



## SICHER UNTERWEGS – VERSCHLÜSSELUNG BEIM TRANSPORT VON DATEN

Millionen vertraulicher Daten werden jeden Tag mittels mobiler Datenträger gespeichert und transportiert. Der damit verbundenen großen Gefahr des Datenverlustes lässt sich durch den Einsatz geeigneter Verschlüsselungssoftware entgegenretreten. Der Schutz vertraulicher Informationen auf dem Transportweg basiert auf vielen Notwendigkeiten: das Bundesdatenschutzgesetz fordert die Verschlüsselung personenbezogener Daten auf mobilen Medien. Compliance ist nur gewährleistet, wenn eine zweckmäßige Protokollierung und Verschlüsselung stattfindet. Nicht zuletzt sind die Unternehmenswerte, die in der Information liegen, zu schützen.

Häufig kann der Benutzer die Sensibilität der Information selbst am besten einschätzen, hat aber weder Expertise im Umgang mit Verschlüsselungstechnologien noch Zeit für eine „Sonderbehandlung“ der Information. Nicht jedem Benutzer kann dieser Freiraum gewährt werden. Deshalb besteht die Forderung nach einer zentral gesteuerten Lösung, welche die notwendige Vertraulichkeit und Protokollierung entsprechend den jeweiligen Benutzerrechten, verwendeten Datenträger und transportierten Dateninhalte, sowie den definierten zulässigen Freiräumen filigran steuern kann - ohne große Betriebskosten.

## Der Bedarf

Viele Firmendaten sind auf dem Transportweg besonders zu schützen – aus eigenem Interesse, Gründen der Compliance oder nach geltendem Datenschutzgesetz. Verschlüsselung und Protokollierung sind technisch die richtigen Lösungen, aber die einfache Nutzbarkeit ist missionskritisch, da wenig IT-Expertise und keine Zeit für eine Sonderbehandlung vorhanden ist – das Letztere gilt für den Endanwender ebenso wie für den Administrator. Der Bedarf an einem in das Betriebssystem ergonomisch integrierten Verschlüsselungsverfahren besteht deshalb in jedem Unternehmen, in welchem mobile Datenträger zum Austausch oder zur zwischenzeitlichen Speicherung von sensiblen, unternehmenskritischen oder personenbezogenen Daten eingesetzt werden. Die zentrale Steuerung nach filigranen, aber einfach definierbaren Kriterien ist projektentscheidend.

## Der Markt

Lösungen, die beispielsweise eine partitionsweise Verschlüsselung durchführen, sind für eine Nutzung unterwegs nicht flexibel genug und weisen deutliche Nutzungsdefizite auf. Ein einziger Schlüssel für eine ganze Partition bietet dem Endanwender zu wenig Flexibilität bei der Kommunikation mit verschiedenen Empfängern. Es gilt also ein Produkt zu finden, welches sowohl in der Lage ist das zentrale, netzweite Management der gewünschten Vertraulichkeit als auch die einfache Nutzbarkeit ohne Anwenderschulung und die geeignete Individualisierung entsprechend der Unternehmensrichtlinie zu ermöglichen. Es versteht sich von selbst, dass zudem noch die Anforderungen aus dem BDSG und der Compliance zu erfüllen sind.

Oftmals findet sich in der Literatur und auch in den Fachzeitschriften der Branche Analysen über Verschlüsselungstechnik und Tests über Verlässlichkeit und Sicherheit von Verschlüsselungs-Software und Hardware, doch selten wird über deren Reifegrad, die Anwenderfreundlichkeit und den administrativen Aufwand gesprochen. Doch genau das sind die entscheidenden Aspekte, wenn es darum geht, die Effizienz bei der Durchsetzung seiner zentralen Sicherheitsrichtlinien zu beurteilen.

