ENDGERÄTESICHERHEIT – DAS BRAUCHT MAN WIRKLICH!

ANFORDERUNGEN UND LÖSUNGEN

Die Sicherheitsdefizite durch die generische Plug & Play-Pforte für Peripheriegeräte wie USB Memory Sticks, Flash Pens, digitale Kameras, Scanner, Modems etc., sind seit langem bekannt: unerwünschte Inhalte und gefährliche Programme bedrohen die Integrität der Netze und entescheidendes Know-how des Unternehmens kann unerkannt abgezogen und vervielfältigt werden (Data Loss oder Data Leakage).

Die IT-Abteilungen der Unternehmen können das Problem mit Bordmitteln nicht in den Griff bekommen. Viele Lösungen sind am Markt, die aber häufig nur einen Teil der Problematik abdecken. Zu den Interessen aus der IT-Sicherheit kommen noch die Anforderungen des Betriebes nach Effizienz und Kostensenkung, sowie die Notwendigkeit den Benutzer bei komplexeren Einsatzszenarien zu unterstützen.

Das Thema der Endgerätesicherheit (Endpoint Security) ist damit viel breiter als nur eine effiziente Zugangskontrolle für jedwede Geräteschnittstelle, sei es USB, Firewire, Bluetooth, PCMCIA, Infrarot etc. zu realisieren. In der Folge führen wir eine Bestandsaufnahme durch, was eine umfassende Lösung für die Endgerätesicherheit heute leisten muss:

Endgerätesicherheit – das braucht man wirklich!

Die Herausforderungen

- **Device Kontrolle** – Wer darf welches Device (Peripheriegerät und fest verbaute Hardware) wann und wo nutzen? Natürlich darf für eine neue Geräteklasse oder Schnittstellenklasse kein Update vom Hersteller nötig werden.
- **Verschlüsselung der mobilen Datenträger** – Die Verfahren der Vergangenheit (z.B. Partitionsverschlüsselung) haben ausgedient, da der Bedarf an Vertraulichkeit zunehmend von den Dateiinhalten und ihrer Sensitivität abhängt und nicht mehr alle Daten einheitlich klassifiziert und behandelt werden können.
- **Personalisierung von Datenträgern** – Günstige Datenträger verfügen über keine eigenen Merkmale wie Seriennummern. Die Verwendung von Datenträgern in besonders kritischen Bereichen (Vorstand, Akquisition, Stabsabteilungen etc.) erfordert es aber aus Gründen der Compliance wesentliche Datenbewegungen beweisbar abzulegen. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier Voraussetzung.
- **Kontrolle der Anwendungen** – Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von Whitelists UND Blacklists.
- **Protokollierung aller verwendeten Geräte und ausgetauschten Dateien** – Blockieren und Freigeben alleine genügt heute schon lange nicht mehr. Die Beweisbarkeit von Datenbewegungen ist in vielen IT-Umgebungen zum kritischen Faktor geworden. Die Begrenzung der Protokollvolumina durch geeignete Verfahren ist hier zwingend; insbesondere, wenn die gesamten Dateninhalte (also nicht nur Dateinamen) protokolliert werden müssen.
- **Kontrolle der verwendeten Netze** – Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung die Kontakte. Entsprechend des erkannten Netzes muss die Security Policy in Echtzeit eingestellt werden – z.B. Heimarbeitsplatz, Firmenzentrale, Standort Produktion, Schulung, etc.
- **Alerting** – Die Benachrichtigung der bereits etablierten *Intrusion Detection* Verfahren, also die unkomplizierte Integration in Drittprodukte, ist hier genauso wichtig wie die Möglichkeit Echtzeitreaktionen auf kritische Ereignisse zu konfigurieren.
- **Management Information, Reports und Quota-Management (*Datenmengen-Management*)** geben historische oder Echtzeit Auskunft über die Nutzung und den Netzzustand nach Standorten, Abteilungen oder anderen Kriterien.

