



NULL ADMINISTRATION – VOLLE SICHERHEIT



Sicherheitsregeln schießen oft über das Ziel hinaus und sind deshalb als „Verhinderer“ verrufen. Oder sie sind zu locker und bieten wenig Schutz für das Unternehmen. Im Top-Management stoßen Investitionen in die IT-Sicherheit häufig auf Widerstände, weil Bedenken bezüglich der weiteren effizienten Nutzung bestehen oder die Sinnhaftigkeit in der Wertschöpfung nicht gesehen wird.

Häufig kann der geschulte Benutzer die Sensibilität der Information selbst am besten einschätzen, hat aber weder Expertise im Umgang mit Sicherheitstechnologien noch Zeit für eine „Sonderbehandlung“. Die Lösung: den richtigen Freiraum, der etwas außerhalb der konsolidierten Sicherheitsrichtlinie liegt, entsprechend dem Wissensstand des Anwenders und der jeweiligen Compliance-Anforderung vollautomatisch zuzuordnen - ohne Administration und damit ohne Betriebskosten.

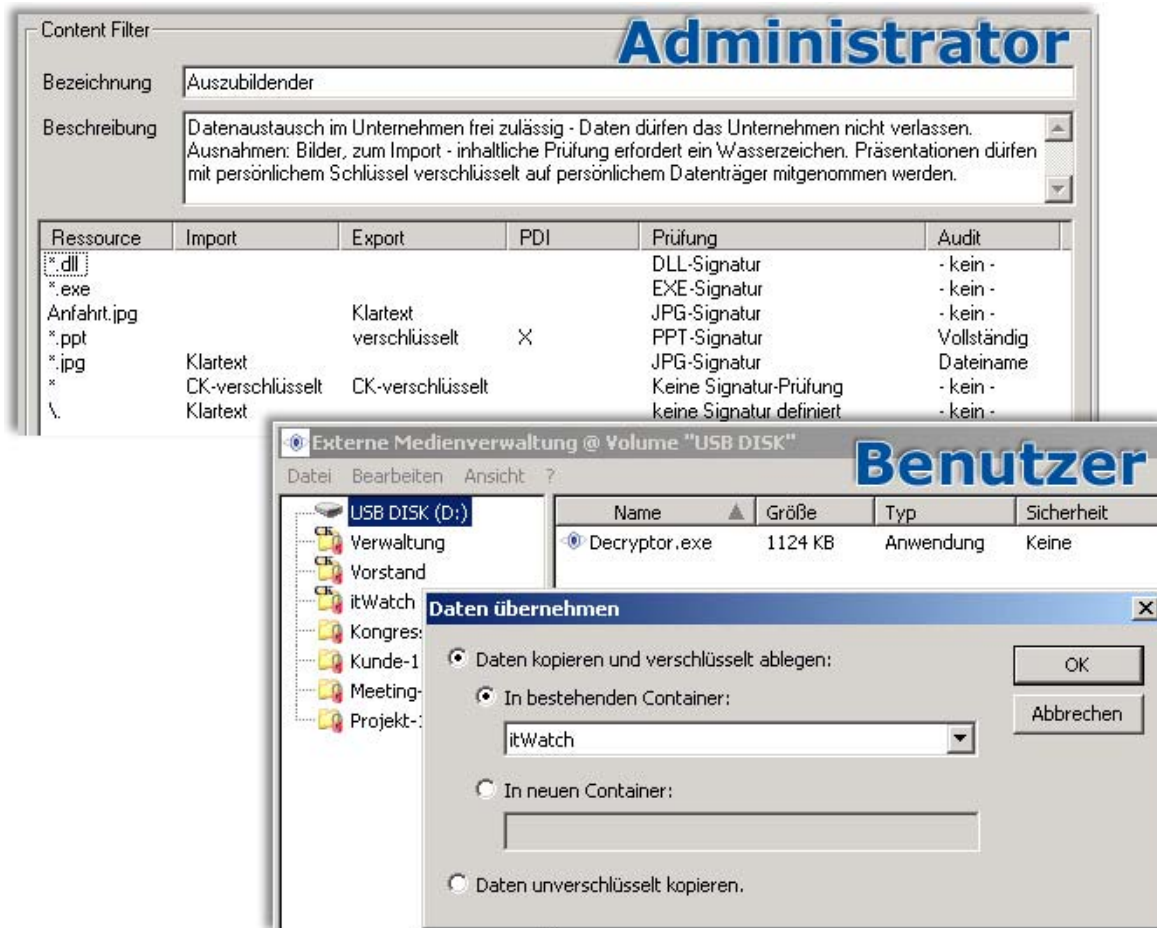
Viele Endpoint Security Projekte scheitern bei der technischen Durchsetzung der Sicherheitsrichtlinie daran, dass die Ausnahmen zu häufig und damit zu teuer sind wenn eine manuelle Administration notwendig ist. Eine Sicherheitsrichtlinie die viele