Der Anwender der Verschlüsselungssoftware, also in den meisten Fällen ein IT-Laie, muss ad hoc in der Lage sein, gewünschte Daten vor dem Transport auf einem mobilen Datenträger entsprechend den Unternehmensrichtlinien für den Transport zu dem jeweiligen Empfänger zu schützen. Einen Schritt weitergedacht bedeutet das, dass die zentralen Richtlinien des Unternehmens zur Protokollierung und Verschlüsselung beim Kopieren der relevanten Daten auf den Datenträger automatisch durchgesetzt werden müssen - ohne weiteres Überlegen des Anwenders.

## Anwendungsfälle aus der Praxis

Aber nicht nur das. Der Freiraum für eigene Entscheidungen der Anwender und die Erkennung bereits vorhandener Sicherheitsmerkmale der Datenträger automatisch erfolgen. Für jeden Mitarbeiter muss der zentral bestimmbar sein und natürlich auch an



muss Freiraum

# Sicherheit beim Datentransport – die Lösung

dezentralen Arbeitsplätzen ohne Netzverfügbarkeit durchgesetzt werden. Dazu sind im Folgenden einige Anwendungsfälle aus der Praxis zusammengestellt:

**„Mobilität“:** Vertriebsmitarbeiter möchten sensible Kundendaten zum Kunden transportieren und dort auf ihren Memory Sticks oder anderen Datenträgern übergeben, ohne dass bei Verlust oder Diebstahl des Datenträgers ein Sicherheitsrisiko für die Daten besteht. Natürlich darf der Vertriebsmitarbeiter den geheimen Unternehmensschlüssel – sofern er ihn kennt – nicht weitergeben und auch nicht auf fremden Systemen hinterlassen, da beispielsweise die Schlüsseleingabe auf einem fremden Rechner durch Tastatur-Sniffer eine unsichere Dateneingabe darstellt und somit den gesamten Datenbestand des Datenträgers gefährden würde. Vorzugsweise sollte der vergebene Schlüssel dann auch noch je nach Anwendungsfall durch den Anwender frei wählbar sein, damit er diesen nicht irgendwo notieren muss.

Diese Anforderung könnte natürlich grundsätzlich durch eine vorkonfektionierte PKI (Public Key Infrastructure) oder Produkte mit benutzerseitiger Schlüsseleingabe erfüllt werden. Eine PKI scheidet jedoch in diesem Szenario aus, da die Infrastrukturanforderungen durch den notwendigen Einsatz von digitalen Zertifikaten und deren Validierung für einen spontanen Datenaustausch zu hoch wären und zumeist keine gemeinsam nutzbare Infrastruktur existiert.

Die Produkte zur Schlüsseleingabe verlangen **vor** der Auslagerung der Daten eine Benutzeraktion – je nach Qualität kann der Benutzer durch eine Aktion im Kontextmenü (z.B. rechte Maustaste) die Verschlüsselung aktiv anfordern. Diese Aktion erfordert aber neben dem Bewusstsein (Security Awareness) des Nutzers auch Zeit und daher Geduld für diesen Vorgang.

Schließlich scheidet hier eine Partitionsverschlüsselung technisch aus, da pro Partition oder Datenträger nur ein Schlüssel verwendet werden kann. Aber was ist, wenn mehrere Kundentermine an einem Tag anstehen oder neben den Kundendaten noch firmeninterne Information auf dem Datenträger liegen?

**„Mehrere Schlüssel auf einem Datenträger“:** Zusätzlich zu der eben beschriebenen Anforderung möchte der Vertriebsmitarbeiter natürlich auf seinem persönlichen Memory Stick möglichst alle Kundendaten unterbringen. Für einen einzelnen Kunden möchte er allerdings nur die für diesen Kunden bestimmten Daten offen legen, unabhängig davon, ob er den Schlüssel und den Datenträger direkt an den Kunden weitergibt oder durch Eingabe eines kundenspezifischen Schlüssels auf einem unsicheren, weil fremden Rechner diesen Datenträger selbst entschlüsselt. Alle weiteren Daten sind dabei weiterhin sicher und damit vor jedem Zugriff geschützt, da sie durch andere Schlüssel gesichert sind. Bei Lösungen, die nur einen einzigen Schlüssel für die gesamte Partition vorsehen, kann diese spezielle Anforderung dann natürlich nicht erfüllt werden.

