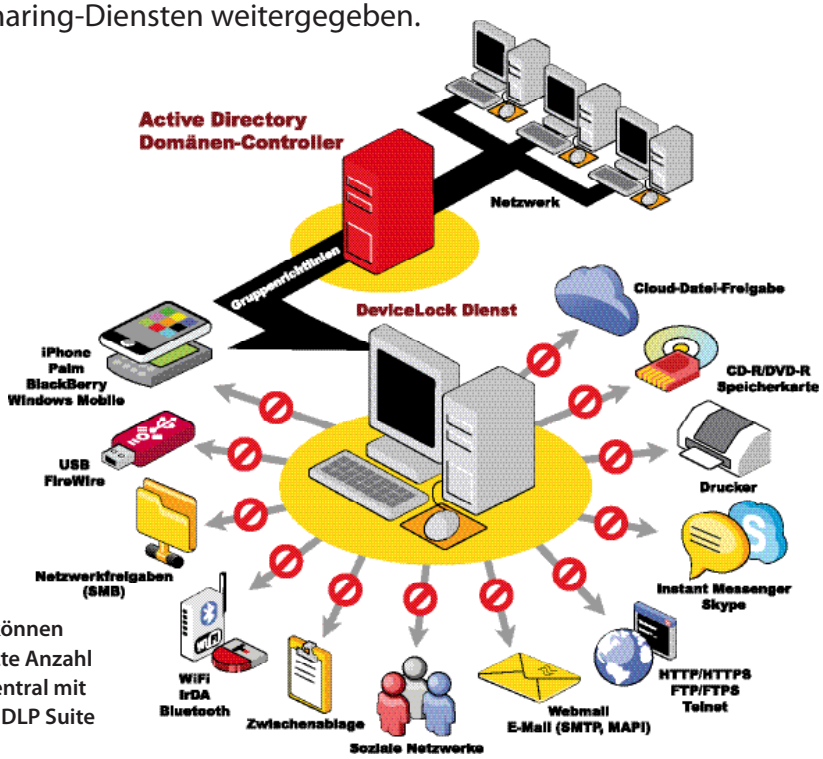
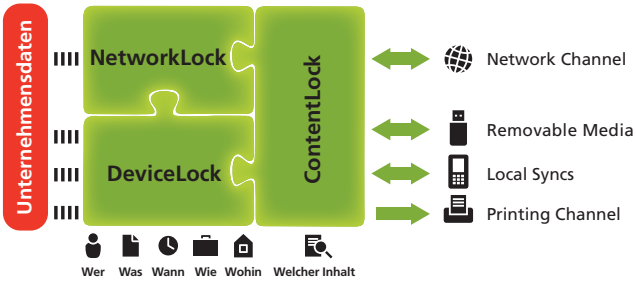
DLP stoppt Datenverlust in der Web- und Netzwerk-kommunikation

Firewalls, komplexe Passwörter und Verschlüsselungslösungen schützen die Daten innerhalb des Netzwerks. Dennoch sind die Daten nicht sicher. Benutzer kopieren – bewusst oder unbewusst – vertrauliche Informationen auf USB-Sticks, Smartphones oder andere Speichergeräte. Alternativ werden sensible Daten in sozialen Netzwerken, über E-Mail, Instant Messenger oder in Cloud-basierten File-Sharing-Diensten weitergegeben.



Unternehmen können eine unbegrenzte Anzahl Workstations zentral mit der DeviceLock DLP Suite schützen.

Die Mobilität nimmt in der IT stetig zu. Doch kabellose Schnittstellen wie Bluetooth oder WLAN – insbesondere durch BYOD – erweitern die Gefahr von ungewolltem Datenabfluss. In wessen Hände die Unternehmensdaten letztlich gelangen, kann kaum noch kontrolliert werden. Die DeviceLock DLP Suite setzt Datenschutzrichtlinien im Hinblick auf den Kontext und Inhalt von Datentransfers durch, um derartige Datenlecks zu verhindern.



Die Datenflusskontrolle der DeviceLock DLP Suite

Schutz von virtualisierten Infrastrukturen

Die virtuelle DLP von DeviceLock erweitert diesen Schutz auf eine Vielzahl von Technologien zur Virtualisierung von Desktops und Anwendungen für sitzungsbasierte, übertragene und lokale virtuelle Maschinen sowie für BYOD-Geräte: Sie umfasst die Kontrolle aller lokalen Schnittstellen und der gesamten Web- und Netzwerkkommunikation, ein Event-Logging und die Datenspiegelung für alle Datenkanäle. Der Content-Filter prüft und bewertet ergänzend zum Kontext den Inhalt der Datenbewegungen.

