MATRIX42

Data Loss Prevention

Effektiver Schutz vor Datenverlust

Solution Paper

Data Loss Prevention im Überblick

Hintergrund – Datendiebstahl auf dem Vormarsch

Darum lohnt sich Data Loss Prevention

Die Lösung: EgoSecure Data Loss Prevention

1 Hintergrund – Datendiebstahl auf dem Vormarsch

7 von 10 Industrieunternehmen wurden Opfer von Sabotage, Datendiebstahl oder Wirtschaftsspionage in den vergangenen zwei Jahren. Dadurch ist ein Schaden von 43,4 Milliarden Euro entstanden. Bei einem Drittel der Unternehmen (32 Prozent) wurden IT- oder Telekommunikationsgeräte gestolen, bei fast einem Viertel (23 Prozent) sind sensible digitale Daten abgeflossen (Quelle: Studie der bitkom vom 13. September 2018).[1]

Mittelständler werden am häufigsten angegriffen

War Ihr Industrieunternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen?

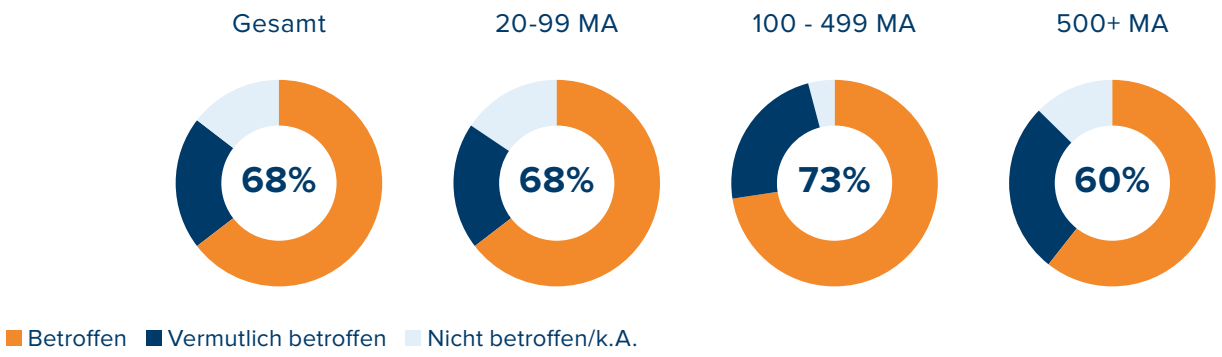

Abbildung 1 – Ergebnisse Bitkom Research

In vielen Fällen ist es für einen Mitarbeiter mit schlechten Absichten besonders einfach wertvolle Daten zu entwenden, da häufig keinerlei Schutzmaßnahmen dagegen existieren. Ein Virenschutz oder eine Firewall sind keine geeigneten Mittel, um das zu verhindern.

Neben dem absichtlichen Datendiebstahl ist der Abfluss von Daten häufig auf menschliches Versagen zurückzuführen: der Mitarbeiter vergisst einen USB-Stick im Zug, sein Firmenhandy im Taxi oder legt vertrauliche Daten an eine falsche (öffentliche) Stelle ab oder schickt Daten aus Versehen an eine verkehrte E-Mail-Adresse.

Selbst eine klassische Verschlüsselungslösung wie zum Beispiel eine Festplatten- oder eine File- und Folder-Verschlüsselungslösung kann dies nicht verhindern, zumindest nicht solange der potenzielle Täter dafür berechtigt ist.

Wie ernst Experten die Lage einschätzen, wird beispielsweise deutlich an der Aussage von Jörg Ziercke, Präsident des Bundeskriminalamtes: „Früher oder später wird jeder mit dem Internet verbundene PC mit Schadsoftware infiziert. Dagegen kann sich keiner schützen“ (Quelle: Gespräch mit TecChannel am Rande eines Symposiums).[2]

Wir teilen den Ernst der Lage, aber nicht die Einschätzung, dass man sich nicht dagegen schützen kann. Auch wenn der Schutz vor internem Datendiebstahl leichter ist.

[1] https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html

[2] https://www.tecchannel.de/a/dlp-schutz-vor-ungewolltem-datenabfluss,2020290

2

Darum lohnt sich Data Loss Prevention

Data Loss Prevention (DLP) wird häufig auch Data Leak Prevention oder Data Leakage Prevention genannt und bedeutet vorbeugenden Schutz gegen Datenverlust. Informationen wie Kreditkartennummern, Zugangsdaten oder personenbezogene Daten lassen sich leicht in Dokumente kopieren und nach außen tragen. Damit riskiert ein Unternehmen den Missbrauch oder Verlust von sensiblen Unternehmensdaten und verstößt darüber hinaus unter Umständen gegen Datenschutzgesetze.
Eine DLP-Software beinhaltet eine oder mehrere Funktionen, mit deren Hilfe Daten vor nicht autorisierten Zugriffen geschützt werden sollen. Häufig gehört auch eine Gerätekontrolle zum Leistungsumfang, um beispielsweise den Einsatz mobiler Geräte kontrollieren zu können.

