Zentrale Unternehmensdaten unter Verschluss

Data Loss Protection

Zentrale Unternehmensdaten sollten nicht unkontrolliert an die Öffentlichkeit gelangen. Ein neuer Ansatz, der dies verhindern soll ist „Data Loss Protection" (DLP). Seine Implementierung hat vor allem eines im Fokus: Die vollständige und automatische Überwachung von Manipulationen dieser Daten unter Einhaltung gesetzlicher Vorgaben. Eine Herausforderung.

AUTOR: DANIEL LIEBHART

Vom klugen Umgang mit Informationen sind viele Unternehmen leider noch weit entfernt. Zwar wird heute kaum ein Unternehmen mehr bestreiten, dass Informationen und damit Daten wichtige Werte darstellen. Sie werden aber in den seltensten Fällen systematisch bewertet, klassifiziert und entsprechend verwaltet. Eine Konsequenz dieser mangelhaften Bewirtschaftung strukturierter und unstrukturierter Daten ist, dass sensitive Unternehmensinformationen unkontrolliert an die Öffentlichkeit gelangen können. Der Verkauf einer CD mit sensitiven Kundendaten an die deutschen Steuerbehörden im letzten Jahr bildet lediglich die Spitze eines Eisbergs von Sicherheitsrisiken, die sich Unternehmen so einhandeln. Die IDC schätzt, dass rund die Hälfte aller Verletzungen der Unternehmensintegrität durch interne Mitarbeiter verursacht wird [1]. Der bewusste und vorsätzliche Verkauf von Daten ist da wohl eher ein seltener Fall. Viel häufiger sind es Unachtsamkeiten und Fehler von pflichtbewussten Angestellten oder schlecht verwaltete Systeme, die dafür verantwortlich sind, dass Daten unkontrollierte Wege in die Öffentlichkeit finden.

WAS IST DATA LOSS ODER DATA LEAKAGE?

Data Loss oder auch Data Leakage bedeutet, dass vertrauliche Daten zum Schaden des Unternehmens in nichtautorisierte Hände oder gar an die Öffentlichkeit gelangen. Von privaten Krankengeschichten über Kontostände und anderen Kundeninformationen, von Finanz- oder Produktinformationen bis hin zu Daten über das geistige Eigentum eines Unternehmens – der Verlust solcher Daten kann ein Unternehmen empfindlich treffen. Experten schätzen, dass ein einziger Vorfall für ein größeres Unternehmen ein Schaden von durchschnittlich zwischen vier und sieben Millionen Dollar verursacht – auf den einzelnen Datensatz bezogen sollen die Kosten des Schadens ca. 200 Dollar betragen [2]. „Data Loss Protection" oder auch „Data Loss Prevention" versucht dies zu verhindern, und zwar auf den drei Ebenen Bewegungsdaten (*Data in Motion*), gespeicherte Daten (*Data in Rest*) und Daten auf dem Endgerät (*Data at the Endpoint*). Die Idee ist einfach; die sensitiven Daten werden so beobachtet, dass sie nicht mehr unkontrollierte Wege gehen können. Sie können weder von unautorisierten Personen gelesen oder kopiert werden noch an falsche Adressen verschickt oder an falschen Orten gespeichert werden. Die Umsetzung steckt jedoch in den Kinderschuhen, auch wenn bereits eine Vielzahl von Herstellern wie beispielsweise Vontu (heute Symantec), Websense, Code Green Networks, Palisade Systems, NextLabs, RSA (EMC), CA, IBM und andere mit Produkten und Produktsuiten auf dem stark wachsenden Markt präsent sind. Gemäß der Website datalossprevention.com soll in diesem Jahr der Markt um 25 Prozent wachsen [3].

