IT-Sicherheit ist nicht nur Gesetz und Compliance, sondern vor allem Unternehmenskultur

IT-Sicherheitsanforderungen sind „von außen“ durch eine Flut von auferlegten, regulierenden Bestimmungen definiert und „von innen“ durch das subjektive Verständnis des Unternehmens und der individuellen Relevanz der Regularien. Neben Bundesdatenschutzgesetz, KonTraG, SOX, HIPPA, Basel II, GOBS, FAMA, TDDG und Euro Sox gibt es viele weitere Vorschriften, die in Teilen oder dem gesamten IT-Markt zu berücksichtigen sind. Mitunter stehen sich Anforderungen an die Beweisbarkeit mit Themen des Datenschutzes scheinbar unvereinbar gegenüber. Letztendlich überlagern sich daher standardisierbare Anforderungen an die Sicherheit mit individuellen zu einem unternehmensspezifischen Anforderungs-Profil. Als entscheidender Faktor kommt letztlich die Unternehmenskultur hinzu, denn im Umsetzen der Aufgabenstellung wird das Unternehmen zwischen technischer und organisatorischer Lösung einen Mittelweg finden. In der Praxis heißt das die richtige Lösung zwischen dem „selbstverantwortlichen Benutzer“ mit allen Freiräumen und dem möglicherweise ungeschulten „Normalnutzer“ zu finden.

Die Komplexität des Themas steigt noch, wenn man sich in die Lage einer international tätigen Firma versetzt, welche in dem skizzierten Spannungsfeld zudem lokal gültige Gesetze mit einbeziehen muss. Nehmen wir an eine deutsche Firma besitzt ein Tochterunternehmen in den USA. Die Richtlinien in den USA erlauben es den Unternehmen, Mitarbeiter auf dem Firmengelände fast beliebig detailliert zu überwachen, während das in Deutschland nach geltendem Recht vollständig untersagt ist, solange keine Zustimmung durch die Mitarbeiter und / oder deren Vertretung vorliegt. Reist nun deutsches Recht mit dem Notebook und dem Mitarbeiter oder sollte vielmehr das jeweils lokale Recht Vorrang haben. Neben der rein juristischen Frage ist dies eben auch eine Frage der Unternehmenskulturen beider Organisationen, die sich über kurz oder lang angleichen werden und es ist eine Frage des Schutzbedarfs an den jeweiligen Standorten.

Es kommen aber auch in kleineren Organisationen Faktoren dazu, die es unmöglich machen, mit einer einzigen - für alle gültigen - Einstellung der IT-Sicherheit allen Nutzungsszenarien gerecht zu werden. Um bei obiger Sprachwahl zu bleiben kann man je Benutzer fragen: Wie „selbstverantwortlich “ darf er denn agieren?. Aus der Antwort schlussfolgert man dann auf die notwendige technische Reglementierung und dem daraus resultierenden und damit adäquaten Freiraum je Nutzer.

Bestimmung des Freiraumes: Einem Datentypisten, der einen Arbeitsüberhang abarbeitet und evtl. in einem Zeitarbeitsverhältnis arbeitet, wird man weniger Verständnis für die Vertraulichkeit der Daten einräumen als dem Geschäftsführer, dessen eigenes Wohl auch von der gesetzmäßig korrekten Arbeitsweise in dem Unternehmen abhängt. Mit Sicherheit ist also die Vertrauenswürdigkeit der Person und die Bindung an das Unternehmen ein Parameter für das Maß des möglichen Freiraums. An dem Beispiel lässt sich gut erkennen, dass in jedem Unternehmen technischer Schutz notwendig ist, da die Aushilfskraft ebenfalls Zugriff auf sensible Daten hat, die am besten im Unternehmen verbleiben sollten, z.B. durch eine Verschlüsselung mit einem Unternehmensschlüssel. Bei Benutzern mit einer hohen Bindung an das Unternehmen und einer hohen Vertrauenswürdigkeit kann auf einen technischen Schutz durch Verbote eventuell sogar ganz verzichtet werden. Trotzdem ist bei einigen Daten eine gesetzliche oder firmeninterne Beweispflicht gegeben, so dass technische Maßnahmen z.B. im Zuge der Protokollierung oder als Echtheitsnachweis notwendig werden.

