Data-Loss-Prevention

Endpoint Protector stellt Next-Generation-DLP vor

Strengere Datenschutz-Vorschriften, zunehmende Digitalisierung und engere Vernetzung machen den Schutz sensibler Inhalte vor unerwünschtem Abfluss zu einer Kernaufgabe der Unternehmen. Hersteller von Data-Loss-Prevention-(DLP)-Lösungen entwickeln angesichts der steigenden Anforderungen neue Erkennungstechnik auf der Grundlage mathematischer Verfahren. Sie ermöglicht, dass die DLP-Lösungen der nächsten Generation auf unternehmensspezifische Themen trainierbar sind und beim Schutz komplexer Inhalte effizient arbeiten.

Von Michael Bauner, Endpoint Protector GmbH

Die DSGVO führt zu einem Lernprozess in den Unternehmen und Organisationen. Sie begreifen die Auswirkungen von Datenverlust auf ihre Marktstellung und erkennen, dass sie neben den personenbezogenen Daten auch Geschäfts- und Firmengeheimnisse sowie Angaben zu kritischen Infrastrukturen vor unkontrolliertem Abfluss schützen müssen. Deren Anfälligkeit für Verlust und Diebstahl nimmt mit der Digitalisierung rapide zu, denn die Datenbestände wachsen exorbitant und immer mehr Mitarbeiter, Zulieferer und Kunden haben mit sensiblen Daten zu tun. Auch die Zahl der Kommunikationskanäle steigt.

Den Schutz vor unkontrolliertem Datenabfluss gewährleisten Lösungen für Data-Loss-Prevention. Deren mächtigstes Instrument ist die Inhaltskontrolle. In Endpoint Protector scannt das Modul „Content Aware Protection“ (CAP) Daten in Bewegung auf das Vorkommen sensibler Informationen, deren Muster in Black- und White-Regeln hinterlegt sind, und erlaubt beziehungsweise blockiert den Transfer entsprechender Dateien über E-Mail oder browserbasierte Anwendungen wie Webmailer, Cloud-Speicher, Filesharing- oder Collaboration-Tools.

In der Software sind Regeln für Gruppen von personenbezogenen Daten hinterlegt, beispielsweise für Adressdaten, Sozialversicherungs-, Kreditkarten-, Pass- und Personalausweisnummern. Diese vordefinierten Erkennungsschemata vereinfachen die Einrichtung der Richtlinien. Sie lassen sich zudem für die Umsetzung von Policies aus gesetzlichen Vorgaben und internationalen Standards wie DSGVO, HIPAA oder PCI-DSS in schnell einzurichtende Pakete zusammenfassen. Zudem können Unternehmen Dateien auf unternehmensspezifische Inhalte prüfen. Dafür lassen sich, beispielsweise zum Schutz des geistigen Eigentums oder kritischer Infrastrukturen, individuelle Wörterbücher mit Schlüsselbegriffen und regulären Ausdrücken zur Analyse von Zeichenketten anlegen.

Die Inhaltskontrolle einer DLP-Lösung prüft Daten in Bewegung auf sensible Informationen.

Da die Digitalisierung die Diversifizierung der Rechnerlandschaften in den Unternehmen beschleunigt, ist für den Erfolg von Data-Loss-Prevention entscheidend, dass sich die Richtlinien auf alle Rechner anwenden lassen. Es sollte keine Bereiche geben, in denen sie nicht umgesetzt werden können, weil die DLP-Lösung nicht alle Betriebssysteme abdeckt. Endpoint Protector funktioniert betriebssystem-übergreifend und gewährleistet in gemischten Umgebungen für alle Rechner den gleichen Schutzumfang.

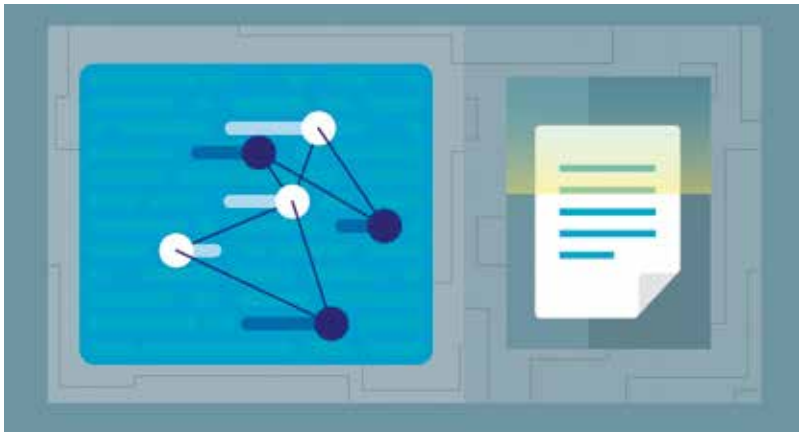
© DATAKONTEXT GmbH · 50226 Frechen · <kes> Special it-sa, Oktober 2018

