TEC WORKSHOP

Link: https://www.tecchannel.de/a/e-mail-mehr-sicherheit-durch-klare-regeln-und-dlp,1778559

**Compliance bei der Geschäfts-E-Mail**

# E-Mail: Mehr Sicherheit durch klare Regeln und DLP

Datum: 09.12.2008
Autor(en): Johann Baumeister

**Der sichere E-Mail-Austausch beginnt bei der Erstellung der Nachrichten. Klare Vorgaben für den Verfasser einer E-Mail erhöhen die Sicherheit und erleichtern die Einhaltung der Compliance. Ein nachgeschaltetes DLP-System spürt Schwachstellen bei den eigenen Mitarbeitern auf.**

Die E-Mail ist längst zur tragenden Säule beim IT-Einsatz geworden. Einem Ausfall des E-Mail-Systems wird oftmals ein größerer Einfluss auf die geschäftlichen Tätigkeiten zugeschrieben, als dies für die traditionellen Geschäftsapplikationen und deren dahinterliegende Datenbanken gilt. Allerdings ist die Absicherung des E-Mail-Systems keine einfache Aufgabe. Die Techniken, Vorgaben und Regularien beim Umgang mit E-Mail passen nicht in das gewohnte Schema der programmierten Applikationen und Datenbanken.

Um beispielsweise eine Bestellung mit einer Geschäftsapplikation zu erfassen, existieren klare Vorgaben, Erfassungsmasken, Geschäftsabläufe, Vorschriften und Techniken zur Aufbewahrung und Sicherung der Daten. Die Bearbeitung der Bestelldaten erfolgt ausschließlich durch vorher fest programmierte Bearbeitungsmasken. Was wo zu stehen hat und in welchen Format eine Bestellung gespeichert, gedruckt, weitergeleitet oder gelöscht wird, ist lange vorher durch die Designer und Entwickler der Applikation in Code gegossen. Der Ablauf kann durch den stets authentifizierten Benutzer auch nicht verändert werden.

Die Situation bei der E-Mail-Nutzung könnte gegensätzlicher kaum sein. Eine E-Mail ist meist im Freitextformat formuliert, jeder Nutzer kann sie nach Gutdünken aufbauen. Dies macht eine nachfolgende rechnergestützte Bearbeitung schwierig. Auch die weitere Bearbeitung ist, im Gegensatz zu den Geschäftsapplikationen, oft nicht definiert. Wer darf die E-Mail sehen, weiterleiten oder löschen? Wo und wie lange wird sie gespeichert? Welche Inhalte muss eine E-Mail aufweisen, dass sie für geschäftsrelevante Entscheidung herangezogen werden kann? All diese Fragen sind bei der E-Mail-Nutzung nicht definiert.

Da E-Mails immer mehr zu den Trägern von Geschäftsprozessen werden, treten hier Konflikte auf. In den Bemühungen um Compliance muss man die E-Mail-Nutzung regelkonform (compliant) machen. Dies umfasst den gesamten Prozess, von der Erstellung einer E-Mail über ihren Transport und die Auslieferung beim Empfänger bis zur nachfolgenden Archivierung

Unsere dreiteilige Artikelserie zur E-Mail-Sicherheit richtet sich nach den chronologischen Abläufen. Sie beginnt bei der sicheren E-Mail-Erzeugung und beschäftigt sich im zweiten Teil mit den Sicherungsmaßnahmen auf Empfängerseite. Der dritte Teil widmet sich der Absicherung des E-Mail-Systems selbst.

Artikelserie

| |
|---|
| Teil 1: **Regeln für das sichere Erstellen von E-Mails**[2] |

Teil 2: **Regeln und technische Schutzmaßnahmen beim E-Mail-Empfang**[3]

Teil 3: **Sichere Infrastruktur für E-Mail-Systeme**[4]

# 1. E-Mail-Sicherheitsaspekte im geschäftlichen Kontext

Im Mittelpunkt der folgenden Ausführungen stehen der Nutzen und der Einsatzzweck von E-Mails für geschäftliche Anwendungen. Dabei geht es sowohl um die die frei erstellte Mail, die zwischen zwei Partnern ausgetauscht wird, als auch um den automatisierten Einsatz von E-Mails als Träger des Geschäftsprozesse. Im Vordergrund stehen dabei die möglichst automatische Klassifizierung, Weiterleitung und Bearbeitung von geschäftlich ausgetauschten Nachrichten.

