. Sicherheitsbeauftragten)
- Übergabe der E-Mail an eine automatische Verschlüsselung
- E-Mail-Information an betroffene Absender
- Vier-Augen-Prinzip für den Versand dieser Informationen

2.1.2 Beispiel: Versand elektronischer Rechnungen

Rechnungen verlassen Unternehmen schon lange nicht mehr nur auf dem postalischen Weg. Mittlerweile hat sich das Medium E-Mail als zuverlässiger und schneller Träger von Rechnungen erwiesen. Dabei kann es notwendig sein, den Versand dieser Rechnungen, die oftmals als PDF angehängt sind, intelligent zu steuern.

So können Dateitypen, wie beispielsweise Rechnung.pdf, durch die iQ.Suite erkannt und entsprechend definierter Regeln behandelt werden. Kommen E-Mails automatisch aus ERP-Systemen, so ist es möglich, diese über den Mail-Server oder ein SMTP-Gateway mit Hilfe der iQ.Suite zu verarbeiten.

Mögliche Aktionen bei der Erkennung dieser Dateiformate sind zum Beispiel:

- Blocken dieser Dateiformate für alle ausgehenden E-Mails
- Blocken kompletter E-Mails, die diese Dateiformate beinhalten
- Definition von Ausnahmen für dedizierte Kommunikationskanäle
- Statistik über Häufigkeit der erkannten Restriktionen
- Report über erkannte Restriktionen an Dritte (z.B. Sicherheitsbeauftragten)
- Übergabe der E-Mail an eine automatische Signierung
- E-Mail-Information an betroffene Absender
- Vier-Augen-Prinzip für den Versand dieser Informationen

2.2 Kontrolle ausgehender Textinhalte

Täglich werden per E-Mail Aufträge, Bestellungen, Rechnungen, Lieferbedingungen und Auftragsbestätigungen versendet. Diese Dokumente haben meistens rechtsverbindlichen Charakter und führen somit zu einer Haftung des jeweiligen Unternehmens.

Branchenspezifische Erfordernisse stellen zudem gesteigerte Anforderungen an den Schutz sensibler Inhalte: So gilt es beispielsweise im Gesundheitswesen die Sicherheit von Patientendaten zu gewährleisten und Fremd-Zugriff zu unterbinden. Im Finanzsektor wiederrum ist der Schutz von Finanz- und Bilanzdaten maßgeblich.

Kunden und Geschäftspartner setzen auf den Schutz ihrer Daten, wenn sie diese Unternehmen anvertrauen. Daher sollte es selbstverständlich sein, diese Schutzbedürftigkeit auch in der E-Mail-Kommunikation umzusetzen.

Mit der iQ.Suite können E-Mails mit über 300 verschiedenen Dateiformaten nach Wörtern, Wortteilen und Textbausteinen untersucht werden. Damit ist eine umfassende und zuverlässige Erkennung von Textinhalten jederzeit gewährleistet.

2.2.1 Analyse rechtsverbindlicher Willenserklärungen

Jede Branche hat ihre Schlüsselbegriffe – sogenannte Keywords, welche Prozesse definieren und den alltäglichen Sprachgebrauch prägen. Die iQ.Suite kann aufgrund ihrer hohen Flexibilität auf diese Spezifika eingehen und anhand gewichteter Wortlisten die entsprechenden E-Mails analysieren.

Die Zusammenstellung von Wortlisten erfolgt anhand der jeweiligen Branche, Unternehmung oder sogar Abteilung. Damit ist sichergestellt, dass beispielsweise Fachbegriffe korrekt berücksichtigt werden und die Steuerung der E-Mail-Kommunikation in Übereinstimmung mit betriebsinternen Vorgaben realisiert wird.

