Cyril Marti

Data Loss Prevention

DLP Basiswissen

Über dieses Buch

Das Thema Informationssicherheit begleitet mich seit bald 20 Jahren in meiner beruflichen Laufbahn. Als Consultant habe ich dabei die Chance, interessante Einblicke in unterschiedliche Branchen und zahlreiche Firmen zu erhalten.

Vor einigen Jahren habe ich begonnen, mich mit dem Thema Data Loss Prevention zu befassen. Schnell begann mich dieses Thema zu faszinieren. DLP ist ein sehr umfassendes Thema und schliesst viele Gebiete mit ein. Ein erfolgreiches DLP Projekt muss sehr vielfältige Aspekte der heutigen Arbeitswelt berücksichtigen, sei dies die IT-Infrastruktur, die Business Prozesse, Gesetze und Regulationen und viele weitere.

Den Einstieg in das Thema fand ich aber einigermassen schwierig. Natürlich sind die DLP Produkte der verschiedenen Hersteller gut dokumentiert. Auch findet man im Internet unter den Herstellerseiten Foren, welche sich mit dem Thema DLP beschäftigen. Leider fand ich aber nur sehr wenig Literatur über das Thema, so dass ich gezwungen war, mir die Informationen selbst mühsam zusammenzusuchen.

Ich fand keine Literatur, welche die praktischen Aspekte, welchen ich in den Projekten begegnete, beschrieb. Ein paar Jahre später habe ich dann nachgeschaut, ob es nun mehr Literatur zu diesem Thema gibt. Da DLP aber nach wie vor unterdokumentiert ist, habe ich beschlossen, diesem Umstand wenigstens ein bisschen entgegenzuwirken.

Dieses Buch soll einem Einsteiger in das Thema den anfänglichen Umgang mit der Materie erleichtern. Mit vielen Beispielen aus der Praxis will ich den Leser an das Thema heranführen. Auch für Fortgeschrittene ist das Buch sicherlich noch interessant, vermittelt es doch einen Einblick in den praktischen Umgang mit DLP und worauf verschiedene Branchen bei der Einführung speziell achten müssen.

DLP verwendet in vieler Hinsicht sehr spezielle Konzepte, welche in anderen Gebieten der Informationssicherheit kaum Einzug halten. Dies mag mit der Komplexität der Prozesse zu tun haben, insbesondere wenn es um die Verarbeitung von DLP Vorfällen geht. Dennoch versuche ich in diesem Buch immer wieder auch den Bogen zu bekannten Methodiken und Frameworks, beispielsweise zu TOGAF oder auch zu NIST, zu schlagen. Ich hoffe damit, dem Leser das Verständnis von DLP etwas zu erleichtern, da er so auf Bekanntem aufbauen kann.

Obwohl ich mir vorgenommen hatte, ein grundsätzliches Buch über DLP zu schreiben, welches insbesondere herstellerunabhängig sein soll, lies ich es mir nicht nehmen, einen kurzen Einblick in Microsoft DLP zu geben. Da Microsoft in diesem Bereich eigene Wege geht, ist ein Vergleich der DLP Konzepte mit denen von anderen Herstellern äusserst spannen.

Nun wünsche ich Ihnen viel Spass beim Lesen und natürlich eine erfolgreiche Realisierung Ihrer DLP Vorhaben!

Konventionen

Obwohl die Sprache in der Informationstechnologie stark durch Anglizismen geprägt ist, habe ich versucht, wo immer möglich und wo es die Lesbarkeit des Buches nicht beeinträchtigt, die deutschsprachigen Bezeichnungen zu verwenden. An manchen Stellen im Buch habe ich auf die englischen Begriffe hingewiesen.

In Passagen, in denen ich Quellen zitiere, sind die Quellverweise hochgestellt in eckigen Klammern als Nummern angegeben, beispielsweise [1]. Das Quellenverzeichnis befindet sich im Anhang des Buches. In der eBook Version sind die Quellverweise als Links auf die jeweiligen Quellen ausgelegt.