**„Einfache Nutzbarkeit“:** Die Anforderungen der einfachen Nutzbarkeit (usability) wurden zu Beginn bereits erwähnt. Welche konkreten Anforderungen resultieren daraus? Zunächst darf dem Benutzer keine planende Tätigkeit zugemutet werden, sondern alle Entscheidungsprozesse und Fragen an den Benutzer müssen voll automatisiert in die Standardprozesse und damit auch in die IT-Infrastruktur –z.B. das Betriebssystem - integriert sein. Da es sich um die Vertraulichkeit während des

# Sicherheit beim Datentransport – die Lösung

Transportes handelt, unterscheiden wir die Auslagerung aus einer sicheren Umgebung (Export) und das Einlesen in eine geschützte Umgebung (Import).

**„Notfall-Schlüssel“:** In beiden Situationen ist dabei wesentlich, dass das Schlüsselmaterial Vor-Ort vorrätig ist. Erfahrungsgemäß ist hier der „Kopf“ des Mitarbeiters der beste Aufbewahrungsort, da er stets am Ort des Geschehens ist. Anforderungen zur Aufbewahrung von Schlüsselduplikaten (Notfallschlüssel) an zentralen Stellen - so genannte key-Escrow Anforderungen - bestehen nicht immer. Bei einem vertraulichen Transport von Daten bleiben die Originale in der jeweils sicheren Umgebung unverändert erhalten; stattdessen werden lediglich Kopien mitgenommen. Von Datenveränderungen direkt auf den mobilen Datenträgern, z. B. durch Öffnen der Datei mit Word, ist bei reinen Transportlösungen aus verschiedenen Gründen abzuraten: ein kurzer Kontaktausfall zu dem speichernden Gerät bedeutet beispielsweise den Verlust der Originaldaten (Ausnahmen stellen hier U3-Lösungen dar, die aber derzeit noch kaum eine Verbreitung haben). Aus diesem Grund ist auch von jenen Produkten abzuraten, welche das Löschen des Originals als Option anbieten, da das Firmeneigentum dann auch aus Versehen vernichtet werden kann.

**„Auslagerung von Daten“:** Bei der Auslagerung von Daten (Datenexport) muss unabhängig von dem verwendeten Verfahren in der Microsoft™ Umgebung (Drag & Drop, Cut & Paste oder Kontextmenü) eine Benutzerführung in wenigen und einleuchtenden Schritten in die Standardprozesse eingebracht sein, die zudem die Sicherheitsverfahren und die jeweils geltenden Richtlinien dabei nicht umgehen können. Falls der Nutzer einen Freiraum zur eigenen Entscheidung haben soll, ist es aus Haftungsgründen trotzdem anzuraten die Verschlüsselung als Voreinstellung in die Prozesse aufzunehmen und auf aktiven Benutzerwunsch hin (bestätigt im Log) kann die Option der Klartext-Auslagerung genutzt werden.

**„Daten ins Netz holen“:** Verschlüsselte Dateien müssen beim Kunden ohne Zeitaufwand oder besondere Rechte entschlüsselt bzw. verfügbar gemacht werden. Auf Zielsystemen darf also keine Installation einer Software erforderlich sein, da die meisten Anwender in einem Firmennetzwerk nicht zur Installation berechtigt sind. Das Entschlüsselungswerkzeug muss darum schon bei dem Verschlüsselungsvorgang automatisch auf jeden Datenträger aufgebracht werden, so dass die Daten nach Eingabe des richtigen Schlüssels sofort zur Verfügung stehen.

**„Öffentliche Daten“:** Was ist aber mit den Trivialdaten oder den öffentlichen Daten? Es gibt in jedem Unternehmen Daten, die unkompliziert und ohne Vertraulichkeitsanforderung kommuniziert werden können. Zum Beispiel sind Firmenbroschüren, Produktbeschreibungen, Anfahrtsskizzen und andere öffentlich zugängliche Informationen die Basisausstattung jedes Vertriebsmitarbeiters. Um keinen „Verschleiß“ des Sicherheitsbewusstseins bzw. der Aufmerksamkeit beim Anwender zu riskieren, ist wie immer ist die richtige Dosierung der Sicherheit von zentraler Bedeutung und die automatische Erkennung von öffentlichen Daten ist sehr hilfreich.

