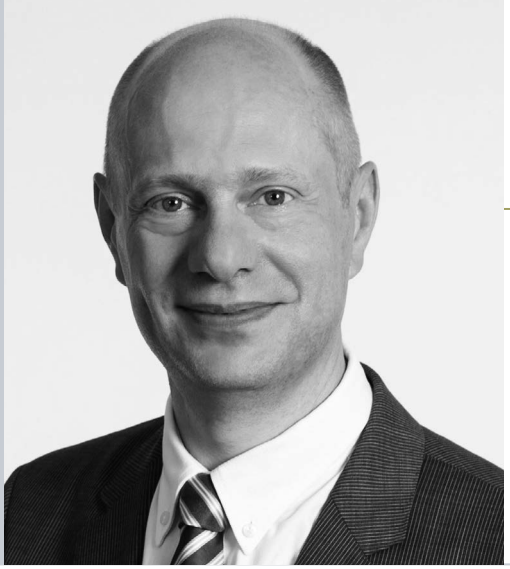
Tom Pasternak
Berater, Cassini Consulting



→ Information Rights Management – zentralisierter Schutz der Information

Stacheldraht, hohe Mauern und schmale Tore – so schützen wir heute.
Die Notwendigkeit des Schutzes von Informationen ist allen, die Bezug zu Konzeption und zum Betrieb von IT haben, vertraut aus der Informationssicherheit, dem Geheimschutz und dem Datenschutz. Im Wesentlichen werden schützenswerte Informationen, neben organisatorischen und prozessualen Regeln, hinter ausgefeilter Firewall- und Filter-Technik versteckt, durch komplexe Verschlüsselungsverfahren geschützt und übertragen oder in elektronischen Verwahrgelassen abgelegt. Schutzmaßnahmen dieser Art wurden in den letzten Jahren immer umfassender und komplexer. Eine Separierung des Datenverkehrs in physikalisch getrennte Zonen und der Transport in unzähligen dedizierten Kryptotunneln erfordern hohe Investitionen für Konzeption und Realisierung. Der Betrieb dieser Festungen ist aufwändig und kostenintensiv. Aus bandbreiten und dynamischen Netzwerken oder flexiblen Wegeführungen werden schmale und starre Ports.

Schützt dieses Vorgehen die Information wirklich?
Dieses dedizierte und ausgefeilte Vorgehen bietet einen technologisch hochwertigen Schutz. Denken wir. Ein Blick auf die der Presse zugespielten Informationen, auf die unter Wikileaks veröffentlichten Dokumente oder auf das Wissen von Plagiatoren und Patentdieben spricht eine andere Sprache.

Einmal gewollt per E-Mail aus dem Hause geleitet, aus Versehen an falsche Empfänger verteilt oder auf einen USB-Stick kopiert, sind die schützenswerten Daten zugängig für beliebige Empfänger: Sie können gelesen, veröffentlicht, kopiert, weitergeleitet oder verfälscht werden. Informationen, die aus Versehen oder grob fahrlässig in offene Netze, beispielsweise das Internet, gelangen, gelten mit einem derartigen Vorfall als öffentlich. Lange Zeit war es nicht vorstellbar, dass es zur gezielten Informationsbeschaffung möglich ist, den nahezu unbeschränkten Datenfluss des Internets zu filtern. Big-Data-Analysemethoden und Veröffentlichungen über geheimdienstliches Vorgehen in diesem Kontext haben uns eines Besseren belehrt.

Verknüpfung der Information mit ihrem Schutzbedarf!
Abhilfe in einem ersten Schritt schafft die Verschlüsselung der Information durch Anwendungen (beispielsweise Microsoft Office, Adobe, E-Mail) oder bei Ablage der Datei. Was mit diesem Ansatz geschützt wird, ist jedoch vornehmlich die lokale Ablage oder die Übertragung. Häufig liegen die Informationen auf gemeinsamen Dateiablagen entschlüsselt oder werden intern ohne Schutz weitergeleitet. Viele Verschlüsselungsansätze sind zudem proprietär, stehen also nicht übergreifend, sondern nur einer jeweiligen Anwendung, einem Produkt oder in Bezug auf einen Hersteller zur Verfügung.

