

<h2>Session Recording mit Filmen und Vier-Augen-Prinzip</h2> <ul style="list-style-type: none">- Methoden zur Prävention- Indizien für die forensische Informationsanalyse	<p>Dipl.-Ing. Tillmann Basien ist Geschäftsführer der Tool Box Solution GmbH, dem weltweit einzigen Anbieter der zentralimplementierten Methode des Session Recordings.</p>
---	---

Der Bedarf an revisionstauglichen Verfahren und Instrumenten zur Kontrolle und Steuerung des Zugangs zu Informationen und Systemen steigt stetig. Das Zusammenwirken von Spezialisten zur Betreuung von IT-Systemen führt zu einem erhöhten Schutzbedarf. Aus diesem Grund ist es zwingend, dass die primären Anforderungen an das Access-Management um die Methoden der Cooperation und des Recordings erweitert werden.

- Aufhebung der Anonymität in kritischen Bereichen in allen Ebenen durch Filmen
- Automatisches Aufzeichnen von Bildschirmdarstellungen (Session Recording mit Filmen)
- Non-invasive und nicht umgehbare Integration
- Vier-Augen-Prinzip auf individuelle Anwendungen
- Keine Client- und Server-Voraussetzungen

Bezeichnen wir Anwender, User, Administratoren und alle, die eine Unternehmens-IT direkt (interne und externe Mitarbeiter) oder indirekt (Kunden am Webshop) nutzen als Individuen, wird spätestens bei der Risikoanalyse festgestellt: Ein Individuum wird, sofern die Security Abteilung korrekt arbeitet, nicht mal versuchen können die Firewallbastion eines Unternehmens zu kompromittieren. Je näher ein Individuum dem IT-Kern ist, desto mehr Rechte, Möglichkeiten und damit Macht hat es. Bzw. ein internes Individuum passiert die Firewall via Authentisierung und VPN und passiert somit auch Intrusion Detection Systeme, da es als bekannt eingestuft werden muss. Firewalls, Virens Scanner, Intrusion Detection Systeme sind notwendig, adressieren aber immer nur Teilaspekte, betrachten Unternehmens-IT nicht ganzheitlich.

Als präventive Maßnahme ist zu untersuchen, wie es zu einem Schaden kommen kann und wie hoch die Eintrittswahrscheinlichkeit für dieses Ereignis ist. Es geht dabei nicht immer um kriminelle Energien, wie Spionage, Vandalismus, Vorteilsbeschaffung. Auch einfache notwendige, aber falsch ausgeführte Handgriffe eines autorisierten Individuums können Schaden anrichten. Werden interne Systeme kompromittiert, ist es sehr wahrscheinlich, dass es sich um einen Innentäter handelt. Wer sind diese autorisierten Individuen, die Möglichkeit haben, mutwillig oder fahrlässig ein Unternehmen zu gefährden? Es sind die internen und externen Mitarbeiter (Outsourcing Partner) der IT-Abteilungen, es sind die sonstigen Mitarbeiter mit Forscherdrang und Netzwerkzugang (promovierte Putzhilfe).

Nach dem Eintritt eines Ereignisses ist das Ziel der Digitalen Forensik, Beweise zu finden, um daraus weitere gesicherte Schritte abzuleiten. Wenn man sich allerdings mit dem Aufbau der heutigen Systeme befasst und den komplexen Vernetzungsgrad berücksichtigt, ist diese Arbeit meist die Suche nach der Stecknadel im Heuhaufen. Untersucht werden Fingerabdrücke und Anomalien auf Festplatten und Logfiles. Die tatsächlichen Interaktionen zwischen Individuum und Computern sind nicht sichtbar (vergleichen kann man dies mit der Archäologie). **Anzumerken ist, dass die Zuordnung einer digitalen Identität (User Account: Administrator oder root) zu einer juristischen, bzw. tatsächlichen Person, schwierig sein kann. Darauf folgen nach der Digitalen Forensik die klassischen Ermittlungstätigkeiten.**

Wäre es nicht sinnvoll, wenn Interaktionen in kritischen Bereichen vollständig dokumentiert werden? So wie es z.B. an Tankstellen, Geldautomaten, in der Bank oder in einem Kaufhaus mit Hilfe von Videosystemen stattfindet. Oder kritische Aufgaben gemeinsam im Vier-Augen-Prinzip durchgeführt werden.

Im ersten Falle ist eine für das Individuum nicht umgehbare, zentrale Methode notwendig (**Session Recording mit Filmen**). Im zweiten ein rollenbasiertes zentrales Zugangskonzept (**Cooperation mit Vier-Augen-Prinzip**). Diese Methoden steigern die Umsicht bei den durchzuführenden Tätigkeiten, helfen später

Störungsursachen zu heben und liefern den Forensikern wertvolle Indizien. Der Ansatz des Server Based Computings (Applikationsportal) schafft hier die notwendige physikalische Barriere zwischen Individuum und Unternehmens-IT.