Steuerungsmöglichkeiten durch eine DLP-Software sind in der Regel das komplette Verbot kritischer Vorgänge und/oder das Hinweisen der Mitarbeiter auf kritische Vorgänge sowie das Protokollieren aller heiklen Datenvorgänge bzw. Datenbewegungen.

Um Datenverlust proaktiv zu vermeiden, sind granulare auf das Unternehmen abgestimmte Richtlinien sinnvoll. Diese sollten nicht nur an Endbenutzer kommuniziert, sondern deren Einhaltung auch beim Speichern und Verwenden sensibler Daten – im Idealfall – automatisch gesteuert werden. Darüber hinaus sollte der Schutz vor Datenverlust in den Arbeitsalltag integriert sein und darf gewohnte Abläufe und Prozesse nicht stören.

Zusätzlich ist es sinnvoll, loyale Mitarbeiter einer Organisation in die Maßnahmen zur Data Loss Prevention einzubeziehen und sie für das Thema zu sensibilisieren. Die ist besonders wichtig, weil vermehrt auch direkte Manipulation von Menschen mittels gezielter persönlicher Ansprache und Aufbau von Vertrauen (Social Engineering) erfolgt.

3

Die Lösung: EgoSecure Data Loss Prevention

Mit **EgoSecure Data Loss Prevention** (DLP) durchsuchen Sie Dokumente nach sensiblen Informationen und verhindern deren Weitergabe nach außen – entweder präventiv durch geplante automatisierte Scans oder in Echtzeit vor dem Speichern auf externe Geräte. Gleichzeitig sensibilisieren Sie Endbenutzer für das Thema Datensicherheit, da dieser bei verbotenen Vorgängen eine entsprechende Hinweismeldung erhält.

Will ein Benutzer ein Dokument auf einem externen Gerät wie z. B. einem USB-Stick speichern, prüft DLP anhand der von Ihnen definierten Suchmustern automatisch, ob sensible Daten im Dokument vorhanden sind. Wird ein Treffer erzielt, kann die Übertragung protokolliert und blockiert werden. Eine Meldung informiert über diesen Vorgang. So beugen Sie Datenverstößen vor und sensibilisieren Ihre Benutzer für den Datenschutz. Durch automatisierte Festplattenscans erhalten Sie gleichzeitig einen Überblick, wo sensible Informationen im Unternehmensnetzwerk abgelegt sind.

Funktionsweise

EgoSecure Data Loss Prevention unterteilt sich in zwei Module:

- **Data in Use (DIU)** zum Echtzeit-Scannen von externen Speichermedien (benutzerbasiert) Mit DIU überprüfen Sie in Echtzeit, ob sensible Daten von Endgeräten auf externe Speichermedien kopiert werden oder umgekehrt. Will ein Benutzer ein Dokument auf einem externen Speichergerät wie z. B. einem USB-Stick speichern, prüft DLP anhand von Ihnen definierter Suchmuster automatisch, ob sensible Daten im Dokument vorhan¬den sind. Wird ein Treffer erzielt, kann die Übertragung protokolliert oder blockiert werden. Eine Meldung informiert den Benutzer über den Vorgang.

- **Data at Rest (DAR)** zum geplanten Scannen von Festplatten und Netzwerkordnern (computerbasiert) Mit DAR beugen Sie Datendiebstahl vor, indem Sie Festplatten und Verzeichnisse regelmäßig nach sensiblen Informationen durchsuchen.

