DLP – IN DEUTSCHLAND ANDERS?

SPANNUNGSFELD, ANFORDERUNGEN UND LÖSUNGEN

Das Spannungsfeld im DLP ist für deutsche und europäische Unternehmen häufig komplexer, denn zur technischen Herausforderung kommt noch eine Vielzahl von organisatorischen und gesetzlichen Randbedingungen – es wäre fatal, diese außer Acht zu lassen. Haftungsdurchgriff in den Vorstand nach KonTraG, nationale Datenschutzgesetze, Mitbestimmungspflicht und nicht zuletzt die häufig bewusst liberale Sicherheitskultur der Unternehmen scheinen auf den ersten Blick im Widerspruch zu einem stringenten Handeln gegen den Datenverlust zu sein. Die verschiedenen DLP Projekte mit der Endpoint Security Suite der itWatch zeigen auf, dass man diesen Widerspruch einfach lösen kann und alle Herausforderungen in einem Projekt abbilden kann. Wie das funktioniert, skizziert dieser Artikel.

DLP – in Deutschland anders?

Organisation und rechtliche Anforderungen

IT-Sicherheitsanforderungen sind „von außen“ durch eine Flut von auferlegten, regulierenden Bestimmungen definiert und „von innen“ durch das subjektive Verständnis des Unternehmens und der individuellen Relevanz der Regularien eventuell auch standort- oder branchenabhängig. Neben BDSG, KonTraG, SOX, HIPPA, Basel II, GOBS, FAMA, TDDG und EuroSOX gibt es viele weitere Vorschriften, die in Teilen oder dem gesamten IT-Markt zu berücksichtigen sind. Mitunter stehen Anforderungen an die Beweisbarkeit den Themen des Datenschutzes scheinbar unvereinbar gegenüber. Letztlich überlagern sich daher standardisierbare Anforderungen an die Sicherheit mit individuellen zu einem unternehmensspezifischen Profil. Als entscheidender Faktor kommt schließlich die Unternehmenskultur hinzu. In der Praxis heißt das, die richtige Lösung zwischen dem „selbstverantwortlichen Benutzer“ mit allen Freiräumen und dem möglicherweise ungeschulten „Normalnutzer“ zu finden (s. dazu auch unser weiterführendes White Paper "Unternehmenskultur & Compliance".)

Empfehlenswert ist es deshalb, zuerst das Thema zu teilen, damit es sich im Projekt leichter beherrschen lässt. Für Vorstände und VIPs werden andere technische Lösungen greifen als für Aushilfen oder kurzfristig Beschäftigte. Die Grafik veranschaulicht verschiedene Gruppierungen. Eine technische Richtlinie, dass „Normalnutzer“ alle Daten in jedem Format überall hin mitnehmen und hinschicken dürfen, diese aber zwangsweise mit einem Unternehmensschlüssel verschlüsselt sind, verhindert Datenlecks zu 100%. Damit hat man schon einmal ein großes Problem beseitigt – ohne einen einzigen Zugriff zu blockieren. Weitere Informationen zu diesem Thema enthält unser White Paper "Verschlüsselung beim Transport von Daten".

Bild1: DLP im Spannungsfeld

Bei den verbleibenden Nutzern - insbesondere den VIPs - wird mittels individueller Verträge die Voraussetzung geschaffen, um rechtskonform und im Unternehmensinteresse die Datenlecks zu schließen. Diese Verträge entstehen natürlich durch elektronische Willenserklärungen im Arbeitsfluss und nicht in Papierform. Dadurch sind die Verträge einfach an die jeweils gültige Gesetzeslage anpassbar – auch wenn sie von einem Standort zum anderen abweichen. Wichtig ist, dass Dialoge, die mit dem Benutzer erfolgen, stets situationsbezogen und in Landessprache geführt werden. So kann ein einfacher Dialog aussehen: *„Die Daten, die Sie gerade auf den mobilen Datenträger kopieren, sind als geheim klassifiziert.*

DLP – in Deutschland anders?