Diese Anforderungen an die Endgerätesicherheit sind natürlich alle in Echtzeit, an allen Schnittstellen (USB, Firewire, Bluetooth, WLAN ...), für alle Geräteklassen, für alle Benutzer und für alle Dateien oder Informationen zu leisten.

Das Tempo der vorgestellten Innovationen in der IT-Branche ist hoch und das Wachstum der Möglichkeiten im IT-Sektor steigt rasant. So ist es kein Wunder, dass mehr und mehr Unternehmen aller Größenordnungen auch ihre wertschöpfenden Prozesse auf den Einsatz von innovativen mobilen Lösungen rund um die Peripheriegeräte ausrichten. Memory Sticks und sonstige mobile Datenträger wie Kameras, PDAs etc. haben in den IT-Umgebungen auf Basis von Innovationsdruck und Kosteneffizienz ihren festen Platz. Doch die unüberschaubare Anzahl neuer Geräte im Netzwerk will auch geplant, verwaltet, organisiert und nicht zuletzt in die Standardprozesse der IT integriert werden. Windows-Bordmittel sind keine große

Endgerätesicherheit – das braucht man wirklich!

Hilfe und so gibt es im Markt zunehmend mehr Produkte zur Security und zum Systems Management. Auch die von Microsoft vorgestellten Betriebssysteme Windows Vista oder Windows 2008 Server bieten hier keine Lösung an.

Bei dem Blick auf die bestehenden Softwarelösungen im Markt zeigt sich, dass die Lösungen auf der Systems Management Seite kaum Funktionen in der IT-Sicherheit haben, die über das Blockieren und Protokollieren hinausgehen. Die Produkte aus der Sicherheitswelt haben aber fast alle keine Mehrwerte im Systems Management. Einzige Ausnahme ist hier die **Endpoint Security Suite** der **itWatch**, die zusätzlich zu den umfassenden Sicherheitsfunktionalitäten auch alle Wünsche aus dem Systems Management erfüllt.

Um sich der Materie zu nähern, muss man zunächst das Spannungsfeld verstehen, in dem sich der IT-Manager befindet. „Volatile“ Peripheriegeräte und immer mehr schnurlose Schnittstellen kommen zu den „festen“ Geräten wie Maus, Tastatur und Drucker in einem Ausmaß hinzu, das bis vor ein paar Jahren unvorstellbar war. Alle diese neuen Geräte müssen inventarisiert und ggf. personalisiert werden, damit weiterhin Überblick herrscht, welche Geräte wann und wo welchen Nutzen bringen. Der IT-Manager wird aber nicht in gleichem Maße Personal- oder Zeitzuwachs erhalten haben, sondern muss weiterhin in einem identischen Zeitrahmen die erhöhten Anforderungen an die IT-Umgebung bedienen. Zudem ist die Verwaltung der Geräte und ihrer Einsatzszenarien wesentlich dezidierter zu betrachten als noch vor Jahren. Abgebrochene Installationen und Konfigurationsfehler müssen ebenso leicht erkennbar und vor allem behebbar sein wie die Integration in die Standardprozesse z.B. Beschaffung, Auslieferung, Freigabe, Validierung, Berechtigung. Der Helpdesk - nun mit einem deutlich höheren Aufkommen an Anfragen konfrontiert - muss in der Lage sein seine Beantwortungszeit entscheidend zu verkürzen und ist dabei auf die Mehrfachverwendbarkeit von automatisierten Lösungen angewiesen, wie z.B. die „on-demand“ Treiber-(Nach-)Installation.

