E-Mail-DLP und wie Sie den Abfluss sensibler Daten über Ihre E-Mails stoppen können

So schützen Sie sich vor böswilligen oder versehentlichen Datenverlusten in Ihrer ausgehenden Kommunikation

Als wichtigster geschäftlicher Kommunikationskanal dient die E-Mail immer noch als primäre Plattform für den Austausch von Daten innerhalb und außerhalb des Unternehmens. Ein großer Teil dieser Daten enthält sensible Informationen. Dies macht die E-Mail zu einem der Hauptziele von Hackern und zum ultimativen Einfallstor für Malware, wie Ransomware und Phishing. Aus diesem Grund sollte eine angemessene Sicherheit der E-Mail-Kommunikation und die Einhaltung der Datenschutzbestimmungen eine der höchsten Prioritäten in der Sicherheitsstrategie eines Unternehmens sein. Die gute Nachricht ist, dass die Anbieter von Sicherheitslösungen kontinuierlich an der Verbesserung und Erweiterung von den Funktionen der E-Mail-Sicherheitstechnologie arbeiten.

Inhalt

Data Loss Prevention – ein regelbasiertes Konzept für datengestützte Sicherheit

Viele Unternehmen haben bereits erkannt, dass die E-Mail-Sicherheit weit über Antiviren-Scanner, Firewalls und Spam-Filter hinausgehen kann. Durch ein Upgrade auf Datenschutz-Tools können Unternehmen ihren E-Mail-Verkehr genauer überwachen, potenzielle Schwachstellen erkennen und den Zugriff auf sensible Daten kontrollieren, ohne die Produktivität zu beeinträchtigen. Es ist nun möglich, ausgehende E-Mails im Einklang mit internen Sicherheitsrichtlinien zu analysieren, verdächtige E-Mail-Aktivitäten zu erkennen und die versehentliche oder absichtliche Weitergabe sensibler Informationen zu verhindern.

Die Technologie, die sich hinter diesen Funktionen verbirgt, wird als Data Loss Prevention (DLP) bezeichnet - ein Begriff, den es schon seit über 15 Jahren gibt. Das Konzept der DLP ist außergewöhnlich und wurde zur Grundlage für viele andere Cybersicherheitsmechanismen und -tools. Eigentlich ist DLP eines der ersten Beispiele für datengestützte Sicherheit.

Data Loss Prevention bezieht sich auf jede Technologie, die dem Datenschutz dient. Dementsprechend ist E-Mail-DLP darauf spezialisiert, Datenlecks im E-Mail-Verkehr zu verhindern, indem Insider-Bedrohungen blockiert, menschliche Fehler eingedämmt und sensible Daten sowie verdächtige Aktivitäten erkannt werden.

Kann DLP gegen Phishing helfen?

Hacker und Datendiebe greifen vorwiegend auf Phishing-Mails zurück, um sich Zugang zu sensiblen Daten zu verschaffen. Ihre stark personalisierten E-Mails sehen so überzeugend echt aus, dass es oft schwierig ist den Betrug zu erkennen, bevor es zu spät ist. Indem sie vorgeben ein vertrauenswürdiger Absender zu sein und ein legitimes Anliegen vorzutäuschen, wird der Empfänger dazu verleitet, vertrauliche Informationen wie Kreditkartendaten oder Passwörter preiszugeben oder einen Dateianhang zu öffnen. Ein Klick kann ausreichen, um die unbemerkte Installation eines Trojaners zu starten, der Daten sammelt und direkt an den Datendieb übermittelt oder Hackern Zugang zum Firmennetzwerk verschafft.

Um dies zu verhindern, sollte die ausgehende Kommunikation analysiert und jede unzulässige Weitergabe von sensiblen Inhalten (z.B. Kundenlisten in Excel-Tabellen) oder jede Verhaltensauffälligkeiten (z.B. E-Mail-Anhänge oder massenhafte Übertragung von Unternehmensdaten) erkannt und blockiert werden. Manuelle Lösungen beeinträchtigen nicht nur die Produktivität, sondern sind auch fehleranfällig, daher lautet hier das Zauberwort "Automatisierung". Moderne DLP-Lösungen zeichnen sich zudem durch Überwachungsfunktionen und Dashboards aus, die für mehr Transparenz sorgen und Einblicke in die aktuelle Bedrohungslage geben.

