

# Bye-bye, digitales Eigentum?

Wirtschaftskriminalität ist ein boomendes Geschäft.

Einfacher als heute war es ja auch noch nie: In der digitalen Welt fällt kaum auf, wenn ein sensibles Dokument den Besitzer wechselt. Wir unternehmen deshalb einiges zum Schutz des digitalisierten, geistigen Eigentums.

Gemäss den Maschinen- und Anlagenbauern in Deutschland ist der Missbrauch von unternehmensrelevanten Daten ein «dramatisches Problem». Ein Hauptgrund sind die vielen (unzulässigen) Kopien, die von den Dateien jeweils gemacht werden. Es ist ja auch nichts einfacher, als digitale Dokumente zu kopieren und weiterzugeben. Aufwand und Kosten sind gering, der Qualitätsverlust gleich Null. Genau darin liegt aber eine grosse Gefahr für das ureigene Know-how eines Unternehmens.

Bei uns werden alle für einen optimalen Service relevanten Dokumente wie z.B. Technische Anleitungen, Ersatzteil- und Serviceinformationen, Arbeitsinstruktionen, Betriebsanleitungen usw. als digitale Daten über diverse Datenkommunikationsnetzwerke in die entferntesten Regionen der Welt übertragen. Zudem sind sie seit im letzten Jahr servicenetzweit die Digitalen-Service-Assistenten

(D-S-A) eingeführt wurden, auf den mobilen Computern der Servicemitarbeiter auch offline abrufbar. Viele dieser Daten sind heikel oder vertraulich. Wie also können sie vor unbefugten Zugriffen optimal geschützt und ein Missbrauch verhindert werden?

## Prävention ist Pflicht

Der beste Schutz ist dafür zu sorgen, dass ein Datenmissbrauch gar nicht erst passieren kann. Für unsere digitalen Informationen im Serviceumfeld sind solche präventiven Massnahmen gleichbedeutend mit elektronischen Schutzmechanismen, auch bekannt als «Digitales Rechtemanagement» (Digital Rights Management). Mit diesem Verfahren lassen sich die Nutzung und die Verbreitung digitaler Medien kontrollieren und schützen. Wir arbeiten in diesem Zusammenhang mit dem Softwareprodukt «Live Cycle Rights Management» von Adobe. Es kann so einiges:

## 1. Verschlüsselung und Haltbarkeit

Die Dokumente sind verschlüsselt und immer nur wenige Tage lesbar. Nach Ablauf eines definierten Zeitraums werden die Zugriffsrechte ungültig und müssen erneuert werden. Und sollte einmal ein Dokument unerlaubterweise im fremden Besitz ausserhalb der ABB gelangen, sei dies beispielsweise auf Grund einer unerlaubten Weitergabe via E-Mail oder USB-Stick, so kann der Empfänger das Dokument erst nach einer Online-Überprüfung mit Verbindung zu einem ABB-Server lesen. Für Drittfirmen ist dies quasi unmöglich.

## 2. Rigide Nutzungsrechte

Die Dokumente sind auch bei geschütztem Zugriff (online sowie offline) mit zusätzlichen Nutzungsrechten versehen. So ist beispielsweise das direkte Ausdrucken dieser Dokumente nicht möglich, sondern es braucht den Einsatz von «Spezialtools».

## 3. Personalisierung

Digitale Wasserzeichen (Watermarking) personalisieren die Dokumente. Auf jeder Seite des Dokuments wird der Vor- und Nachname des Benutzers, diagonal in Form eines Wasserzeichens dargestellt. Somit ist eine gewisse Abschreckung vorhanden, das Dokument weiterzugeben.

## 4. Protokollierte Kontrolle

Alle Aktivitäten mit geschützten Dokumenten – wann wird wie oft und von wem auf eine Datei zugegriffen und was wurde damit gemacht – können vom Server protokolliert und überprüft werden.

## Nicht 100%, aber immerhin

Mit den elektronischen Schutzmechanismen kann sicher nie eine 100%ige Sicherheit erreicht werden, aber das Risiko der unerlaubten Weitergabe von digitalen Dokumenten kann erheblich minimiert und erschwert werden. Aufgrund der guten Erfahrungen, welche mit dem «Live Cycle Rights Management» im Projekt «D-S-A» (Digital Service Assistance) gemacht wurden, sollen in einem nächsten Schritt nun auch die Dokumente auf dem DOC@WEB-System mit dieser Technologie geschützt werden. Damit das geistige Eigentum der CHTUS auch in Zukunft bei CHTUS bleibt.