Natürlich bewertet der Kunde seine Prioritäten bem Abwägen zwischen Systems-Management und IT-Sicherheit. In Zeiten von organisierten Angriffen auf Firmeninformationen aus Drittstaaten darf ein Aspekt nicht vernachlässigt werden. Der Sicherheitsaspekt, der wichtiger ist als je zuvor, um das Risiko von Datenlecks („*Information Leakage*“ oder „*Information Loss*“) zu minimieren und um die Gefahren der Industriespionage zu bekämpfen. Dabei muss es nicht unbedingt die böse Absicht des Nutzers sein, die derartige Sicherheitsrisiken erhöht. Es reicht schon, wenn Dateien oder Dokumente ohne Verschlüsselung auf mobile Datenträger kopiert werden und der Datenträger in der U-Bahn aus der Tasche fällt.

Da muss also die „alleskönnende“ Software zunächst eine optionale Verschlüsselung anbieten, die für jeden Benutzer einfach zu bedienen, also am besten gleich ins Betriebssystem integriert ist. Noch geschickter ist es zu prüfen, welchem User es erlaubt ist Daten mitzunehmen. Bei dieser Frage müssen viele Optionen durch die Lösung geboten werden, so dass der Kunde geeignet entscheiden kann:

- welche Dateien
  - nach Dateiname und
  - nach Inhalten (z.B. firmenvertraulich) und der Lokation des Inhalts im Dokument (z.B. Header eines Word Dokuments)
- Klartext oder verschlüsselt – und unterscheidbar mit welchen Schlüsseln
  - Schlüssel für die Weitergabe

  - Schlüssel nur für die interne Nutzung (Firmenschlüssel)
- auf welchen mobilen Datenträger
  - ein digitales *Imaging* System (z.B. Kamera versteht keine verschlüsselten jpg)
  - ein selbstverschlüsselnder Datenträger benötigt evtl. keine weitere Verschlüsselung
- mit Protokollierung
- nur auf persönlichen Datenträger

Eine reibungslose, einfache Nutzung sowohl für den Anwender als auch den Administrator zu garantieren, hat wiederum einige Facetten. Zentral definierbare, aber dezentral gültige Policies, die nach Belieben auf die aktuelle Situation – in Echtzeit – angepasst werden können sind eine Grundvoraussetzung. Beim Anwender darf kein Schulungsbedarf entstehen.

Die Lösung

Derzeit ist nur ein Produkt am Markt in der Lage, alle o.g. Risiken und Herausforderungen aus einer Hand erfolgreich abzudecken: Die **itWatch Endpoint Security Suite**, die u.a. alle Funktionen des bekannten **DeviceWatch** enthält. KMU als auch Großunternehmen sowie das Militär und viele staatlichen Institutionen vertrauen seit Jahren darauf. Es ist wenig überraschend, dass die Lösung der **itWatch** alle öffentlichen Ausschreibungen in Deutschland zum Thema Schnittstellenschutz gewonnen hat.

Die **Endpoint Security Suite** der **itWatch** (www.itWatch.de) löst alle skizzierten Herausforderungen und erlaubt das Management selbst größter Netzwerke von zentraler Stelle oder mehreren zentralen Stellen. Am besten erklären sich die vielschichtigen Lösungsmöglichkeiten an einigen realen Beispielen. Nachfolgend werden an einigen Beispielen und Nutzungsszenarien (Use Cases) kurz Lösungsmöglichkeiten skizziert, die das weite Einsatzspektrum und die Effizienz bei der Umsetzung mit der itWatch Endpoint Security Suite belegen.

- **Security Awareness**
  - Datenschutzführerschein – ein Kunde hat eine E-Learning Anwendung „Datenschutzführerschein“ implementiert. Die Nutzung von mobilen Datenträgern ist an die korrekte Beantwortung der Schlussfragen des elektronischen Lernprogrammes gekoppelt. Die Berechtigung wird in Echtzeit geprüft und dadurch ohne manuelle, administrative Prozesse quasi kostenfrei immer korrekt gesetzt. Nebenbei erreicht der Kunde die Compliance Anforderungen nach beweisbarer Wissensprüfung.
  - Zum Nutzungszeitpunkt besonderer Technologien kann beispielsweise automatisch ein Video einspielt werden
    - Einmalig für einen Benutzer
    - Einmal im Vierteljahr
    - Wechselnd mit anderen Awareness Maßnahmen
  - Nachrichtentexte zur Nutzung
    - Vor, nach oder während der Nutzung als
    - Benutzer-Information, -Dialog oder –Hilfe