Die Hauptkapitel sind so angeordnet, dass der Leser das Buch von vorne nach hinten durcharbeiten kann und so einen immer tieferen Einblick in die Thematik erhält. Die einzelnen Hauptkapitel bilden aber abgeschlossene Einheiten. Wer sich bei einem Thema schon gut auskennt oder dafür kein Interesse hat, kann das Kapitel überspringen und wird dem weiteren Verlauf des Textes dennoch folgen können.

In einigen Abbildungen in diesem Buch sind grau hinterlegte Nummern eingefügt. Diese Nummern werden jeweils unter der Abbildung erklärt.

Inhaltsverzeichnis

1 Übersicht über DLP Systeme

DLP Systeme arbeiten alle nach denselben Prinzipien, unabhängig vom Hersteller der jeweiligen Lösung. Dieses Kapitel stellt diese Prinzipien vor und gibt somit eine Übersicht, wie heutige DLP Systeme aufgebaut sind.

Kapitel	Inhalt
1.1	In Kapitel 1.1 folgt eine Beschreibung, was DLP ist. Dieses Unterkapitel zeigt auf, wie DLP arbeitet und welche Themenfelder zu DLP gehören.
1.2	Das Kapitel 1.2 zeigt auf, was der Unterschied zwischen «Data Loss Prevention» und «Data Leak Prevention ist».
1.3	Einen kurzen Abriss der Geschichte von DLP und welche Hersteller heute am Markt agieren wird in Kapitel 1.3 beleuchtet.
1.4	Ein DLP System umfasst fünf eng ineinander verwobene Themengebiete. Diese werden in Kapitel 1.4 erläutert und deren Zusammenhang wird aufgezeigt.
1.5	Die Komponenten eines DLP Systems, das DLP Management-Tool und die DLP Scanner, werden in Kapitel 1.5 betrachtet.

Tabelle 1: Übersicht Kapitel 1

1.1 Was ist Data Loss Prevention?

Kurz gesagt: Data Loss Prevention (DLP) analysiert den Inhalt von Daten. Basierend auf dieser Analyse wird Anhand eines Regelsets entschieden, welche Daten transferiert werden dürfen und welche blockiert werden sollen. Aus dieser kürzest möglichen Definition von DLP leiten sich sofort zahlreiche Fragestellungen ab, etwa «Welche Daten werden analysiert?» oder «Was passiert, wenn Daten nicht transferiert werden dürfen?».

Dieses Buch gibt Antworten auf diese und weitere Fragen rund um das Thema DLP. Wird DLP in einem Unternehmen eingeführt, hat dies Auswirkungen auf die Geschäftsprozesse. DLP darf somit nicht als eine rein technische Lösung betrachtet werden. Oft müssen bestehende Prozesse angepasst werden. Praktisch immer müssen neue Prozesse zur Behandlung von DLP Vorfällen erarbeitet werden, da nur in ganz wenigen Ausnahmefällen die DLP-Prozesse in die bestehenden Sicherheits-Prozesse integriert werden können. DLP-Prozesse werden in allen Unternehmen unterschiedlich implementiert. Es gibt aber gemeinsame Grundelemente, welche in diesem Buch behandelt werden.

DLP tritt nicht als einzelne Schutzmassnahme auf. DLP arbeitet stets im Verbund mit weiteren Schutzmechanismen wie Monitoring, Zugriffskontrollen und Verschlüsselung. DLP ist somit auf eine komplementäre und funktionierende Sicherheitsinfrastruktur angewiesen, um den gewünschten Effekt zu erreichen.

DLP ist somit ein wichtiger Baustein in einem ganzheitlichen Sicherheitskonzept, mit dessen Hilfe Fehlmanipulationen durch Benutzer erkannt und allenfalls verhindert werden können. Solche Fehlmanipulationen können das Versenden von geheimen Dokumenten über einen unsicheren Kanal sein oder auch das Verschicken von internen Dokumenten an eine fälschlicherweise eingegebene, externe E-Mail-Empfänger Adresse.

