Mit DLP potentielle Datenlecks abdichten

Marktübersicht Den Abfluss sensibler Daten aus einem Unternehmen zu verhindern, ist die Aufgabe von Data-Loss-Prevention-Lösungen. Wir zeigen, was die Produkte verschiedener Hersteller bieten.

Von Luca Cannellotto

Mehrere eklatante Fälle aus jüngster Vergangenheit haben gezeigt, wie schnell sensible Daten eines Unternehmens in falsche Hände oder an die Öffentlichkeit gelangen können – oft mit verheerenden Folgen sowohl für die betroffenen Unternehmen selbst als auch für deren Kunden. Es ist kaum von der Hand zu weisen, dass die Bedrohungen für die Datensicherheit stetig zunehmen und im Zeitalter der Cloud und der steigenden Mobilität im Geschäftsalltag auch vielfältiger werden und dadurch schwerer zu bekämpfen sind. Nach wie vor sind Bedrohungen aus dem Inneren eines Unternehmens die grösste Gefahr für die Sicherheit und die Integrität der Unternehmensdaten. Diese entsteht entweder durch Unwissen oder Unachtsamkeit der Mitarbeiter oder aber durch gezielte Angriffe, deren Motivationen vielfältig sein können (zum Beispiel Industriespionage). Datenschutz und Datensicherheit bleiben also zentrale Herausforderung für jedes Unternehmen, unabhängig von der Branche.

DLP als Wächter über die Daten

Um Technologien zu beschreiben, die den ungewollten Abfluss von Daten verhindern sollen, wird seit rund einem Jahrzehnt das Etikett Data Loss Prevention (DLP) verwendet. Früher waren damit vor allem physische Massnahmen gemeint, wie die Sperrung oder das Entfernen von Diskettenlaufwerken und USB-Ports. Heute wird mit DLP in erster Linie Software und Hardware bezeichnet, deren primäre Funktion es ist, den Verlust sensibler Daten zu verhindern, indem diese überprüft werden, während sie entweder stationär im Unternehmen oder in der Cloud gespeichert sind, sich durch das Netzwerk bewegen oder sich auf einem Endgerät in Benutzung befinden. DLP-Lösungen sind darauf ausgelegt, einen drohenden Datenverlust vorzeitig zu erkennen und nach definierbaren Richtlinien entsprechend darauf zu reagieren, indem sie den jeweiligen Mitarbeiter darüber informieren oder den aktuellen Vorgang gänzlich unterbinden, damit die Daten nicht ungehindert nach aussen gelangen können.

Wichtig ist das übergeordnete Sicherheitskonzept

Gepaart mit den entsprechenden Prozessen und weiteren Technologien zum Schutz von Unternehmensdaten als Teil eines übergeordneten Sicherheitskonzeptes können DLP-Lösungen ein Schlüsselelement sein, um das Risiko eines Datenverlustes zu minimieren. Dennoch werden solche Systeme nur von jedem zweiten Unternehmen eingesetzt, wie Gartner in einer Studie von 2016 aufzeigt.

Ein Grund dafür dürfte sein, dass Data-Loss-Prevention-Systeme noch immer im Ruf stehen, komplex zu sein und schwer in bestehende IT-Infrastrukturen zu implementieren. Auch deren Verwaltung und Pflege stellt durch die zunehmende Verbreitung und Verwendung von Cloud-Diensten und mobilen Geräten in Unternehmen eine wachsende Herausforderung dar. Data-Loss-Prevention-Projekte können ausserdem langwierig sein und bedürfen einer klaren Vorstellung davon, was abgedeckt werden soll, denn nur so lassen sich stringente Richtlinien definieren, mit denen das System arbeiten und die Daten auch wirklich schützen kann.

Die Renaissance von Data Loss Prevention

Kaum ein Unternehmen kann es sich jedoch leisten, Daten zu verlieren, denn zu gross ist die Gefahr eines nachhaltigen Image-Schadens. Gartner stellt denn auch fest, dass DLP-Lösungen aufgrund neuer Bedrohungen und steigender Zahlen öffentlich bekannt gewordener Datenlecks eine wahre Renaissance erleben würden und prophezeit, dass bis 2018 rund 90 Prozent der Unternehmen solche Systeme in irgendeiner Form einsetzen werden. Die Unternehmen hätten erkannt, so Gartner, dass DLP ein zentraler Bestandteil des Daten-Lebenszyklus ist und nicht bloss ein weiterer Kostenfaktor.