Durch eine einzuführende Verknüpfung der Information mit ihrem Schutzbedarf lassen sich eine Vielzahl, aber auch sehr detaillierte Steuer- und Schutzmechanismen für diese Information etablieren: Die umfassende Implementierung und die damit verbundene Rechteverwaltung wird als **„Information Rights Management“** bezeichnet (IRM).

Mit IRM werden alle Informationen, für die ein Schutzbedarf bezüglich ihrer Vertraulichkeit besteht, den Richtlinien einer starken Kryptierung entsprechend verschlüsselt. Eine sicherheitsbezogene Einstufung wird mit der Erstellung des Dokuments festgelegt, kann aber später durch Personen mit entsprechenden Rechten auch geändert werden. Gleichzeitig wird bei der Dokumentenerstellung aus dem Schutzbedarf der Information abgeleitet und verknüpft, wer später mit dem Dokument welche Aktionen durchführen darf: beispielsweise öffnen, bearbeiten, weiterleiten, kopieren, löschen, Screenshots anfertigen oder drucken. Zusätzlich lässt sich festlegen, wo (beispielsweise auf welchen Geräten, in welchen Netzsegmenten, in welchen Gebäuden oder Liegenschaften) diese Aktionen jeweils erlaubt sind.

Wie wird der verknüpfte Schutz umgesetzt?
Diese Rechtezuordnung verlangt sowohl ein ausgefeiltes und stets aktuell gepflegtes Identitätenmanagement (IAM) als auch eine damit eng verbundene, zertifikatsbasierte PKI. Über das IAM wird dem IRM übermittelt, wer (beispielsweise Zwei-Faktor-Authentisiert) an welchem Gerät (Identifikation über TPM) gerade eine Aktion am Dokument durchführen will und ob diese Aktion innerhalb eines Schutzbereiches (beispielsweise Kontroll- oder Sperrzone), innerhalb eines Hauses oder innerhalb einer Organisation (zugewiesene IP-Adresse, port security) stattfindet. Nach erfolgreicher Feststellung der Identitäten (Person, System, Ort) prüft das zentrale IRM gegen die mit dem Dokument verknüpften Rechte für Aktionen. Anhand der Identitäten und der Zertifikate erfolgt dann unter Zuhilfenahme der PKI die notwendige Ent- oder Verschlüsselung. Weitere Funktionen wie das Drucken, Weiterleiten oder Kopieren der Datei oder enthaltener Informationen werden je nach Schutzbedarf und Freigabe erlaubt. Diese Steuerung erfolgt auf dem System des Endanwenders über das Betriebssystem oder anhand einer dort einzuführenden IRM-Middleware.

IRM ermöglicht es, Dokumente und Informationen umfassend und nachhaltig während des gesamten Dokumentenlebenszyklus zu schützen. Bezüglich des Aspektes Vertraulichkeit sind Zielgenauigkeit und Effektivität eines IRM unerreichbar. Hinzu kommt, dass die anfangs erwähnten hohen Aufwände für hardwarebasierte Kryptierung und Zonierung erheblich reduziert werden können. Die Verschiebung eines Großteils der Schutzmaßnahmen vom Transportweg in die zentralen und dezentralen Systeme, macht das IRM als zusätzliche und von etablierten, netzbezogenen Schutzansätzen unabhängige Maßnahme interessant.

Derzeit bieten unter anderem die großen Hersteller Microsoft, Oracle und Adobe für ihre Dokumente und Daten jeweils proprietäre IRM-Lösungen an. Zusätzlich etablieren sich Firmen, die bereits Fachspezialisten im Markt der Sicherheitslösungen sind, mit organisationsbezogenen Implementierungsangeboten, die diese proprietären Ansätze mit etablierter IAM und PKI zusammenführen und somit anwendungsübergreifende IRM-Systeme erschaffen.