Eine Grundvoraussetzung für alle auf E-Mails basierenden Geschäftsprozesse stellt die Sicherheit dar. Dabei gilt es mehrere Facetten zu berücksichtigen:

- Sicherheit beim Erzeugen und Versenden einer E-Mail: Werden alle firmeninternen Regeln eingehalten? Welche Informationen sind in der E-Mail enthalten? Ist der Sender berechtigt, diese Daten zu verbreiten? An wen wird die Mail gesandt?
- Sicherheit gegen Angriffe beim Transport: Verschlüsselung und Signatur schützen vor Spionage und Verfälschung.
- Absicherung gegen Angriffe, die auf eingehenden E-Mails basieren: SPAM, Viren und Trojaner.
- Abgesicherter Zugriff der Benutzer auf das E-Mail-System und seine Postfächer
- Gesicherte Aufbewahrung der E-Mails und Klassifizierung, um sie wiederzufinden. Dabei ist auch der Schutz vor versehentlichem Löschen zu berücksichtigen.
- Absicherung des Mail-Systems gegen einen Ausfall, wie etwa durch Cluster- oder Failover-Techniken.

# 2. Sicherheit bei der E-Mail-Erstellung

Bei der Erstellung einer E-Mail unterscheidet man drei grundsätzliche Varianten.

- Die erste ist die manuell erstellte Freitext-Mail. Sie wird durch einen Benutzer in einem Mail-Programms mit POP3-, SMTP- oder IMAP-Anbindung erstellt und versendet. Inhalt und Empfänger der E-Mail werden komplett durch den Ersteller der Mail vorgegeben.
- Der zweite Weg ist die automatisiert erzeugte Mail. Der Inhalt wird durch die Applikationssysteme erzeugt und als Mail versandt. Dazu stehen in den gängigen Entwicklungs-Kits oder -Sprachen meist direkte Funktionen zum Versenden von E-Mails bereit. Beispiele dazu finden sich allerorten. eBay, Amazon oder etwa Buchungssysteme versenden nach der Änderung des Auftragsstatus solche Bestätigungen. Der Inhalt der Mail besteht aus vorgegebenen Texten, in denen die relevanten Kundenangaben oder der Bestellstatus in die reservierten Positionen eingefügt werden.
- Eine Mischform aus den beiden obigen Varianten ist die Massen-E-Mail zu Werbezwecken; zu dieser Variante gehört auch die Spam-Mail.

Diese drei Varianten werden hier deshalb getrennt erwähnt, weil die Reaktion seitens des Empfängers unterschiedlich sein wird. Dies wird im zweiten Teil unserer Artikelserie besprochen.

Der Sicherheitsaspekt aus Sicht des Absenders ist bei der automatisch generierten E-Mail unkritisch. Inhalte und Empfängerkreis werden durch Programmierung und Datenbankinhalte klar festgelegt. Alle Daten, die für den Versand der Mail herangezogen wurden, lassen sich jederzeit rekonstruieren. Die verschickte E-Mail aufzubewahren wäre damit nicht mehr notwendig. Aus Gründen der Beweissicherung und Compliance kann es allerdings notwendig sein, die E-Mail selbst abzulegen.

Ganz anders ist die Situation für frei erstellte Mails durch die Benutzer. Inhalte und Empfängerkreis sind per se frei definierbar. Der lockere Umgangston, den die Benutzer bei E-Mails an den Tag legen, mag im einfachsten Fall lediglich zu Kopfschütteln führen. Er kann aber auch schwerwiegende Konsequenzen für den Mitarbeiter oder das Unternehmen haben. Dies gilt beispielsweise dann, wenn vertrauliche Informationen an Empfänger weitergereicht werden, die diese Inhalte nicht zu Gesicht bekommen sollten.

