Datenschutz und Datensicherheit für Firmen-Macs

Mehr Sicherheit für Firmendaten mit DLP-Lösungen

Beim Thema Datenverlust denken die meisten Administratoren und Firmeninhaber an Hardware-Diebstähle oder Defekte mit Datenträgern. Es gibt aber noch einen Weg, wie vertrauliche Dokumente in falsche Hände gelangen können: über die eigenen Mitarbeiter. DLP-Systeme bieten hier Schutz.

Massenspeicher im System wirkungsvoll gegen den Verlust von wichtigen, vielleicht sogar unternehmenskritischen, Daten wehren. Und gegen gezielte Hackerangriffe schützen fachmännisch konfigurierte Firewalls und eine optimierte Netzwerkstruktur. Diese Sicherheitsmaßnahmen laufen aber gegenüber Innentätern ins Leere.

Ein typisches Beispiel sind Mitarbeiter, die das Unternehmen verlassen wollen, aber wichtige Firmendaten mit zu ihrem neuen Arbeitgeber nehmen wollen. Mit wenigen Klicks landen Kundendaten oder wichtige Konzepte auf einem USB-Stick und anschließend bei der Konkurrenz. Und es muss noch nicht einmal böse Absicht vorliegen. Um rasch am Abend noch die wichtige Präsentation fertigzustellen, schicken sich Mitarbeiter oft die notwendigen Dateien bequem und schnell per E-Mail an das eigene Postfach. Geraten diese Informationen dann in falsche Hände, ist der Schaden enorm. Gegen diesen unerwünschten Abfluss von Daten bieten sich "Data Loss Prevention" (DLP) System an.

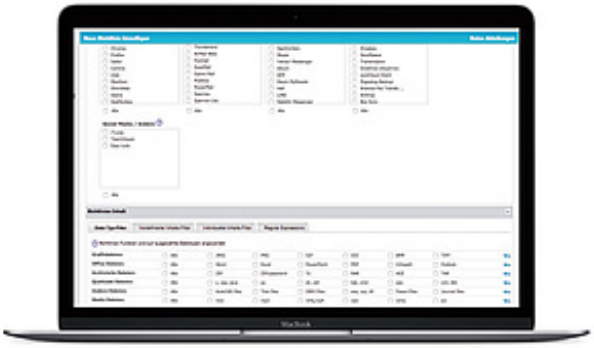
Wenige Hersteller unterschiedlichste DLP-Ansätze.

Der Markt hält eine ganze Reihe von unterschiedlichen DLP-Lösungen bereit. Einzellösungen oder eingebettet in eine Sicherheits-Suite, On Premise oder als Cloud-Lösung. Die Entscheidung für oder gegen ein System ist eine Frage des Budgets und des Sicherheitsbedürfnisses. Ratsam ist es, beim Hersteller entweder (sofern angeboten) zunächst eine Trialversion anzufordern oder ein Gespräch mit dem Sales-Team zu suchen. Denn nicht alles, was als DLP verkauft wird, deckt auch alle Bedürfnisse ab.

DLP arbeitet grundsätzlich auf zwei Ebenen. Zum einen werden schutzbedürftige Daten klassifiziert. Als Orientierung kann das Berechtigungssystem im Unternehmensnetzwerk dienen. Welcher Mitarbeiter muss und darf auf welche Dokumentarten zugreifen? Da bereits Unmengen an neuen Dateien und Informationen während

eines Arbeitstages angelegt werden, genügt die reaktive Überprüfung auf einen bereits vorhandenen Bestand natürlich nicht aus. Deswegen setzen alle Systeme auch auf interne Erkennungsleistung. Der Administrator des Systems legt mittels Schlüsselbegriffen fest, welche Informationen überprüft werden müssen, um dann das Kopieren oder Versenden zu verhindern. So ist es denkbar, dass ein Mitarbeiter des Controllings etwa eine Excel-Datei mit dem Inhalt "Quartalsbericht Cashflow" auch speichern oder versenden darf, der Kollege aus der Kundenbetreuung aber nicht.

DLP-Lösungen bieten dem Administrator üblicherweise Vorlagen, um eigene Regeln entwerden zu können, wie hier beim Endpoint Protector.