Es stehen zahlreiche Aktionen zur Verfügung:

- Blocken kompletter E-Mails mit definierten Wörtern/Texten
- Definition von Ausnahmen für dedizierte Kommunikationskanäle
- Statistik über Häufigkeit der erkannten Restriktionen
- Report über erkannte Restriktionen an Dritte (z.B. Sicherheitsbeauftragte)
- Übergabe der E-Mail an eine automatische Verschlüsselung
- E-Mail-Information an betroffene Absender
- Vier-Augen-Prinzip für den Versand dieser Informationen

3 Weitere Schutzmechanismen

Neben den genannten Szenarien spielen weitere Aspekte beim Schutz der E-Mail-Kommunikation eine entscheidende Rolle. So ist zum Beispiel die Erfassung und Analyse von Informationen über Kommunikationsströme ein wichtiger Punkt. Dies ermöglicht Einblicke in das Kommunikationsverhalten und erleichtert das Auffinden von Anomalien.

Auch die automatische Verschlüsselung sensibler Informationen gehört zu einer umfassenden Sicherheitsstrategie. Und hier insbesondere die Berücksichtigung der Bedürfnisse von Kommunikationspartnern im B2B- und B2C-Umfeld. Auch dies kann mit der iQ.Suite zuverlässig umgesetzt werden.

3.1 Analyse des E-Mail-Verkehrs

Nur wer weiß, welche Daten regelmäßig das Unternehmen erreichen und verlassen, kann einen durchgängigen E-Mail-Prozess aufsetzen. Dabei gilt es, Aspekte wie Datenschutz oder Effizienz der E-Mail-Kommunikation zu beherrschen. Das Wissen über die eigene E-Mail-Infrastruktur ist unabdingbar.

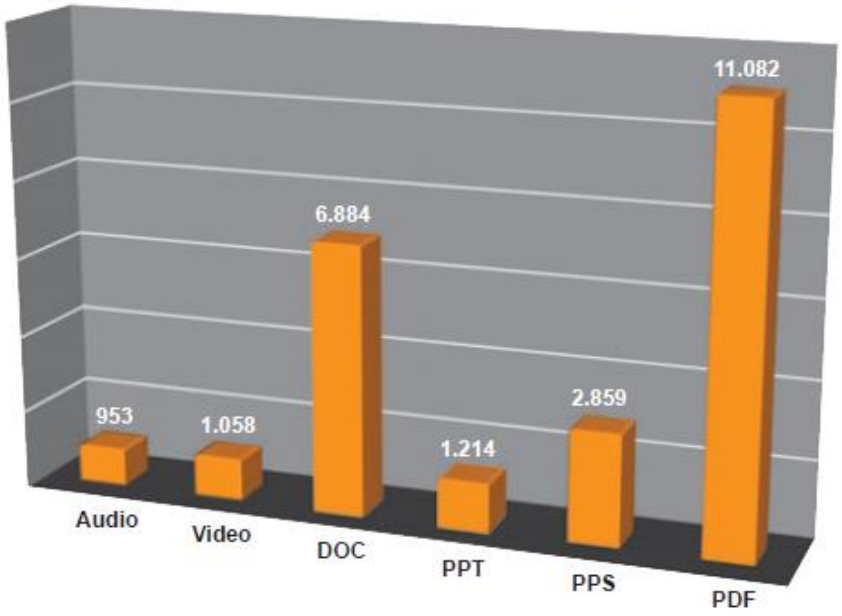

Abbildung 2: Anzahl E-Mail-Anhänge ausgehend

Mit der iQ.Suite bietet GBS Software diesen umfassenden Überblick. Die Lösung analysiert den gesamten E-Mail-Verkehr und erfasst eine Vielzahl an Parametern, die benötigt werden, um die E-Mail-Nutzung zu analysieren. So können zum Beispiel Informationen über die Art und Größe von Dateianhängen erfasst werden.