DIE IDEALE LÖSUNG

Eine DLP-Lösung identifiziert, überwacht und schützt sensitive Daten (gespeicherte Daten, Bewegungsdaten

und Daten auf dem Endgerät) durch Analyse der Dateninhalte in Echtzeit basierend auf zentral verwalteten Regeln und Richtlinien. Eine ideale DLP-Lösung deckt zwei sich widersprechende Anforderungen ab; sie soll einerseits unbemerkt in Echtzeit ihre Aufgabe erfüllen und andererseits alle sensitiven Daten eines Unternehmens durchgehend schützen. Die sensitiven Daten aus dem Datenmeer, in dem täglich alle Mitarbeitenden eines Unternehmens schwimmen, herauszufiltern ist eine Sache, die der Echzeitanforderung eigentlich widerspricht. Es müssen sämtliche Daten, egal ob sie nun gerade irgendwo gespeichert sind oder ob sie gerade von A nach B unterwegs sind, auf ihre Sensitivität hin geprüft werden. Da geht es nicht nur darum, E-Mails und Messaging zu überwachen, eine durchgehende DLP-Lösung muss sogar jedes „Copy Paste" auf einem Endgerät prüfen und gegebenenfalls verhindern und das auch noch, ohne bei der Arbeit zu stören. Eine ideale DLP-Lösung ist zudem fähig, sämtliche Manipulationen zu melden, falls sie nicht den Vorschriften der Firma entsprechen. Eines gleich vorweg – eine ideale Lösung bietet heute kein Hersteller an. Eine gute Umsetzung von DLP basiert also immer auf einer Kombination verschiedener Techniken sowie dem geschickten Einsatz verschiedener Produkte und Tools.

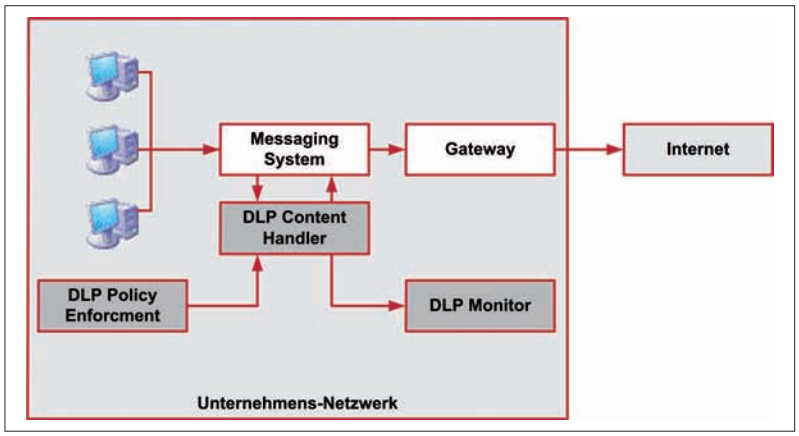

Abb. 1: Schutz der Bewegungsdaten durch Prüfung übermittelter Inhalte

DIE DREI EBENEN DER DLP

Die drei Ebenen einer durchgehenden DLP-Lösung sind der Schutz der Bewegungsdaten (*Data in Motion*), Überwachung der gespeicherte Daten (*Data in Rest*) und Absicherung der Daten auf dem Endgerät (*Data at the Endpoint*). Im Prinzip gehört der Bereich der ausgedruckten Informationen, gemäß einer Studie der Japan Network Security Association, der Weg auf dem 40 Prozent der betroffenen Daten gehen, wenn sie nach außen gelangen, auch zu einer DLP-Lösung [4]. Dieser Bereich wird jedoch oftmals durch Funktionalität auf der Ebene der Bewegungsdaten abgedeckt – wenn überhaupt. Das automatisierte Verhindern vom Verlust oder von der bewussten Weitergabe sensitiver ausgedruckter Daten kann jedoch nur sehr beschränkt durch den Einsatz einer DLP-Lösung gewährleistet werden.

