

Trend Micro™

LeakProof™ 3.0

Umfassender Schutz kritischer Daten – im Speicher, bei der Bearbeitung und bei der Übertragung

Der Verlust von Unternehmensdaten und geistigem Eigentum kann Geldstrafen, Rechtsstreitigkeiten, Imageschäden und sogar negative Schlagzeilen nach sich ziehen. Daher benötigen Unternehmen eine wirksame Lösung zum Schutz vor Datenverlust (Data Leak Prevention, DLP), die mögliche Schlupflöcher dort überwacht, wo die Daten verwendet werden. Doch angesichts der Vielzahl von Messaging-Systemen, kabelloser Datenübertragung und USB-Speichermedien gestaltet sich der Schutz wichtiger Unternehmensdaten zunehmend schwierig – die Folge: In Unternehmen kommt es immer häufiger zu Datenverlust oder sogar Diebstahl durch Mitarbeiter oder Zulieferer, die Daten vorsätzlich oder versehentlich an Dritte weiterleiten.

Die Einhaltung unternehmensinterner Sicherheitsrichtlinien und Datenschutzbestimmungen wie SB-1386, GLBA, EU DPD, Sarbanes-Oxley und HIPAA (Healthcare Insurance Portability and Accountability Act) erfordert außerdem umfassende Sicherheitsrichtlinien zum Schutz von vertraulichen Daten und Privatsphäre der Benutzer. Um sich diesen Herausforderungen zu stellen, benötigen Unternehmen eine intelligente Content-Filter-Lösung, die Sicherheitsrichtlinien durchsetzt und Mitarbeiter im angemessenen Umgang mit Informationen schult.

Trend Micro Leak Proof™ verhindert den Verlust wichtiger Daten in Unternehmen. Dazu setzt die Lösung auf eine einzigartige Kombination aus endpunktbasierter Durchsetzung und hochpräziser Technologie zur Authentizitätsprüfung und zum Abgleich von Inhalten. Die vollständige LeakProof Lösung besteht aus einem Software-Client und einem Server:

- **LeakProof Anti-Leak Client:** Eine im Hintergrund ausgeführte, leistungsstarke Software zur Überwachung und Durchsetzung, die an den Endpunkten Datenverluste entdeckt und verhindert. Der Client kommuniziert mit dem DataDNA™ Server, von dem er Richtlinien- und Authentizitätsdaten-Updates erhält; im Gegenzug meldet der Client dem Server Verstöße gegen die Sicherheitsrichtlinien.
- **LeakProof DataDNA™ Server:** Der Server bietet einen zentralen Überblick über das System, Richtlinienkonfiguration und die Extraktion von Authentizitätsdaten aus Inhaltsquellen. Die webbasierte Oberfläche unterstützt den Administrator bei der Erkennung, Klassifizierung, Richtlinienanpassung, Überwachung und Berichterstattung.

UMFASSENDE SCHUTZ: DATEN, PORTS, PROTOKOLLE, NETZWERKE

LeakProof bietet den derzeit umfassendsten Schutz für Netzwerkperipherie und Endpunkte. Geschützt werden Protokolle, wie z. B. HTTP/S, FTP, SMTP, Webmail und Instant Messaging, sowie Ein- und Ausgang von Daten an den Endpunkten (beispielsweise Dateiübertragungen auf USB-Laufwerke). Integrierte Filtermodule überprüfen den Inhalt vor der Verschlüsselung, um Aktivitäten durch Webbrowser und E-Mail-Anwendungen zu schützen. Mehrere Abgleichs-Engines filtern Inhalte in Echtzeit über Authentizitätsdaten, reguläre Ausdrücke, Schlüsselwörter und Metadaten. Die leistungsstarken Algorithmen extrahieren Informationen aus dem Inhalt, um für jedes Dokument einen einzigartigen „Fingerabdruck“ in Form einer Abfolge spezifischer Merkmale zu erstellen, mit dem Richtlinien an jedem Endpunkt on- oder offline durchgesetzt werden können.

NEU! INTERAKTIVE MITARBEITER-AUFKLÄRUNG, VERSCHLÜSSELUNG UND ARBEITSABLÄUFE

Über interaktive „Warnmeldungen“ können IT-Manager kontextsensitive Dialogfelder erstellen, die direkt auf dem Bildschirm eines Mitarbeiters angezeigt werden. Diese Felder enthalten benutzerdefinierte Links zu Informationen, die Mitarbeiter im angemessenen Umgang mit vertraulichen Daten schulen. Die Übertragung nicht autorisierter Daten wird gesperrt, oder die Mitarbeiter müssen das integrierte Datenverschlüsselungsmodul verwenden, um Daten auf USB-Geräte zu kopieren.

DATENERKENNUNG UND SICHERHEITSSUCHLÄUFE

Die kontinuierliche Überwachung durch LeakProof™ bietet unternehmensweite Sicherheit; Richtlinienbeauftragte können wie mit einem Radar kritische Daten orten und dadurch das Risiko von Datenverlust vermindern. LeakProof entdeckt nicht autorisierte Daten an Endpunkten, wie Laptops, Desktops und Server.

