Mit einer Lösung dreimal compliant

Unternehmen sind umzingelt von Gesetzen, Vorgaben und Standards, die unter anderem den Umgang mit sensiblen Daten regulieren. Häufig müssen drei oder mehr Regelungen umgesetzt werden: Zur DSGVO, die für alle Unternehmen in der EU verpflichtend ist, kommen das Geschäftsgeheimnisschutzgesetz (GeschGehG) für Firmeninformationen mit wirtschaftlicher Bedeutung. Im Kontakt mit Partnern ab einer gewissen Größe und in bestimmten Branchen sowie im internationalen Kontext ist eine Zertifizierung nach ISO 27001 erforderlich.

Laut DSGVO muss die Vertraulichkeit personenbezogener Daten, beispielsweise die der eigenen Mitarbeiter, bei der Verarbeitung durch „geeignete technische und organisatorische Maßnahmen“ gewährleistet werden. Das GeschGehG stellt Bedingungen, damit Firmen den Diebstahl und die Verwendung von geschäftskritischen Informationen untersagen und verfolgen können: So müssen Geschäftsgeheimnisse „durch technische und organisatorische Maßnahmen geschützt werden, die geeignet sind, interne und externe Verletzungen der Geheimhaltung zu verhindern“. In ISO 27001 sind in den sogenannten „Controls“ im Anhang A der Norm Sicherheitsanforderungen und Ziele zum Schutz von sensiblen Daten vorgegeben. Sie stehen beispielsweise im Zusammenhang mit der Verwaltung der Werte (A.8), der Informationsübertragung (A.13.2) sowie der Compliance mit gesetzlichen, vertraglichen oder selbstauferlegten Anforderungen (A.18).

Keine Angaben zu „geeigneten technischen Maßnahmen“

Konkretisiert werden die technischen Maßnahmen, mit denen die Anforderungen umzusetzen wären, in keiner der drei Regelungen; allenfalls verweisen Kommentare zu den ISO 27001-Controls auf den Einsatz einer DLP-Lösung. In jedem Fall müssen passende Lösungen den Schutz der Vertraulichkeit für unterschiedliche Arten von sensiblen Daten gewährleisten und sich möglichst ressourcenschonend für die Herstellung von Compliance mit unterschiedlichen Regelungen eignen.

DLP-Lösungen bieten ein geeignetes Funktionsspektrum

Dies ermöglichen Lösungen für Data Loss Prevention wie Endpoint Protector an entscheidenden Punkten. Zunächst einmal stellen sie sicher, dass Transfers unterbunden werden, die die Vertraulichkeit von Daten potenziell gefährden können und dass Firmenrichtlinien technisch überwacht werden. Die zentralen Funktionsbereiche von DLP-Lösungen sind:

- Device Control-Funktionalität verhindert, dass Mitarbeiter USB-Sticks, Notebooks und andere mobile Geräte am Arbeitsplatzrechner anschießen und Daten darauf speichern.
- Sind Daten als sensibel in die Inhaltskontrolle definiert, können sie nicht per E-Mail versandt, in Cloud-Speicher oder Filesharing-Tools geladen oder mit Social-Media-Anwendungen verwendet werden. Auch das Ausdrucken der Daten und Screenshots der Bildschirmansicht werden blockiert.
- eDiscovery-Funktionen finden Daten, die auf Arbeitsplatzrechnern gespeichert sind und deren Inhalte als sensibel eingestuft wurden.

Die besondere Bedeutung von Logs und Reports

Gute DLP-Lösungen erfassen alle Ereignisse und erstellen Aufzeichnungen. Dazu gehören die revisionssichere Protokollierung aller Übertragungen sowie Übertragungsversuche von Dateien auf Wechseldatenträger und mobile Devices, in und über Online-Anwendungen und Cloud-Dienste sowie Mitschnitte sämtlicher übertragenen Dateien. Auswertungen der Logfiles machen Verstöße gegen Richtlinien und entsprechende Versuche sowie Datenlecks oder potentielle Datenlecks sichtbar, die beispielsweise durch verändertes Mitarbeiterverhalten oder die Verwendung neuer Tools und Anwendungen entstehen können. Zudem ermöglichen sie kontinuierliche Anpassungen und Verbesserungen von Richtlinien und Schutzmaßnahmen, mit denen sich die Eintrittswahrscheinlichkeit oder die Auswirkungen von Vorfällen verringern lassen.

Nachweispflichten werden erfüllt

Weiterhin sind die Reports Grundlage für die Erfüllung von Nachweispflichten: bei Audits, gegenüber der Datenschutzbehörde und für gerichtliches Vorgehen. Mit ihnen lassen sich für ISO 27001 Teilbereiche des für ein ISMS enorm wichtigen Ziels der Protokollierung und Erbringung von Nachweisen (A.12.4) abdecken. Im Rahmen der DSGVO sind die Firmen durch die Aufzeichnungen hinsichtlich der Umsetzung von Schutzmaßnahmen gegenüber den Datenschutzbehörden nachweisfähig. Im Fall eines Datenverlustes können sie mit Hilfe der Logs Verursacher und Umfang des Schadens sowie Austrittspunkte ermitteln und sind in der Lage, eine forensische Untersuchung zu betreiben. Beim Abfluss von Geschäftsgeheimnissen können sie Maßnahmen zum Schutz der Informationen sowie Verletzungen gerichtsfest nachweisen und Ansprüche gegen Verursacher von Verletzungen durchsetzen.

Fazit

DLP-Lösungen wie Endpoint Protector sind ausgereifte Systeme mit umfassender Funktionalität zum Schutz vor nicht erwünschtem Datenabfluss. Unternehmen können mit dem Einsatz einer einzigen Lösung personenbezogene Daten und digitale immaterielle Werte gleichermaßen schützen und im Rahmen von DSGVO, GeschGehG, ISO 27001 und weiteren internationalen Standards ihren Nachweispflichten nachkommen. So entsteht mehrfacher Nutzen bei gleichen Kosten.

ENDPOINT PROTECTOR

Endpoint Protector GmbH
Gebhardstrasse 7 · 88046 Friedrichshafen
Deutschland
Tel.: +49 7541 978267 30 · Fax: +49 7541 9782627 9
E-Mail: info@endpointprotector.de
Internet: www.endpointprotector.de