DATA LOSS PREVENTION & ENDGERÄTE SICHERHEIT WAS BRAUCHT MAN WIRKLICH?

ANFORDERUNGEN UND LÖSUNGEN

AUTOR: THORSTEN SCHARMATINAT, KEY ACCOUNT MANAGER ITWATCH GMBH

Daten sind der »Rohstoff« des 21. Jahrhunderts. Datenklau ist ein lukrativer Zweig aktueller Wirtschaftskriminalität – nicht erst seit Millionen für Steuersünder-CDs bezahlt werden und nebenbei die Reputation beteiligter Organisationen geschädigt wird. Daten von bester Qualität haben den höchsten »Wiederverkaufswert«. Für einen Datensatz wird je nach Qualität und Inhalt von ein paar Cent bis hin zu weit über 100 Euro bezahlt. Die Abnehmer und Datenbroker verdienen und sehen gerne über die Strafbarkeit ihres Handelns hinweg. Es gibt Innen- und Außentäter – und Mechanismen, wie man »von außen« den Mitarbeiter zum unbewussten Mittäter macht. Einige dieser Mechanismen gehen immer wieder durch die Presse. Methoden, die gegen den unerlaubten oder nicht gewünschten Abfluss von Daten schützen, werden mit DLP (Data Loss oder Data Leakage Prevention) abgekürzt.

Data Loss, Spionage, Compliance – alles hängt zusammen!

Wirtschaftsspionage wird heute elektronisch betrieben. Die Angriffe werden über Standardsituationen, z.B. PDF-Dateien oder den Browser, eingeschleust, um dann die Unternehmensdaten unbemerkt »nach draußen« zu transportieren. Insofern ist eine gute Informationssicherheit nur erreichbar, wenn man die eingehenden Angriffe abwehrt und den unerwünschten Datenabfluss verhindert. Den zentralen Schutz mittels eines guten Firewallsystems kann man heute voraussetzen. Was häufig noch vernachlässigt wird, sind die Leckagepunkte direkt auf den Endgeräten und das Bewusstsein der Anwender im richtigen Umgang damit. Angriffe über PDF-Dateien nehmen in der Bedrohungsliste von Bitdefender den ersten Platz ein, der Internet Explorer hat eine Schwachstelle, die sofort für Angriffe ausgenutzt wird (ein

sogenannter Zero Day Exploit), selbstverschlüsselnde USB-Sticks sind unsicher – nur drei Meldungen aus einem Monat (Januar 2010), die uns Sorgen machen, weil wir reagieren müssen, denn die genannten Technologien sind in fast jedem Unternehmen im Einsatz. Natürlich treffen alle Unternehmen Vorkehrungen technischer und organisatorischer Natur und fassen diese zu ihrer Sicherheitsrichtlinie zusammen. Ein Auditor oder Prüfer wird diese Sicherheitsrichtlinie, ergänzt um rechtliche Rahmenbedingungen, weniger inhaltlich hinterfragen als vielmehr beurteilen, ob das Unternehmen in der Lage ist diese Richtlinie einzuhalten oder sogar beweisbar umzusetzen, also ob es zu seinen eigenen Vorgaben compliant ist. Dadurch entstehen Anforderungen an Auditing, Shadowing, Monitoring und Forensik. Diese aktuellen Risiken zeigen auf, dass das Sicherheitssystem eines Unternehmens einige Grundeigenschaften benötigt: Monitoring des IST-Zustandes aller »Leckagepunkte« und der Bedrohungen an diesen, Benchmarking der Sicherheitssituation des Unternehmens über Reports, spontane Reaktionsfähigkeit mit Echtzeit-Awareness-Maßnahmen und einer feinen Granularität technischer Maßnahmen (beispielsweise nur PDF auf aktuell neu erkannte schädliche Anteile prüfen). Bei der technischen Umsetzung der Schutzmaßnahmen stellt man fest: die Wirklichkeit erfordert viele Ausnahmen und damit hohe Flexibilität. So sollen z.B. für die VIP-Anwender andere Regeln gelten oder im Außendienst elektronische Willenserklärungen den Haftungsdurchgriff (z.B. KonTraG) in die Geschäftsleitung verhindern, während vertrauenswürdige, aber technisch wenige versierte Anwender nur durch Hinweistexte vor bestimmten Bedrohungen gewarnt werden.

