Den richtigen Schlüssel für die Klassifizierung finden.

classify or die

Provokation oder Notwendigkeit bei der Klassifizierung

von René Eberhard

Über die Notwendigkeit der Klassifizierung von Daten als Voraussetzung für Sicherheit und den Schritt in die Cloud.

Zugegeben, der Titel dieses Beitrags ist etwas provokativ. Dennoch widerspiegelt er in etwa unsere Erfahrungen, die wir in den letzten Monaten und Jahren in vielen Gesprächen mit Unternehmensvertretern und Experten sammeln konnten. Um sensible Daten effizient zu schützen, müssen diese erst identifiziert und gekennzeichnet (klassifiziert) werden. Zudem muss verstanden werden, wer die Daten in den jeweiligen Geschäftsprozessen wo und mit welchen Hilfsmitteln verarbeitet.

Evergreen Klassifizierung

Über die Notwendigkeit der Klassifizierung ist man sich wohl einig. Die meisten Unternehmen verfügen auch über Klassifizierungsrichtlinien, die festlegen, welche organisatorischen und technischen Massnahmen in Bezug auf Verarbeitung, Übermittlung oder Speicherung von Daten umgesetzt werden müssen. Die Richtlinien unterteilen die Klassifizierung typischerweise in die Stufen Public, Intern, Vertraulich und Geheim.

Viele Unternehmen haben sich bisher aus Mangel an technischen Möglichkeiten schwer getan, unternehmensweite Klassifizierungen einzuführen und durchzusetzen. Oftmals wurden Klassifizierungen nur in spezifischen Applikationen wie beispielsweise SharePoint oder Archivsystemen eingeführt. Die jeweiligen Klassifizierungsstufen gingen ausserhalb solcher Systeme aber oftmals verloren und konnten nicht mehr maschinell ausgewertet werden.

Sinn und Zweck

Das Klassifizieren von Daten bedeutet nicht einfach, eine bestimmte Klassifizierungsstufe in die Kopf- oder Fusszeile eines Dokuments zu schreiben. Vielmehr sollten die Klassifizierungsstufen als Metadaten maschinell lesbar in die Dokumente integriert werden. Diese können dann dazu genutzt werden, technische Massnahmen zu unterstützen, um die Informationen der jeweiligen Klassifizierungsstufe zu schützen. Folgend sind ein paar Beispiele aufgeführt:

- **Data Leakage Prevention (DLP)**
  Ein DLP-System kann den Versand von Vertraulich oder Geheim klassifizierte Daten im Klartext verhindern;
- **Benutzersensibilisierung**
  Benutzer können visuell in der E-Mail- oder Browser-Applikation darauf hingewiesen werden, dass sie Vertraulich oder Geheim klassifizierte Daten im Klartext extern übermitteln möchten. Abhängig vom Geschäftsprozess können sie den Versand explizit bestätigen oder eine alternative Übermittlungsart wählen;
- **Automatische Verschlüsselung**
  Daten können auf Basis von bestimmten Klassifizierungsstufen automatisch verschlüsselt werden. Hierbei werden unterschiedliche Kanäle wie beispielsweise E-Mail, Web-Applikationen oder Fileshares (One-Drive, Dropbox) unterstützt.

Die strategische Lösung

Das Klassifizieren und Verschlüsseln von Daten sind Schlüsseltechnologien, um Daten effizient on-prem oder in der Cloud zu schützen. Die Klassifizierungs- und Verschlüsselungsverfahren müssen plattformneutral und auf unterschiedlichen Applikationen und Geräten verfügbar sein. Microsoft bietet mit Rights Management (AD RMS oder Azure RMS) ein entsprechendes Verschlüsselungsverfahren. Secure Islands hat mit dem IQProtector eine automatisierte Klassifizierungs- und Verschlüsselungslösung auf Basis von Microsofts Rights Management angeboten. Mit der Akquisition von Secure Islands treibt Microsoft die Integration und Verbreitung dieser automatisierten Klassifizierungs- und Verschlüsselungsverfahren als Teil der «Mobile First, Cloud First»-Strategie voran. Auf Basis dieser etablierten Technologien wurden schon viele Klassifizierungs- und Verschlüsselungslösungen nationaler und internationaler Unternehmen umgesetzt.

Rights Management

Mit Rights Management können sensible Daten vor unberechtigtem Zugriff effizient geschützt werden. Im Unterschied zu anderen Technologien ist die Klassi-

fizierung und Verschlüsselung untrennbar mit den jeweiligen Daten verbunden und bietet somit einen fortwährenden und für den Benutzer transparenten Schutz, unabhängig von der Datenübermittlung oder vom Speicherort. So ist es beispielsweise möglich, die Zugriffsberechtigung von SharePoint direkt auf die Daten zu replizieren. So wird sichergestellt, dass auch ausserhalb von SharePoint nur berechtigte Personen Zugriff auf die Daten haben.

Die Berechtigungen einzelner Benutzer und Gruppen können dynamisch verwaltet werden. Mit Anwendung von unterschiedlichen Profilen können ganze Gruppen oder Organisationseinheiten voneinander getrennt werden.

Automatisierung ist der Schlüssel
Rights Management bietet die plattformneutrale, technische Basis für die Klassifizierung und Verschlüsselung von Daten. Der Benutzer soll effizient und transparent mit Klassifizierungsstufen und Verschlüsselung arbeiten können. Dies wird über automatisierte Prozesse und intuitive grafische Benutzerschnittstellen sichergestellt.

Automatische Klassifizierung und Verschlüsselung
Daten können auf Basis von Lokationen, Applikationen, Gruppenzugehörigkeiten, Empfängern oder Schlüsselwörtern automatisch klassifiziert und verschlüsselt werden. Beispielsweise ist es auch möglich, Daten beim Hochladen in SharePoint Online automatisch zu klassifizieren und zu verschlüsseln.

Manuelle Klassifizierung und Verschlüsselung
Daten können durch den Benutzer manuell klassifiziert und verschlüsselt werden. Hierfür werden intuitive GUI in den jeweiligen Applikationen bereitgestellt.

Defaults und Machine Learning
Sofern keine automatische oder manuelle Klassifizierung erfolgte, können Daten mit einem Standardwert klassifiziert werden. Alternativ hierzu kann das System auf Basis des bisherigen Verhaltens von Benutzern lernen und die Daten entsprechend klassifizieren.

Document Tracking
Rights Management bietet die Möglichkeit, den Zugriff auf Dokumente nachzuverfolgen und zu jedem Zeitpunkt zu steuern. Abhängig von den zur Verfügung stehenden Informationen kann beispielsweise aufgezeichnet werden, wer wann und wo versucht hat, ein bestimmtes Dokument zu öffnen, zu entschlüsseln oder neu zu klassifizieren.

Fazit
Mit Rights Management von Microsoft können Daten automatisiert und für den Benutzer transparent klassifiziert und verschlüsselt werden. Dies ist eine wesentliche Voraussetzung für die sichere und effiziente Verarbeitung von Daten on-prem oder in der Cloud. ■

René Eberhard

ist CEO von Keyon.

www.keyon.ch