Kritikalität der Daten: Der Schutzbedarf oder die anzuwendende Mechanismusstärke beim Schutz der Daten hängt hauptsächlich von der Interessenslage des Unternehmens ab. Der Verlust von firmeneigenen Daten hat viele Facetten: Information Leakage, Data Loss, Wirtschaftsspionage, Datendiebstahl und viele mehr. Ein gestohlenes Notebook bemerkt man sofort – illegal kopierte Geschäftsdaten, die über dunkle Kanäle Dritten zugänglich sind, bemerkt man nie oder erst, wenn es viel zu spät ist. Eine Rückrufaktion für „versehentlich“ offen gelegte Daten ist unmöglich. An einem Produktionsstandort sind andere Daten kritisch als an einem Vertriebsstandort. Die Schutzwürdigkeit der Daten hängt also ebenfalls von vielen Aspekten ab

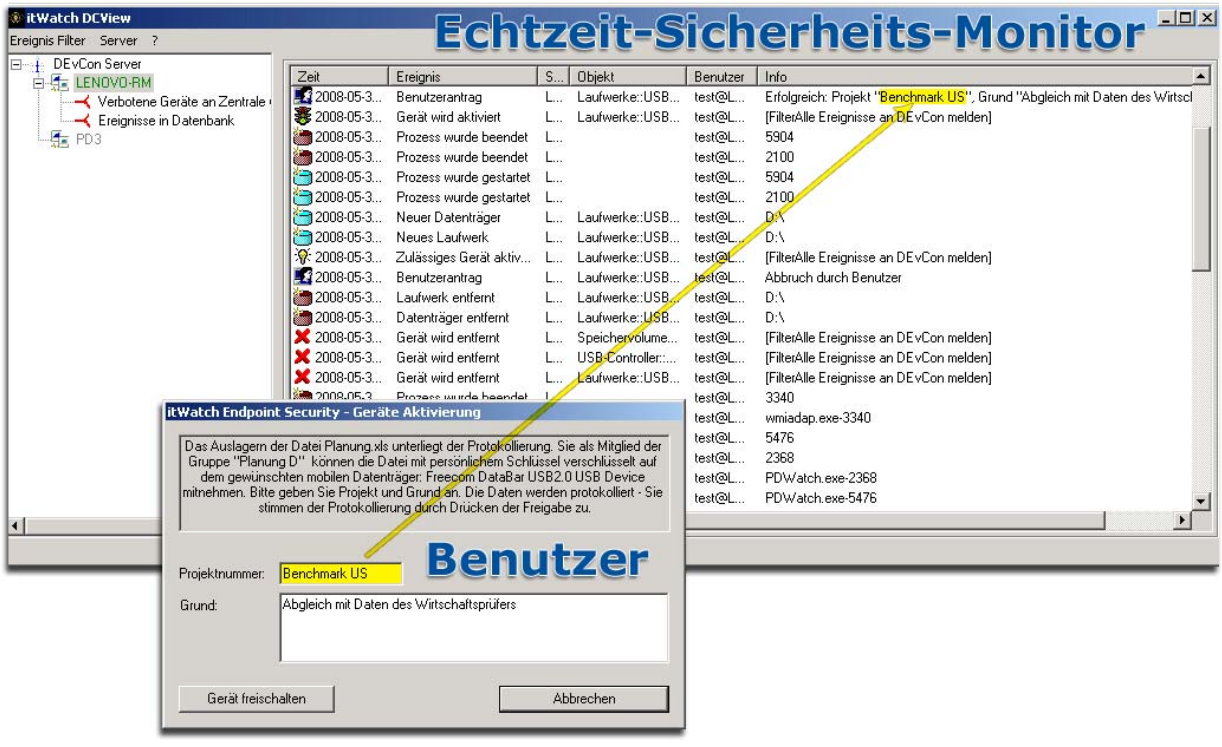
Personendaten – oder Daten zu Unternehmen - werden im Internet zwischen 0,10 und 100 Euro je Datenpaket gehandelt. Der Preis hängt von der Datenqualität ab, also wie viel Information zur Person oder zum Unternehmen ist verfügbar und ist diese Information auch aktuell und „verwertbar“. Viele Firmen haben bereits erkannt,

dass ihre Kundendaten, die CAD-Daten der neuen Produktreihe, die Kalkulatoren für komplexe Produkte oder auch Einkaufskonditionen hier einen erheblichen Wert darstellen. Interessanterweise ist der Wert für Dritte, Außenstehende manchmal höher als für den Besitzer.