Highlights

- **Definition der Suchmuster über einfache lexikalische oder komplexe reguläre Ausdrücke**
- **Vordefinierte, gebräuchliche Suchmuster für nationale und internationale Nummerncodes wie Versicherungsnummern, Passwort-IDs, IBAN & Swift, Kreditkartennummern etc.**
- **Unterscheidung zwischen Lese- und Schreibzugriff (DIU)**
- **Unterschiedliche Aktionen für jede Regel definierbar**
- **Automatisierte detaillierte Protokollierung von Ereignissen**
- **Globale, gruppenspezifische oder individuelle Regelzuweisung**

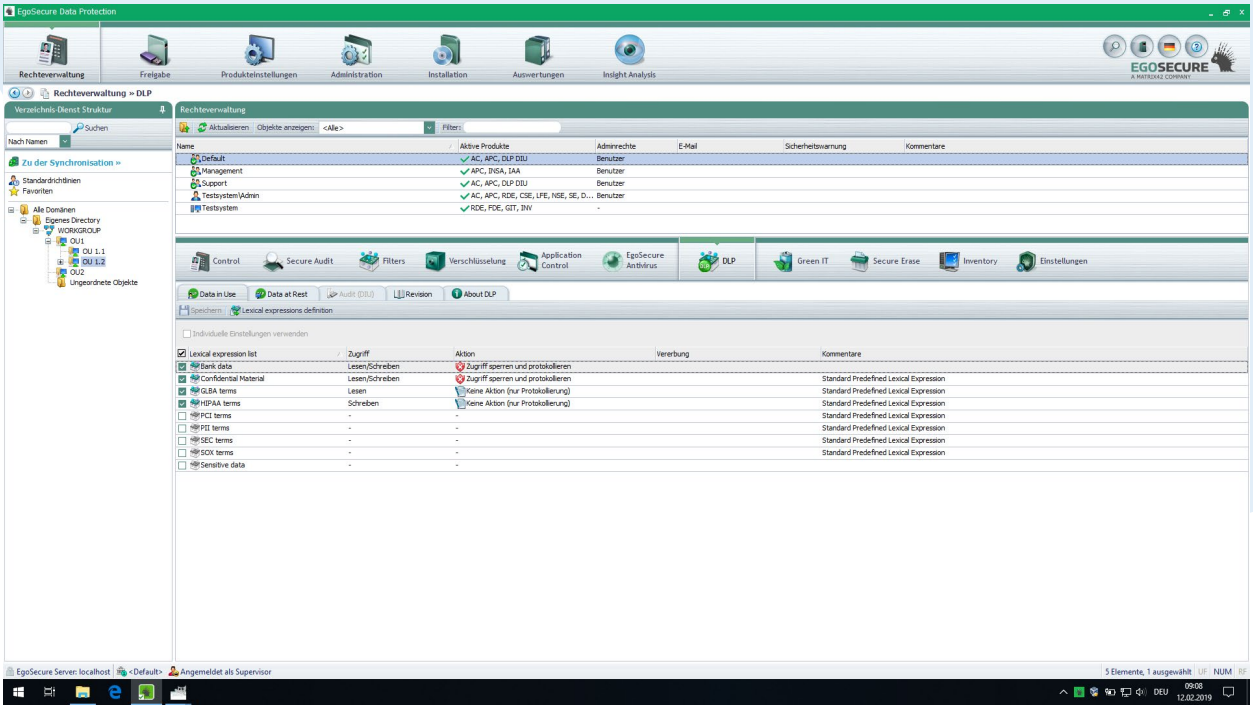

Abbildung 2 – Filter für einen Benutzer oder eine Gruppe aktivieren

Definition von Regeln

- Verwendung von vordefinierten Suchmustern, einfachen Ausdrücken (ganze Zeichenketten) oder regulären Ausdrücken
- Verknüpfung von Suchmustern mittels Operatoren (Und, Und nicht, Oder, Entweder-Oder, Vor, Nach, Gefolgt von, Nahe bei)
- Ein oder mehrere Ausdrücke innerhalb einer Regel definierbar
- Gewichtung von Ausdrücken und Definition eines Schwellenwertes für Treffer, die Aktionen auslösen sollen Beispiel:
  - Ausdruck 1: Gewichtung 3
  - Ausdruck 2: Gewichtung 2
  - Schwellenwert: 5, wenn beide Ausdrücke gefunden werden (3+2) oder Ausdruck 1 zweimal gefunden wird (3+3), wird der Schwellenwert erreicht, ein Treffer erzielt und eine Aktion ausgelöst.
- Regelzuweisung global, benutzerspezifisch oder gruppenspezifisch möglich
- Regelauswertung mit/ohne Berücksichtigung von Groß-/Kleinschreibung