Erster Schritt: Schnelle Projekt-Erfolge – nachhaltige Risikominimierung

Es sieht zu Beginn aus, als müsste man einen Sack Flöhe hüten: Jede Menge Daten, viele Bedrohungen und einige bereits umgesetzte Lösungen stehen organisatorischen Sicherheitsanweisungen gegenüber, die im Zweifel nur halbherzig befolgt werden, aber man hat keine Echtdaten zur Bedrohungslage. Übersicht lässt sich aber verblüffend einfach in das Thema bringen. Zuerst werden die Leckagepunkte identifiziert, die zugleich auch die potentiellen Eintrittspunkte für Angriffe und damit für Wirtschaftsspionage sind:

1. Netzwerkübergangspunkte zwischen privaten (eventuell auch besonders zu schützenden) Netzen und öffentlichen oder einfach angreifbaren Netzen

2. Kommunikationsanwendungen wie Browser und E-Mail
3. Kommunikationsgeräte wie Modems, Netzwerkkarten und Bluetooth
4. Mobile Datenträger wie Memory Sticks, gebrannte DVDs oder externe Festplatten an S-ATA oder SCSI

Deren Verwendung zu protokollieren oder gar zu blockieren bringt aber keine brauchbaren Ergebnisse, denn die Bedrohung liegt ja in der ausgetauschten Information. Protokolliert man jedes ausgetauschte Datenpaket, wird man die Nadel im Heuhaufen nie finden. Deshalb ist es wichtig, in Echtzeit die Spreu vom Weizen zu trennen und nur die interessanten Ergebnisse zu behandeln. Wie zuvor bereits erwähnt, ist es zudem sinnvoll entsprechend des Datenweges, sprich dem Import oder Export von Daten, die Kritikalität bestimmter Muster vorab einzuschätzen, um das Datenvolumen zu begrenzen.

Welche Daten sind »kritisch«?

Einem einzelnen Bit kann man nicht ansehen, ob es vertraulich, verschlüsselt oder öffentlich ist. Ein vertraulicher Inhalt ist als Ausdruck, Teil eines Archives (z.B. ZIP-File), Kopie eines Bildschirms, verschlüsselter Mail-Anhang oder eingebettet in eine Powerpoint-Datei immer noch vertraulich. Beim Etikettieren entsprechend der Kritikalität (z.B. »öffentlich«, »vertraulich« etc.) bringt jeder vollautomatische Prozess Unschärfen mit sich. Selbst wenn die Kritikalität der Datei dann in Echtzeit erkennbar ist, benötigt man für eine korrekte Entscheidung noch die wesentliche Information, in welchem Kontext gerade gehandelt wird. Die echte Entscheidung wird immer situationsbedingt und eingebettet in einen komplexen Prozess sein – deshalb liegen die schnellen Erfolge zum Schutz der Daten nicht im Etikettieren.