# 3. Vorgaben für das Erstellen von E-Mails

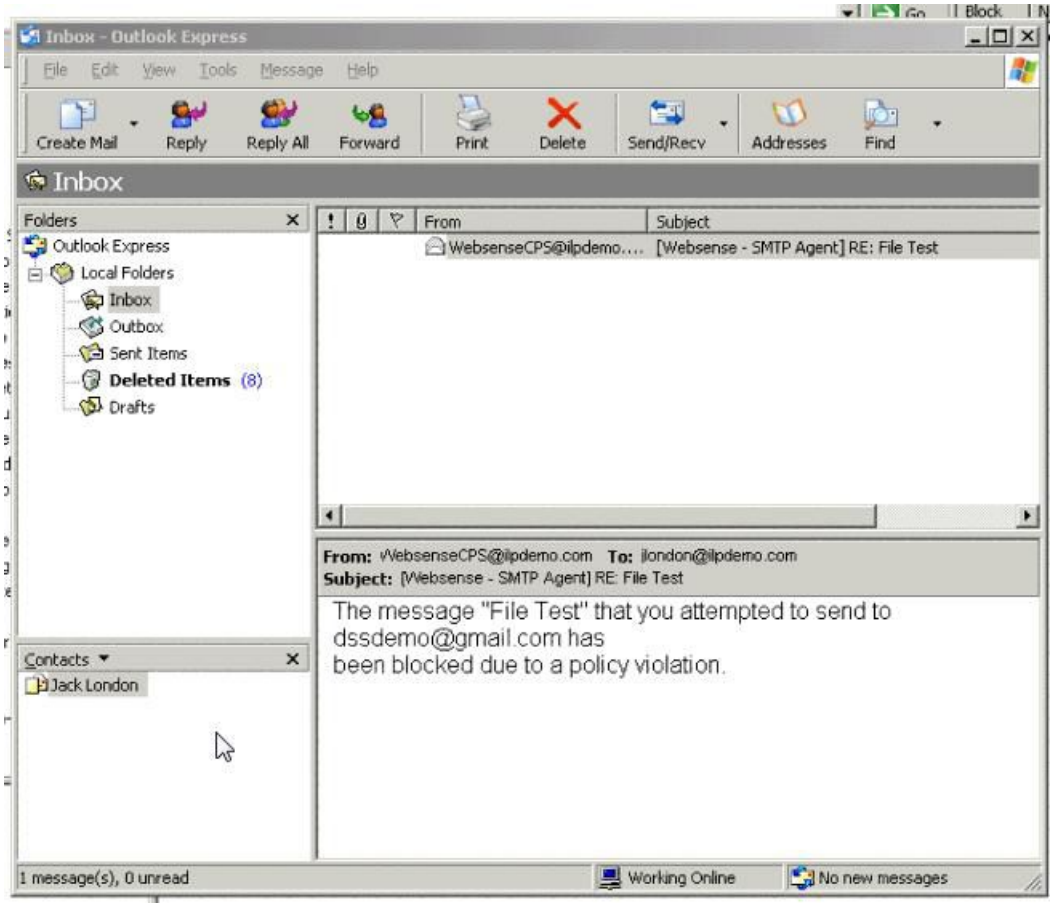
Um die Sicherheit bei der manuellen Erzeugung von E-Mail zu gewährleisten, existieren derzeit zwei Ansätze: automatisierte Kontrollverfahren und verbindliche Regeln für die Mitarbeiter.

Trotz aller technischen Hilfsmittel müssen zunächst allgemeine Vorgaben für den Umgang mit dem Mail-System geschaffen werden. Diese Regeln beschreiben beispielsweise

- die Nutzung von Mail-Verteilern,
- den Gebrauch sinnfälliger Betreffzeilen,
- die Vermeidung von überflüssigen Anhängen,
- die Kennzeichnung rein informativer E-Mails
- und eventuell auch das Verbot, die E-Mail-Adresse öffentlich zugängig zu machen.

