Sensible Daten aufspüren und schützen: Best Practices für strukturierte und unstrukturierte Daten

Daten gehören zu den wertvollsten Rohstoffen des 21. Jahrhunderts. Doch immer grössere Mengen an sensiblen Informationen gegen Cyber-Angriffe zu schützen, ist für Unternehmen eine Herausforderung. Viele Sicherheitsstrategien konzentrieren sich auf den Schutz strukturierter Daten in Datenbanken. Jedoch fehlen häufig Massnahmen für die ebenso sensiblen, aber oft schwieriger zu schützenden unstrukturierten Daten, beispielsweise in E-Mails oder Dokumenten. 80 Prozent der Daten in einem Unternehmen zählen laut IBM mittlerweile zu den unstrukturierten Daten. In diesen Datenmassen verbergen sich häufig geschäftskritische oder personenbezogene Informationen. Sie stellen damit ein Risiko für Unternehmen dar, wenn sie nicht ausreichend gegen unberechtigten Zugriff abgesichert werden. Im Folgenden ein kurzer Ãœberblick zu den beiden Datenformen sowie Best Practices zu deren Schutz.

Maschine versus Mensch: Strukturierte und unstrukturierte Daten

Strukturierte Daten sind so organisiert, dass sie für Maschinen einfach zu verarbeiten sind. Sie werden im Allgemeinen in relationalen Datenbanken gespeichert und in definierten Spalten und Zeilen angezeigt. Dadurch können Data-Mining-Tools und -Algorithmen darauf zugreifen und sie leicht analysieren. Traditionell verlassen sich Unternehmen bei ihren Geschäftsentscheidungen auf strukturierte Daten, beispielsweise im Lagerverwaltungs- oder Customer Relationship Management.

Unstrukturierte Daten werden hingegen in für Menschen leicht zugänglichen Formaten gespeichert. Diese Zugänglichkeit erschwert allerdings wiederum Maschinen und Algorithmen den Zugriff. Unstrukturierte Daten finden sich etwa in E-Mails, Textverarbeitungsdokumenten, PDF-Dateien, Bild-, Audio- und Videodateien, Social Media-Beiträgen oder mobilen Textnachrichten. Diese Formate erleichtern die menschliche Kommunikation, machen unstrukturierte Daten aber auch anfälliger für unberechtigten Zugriff und Datenlecks.

Best Practices zur Sicherung strukturierter und unstrukturierter Daten

Strukturierte Daten in Datenbanken lassen sich vergleichsweise einfach sichern. Der Zugang kann nach strengen Richtlinien eingeschränkt werden. Diese sollten folgende Punkte beinhaltet:
? Schaffung eines sicheren, zentralen Speichers
? Verfolgung der Dateneingabe und -nutzung
? Verwaltung von Authentifizierung und verschlüsselter Kommunikation mit SSL-Protokoll
? Schutz von Geräten durch sichere Passwörter
? Möglichkeit des Fernzugriffs zur Datenlöschung auf verlorenen Geräten
? Schulung der Mitarbeiter über Richtlinien und bewährte Sicherheitsverfahren

Der Schutz unstrukturierter Daten stellt eine grössere Herausforderung dar. Denn diese existieren überall im System, wo Benutzer auf Inhalte zugreifen oder diese erstellen. Dadurch kann es schwierig sein, überhaupt zu wissen, dass diese Daten existieren, wer Zugang zu ihnen hat oder sie verwendet. Auch die Verfolgung des Datenflusses durch einen Audit-Trail gestaltet sich schwieriger: Content Pattern Matching-Technologien können Server und Workstations scannen, um unstrukturierte Daten zu klassifizieren, aber diese Lösungen führen oft zu False Positives und Negatives, was sich negativ auf den Workflow auswirken kann. Folgende Best Practices helfen, unstrukturierte Daten zu schützen:

Identifizierung des Zugriffs auf strukturierte und unstrukturierte Daten

Unternehmen sollten identifizieren, welche Mitarbeiter Zugriff auf strukturierte und unstrukturierte Daten haben und den Zugriff auf sensible Datenquellen einschränken. Zudem sollte verwaltet werden, wie Mitarbeiter von Remote-Geräten darauf zugreifen dürfen. Die Äœberwachung der Benutzeraktivitäten bietet zusätzlichen Schutz, um beispielsweise Anomalien zu erkennen, die auf eine Cyberattacke hinweisen.

Strukturierte und unstrukturierte Daten sind für Unternehmen gleichermassen von Bedeutung. Vor dem Hintergrund der DSGVO muss deshalb sichergestellt sein, dass beide Arten geschützt sind, da bei einem Datenleck hohe Geldbussen und Reputationsschäden drohen. Datenzentrierte Sicherheitstechnologien können Unternehmen zudem unterstützen, durch kontextbasierte Klassifikation und Verschlüsselung sensible Daten gegen Diebstahl und Cyberangriffe zu schützen, selbst im Fall eines Sicherheitsverstosses.