Ob sich die Implementierung eines solchen Systems aber lohnt, hängt von verschiedenen Faktoren ab. Letztlich gilt für die Entscheidung für oder wider den Einsatz einer Data-Loss-Prevention-Lösung, dass mit einer umfassenden Bedarfsanalyse geklärt werden sollte, wo und wie sensible Daten in einem Unternehmen gespeichert sind, wie und wohin diese übermittelt werden dürfen und auf welchen Endgeräten sie verarbeitet werden. Digitale Kommunikationsmittel wie E-Mail und Messenger, kleine und tragbare Speichermedien wie USB-Sticks sowie Endgeräte wie Smartphones und Tablets sind klassische Kanäle, über die sensible Daten ungewollt aus einem Unternehmen entweichen können. Diese gilt es wie auch die übrigen Systeme zu überwachen und zu sichern, noch bevor ein Schaden entstehen kann. ■

SIEBEN DLP-LÖSUNGEN

	Check Point SOFTWARE TECHNOLOGIES LTD.	ENDPOINT PROTECTOR	DIGITAL GUARDIAN
Hersteller	**CHECK POINT**	**COSOSYS**	**DIGITAL GUARDIAN**
Lösung	DLP Software Blade Version R77/ R80 + Endpoint Security Solution	Endpoint Protector 4	Threat Aware Suite
Art der Lösung	integrierte Lösung	umfassende DLP-Suite, Container-verschlüsselung und MDM	DLP-Suite
Komponenten/Bestandteile der Lösung	DLP Software Blade Version R77/ R80 + Endpoint Security Solution	zentrale Appliance, Agent auf Endgerät, Gerätekontrolle, Dateninspektion	Agent und Appliance
Unterstützte Plattformen	Windows, MacOS, Android, iOS	Windows, MacOS, Linux	Windows, MacOS, Linux
Analyse und Erfassung der Informationen			
Wird der Dateneigentümer identifiziert?	■	■	■
Analyse der Datenzugriffs-Profile?	■	■	■
Welche Datentransporttypen werden überwacht?	SMTP, HTTP, HTTPS, FTP, TLS	Datenüberwachung bei Übergang zwischen OS und Applikationen	alle, da Event-basiert
Erkennung & Analyse der Speicherorte?	■	■	■
Welche Datenquellen werden ausgewertet?			
…Fileserver mit folgenden Betriebssystemen	alle	Windows, Linux Samba	Windows, MacOS, Linux
…E-Mail-Server	Exchange	keine Angabe	Exchange, Lotus
…Storage-Systeme	alle, Klassifizierung/Verschlüsse-lung Bestandteil des Dokumentes	SAN, NAS, Dropbox, Google Drive, iCloud, Onedrive (Skydrive)	SAN, NAS, Cloud
…Sonstige	Endgeräte, mobile Geräte, Objekte in Datenbanken	Endgeräte	USB, mobile Geräte
Organisation der Daten			
Analyse strukturierter Daten (z.B. Datenbanken)	■	■	■
Analyse unstrukturierter Daten (z.B. Mail Messaging)	■	■	■
Analyse beschriebener Daten (Kundennummern, Bilddateien…)	■	■	■
Konkrete Kennzeichnungen einzelner Daten(-bereiche)	■	■	■
Intelligentes Lernen anhand von Beispielen	■	❑	❑
Nutzungsrichtlinien durch vorgegebene Templates	■	■	■
Nutzungsrichtlinien frei definierbar	Regex	Regex	XML
Richtlinien-basierte Verschlüsselung der Inhalte	■	■	■ teilweise
Suche nach Schlüsselwörtern (Keyword Matching)	■	■	■
Suche nach Dateitypen	■	■	■
Durchsuchen der Anhänge	■	■	■
File Fingerprinting	■	■	■
Linguistische Analyse	■	❑	■
Import schädlicher Objekte kontrollieren oder ganz verbieten	verbieten	❑	kontrollieren
Manuelle und automatische Quarantänefunktion	automatisch	❑	automatisch oder manuell
Whitelisting	■	■	■
Was geschieht bei unzulässiger Aktivität?			
…Warnung an Anwender	■	■ konfigurierbar	■
…Nachricht an übergeordnete Instanz	■	■ konfigurierbar	■
…automatischer Remediation-Prozess	■	■ konfigurierbar	■
…Blockierung der Datenübertragung	■	■ konfigurierbar	■
…Blockierung von Rechnerports	■	■ konfigurierbar	■
…Sperren von USB-Geräten	■	■ konfigurierbar	■
…Beenden des Prozesses (Druckauftrag, PDF-Erstellung usw.)	■	■ konfigurierbar	■
Was geschieht, wenn der User offline eine unzulässige Aktivität startet?	User Check mit Dialogfeld, Multispect Inspection Engine (600 Fileformate, über 250 Datentypen)	alle Regeln bleiben offline aktiv und Aktivitäten werden proto-kolliert	Agent ist auch offline aktiv und überwacht sämtliche Aktivitäten
Zusätzliche Informationen			
Zentrales Management-Tool	■	■ (Administration über Browser)	■
Zentrales Reporting/Monitoring	■	■ (Reporting über Browser)	■
Rechtssichere Dokumentation	■	keine Angabe	■
Info	www.checkpoint.com	www.endpointprotector.de	www.digitalguardian.com
Preismodell/Preis	per User, ab 25 Dollar/User, zzgl. 3000 Dollar (DLP Software Blade)	per Seat, ab 29 Euro/Seat (unbefristet)	per User, auf Anfrage