Schlupflöcher enthält ist andererseits ihr Geld nicht wert. Ein Anwender kann einen guten Grund haben, z.B. einen WLAN-Konverter an USB einzusetzen, wenn seine WLAN Karte im Notebook defekt ist oder das Protokoll des hoteleigenen Hotspots nicht unterstützt. Für solche Ausnahmen ist ein 7/24 Service zur Gerätefreigabe oder Richtlinienänderung zu teuer. Die Endpoint Security Lösungen der itWatch bieten hier verschiedene, kosteneffiziente Verfahren an, die Richtlinie in Echtzeit abhängig vom Systemzustand kontrolliert zu ändern. Eine Möglichkeit für den selbstverantwortlichen Benutzer liegt z.B. im folgenden Dialog:

Der Benutzer kann mit einem gültigen Projektnamen das benötigte Gerät selbst frei geben, unterliegt dann aber einer detaillierten Protokollierung, der er in Echtzeit zugestimmt hat. Was ein gültiges Projekt ist und über welches Wissen (oder welche Security Awareness) der Benutzer beweisbar verfügen muss, kann der

Kunde der itWatch algorithmisch definieren. Dazu wird der gewünschte Algorithmus als Plug-In eingehängt - ohne jedes Zutun des Herstellers. Der vom Benutzer eingegebene Text erscheint im zentralen Logging des Echtzeitmonitors der itWatch. Dadurch sind Revisionssicherheit und Compliance garantiert. Texte im Dialogfeld sind wie immer bei itWatch kundenseitig frei definierbar.

Ein weiterer Anwendungsfall ist die Verschlüsselung. Sensible oder personenbezogene Daten müssen auf mobilen Datenträgern schon aus Compliance-Gründen (z.B. wegen nationaler Datenschutzgesetze) verschlüsselt gespeichert werden. Mitarbeiter haben in der Alltagshektik selten Zeit daran zu denken. Der Anwender, zumeist ein IT-Laie, muss ad hoc in der Lage sein, gewünschte Daten vor dem Transport mit einem mobilen Datenträger den Unternehmensrichtlinien entsprechend zu schützen. D.h. die zentralen Unternehmensrichtlinien zur Protokollierung und Verschlüsselung beim Kopieren kritischer Daten auf externe Datenträger sind ohne weiteres Zutun des Anwenders automatisch umzusetzen. Der erzwungene oder optionale Schutz durch einen oder mehrere Unternehmensschlüssel (siehe Bild: CK entspricht Company Key) verhindert Data Leakage dabei zu 100%, weil die Information nur innerhalb der Firma wieder entschlüsselt werden kann. Folgendes Bild zeigt die Einfachheit für Nutzer und Administrator:



So wird Security zum „Enabler“ - unternehmenskritische Information wird wirksam geschützt, ohne dass die Produktivität der Mitarbeiter leidet.

Informieren Sie sich im Detail über unsere Innovation und kontaktieren Sie uns unter

info@itWatch.de für Produktanfragen,
PR@itWatch.de für Presseanfragen,

per Telefon unter 089 / 620 30 100
oder **besuchen Sie uns:** www.itWatch.de

itWatch GmbH
Stresemannstraße 36
D-81547 München