Sofern keine automatisierten Verfahren zur Bearbeitung und Speicherung der E-Mails bestehen, gehören zu diesem Regelsatz auch Vorgaben über Speicherort der E-Mails, Postfachgröße, Aufbewahrungszeiten oder Löschintervalle.

Wichtig ist zu klären, ob und wie geschäftlich nicht relevante E-Mails erkannt und behandelt werden. Die Benutzer sind zudem im Umgang mit unerwarteten Mails zu schulen. Der generelle Rat, E-Mails von unbekannten Absendern erst gar nicht zu öffnen, ist im geschäftlichen Umfeld fehl am Platz.



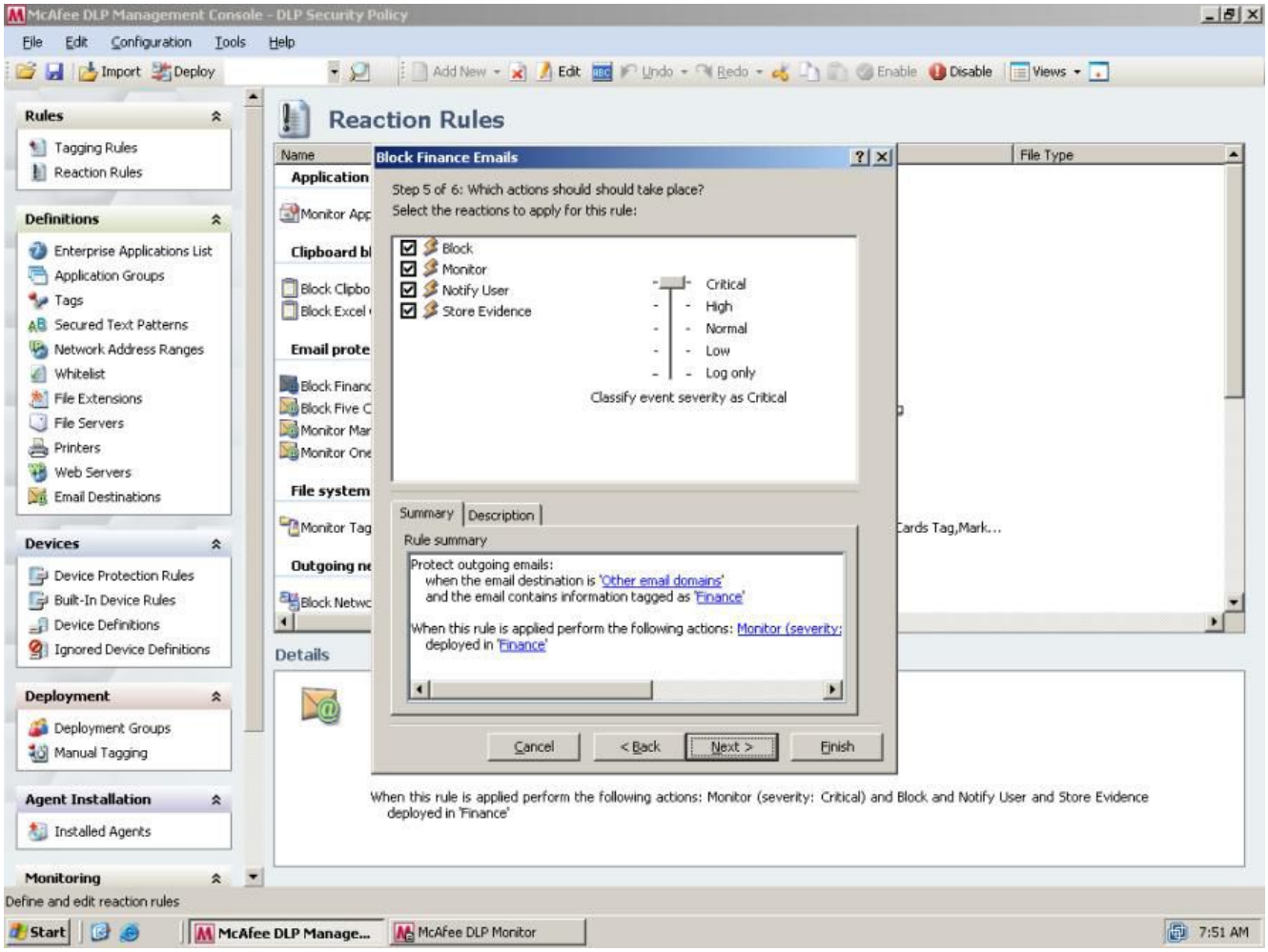

Klare Regeln: Websense blockiert den Mail-Versand in Outlook, falls die Mail gegen feste Regeln verstößt.

Klare Regeln zur E-Mail-Erstellung, egal ob manuell oder maschinell, haben einen entscheidenden Einfluss auf die nachfolgenden Weiterverarbeitung. So vereinfacht die Verwendung von Schlüsselwörtern die anschließende Klassifizierung extrem, beispielweise wenn der Benutzer schon im Betreff festlegt, dass es sich um eine „Produktanfrage“ handelt. Andernfalls muss das Anliegen des Benutzers durch Textanalyse-Algorithmen oder gar manuell mühsam ermittelt werden.

Ein wichtiger Punkt wird nach der Einführung von Regeln oft vernachlässigt: Nur wenn deren Einhaltung auch mit Nachdruck kontrolliert wird, erhalten die Anweisungen einen rechtsverbindlichen Status. Ansonsten kann sich der Arbeitnehmer auf eine Duldung des Regelverstoßes berufen.

