# Security-Tipps: Wie die Einführung von Data Leak Prevention gelingt

29.02.2016 von Autor: Michael Bauner / Redaktion: Axel Pomper

**Komplexe Security-Lösungen wie Systeme für Data Leak Prevention unterbinden Datenverlust und Datendiebstahl durch Mitarbeiter. Allerdings scheitert die Implementierung einer Lösung häufig an der Befürchtung, das System mit den bestehenden Ressourcen nicht beherrschen zu können. Einfache Bedienbarkeit und vor allem die unternehmensspezifische Abstimmung des DLP-Produktes mit der Hilfe von Experten ermöglichen umfassenden Schutz auch für Unternehmen ohne Spezialisten-Know-how.**


Bildquelle: © Endpoint Protector

Neben Angriffen von außen stellen Datenverlust und Datendiebstahl durch die Mitarbeiter eines Unternehmens eine erhebliche Gefährdung dar. Die Mehrheit der Sicherheits-Verantwortlichen wissen um das Risiko, wie Untersuchungen beispielsweise von IDG oder Techconsult zeigen. An der Implementierung von Schutzfunktionen, die Datenverlust und Datendiebstahl durch Innentäter vorbeugen, hapert es jedoch, vor allem in kleineren und mittelständischen Unternehmen.

**Was DLP-Lösungen leisten**

Umfassende Lösungen für Data Leak Prevention, die sämtliche Datenbewegungen im Unternehmen überwachen und sich als komplementär zu Security-Produkten wie Virenschutz und Firewall verstehen, sind technisch sehr komplex und gelten als aufwendig und teuer. Sie enthalten neben der Funktionalität für die Überwachung der an den Endpoints angeschlossenen Devices eine Komponente, die Inhalte und Formate von Dateien prüft. Zusätzlich können Verschlüsselungsoptionen integriert sein sowie ein Modul für Mobile Device Management, sodass alle Geräte im Unternehmen über eine Oberfläche überwacht und administriert werden können. Allerdings trauen sich viele Unternehmen angesichts knapper Ressourcen für IT-Sicherheit Einrichtung und Betrieb einer solchen Lösung nicht zu; sie befürchten langwierige Implementierungsphasen oder gar das Scheitern des Projektes.

**Die technische Umsetzung**

Die derzeit am Markt erfolgreichen Anbieter von DLP-Lösungen kommen den Unternehmen deshalb in drei Bereichen entgegen. Zunächst stehen Produkte der jüngsten Generation kostengünstig als vorinstallierte Hardware- oder virtuelle Appliances zur Verfügung, die mit minimalem Aufwand und Anpassungsbedarf eingerichtet werden

können. Als Cloud-Dienste eignen sie sich selbst für kleine Unternehmen und Büros. Weiterhin sorgen Benutzeroberflächen mit übersichtlicher Gliederung und detaillierten praxisorientierten Einstellmöglichkeiten für die Policies für eine nahezu voraussetzungslose Bedienbarkeit, so dass die komplexen Aufgaben von Data Leak Prevention einfach und komfortabel und ohne Spezialkenntnisse umzusetzen sind.

## Beratung ebnet den Einstieg

Ob die Einführung der DLP-Lösung gelingt, steht und fällt mit der Vorbereitung. Die Anbieter stellen deshalb zum dritten den Einsteiger-Unternehmen Beratung durch Experten zur Verfügung, die die Anpassung der Lösung an die unternehmensspezifischen Gegebenheiten begleiten. Der Berater führt das Unternehmen durch einen Prozess, in dessen Verlauf gemeinsam die Voraussetzungen für den Einsatz der Lösung geklärt und passende Policies erarbeitet und technisch umgesetzt werden. Im Vordergrund steht dabei das Vorgehen nach Wichtigkeit und Dringlichkeit, damit die Lösung möglichst zügig in den Produktivbetrieb gehen kann und die Grundlage für kommende Anpassungen und Verfeinerungen gelegt ist.