Die ermittelten Ergebnisse können dann auf vielfältige Weise genutzt werden:

- Umfassende Ist-Analyse der E-Mail-Kommunikation
- Erkennen von Verstößen gegen E-Mail-Richtlinien
- Auswertung des E-Mail-Verkehrs, z.B. hinsichtlich versendeter Dateitypen
- Systematischer Sicherheitscheck und gezielte Risikoreduktion
- Effizienzsteigerung und Optimierung der E-Mail-Prozesse
- Produktivitätssteigerung und Senkung der Betriebskosten

3.2 Verschlüsselung der ausgehenden Kommunikation

Jeder kennt die Analogie: der Versand einer E-Mail gleicht dem Versand einer Postkarte – ungesichert, für jedermann les- und manipulierbar. Dass dies nicht im Sinne von Unternehmen ist, versteht sich von selbst. Gefragt sind Schutzmechanismen, die Know-how und Kundendaten zuverlässig schützen.

E-Mail-Verschlüsselung bietet diese Sicherheit. Damit wird jede E-Mail auf ihrem Weg zum Empfänger umfassend abgesichert. Doch bislang machte der Einsatz einer Vielzahl von Schlüsseln und Zertifikaten das Thema zu einem anspruchsvollen Unterfangen.

Mit der iQ.Suite nimmt GBS Software der E-Mail-Verschlüsselung diese Komplexität. Der Verzicht auf ein client-basiertes Verfahren ist dabei der Schlüssel zu mehr Effizienz und Anwenderfreundlichkeit. Denn nur serverbasierte Verfahren entlasten die Mitarbeiter in Unternehmen und sorgen zugleich für die erforderliche Sicherheit.

Dabei bietet die iQ.Suite zwei Verfahren im Bereich E-Mail-Verschlüsselung:

1. Im Bereich der B2B-Kommunikation ermöglicht iQ.Suite Crypt Pro die Absicherung der E-Mail-Kommunikation durch ein regel- und serverbasiertes Verfahren zur E-Mail-Verschlüsselung. Ob PGP oder S/MIME – sowohl schlüssel- als auch zertifikatsbasierende Technologien werden unterstützt. E-Mails werden anhand zentral definierter Regeln durchgängig verschlüsselt – und das ganz ohne Interaktion der Endanwender. So lässt sich je Empfänger eine dedizierte Regel aufsetzen. Dies ermöglicht eine flexible Steuerung der verschlüsselten Kommunikation.

2. Im Umfeld der B2C-Kommunikation lassen sich nicht immer bestimmte Verfahren durchsetzen. Empfänger verfügen nur selten über eine eigene Verschlüsselungslösung. Um auch hier für die notwendige Vertraulichkeit beim Versand sensibler Daten zu sorgen, bietet GBS Software mit iQ.Suite WebCrypt Pro eine weitere Verschlüsselungslösung an, die ganz ohne Schlüssel und Zertifikate auskommt. Der Clou dabei: der Empfänger benötigt lediglich einen Webbrowser zum Anzeigen verschlüsselter Inhalte. Damit können Unternehmen an jeden Kunden oder Partner verschlüsselte E-Mails versenden.

4 Fazit

Data Leakage Prevention sollte mittlerweile fest im Bewusstsein von IT-Verantwortlichen und Geschäftsführung verankert sein. Denn nur durchdachte DLP-Strategien gewährleisten den zuverlässigen Schutz von Know-how, Kundendaten und wettbewerbsrelevanten Informationen. In der E-Mail-Kommunikation bedeutet dies, einen durchgängigen E-Mail-Prozess aufzusetzen. Dieser Prozess muss alle Aspekte der elektronischen Kommunikation betrachten – also sowohl eingehende als auch ausgehende E-Mails.

Entscheidend ist dabei die Berücksichtigung betrieblicher und gesetzlicher Vorgaben, die teilweise durch branchenspezifische Regularien zusätzlich detailliert werden. Erst wenn all diese Aspekte in den E-Mail-Prozess einfließen, ist der Schutz von E-Mails und den enthaltenen Daten zuverlässig gewährleistet.

Über GBS

GROUP Business Software ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die IBM und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Weitere Informationen unter www.gbs.com