# Data Loss Prevention

Data Loss oder Leakage Prevention (DLP) schützt das Unternehmen vor dem unerwünschten Abfluss von Information. Alle Unternehmen haben ein Interesse daran, dass ihre Daten nicht einfach unerlaubt abwandern. Leider gibt es keinen magischen Knopf, den man nur drücken muss und der Abfluss der sensiblen Daten ist verhindert.


Das Projektteam sieht sich also bei der Umsetzung Herausforderungen gegenüber, die anschließend analysiert und mittels Best Practice zu kurzfristig umsetzbaren Lösungen geführt werden.

Folgende Themen gilt es im Projekt zu bearbeiten:

1. Welche Daten sind schützenswert, woran können sie in Echtzeit erkannt werden. Wer darf auf diese Daten zugreifen – in welchen Prozessen werden sie verwendet?
2. Welche Datenaustrittspunkte (potentielle Leckagestellen)gibt es im Netzwerk?
3. Was ist eine geeignete Kontrolle, die an diesen Leckagestellen etabliert werden muss?
4. Wie kann mit „Sonderfällen“ umgegangen werden?

## Kritikalität der Daten

Einem einzelnen Bit kann man sicher nicht ansehen, ob es vertraulich, verschlüsselt, streng geheim oder öffentlich ist. Alle Texte bestehen aus den gleichen Buchstaben. Das Wort „Kündigung“ zum Beispiel ist nur in einem bestimmten Kontext vertraulich. Ein vertrauliches Dokument kann unterschiedliche Repräsentationen haben: Ausdruck, Teil eines Archives (zum Beispiel zip-File), ein Abzug des Bildschirminhalts als Bild (etwa als jpeg-Format), verschlüsselter Mail-Anhang, eingebettet in ein anderes Objekt (zum Beispiel in ein Powerpoint-Objekt), steganografisch eingebettet und viele andere Möglichkeiten. Zudem erschwert die Umformung von Text, zum Beispiel „ü“ zu „ue“, Kleinbuchstaben zu Großbuchstaben, 8-bit Repräsentation in 16-bit Repräsentation, ASCII, DOS, EBCDIC etc. die Handhabung. Können also alle Dateien vollautomatisch entsprechend ihrer Kritikalität mit Etiketten wie „öffentlich“, „firmenvertraulich“, „vertraulich“, „geheim“ oder ähnlich versehen werden (neudeutsch gelabelt)? Jeder vollautomatische Prozess wird hier eine Reihe von Unschärfen mit sich bringen, die es später - wie unter Punkt 4 oben erwähnt - wieder im Betrieb „einzufangen“ gilt. Das ganze gleicht einer „Sisyphus“-Arbeit, denn in

größeren Unternehmen fallen während der Etikettierung bereits wieder viele neue Daten und Repräsentationen alter Daten an, die dann erneut etikettiert werden müssen.

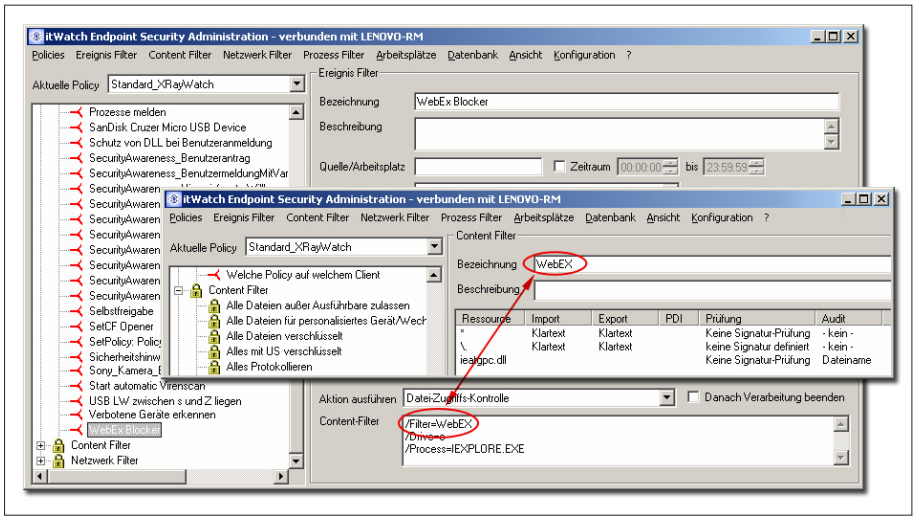


Bild 1: DLP bei Applikationen. (Quelle: itWatch GmbH)

tionsverschlüsselung) lösen hier nur wenige Herausforderungen, da der Bedarf an Vertraulichkeit im Bereich DLP von den Dateiinhalten, bezeihungsweise dem Sicherheitsetikett und ihrer Sensitivität abhängt und nicht alle Daten einheitlich behandelt werden sollen.

