

DIGITALE HOCHSICHERHEITSTRAKTE – ABER BITTE FLEXIBEL!

VON JÜRGEN HÖFLING | juergen.hoefling@informationweek.de

Unternehmen wollen digitale Dokumente mit vertraulichen Inhalten sicher austauschen können. Gleichzeitig will man einen flexiblen Zugriff aller Berechtigten sicherstellen. Als sei das nicht Komplexität genug, kommen letztere oft auch noch von außerhalb.

Ganz gleich, ob es sich um Vertragstexte, Vorstandsunterlagen oder Projekt- und Patentdateien handelt: vertrauliche Dokumente dieses Kalibers wecken grundsätzlich die Neugier Unbefugter und müssen vor solchen Unbefugten geschützt werden. Im digitalen Zeitalter sind natürlich entsprechende digitale Sicherheitsvorkehrungen das Mittel der Wahl.

Identitätsmanagement-Systeme sind in diesem Kontext notwendig, aber nicht hinreichend. Vielmehr müssen festgelegte Rollen und Rechte innerhalb des Identitätsmanagement-Systems mit genauen Rechteaussagen (»Attributen«) verknüpft werden. Konkret bedeutet das,

dass festgelegt wird, wer was wann mit einem Dokument machen darf (zum Beispiel Anschauen, Kopieren, Weitergeben, Ausdrucken, Speichern). »Entsprechende Attribute sollten dabei so spät wie möglich vergeben werden, da die Vertrauenswürdigkeit bestimmter Personen durchaus sehr schnell wechseln kann«, sagt dazu Markus Seyfried, Technikchef beim Münchner Dokumentensicherheits-Spezialisten Brainloop. Seyfried bringt als Beispiel einen Bieter innerhalb eines Fusionsverfahrens, der gleichzeitig Mitbewerber ist und dem sofort alle oder viele Rechte innerhalb einer Bücherprüfung entzogen werden müssten, sobald ein anderer Bieter den Zuschlag bekommen hat.

UNSICHERES INTRANET

Der »Secure Dataroom« von Brainloop hat speziell in Umgebungen, wo Externe und Interne vertraulich zusammenarbeiten müssen, besondere Vorteile. Die Notwendigkeit zur Einbeziehung Externer ist viel häufiger der Fall, als allgemein angenommen wird. So ist zum Beispiel auch der Aufsichtsrat eines



Foto: Cirosec

STEFAN STROBEL

»Die größten Hemmnisse beim dokumentenbasierten Rechtemanagement-Ansatz bilden die nur schwer erfüllbaren Kompatibilitätsanforderungen zwischen Kommunikationspartnern.«

STEFAN STROBEL, Geschäftsführer von Cirosec

Unternehmens von der Funktion her ein externes Organ, nicht zu reden von beratenden Anwaltskanzleien. Seyfried schildert den Fall eines Brainloop-Kunden, der lange intern diskutiert habe, ob man den »sicheren Datenraum« ins unternehmenseigene Intranet einfügt oder extern platziert und der sich letztlich für die externe Lösung entschieden hat, weil im Intranet »zu viele interne potenzielle Angriffspunkte existierten«.

Brainloop ist sozusagen der Königsweg zur sicheren Dokumentenverwahrung, über den einfachere Verfahren eingebunden und infrastrukturell unterfüttert werden. Da die Münchner unter anderem das »Rights Management System« von Microsoft integrieren, lässt sich im »Secure Dataroom« die Attributvergabe nachspielen, die Microsoft in seine Mail- und Office-

»Die Rechte-Attribute sollten erst vergeben werden, wenn ein vertrauliches Dokument auf den Client geladen wird.«

MARKUS SEYFRIED, Technikchef von Brainloop Software



Foto: Brainloop Software

MARKUS SEYFRIED

Dokumente integriert hat. Durch die Einbindung in den »Sicheren Datenraum« ist der Nutzer vieler Ärgernisse enthoben, die die »nackte Nutzung« des Rechtemanagements von Microsoft mit sich bringt. Denn um letzteres einsetzen zu können, bedarf es mindestens eines Windows-2003- und eines SQL-Servers sowie einer speziellen Zugangslizenz für alle Clients, die in

sehen aber beliebig viele Sicherheits- und Verwaltungsprobleme auf, sodass die Unternehmen am Ende dann wiederum bei Lösungen landen dürften, die der von Brainloop zumindest ähnlich sind. Darüber hinaus sind Rechtemanagement-Systeme wie die von Microsoft oder Adobe natürlich an bestimmte Applikationen (PDA, MS Office) gebunden, wobei zumindest bei Adobe auch andere Formate, beispielsweise aus dem CAD-Bereich, in PDF-Dateien »eingewickelt« werden können. »Die größten Hemmnisse beim Rights-Management-Ansatz bilden die nur schwer erfüllbaren Kompatibilitätsanforderungen zwischen den Kommunikationspartnern« gibt Stefan Strobel, Geschäftsführer des Heilbronner Sicherheitsspezialisten Cirosec zu bedenken und weist darüber hinaus auf die vielfältigen Fehlerquellen hin, die sich »dadurch ergeben, dass bei diesem Verfahren die zu schützenden Daten und Dateien selbst verändert werden«.