**Schutzziele erarbeiten**

Zunächst unterstützt der Berater das Unternehmen bei der Bestimmung und Klärung der Schutzziele, wobei interne Ziele ebenso berücksichtigt werden wie externe Vorgaben. Im zweiten Schritt werden die Daten festgelegt, die aus unternehmerischer Hinsicht und aufgrund gesetzlicher Bestimmungen besonders schutzwürdig sind. Die Zuordnung erfolgt pragmatisch; der Stellenwert größerer Datenmengen wird sich in diesem ersten Durchgang nicht eindeutig festlegen lassen. Über sie muss zu einem späteren Zeitpunkt entschieden werden.

**Ausgangslage ermitteln**

Ist das DLP-System installiert und die je nach Produkt erforderliche Client-Software auf die Endpoints verteilt, sollte die Lösung zunächst im Monitoring-Modus betrieben werden. Erfahrungsgemäß ist ein Beobachtungszeitraum von wenigen Wochen in einer möglichst aktiven Abteilung, beispielsweise dem Marketing, ausreichend. Dabei werden alle Transfer-Aktivitäten erfasst und aufgezeichnet, aber noch keine Warnungen oder Restriktionen gesetzt. Durch das Monitoring wird ermittelt, welche Devices, welche Schnittstellen und Tools die Mitarbeiter überhaupt nutzen, welche Dateien wohin bewegt oder geteilt werden, welche Mitarbeiter und Gruppen aktiv sind.

## Datenbewegungen analysieren

Den Ist-Zustand hinsichtlich der Datenbewegungen wertet der Berater in Hinblick auf die Schutzziele des Unternehmens aus und ermittelt den Handlungsbedarf: Welche Aktionen muss das Unternehmen aus Gründen des Datenschutzes unterbinden, welche sollten blockiert werden, weil die Risiken mit den verfügbaren Ressourcen nicht zu beherrschen sind? Welche Mitarbeitergruppen müssen bestimmte Datenbewegungen durchführen können, um ihre Aufgaben zu erfüllen? Daraus werden die Policies entwickelt: beispielsweise keine unbekannten USB-Sticks an den Endpoints zulassen, die Übermittlung personenbezogener Daten in Cloud-Speicher unterbinden, jegliche Transfer-Aktionen von Dateien mit mehr als fünf Kontonummern blockieren.

**Policies einrichten**

Damit ist die Richtung für die technische Umsetzung in der DLP-Lösung vorgegeben; der Administrator im Unternehmen agiert ab diesem Prozessschritt eigenständig. Er erstellt für die Inhaltsüberwachung ein Wörterbuch mit unternehmensspezifischen Signalwörtern und aktiviert Einschränkungen auf der Benutzeroberfläche der Lösung einfach per Klick. Je nach den Schutzzielen kann er definierte Aktionen blockieren oder die Mitarbeiter vor potenziell gefährlichen Datentransfers warnen lassen. Unter Umständen kann es beim reinen Monitoring bleiben, das als Frühwarnsystem für Trends im Mitarbeiterverhalten dient und etwaige Datenverluste nachvollziehbar und nachweisbar macht.

**Policies kontinuierlich anpassen und verfeinern**

Data Leak Prevention ist als Prozess zu verstehen, bei dem die Datenbewegungen fortlaufend beobachtet, ausgewertet werden und über die DLP-Lösung reguliert werden. Die zunächst nicht klassifizierten Daten müssen nach und nach aufgearbeitet werden; der Datenbestand im Unternehmen wächst und muss ebenfalls berücksichtigt werden. Technische Neuerungen, aber auch neue Mitarbeiter beeinflussen die Kommunikationsgepflogenheiten im Unternehmen und müssen in den Policies abgebildet werden; Sicherheitsanforderungen Dritter werden verschärft.

Als Prozess auf einer technischen Grundlage verhindert Data Leak Prevention mit sehr hoher Zuverlässigkeit versehentliche oder durch Anwenderfehler verursachte Datenverluste und stellt Datendiebstahl hohe Hürden in den Weg. Die Unterstützung durch geschulte Berater ebnet den Einstieg, die einfache Bedienbarkeit der Lösung ermöglicht dann den eigenständigen Betrieb.

*Michael Bauner ist Geschäftsführer von Endpoint Protector*

*Redaktion: ap*