# 4. Data Leakage Protection sorgt für Compliance

Im Mittelpunkt jeglicher IT-Nutzung stehen immer die Daten. Ihr Schutz kann kaum als zu hoch eingestuft werden. In vielen Bereichen wird dieser Schutz auch durch passende Konzepte unterstützt. Firewalls, Berechtigungssystem, Benutzergruppen oder Passwörter sind dafür nur die gängigsten Lösungen. Der unachtsame Versand von E-Mails kann jedoch diese Schutzmaßnahmen vollständig untergraben. Ohne weitere Hilfsmittel kann jeder Benutzer Daten durch das E-Mail-System nach außen schleusen. Derzeit etablieren sich Werkzeuge, die dies verhindern sollen: Data-Leakage-Protection-Tools überwachen und protokollieren dazu den Transfer der Daten und ihre Nutzung.



Ernstfall: In McAfee DLP werden Regeln darüber eingestellt, was mit auffälligen E-Mails passieren soll.

Nach einer Untersuchung von **Infowatch**[1] ist die Bedrohung durch den Datenverlust mittlerweile größer als viele andere Gefahren des Internets. 78 Prozent der befragten Unternehmen räumen dem Datendiebstahl die höchste Priorität gegenüber allen anderen Sicherheitsbedrohungen ein. Die Veröffentlichung von Daten durch nachlässiges Verhalten der Mitarbeiter steht mit 65 Prozent an zweiter Stelle.

