

Leckage-Sensoren mit Nebenwirkungen

von [Jürgen Höfling](#)

Daten sind das wertvollste Gut eines Unternehmens. Diese Daten müssen optimal für die Mitarbeiter bereitstehen und gleichzeitig vor Missbrauch und Fahrlässigkeit durch eben diese Mitarbeiter geschützt werden.



Vertrauliche Daten wie Konstruktions-, Patent- oder Vertragsdokumente sind die Kronjuwelen eines jeden Unternehmens. Eine undichte Stelle in diesem Bereich kann eine Firma unter Umständen ruinieren. Ungemach bringt auch der unkontrollierte Abfluss oder die vorsätzliche Weitergabe von Personendaten. Hier sind die entsprechenden Gesetze in den deutschsprachigen Ländern besonders streng.

Wagenburg-Mentalität Angesichts der weitgehenden Digitalisierung der genannten Daten kommt digitalen Schutzmechanismen immer größere Bedeutung zu. Die meisten Unternehmen haben bei den entsprechenden digitalen Abwehrmechanismen aber immer noch eine Wagenburg-Mentalität: man schottet sich gegen äußere Eindringlinge durch mehrere digitale Wälle solide ab, damit wähnt man die eigenen Daten in Sicherheit. Nichts ist falscher als eine solche Vorstellung. Im Grund weiß das jeder mittelmäßige Spion aus alten und kalten Tagen. Interessante Daten holt man sich nicht mit der Brechstange, die in der digitalen Welt die Form eines trojanischen Pferds haben kann, sondern viel einfacher über »vertrauensbildende Maßnahmen« im Umgang mit Insidern.

A screenshot of a software interface titled 'Semantik-Filter'. It shows a list of files and folders with columns for Name, Date, Size, and other attributes. The interface is in German and appears to be a file management or filtering tool.

Die Kaspersky-Tochter Infowatch untersucht mit Hilfe von linguistischen - Algorithmen Dokumente und Dateien auf ihre Brisanz.

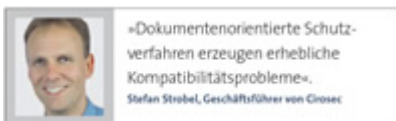
Daten sind zum Arbeiten, nicht zum Wegsperrern Auch wenn alle möglichen Umfragen bei den IT-Verantwortlichen der Firmen das große Gefahrenpotenzial von fahrlässig oder vorsätzlich provozierten Datenlecks belegen: tatsächlich tun die meisten Unternehmen sehr wenig, um Datenverluste zu verhindern. Das liegt nicht zuletzt daran, dass Schutzmaßnahmen technisch aufwändig und entsprechend teuer sind, oder aber, wenn sie preiswerter sind, weitgehenden Plazebo-Charakter



cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

haben. Die grundsätzliche Crux liegt darin, dass die internen, vertraulichen Daten eines Unternehmens ja dazu da sind, benutzt zu werden. Sie sind die Pfunde, mit denen die Firma wuchern muss. Und es sind natürlich die eigenen Mitarbeiter, die mit diesen Daten arbeiten müssen und sollen. Ob und wann ein loyaler Mitarbeiter zu einem Innetäter wird, der die ihm anvertrauten Daten veruntreut oder fahrlässig weitergibt, kann logischerweise auch vom ausgeklügeltsten digitalen Sicherungsprogramm bestenfalls post festum erkannt werden. Insofern müssen alle entsprechenden Programme erst einmal mit einem Vertrauensvorschuss arbeiten und sich darauf konzentrieren, die Lese-, Kopier- und Weitergabevorgänge minutiös aufzuzeichnen: wer hat wann was gemacht? Sperren wird man bestimmte Dokumente nur dann, wenn es offensichtlich ist, dass ein Dokument für einen Mitarbeiter tabu ist.

