Sichere Daten durch Klassifizierungen

Richtig sortiert

Christoph Hannebauer, Marco Scheel

Wenn wertvolle Informationen aus einem Unternehmen heraussickern, kann das teuer, peinlich oder beides werden. Wer solche Missgeschicke wirksam verhindern will, muss die richtigen Schutzmaßnahmen treffen.

Nicht alle in einem Unternehmen oder einer Behörde gesammelten Informationen sind gleich wichtig und gleich wertvoll. Einige benötigen starken Schutz, für andere reichen lockere Maßnahmen. Voraussetzung für die ungleiche Behandlung: Es muss klar sein, welche Daten in welche Kategorie gehören.

Klarheit erreicht man durch Klassifizierung. Sie kann organisatorischer Natur sein, beispielsweise könnte man Textdokumente in der Fußzeile als „öffentlich", „vertraulich" oder „streng vertraulich" kennzeichnen. Es gibt Software, die solche Informationen in die Metadaten verschiedener Dateitypen schreibt, um das Auswerten und Einhalten von Regeln zu automatisieren. Ein Beispiel ist Azure Information Protection (AIP), das Office-Dokumente, PDFs und andere Dateien klassifiziert und geeignete Schutzmaßnahmen umsetzt.

Informationssicherheit definiert die drei Ziele Verfügbarkeit, Integrität und Vertraulichkeit. Ihre Wichtigkeit kann stark schwanken. Beispielsweise könnte die Verfügbarkeit eines Schichtplans sehr wichtig sein, weil sonst die Mitarbeiter nicht erscheinen und der Betrieb stillsteht, der Schichtplan ist hingegen nicht sonderlich vertraulich. Hohe Integrität ist vielleicht weniger relevant, Hauptsache, die Arbeiter sind zur Stelle. Und an das gut gehütete Rezept einer koffeinhaltigen Limonade muss man nur heran, wenn etwa Produktionsmaschinen neu eingestellt werden müssen. Dann kommt es womöglich auf ein paar Tage nicht an.

Daten lassen sich in mehreren unabhängigen Dimensionen klassifizieren, zum Beispiel nach jedem der drei genannten Ziele. Dieser Artikel befasst sich mit der Vertraulichkeit, einige Prinzipien gelten jedoch auch für die anderen Schutzziele.

Vertraulichkeit ist ein hohes Gut

Es gibt interne und externe Gründe, Vertraulichkeit herzustellen. Unternehmen haben zum Beispiel ein starkes Interesse daran, ihr geistiges Eigentum zu schützen. Vor allem will man verhindern, dass der Konkurrenz wertvolle Daten etwa über Prototypen, Patentanträge und Produktionsabläufe in die Hände fallen. Das gilt auch für Geschäftsstrategien, Preisgestaltungen, Fusionspläne und Zukäufe. Falls solche Informationen oder Daten über Kunden und Angestellte unbeabsichtigt an falscher Stelle auftauchen, bleibt meist ein ramponiertes Image.

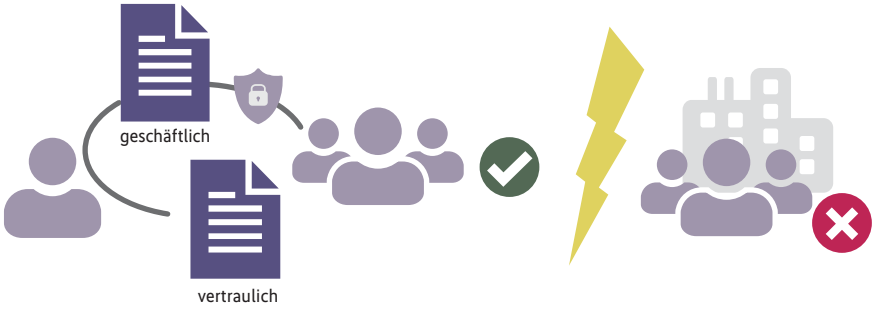
Bei den fremdbestimmten Gründen geht es um das Einhalten von Gesetzen, Verordnungen und Zertifizierungsrichtlinien. Besonders zu erwähnen ist hier die DSGVO, an die sich jeder halten muss, der personenbezogene Daten verarbeitet. Um diese wirksam schützen zu können, muss man sie zwecks Sonderbehandlung zunächst herausfiltern. Anderes Beispiel: Aktiengesellschaften sind gesetzlich verpflichtet, ihre Umsatzzahlen bis zum offiziellen Veröffentlichungstermin geheim zu halten.

