

Link: <https://www.computerwoche.de/a/missbrauch-im-digitalfilm-dokumentieren,1906250>

Überwachung für externe Admins

## Missbrauch im Digitalfilm dokumentieren

Datum: 23.09.2009  
Autor(en): Marcus Wenning

**Nicht nur (Ex-)Mitarbeiter sind ein Risiko für die Unternehmen, auch die externen Administratoren. Systeme, die mittels Videofilm und Schriftprotokoll alle Administratorarbeiten dokumentieren, sollen jetzt Anhilfe schaffen.**



Theoretisch könnten also Unbefugte leicht an sensible Daten gelangen, sie herunterladen oder abändern.

Welche In immer mehr Unternehmen liegt die Verwaltung der Rechenzentren in den Händen externer Administratoren, die von Außen Zugriff auf die Daten haben. Und zwar auf alle Daten im Firmennetz. Meist ist jedoch nicht dokumentiert, warum und wann die Dienstleister auf das System zugegriffen haben. Theoretisch könnten also **Unbefugte leicht an sensible Daten gelangen**<sup>1</sup>, sie herunterladen oder abändern. Auch wenn es eher Ausnahmen unter den Administratoren sind, die ihre weit reichenden Befugnisse für illegale Machenschaften ausnutzen, kann das zum Problem werden - speziell für jene Unternehmen, die mit Bank- und anderen sensiblen Daten zu tun haben. Schon allein aus gesetzlichen Gründen, Stichwort Compliance.

## Zugriffszeit und Name des Dienstleisters registriert

Um schwarze Schafe unter den Administratoren zu finden oder gleich von vornherein entsprechende Vorhaben unterbinden zu können, setzen Anbieter nun auf Kontrolle. Alle Arbeitsschritte in der Systemadministration müssen sich im Nachhinein rekonstruieren lassen. Mit Hilfe der "VideoLog-Technologie" beispielsweise . Die von **ToolBox Solution entwickelte Lösung**<sup>2</sup> erstellt neben einem Schriftprotokoll einen Digitalfilm, um alle Administrator-Handgriffe zu dokumentieren. Auch Zugriffszeit sowie Name des Dienstleisters werden dokumentiert. Mit anderen Worten: Das Videosystem hält lückenlos jeden Administratorzugriff fest und stellt so die vorgeschriebene interne Überwachung sicher.

Gleichzeitig können externe Dienstleister durch die Aufzeichnungen auch ihre erbrachten Leistungen nachweisen. So entsteht Gewissheit auf beiden Seiten: Die **Überwachung**<sup>3</sup> der Mitarbeiter erfolgt, wo es nötig ist und keine Persönlichkeitsrechte verletzt werden. Vergleichbar ist das Vorgehen in etwa mit einem Bezahlvorgang am Geldautomaten oder dem Tanken an der Zapfsäule: Aufgezeichnet werden nur die "Handgriffe", keine schützenswerten Informationen.

Neben dem beschriebenen System benötigt man noch eine **Management-Software**<sup>4</sup>, mit der die Verantwortlichen verbindliche Zugriffsregeln festlegen können. So hat das Unternehmen den nötigen Überblick darüber, welcher (externe oder interne) Mitarbeiter wann auf welche Daten zugreifen kann. Damit ist einerseits **der Datenschutz gewährleistet**<sup>5</sup>, andererseits auch die Arbeitsleistung externer Dienstleister dokumentiert.

## Passwort zwischen internem und externem Mitarbeiter teilen

Gerade im Umgang mit vertraulichen Daten hat sich das Vier-Augen-Prinzip bewährt. So ist es beispielsweise möglich, dass ein interner und ein externer Mitarbeiter je eine Hälfte eines geteilten Passwortes nutzen; erst wenn beide Teile zusammengefügt werden, ist der Zugriff möglich. So lassen sich natürlich auch bei zwei internen Kräften die **Kontrolle und der Schutz erhöhen**<sup>6</sup>.

Alternativ ist es möglich, dass der Firmenmitarbeiter und der externe Dienstleister gemeinsam auf das System zugreifen, wobei Ersterer Letzterem durch die Eingabe des Kennworts "Eintritt" verschafft.

## Links im Artikel:

<sup>1</sup> <https://www.computerwoche.de/virtualdatacenter/sicherheit/1899588/>

<sup>2</sup> <http://www.tbsol.de/>

<sup>3</sup> <https://www.computerwoche.de/subnet/hp-intel/1893589/>

<sup>4</sup> <https://www.computerwoche.de/subnet/hp-intel/1894450/>

<sup>5</sup> <https://www.computerwoche.de/virtualdatacenter/sicherheit/expertenwissen/1869914/>

<sup>6</sup> <https://www.computerwoche.de/newsletter/security/1904227/index3.html>