Alle Wege des potenziellen Datenverlusts durch z.B. externe Geräte, Netzwerk-/Webverbindungen, Smartphones oder Wechseldatenträger werden kontrolliert, auch innerhalb von Terminal-Sessions auf Thin-Clients. Klar definierte Regeln garantieren risikofreie Datentransfers und setzen individuelle Sicherheitsrichtlinien im Hinblick auf den Kontext um. In Abhängigkeit ihrer Position erhalten Benutzer verschiedene Rechte für das Übermitteln, Empfangen und Speichern von Daten. Dadurch gehen sie ungehindert ihren Aufgaben nach, ohne der Gefahr unberechtigter Datenoperationen ausgesetzt zu sein. Die inhaltliche Analyse und Filterung kontrolliert jeden Datenaustausch mit Wechseldatenträgern, PnP-Geräten und Netzwerk-/Webverbindungen.

Einfache Werkzeuge für ein umfassendes DLP-Management

DeviceLock bietet einfache und transparente Werkzeuge für ein umfassendes DLP-Management und wendet zentral definierte DLP-Richtlinien an. So kann der erfolgte und/oder unterbundene Datentransfer von Benutzern auf Peripheriegeräte, über lokale Schnittstellen und Netzwerk-/Webverbindungen zentral gesteuert, protokolliert, gespiegelt, analysiert und mit einer Alarmierung verbunden werden. Zusätzlich werden Hardware-Keylogger erkannt und ihre Benutzung blockiert, um den Verlust von Passwörtern und anderen proprietären Daten zu verhindern.

Feingliedrige Kontextkontrollen

Die DeviceLock DLP Suite reduziert das Risiko eines Datenverlusts durch feingliedrige Kontextkontrollen aller Datenkanäle an den Mitarbeiter-PCs und durch die Inhaltsfilterung von Datentransfers. Gleichzeitig übernimmt sie die Rolle eines Werkzeugs zur Durchsetzung interner Sicherheitsrichtlinien und stellt die Einhaltung gesetzlicher Vorgaben nach dem Bundesdatenschutzgesetz (BDSG), dem Sarbanes-Oxley-Act (EURO/SOX) und den ISO/BSI-Normen sicher.

Die Kontextkontrolle aller lokalen Schnittstellen inklusive Event-Logging und Datenspiegelung erfolgt durch DeviceLock. Diese umfasst zusätzlich auch Gerätetypen wie Wechseldatenträger, verbundene Smartphones/PDAs, optische Laufwerke, Drucker und die Zwischenablage. Die Kontrolle dieser Typen kann auch innerhalb einer RDP/Terminal-Session auf einem Thin-Client durchgesetzt werden. Daneben umfasst DeviceLock die zentralen Management- und Administrationskomponenten.

Schutz der Web- und Netzwerkkommunikation

Durch NetworkLock wird die Kontextkontrolle auf die Web- und Netzwerkkommunikation ausgedehnt. Die verwendeten Protokolle und Anwendungen werden Port-unabhängig erfasst und wahlweise gesteuert.

Als vollwertiger Inhaltsfilter ermöglicht ContentLock die Protokollierung und Filterung von Daten, die auf oder von Wechseldatenträgern und PnP-Geräten kopiert werden. Ergänzend erfolgt die Analyse und Steuerung verschiedener Dateiobjekte innerhalb der Netzwerk-/Webkommunikation. Über die Content-Filtering-Technologien können Echtzeit-Alarme generiert werden, die per SMTP, E-Mails oder das SNMP-Protokoll versendet werden.

Die Volltextsuche in der zentralen Dateispiegelungs-/Protokolldatenbank ermöglicht der DeviceLock Search Server. Unternehmen erhalten eine präzise, einfach zu handhabende und effiziente Unterstützung in den arbeitsintensiven Prozessen der Informationssicherheitsprüfungen, Untersuchung von Vorfällen und der Dateiforensik.

Kontrolle der „ruhenden Daten"

Um proaktiv Datenverluste zu verhindern und Compliance mit regulatorischen und unternehmerischen Datensicherheitsrichtlinien zu erreichen, benutzen Unternehmen DeviceLock Discovery, das sich mit den „ruhenden Daten"

Kontrolle ruhender Daten mit DeviceLock Discovery

befasst. Durch das automatische Scannen von Daten auf Netzwerkfreigaben, Speichersystemen und Windows basierten Computern innerhalb und außerhalb des Unternehmensnetzwerks sucht DeviceLock Discovery Dokumente mit sensiblen Inhalten, bietet Optionen, um diese durch Korrekturmaßnahmen zu schützen und Incident-Management-Verfahren einzuleiten, indem Echtzeit-Alarmierungen zu einem in der Organisation verwendeten SIEM-System (Security Information und Event Management) gesendet werden. *Thomas Tuckow, DeviceLock* ■

Kontakt

DeviceLock Europe GmbH
Halskestr. 21, 40880 Ratingen
Tel.: 02102/131840
Fax: 02102/1318429
E-Mail: info@devicelock.de
Web: www.devicelock.de