Bei einem unbeabsichtigten Datenabfluss oder einer ungeplanten Veröffentlichung haben in der Regel entweder Mitarbeiter Fehler gemacht oder böswillige Akteure die Daten entwendet. Einige Schutzinstrumente verhindern Irrtümer, andere helfen gegen aktive Angriffe, manche auch gegen beides.

Eine wirkungsvolle Maßnahme wäre, die Mitarbeiter darüber aufzuklären, wie vertrauliche Daten zu behandeln sind. Beispielsweise sollten alle Beteiligten in der Lage sein, Phishing-Mails zu erkennen, und wissen, an wen sie welche Dokumente weitergeben dürfen.

Zudem ist es ratsam, Wichtiges auf einer oder mehreren Ebenen zu verschlüsseln, sowohl beim Speichern als auch beim Transport. Geht ein Gerät verloren, kann sich eine Festplattenverschlüsselung als nützlich erweisen. Dateien lassen sich via PGP oder AIP verschlüsseln und Datenbanken kann man so ebenfalls vor unberechtigten Zugriffen schützen.

Der Erfolg dieser Maßnahmen hängt wesentlich davon ab, wer Zugriff auf die Entsperrmechanismen hat. Auch ein Berechtigungssystem, etwa auf einem Fileserver oder im Cloud-Speicher, kann unberechtigten Umgang mit Daten verhindern. Hierbei gilt, dass es so wenige Berechtigte wie möglich und so viele wie nötig geben sollte. Eine exakte und feingranulare Berechtigungsstruktur ist jedoch praktisch kaum umsetzbar, weil oft nur der Zugreifende selbst entscheiden kann, welche Daten er für sein aktuelles Anliegen benötigt. Daher erhalten neben Einzelpersonen oft ganze Teams, Abteilungen oder die gesamte Organisation Freigaben.



Das Dateisystem bestimmt, wer auf Dokumente zugreifen darf. Bei fehlerhafter Rechtevergabe verhindert eine zusätzliche Verschlüsselung das Datenleck (Abb. 1).

Mit Netz und doppeltem Boden

Bei dateibasierter Verschlüsselung und zusätzlicher Zugriffssteuerung entstehen zwei Berechtigungsebenen. Vergibt man in beiden Fällen gleiche Rechte, erhöht sich der administrative Aufwand. Stattdessen empfiehlt es sich, den Zugriff präzise zu regeln und die Verschlüsselung als Sicherheitsnetz auf Unternehmensebene mit wesentlich großzügigeren Berechtigungen zu verwenden. Mit AIP zum Beispiel lassen sich Dokumente so verschlüsseln, dass alle internen Mitarbeiter sie dennoch lesen können. Datei- und Verzeichnisberechtigungen legen den Kreis berechtigter Personen fest. Die Verschlüsselung stört dann bei der Arbeit nicht; sie verhindert aber, dass Externe Dateiinhalte anschauen können, die ihnen zufällig in die Hände fallen (Abbildung 1).

AIP kann mit seinem Rights Management Service (RMS) näher bestimmen, was ein Bearbeiter mit einem Dokument anstellen darf, etwa nur drucken. Oder eine E-Mail zwar lesen, aber nicht weiterleiten.