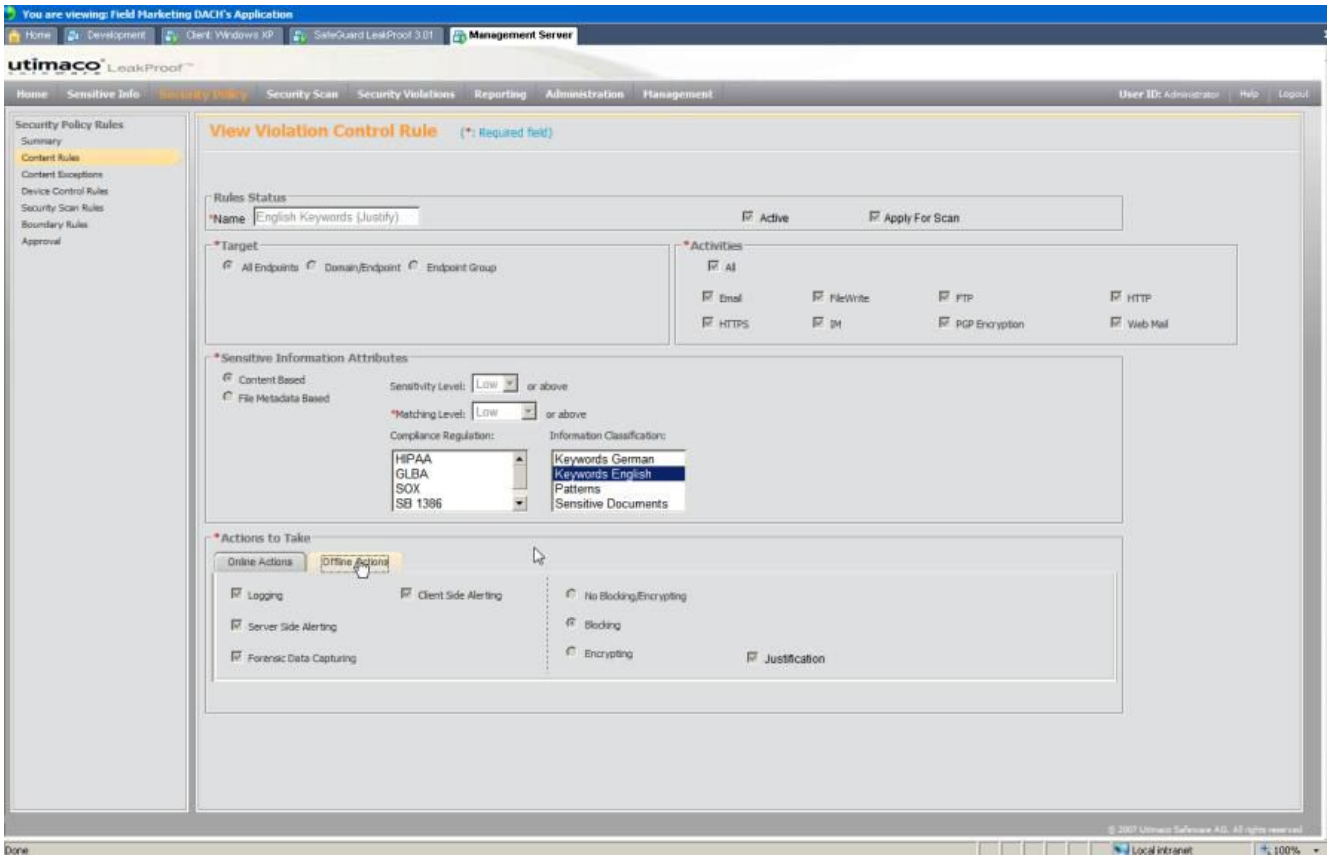
Ob es sich um einen gezielten Einbruch, verlorene Notebooks oder den übersehenen Anhang einer E-Mail handelt, spielt aber für das Ergebnis keine Rolle: Firmeninterne Daten sind in die falschen Hände gelangt. Die Data Leakage Protection versucht, alle Kommunikationskanäle gegen diesen Datenverlust abzusichern. Der Schutz umfasst dabei die Armada der USB-Geräte, den direkten Zugriff auf Dateiverzeichnisse und die Kommunikationskanäle wie E-Mail, Instant Messaging oder Peer-to-Peer-Netze.

Da E-Mail eines der wichtigsten Kommunikations-Interfaces darstellt, wird es durch die DLP-Tools besonders abgesichert. Um mehr Sicherheit zu erreichen, werden E-Mails nach sensiblen Inhalten durchsucht. Ferner lassen sich die Anhänge analysieren oder generell einschränken.

# 5. Content Filtering untersucht den Mailinhalt

Das Content Filtering der DLP-Tools analysiert den E-Mail-Text und die Anhänge. Bewertet werden dabei nicht nur Schlüsselwörter (Keyword-Matching) und Dateitypen des Anhangs, sondern etwa auch die E-Mail-Adreese des Empfängers und die Sendezeit. Alle Parameter tragen zu einem Gesamtwert bei, der die Wahrscheinlichkeit eines Verstoßes angibt.