Als Vorstandsmitglied können Sie diese Daten mit Ihrem persönlichen Schlüssel verschlüsselt mitnehmen. Diese Aktivitäten werden aufgrund der aktuellen Gesetzeslage und der SOX-compliance vollständig protokolliert. Sie stimmen der Protokollierung durch den „Akzeptieren“ Knopf zu. Bitte vergessen Sie nicht, diese Daten auf einem Drittrechner wieder zu löschen.“

Dieser Dialog ist an eine inhaltliche Prüfung der Dateien, z.B. über eine Verschlagwortung oder eine freie Patternprüfung, gekoppelt, so dass der Benutzer den Dialog auch nur in dem relevanten Kontext erhält. Wie häufig diese elektronische Willenserklärung abzugeben ist wird frei definiert. Nebenbei wird auch ein Sicherheitsbewusstsein bei den Anwendern erzielt – "Security Awareness in Echtzeit". Die Aufbewahrung der Daten ist beweis- und revisionssicher. Das Recht zum „Mitnehmen“ der Daten wird erst nach der erfolgten elektronischen Willenserklärung gewährt. Die Sicherheitsrichtlinie wird in Echtzeit abhängig vom Wissensstand und der vertraglichen Bindung des Nutzers vollautomatisch umgeschaltet.

Elektronischer Wissenstransfer

Auf der **SYSTEMS 2008** wurde erstmalig eine Integration eines elektronischen Wissenstransfers (e-briefing) mit einem regelbasierten Schutzverfahren vorgestellt. Die Firmen **MainSkill** (e-briefing) und **itWatch** (patentierte regelbasierte Kontrolle mobiler Information) haben die Produkte so integriert, dass der Nutzer sein Wissen vor bestimmten Aktionen einmalig nachweisen muss, z.B. lokal gültiges Datenschutzgesetz. Sobald der Benutzer einmal den e-Briefing Baustein zum Datenschutzgesetz erfolgreich abgearbeitet hat, ist er automatisch für bestimmte mobile Datenträger freigeschaltet – das senkt Administrationskosten und wertet die letzte Bastion, den Benutzer, auf. Der Benutzer ist nun aktiver Teil der Sicherheitskultur des Unternehmens geworden und erhält neue Lerninhalte automatisch.

Nachdem die organisatorische Einbettung mittels technischer Maßnahmen in Echtzeit abgebildet ist, stellt sich das Projekt den technischen Fragestellungen – allen voran den Leckagepunkten. Wo können Daten ungewollt, unbeobachtet oder gesetzeswidrig nach außen gebracht werden? E-Mail, http(-s), USB, Firewire, Modem, ftp, Drucken und viele weitere Leckagepunkte gilt es zu behandeln. Will man das Problem an der Wurzel packen muss man aber auf den Endpoint gehen (vgl. dazu auch "Endpoint Security Leicht Gemacht - Risikomanagement von Anfang an"). Eine Endpoint Security Lösung, muss sich also um folgende Themen kümmern:

- **Datenträger Kontrolle** – Wer darf welche Daten in welchem Format auf welchem Datenträger mitnehmen.
- **Verschlüsselung der mobilen Datenträger** – Die Verfahren der Vergangenheit (z.B. Partitionsverschlüsselung) haben ausgedient, da der Bedarf an Vertraulichkeit zunehmend von den Dateiinhalten und ihrer Sensitivität abhängt und nicht mehr alle Daten einheitlich klassifiziert und behandelt werden sollen. Im in der *LANline* von uns veröffentlichten Artikel "Zentral definierte Verschlüsselung" finden Sie weitere Informationen zum Thema.

DLP – in Deutschland anders?

- **Personalisierung von Datenträgern** – Günstige Datenträger verfügen über keine individuellen, sicheren Merkmale wie Seriennummern. In besonders kritischen Bereichen (Vorstand, Akquisition, Stabsabteilungen etc.) erfordert die Compliance, wesentliche Datenbewegungen beweissicher abzulegen. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier ein effizientes Mittel.
- **Kontrolle der Anwendungen** – Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von White- UND Blacklists. Die Umsetzung „welche Dateien darf eine Anwendung denn Lesen?“ löst das DLP-Problem an der Wurzel. So darf z.B. der Browser keine vertraulichen Informationen lesen – dann kann der böswillige Benutzer diese auch nicht über http-s in das Internet laden. Im Beispiel ist eine technische