Zweifelsohne ist das also ein attraktives Feld für Angreifer oder interne Täter mit fragwürdiger Interessenslage, insbesondere da sich die illegal beschafften Datensätze beliebig vervielfältigen und damit mehrfach in bares Geld umsetzen lassen. Krisenstimmungen im Unternehmen oder persönliche Problemsituationen von berechtigten Personen wirken hier häufig als auslösendes Moment.

Awareness effizient organisieren: Das Bindeglied zwischen Unternehmensinteresse, gesetzlichen Anforderungen, Schutzbedarf und adäquaten Reaktionen durch den Benutzer ist der Informationsfluss. Kann das Unternehmen dem Nutzer alle entscheidungsrelevanten Informationen zum passenden Zeitpunkt zur Verfügung zu stellen, so wird das positiv unterstützend wahrgenommen und erleichtert die Einhaltung der Regularien. Der Informationsfluss ist aber in beiden Richtungen notwendig. Vom Benutzer wird in besonders kritischen Stuationen erwartet, dass er Gründe für sein Handeln, Zustimmung zu den genannten Regularien, z.B. auch bestimmten Protokollierungen oder weiterführende Angaben verbindlich bestätigt. Gleichzeitig bestätigt der jeweilige Protokolleintrag natürlich auch den Erhalt der Information, sowie die Zustimmung des Nutzers und ist damit der Beweis für die Einhaltung der Regularien und *der* wesentliche Baustein für die Compliance.

Direkt auf die Situation bezogene Dialoge mit dem Benutzer funktionieren am besten in Echtzeit, um die Aufmerksamkeit des Benutzers auf das Wesentliche zu lenken und damit effizient und zeitschonend die Prozesse zu motivieren und umzusetzen. Ein praktisches Beispiel:



Die Zustimmung gilt als elektronische Willenserklärung und kann auch um Integritätsbeweise wie z.B. eine Signatur ergänzt werden, da die Steuerung durch ein Plug-In kundenseitig erweiterbar ist.

Sicherheitsziele können also durch

1. einen proaktiven Schutz mit Verboten,
2. eine abschreckende Wirkung über die Beweisbarkeit und eventuell eintretende Haftung im Nachhinein,
3. organisatorische und vertragliche Vereinbarungen,
4. bewusstseinsverbessernde Maßnahmen – Security Awareness
5. oder Kombinationen davon