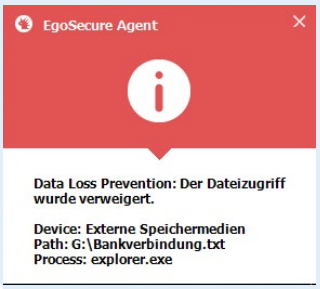

Abbildung 3 – Gesperrter Zugriff aus Nutzersicht

Aktionen und Auswertung

- **Mögliche Aktionen bei Ereignissen**
  Blockieren der Datenübertragung (DIU), unter Quarantäne stellen (DAR), Ausgabe einer Benutzermeldung, Proto_ kollierung des Vorgangs
- Unterscheidung von Aktionen bei Lesezugriff, Schreibzugriff oder beiden Zugriffsarten (DIU)
- **Protokolldaten eines Ereignisses**
  Speichermedium, Computername, Datei, Datum und Uhrzeit, Art des Zugriffs, ausgelöste Aktion, Name der Regel, Suchmuster der Regel, Anzahl der Ereignisse, gefundener Text (auch versteckt darstellbar mittels Asterisk-Symbol)

Sinnvolle Ergänzungen für DLP ermöglichen noch mehr Datensicherheit

- **Insight** – sammelt Fakten über die datenschutzrelevante Situation in Ihrem Netzwerk und stellt diese als Grafiken und sehr detaillierte Tabellen zur Verfügung. Im Zusammenspiel mit **IntellAct** können die Fakten ausgewertet werden und aufgrund vorher definierter Regeln Schutzmaßnahmen automatisch ausgelöst werden.
- **Control** ermöglicht die Zugriffskontrolle und Steuerung von Geräten und Schnittstellen.
- Secure **Audit** macht die Datenflüsse im Detail sichtbar, zeigt mögliche Schwächen in den Schutzeinstellungen und ermöglicht die Ermittlung forensischer Informationen. Das Bundesdatenschutzgesetz schreibt eine solche Protokollierung zwingend vor.
- **Umfassende Verschlüsselung** für Daten in lokalen Ordnern, Netzwerkordnern, Cloudspeichern und Festplatten
- Automated **Endpoint Detection & Response (EDR)**. Da wo der klassische Virenschutz aufhört, fängt die Post-Infection-Lösung Automated EDR an: es werden nur legitime Verbindungen und Dateimodifizierungen zugelassen, so dass Datendiebstähle oder das Ausführen von Schadcode erfolgreich verhindert werden – auch nach einer Infektion. Und das in Echtzeit.

Datensicherheit wird integraler Bestandteil

Matrix42 bietet weitere Lösungen, die das IT-Arbeitsplatzmanagement standardisieren und vereinfachen. Durch die Kombination von Software- und Gerätemanagement mit Datensicherheit untereinander ergeben sich Szenarien, die die Vorteile weiter maximieren. Das bedeutet für Ihre IT: Weniger Risiken und mehr Entlastung im operativen Tagesgeschäft.

- **Unified Endpoint Management:** Das Beste aus zwei Welten. Client Management und Enterprise Mobility Management vereint in einer Lösung

- **Service Management.** Abbildung und Automatisierung von Services und Serviceprozessen für mehr Kostentransparenz und gesteigerte Servicequalität

- **Software Asset Management.** Mit Lizenz-, Asset-, und Vertragsmanagement ganz einfach die Kosten im Griff behalten und optimal vorbereitet für das nächste Software Audit sein

„Bleiben Sie zum Thema Datensicherheit auf dem Laufenden, schreiben Sie eine Email an **marketing@matrix42.com** mit dem Betreff **„Ich will Datensicherheit“** und wir informieren Sie zukünftig zu vergleichbaren Themen als erstes, und das unverbindlich und kostenlos.

Standorte

Hauptsitz Deutschland
Matrix42 AG
Elbinger Straße 7
60487 Frankfurt am Main
Deutschland
Telefon: +49 69 66773-8380
Fax: +49 69 66778-8657
info@matrix42.com

Niederlassung Schweiz und Österreich
Matrix42 Helvetia AG
Habsburgerstrasse 52A
6003 Luzern
Telefon: +41 41 720-4220
info@matrix42.ch

Weitere Niederlassungen im Ausland finden Sie auf unserer Website.

www.matrix42.com

Über Matrix42

Matrix42 unterstützt Organisationen dabei, die Arbeitsumgebung ihrer Mitarbeiter zu digitalisieren und sicherer zu machen. Die Software für Digital Workspace Experience verwaltet Geräte, Anwendungen, Prozesse und Services einfach, sicher und konform. Die innovative Software integriert physische, virtuelle, mobile und cloudbasierte Arbeitsumgebungen nahtlos in vorhandene Infrastrukturen.

Die Matrix42 AG hat den Hauptsitz in Frankfurt am Main, Deutschland, und vertreibt und implementiert Softwarelösungen weltweit mit lokalen und globalen Partnern.

Webversion-Solution-Paper-Data-Loss-Prevention-DE-201901-v01