Kompatibilitätsprobleme Zur Kontrolle bietet sich die Etablierung einer Verbindung von Identitäten und deren Rollen und Rechte mit detaillierten Rechteaussagen («Attributen») an. Dadurch wird festgelegt, wer wann was mit einem Dokument machen darf. Systeme wie das Rechtemanagement von Adobe für PDF-Dateien oder von Microsoft DRM innerhalb von Windows XP und MS Office verändern indes zum einen die Dokumente selbst und erzeugen zum anderen sehr schnell einen immensen Verwaltungsaufwand. Das ist dann umso mehr der Fall, wenn man (wohl zu recht) davon ausgeht, dass die Vertrauenswürdigkeit von Personen ständig (wöchentlich, täglich, minütlich?) neu überprüft werden sollte. Darüber hinaus sind die erwähnten dokumentenorientierten Verfahren nur für bestimmte Dateiformate verfügbar. »Das größte Problem bei solchen Systemen stellt freilich die Kompatibilität dar«, bemerkt Stefan Strobel vom Heilbronner Sicherheitsspezialisten Cirosec. Wie soll man zwischen verschiedenen womöglich sogar externen Kommunikationspartnern die Rechte abprüfen. Als Lösung werden sogenannte Richtlinienserver angeboten. Das klingt gut, wirft aber alle möglichen Probleme in der Praxis auf. Wo wird dieser Richtlinienserver platziert und wer verwaltet ihn? Wer entscheidet, ob Firma X und Person Y Rechte erhalten und wenn, dann bitte welche? Firmen wie Brainloop in München haben für sehr spezielle Anwendungen, bei denen es um große Vermögenswerte geht, einen PKI-gesicherten Richtlinienserver als »sicheren Datenraum« entwickelt, der von einem direkt der Firmenleitung unterstellten Administrator verwaltet wird. Das ist eine sehr gute und sichere, aber auch sehr aufwändige und teure Lösung.



Semantische Analyse bei Kaspersky Für den normalen Firmenalltag wird man wohl Verfahren wählen, die für beliebige Dateiformate verwendbar sind und die weder einen betriebswirtschaftlich kaum darstellbaren Aufwand bei der Rechteverwaltung noch die Kompatibilitätsprobleme von dokumentenzentrierten Systemen erzeugen. De facto machen derartige Systeme wie sie beispielsweise von McAfee, Workshare, Websense, ITwatch, Verdasys, Vontu oder Infowatch angeboten werden entsprechende Sicherheitsmechanismen am Datei- oder Verzeichnisbaum des Betriebssystems fest. Darauf aufbauend wird dann der Datenfluss im Netzwerk eines Unternehmens überwacht. Die Überwachung basiert notwendigerweise auf relativ statischen Einstellungen. Wenn beispielsweise ein Dokument ursprünglich in einem als vertraulich eingestuftem Verzeichnis erstellt worden ist, dann sind

damit nur ganz bestimmte Operationen zulässig. Eine interessante Pointe bringt die Kaspersky-Tochter Infowatch ins Spiel. In die Überwachungsprogramme von Infowatch sind linguistische Algorithmen integriert, welche die semantische Struktur der Inhalte analysieren und klassifizieren.



Effizienz erfordert Aufwand Die Verwendbarkeit dieser Systeme für beliebige Dateiformate hat natürlich einen Preis. Die Arbeitsabläufe müssen an das verwendete System angepasst werden. Und je nachdem, wie ausgeklügelt eine Lösung ist, entsteht Verwaltungsaufwand. Die semantischen Filter von Infowatch sind sicher interessant, aber sie müssen kompetent eingestellt und gewartet werden. Gleiches gilt für die eingesetzte Sensorik. Systeme, die nur mit wenigen Sensoren den Verkehr im Netz abgreifen, sind einfach zu warten, aber sie werden auch nicht allzu viel mitbekommen. Systeme, bei denen eine spezielle Software auf allen Knoten im Netz beziehungsweise auf allen Endgeräten platziert wird, sind natürlich viel effizienter, der Verwaltungsaufwand dafür ist aber nicht unerheblich.

Verstöße dokumentieren Das Fazit ist einfach und schwierig zugleich: Es gibt wirkungsvolle technische Methoden, um Daten und Dokumente vor Innentätern aus dem Intranet und Extranet zu schützen. Alle haben ihren Preis, sowohl finanziell als auch hinsichtlich der Nebenwirkungen auf die Arbeitsabläufe. Auch kann das beste System nur sehr bedingt die Wandlung eines loyalen Mitarbeiters zu einem untreuen Kollaborateur erkennen und entsprechende Sofortmaßnahmen ergreifen. Aber immerhin könnten die besten der Leckage-Sensoren minutiös dokumentieren, wer was wann wo gemacht hat. Und das ist ja immerhin eine ganze Menge, wenn es zum Rechtsstreit kommt oder wenn Rechtfertigungszwang vor dem Gesetzgeber besteht.

Informationweek 08.06.2007