Beim Keyword-Matching werden die übermittelten Daten nach bestimmten Schüsselworten wie etwa „Quartalszahlen“ oder „Monatsabschluss“ durchsucht. Dafür sind aber umfassende Konfigurationen nötig. Eine einfache Liste an Schlüsselworten führt selten zum erwünschten Ergebnis. Erst die Kombination mehrere Wörter ergibt den kritischen Kontext.



Keyword Matching: Utimacos Mail-Analyse untersucht die E-Mail auch nach Schlüsselworten. Hierzu ist eine Vielzahl an Schlüsselworten bereits hinterlegt.

Eine weitere Technik, den Datenabfluss zu unterbinden, ist das Fingerprinting. Hierbei werden eindeutige Merkmale der Daten, ähnlich einem Fingerabdruck, ermittelt. Selbst wenn die Daten dann kopiert oder in einen anderen Zusammenhang gestellt werden, bleibt der Fingerabdruck erhalten, und die Daten sind nach wie vor eindeutig zuordenbar. Um auch jene Fälle zu erkennen, in denen der Text in einen anderen Zusammenhang kopiert oder in einen anderen Text eingeflochten wird, gilt der Fingerprint nicht für den kompletten Text. Das Fingerprinting operiert vielmehr auf Textblöcken und Passagen, sodass auch deren Versand in E-Mails erkannt wird.

Übersicht wichtiger DLP-Anbieter

| **Hersteller** | **Produkt** |
|---|---|
| **Centennial Software**[5] | DeviceWall |
| **EMC**[6] | Data Loss Prevention Suite |
| **Ironport**[7] | Data Leakage |
| **McAfee**[8] | Total Protection |
| **INFOWATCH**[9] | Traffic Monitor, Device Monitor |
| **Proofpoint**[10] | Proofpoint DLP |
| **Symantec**[11] | Vontu Data Loss Prevention |
| **Trend Micro**[12] | Leakproof |
| **Websense**[13] | Essential Information Protection |
| **Tizor Systems**[14] | DLP |

Zu den ambitioniertesten Techniken der Textanalyse zählen linguistische Analysen. In der einfachsten Version erkennt das DLP-System dabei die Grundform der Wörter und führt etwa Verben auf den Infinitiv zurück.

# 6. Fazit

E-Mails sind aus dem Geschäftsalltag nicht mehr wegzudenken. Ging es früher vor allem darum, das eigene Unternehmen vor der eingehenden E-Mail-Flut zu schützen, so achtet man nun auch darauf, dass keine vertraulichen Daten die Firma verlassen. Der Einsatz eines Tools zur Date Leakage Protection und ein Regelwerk für die Mitarbeiter zum Umgang mit dem Mail-System leisten dabei wertvolle Hilfe. (ala)

Artikelserie

| |
|---|
| Teil 1: **Regeln für das sichere Erstellen von E-Mails**[15] |
| Teil 2: **Regeln und technische Schutzmaßnahmen beim E-Mail-Empfang**[16] |
| Teil 3: **Sichere Infrastruktur für E-Mail-Systeme**[17] |

## Links im Artikel:

1 **http://www.infowatch.com/de/**
2 **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
3 **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
4 **https://www.tecchannel.de/link.cfm?pk=1779571**
5 **http://www.centennial-software.de/**
6 **http://germany.emc.com/**
7 **http://www.ironport.com/de/**
8 **http://de.mcafee.com/**
9 **http://www.infowatch.com/de/**
10 **http://www.proofpoint.com/**
11 **http://www.symantec.com/de/de/index.jsp**
12 **http://de.trendmicro.com/de/home/**
13 **http://www.websense.com/global/de/**
14 **http://www.tizor.com/**
15 **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
16 **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
17 **https://www.tecchannel.de/link.cfm?pk=1779571**

---