**„Richtlinie: Nichts nach draußen mitnehmen“:** Für manche Benutzer, z.B. Aushilfskräfte oder auf manchen Arbeitsplätzen, wie z.B. öffentlich zugänglichen Firmenarbeitsplätzen, muss es möglich sein eine Richtlinie durchzusetzen, die es

verbietet, dass Daten mit „nach Hause“ oder auf andere nicht zum Unternehmen gehörige Arbeitsplätze mitgenommen werden. Trotzdem kann es nötig sein, dass Daten von diesen Nutzern oder auf diesen Arbeitsplätzen innerhalb des Unternehmens oder auch nur einer Abteilung dieses Unternehmens ausgetauscht werden müssen. Da ein mobiler Datenträger nicht in seinem Einsatzgebiet überwacht werden kann, ist es notwendig die Daten beim Mitnehmen so zu verschlüsseln, dass sie nur wieder auf dafür berechtigten Arbeitsplätzen eingelesen werden können. Ein geeignetes Schlüsselmanagement für Unternehmens- oder auch nur Abteilungsschlüssel ermöglicht das. Später im Dokument wird dieses Konzept unter dem Namen *Company Key* oder *Unternehmensschlüssel* technisch ausgeführt.

**„Ziel- und inhaltsabhängige Wahl der Verschlüsselung“:** Es sollte möglich sein, auf Datenträgern wie etwa Memory Sticks oder mehrfach beschreibbaren CDs oder DVDs auch unverschlüsselte Daten zuzulassen, die ohne weiteres direkt ausgelesen werden können. Je nach Firmenrichtlinie wird prinzipiell alles verschlüsselt

und nur einige speziell definierte Dateien können unverschlüsselt ausgetauscht werden (White List Policy) oder es ist grundsätzlich alles unverschlüsselt und nur einzelne besondere Daten werden einer zwangsweisen Verschlüsselung unterworfen (Black List Policy). Auf Basis dieser Vorgaben sollten also unverschlüsselte und verschlüsselte Daten auf einem Datenträger koexistieren können.

Hingegen bei der Auslagerung von Bilddaten auf digitale Fotoapparate, Bilddrucker oder andere Geräte zur Ansicht ist eine unverschlüsselte Auslagerung zwingend erforderlich, da sonst das Gerät nicht mehr booten und damit nicht arbeiten kann. Die Verschlüsselung ist also durch eine zentrale Vorgabe je nach Zielgerät zu steuern.

## Anforderungen an die Vertraulichkeit beim Datentransport in Kürze:

1. Verschlüsselung mit **verschiedenen Schlüsseln auf einem Datenträger**
  - a. im Bedarfsfall werden die Schlüssel durch den Benutzer gewählt
  - b. Unverschlüsselte Dateien liegen neben verschlüsselten auf einem Datenträger
2. **Zentrale Definition der Schlüsselstärke**, evtl. der Verschlüsselungsverfahren und Richtlinien
  - a. Wer darf unverschlüsselt auslagern?
  - b. Die Schlüsseleigenschaften eines starken Schlüssels sind zentral zu definieren.
  - c. Welche Dateien/Contents dürfen unverschlüsselt ausgelagert werden?
  - d. Auf welche Geräte/Devices darf unverschlüsselt ausgelagert werden – für welche wird eine Verschlüsselung erzwungen?
  - e. Unterliegt die Weitergabe einer Protokollierung bzw. einem Shadowing
3. **Vollautomatisierte Integration in Windows:** alle Standard Windows Mechanismen für das Dateimanagement müssen automatisch in der Verschlüsselung münden
  - a. Drag & Drop
  - b. Cut & Paste
  - c. Kontext Menüoperationen (Kopieren und Einfügen)
4. **Keine Umgehung der Sicherheitseinstellungen** für sensible Daten
5. **Entschlüsselungssoftware** muss **automatisch mitgeliefert** werden und darf keine Installation im Zielsystem erfordern