Suche nach unstrukturierten Daten

Die Verfahren und Richtlinien für Daten in Bewegung nutzt Endpoint Protector auch für die Suche nach ruhenden Daten. Diese befinden sich nicht nur in Systemen wie ERP oder CRM, sondern in unstrukturierter oder semistrukturierter Form auch auf den Festplatten der Arbeitsplatzrechner sowie in Cloud-Speichern wie Dropbox, OneDrive, iCloud, Google Drive. Dabei handelt es sich oft um Exporte aus den zentralen Systemen sowie um eingehende Dokumente wie Bewerbungen, Teilnehmerlisten und Ähnliches. Sie alle müssen ebenfalls der DSGVO entsprechend behandelt werden, wenn das Unternehmen sich nicht strafbar machen will. Das Modul „eDiscovery" scannt die Desktop-Computer und findet über sie auch sensible Daten in den Cloud-Speichern. Die Ergebnisse werden als Report ausgegeben, sodass die Daten gelöscht oder verschlüsselt werden können.

Der Vorteil der Mustererkennung ist ihre Zuverlässigkeit. Aber Muster können übereinstimmen und trotzdem nicht zutreffen. Sind beispielsweise Produktkennungen aufgebaut wie eine Steuer- oder Kontonummer, blockiert die DLP-Lösung den Versand von Datenblatt oder Bestellformular. Um die Quote der sogenannten False-Positives zu verringern, hat Endpoint Protector der Mustererkennung eine Umfeldsuche beigestellt, die sich als individuelle Suche innerhalb der Suchergebnisse konfigurieren lässt.

DLP-Technologie vergleicht Muster anhand von Black- und White-Regeln. Die Ergebnisse sind tadellos, solange Vergleiche ein Resultat erbringen. An ihre Grenzen kommt DLP, wenn die Muster sehr komplex werden. Dann beansprucht der Abgleich so viele Ressourcen, dass die Leistungsfähigkeit des Systems darunter leiden kann.



Für komplexe Inhalte setzt Endpoint Protector eine trainierbare Erkenungstechnologie ein.

N-Gramm-Kategorisierung als DLP-Technologie

Die digitale Transformation bewirkt, dass das, was Unternehmen als ihr geistiges Eigentum ansehen und vor unkontrolliertem Abfluss schützen wollen, an Individualität zunimmt. Gemeint sind Inhalte wie Quellcode. Damit exakt bestimmt werden kann, ob ein Text Quellcode enthält und in welcher Programmiersprache er codiert wurde, würden Bibliotheken mit enormem Datenvolumen benötigt. Das ist für einen Anbieter von Enterprise-DLP wie Endpoint Protector, der seine Lösung schlank und ressourcenschonend halten will, keine Option. Die Lösung ist eine trainierbare, ressourcensparende Technologie.

Für hochkomplexe Aufgaben wie die Suche nach Code nutzt Endpoint Protector ein mathematisches Verfahren, die N-Gramm-Kategorisierung. N-Gramme sind Fragmente einer Zeichenkette. Wie häufig bestimmte Fragmente auftreten, wird vom Thema bestimmt. Anhand von Trainingstexten lassen sich daraus Profile für thematische Kategorien erstellen. Für Dateien, deren Inhalt im Hinblick auf die Zulässigkeit einer Übermittlung bewertet werden soll, wird ebenfalls ein N-Gramm-Profil erzeugt. Die Entscheidung fällt anhand der Nähe des Dateiprofils zu einem Kategorie-Profil.

Die N-Gramm-Kategorisierung will die herkömmliche Mustererkennung nicht ersetzen, denn diese funktioniert für bestimmte Bereiche ausgezeichnet. Das neue Verfahren soll Aufgaben bewältigen, die die normale Mustererkennung überfordern. Dabei kommt nicht nur der Vorteil eines erheblich geringeren Ressourcenbedarfs zum Tragen. Darüber hinaus kann ein Unternehmen künftig eigene Trainingssets und Kategorien für spezifische Themen erstellen und den Schutz vor Datenabfluss passgenau auf die Bedürfnisse ausrichten.

Fazit

Lösungen für Data-Loss-Prevention von heute sind ausgereifte Systeme, die ein breites Spektrum an Funktionalität auf der Grundlage von Mustererkennung anbieten. Unternehmen können damit den Schutz von Daten im Rahmen von internationalen Standards und gesetzlichen Vorgaben sowie von Daten gewährleisten, die immaterielle Werte repräsentieren. Da die Anforderungen an die Erkennungstechnologie stetig steigen, geht Endpoint Protector einen Schritt weiter und entwickelt Next-Generation-DLP mit dynamischen Verfahren, die für die Erkennung unternehmensspezifischer Inhalte trainiert werden können. ■

Messestand: Halle 10.0, Stand 10.0-109