Sag mir, wo die Daten sind

Michael Bauner (Experte)

Die Sicherheitsinfrastrukturen mittelständischer Unternehmen sind überwiegend auf den Schutz vor Angriffen von außen ausgelegt. Datenverlust und Datendiebstahl erfolgen jedoch mehrheitlich aus dem eigenen Unternehmen heraus, wie der IBM Cyber Security Intelligence Index 2015 aufzeigt.

Ob erlaubt oder mit kriminellen Hintergedanken - Firmendaten sollten nur kontrolliert das Unternehmen verlassen.
Foto: alexskopje - shutterstock.com

Schließlich sind die Mitarbeiter diejenigen, die täglich mit den Daten umgehen. Zunehmende Mobilität, eine Vielzahl von Geräten und Kommunikationstools sowie kontinuierlich wachsende Datenmengen erhöhen die Wahrscheinlichkeit, dass Daten gestohlen werden oder versehentlich die Firma verlassen. Die Unternehmen stehen deshalb vor der Aufgabe, den Schutz ihrer Daten auszuweiten.

Viele reden darüber, aber kaum einer macht es

Laut Studienbericht zu Wirtschaftsschutz im digitalen Zeitalter, den der Branchenverband Bitkom 2015 herausgegeben hat, geben weniger als 30 Prozent der befragten Unternehmen an, dass sie über eine Lösung für Data Leak Prevention (DLP) verfügen. Experten schätzen allerdings, dass der Anteil der Firmen, die DLP, also die Überwachung der Schnittstellen sowie der Inhalte der Dateien, die das Unternehmen über die unterschiedlichen Schnittstellen verlassen, tatsächlich betreiben, bei weniger als zehn Prozent liegt.

Viel besser als ihr Ruf

DLP-Systeme sind in der Tat in Ihrer Wirkungsweise hochgradig komplex. Das heißt aber nicht, dass die Komplexität an die IT-Administratoren durchgereicht wird. Zum einen sind moderne Lösungen "out of the box" als vorinstallierte Hardware- oder virtuelle Appliances auf dem Markt, die sich mit wenig Aufwand und Anpassungsbedarf in Betrieb nehmen lassen. Kostengünstige Systeme oder Cloud-Dienste eignen sich auch für mittlere und kleine Unternehmen und Büros. Zum anderen umfasst eine gute DLP Lösung heute Funktionalitäten und vordefinierten Regeln nicht nur für die Schnittstellen-Kontrolle, sondern auch für die Content-Überwachung, ohne dass spezielle Fachkenntnis vorausgesetzt wird.
Die eigentliche Herausforderung von DLP liegt in der Vorbereitung.

Analysten ebnen den Weg

Auch diese muss ein Unternehmen nicht alleine stemmen. Wo Ressourcen und Know-how dafür fehlen, ebnet ein entsprechend geschulter Analyst oder Berater, in Zusammenarbeit mit dem Unternehmen, den Einstieg in DLP. So werden die Schutzziele unter Berücksichtigung externer Vorgaben entwickelt und geklärt und sehr pragmatisch die Daten festgelegt, die aus unternehmerischer Hinsicht und aufgrund gesetzlicher Bestimmungen besonders zu schützen sind. Über Daten, die sich in einem ersten Durchgang nicht eindeutig zuordnen lassen, wird zu einem späteren Zeitpunkt entschieden. So etabliert sich ein kontinuierlicher Verbesserungsprozess.

EU-Datenschutzreform 2016: Die wichtigsten Änderungen

1/15

- 

Ein Gesetz für alle

EU-weit gelten die gleichen Datenschutzregeln. Das bedeutet auch eine gestiegene Verantwortung und Haftung für alle, die persönliche Daten verarbeiten.
Foto: Yvonne Bogdanski - Fotolia.com

Weiterhin berät der Analyst bei der Auswahl der passenden Lösung. So kann für ein Unternehmen, das Compliance nachweisen muss, beispielsweise eine in die Antivirenlösung integrierte Basis-DPL-Funktionalität passen. Einem anderen Unternehmen, das Endpoints mit unterschiedlichen Betriebssystemen oder gesamte Netzwerke mit ausgefalleneren Rechnern wie Macs, Linux-Rechnern oder Thin Clients überwachen muss, mag er den Einsatz einer Best-of-Breed-Lösung empfehlen. Diese warten dann auch meist mit komfortablen Funktionen wie Reports auf Knopfdruck und einfacher, intuitiver Bedienung auf.

Datenbewegungen überwachen und blockieren

Ist das System installiert, wird es zunächst einmal im Monitoring-Modus betrieben, um die Datenbewegungen aufzeichnen:

- Welche Schnittstellen und Geräte, welche browserbasierten Tools nutzen die Mitarbeiter überhaupt?
- Welche Dateien werden auf USB-Sticks oder Notebooks kopiert, auf DVDs gebrannt, über Dropbox oder TeamViewer geteilt?
- Welche Mitarbeiter und Gruppen werden aktiv?

Der Ist-Zustand wird im Hinblick auf die Schutzziele ausgewertet:

- Welche Aktionen bergen Risiken, welche Kommunikationstools lehnen wir grundsätzlich ab?
- Welche Mitarbeitergruppen müssen bestimmte Aktionen durchführen können, damit sie ihre Aufgaben erfüllen können?

Das Ergebnis der Analyse gibt dann die Richtung für die technische Umsetzung in der DLP-Lösung vor. Dabei kann es beim Monitoring bleiben, das als Frühwarnsystem für Trends im Mitarbeiterverhalten dient und etwaige Datenverluste nachvollziehbar und nachweisbar macht. Zudem können Mitarbeiter vor potenziell gefährlichen Aktionen gewarnt werden; in der höchsten Eskalationsstufe werden definierte Aktionen blockiert.

Data Leak Prevention als Prozess

Die Arbeit mit einer DLP-Lösung ist als Prozess zu verstehen, bei dem die Datenbewegungen kontinuierlich ausgewertet und ihre Regulierung an Veränderungen in Unternehmen und Umfeld angepasst werden. Neue Mitarbeiter bringen andere Kommunikationsgewohnheiten mit, neue Inhalte entstehen, neue rechtliche Bestimmungen und Vorgaben seitens Dritter, beispielsweise im Rahmen des IT-Sicherheitsgesetzes zum Schutz kritischer Infrastrukturen, müssen umgesetzt werden.

Selbstverständlich bietet eine DLP-Lösung, wie jede andere Sicherheitslösung, keinen hundertprozentigen Schutz. Sie verhindert aber mit sehr hoher Zuverlässigkeit Datenverluste, die versehentlich, durch Unachtsamkeit oder Bedienerfehler entstehen können. Gegen Datendiebstahl baut sie hohe Hürden auf, die nur mit viel krimineller Energie und technischem Know-how zu überwinden sind.