## Sicherheit beim Datentransport – die Lösung

Besteht nun nicht die Gefahr, dass auf diesen unverschlüsselten Geräten sensible Daten unverschlüsselt das Netz verlassen? Nicht, wenn man durch eine inhaltssensitive Prüfung der Dateien und deren Inhalte sicherstellt, dass nur nach den geltenden Sicherheitsrichtlinien freigegebene Daten auf solchen Geräten gespeichert werden können. Die Entscheidung, welche Daten zur Verschlüsselung anstehen, ist deshalb nicht nur vom Ziel der Kopieroperation abhängig, sondern wird stets auch in Abhängigkeit des Inhalts getroffen. Sie kann nicht auf der Basis des Dateityps getroffen werden, da bei einer Umbenennung einer Datei und deren -endung das Kontrollsystem überlistet werden könnte, sondern muss auch die Möglichkeit der inhaltlichen Prüfung (Content- und Pattern-Prüfung) mit einbeziehen.

**Verschlüsselung mobiler Datenträger nach Bundesdatenschutzgesetz:** Das Bundesdatenschutzgesetz, kurz BDSG, fordert die Verschlüsselung personenbezogener Daten auf externen Datenträgern nicht explizit. Es fordert aber in § 9 BDSG technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten und verweist dabei insbesondere auf die Anlage zu § 9 BDSG. In der Anlage steht dann:

"Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

[...]

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, [...]"

Dabei ist zu beachten, dass nach § 9 BDSG entsprechende Maßnahmen nur zu treffen sind, wenn sie in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen. Verschlüsselung ist demnach zwar nicht in jedem Fall erforderlich, aber bei sensibleren Daten dürfte Verschlüsselung die einzig sinnvolle Möglichkeit sein dieser Anforderung gerecht zu werden. Das Wegsperrern von Memory Sticks in geeignete Safes ist natürlich keine praktikable Lösung, da sie der Anwendung von Memory Sticks im Normalfall entgegensteht.

Nr. 4 der Anlage betrifft aber nicht nur mobile Datenträger wie Memory Sticks, gebrannte CDs oder DVDs. Im Übrigen ist insbesondere bei mobilen Speichermedien, die an den Betroffenen ausgegeben werden (z.B. Smartcards), die Spezialvorschrift des § 6c BDSG zu beachten.

Relevante Gerichtsentscheidungen zu § 9 BDSG oder der Anlage gibt es nicht. Auch die juristische Literatur hat sich mit dem Thema bisher kaum auseinandergesetzt. In Ernestus, NK-BDSG, 2006, § 9 Rn. 112 findet sich im Rahmen eines Kommentares zum BDSG die Feststellung, dass Verschlüsselung und Signatur mögliche Maßnahmen zum Schutz der Übertragungswege sind.

## Gibt es eine einfache Lösung?

All diese Anforderungen zeigen auf, dass man eine Softwarelösung benötigt, die nicht nur den Sicherheitsaspekt durch einen guten und zuverlässigen Verschlüsselungsalgorithmus umsetzt, sondern für den Anwender einfach und ohne jede IT-Expertise nutzbar sein muss und in der zentralen Administration ohne großen Aufwand eingesetzt werden kann. Bei vielen Produkten am Markt hat man aber nicht an die Anwenderfreundlichkeit und an die Betriebs-Komplexität gedacht. Starre Ein-Schlüssel-Lösungen wie einige Partitions-Verschlüsselungen sind heutzutage weit verbreitet - sehr zum Leidwesen vieler Nutzer.