■ = ja, ❑ = nein; 1) MS Azure, OCR, Analytics Engine, Server: Triton Unified Mgmt, Log, Analyse, 3rd Party Integration über ICAP; 2) Agents: Exchange, Outlook, Domino Discovery Tasks;

FORCEPOINT DEUTSCHLAND	INTEL SECURITY	SAFETICA TECHNOLOGIES	SYMANTEC
AP-DATA (Version 8.3)	McAfee Total Protection for Data Loss Prevention (DLP) (Version 10)	Safetica 7	Data Loss Prevention (Version 14.6)
umfassende DLP-Suite (auch modular erhältlich)	umfassende DLP-Suite	umfassende Kontext-basierte DLP-Lösung	umfassende DLP-Suite
Web-/E-Mail-Gateway add-on, SMTP MTA, HTTP/S Proxy, Network Monitor, Endpoint Agent, Data Crawler [1]	Netzwerk-Appliance, Agent auf Endgerät, Discovery-Scanner	Agent auf Endgerät, Server-Konsole, Server-Dienst, Websafetica	Agent auf Endgerät, Netzwerk-Appliance, Daten-Scanner, Cloud-Scanner, Cloud-Agent, CASB, Mail
Windows, MacOS, Linux, Citrix XenApp / XenDesktop, VMWare View Horizon	Windows, MacOS	Windows	Windows, MacOS, Linux, Citrix XenApp / XenDesktop, Android, iOS, Blackberry
■	■	■	■
■	■	■	■
SMTP, HTTP, HTTPS, FTP, Monitoring jedes Clear-Text-Protokolls	SMTP, HTTP, HTTPS, FTP,	alle Netzprotokolle und Applikationen werden überwacht/geschützt	SMTP, HTTP, HTTPS, FTP, TLS, IM
■	■	■	■
NDS, NFS File Shares; OS-unabhängig	Windows, MacOS	NTFS	Windows, Linux
keine Installation am Mailserver, Kontrolle v. Endpoint-E-Mail-App/Mail-Channel [2]	Exchange, Lotus Domino	Exchange, IceWarp, allgemein jeder E-Mail-Client auf dem Endgerät	Exchange, Lotus Notes, Office 365, Sharepoint, Documentum, Livelink
keine Installation am Storage Server, Scannen von Shares über Crawler Agents	SAN, NAS, Cloud, CIFS	Alle Storage-Systeme mit NTFS	Netapp, EMC, Windows Storage, Cloud
Office 365 Solution for Azure Cloud [3]	Endgeräte, mobile Geräte, Datenbanken	mobile Geräte, tragbare Laufwerke (verschlüsselt)	Endgeräte, mobile Geräte, Oracle-DB, SQL-DB, IBM DB2-DB, Websites
■	■	■	■
■	■	■	■
■	■	❑	■
■	■	■	■
■	❑	❑	■
■	■	❑	■
■	Regex, Tagging nach Datenlokation und nach Applikation	kontextuelles Tagging nach verschiedenen Kriterien [4]	Regex, EDM, IDM, VML, Form Recognition, Data Identifiers
■	■	■	■
■	■	❑	■
■	■	■	■
■	■	❑	■
■	■	❑	■
■	❑	❑	■
kontrollieren und/oder verbieten	kontrollieren und verbieten	kontrollieren und verbieten	verbieten (Symantec Endpoint Protection)
automatisch	automatisch	keine	automatisch (Symantec ATP, Email.cloud)
■	■	■	■
■ konfigurierbar	■	■	■
■ konfigurierbar	■	■	■
■ konfigurierbar	■	■	■
■ konfigurierbar	■	■	■
❑	■	■	■ (Symantec Endpoint Protection)
■	■	■	■
■	■	■	■
keine permanente Verbindung zum Server nötig, Incidents und Logs werden lokal gespeichert, bis der Client wieder online ist	identisch wie Online Client (konfigurierbar)	Agent auf dem Endpoint garantiert die gleiche Sicherheitspolitik wie beim Online-Mode	Warnung an Anwender und eine spezifische Offline-Message kann ausgegeben werden
■	■	■	■
■ (auch Weitergabe an z.B. SIEM, Incident Risk Ranking für Risikoanalyse)	■	■	■
■	■	■	■
www.forcepoint.com	www.mcafee.com	www.safetica.com	www.symantec.com
per User, auf Anfrage	per Node, 70,56 Euro/Node (bei 26–50 Nodes) ohne Device Control	per Seat, 46 Euro/Seat/Jahr (Unternehmen mit 200 Seats)	per User, auf Anfrage

3) Agents: Salesforce, Box, Exchange Online, Sharepoint Online; 4) Datenlokation, Benutzer, Applikation, Netzwerk-/Systemplatzierung, Titel, Sicherheitspolitik