DLP verhindert sowohl böswillige als auch versehentliche Sicherheitsschwachstellen in ausgehenden E-Mails

Es kann zwischen zwei Hauptkategorien von Datenverlusten durch ausgehende E-Mails unterschieden werden - versehentlich (einschließlich unbeabsichtigt) und böswillig. Hier sind einige Beispiele vonbeiden.

- Mitarbeiter sendet versehentlich sensible Informationen an den falschen Empfänger
    - Wenn er auf "Allen antworten" statt nur auf "Antworten" klicken
    - Durch einen Tippfehler im Empfängernamen
- Mitarbeiter hängt die falsche Datei an, die sensible Daten enthält
- Mitarbeiter sendet unwissentlich Informationen oder antwortet
    - an eine nicht autorisierte Person
    - auf eine Phishing-E-Mail
    - auf eine durch Identitäts-/Kontendiebstahl manipulierte E-Mail
    - auf eine durch Supply-Chain-Attack kompromittierte E-Mail
- Mitarbeiter, der fahrlässig Dokumente mit sensiblen Informationen von der Arbeit an die persönliche E-Mail (ungesicherte Geräte) weiterleitet, um sie zu Hause weiter zu bearbeiten
- absichtliches oder unwissentliches Senden an einen auf der schwarzen Liste stehenden Empfänger/Domäne
- vorsätzliches Versenden von sensiblen Informationen und Anhängen

Ohne eine DLP-Lösung ist die Erkennung der oben genannten Punkte eine ziemlich schwierige Aufgabe. Nehmen wir einmal an, dass jeder Mitarbeiter etwa 10 E-Mails pro Tag versendet. Bei 100 Mitarbeitern ergibt das 1000 E-Mails pro Tag, die von Hand überprüft werden müssen. Ganz zu schweigen von den Verzögerungen bei der Zustellung, Fehlern und der Zugriffsüberprüfung.

Eine Lösung, die den E-Mail-Verkehr überwacht und analysiert, kann anormale Aktivitäten, die auf ungewöhnliche Vorgänge bei ausgehenden E-Mails hindeuten, leicht erkennen. Die Aufgabe einer DLP-Lösung ist die folgenden Leistungsindikatoren zu überwachen, diese mit den vom IT-Administrator festgelegten Durchschnittswerten zu vergleichen und eine Warnung sowie eine vordefinierte Aktion auszulösen, wenn eine signifikante Abweichung auftritt.

- Anzahl der Emails
- E-Mail-Volumen
- Anzahl von Empfängern

Wer profitiert am meisten durch den Einsatz von E-Mail-DLP-Technologie?

Ein Blick darauf, was als sensible Daten gilt, gibt Aufschluss darüber, wer am meisten von der DLP-Technologie profitieren kann.

Beispiele für sensible Daten sind:

- persönliche Ausweisdaten
- Führerscheinnummern
- Kreditkartennummern
- Sozialversicherungsnummern
- Bankkontonummern und Transaktionen
- Login-IDs und Passwörter
- Gesundheitsdaten
- geistiges Eigentum
- Finanzdaten
- Geschäftsgeheimnisse

Ordnet man diese Daten den jeweiligen Funktionen im Unternehmen zu, wird deutlich, welche Abteilungen in einem Unternehmen mit den sensibelsten Daten arbeiten, welche den Datenschutzbestimmungen unterliegen.

Unternehmensbereiche, die von DLP profitieren:

- Personalabteilung (persönliche Daten, Sozialversicherungsnummern usw.)
- Finanzen und Buchhaltung (Kreditkarten, Überweisungen, IBANs, Passwörter usw.)
- Vertrieb und Kundendienst (Kundendaten)
- Forschung und Entwicklung (geistiges Eigentum)

Daten sind das neue Gold der Geschäftswelt. Branchen, die in der Regel große Datenmengen erzeugen und verarbeiten, sind die Ersten, die ins Visier von Hackern geraten. Angesichts dieser Tatsache und ihrer kritischen Bedeutung für die Wirtschaft, unterliegen diese Branchen einer strengen gesetzlichen Kontrolle durch den Staat und der EU.

Branchen, die am meisten von DLP profitieren:

- Versorgung (Energie, Wasser, etc.)
- Telekommunikation
- Gesundheit und Pharma
- Finanzen und Versicherungen
- Öffentliche Verwaltungen
- Juristische Einrichtungen
- Anbieter digitaler Dienste

Zur Konfiguration Ihrer E-Mail-DLP-Lösung benötigen Sie zunächst Definitionen

Ein wichtiger Punkt bei der DLP-Technologie ist, dass sie, um richtig zu funktionieren, auf Regeln beruht. DLP ermöglicht Unternehmen diese Regeln flexibel in voller Übereinstimmung mit ihren internen Richtlinien zu definieren und Schlüsselindikatoren und Schwellenwerte festzulegen, welche ihren Anforderungen am besten entsprechen.