    - Die Benutzereingaben im Dialog können natürlich protokolliert werden
  - Standortabhängige Reaktionen oder Sprachabhängigkeiten werden berücksichtigt
  - Die Durchführung „sensibler“ Aktionen kann von den sicherheitsrelevanten Umständen (z.B. welches Netzwerk ist angeschlossen?) abhängig erlaubt, verboten oder überwacht werden und an beliebige „Zusatzqualifikationen“ (z.B. Token-Authentisierung) geknüpft werden.
- **Sicherheits Management**
  - „Ich möchte eine Risikoeinschätzung der Ist-Situation für den Einsatz und die Nutzung aller Devices im Netzwerk.“ Die Endpoint Security erlaubt eine Policy mit der Funktion „Nur Monitoring“ und liefert dann zusätzlich zu dem Gerätebestand auch Echtzeitdaten über die Verwendung (Dateien – Lesen und Schreiben, Gerätenutzungsdauer und –häufigkeit etc.).
  - Quota an internationalen Standorten im Vergleich – Werden in China tatsächlich mehr Daten abgezogen als an einem vergleichbaren Standort in Europa? Auf welchen Datenträgern, zu welchen Zeiten? ...
  - Das gesamte „Inventar“, welches real im Netz verwendet wird, liegt in Echtzeit für Analysen vor
    - Alle Applikationen / Anwendungen – neue können einfach übermittelt werden und zur Freigabe oder Sperre in Black oder White Lists übertragen werden
    - Devices Geräte – Schnittstellen, Geräteklassen
    - Dateien, Quotas ...
  - In einem Klinikum ist der im Bereich Röntgen jeder Rechner mit CD/DVD Brennern ausgestattet. Durch die Patternprüfung in XRayWatch wird mit einer einfachen Richtlinie durchgesetzt, dass nur Röntgenbilder eingelesen und geschrieben werden dürfen - Der Kunde kann die vordefinierten Prüfungen erweitern und damit seine „Markierungen“ prüfen (z.B. firmenvertraulich im Word Header)
- **Application Control**
  - Die übliche 80/20 Regel spricht gegen einen flächigen Einsatz von Whitelists. Viele „kleine“ Programme sind auf einigen Rechnern im Unternehmen spontan notwendig. Die Rechner des Außendienstes oder in den Stabstellen sind hier Beispiele. Für diese muss steht ein Blacklisting zur Verfügung, welches in Echtzeit neue Anwendungen an eine zentrale Stelle meldet und zur sofortigen Entscheidung meldet. Die „Latenzzeit“ kann also durch ein SLA definiert werden.
  - Die Anwendung für einen bestimmten Nutzen (z.B. CD Brennen) kann dadurch zentral definiert und überwacht werden.
- **VIP - selbstverantwortliche „erwachsene“ Benutzer verantworten die Nutzung selbst**
  - „Ich möchte, dass meine Mitarbeiter durch technische Maßnahmen unterstützt und nicht gegängelt werden. Dabei

soll trotzdem die Revisionssicherheit der Geschäftsprozesse garantiert werden.