Eine DLP-Lösung verhindert auf der Ebene „Schutz der Bewegungsdaten" die unkontrollierte Kommunikation über das Netz. Folgendes sind typische Szenarien, die es zu verhindern gilt:

- Eine Spitalangestellte sendet vertrauliche Patienteninformationen an die falsche Person
- Ein Angestellter schickt ein sensitives Dokument an seine private E-Mail-Adresse, um zuhause weiterarbeiten zu können
- Ein Webmaster stellt versehentlich private Kundeninformationen in den öffentlich zugänglichen Bereich der Website seines Unternehmens

Um solche Probleme zu vermeiden, überwacht ein DLP-System sämtliche Kommunikationskanäle wie E-Mail, Instant Messaging, FTP und HTTP. Die wichtigste Technik zur Überwachung ist das so genannte *Content Monitoring* oder auch *Content Scanning*. Basierend auf einem Regelwerk, das die unternehmensweiten Richtlinien für den Schutz sensitiver Daten abbildet, wird dabei die gesamte Kommunikation überwacht. Content-Monitoring-Systeme sind ähnlich wie moderne Firewalls oder Intrustion-Detection-Systeme aufgebaut. Mit Sensoren werden die Kommunikationskanäle an verschiedenen Stellen überwacht und Verletzungen der Regeln verhindert.

Auf der Ebene der Überwachung der gespeicherten Daten müssen die drei Aspekte Sichtbarkeit, Zugriff und Sicherheit abgedeckt werden. Sichtbarkeit bedeu-

DLP wirkt auf 3 Ebenen

- Data in Motion: Über das Netzwerk aus dem Unternehmen heraus via Internet transferierte Daten
- Data in Rest: In Dateisystemen, Datenbanken und mittels anderer Speichermethoden abgelegte Daten
- Data at the Endpoint: Auf Endgeräten gespeicherte Daten (Laptop, USB Stick, MP3 Player, Smartphones)

tet in diesem Zusammenhang, dass bekannt ist, wo sensitive Daten überall abgespeichert sind. Gerade in größeren Unternehmen ist das keine einfache Aufgabenstellung, wie zahlreiche Studien zeigen. So geht die Tower Group beispielsweise davon aus, dass zentrale strukturierte Daten eines Unternehmens bis zu elf Mal in verschiedenen Systemen abgelegt werden. Die durchschnittliche Anzahl der Kopien unstrukturierter Daten, wie Office-Dokumente oder -Bilder, dürfte in jedem Unternehmen weit mehr als elf Kopien betragen. Im Schnitt enthält eines von 50 Dokumenten sensitive Daten. Mittels DLP kann ein unkontrolliertes Kopieren dieser Daten verhindert werden. Allerdings ist dazu die Abdeckung des zweiten Aspekts „Zugriff auf vertrauliche Informationen" notwendig. Die wichtigste Fragestellung ist: Wer darf welche Daten wie manipulieren oder einsehen? Die Umsetzung von Zugriffsregeln ist nicht Aufgabe eines DLP-Systems, die Überwachung in Echtzeit der Einhaltung dieser Regeln jedoch schon. Dasselbe gilt für den dritten Aspekt: die Sicherheit. Die sichere Speicherung und allfällige Verschlüsselung gespeicherter Daten wird direkt auf der Ebene der Speichermechanismen realisiert. Die Überwachung der Einhaltung der Regeln und der direkte Eingriff im Falle einer Regelverletzung und das Reporting sind jedoch Sache des DLP-Systems.

Für die Ebene „Absicherung der Daten auf Endgeräten" existiert eine Vielzahl guter und etablierter Lösungen. Von der einfachen Verschlüsselung der Festplatte eines Laptops über USB-Sticks mit automatischen Mechanismen zum Löschen von Daten bis hin zu sich selbst zerstörenden Dateien: Bereits heute ist eine Vielzahl von Technologien verfügbar und weitere werden zurzeit entwickelt. Wichtig für die Absicherung der Daten auf Endgeräten ist jedoch die Gesamtsicht auf den Arbeitsplatz. Dabei steht das Szenario des Verlusts eines Endgeräts im Vordergrund, da gemäß einer Umfrage des Ponemon Institute 42 Prozent aller Sicherheitsprobleme allein durch verlorene Geräte verursacht werden [5]. Zentrale Aspekte der Absicherung sind die Kontrolle der Auslieferung der Endgeräte und der Speicherung der Unternehmensdaten auf diesen Geräten, die Verwaltung der Endgeräte, deren Software und Privilegien sowie die zentralisierte Überwachung verteilter IT-Infrastrukturen.