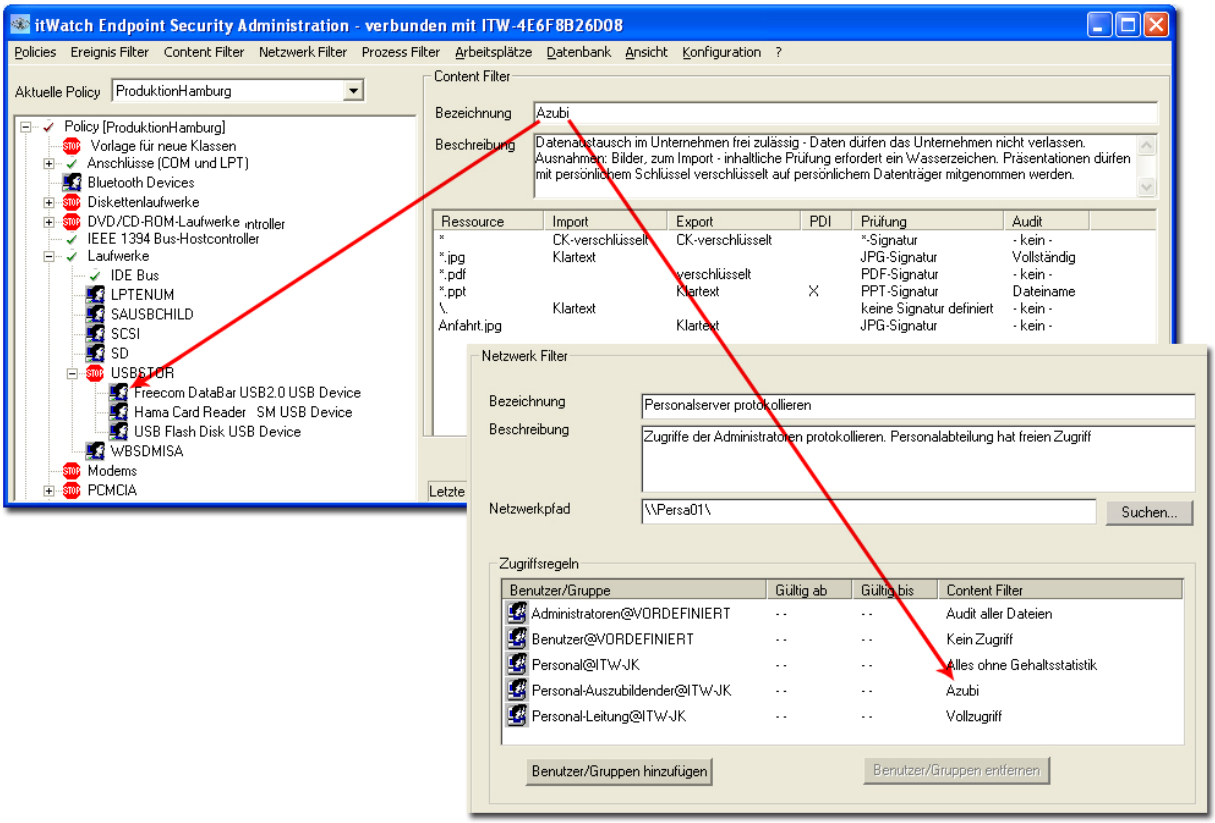
umgesetzt werden. Welches Verfahren ist nun am besten geeignet, die Sicherheitsziele des Unternehmens umzusetzen?

Steigt auf der einen Seite die Sicherheit durch eine höhere Stärke des Schutzmechanismus, ist auf der anderen Seite der Eingriff in die Unternehmensabläufe und -kultur größer und die Sicherheit wird als Verhinderer wahr genommen, wenn die Maßnahme im Einzelfall überzogen ist. Die richtige Balance ist also entscheidend dafür, dass eine Unternehmenskultur einerseits den Sicherheitsbedarf reflektiert und andererseits von den Mitarbeitern einheitlich als hilfreich, positiv und „passend“ wahrgenommen wird.

Durch die vielen Faktoren, die im Einzelfall wirken und die stete Veränderung der Rechtslage und der Regularien ist die *Dynamik* das stabile Element in dem Bereich. Der Sicherheitsmanager eines Unternehmens muss deshalb in der Lage sein, geänderte Bedrohungs-Lagen oder modifizierte Regularien sofort umzusetzen und insbesondere die neuen Erkenntnisse in die Kommunikation mit dem Benutzer einzubinden, so dass dieser auch zeitnah informiert wird. Security Awareness ist - so verstanden – der Mörtel zwischen den Bausteinen der IT-Sicherheit und erlaubt durch individuelle, kontextabhängige Benutzerdialoge verständliche, auf die spezielle Zielgruppe ausgerichtete, Kommunikation.

Benötigt wird also *ein* Werkzeug „für alle Fälle“, welches technische Sicherheit in Form von Verboten möglichst fein-granular erlaubt und die Protokollierung von Aktionen und kundenspezifischen Informationen ohne Medienbruch in einer Datenbasis ermöglicht und die organisatorischen Abhängigkeiten stets nach Bedarf verständlich in Echtzeit an den Benutzer kommuniziert. Folgendes Bild zeigt technische Granularität, die mit den zuvor genannten Benutzerdialogen zusammen die gesamte Palette der technischen und organisatorischen Sicherheit unterstützt – natürlich zentral administriert:

Endpoint Security – Security Awareness in Echtzeit



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

Weitere Literatur:

- Sicherer Datentransport
- Einsatzbericht Landespolizei Bayern
- Mobile USB-Sicherheit
- Null Administration - Volle Sicherheit