- Um eine optimale Leistung der DLP-Technologie zu gewährleisten, müssen Unternehmen die folgenden Schlüsseldefinitionen für ihre Regeln festlegen.
- Definition, welche Informationen als sensibel gelten und was die Kennzeichen dafür sind
- Definition von Textinhalten, die als kritisch eingestuft werden
- Festlegen von Benchmark-Werten und Schwellenwerten für die Bewertung des E-Mail-Verkehrs
- Definition von Positionen und Verantwortlichkeiten für den Umgang mit kritischen E-Mails
- Definition von Prozessen, die ausgelöst werden, sobald ein Verstoß festgestellt wurde
- Festlegen von Quarantäneregeln
- Festlegen von automatischen Sperren
- Weiterleitung an Prüfpersonen festlegen
- Einstellen von Alarmen und Benachrichtigungen an Benutzer für verschiedeneAktionen Set alerts and notifications to users for different actions

iQ.Suite DLP von GBS – erweiterte Data Loss Protection Lösung für Ihre E-Mails

iQ.Suite DLP von GBS ist eine erweiterte Lösung zum Schutz vor böswilligen und versehentlichen Datenlecks in der ausgehenden E-Mail-Kommunikation. Die Software ist für Domino, Microsoft, On-Premises, Cloud und als Service verfügbar.

Die iQ.Suite analysiert jedes Element der E-Mail, ihren Textkörper, die Betreffzeilen, die Anhänge und den HTML-Code nach vordefinierten Richtlinien und Werten. Gleichzeitig werden die Vorgänge des Absenders auf Abweichungen von normalen Aktivitäten und Schwellenwerten untersucht. Wurde ein verdächtiges Muster erkannt, wird ein automatischer Prozess, je nach Problemfall eingeleitet. Die E-Mail kann blockiert, in Quarantäne gestellt oder zur Überprüfung an andere weitergeleitet werden und die entsprechenden Benachrichtigungen werden versandt.

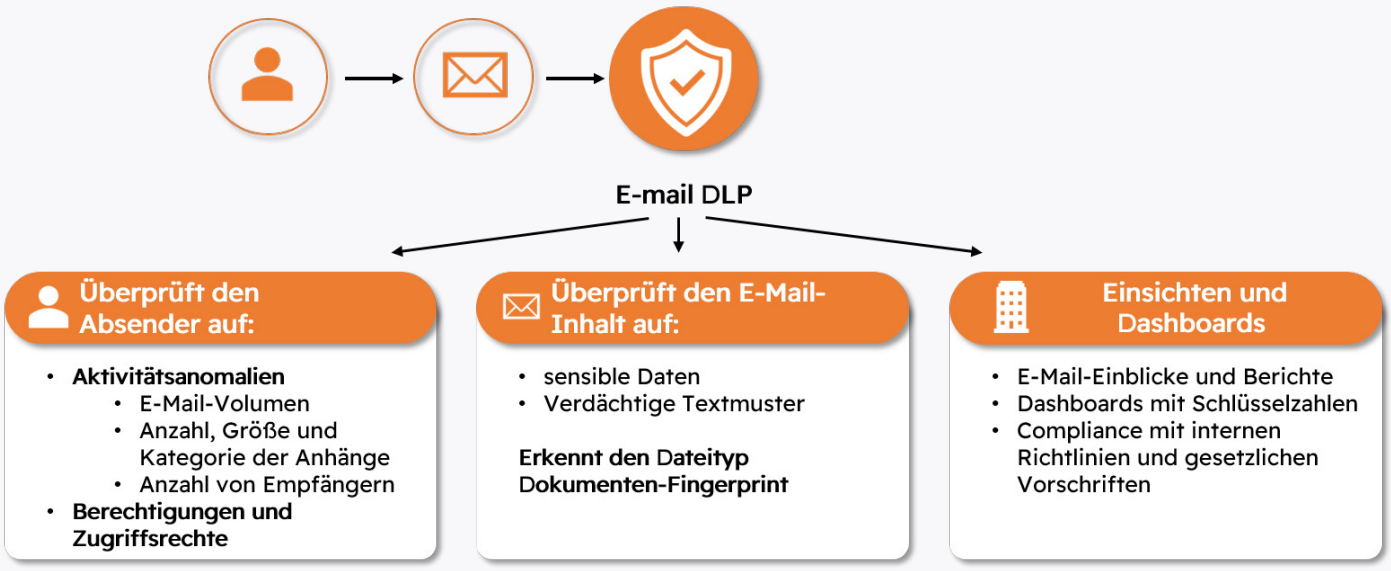
iQ.Suite DLP workflow

Wie gewährleistet iQ.Suite DLP erweiterte Sicherheit für Ihre sensiblen Daten?