Ursachen für Sicherheitsprobleme

Gemäß einer Umfrage des Ponemon Institute waren 85 Prozent aller befragten Unternehmen in den letzten 24 Monaten von einem Data-Loss-Problem betroffen. Die wichtigsten Ursachen für Sicherheitsprobleme in Unternehmen sind:

- Verlorene Endgeräte (42 Prozent)
- Nachlässige Angestellte (16 Prozent)
- Nachlässige Externe (10 Prozent)
- IT-Fehler (7 Prozent)
- Kriminelle Aktivitäten (6 Prozent)

ZENTRALE FRAGESTELLUNG: WAS SIND SENSITIVE DATEN?

Die Umsetzung einer Data-Loss-Protection-/Prevention-Lösung auf Unternehmensebene setzt voraus, dass ein Unternehmen überhaupt zwischen sensitiven und nichtsensitiven Informationen unterscheiden kann. Eine einfache pragmatische Klassifizierung aufgrund der Wichtigkeit der Daten für ein Unternehmen ist beispielsweise die Unterscheidung zwischen kritischen Daten, Business-Performance-Daten, essentiellen Daten, sensiblen Daten und nichtkritischen Daten. Kritische Daten sind Daten, die für die wichtigen Geschäftsprozesse benötigt werden und deren Verlust zu einer operativen Katastrophe führen kann (die Unternehmensleistung kann nicht mehr erbracht werden) und Daten, die aus rechtlichen Gründen aufbewahrt werden müssen, respektive auf keinen Fall öffentlich zugänglich gemacht werden dürfen. Business-Performance-Daten sind Daten, die für die Steuerung und die Planung eines Unternehmens relevant sind und deren Verlust zu einer unternehmerischen Katastrophe führen kann. Essentielle Daten sind Informationen, die für das Tagesgeschäft notwendig sind und das Know-how eines Unternehmens darstellen. Sensible Daten hingegen sind leicht wiederbeschaffbar, nichtkritische mehrfach verfügbar. Ein DLP-System ist für die Überwachung der kritischen und der Business-Performance-Daten zuständig, also für Informationen, die aufgrund der Vielzahl gesetzlicher Regulatorien klar definierten Regeln für den Umgang unterliegen. Gleiches gilt für Daten wie etwa Produktinformationen, deren Veröffentlichung bereits mittelfristig zu nachhaltigen Verlusten führen kann. Die Zahlen der Internationalen Handelskammer zum Thema Produktfälschungen und Produktpiraterie belegen eindrücklich diese mittelfristige Problematik. Der Schutz des geistigen Eigentums ist in 53 Ländern sehr schlecht, was fatale Konsequenzen hat. Die Investitionen für Innovationen können nicht amortisiert werden. Nicht zuletzt aufgrund der Tatsache, dass Produkt- und Produktionsinformationen in die falschen Hände gelangen und damit leicht nachgebaut werden können. Der Schaden wird von der Deutschen Industrie- und Handelskammer jährlich auf rund 30 Milliarden Euro alleine in Deutschland geschätzt. Dem gegenüber sind die Kosten einer DLP-Lösung durchaus zu vertreten.

ZENTRALE FRAGESTELLUNG: WIE DEN DATENFLUSS ERFASSEN?