**itWatch** löst die Herausforderung mit Endgerätesicherheit. **PDWatch** ist ein leistungsstarkes Verschlüsselungsprogramm, das den sicheren Datentransport von oder zu mobilen Datenträger und Netzwerken nun kinderleicht macht. **XRyWatch** überwacht jeden Inhalt und kann neben der inhaltsabhängigen Protokollierung auch bestimmte Verschlüsselungsformate erzwingen. Mit **XRyWatch** können Unternehmen auch „exotische“ Anforderungen zentral verwalten und netzwerkweit durchsetzen. So kann beispielsweise definiert werden, dass Word Dokumente mit dem in der Fußzeile befindlichen Zusatz „firmenvertraulich“ zu verschlüsseln sind und nicht mitgenommen werden können, wenn dem Logging nicht zugestimmt wurde. Nicht sensible Daten können dagegen bei Bedarf unverschlüsselt ausgelagert werden. **DeviceWatch** setzt alle geräteabhängigen Einstellungen durch. Mit der **Endgerätesicherheit der itWatch** kann jede geltende Firmenrichtlinie, egal ob freizügig oder restriktiv angelegt, zentral verwaltet und netzwerkweit durchgesetzt werden. Völlig frei vom Administrator definierbar in Bezug auf Dateityp, Dateinhalt und verwendetem Datenträger können Rechte an Benutzer oder Gruppen vergeben werden, z.B. Lesen, Schreiben, verschlüsselt, in Klartext schreiben, mit Firmenschlüssel verschlüsselt und natürlich mit Audit (Compliance und Revisionsicherheit), damit sämtliche Schreib- und Kopiervorgänge einfach und übersichtlich protokolliert und Datenvolumina korrekt aufgezeichnet werden. Zudem können mobile Datenträger auf einzelne Benutzer oder Benutzergruppen personalisiert werden, um z.B. besonders sensiblen Vorgängen in Projekten oder im Vorstand, bei Stabsstellen Rechnung zu tragen.

Ein Anwenderbericht zum Gebrauch des *Content Filters* aus dem Produkt **XRyWatch**, der bei der Polizei Bayern seit 2004 auf ca. 20.000 Arbeitsplätzen im

produktiven Einsatz ist, wurde auf der Microsoft Polizeikonferenz bereits vorgestellt [Wust2006].



# Sicherheit beim Datentransport – die Lösung

## Eine einfache Lösung – im Beispiel

Eine Aushilfskraft, soll in einfacher Weise alle Daten im Unternehmen transportieren können, d.h. also mit einem dem Nutzer unbekanntem „Firmenschlüssel“ (im Bild CK für *Company Key*) gegen das Einlesen in Fremdsystemen geschützt werden. Bilddateien können von digitalen Fotoapparaten nur unverschlüsselt gelesen werden, da diese Geräte keine Verschlüsselung zur Verfügung stellen. Darum sind die Bilddaten detailliert auf deren Inhalte durch das Pattern-Matching zu prüfen (im Bild *JPG-Signatur*), wohingegen eine Präsentation z.B. im Powerpoint Format durchaus sensible Informationen enthalten kann und darum geschützt auf fremde Rechner transportiert werden soll. Deshalb ist eine erzwungene, nutzerspezifische Verschlüsselung eine sinnvolle Lösung. Damit die Daten auch prüfbar sind, wurde hier ein vollständiges Auditing eingestellt, das die exportierten Powerpoint-Daten komplett in ein zentrales Schattenarchiv kopiert, auf welches der Benutzer keinen Zugriff hat.