Denn genau hier liegt – wie so oft – die Herausforderung: Technologische Lösungen existieren am Markt, es fehlt an durchgängig einsetzbaren IAM-Lösungen sowie der kritischen Masse zur Etablierung der Mehrwerte von organisationsübergreifenden PKI-Infrastrukturen.

Jetzt: Implementierung im Rahmen der IT-Konsolidierung des Bundes
Nach Einschätzung der Cassini Consulting bietet sich dem Bund jetzt mit dem Vorhaben IT-Konsolidierung die einmalige Möglichkeit, Rahmenbedingungen zu schaffen: Ein übergreifendes Bundes-IAM soll im Rahmen der Dienstkonsolidierung bereitgestellt werden, ebenso eine PKI. Abgestimmte Vorgaben, zentrale Verwaltung und einheitliche Implementierung von Identitäten, die Möglichkeit, für Behörden einen in den für IRM erforderlichen Punkten vereinheitlichten Bundesclient aufzusetzen oder auch das Zusammenspiel der Basis- und Querschnittsdienste mit den Funktionen des IAM und der PKI für alle Behörden und Nutzer konsolidiert einzusetzen, sind wesentliche Grundpfeiler des IRM. Die Einführung einer IRM-Lösung liegt also auf der Hand.

Cassini Consulting empfiehlt, gemeinsam mit Herstellern und Fachexperten ein strategisches Ziel zu definieren, aber ebenso parallel zu evaluieren, welche Möglichkeiten sich bereits heute bieten, um kurzfristig eine IRM-basierte Schutzebene für besonders schützenswerte oder abgrenzbare Informationsverbünde (Fokus auf ausgewählte Dateitypen, Beschränkung auf festzulegende Anwendungen, Implementierung innerhalb einer Behörde oder für ein Verfahren) zu etablieren. Für eine zielgerichtete weitere Bearbeitung des Themas und eine erfolgreiche Bündelung von Nachfrage, Lieferbarkeit und Fachwissen bietet sich das Etablieren des Fachthemas IRM in einer Arbeitsgruppe des bitkom e.V. an.

Langfristig: IRM ist ein Schlüssel für eine sichere und wirtschaftliche Konsolidierung
Darüber hinaus wird IRM auch ein Schlüssel dafür sein, eine Konsolidierung im Hinblick auf Beibehaltung des durch Trennung und Separierung in Behörden-IT gewohnten Sicherheitsniveaus überhaupt durchführen zu können. Konsolidierung heißt auch zentralisieren und zusammenführen, beispielsweise durch das Aufsetzen einer E-Akte-Lösung für den gesamten Bund oder durch Virtualisierung von Dateiserverdiensten in einer Cloud. Dem Zusammenlegen von Informationen, die nur noch durch virtuelle Umgebungen getrennt werden, setzt ein IRM einen wirksamen Schutz entgegen: Alle Informationen liegen zwar gemeinsam in einem entsprechend gesicherten und geschützten zentralen System vor. Wer jedoch darauf in welcher Art und Weise zugreifen kann, sich Informationen anzeigen und zur Bearbeitung übermitteln lassen kann, könnte ein IRM, gekoppelt mit Sicherheitselementen regeln.

Aus der Sicht der Cassini Consulting ist ein IRM ein ganz wesentlicher Lösungsansatz zur Aufrechterhaltung der Sicherheit bei gleichzeitiger Konsolidierung, die die effiziente Nutzung zentraler, übergreifender und virtualisierter IT-Ressourcen zur Grundlage hat.

Cassini Consulting
Niederlassung Berlin
Oberwallstraße 24
10117 Berlin

E-Mail: *tom.pasternak@cassini.de*
Internet: *www.cassini.de*