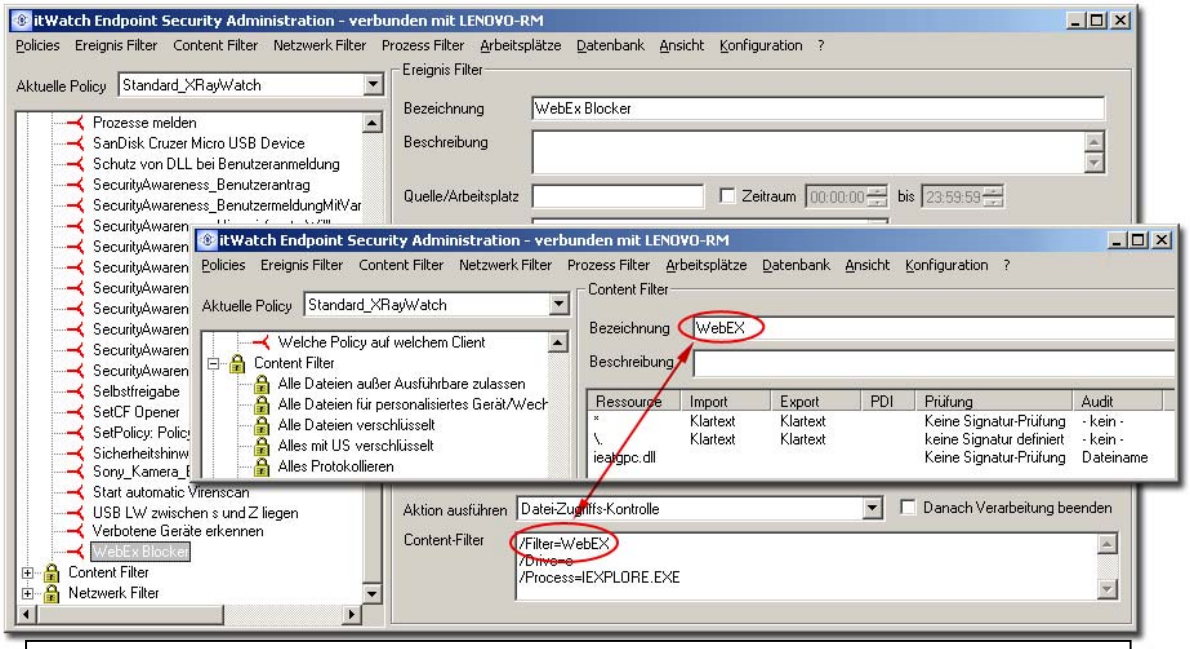

Bild2: DLP bei Applikationen

Einstellung dargestellt, wie der Zugriff auf WebEx als Plug-In in den Internetexplorer zwingend verhindert werden kann.

- **Protokollierung des Dateiaustausches** – Blockieren und Freigeben alleine genügt heute schon lange nicht mehr. 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.
- **Kontrolle der verwendeten Netze** – Entsprechend des erkannten Netzes muss die Security Policy in Echtzeit eingestellt werden, z.B. 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.

DLP – in Deutschland anders?

- **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.
- **Mehr zu** Anforderungen und Lösungen können Sie in dem White Paper "Endgerätesicherheit - Das braucht man wirklich" wirklich nachlesen.

Bild3: Die Datenlecks im Griff

Diese Anforderungen sind natürlich auch auf Terminalservern und im CITRIX® Umfeld zu leisten. Bei der Projektierung ist es wichtig, mit dem gleichen Software Agenten und einem zentralen Management sowohl ein Monitoring als auch Schutzfunktionen (Blocking, Verschlüsselung, elektronische Willenserklärung etc.) umzusetzen, da man den Ist-Stand der Datenbewegungen jeweils in den Risikomanagement Prozess eingibt, und daraus eventuell notwendige Verfeinerungen oder Verschärfungen der Sicherheitsrichtlinie ableitet. Denn auch DLP ist immer ein Prozess – mit dem man aber heute bereits anfangen kann – auch unter den komplexeren rechtlichen Situationen in Deutschland oder Europa.

Fazit

Zwischen den unabhängigen „Welten“ Systems Management, IT-Sicherheit, einfache Nutzbarkeit für Endanwender und Administratoren, Compliance und User Awareness können mit der **Endpoint Security Suite** von **itWatch** effektive Brücken gebaut werden. Sogar hohe Kosteneinsparpotentiale können ausgenutzt werden (s. dazu auch "Null Administration - Volle Sicherheit"). Einfacher Roll-Out mit der automatisierten Integration in alle vorhandenen Prozesse ermöglichen die kosteneffiziente Nutzung.

Die **Endpoint Security Suite** der **itWatch** bietet Sicherheit, Usability und SystemsManagement in einem. Überzeugen auch Sie sich von seiner Leistungsfähigkeit und kontaktieren Sie uns unter:

DLP – in Deutschland anders?

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

Weitere Literatur:

- Unternehmenskultur & Compliance
- Verschlüsselung beim Transport von Daten
- Security Awareness in Echtzeit
- Endpoint Security Leicht Gemacht - Risikomanagement von Anfang an
- Zentral definierte Verschlüsselung
- Endgerätesicherheit - Das braucht man wirklich
- Null Administration - Volle Sicherheit