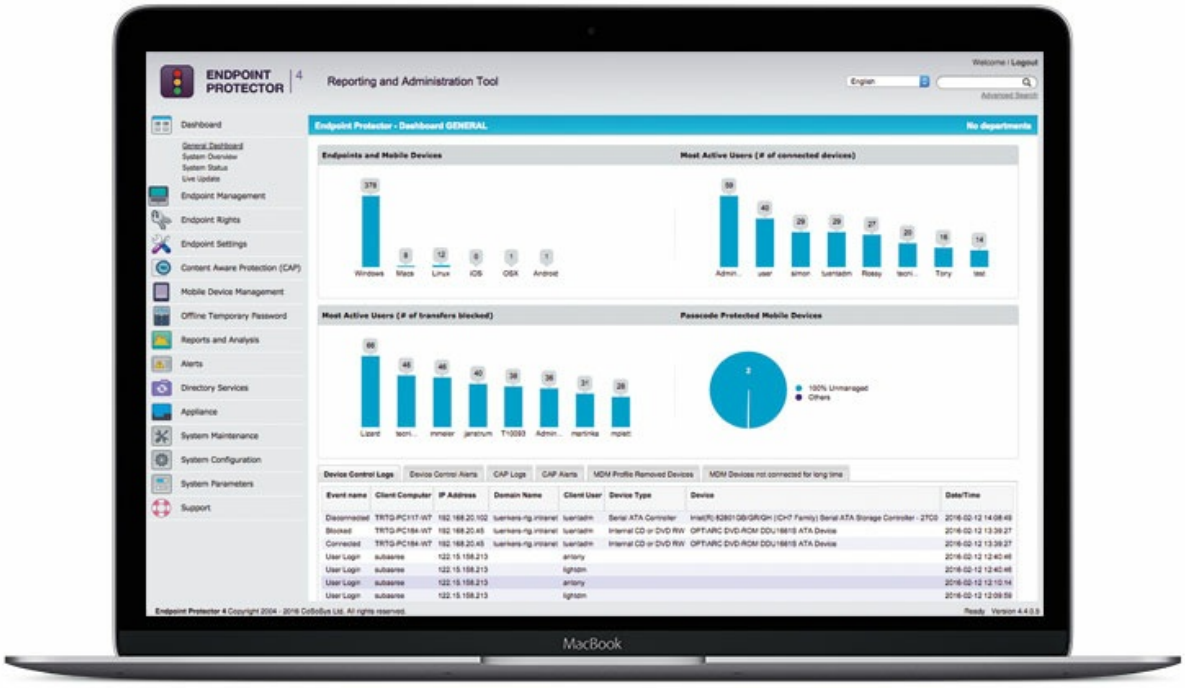


Auf der zweiten Ebene überwachen DLP-Systeme die Schnittstellen der Unternehmens-IT. USB-Ports, E-Mail-Ausgang, Bluetooth usw. Die Administratoren des Systems legen exakt fest, wer an welchem System bestimmte Dateien über eine Schnittstelle weitergeben darf oder nicht. Um nicht bei Null anzufangen, liefern die Hersteller üblicherweise bereits Template und Schablonen mit, die beim Anlegen eines passenden Regelwerks helfen.

DLP-Lösungen basieren auf dem Client-Server-Ansatz. Regeln und Überwachung finden zentral auf dem Server statt. Die Informationen über Aktionen auf dem System des Nutzers werden von darauf installierten Clients geliefert, die im Hintergrund als Dienst ausgeführt werden.

Data Loss Prevention - Datenschutz beachten.

Es liegt in der Natur der Sache, dass eine DLP-Lösung nur dann sicher ist, wenn das Dateimanagement jedes Clients überwacht wird. Das bedeutet aber eben auch, dass die Aktionen jedes Mitarbeiters transparent werden und sich bei der (nicht erlaubten) Auswertung der Protokolle auch Rückschlüsse über die Arbeitsleistung eines Mitarbeiters ergeben. Unternehmen, die DLP einführen wollen, müssen also die Mitarbeiter darüber informieren. Dort, wo es eine Mitarbeitervertretung gibt, unterliegt die Einführung eines solchen Systems der Zustimmung.



Über zentrale Dashboards hat der Administrator alles im Blick. Die Protokollfunktion birgt aber auch das Risiko der Mitarbeiterüberwachung.

DLP-Lösungen mit Mac-Unterstützung.

Bei der Entwicklung ihrer Lösungen haben die die meisten Hersteller auch heterogene Netzwerke aus Windows- und Mac-Systemen im Blick. Das ist bei der zentralen Komponenten allerdings nicht immer der Fall.

- **Endpoint Protector:** Von Endpoint Protector gibt es eine Basisvariante, die gerade kleinere Büros im Blick hat und auch als Mac-Software angeboten wird. Damit können gezielt einzelne Geräte abgesichert werden, zum Beispiel die Macbooks der Außendienstmitarbeiter oder Hardware, die auf Messen zum Einsatz kommt. Für den Schutz der im Netzwerk angemeldeten Geräte wird dagegen die aktuelle Version 4 genutzt. Sie wird als Hardware Appliance angeboten, kann aber auch On Premise, sogar in virtuellen Instanzen, installiert werden. Bei der Einrichtung des Regelwerks helfen Schablonen, die Daten werden inhaltsbasiert klassifiziert und analysiert. Optional ist ein Management für mobile Geräte mit iOS und Android möglich.

Kommt es zu einem Zwischenfall, wird der Admin informiert und kann Datentransaktionen auch nachträglich genehmigen (Proofpoint)

- **Proofpoint:** Die DLP-Lösung von Proofpoint kann On Premise, als Appliance und auch als Software as a Service (SaaS) eingesetzt werden. Das Produkt "Enterprise Privacy" bietet die typischen Komponenten einer solchen Lösung: Scan klassifiziert die Dateien, die Weitergabe wird mit den Client-Diensten verhindert. Derzeit ist aber noch kein Modul vorhanden, das die Hardware-Schnittstellen der Clients blockiert. Im Fokus der Produktfamilie steht die Absicherung von Mail und Cloud.

- **Intel Security:** Das bisher unter den Namen "McAfee DLP" vermarkete Produkt sichert Inhalte und Hardware-Schnittstellen der Clients (Windows und Mac) und kann auch virtuelle Umgebungen auf Basis von VMWare oder Citrix kontrollieren. Die zentrale Instanz zur Definition der Regeln setzt den "ePolicy Orchestrator Server" des Herstellers voraus. Dieser benötigt als Hardwarevoraussetzung allerdings einen Microsoft Server in den Versionen 2008 oder 2012. Damit eignet sich die Lösung nicht für reine Mac-Netzwerke.

- **Symantec DLP:** Gemeinsam mit Intel spielt Symantec in der obersten Liga der Sicherheitslösungen. Als Basis dient entweder ein Microsoft Server, als Alternative ist ein Enterprise Linux von Red Hat möglich. Clients werden sowohl für Windows, MacOS und Citrix angeboten. Auch das Härten von Schnittstellen von Tablet und Smartphone ist integriert. Das Device Management (z.B. für das Verbot zur Installation eigener Apps) hat Symantec aber inzwischen in einer eigenen Produktlinie zusammengefasst.