## Leckagepunkte

Den oben angegebenen Leckagepunkten geht man am besten systematisch auf den Grund. Einige der Leckagepunkte sind sicherlich durch Firewall, Content Filter auf dem SMTP Gateway und ähnliche Verfahren bereits bewacht. Bei der weiteren Betrachtung stellt man fest, dass man DLP ohne Endpoint Security nicht umsetzen kann, da man vielen Leckagepunkten nur auf dem Endpunkt begegnen kann: USB, Firewire, http-s über den Browser etc.

- Datenträger Kontrolle –
  Wer darf welche Daten in welchem Format auf welchem Datenträger mitnehmen.

- Device Kontrolle –
  Welche Kommunikationsgeräte, zum Beispiel Modems, PDA, Peer to Peer Kommunikation über Bluetooth, dürfen verwendet werden? Welche Daten dürfen über diese Kommunikationsgeräte versendet werden? Gibt es Einschränkungen bezüglich der Empfänger?

- Verschlüsselung der mobilen Daten –
  Die klassischen Verfahren (etwa Parti-

- Personalisierung von Datenträgern –
  Günstige Datenträger verfügen über keine individuellen, sicheren Merkmale wie Seriennummern. In besonders kritischen Bereichen (Vorstand, Akquisition, Stabsabteilungen) erfordert die Compliance, wesentliche Datenbewegungen beweissicher abzulegen. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier ein effizientes Mittel, da die Firmenzugehörigkeit eines Datenträgers auch bei günstigen Datenträgern authentisiert werden kann.

- Kontrolle der Anwendungen –
  Zuallererst ist es wichtig, dass Sie alle in Ihrem Netzwerk verwendeten Anwendungen kennen. Es genügt hier nicht die installierten Anwendungen zu inventarisieren – es müssen auch alle portablen Anwendungen automatisch in Echtzeit erfasst werden, um die automatisierte Datenumwandlung sicher zu erkennen (auch steganografische Verfahren) und gegebenenfalls zu verhindern. Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus Kosten-Gründen den Einsatz von White- UND Blacklists.

- Rechte der Anwendungen:
  Die Umsetzung „Welche Dateien darf eine Anwendung denn Lesen?“ löst das DLP-Problem an der Wurzel. So darf beispielsweise der Browser keine vertraulichen Informationen lesen – dann kann der böswillige Benutzer diese auch nicht über http-s in das Internet laden. Im Beispiel (siehe Bild 1) ist eine technische Einstellung dargestellt, wie der Zugriff auf WebEx als Plug-In in den Internetexplorer zwingend verhindert werden kann. Wichtig ist hier, dass der gleich eContent Filter, der auch schon den USB-port „bewacht“ auch den Leckagepunkt „Browser“ bewacht, so dass es keine zusätzlichen Aufwände im Betrieb gibt.

- Protokollierung des Dateiaustausches –
  Verschlüsseln, Blockieren und Freigeben alleine genügt im DLP-Umfeld nicht. Die Beweisbarkeit von Datenbewegungen ist in vielen IT-Umgebungen zum kritischen Faktor geworden. Die Begrenzung der Protokollvolumina durch geeignete Verfahren ist hier zwingend; insbesondere, wenn die gesamten Dateninhalte (also nicht nur Dateinamen) protokolliert werden müssen. Die Planbarkeit und die Zielkontrolle von DLP Projekten hängen eng an der Möglichkeit des Monitorings. Neue Leckagepunkte oder Angriffe werden zuerst über das Monitoring erkannt und dann in das aktive Risikomanagement übergeben, so dass der Prozess IT-Sicherheit davon geeignet profitiert.

- Kontrolle der verwendeten Netze –
  Entsprechend des erkannten Netzes muss die Security Policy in Echtzeit darauf eingestellt werden, zum Beispiel Heimarbeitsplatz, Firmenzentrale, Standort Produktion, Schulung, etc., sonst kann der Angreifer zu Hause das Firmennetz nachbauen und die

„heiligen“ Daten einfach auf ein Fileshare schreiben, welches dem Fileshare im Firmennetz in allen Aspekten entspricht.