Datei wird dabei durch deren ursprünglichen Speicherort festgelegt und nicht durch den Inhalt. Um den korrekten Umgang mit Dateien, die als vertraulich eingestuft worden sind, gewährleisten zu können, muss sich das Sicherungssystem tief ins Betriebssystem der verschiedenen Endgeräte einklinken und sämtliche Dateioperationen inklusive der Benutzung der Zwischenablage überwachen.

»Die Überwachung der Operationen ist aber nur die halbe Miete«, meint Stefan Strobel. Schließlich müsse ja reagiert werden, wenn ein Verstoß festgestellt werde. Die genannten Produkte böten hier alle abgestufte Reaktionsmuster, die von Protokollieren und Warnen des Benutzers über das Abfragen einer Begründung bis hin zum Sperren einer bestimmten Operation reichen.

Mit Systemen wie dem von Verdasys lassen sich im Vergleich zu den dokumentenorientierten Rechtemanagement-Systemen beliebige Dateiformate schützen, dafür sei aber auch »ein erheblicher Eingriff in die Unternehmensabläufe notwendig«, sagt Peter Körner, Technischer Manager bei Adobe in Deutschland. Dagegen könne der Rechteserver von Adobe »weitgehend automatisch in das Unternehmensnetz eingehängt werden«.

DIE MÜHEN DER VERWALTUNG

Letztlich sind weder die agentenorientierte Verdasys-Lösung noch die dokumentenbasierten Lösungen für Umgebungen geeignet, bei denen externe Protagonisten eingebunden werden müssen. Ob die beiden Lösungen für unternehmensinterne Lösungen taugen, hängt nicht zuletzt davon ab, wie weit ein Unternehmen seinen eigenen Mitarbeitern in toto vertrauen kann. Letztlich dürften Sicherheitserwägungen fast immer dazu führen, dass der Policy Server in eine geeignete spezielle Infrastruktur eingebettet wird, womit man wieder bei einer »Secure Dataroom«-Lösung angelangt wäre. Wie oft in der IT wirken die technischen Verfahren im Einzelfall äußerst pfiffig, werden aber in der Verwaltung sehr mühselig, wenn man sie in der Fläche anwenden will. ■

»Mit Systemen wie dem von Verdasys ist ein erheblicher Eingriff in die Unternehmensabläufe notwendig.«

PETER KÖRNER, Technischer Manager bei Adobe



Foto: Adobe

PETER KÖRNER

das System eingebunden werden sollen. Darüber hinaus prüft der Rechteserver von Microsoft nur einmal die jeweiligen Rechte, zeitnahe Anpassungen an sich ständig ändernde Rechte sind daher nicht oder nur sehr umständlich möglich.

KOMPATIBILITÄTSPROBLEME

Ein ähnliches Konzept verfolgt Adobe mit seinem »Policy Server«. Der Verfasser eines Dokuments kann bei der Erstellung selbst entscheiden, welche Rechte-Attribute er anderen Bearbeitern geben will. Adobe bietet dabei unterschiedliche Sicherheitsstufen, die vom reinen Passwortschutz über Zertifikate bis hin zu einer ständigen Rechteüberwachung (»LifeCycle Policy Server«) reichen. Zumindest mit der letztgenannten Version hat man die Möglichkeit, die Rechte auf ein Dokument jederzeit zu ändern. Für den Empfänger der Datei bedeutet das allerdings, dass er sich vor der Benutzung des Dokuments mit dem Policy Server verbinden muss. Dieser sollte deshalb außerhalb der Firewall-Grenzen des jeweiligen Unternehmens stehen. Das dürfte für sicherheitsbewusste Unternehmen kaum akzeptabel sein. De facto sind deshalb Lösungen wie die von Adobe und Microsoft auf den ersten Blick sehr interessant, werfen bei genauerem Hin-

AGENTENBASIERTE SENSOREN

Strobel hält Verfahren, die Sicherheitsmechanismen am Datei- oder Verzeichnisbaum des Betriebssystems festmachen, in vielen Fällen für besser geeignet, die Vertraulichkeit von Daten zu schützen. Er verweist auf Firmen wie Verdasys, Fidelis, Code Green Networks, Vontu und Vericept, die den Datenfluss im Netzwerk eines Unternehmens regelmäßig überwachen. Leider seien fast alle diese Systeme – einzige Ausnahme ist Verdasys – netzorientiert, bedauert Strobel. Da die netzorientierten Systeme nur wenige Sensoren an zentralen Stellen im Netz installierten, seien sie zwar einfach auszubringen, aber in ihrer Wirkung auch arg begrenzt. Sie könnten natürlich nur Datenabflüsse entdecken, die über das Netz gingen. Strobel plädiert deshalb für agentenbasierte Systeme wie das von Verdasys, bei denen freilich auf jedem involvierten Endgerät eine entsprechende Software aufgespielt und gepflegt werden müsse. Die Schutzklasse einer