Das Protokollieren der Tätigkeiten der Nutzer hilft nicht nur beim Aufklären von Datenabflüssen, sondern wirkt zusätzlich präventiv. Anhand der Protokolle lässt sich ein etwaiges Leck erkennen und beheben, bevor ein Schaden entsteht. Beispielsweise ist ersichtlich, wenn vertrauliche Dokumente an einem unsicheren Speicherort landen. Schon der Hinweis, dass mitgeschnitten wird, dürfte einen bewussteren Umgang mit vertraulichen Daten befördern.

Systeme zur Data Leakage Prevention stellen weitere an die Umgebung angepasste Sicherheitsmaßnahmen für vertrauliche Daten bereit. So bietet Microsoft unter dem Namen Data Loss Prevention einen Schutz vor ungewollten Datenabflüssen für Exchange Online und SharePoint Online. Es ist damit nicht mehr möglich, als vertraulich erkannte Dokumente über einen SharePoint-Link oder in einer E-Mail an Externe weiterzugeben.

Zuletzt bestimmt auch der physische Speicherort darüber, wer unberechtigt Zugriff auf Daten erlangen könnte. Zu unterscheiden sind hier Server und Services zur Datenspeicherung sowie alle anderen Arten von Ablagegerätschaften.

Ob man bestimmte Daten nur auf internen Servern verwalten möchte oder ob externe Dienstleister, insbesondere Cloud-Betreiber, infrage kommen, hängt vom Vertrauen in Letztere ab. Sie können meist ein höheres Sicherheitsniveau garantieren als das Unternehmen selbst. Allerdings unterliegen Cloud-Anbieter in den USA den dortigen Bestimmungen. Gegen übergriffige US-Regierungen gibt es im Zweifel keinen wirksamen Schutz.

Wenn Tablets, Mobiltelefone, USB-Sticks und andere Geräte dem Unternehmen gehören, hat es die sicherheitsrelevanten Einstellungen unter seiner Kontrolle. Das gilt jedoch nicht mehr, wenn auch externe Beteiligte Daten auf diesen Geräten ablegen oder private Devices zugelassen sind. Ihr Einsatz lässt sich jedoch organisatorisch und technisch einschränken und die Organisation kann Verschlüsselung erzwingen. Beispiele wären BitLocker To Go für USB-Sticks und Speicherkarten, Mobile Device Management für Mobilgeräte, Mobile Application Management für BYOD (Bring Your Own Device) und Downloadbeschränkungen über Systeme wie Azure AD Conditional Access.

Viel hilft nicht immer viel

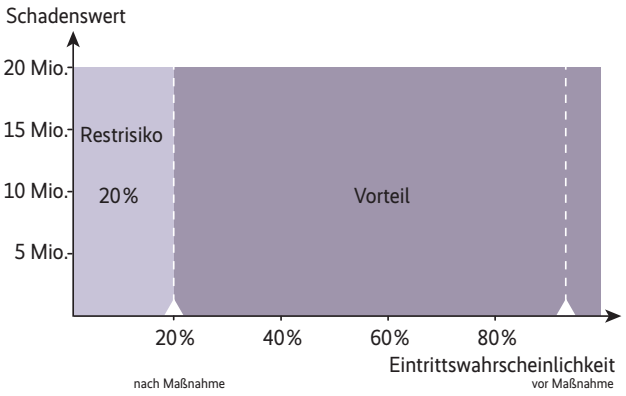
Solche Schutzmaßnahmen haben ihren Preis: Das Einrichten und der Betrieb kosten Zeit und Geld und sie können die Systembedienung beeinträchtigen. Diese Nachteile lassen sich finanziell bewerten, mangelnde Bedienerfreundlichkeit kann sogar ein Grund dafür sein, dass die Anwender bestimmte Programme boykottieren. Daher ist es selten sinnvoll, die gesamte Bandbreite der Schutzmaßnahmen auszuschöpfen. Um hier nicht für jedes einzelne Dokument abwägen zu müssen, sollte man sie nach ihrem Schutzbedarf kategorisieren.