1.2 «Leak» oder «Loss»?

Allgemein versteht man unter «Data Loss Prevention» den Schutz vor unerwünschten Abfluss von Daten. Dieser Abfluss verursacht einen feststellbaren und somit messbaren Schaden. Diese Art des Abflusses passiert schnell, beispielsweise durch den ungewollten Versand einer E-Mail mit einem Attachement.

«Data Leak Prevention» oder auch «Data Leakage Prevention» dagegen bietet einen Schutz gegen kaum messbare Datenabflüsse. Werden Daten über mehrere Monate oder sogar Jahre sehr langsam aus einer Organisation an einen unerwünschten Empfänger geschickt, ist dies äusserst schwierig zu erkennen. Dies passierte einem grossen Schweizer Rüstungsbetrieb. Der Datenabfluss wurde durch eingeschleppte Schadsoftware verursacht und erst nach mehreren Jahren entdeckt.

Die technischen Massnahmen zur Erkennung der beiden Fälle von unerwünschtem Datenabfluss ähneln sich sehr stark. Die Unterschiede liegen vor allem in der Prozessierung der Vorfälle. In diesem Buch wird die neutrale Abkürzung «DLP» verwendet. Wo nichts Gegenteiliges vermerkt ist, gelten alle Aussagen in diesem Buch für beide Szenarien.

1.3 Geschichte

DLP ist aus der «Extrusion Prevention» Technologie heraus entstanden. Die ersten Systeme wurden von militärischen Organisationen eingesetzt. Die Systeme bestanden in den meisten Fällen aus einer Kombination aus Hardware und Software – was sich bis heute nicht wesentlich geändert hat. Die Extrusion Prevention Systeme waren noch deutlich weniger auf den Inhalt der Daten fokussiert. So wurden Funktionen zu dieser Technologie angerechnet, welche einen USB-Stick verschlüsselten und ihn nur für eine bestimmte Zielgruppe lesbar machten. Aus heutiger Sicht würde man dies wohl eher als flankierende Massnahme eines DLPs betrachten und nicht zum System selbst zählen.

Im Dezember 2001 wurde die Firma Vontu in den USA gegründet. Vontu war eine der ersten Firmen, welche Extrusion Prevention für die Privatindustrie verfügbar machte. 2007 wurde Vontu von Symantec gekauft. Fast gleichzeitig kaufte McAfee eine kleine DLP Firma namens Onigma. McAfee und Symantec wurden dadurch zu den Leadern im DLP Markt. Nachdem 2006 der frühere McAfee CEO Gene Hodges neuer CEO der bereits 1994 gegründeten Firma Websense (seit 2016 Forcepoint) wurde, etablierte sich diese Firma unter der neuen Führung als erfolgreicher Player im DLP Markt. 2020 wurde Symantec von Broadcom gekauft, wie sich das auf die DLP Produkte auswirken wird, muss sich zuerst noch zeigen. Momentan sind diese drei Firmen die führenden Anbieter von DLP Systemen, zusammen mit Digital Guardian, einem eher kleineren Unternehmen, das sich ebenfalls auf DLP Systeme spezialisiert hat. [19]

Seit mehr und mehr Anwendungen als Cloud-Lösungen angeboten werden, rücken die DLP Lösungen aus ihren klassischen Standorten in den Rechenzentren oder auf den

Endgeräten der Benutzer ebenfalls vermehrt in die Cloud. Microsoft hat diesen Trend erkannt und bietet hochintegrierte DLP Lösungen in den Windows Server Systemen an. Diese Lösung profitiert von der riesigen Installed-Base der Microsoft Betriebssysteme. Der Microsoft DLP Lösung gelingt es in den letzten Jahren immer besser, den etablierten Hersteller in diesem Bereich Marktanteile abzujagen.