Die zweite zentrale Fragestellung lautet: Wie kann ein Unternehmen die Datenflüsse als Ganzes erfassen, um die richtigen Messpunkte für ein DLP-System festzulegen? Der Fluss sensitiver Daten kann auf dieselbe Art und Weise erfasst werden, wie der Fluss aller Unternehmensinformationen dokumentiert wird. Viele Unternehmen, die mit einer vernünftigen IT-Strategie mit abgeleiteter Anwendungs- und Informationsarchitektur und mit einem guten Governance- und Security-Modell arbeiten, können direkt auf diesen Erkenntnissen aufsetzen. Die Regeln für die Prüfung der DLP-Schutzmaßnahmen können aus den Sicherheitsrichtlinien abgeleitet werden. Der Datenfluss der zu überwachenden Informationen kann aus dem Datenfluss aller Unternehmensdaten abgeleitet oder auch gesondert isoliert werden. Eine bewährte Methode, den Datenfluss als Ganzes zu betrachten ist das Lifecycle-Management von Daten. Ein solcher Lebenszyklus durchläuft typischerweise folgende Phasen: Create (Erzeugen von Daten), Transport (Data in Motion), Modify (lediglich 10 Prozent aller Daten werden täglich verändert), Use/Store (nur auf 20 Prozent aller Daten wird nach einem Monat überhaupt noch zugegriffen) sowie Archive und Shred (gemäß gesetzlicher Vorgaben). Hat ein Unternehmen ein Lebenszyklusmodell umgesetzt und die entsprechenden Zuständigkeiten für die verschiedenen Datenarten festgelegt, so wird die Umsetzung einer DLP-Lösung stark vereinfacht. Zusätzlich zum Datenfluss müssen dann nur noch die Regeln für die Berechtigung der einzelnen internen und externen Mitarbeitenden bezüglich Datenzugriff und Datenmanipulation umgesetzt werden.

Für viele Unternehmen dürfte jedoch der Ansatz, den unternehmensweiten Datenfluss aus Sicht der Anforderungen an ein DLP-System zu erfassen, ein vernünftiges Vorgehen darstellen, da kein unternehmensweites Lebenszyklusmodell besteht. Die Universität Kuwait hat dieses Jahr in der Zeitschrift „International Journal of Digital Content Technology and its Applications“ eine Methodik veröffentlicht, die genau dieses Vorgehen zum Ziel hat [6]. Basis der Methodik ist ein so genanntes *Flowthing Model*, das die Erfassung von Daten, die ausgetauscht, verarbeitet, erzeugt, transferiert und kommuniziert werden, erlaubt. Für sensitive Daten werden solche Flow-Modelle erfasst, um zwei zentrale logische Mechanismen zu etablieren – Prüfkontrolle (*Detective Control*) und Präventionskontrolle (*Preventive Control*). Basis ist der Detective Flow als Karte, die sämtliche Wege, Stationen und Endpunkte eines Datenflusses darstellt. Dies erlaubt die Isolation möglicher „Löcher“ (*Leaks*) und anderer kritischer Problemstellen im Datenfluss. Genau an diesen Stellen werden die Mechanismen für die Prüfkontrolle eines DLP-Systems platziert. Damit jedoch das absichtliche oder unabsichtliche Veröffentlichen von Daten vermieden werden kann, werden zusätzlich Instrumente für die Präventionskontrolle eingesetzt. Sie verhindern, dass überhaupt etwas geschehen kann. Die Präventionsstellen werden ebenfalls auf der *Detective Flow*-Karte des Datenflusses abgebildet. Die Abbildung in eine bestehende Systemlandschaft geschieht anschließend durch eine einfache Zuordnung der Wege, Stationen und Endpunkte des Datenflusses auf die verarbeitenden Systeme. Die Umsetzung der Kontrollstellen und Präventionsinstrumente erfolgt dann aufgrund der Rahmenbedingungen dieser Systeme. Einzig das DLP-Regelwerk und das Monitoring werden als zentrale logische Funktionen realisiert. Die Methodik der Universität Kuwait geht davon aus, dass die sensiblen Unternehmensdaten vorgängig isoliert worden sind und dass ein Modell für den Lebenszyklus der Daten vorliegt.