Gelangen vertrauliche Daten in die falschen Hände, richtet sich der entstandene Schaden nach der Art des Dokuments – vielleicht verliert man einen technischen Vorsprung, kassiert eine Vertragsstrafe oder die Außendarstellung leidet. Schutzmaßnahmen senken die Eintrittswahrscheinlichkeit eines solchen Ereignisses. Die Wahrscheinlichkeitsdifferenz mal dem potenziellen Verlust steht als positiver Effekt den Kosten der Schutzmaßnahmen entgegen (Abbildung 2).

Wertvolle Dokumente rechtfertigen daher aufwendige Schutzmaßnahmen. Es ist naheliegend, Dokumente nach dem (maximalen) Schadenswert zu klassifizieren, beispielsweise so:
– niedrig – bis 10 000 Euro
– mittel – bis 5 Mio. Euro
– hoch – ab 5 Mio. Euro

iX-TRACT

- Zahlreiche Schutzmaßnahmen sind geeignet, einen Informationsabfluss aus dem Unternehmen zu verhindern.
- Alle Schutzmaßnahmen müssen sich nach der Wichtigkeit und dem Wert der zu schützenden Daten richten.
- Um zu erkennen, welche Daten wichtig sind, sollten die Verantwortlichen Dateien, Dienste und Datenablagen nach Vertraulichkeit klassifizieren.



Wenn Dokumente einen hohen Schadenswert besitzen, sollte das Unternehmen bei den Schutzmaßnahmen nicht knausern (Abb. 2).

Die Verantwortlichen müssen nun für jede Dokumentenklasse die Vorkehrungen treffen, die zum erwarteten Schaden passen. Allerdings ist die Schadenshöhe oft schwer zu beziffern, etwa wenn es um einen Imageverlust geht. Hinzu kommt, dass die Autoren eines Dokuments es auch klassifizieren sollten, weil sie den Inhalt gut kennen. Sie wissen aber nicht unbedingt am besten, welchen Schaden Datenlecks anrichten können.

In die richtigen Töpfe sortieren

Wenn sich der Schadenswert eines Dokuments schwierig bestimmen lässt, bietet sich ein indirektes Klassifizierungsschema an. Dabei legt eine zentrale Stelle Regeln fest, zum Beispiel:

Geschäftlich: alle Daten, die nicht in eine andere Klassifizierung fallen.

Vertraulich: personenbezogene und Kreditkartendaten.

Streng vertraulich: Pläne zu Fusionen und Zukäufen, Prototypen und Patente.

Solche Einordnungen bieten nur eine Annäherung an die Klassifizierung nach Schadenswert. Fehleinschätzungen gibt es gelegentlich in beide Richtungen. Im obigen Beispiel wäre ein Dokument mit einer Kreditkartennummer ebenso vertraulich wie eines mit Tausenden. Ein bestimmter Prototyp entsteht vielleicht offen in Kooperation mit einer Universität und ist somit nicht vertraulich. Klare Regeln haben jedoch den Vorteil, dass Autoren sie einfacher anwenden können, als sich mit der Klassifizierung nach Schadenswert herumzuschlagen. In manchen Unternehmen bekommen die Nutzer ein Werkzeug zur Verfügung gestellt, das nach einigen Fragen zum Inhalt das Dokument richtig einordnet.

Eine Organisation muss nun festlegen, welche Klassifikation welche Schutzmaßnahmen erfordert. Das Zuordnen kann je nach Maßnahme organisatorisch erfolgen oder technisch erzwungen werden. Ein Beispiel für eine Zuordnung:

Geschäftlich/niedrig: Protokollierung der Zugriffe, Berechtigungen auf Gruppenebene.

Vertraulich/mittel: Verschlüsselung, Zugriff nur mit Authentifizierung.