VERHINDERT DATENVERLUST

- Mobile Mitarbeiter, Zweigstelle, Hauptsitz
- Endpunkte – online oder offline
- Unternehmensnetzwerke
- Öffentliche Netzwerke
- USB, Bluetooth, WiFi, E-Mail
- Daten im Speicher, bei der Bearbeitung oder Übertragung

SCHUTZUMFANG

- Datenlecks
- Datenverlust

ENTSCHEIDENDE VORTEILE

- **Schutz der Privatsphäre:** Unangemessene Nutzung von Benutzer- und Mitarbeiterdaten überwachen und verhindern
- **Geistiges Eigentum schützen:** Kritische Unternehmensdaten aufspüren, klassifizieren und schützen
- **Datenschutzrichtlinien einhalten:** Nutzung überwachen, Endpunkte durchsuchen und Mitarbeiter schulen, um das Risiko zu mindern
- **Mitarbeiter schulen:** Interaktive Dialoge an Informationsstand und Arbeitsabläufe von Mitarbeitern anpassen
- **Kritische Daten entdecken:** Kritische Daten auf Laptops, Desktops und Servern finden

„Mit Trend Micro LeakProof™ hat der Administrator mehr Kontrolle darüber, was die Mitarbeiter sehen können und was sie tun dürfen. Interaktive, informative Dialoge helfen bei der Behebung von Sicherheitsproblemen.“

Martin Hodgett, CIO
Orchard Supply Hardware (OSH)

LEAKPROOF SCHUTZ VOR DATENVERLUST – DIE FUNKTIONEN IM ÜBERBLICK

Abgleich kritischer Daten

- Authentizitätsdaten, reguläre Ausdrücke, Schlüsselwörter, Abgleich mit Metadaten
- Strukturierte und nicht strukturierte Daten
- Sprachunabhängig

Zielgenaue Sicherheitsrichtlinien

- Protokollierung, Warnmeldungen auf Server- und Client-Seite, Sperren, Verschlüsselung, Begründung
- Gesonderte Richtlinien für Online- und Offline-Verstöße
- Endpunkt-Sicherheitsrichtlinien gemäß Domäne und Gruppe
- Konfigurierbare Sicherheitsgrenzen: LAN, PC, vertrauenswürdige/nicht vertrauenswürdige Mail-Domains

Erkennung und Verwaltung von Endpunkttopologien

- Erkennung von Computern an Unternehmensendpunkten
- Echtzeitanzeige des Endpunktstatus in Kartenform
- Zentrale Überwachung und Verwaltung des Client-Status
- Detaillierte Anzeige des Status der Endpunkte
- Erkennung nicht autorisierter E/A-Geräte an den Endpunkten

Überwachung von Geräten und Anwendungen

- Überwachung aller E/A-Geräte: USB, Disketten, Bluetooth, IrDA, bildgebende Geräte, COM- und LPT-Ports, usw.
- Sperren der PrintScreen- (PrtSc) Funktion

Überwachung und Berichterstattung

- Echtzeit-Dashboard und Berichte über Sicherheitsverstöße gemäß Endpunkten, Benutzern, usw.
- Entwicklungsanalyse und Abschottung von Sicherheitslücken
- Zeitgesteuerte und nach Bedarf erstellte Berichte über Sicherheitsverletzungen
- Optionale forensische Erfassungsfunktion protokolliert den tatsächlichen Dateiverstoß auf dem DataDNA Server zur späteren Begutachtung

Vorlagen zur Richtlinieneinhaltung

- Vorkonfigurierte Klassifikationen und Richtlinien zur Einhaltung von Richtlinien wie PCI, GLBA, SB-1386 und SOX
- Integrierte Regeln mit Validierungsmodulen

Systemadministration und -skalierbarkeit

- Verwaltungsschnittstelle für Webbrowser
- Rollenbasierte Administration und gesteuerter Zugriff auf kritische Inhalte
- Sichere Kommunikation zwischen Endpunkt und Server über SSL

SYSTEMVORAUSSETZUNGEN

LeakProof Anti-Leak Client Software

- **Unterstützte Plattformen:** Microsoft Vista, Windows XP, Windows 2000, Windows 2003 Server

LeakProof DataDNA Server Appliance

- Zweckmäßige 1U-Rack-montierbare Appliance
- Sicherheitsoptimiert
- Gigabit Network Interface Card (NIC)
- Erhältlich als Einzel-/Dualprozessor
- Arbeitsspeicher: 2 GB/4 GB
- Speicherplatz: 160 GB/300 GB RAID

UMFASSENDE SCHUTZ VON DATEITYPEN, ANWENDUNGEN UND GERÄTEN



LeakProof DataDNA Server

Die LeakProof DataDNA Server Appliance kommuniziert mit der LeakProof Anti-Leak Client Software, um kritische Daten vor Verlust, Diebstahl und internen Bedrohungen zu schützen.

Unterstützte Dateitypen

- Erkennt und verarbeitet mehr als 300 Dateitypen
- Microsoft™ Office Dateien, u. a. Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™ E-Mails; Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, Text, usw.
- Grafikdateien: Visio, Postscript, PDF, TIFF, usw.
- Software-/Entwicklerdateien: C/C++, JAVA, Verilog, AutoCAD, usw.
- Archivierte/komprimierte Dateien: Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH, usw.

Unterstützte Netzwerkanwendungen

- E-Mail: Microsoft Outlook, Lotus Notes und SMTP Email
- Web-Mail: MSN/Hotmail, Yahoo, GMail, AOL Mail und andere
- Instant Messaging: MSN, AIM, Yahoo und andere
- Netzwerkprotokolle: FTP, HTTP/HTTPS und SMTP

Unterstützte Endpunktgeräte

- USB, SCSI, (S)ATA, EIDE, PCMCIA, CD/DVD, Disketten, Bluetooth, IrDA, WiFi, Drucker, bildgebende Geräte COM-Port, LPT-Port, usw.