- Die Nutzung kritischer Geräte oder die Verwendung von sensiblen Dateien wird durch einen Nutzerdialog bestätigt – optional ist eine Zustimmung zur „Auditierung“ mit im Text enthalten. Dadurch entsteht eine klare Verantwortungstrennung zwischen den VIP-Nutzer und der IT-Abteilung
- Selbstfreigaben für den „erwachsenen“ oder selbstverantwortlichen Nutzer mit Compliance. Eine Selbstfreigabe gekoppelt an Gruppenzugehörigkeit und der Sensitivität der Aktion mit zentralem Logging der vom Benutzer eingegebenen Begründung für die Selbstfreigabe ermöglicht Compliance und kosteneffiziente Administration. Durch den einzigartigen Plug-In Mechanismus, kann hier eine kundenseitig definierte algorithmische Prüfung – auch eine Authentisierung oder ein Einmalpasswort – integriert werden.

- **Deployment**
  - Sanfter Roll-Out – Benutzer, denen von einem Tag auf den nächsten Berechtigungen entzogen werden, melden sich im Call Center oder beschweren sich. Diesem Problem wird durch einen sanften Roll-out vorgebeugt. Statt vom ersten Tag allgemein genutzte Geräte zu sperren wird ein Nutzungshinweis über das baldige Verbot mit den im Intranet beschriebenen Nutzungsalternativen ausgegeben. So kann man auch kritische Sicherheitsrichtlinien mit Standardprojektorganisation umsetzen.
  - Dadurch gibt bei der Projektkapazität keine „Spitzenbelastungen“ durch unerwartete Benutzerreaktionen.
- **Automatisierung**
  - Fehlerbehebung bei Plug and Play Fehlern – vollautomatisch auf dem PC beim Auftreten des Fehlers – sogar wenn der PC offline ist. Die Probleme der Plug&Play Geräte entziehen sich den Werkzeugen. Administration, Help Desk sollten zeitnah Zugriff auf alle relevanten Infos haben und Standardfehler können sofort und automatisch behoben werden.
  - Automatische Synchronisation mit PDAs - Dienstbeginn des Chefarzt: Alle relevanten Patientendaten der Nachtschicht werden vollautomatisiert mit seinem PDA synchronisiert
  - On Demand Device Driver Management
  - Schwierige Geräteinstallationen (z.B. UMTS-Karten) automatisieren und im Rechteraum der itWatch Endpoint Security durchführen.
  -
- **System Management**
  - Echtzeitmonitor kaskadierend – dadurch wird die Information in Echtzeit an den Bedarfspunkt („Point of Need“) weiter geleitet
    - Netzwerkadministrator sieht alle WLANs, die in Betrieb sind
    - Chief Security Officer sieht die Quota Kennzahlen der Standorte mit den jeweiligen zulässigen Schwellwerten
    - Datenschutzbeauftragte sieht alle versuchten Verstöße gegen die Richtlinie „mobile Datenträger“
    - Helpdesk PnP Fehler in Echtzeit an den Help Desk schicken
  - Frei definierbare Reaktion auf Ereignisse
  - Policy Wechsel in Echtzeit Veränderung der Policy in Echtzeit abhängig von der Situation (z.B. Stand-alone-Nutzung oder im Netz, werktags oder feiertags,)