DIE SCHWIERIGKEIT DER ABGRENZUNG

Data Loss Protection/Prevention kann nur dann durchgängig realisiert werden, wenn die unterstützenden Informationssysteme als Ganzes betrachtet werden. Allerdings ist die Zuordnung der für eine DLP-Lösung notwendigen Funktionalität in einzelne Systeme nicht ganz einfach. Die zentrale Frage ist: Welches System ist für welche DLP-Funktion zuständig? Die typischen Lösungen für Identity und Access Management beispielsweise sind für die Kontrolle des Zugriffs auf Daten zuständig. Je nach bestehender Funktionalität sind diese Lösungen ausreichend, um den Anforderungen hinsichtlich des Zugriffsschutzes zu genügen. Sie müssen nur noch entsprechend umgesetzt werden. Dasselbe gilt für die Verschlüsselung von Informationen. Lösungen für die Datenverschlüsselung auf Ebene der einzelnen Datei, auf Ebene von Festplatten oder USB-Sticks, auf Ebene einer relationalen Datenbank und auf Ebene von Gesamtsystemen sind in den meisten Unternehmen bereits im Einsatz. Die spezifischen DLP-Anforderungen müssen lediglich in den entsprechenden Lösungen implementiert werden. Weitere Beispiele sind Technologien für die digitale Signatur, Filter- und Zugriffsysteme für Websites oder Systeme zur Verwaltung mobiler Endgeräte.

Zwei Aspekte eines DLP-Systems sind jedoch in den meisten Fällen weitaus einfacher als zentrale Funktionalität umzusetzen: das Regelwerk und die Überwachung. Die Erfassung eines Regelwerks ist sinnvoll, um überhaupt den organisatorischen und technischen Rahmen eines DLP-Systems einhalten zu können. Unabhängig davon, welche Regeln genau in welchem Grad überhaupt

erzwungen werden können, ist es für jedes Unternehmen wichtig, die Grundlagen des Umgangs mit sensitiven Daten festzulegen. Im einfachen Fall werden diese Regeln schriftlich festgelegt und sind Teil des „Code of Conduct“ an den sich alle Mitarbeitenden halten sollten. Weitaus anspruchsvoller ist die Formulierung von formalen Regeln beispielsweise für die automatisierte Prüfung kritischer Inhalte von E-Mails oder anderen Dokumenten, die nach außen verschickt werden. In diesem Fall sind die Richtlinien des Unternehmens für den Umgang mit sensitiven Informationen in semantischen Regelsystemen abzubilden, die von spezialisierten DLP-Lösungen für die Prüfung verwendet werden können. Die Überwachung und damit auch das Reporting möglicher Regelverletzungen ist der zweite Aspekt der DLP-Funktionen, der wesentlich einfacher in einer getrennten Lösung umgesetzt wird. Nur so kann sich ein Unternehmen gezielt auf einen möglichen Schadensfall vorbereiten und die entsprechenden Maßnahmen ergreifen. Allerdings ist eine durchgängige Überwachung nur dann möglich, wenn sämtliche an einer DLP-Lösung beteiligten Komponenten auch entsprechende Daten liefern. Dies reicht von der Anzeige eines Geräteverlusts über die Meldung, dass eine E-Mail mit kritischem Inhalt an eine falsche Adresse geschickt wurde, bis hin zum Auffinden fehlgeleiteter Kopien einer sensitiven Datei.

