Praxis: Die Qualität eines DLP-Systems bewerten

von Bernd Reder, Nikolay Fedotov (Infowatch)
CRN.de, 22.07.2010

Wie gut oder schlecht ist eine Lösung, die das Abfließen von unternehmenskritischen Informationen verhindern soll, Stichwort Data Leak Prevention (DLP)? Viele IT-Manager wissen auf diese Frage keine Antwort. Hier einige Kriterien, anhand derer sich die Qualität von DLP-Systemen bewerten lässt.

Datenlecks sind kein Kavaliersdelikt mehr, über das Firmen und Behörden mit einer gewissen Nonchalance hinweggehen können. Verschärfte Datenschutzregelungen, etwa im Bundesdatenschutzgesetz, und Vorgaben wie das Sarbanes-Oxley-Act und Basel II sehen für den Verlust unternehmenskritischer Informationen teils drastische Sanktionen vor, bis hin zu Haftstrafen für Geschäftsführer und IT-Leiter.

Data-Leak-Prevention ist ein Muss für jedes Unternehmen, nicht nur aus wirtschaftlichen, sondern auch aus juristischen Gründen.

Doch potenzielle Sicherheitslöcher zu stopfen, ist alles andere als trivial. Wie die russische Sicherheitsfirma Infowatch ermittelt hat, geht »nur« die Hälfte der Datenlecks auf kriminelle Machenschaften zurück, etwa durch illoyale oder gefeuerte Mitarbeiter. Fast 43,5 Prozent der Datenverluste geschieht unabsichtlich – durch Fehlbedienung oder Fahrlässigkeit.

Ein Data-Leak-Prevention-System (DLP) soll solche Daten-GAUs verhindern. Hersteller solcher Lösungen gibt es viele, und natürlich verspricht jeder von ihnen dem Interessenten, dieser erhalte »das Beste vom Besten«.

Oft stehen Anwender solchem Marketing-Blabla hilflos gegenüber, selbst dann, wenn es sich um IT-Fachleute handelt. Um wirklich »das beste« System zu finden, sollte der Interessent den Blick auf die unten genannten Kriterien werfen.

Die Menge der kontrollierten Kanäle

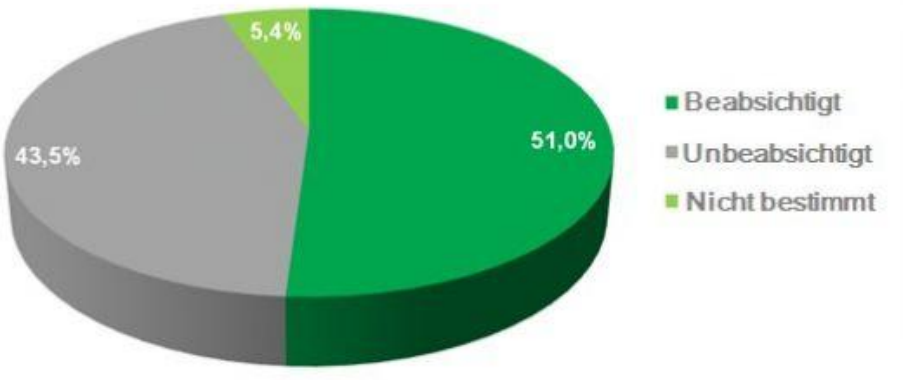
Ein DLP-System sollte möglichst viele Kanäle überprüfen, über die Daten verloren gehen können. Vorsicht ist angeraten, wenn eine Lösung weniger als fünf solcher Wege überprüfen kann. Die Systeme von Infowatch beispielsweise analysieren sechs Datenübertragungskanäle: SMTP, HTTP, ICQ, Netzwerkdrucker, lokale Drucker sowie andere Anschlüsse an Workstations.

Verwirrend für den Anwender ist, dass die Anzahl der Kanäle auf verschiedene Arten gezählt werden kann. Ein Beispiel: Web-Traffic lässt sich als ein möglicher Kanal für Datenverluste festlegen. Doch Internet-Verkehr kann wiederum nach unterschiedlichen Kanälen differenziert werden HTTP, HTTPS oder SOCKS.

Wie »gefährlich« jeder Kanal ist

Unter Technikern existierte die Idee, jeden Kanal mit dem Anteil des über ihn transportieren Verkehrs zu multiplizieren, um die gefährlichsten potenziellen Sicherheitslöcher zu ermitteln. Dies ist jedoch keine gute Lösung.

Denn erstens ist es schwierig, die Menge des Datenverkehrs zu schätzen, der über solche Verbindungen läuft und möglicherweise das Unternehmen verlässt, etwa beim Drucken oder dem



Kopieren auf DVD.

Zweitens unterscheidet sich die Informationssättigung in jedem Kanal. Vertrauliche Informationen werden selten über Peer-to-Peer-Netzwerke übertragen, obwohl über diese normalerweise viel Traffic läuft. Dagegen ist der Anteil von Instant Messengern am Datenverkehr gering; dennoch werden viele wichtigen Informationen über diesen Kanal aus dem Unternehmen hinausbefördert.

Die Anzahl der unterstützten Protokolle und Formate

Wie bereits erwähnt, sollte eine DLP-Lösung möglichst viele Übertragungsprotokolle und Datenformate kontrollieren. Wichtig dabei ist für einen Anwender, dass er prüft, wie viele der Daten, die über sein Unternehmensnetz laufen, diesen Protokollen und Formaten entsprechen.

Es nützt beispielweise nichts, wenn eine DLP-Lösung einen exzellenten Schutz vor Lecks via Instant-Messaging-Systemen bietet, wenn ein Unternehmen den Einsatz solcher Tools untersagt hat und die Einhaltung dieser Policy kontrolliert. Dies lässt sich beispielweise mithilfe von Next-Generation-Firewalls oder eben entsprechenden DLP-Systemen erreichen.