Eine leistungsfähige E-Mail-DLP-Lösung identifiziert sensible Informationen, verhindert Datendiebstahl und stoppt Datenverluste. Nach diesem Prinzip bietet iQ.Suite DLP umfassende Datensicherheit in nur drei Schritten: Sie analysiert, bewertet und blockiert.

Schritt 1 - E-Mail-Verkehr analysieren

- Echtzeit-Analyse der ausgehenden E-Mail-Kommunikation, unternehmensweit oder für ausgewählte Abteilungen
- detaillierte Prüfung von E-Mails vor dem Versand
- Erkennung von verdächtigen Textmustern (Kreditkartendaten, Kundennummern, etc.) in E-Mail-Texten und -Anhängen
- eindeutige Identifizierung von Dateianhängen wie z.B. Office-Formaten dank der fortschrittlichen Fingerprint-Technologie
- Erkennung von Verhaltensanomalien im E-Mail-Verkehr. Zu diesem Zweck werden Informationen, wie Anzahl und Größe der in einem bestimmten Zeitraum versendeten E-Mails, gesammelt und mit dem aktuellen Verhalten der Nutzer verglichen. Auf diese Weise kann ein unverhältnismäßiger Anstieg des E-Mail-Volumens oder das Versenden großer Datenmengen erkannt werden, was auf ein Leck in vertraulichen Daten hinweisen könnte.



iQ.Suite DLP features

Schritt 2 - Bewertet Indikatoren und visualisiert Schlüsselwerte

- webbasiertes Dashboard zur Visualisierung von Schlüsselzahlen
- detaillierte Einblicke in die ausgehende E-Mail-Kommunikation hinsichtlich E-Mail-Volumen, Anzahl, Größe und Kategorie der Anhänge, Anzahl der Empfänger pro E-Mail etc.
- einfacher Export und Verwendung von Daten für die Berichtserstattung
- integriertes Rechte- und Rollenkonzept: Benutzer können nur, auf für sie relevante Informationen, zugreifen, wenn sie dazu berechtigt sind.
- konfigurierbare Datenlöschung nach einem bestimmten Zeitraum, gemäß den aktuellen Datenschutzrichtlinien

Schritt 3 - Blockiert verdächtige E-Mails

- flexible Regeln und Schwellenwerte - Festlegen, wie E-Mails mit vertraulichem Inhalt zu behandeln sind
- Handlungsmöglichkeiten
    - E-Mails bis zur weiteren Prüfung in Quarantäne stellen
    - zusätzliche Benachrichtigung des Absenders und Dritter
    - Überprüfung nach dem Vier-Augen-Prinzip durch eine vorher festgelegte Person, welche die endgültige Entscheidung trifft, ob die E-Mail freigegeben oder blockiert werden soll
- Im Rahmen der Unternehmensrichtlinien ist jede Kombination von Maßnahmen möglich

4-Augen-Prinzip (Doppelkontrolle) bei der Überprüfung von gestoppten E-Mails

Wenn eine E-Mail mit kritischem Inhalt erkannt wird und es nicht eindeutig ist, ob das Versenden sicher ist, bietet iQ.Suite DLP die Möglichkeit, das 4-Augen-Prinzip anzuwenden. Das Vier-Augen-Prinzip (auch bekannt als Zwei-Mann-Regel) ist ein interner Kontrollmechanismus, der festlegt, dass eine bestimmte kritische Aktivität, ein Prozess oder eine Entscheidung, von zwei vorher festgelegten und kompetenten Personen, genehmigt werden muss, um sicherzustellen, dass die bestmögliche Entscheidung getroffen wird. Dieses Prinzip ist in einer Vielzahl von Bereichen anwendbar - so müssen beispielsweise viele Rechtsdokumente mit zwei Unterschriften beglaubigt oder Dokumentenänderungen in bestimmten Datenverwaltungssystemen genehmigt werden, bevor die Änderungen der Daten zulässig sind. In anderen Worten: iQ.Suite DLP leitet fragwürdige E-Mails an vorher festgelegte Personen weiter, die entscheiden können, ob die E-Mail sicher genug ist, um an den Endempfänger weitergeleitet zu werden. who can decide whether the email is safe enough to be sent on to the final recipient.