DIE UMSETZUNG EINES DLP-PROJEKTS

Der Umgang mit kritischen Unternehmensinformationen bedeutet nichts anderes als den Umgang mit den wichtigen Unternehmenswertdaten. Die Komplexität der bestehenden Systemlandschaft und die Vielzahl der täglich zu verarbeitenden Daten machen es schwer zu definieren, wo ein DLP-Projekt beginnt und wo es endet. Aus diesem Grund ist es empfehlenswert, das Projekt mit klarem Fokus zu beginnen. In den meisten Fällen ist unkontrollierte Kommunikation der wichtigste Treiber hinter einer DLP-Initiative. Auf jeden Fall helfen die Darstellung der Datenflüsse und die Isolation der kritischen Stellen im Umgang mit Daten. Und ohne eine Identifikation der sensitiven Daten ist eine Umsetzung überhaupt nicht möglich. Dabei muss neben den präventiven Sicherheitsaspekten und den gesetzlichen Vorgaben unbedingt der Wert der Daten für das Unternehmen berücksichtigt werden. Die zentrale Frage lautet: Welche Daten dürfen auf keinen Fall nach außen gelangen?, beziehungsweise: Was schadet dem Unternehmen am meisten? Die Risiken und möglichen Kosten sind zu erfassen und zu klassieren. Allerdings kann kein DLP-Projekt eine fehlende Informationsarchitektur ersetzen. Fehlen beispielsweise die Zuständigkeiten für die zentralen Informationsobjekte oder existiert kein Lebenszyklusmodell für Unternehmensinformationen, so muss das DLP-Projekt auf einen Teilaspekt fokussieren und bewusst diese Aufgaben anderen überlassen. Sonst läuft das Projekt Gefahr aus dem Ruder zu laufen.

Und es ist vor allem eines nicht zu vergessen: Niemand darf durch DLP daran gehindert werden, vernünftig zu arbeiten. Die ideale DLP-Lösung verrichtet ihre Arbeit ohne zu stören im Hintergrund. Eine zu restriktive Anwendung der Regeln für den Schutz sensitiver Daten verhindert eine Akzeptanz der Technologien und Verhaltensregeln.

FAZIT

Unternehmensinformationen, die unkontrolliert an die Öffentlichkeit oder in falsche Hände geraten, können hohe Kosten verursachen und stellen ein großes Risiko für eine Firma dar. Data-Loss-Protection/Prevention-Lösungen helfen, dies zu verhindern. Der Markt für die entsprechenden Produkte wächst stark und es ist zu erwarten, dass in nächster Zeit eine Vielzahl innovativer Ansätze die Umsetzung einer durchgängigen DLP-Lösung auf Unternehmensebene unterstützen wird. DLP ist jedoch weit mehr als eine isolierte Technik, um die elektronische Kommunikation nach außen zu kontrollieren oder die Konsequenzen eines Verlusts von Endgeräten zu minimieren. DLP bedeutet nichts anderes als den sorgfältigen Umgang mit dem immer wichtigeren Unternehmenswert Information als Ganzes. DLP ist in diesem Sinne nicht einfach nur Teil der Sicherheitsrichtlinien, sondern Teil der systematischen Bewertung und klugen Verwaltung strukturierter und unstrukturierter Daten mit dem Fokus auf die unternehmenswichtigen Informationen und des Umgang mit ihnen.

Daniel Liebhart ist Dozent für Informatik an der Hochschule für Technik in Zürich und Solution Manager der Trivadis AG. Er ist Autor des Buches „SOA goes real“ (Hanser Verlag) und Koautor verschiedener Fachbücher.

Links & Literatur

[1] Gijo, Mathew: The Many Faces of Data Loss Prevention, ISSA Journal, March 2010

[2]. Hunter, Bradley R: Data Loss Prevention Best Practices, Ironport Systems July 2007

[3] http://datalossprevention.com

[4] Takebayashi, Tomyoshi; Tsuda, Hiroshi; Hasebe, Takayuki; Masuoka, Ryusuke: Data Loss Prevention Technologies, FUJITSU Sci, Tech. J. Vol. 46, No. 1, January 2010

[5] www.ponemon.org

[6] Al-Fedaghi, Sabah: A Conceptual Foundation for Data Loss Prevention, in: International Journal of Digital Content Technology and its Applications. Volume 5, Number 3, March 2011