Streng vertraulich/hoch: Zugriff erfolgt nur von einzeln benannten Personen (Need-to-know-Prinzip), Zugriff durch Externe nur mit unterzeichneter Vertraulichkeitserklärung (NDA) und Ablage der Daten zwingend in Europa.

Die zu klassifizierenden Daten liegen natürlich nicht nur im Dateisystem, sondern auch in E-Mails oder Chats. Das Vertrauen in die beteiligten Systeme lässt sich erhöhen, indem man jedes für eine bestimmte Klassifizierungsstufe freigibt. Spezielle Dateiserver können sicherstellen, dass nur ein kleiner Benutzerkreis sensible Daten einsehen darf. In manchen Organisationen gibt es etwa gesonderte Speicherorte nur für den Vorstand.

Außenstehende in den Prozess einbinden

In vielen Projekten arbeiten externe Beteiligte mit unterschiedlichen Vertrauensverhältnissen mit. Der Angestellte muss wissen, in welchen Bereichen er unterwegs ist und wen er hier möglicherweise antrifft. Nur dann kann er gegebenenfalls notwendige Schutzmaßnahmen selbstständig einleiten. Zur Veranschaulichung ein Beispiel einer möglichen Klassifizierung von Systemen und Ablagen:

Offen: Eine externe Beteiligung ist zu erwarten und die Berechtigungen können weitreichend sein (authentifizierte Benutzer).

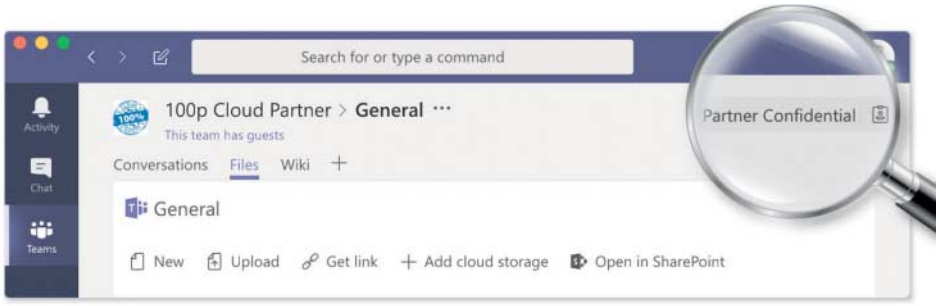
Geschäftsdaten: Hier ist die alltägliche geschäftliche, externe Beteiligung möglich, aber nicht für alle Daten, besonders sensible Informationen müssen gesondert geschützt werden. Spätestens alle zwölf Monate wird die Berechtigung geprüft.

Partnervertraulich: Der Austausch mit befreundeten Unternehmen ist möglich, mit Kunden jedoch nicht. Die Review der Berechtigung erfolgt spätestens alle drei Monate.

Kundenvertraulich: Der Austausch mit einzelnen Kunden ist erlaubt, der Zugriff für Partner nicht gestattet. Spätestens alle drei Monate findet eine Berechtigungsprüfung statt.

Streng vertraulich: Die Ablage enthält sensible Daten und der Zugang für externe Benutzer ist technisch gesperrt. Eine Review der Berechtigung erfolgt spätestens alle 30 Tage.

In Microsoft Office 365 beispielsweise kann man organisationsweit einstellen, dass alle Gruppen klassifiziert werden müssen. Einige der genannten Schutzmaßnahmen lassen sich technisch umsetzen, andere organisatorisch (Abbildung 3). (jd@ix.de)



Anwender können an der Klassifizierung erkennen, welche Teams externe Beteiligte zulassen (Abb. 3).

Dr. Christoph Hannebauer

ist Senior Consultant bei Glück & Kanja und beschäftigt sich mit Sicherheitsthemen in der Microsoft-Cloud.

Marco Scheel

ist Lead Cloud Architekt bei Glück & Kanja und beschäftigt sich mit Modern Collaboration im Umfeld von Microsoft 365.