  - Permanenter Überblick über alle Geräte im Einsatz durch Inventory/Asset Schnittstelle
  - Devicehersteller liefern oft kleine Mehrwertpakete, die in Echtzeit durch einen Event Filter genutzt werden können – z.B. um Fehlersituationen sofort zu beheben
  - Polizei Bayern: siehe http://www.kes.info/archiv/online/BayPolDiFo.html
  - Monitoring / Statistik - sich stets wiederholende Fehlermeldungen statistisch erfassen; statistischer Überblick – z.B. „wie viele Calls pro 1000 Mal anstecken?“
  - Ein Textilhersteller identifizierte in seinem Werk in Thailand, dass der Mitarbeiter, der die Qualitätsdaten über einen mobilen Datenträger von den Messstationen einsammeln sollte immer „langsamer wurde“. Die Verspätung lag daran, dass er in dem auf dem Memory Stick mitgebrachten Spiel immer besser wurde und an jeder Messstation ein „Spielchen wagte“ – natürlich entgegen der Sicherheitsrichtlinie des europäischen Unternehmens. Die Lösung mit Hilfe der Endpoint security der itWatch war ganz einfach. Auf einem speziellen Datenträger werden nun vollautomatisch, außerhalb der Benutzeranmeldung – also ohne Login auf den Messstationen – die Messdaten aufgebracht. Die Zeit der unerlaubten Spiele ist vorbei.
  - Das automatisierte Einsammeln von verschlüsselten Logfiles ohne Zugriffsrechte auf standalone Systemen ist ein häufiger auftretendes Lösungsszenario – z.B. auf Schiffen (die Rechner sind meist nicht vernetzt – trotzdem besteht Bedarf nach Auditing z.B. wegen der Abrechnung der Satelliten-Kommunikation)
- **Kostensenkung**
  - Polizei Bayern 1,2 Mio. EUR Einsparung pro Jahr durch Automatisierung von Geschäftsprozessen
  - Reduktion der Call Kosten durch
  - Weniger Calls
  - Bessere Information
  - Kürzere Reaktionszeiten
  - Reduktion der Management Kosten
  - Qualitätsverbesserung der Services
  - Zentrale 7/24 Services – z.B. kann ein Kunde seine Datentypistenkosten deutlich senken. In der Umgebung fallen an vielen dezentralen Stellen Interviews auf „Voicerekordern“ in MP3 Formaten an. Diese müssen schnellstmöglich abgetippt und in elektronische Dokumente überführt werden. Statt nun dezentral Datentypisten vorzuhalten werden alle MP3-Daten – ohne dass der Benutzer ein Leserecht auf externen Datenträgern hat – automtisch per Email an eine zentrale übermittelt abgetippt und zurückgesendet. Zusätzlich erhält der Kunde jetzt detaillierte Auswertungen und beweissichere Ablaufberichte.
  - CDWatch erwirtschaftet eine Aufwandsrendite von über 200% bei einem ROI von über 160%: http://www.itwatch.de/download/cdwatch-erfahrungsberichtpraxis.pdf
- **Thema „Controlling/Accounting“ - Ausgangssituation:**
  - „Ich möchte den Einsatz meiner Peripheriegeräte nach Nutzungsdauer abrechnen.“

