



DLP BEST PRACTICE SCHNELLE ERFOLGE - NACHHALTIGE RISIKOMINIMIERUNG

Daten sind wie jedes Eigentum vor unberechtigter Mitnahme und Diebstahl zu schützen - da sind sich alle einig. Doch wie macht man das am besten? Wie kann man möglichst schnell nachweisbare Erfolge erbringen und wie vermeidet man die versteckten Fallen in den DLP (*Data Leakage Prevention*) Projekten?

Kritikalität erkennen

Einem Bit sieht man nicht an, ob es vertraulich, verschlüsselt oder öffentlich ist. Ein vertraulicher Inhalt ist als Ausdruck, Teil eines Archives (z.B. zip-File), Kopie eines Bildschirms, verschlüsselter Mail-Anhang oder eingebettet in eine Powerpoint Datei immer noch vertraulich. Repräsentationen des Textes, z.B. ü/ue, Klein-/Großbuchstaben, 8-bit/16-bit Repräsentation, ASCII, DOS, EBCDIC und viele Varianten erschweren die Wiedererkennung. Beim Etikettieren (neudeutsch: *labeln*) nach Kritikalität („öffentlich“, „vertraulich“ etc.) bringt jeder vollautomatische Prozess Unschärfen mit sich.

Rechteprüfung

Für die richtige Entscheidung in Echtzeit benötigt man noch die wesentliche Information, in welchem Kontext gerade gehandelt wird. Das Backup lokaler Daten auf eine DVD, verschlüsselt mit einem nur innerhalb der Firma verwendbaren Unternehmensschlüssel ist ok, das Mitnehmen der gleichen Daten mit einem Transportschlüssel durch einen Auszubildenden soll verhindert werden. Die echte Entscheidung wird also immer situationsabhängig sein und muss dennoch proaktiv in der gültigen Sicherheitsrichtlinie verankert sein.

Fallen vermeiden

Die häufigsten Fehler bei DLP Projekten:

1. Wer zuerst versucht alle vorhandenen Daten nach deren Kritikalität zu markieren - und dafür viel Zeit und Energie aufbringt - wird lange auf die erwarteten positiven Resultate warten. Das eigentliche Ziel, Daten vor unerlaubtem Abfluss zu schützen, wird man dann nicht mehr erreichen.
2. Ignoriert man die systembedingten Ungenauigkeiten in der Klassifikations-Phase werden viele „falsche Fehler“ (neudeutsch: *false positives und false negatives*) dazu führen, dass man im Betrieb entweder häufig nachbessert und hohe administrative Kosten generiert oder die

echten Schutzkriterien so lax einstellt, dass das Ergebnis den Aufwand nicht mehr wert ist. Der Unmut über die systembedingte Ungenauigkeit steigt so mit der Zeit und gefährdet das Projekt.

3. Liegt der Fokus nur auf dem Datenabfluss, verstellt man den Blick auf Angriffe von außen, die erst im Ergebnis zum unerwünschten Datenabfluss führen. Häufig wird über Angriffe auf die Schwachstellen von Standardanwendungen (InternetExplorer-Exploit) oder Standardformate (PDF-Exploit) erst der unerwünschte Datenkanal nach außen geöffnet. Der Angriff kommt aber von außen, weshalb es zu einer wesentlichen Aufgabe des DLP gehört den „Import von schädlichen ausführbaren Objekten“ zu kontrollieren oder ganz zu verbieten, z.B. Java-Skript in PDF, DLL-Download über Browser etc.

Best Practice Phase 1

Einfache, weil im Betrieb unkritische Sicherheitsmaßnahmen (neudeutsch: *Quick Wins*) sind zuerst an der Reihe. Die potentiellen Leckagepunkte sind schnell benannt: Netzkontaktpunkte und lokale Kontaktpunkte über Kabel oder Luftschnittstelle (Bluetooth, WLAN...), kommunizierende Anwendungen (Email, Browser...) und mobile Datenträger. Die Schutzmaßnahmen sollten im ersten Schritt so gewählt werden, dass der Betrieb nicht behindert wird. Das heißt Maßnahmen wie Benutzersensibilisierung, Monitoring und Alerting stellen die ersten Schritte dar und erlauben es die Kritikalitäts-Einschätzungen iterativ zu verfeinern. Die zyklische Untersuchung der statistischen Auswertungen zeigt zum einen die realen Risiken und pragmatische Verstöße gegen die bestehenden Vorschriften auf. Bereits nach dieser ersten Phase, die mit wenigen Arbeitsstunden erledigt ist, kann man klare Antworten auf die drängende Frage „Wie sicher sind wir?“ geben.

Best Practice - weitere Schritte

Das bildet die Grundlage für die regelmäßigen Verfeinerungen der technischen Sicherheitsmaßnahmen wie Blockade und Zwangsverschlüsselung, die erst in der zweiten Phase in die fallspezifisch adäquate Maßnahme münden. Je nach Applikation, Netzwerk, Datenträger, handelndem Benutzer und natürlich identifiziertem Dateninhalt werden folgende Maßnahmen erzwungen: Verschlüsselung mit Unternehmensschlüssel oder persönlichem Schlüssel, Bewusstseins- oder Wissensbildende Informationen über das konkret identifizierte Risiko an den Anwender in Echtzeit, elektronische Willenserklärung zum Haftungsübergang, revisions sichere Beweiserhebung oder auch Blockade. Bei der Wahl eines technischen Produktes ist es wesentlich, dass auch eigene algorithmische Prüfungen und solche von Drittprogrammen eingebunden werden können, so dass eine Sequenz voneinander abhängiger Prüfungen nach unterschiedlichen Kriterien entsteht. Mittelfristig sollte man dann die sensibelsten Daten in eigenen Sub-Netzen (*Read up - No write down*) sammeln und diese Sub-Netze nur über virtuelle Mechanismen einbinden.

Fazit

Bei der richtigen Wahl der Lösung kann man auch bei dem komplexen Thema DLP Investitionsschutz, Skalierbarkeit, Zukunftsfähigkeit und Kosteneffizienz im Betrieb mit einem schnellen Projekterfolg kombinieren. Am besten natürlich technisch unterstützt mit einem Werkzeug, welches das Risikomanagement und die Schutzfunktionen in einem Produkt anbietet und dadurch die Lebenszyklen von Risiken und Daten vollständig abbildet.

Kontakt

info@itWatch.de für Produktanfragen,
PR@itWatch.de für Presseanfragen,

per Telefon unter 089 / 620 30 100
oder **besuchen Sie uns:** www.itWatch.de

itWatch GmbH
Stresemannstraße 36
D-81547 München