Benachrichtigungen, die aufklären und das Sicherheitsbewusstsein erhöhen

Wird eine E-Mail als kritisch eingestuft, bietet die iQ.Suite die Möglichkeit, eine Benachrichtigung darüber an den Absender, die Empfänger oder an jede andere Person oder Gruppe zu senden. Diese Benachrichtigungen können beliebige Texte, Links oder Grafiken enthalten, welche den Unternehmen die Möglichkeit geben, ihre Mitarbeiter über Sicherheitslücken und die unternehmensinternen Sicherheitsrichtlinien aufzuklären. Es ist einfach, vorgefertigte Texte zu verfassen, in den erklärt wird, warum die E-Mail blockiert/unter Quarantäne gestellt/überprüft wurde und wie die darin enthaltenen Daten gefährdet werden könnten. Ein einfaches Zitat aus der internen Sicherheitsrichtlinie oder ein Link kann zur Unterstützung der Erklärung hinzugefügt werden. Auf diese Weise kann der Mitarbeiter das Risiko besser einschätzen und sein Sicherheitsbewusstsein schärfen, sodass er wachsamer wird und in der Lage ist, die E-Mail zu korrigieren und die ungeschützte Weitergabe von Daten in Zukunft zu vermeiden.

Funktionen der iQ.Suite DLP:

- Erkennung von Anomalien beim E-Mail-Versand
- 4-Augen-Prinzip: Überprüfung und Freigabe von gestoppten Emails
- Stoppt die Übertragung von verdächtigen E-Mails
- Überwachungsfunktionen und Dashboards, die für mehr Transparenz sorgen und Einblicke in die aktuelle Bedrohungslage geben
- Auslösung der E-Mail-Verschlüsselung durch die Kennzeichnung einer E-Mail mit sensiblen Informationen

Vorteile von iQ.Suite DLP:

- Automatisierung und Verwaltung von einem zentralen Punkt
- Beseitigung menschlicher Fehler und Reduzierung der Arbeitsbelastung
- Ermöglichung einer Umsetzung von internen Richtlinien
- Einhaltung gesetzlicher Vorschriften durch hohe Datensicherheit

Einfacher Datenexport für BerichtszweckeIn den anerkannten ISG Provider Lens™ Quadrant Reports werden jedes Jahr die besten Lösungen in der Kategorie "Data Leakage/Loss Prevention (DLP) and Data Security" bewertet und gewichtet. Mit ihrer Sicherheitslösung iQ.Suite DLP zählt die GBS im Jahr 2022 bereits zum vierten Mal im Bereich "Cybersecurity - Solutions and Services" zu den führenden Unternehmen auf dem deutschen Markt. Die mehrmalige Auszeichnung in der gleichen Kategorie der stärksten Player im IT- und Security-Markt beweist, dass die GBS-Lösung mit ihren herausragenden innovativen Features in puncto Datensicherheit ohne Kompromisse zu überzeugen weiß.

Über GBS

GBS ist ein renommierter Anbieter von E-Mail- und Collaboration-Sicherheitslösungen in Deutschland mit rund 30 Jahren Erfahrung in den Bereichen Datenschutz, Produktivität und Compliance. Das Unternehmen wird von namhaften Marktforschern in Deutschland und von seinen Partnern als führendes Unternehmen für Cybersicherheitslösungen anerkannt und insbesondere in den Bereichen Data Loss Prevention und Collaboration-Sicherheit.

GBS bietet umfangreiche Lösungen der nächsten Generation für E-Mail Produktivität, Compliance sowie einen mehrstufigen Schutz bei der E-Mail Kommunikation und Datenaustausch über verschiedene Collaboration-Plattformen gegen alle Arten von Sicherheitsbedrohungen. Die Lösungen für Microsoft 365, Exchange und HCL-Domino sind einfach zu bedienen, flexibel und decken Schlüsselbereiche wie Malware-Schutz, Verschlüsselung, E-Mail Produktivität, Datenverluste, Workflow und Compliance ab.

Die Lösungen von GBS schützen mehr als 2 Millionen Endbenutzer weltweit. Das Unternehmen pflegt langjährige Beziehungen zu über 2.000 Kunden.