  - Die Endpoint Security der itWatch kann die Nutzungsstrukturen und -häufigkeiten z.B. außergewöhnlich teurer Geräte (Medizin) statistisch erfassen und per Dialog die Eingabe einer Buchungs-/Rechnungsnummer o.ä. verlangen – oder diese algorithmisch erzeugen, um automatisierte Abrechnungsverfahren zu unterstützen.
- **Schutz von Standalone Systemen**
  - In dem RFID Ausweisleser SwissDoc schützt DeviceWatch das System vor Modifikationen der angeschlossenen Geräte (Scanner etc.)
  - In einem Großprojekt aus dem Automotive Bereich unter Führung der DEKRA werden die Prozesse bei dem digitalen Fahrtenschreiber mit der Endpoint Security der itWatch geschützt
- **Verschlüsselung**
  - „Meine Vertriebsmitarbeiter möchten sensible Kundendaten mit einem mobilen Datenträger zum Kunden transportieren und dort übertragen, ohne dass ein Sicherheitsrisiko für die Daten beim Transport besteht. Der Mitarbeiter möchte gleichzeitig auf dem gleichen Datenträger firmenvertrauliche Daten speichern, die der Kunde nicht über eine Angriffssoftware herunterladen kann.“
  - Daten, die mit unterschiedlichen Schlüsseln verschlüsselt sind, können gemeinsam auf einem Datenträger liegen.
  - Benutzerfreundliche Komplexitätsvorgabe der Schlüssel
  - Haftungsübergang durch Voreinstellung „Verschlüsselung“ auch wenn diese nur optional gewählt wird
  - Company Key – und die Daten bleiben im Unternehmen
  - Trivialdaten, z.B. Wegbeschreibungen o.ä. können in Koexistenz zum verschlüsselten Datenmaterial unvesrchlüsselt auf mobilen Datenträgern gespeichert werden.
  - Zielabhängige Wahl der Verschlüsselung: Etwa für „Bildverwertende Geräte“ ist unverschlüsselte Auslagerung zwingend erforderlich!
  - Benutzerfreundliche Bedienung für alle User: Kein Know How von Verschlüsselungssoftware nötig, keine extra Aktion und kein Zeitaufwand nötig, da automatisch in alle Funktionen des Betriebssystems integriert.
  - Mit PDWatch kann jede geltende Firmenrichtlinie, egal ob freizügig oder restriktiv angelegt, umgesetzt werden – abhängig von Dateityp, Dateiinhalt und verwendetem Datenträger können Rechte an Benutzer oder Gruppen vergeben werden (Lesen, Schreiben, Verschlüsselt, Klartext, mit Firmenschlüssel verschlüsselt, mit Audit, nur auf personalisiertem Datenträger)
  - Verschränkung der Inhalte mit der Verschlüsselung verbindet Security und Usability
  - „Back Up/ Recovery“ - „Meine Außendienst-Mitarbeiter müssen in der Lage sein Daten ihrer Notebooks selbstständig wiederherzustellen. Dabei dürfen die sensiblen Daten nicht unverschlüsselt auf den Datenträgern liegen.“
- **Thema „Compliance“ - Ausgangssituation:**
  - GEZ Gebühren für TV-Karten an USB
  - SOX-Compliance erfordert es die lebenswichtigen Daten eines Unternehmens auf allen Wegen beweissicher zu protokollieren
  - Nutzung und Veränderung von Compliance relevanten Information beweisbar protokollieren

- Schulungsinhalte deren Kenntnis die (gesetzlichen) Vorgaben einfordern (z.B. HIPPA), können vor Nutzung beweisbar geprüft werden (siehe auch Datenschutzführerschein)
- Illegale DVD Kopierer erkennen, sperren und melden

Die Landespolizei Bayern, die seit der Einführung von DeviceWatch Kosten aus der automatischen Verarbeitung digitaler Fotos von der Entstehung am Tatort bis zur gerichtlichen Nutzung in Höhe von 1,2 Mio EUR pro Jahr einspart, ist das beste Beispiel, um zu beweisen, dass Endgerätesicherheit ebenfalls durch einen guten ROI überzeugen kann. Vorbei sind die Zeiten, in denen Sicherheitsprodukte sich zu kostentreibende „Monstern" im Betrieb entwickelten; geringe Betriebs- und Ausbildungskosten sowie flexible Prozesse, die sich den aktuell bestehenden Geschäftsprozessen anpassen, statt umgekehrt, zeichen die itWatch Endpoint Security Suite aus.

Fazit

Zwischen den unabhängigen „Welten" Systems Management, IT-Sicherheit, einfache Nutzbarkeit für Endanwender und Administratoren, Compliance und User Awareness können mit der Endpoint Security Suite von itWatch effektive Brücken gebaut werden. Sogar hohe Kosteneinsparpotentiale können ausgenutzt werden. Einfacher Roll-Out mit der automatisierten Integration in alle vorhandenen Prozesse ermöglichen die kosteneffiziente Nutzung.

Die Endpoint Security Suite der itWatch bietet Sicherheit, Usability und SystemsManagement in einem. Überzeugen auch Sie sich von seiner Leistungsfähigkeit und kontaktieren Sie uns unter

Info@itWatch.de oder 089 / 620 30 100.

itWatch GmbH in München
Stresemannstraße 36
81547 München

Quellenangabe:

- Security Awareness
- Einsatzbericht Landespolizei Bayern
- LANline – Daten sicher transportieren
- LANline – User Awareness in Echtzeit

[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