- Alerting –
  Die Benachrichtigung der bereits etablierten Intrusion Detection Verfahren, also die unkomplizierte Integration in Drittprodukte, ist hier genauso wichtig wie die Möglichkeit, Echtzeitreaktionen auf kritische Ereignisse zu konfigurieren. Denn manchmal ist auch der berechtigte Benutzer ein Angreifer – ein sogenannter Innentäter, wie die Fälle in Liechtenstein oder bei der Deutschen Telekom belegen.

- Management Information, Reports und Quota-Management
  (Datenmengen-Management) geben historische oder Echtzeit-Auskunft über die Datenbewegungen nach Formaten und anderen Kriterien sortiert und liefern natürlich auch Erkenntnisse über potentielle Angriffe bzw. neue Risiken im IST-Betrieb.

## Geeignete Maßnahmen

Die oben erwähnten Maßnahmen Verschlüsselung Beweissicherung, Blockade, Freigabe (unter Auflagen) sind natürlich jeweils abhängig von der Umgebung, von dem angemeldeten Benutzer, dem Systemzustand des PCs oder Notebooks, zum Beispiel unterwegs oder im Hausnetz, und vielen weiteren Faktoren. Bei der Verschlüsselung ist am Beispiel eines Trainees klar, dass die Mobilität der Daten gewünscht, der Transport in Fremdnetze nicht gewünscht ist. Durch die Verwendung einer Zwangsverschlüsselung mit einem nur im Unternehmen verwendeten Schlüssels (Firmenschlüssel) kann diese Anforderung leicht erfüllt werden. Für den Außendienst ist diese Einstellung aber nicht zielführend.

## Sonderfälle

Wie oben begründet findet sich eine hohe Unschärfe in der vollautomatischen Klassifikation der Daten. So gibt es zwei unterschiedliche Fehlerfälle:

1. Zu unrecht abgewiesen
2. Zu unrecht erlaubt

### Infobox:

Mehr zu Anforderungen und Lösungen können Sie in dem White Paper „Endgerätesicherheit - Das braucht man wirklich“ nachlesen auf www.itWatch.de unter Downloads.

Wie in allen unscharfen Sicherheitsbeurteilungen ist hier der geschulte Benutzer die letzte Bastion. Für den Fall „Zu unrecht abgewiesen“ sollte man dem Benutzer, je nach seiner Vertrauenswürdigkeit, die Möglichkeit geben, in Echtzeit eine neue Klassifikation für das Dokument zu erwirken. Gut geschulte und vertrauenswürdige Mitarbeiter können diese Klassifikation tatsächlich ändern – andere Mitarbeiter müssen zunächst in einem Online Dialog die Änderung beantragen. Bei „zu unrecht freigegebenen Dokumenten“ muss man auf die gut geschulten Mitarbeiter setzen und die Daten im laufenden Betrieb neu klassifizieren lassen.


Bild 2: Die Datenlecks im Griff. (Quelle: itWatch GmbH)

## Projektlaufzeit als kritischer Faktor

Ob man ein Etikett an allen Dateien oder ein „klassifiziertes“ Subnetz, ein Digital Rights Management (DRM) System oder andere Verfahren zur Etikettierung verwendet, oder in Echtzeit nach Schlagworten im Text sucht, ist bezüglich der Projektlaufzeit relevant. Möchte man früh die «Früchte» des Projektes ernten, dann sollte man auf lange Vorlaufzeiten verzichten. Die beste Strategie liegt also darin eine flexible Infrastruktur als Lösung zu wählen, welche folgende Punkte erfüllt:

- Beliebige Drittprodukte können später eingebunden werden, um die Dateien zu etikettieren und die Etikette dann jeweils in Echtzeit auszuwerten.
- Alle Leckagepunkte können mit einer zentral verwalteten Lösung mit den geeigneten Maßnahmen geschützt werden. Wesentlich ist hier auch, dass man mit einem Thema, zum Beispiel Kontrolle des Modems oder „Vertraulich im Header eines Word Dokuments“ produktiv werden kann ohne sich um alle anderen Themen zu kümmern.
- Über Echtzeitdialog mit den Anwendern nach zentraler Richtlinie werden fallabhängig geeignete Maßnahmen zum Umgang mit Grenzfällen ausgelöst.

## Fazit

Bei der richtigen Wahl der Lösung kann man Investitionsschutz, Skalierbarkeit, Zukunftsfähigkeit und Kosteneffizienz im Betrieb mit einem schnellen Projekterfolg kombinieren.

*Thorsten Scharmatinat*
Thorsten.Scharmatinat@itWatch.de