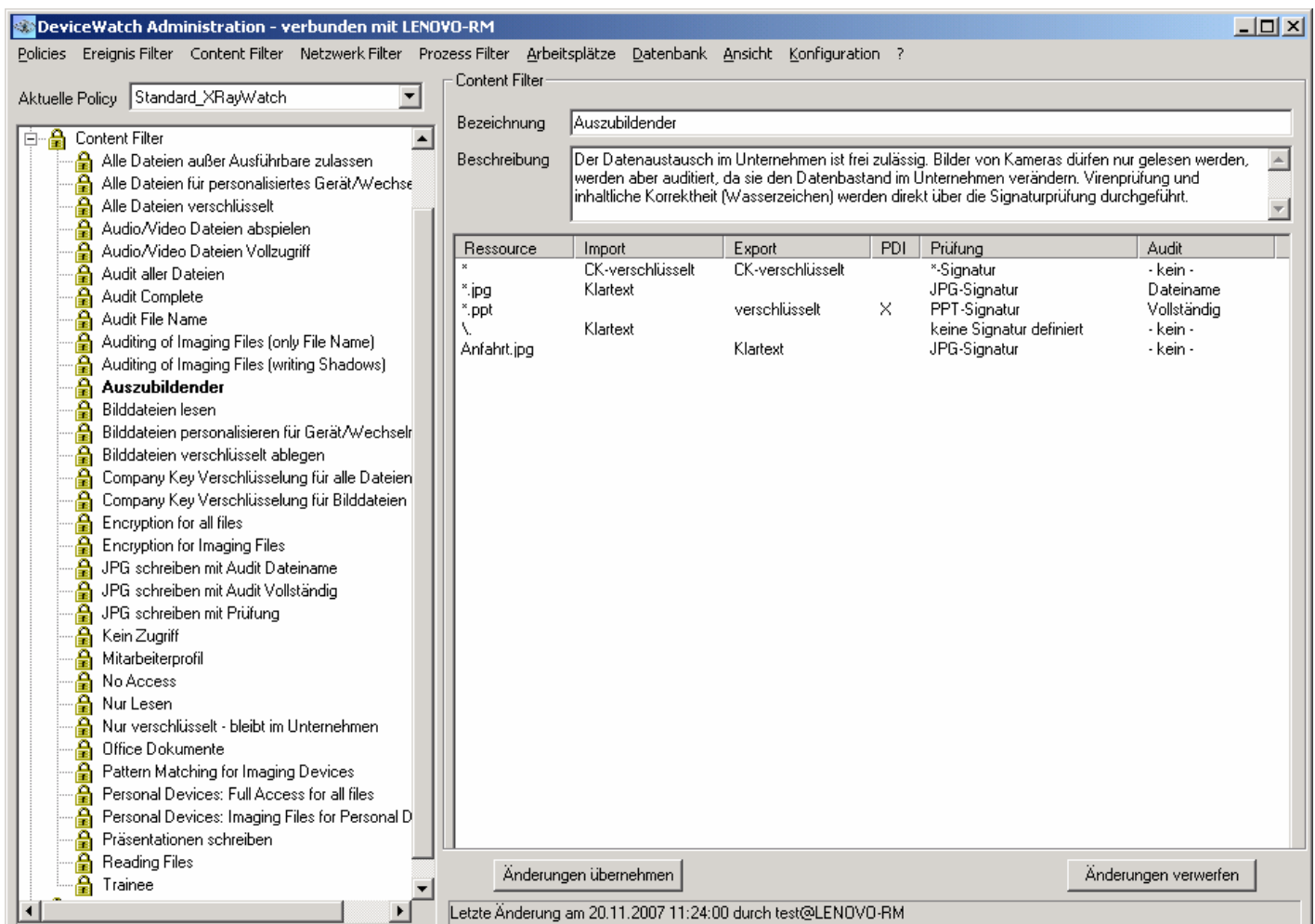


Bild: Ausschnitt aus der zentralen Administration der itWatch Endgeräte Sicherheit.

Der hier gezeigte Ausschnitt aus der Administration der **itWatch** Produktsuite zeigt auf, dass es bereits heute möglich ist, an bestimmte Dateien - nach namens- oder auch inhaltspezifischen Kriterien - die Anforderung der Zwangsverschlüsselung (je nach gewähltem Datenträger und angemeldeten Nutzer) zu stellen. Eine Verschränkung der Vertraulichkeitsanforderung mit den Inhalten ist somit einfach

## Sicherheit beim Datentransport – die Lösung

profilbasiert möglich. In der obigen, in der Produktsuite als *Content Filter* bezeichneten Einstellung, wird eine Verschlüsselung mit einem dem Nutzer unbekanntem Firmenschlüssel für alle Daten beim Lesen und Schreiben gefordert. Nur Bilddaten in JPEG Formaten dürfen im Klartext gelesen (aber nicht wieder geschrieben) werden, da Imaging Systeme wie digitale Kameras keine verschlüsselten Daten liefern.