Unterstützung aller verwendeter Sprachen

Eine zentrale Funktion von DLP-Lösungen ist die Kontrolle des Wortlauts von E-Mails oder Dokumenten, die das Unternehmen verlassen. Diese lassen sich auf bestimmte Keywords hin untersuchen.

Allerdings reicht es nicht aus, eine entsprechende Kodierung und das Vokabular (Wörterbuch) hinzuzufügen, wenn Texte in einer bestimmten Sprache überprüft werden sollen. Es ist zudem erforderlich, die Analysealgorithmen entsprechend anzupassen.

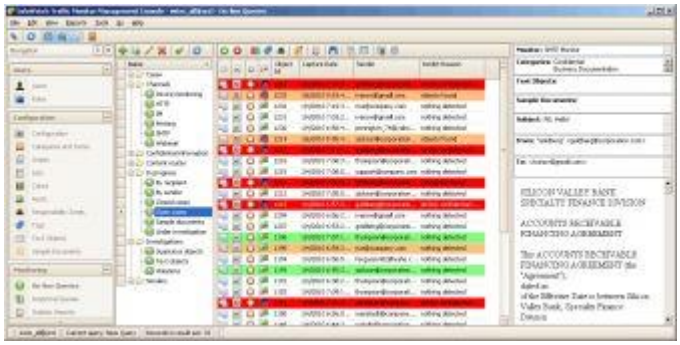
Der Grund ist, dass jede Sprache unterschiedliche Regeln bei der Wortbildung aufweist. Englisch und Chinesisch sind recht einfache Sprachen, was Wort- und Satzbildung betrifft. Die Analyse von Dokumenten, die in Russisch oder Türkisch abgefasst sind, ist dagegen eine höchst komplexe Aufgabe.

Ein Anwender, der eine DLP-Lösung ins Auge fasst, die mehrere Sprachen unterstützt, sollte daher diesen Punkt mit dem Anbieter abklären. Eine allzu grobe »Wald-und-Wiesen«-Analyse von Texten führt dazu, dass entweder zahllose Fehlalarme ausgelöst werden oder Dokumente und E-Mails trotzt DLP-System das Unternehmen verlassen.

Die Anzahl der Warnmeldungen

Wie erwähnt, ist die Zahl der Fehlalarme einer DLP-Lösung ein weiteres Qualitätskriterium. Allerdings hängt dieser Faktor nicht nur vom DLP-System ab. Mitentscheidend ist, welche Sicherheitsregeln ein Anwender definiert und dem System vorgibt.

Allzu eng gefasste Regeln führen dazu, dass die Lösung häufig – und oft zu Unrecht – Alarm auslöst. Umgekehrt gilt das Gleiche: Keine Alarme sind ein Indiz dafür, dass zu laxe Policies gelten. In beiden Fällen sollte der Nutzer die Regeln überprüfen beziehungsweise anpassen.



Treten weiterhin zu viele Fehlalarme auf, deutet dies entweder auf eine schlechte Qualität des DLP-Produkts hin oder das System ist schlichtweg für die speziellen Gegebenheiten in einem Unternehmen nicht geeignet. Das lässt sich im Rahmen einer Teststellung durch den Anbieter eines DLP-Systems herausfinden.

Nutzungsmetriken

Das DLP-System sollte nach der Integration in das Unternehmensnetzwerk mit der Weiterentwicklung der IT-Umgebung Schritt halten. Dies ist leichter gesagt als getan. Denn etwa alle sechs Monate wird eine neue Technologie eingeführt. In jedem Quartal taucht ein neues Datenformat oder Protokoll auf.

Hinzu kommen neue Versionen von Betriebssystemen und Anwendungen. Damit nicht genug: Auch die Geschäftsprozesse in einem Unternehmen ändern sich. Das bedeutet, dass sich auch die DLP-Lösung entsprechend anpassen muss.

Systeme, die zu starr sind, Stichwort mangelnde Upgrade-Fähigkeit und Modularität, sind für die meisten Anwender untauglich. Und wer kann oder will sich schon den Luxus leisten, bei größeren Änderungen an der IT-Infrastruktur oder der Geschäftsprozesse die DLP-Lösung zu ersetzen?

Deshalb wird empfohlen, einen speziellen Indikator zu berücksichtigen, der die Flexibilität eines DLP-Systems beschreibt, etwa wie oft der Hersteller Anpassungen – am besten ohne Aufpreis – herausbringt.

Aufgaben für den Anwender

Allerdings muss auch der Anwender seine Hausaufgaben machen. Wichtig ist beispielsweise, dass regelmäßig überprüft wird, welche Informationen als unternehmenskritisch eingestuft werden. Muster und Signaturen sind entsprechend anzupassen.

Gegebenenfalls müssen beispielsweise neue Schlüsselwörter in die Datenbank der DLP-Lösung eingegeben werden, anhand der das System elektronische Informationen überprüft. Das kann ein neuer Produktname sein, aber auch der Name eines neuen Mitarbeiters oder die Tarnbezeichnung für ein Projekt.

Weitere Aufgaben für die IT-Abteilung:

- die regelmäßige Überprüfung des DLP-Systems und der Arbeitsplatzrechner bezüglich der Funktionsfähigkeit der DLP-Module,
- die Schulung der Mitarbeiter, und zwar bezüglich der Sicherheitsrichtlinien und der Bedienung der DLP-Lösung.

Der Autor: Nikolay Fedotov ist Analytiker beim russischen DLP-Spezialisten Infowatch.

http://www.crn.de/security/artikel-84678.html