1.4 Themenbereiche

Ein DLP System ist nicht kein monolithisches Gebilde. Vielmehr ist ein DLP System ein Konglomerat aus fünf eng ineinander verwobenen Themenbereichen, wie Abbildung 1 zeigt:

Abbildung 1: DLP Themenbereiche

- **Governance**

  Im Bereich Governance wird die DLP Strategie definiert. Der wichtigste Punkt dieses Themenbereichs ist die Definition der zu schützenden Daten. Jedes Unternehmen muss festlegen, welche Daten geschützt werden müssen und auch in welchem Masse. Dabei darf

der Schutzbedarf der kritischen Daten nicht nur aus IT Security Sicht definiert werden. Es ist für jedes Unternehmen essenziell, eine gesunde Balance zwischen dem nötigen Schutz und geringen Einschränkungen der Business-Prozesse zu finden.

- **Infrastruktur**

  Sind die zu schützenden Daten bekannt, muss sich das Unternehmen überlegen, wo DLP Scanner platziert werden sollen, um die optimale Wirkung zu entfalten. Sollen kritische Daten nicht versehentlich per E-Mail nach aussen verschickt werden, ist ein DLP Scanner innerhalb des SMTP Flusses die erste Wahl. Dürfen bestimmte Daten nicht auf USB-Sticks geschrieben werden, greifen natürlich Schutzmassnahmen im Perimeter des Firmennetzes viel zu kurz. In einem solchen Szenario muss der DLP Scanner als Software-Agent auf dem Client der Mitarbeitenden installiert werden und die USB-Schnittstellen überwachen.

- **Regeln**

  Auf die DLP Scanner werden DLP Regeln ausgerollt. Anhand dieser Regeln wird der Datenfluss untersucht. Der Aufbau dieser Regeln hängt wiederum stark von der Art der zu entdeckenden Daten ab. Müssen nur Kreditkarten-Nummern erkannt werden, kann man dies problemlos mit regulären Ausdrücken erreichen. Wird aber in der Governance definiert, dass Quellcode nicht verschickt werden darf, wird man sehr schnell an die Grenzen der Möglichkeiten mit regulären Ausdrücken stossen. In diesem Fall wird man auf die Möglichkeiten von maschinellem Lernen, welches moderne DLP Systeme anbieten, zurückgreifen.

- **Scanning**

In den meisten Fällen besteht eine DLP Lösung nicht aus einer Infrastruktur-Komponente und einem Regelset. Vielmehr gibt es mehrere Scanner und eine Vielzahl von Regeln. Die daraus resultierenden Möglichkeiten verschiedener Scans werden im Bereich Scanning orchestriert: Ein Scan muss die richtigen Regeln dem richtigen Scanner zuweisen. Der Scanner muss die richtigen Daten überprüfen. Der Scanner wiederum erkennt, ob ein Vorfall generiert werden muss und eventuell auch eine Aktion durchgeführt werden soll. Eine Aktion kann beispielsweise das Hinzufügen eines X-Headers bei einer E-Mail sein oder die Unterbrechung eines Uploads von Dateien in das Internet.

- **Vorfälle**

  Erzeugt ein Scan Vorfälle, müssen diese verarbeitet werden. Die Bewertung von Vorfällen führt zu Handlungen. Beispielsweise muss ein Mitarbeiter zur Vorsicht ermahnt werden oder sogar ganze Prozesse müssen angepasst werden. Die Behandlung von Vorfällen ist die grösste Herausforderung rund um DLP. Jedes Unternehmen muss entsprechende Strategien definieren und umsetzen.

In den folgenden Unterkapiteln sind die einzelnen Themen beschrieben. Im weiteren Verlauf dieses Buches werden all diese Aspekte wieder aufgegriffen. Die folgenden Unterkapitel geben somit nur einen ersten Überblick über DLP als Gesamtthema.