Diese strategische Komponente der Kombination „Geräteschutz und Verschlüsselung“ wird nach aktuellen Marktbeobachtungen in Zukunft den Markt weiter separieren und die High-End Produkte von den einfachen Lösungen unterscheiden. Kundenseitig ist diese Anforderung vielfach bekannt und hat bereits eine hohe praktische Auswirkung.

## Fazit

Die heute häufig vertretene Philosophie von Unternehmen „nicht gängeln sondern unterstützen“ setzt viel Vertrauen in die Mitarbeiter. Nicht nur diese Philosophie sondern auch klassische Sichtweisen der technischen Sicherheit werden durch die vollautomatisierte Integration der Endgerätesicherheit der itWatch in das Windows™ Betriebssystem umgesetzt. Dadurch kann beispielsweise der Datenschutzbeauftragte oder Information Security Officer eines Unternehmens mit einer einfachen, bereits standardmäßig im Produkt enthaltenen Sicherheitspolicy die Verschlüsselung bei der Auslagerung anfordern. Falls einem Benutzer durch das zentrale Management ein Recht für das unverschlüsselte Auslagern zugesprochen wird, geht die Verantwortung auf den Benutzer über, der durch eine persönliche Aktion seine Zustimmung zur unverschlüsselten Auslagerung jeweils im Einzelfall bestätigt. Damit hebt sich das Produkt eindeutig von der Konkurrenz ab und hat neue Maßstäbe in der IT-Sicherheitsbranche gesetzt.

Einer der weltgrößten Finanz- und Versicherungskonzerne vertraut auf die umfassende Leistungsfähigkeit des Programms durch die Installation von PDWatch auf 40.000 Außendienstmitarbeiter-Laptops, die im Jahr 2005 zur Zufriedenheit aller Anwender stattgefunden hat. Die Bankengruppe Santander hat sich im Frühjahr 2007 bei einem weltweiten Vergleich der Endgerätesicherheitslösungen für die Produkte der itWatch entschieden. Die Endgerätesicherheit der itWatch bildet die Anforderungen von Nachrichtendienst und Militär, Großunternehmen und Mittelstand mit nur einer Lösung ab. Überzeugen auch Sie sich von seiner Leistungsfähigkeit und kontaktieren Sie uns unter

[Info@itWatch.de](mailto:Info@itWatch.de) oder 089 / 620 30 100.

itWatch GmbH  
Stresemannstraße 36  
D-81547 München

## Quellenangabe:

- [Security Awareness](#)
- [Einsatzbericht Landespolizei Bayern](#)
- [LANline – User Awareness in Echtzeit](#)
- [Mobile USB-Sicherheit](#)

[BDSG] Bundesdatenschutzgesetz §9

[Sch05] Peter Scholz: *Unbekannte Schwachstellen in Hardware und Betriebssystemen*. Handbuch der Telekommunikation, Wolters Kluwer Verlag, März 2005.

[Wust2006] Digitale Fotografie auf dem XP-Arbeitsplatz der Bayer. Polizei, Erfahrungen im Zusammenhang mit der Einführung eines fachspezifischen Polizeiarbeitsplatzes und im Umgang mit Bilddaten, PP Oberbayern und PP Niederbayern Oberpfalz, 11. Microsoft Polizeikongress 3./4. April 2006 in Bad Homburg

## Anlage zum Bundesdatenschutzgesetz (BDSG)

In der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)

### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

## § 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien

- (1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen
1. über ihre Identität und Anschrift,
  2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
  3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
  4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen
  5. unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.
- (2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.
- (3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

## § 3 Weitere Begriffsbestimmungen

- (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
- (2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

[...]

- (10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,
1. die an den Betroffenen ausgegeben werden,
  2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.