1.4.1 Governance

Wie jede Massnahme in der Informationssicherheit, muss auch DLP von den strategischen Organen eines Unternehmens mitgetragen werden. Das Governance Team

muss wissen, welche Daten im Unternehmen besonders wichtig sind und die Risiken. Ein allfälliger Verlust solcher Daten muss quantifiziert werden können. Diese Informationen müssen mit den Strategie- und Führungsgremien des Unternehmens abgestimmt. Diese Gremien müssen die Governance mittragen. Folgende Fragen müssen eindeutig beantwortet werden können:

- Welche Daten müssen geschützt werden?
- Was sind die Konsequenzen für das Unternehmen bei einem Datenverlust?
- Was sind die Konsequenzen für Mitarbeitende bei Verstössen?
- Welche Massnahmen dürfen eingeführt werden?
- Für welche Organisationseinheiten gelten besondere Regeln?

Aus den Antworten leiten sich die Schutzziele des DLP Systems wie auch die Umsetzungsziele des DLP Vorhabens ab.

Die Frage, welche Daten geschützt werden sollen, ist eng mit der Frage nach der Klassifizierung von Daten und Dokumenten verbunden (siehe Kapitel 4). Eine existierende Klassifizierung ist zwar keine zwingende Voraussetzung für die Einführung eines DLP Systems. Allerdings ist ein zumindest konzeptionell vorliegender Ansatz von Vorteil. Welche Daten schlussendlich für ein Unternehmen schützenswert sind, ist sehr individuell. Oftmals wird diese Frage auch bereits teilweise vom Gesetzgeber beantwortet. So gehören in der Finanzindustrie Kundenidentifizierende Daten (CID, Customer Identifying Data) zu den kritischen Daten. In der Gesundheitsbranche sind es Patientendaten, welche auf keinen Fall in falsche Hände gelangen dürfen. In weniger regulierten Branchen gehören oftmals Firmengeheimnisse, wie Formeln, Rezepte,

Fertigungsmethoden, etc. zu den besonders schützenswerten Daten. Eine genaue Analyse ist aber auf jeden Fall unumgänglich, damit die Massnahmen, welche mit einem DLP System umgesetzt werden, nicht ins Leere laufen.

Die Governance ist für die Kommunikation verantwortlich. Der korrekte Umgang mit Daten muss in Form von Richtlinien genaustens beschrieben sein. Die Mitarbeitenden müssen ihre Rechte und Pflichten im Umgang mit Daten kennen. In vielen Ländern gilt, dass der Datenverkehr von Mitarbeitenden erst dann überwacht werden darf, nachdem sich die Mitarbeitenden einverstanden erklärt haben. Das Mass der Konsequenzen muss von der Governance in Absprache mit der Personal- und der Rechtsabteilung definiert werden. Dabei spielen Faktoren wie der Schweregrad des Verstosses und die Anzahl der Verstösse in einem bestimmten Zeitraum eine wichtige Rolle.

Bei der Kommunikation ist Feingefühl gefragt. Gerade Sicherheitsmassnahmen werden nur all zu leicht als Kontrolle und Schikane missverstanden. Es gilt den Mitarbeitenden aufzuzeigen, dass es hierbei nicht um Misstrauen gegenüber ihnen geht, sondern vor allem darum, die Mitarbeitenden zu unterstützen und unabsichtliche Fehler zu vermeiden helfen. Die Informationssicherheit ist ein kompliziertes Konstrukt. Nur all zu leicht werden Daten unwissentlich und in guter Absicht verschickt. Dennoch kann der Schaden immens sein. Genau solche Schäden zu vermeiden ist die Aufgabe eines DLP Systems. Es dient nicht zur Überwachung von Mitarbeitenden. Es unterstützt sie in ihrer täglichen Arbeit bei der Vermeidung von Fehlern.

Es ist aus rechtlicher Sicht heikel, die Daten von Mitarbeitenden zu überprüfen. Viele Unternehmen erlauben den Mitarbeitenden die IT-Infrastruktur in vernünftigem