Import – Das Einbringen von Angriffssoftware unterbinden

Word- und PDF-Dokumente werden beim Import in das Firmennetzwerk aus der Sicherheitsperspektive eher uninteressant sein – außer sie enthalten eingebettete ausführbare Programme. Diese eingebetteten Programme sind der Grund für die Angriffsmeldungen mittels PDF. Eine gute Patternanalyse – hier z.B. das Modul XRayWatch – kann durch eine intelligente Inhaltsüberprüfung diese eingebetteten Programme erkennen und je nach Notwendigkeit reagieren. Der Schutz muss vollständig sein, also auch in beliebig geschachtelten Archiven oder verschlüsselten Dateien nach diesen Mustern gesucht werden. Sind auf mobilen Datenträger aber dazu noch portable Anwendungen vorhanden, dann kann jeder Anwender diese ohne administrative Rechte ausführen, und die potentielle Schadsoftware ist im Firmennetz angekommen. Wegen des fehlenden Installationsvorganges helfen traditionelle Anwendungsinventarisierungen hier nicht und somit tauchen diese Arten von Anwendungen nie im Softwarekatalog auf und hinterlassen auch sonst keine Spuren auf dem Rechner. Nur Werkzeuge, welche in Echtzeit alle Programme melden, deren Ausführung versucht wurde, lösen dieses Problem ohne großen administrativen Aufwand.

Export – die Mitnahme von Daten sauber regulieren

Es gilt zu definieren, wer welche Daten in welcher Form (verschlüsselt oder unverschlüsselt) auf welchem Datenträger bzw. durch welche Kommunikationsanwendung »nach draußen« mitnehmen oder senden darf. Für eine gute Entscheidung in Echtzeit benötigt man darum die wesentliche Information, in welchem Kontext gehandelt wird:

- Ein Backup lokaler Daten, das mit einem nur innerhalb der Firma verwendbaren Unternehmensschlüssel verschlüsselt ist, ist okay,
- das Mitnehmen dieser Daten mit einem Transportschlüssel durch einen Auszubildenden soll aber verhindert werden.

Die Entscheidung wird also von dem Anwender, von den verwendeten Anwendungen und Datenträgern sowie der Situation abhängen.

Die letzte Bastion: der Anwender

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 lokal gültigen Datenschutzgesetzen wie (Euro)SOX und HIPPA, gibt es viele weitere Vorschriften, die in Teilen oder im gesamten ITMarkt zu berücksichtigen sind. Mitunter stehen sich Anforderungen an die Beweisbarkeit mit Themen des Datenschutzes scheinbar unvereinbar gegenüber. Letztendlich überlagern sich darum standardisierbare und individuelle Anforderungen an die Sicherheit zu einem unternehmensspezifischen Anforderungsprofil. Als entscheidender Faktor kommt zudem die Unternehmenskultur hinzu, da das Unternehmen in der Umsetzung der Aufgabenstellung mit technischen und organisatorischen Lösungen einen individuellen Weg finden wird. In der Praxis heißt das, die richtige Lösung zwischen dem »selbstverantwortlichen Benutzer« mit allen Freiräumen und dem möglicherweise ungeschulten »Normalnutzer« zu finden. Fast jeder Verantwortliche für die IT-Sicherheit kennt das Dilemma: Entweder die IT-Sicherheit leidet, weil nicht jeder Mitarbeiter auf jede kritische Situation innerhalb der Verwendung seiner IT geschult werden kann, oder die Mitarbeiter sind unzufrieden, weil prophylaktisch alles verboten ist und sie sich durch »die Sicherheit« in Ihrer Entscheidungsfreiheit und Produktivität eingeschränkt sehen.
Ein Anwender, dem man höhere Rechte im Umgang mit (oder hier zur Mitnahme von) sensiblen Daten einräumt, sollte also verstehen was er tut. Dieses Wissen zur IT-Sicherheit vermittelt man häufig in sogenannten Security Awareness Programmen. Das Wissen des Anwenders und die technisch umgesetzten Regeln zur IT-Sicherheit sollten voneinander profitieren. Sinnhaft ist es, den Anwender in Echtzeit auf die

Risiken seines Handelns, die geltende Richtlinie und Möglichkeiten des sicheren Handelns aufmerksam zu machen, kritische Aktionen technisch zu überwachen und bei Bedarf den Anwender vor der kritischen Aktion online zu schulen. Die Compliance des Unternehmens wird dadurch beweisbar, denn die relevanten Aktionen des Anwenders werden protokolliert oder sogar als elektronische Willenserklärung revisionssicher gespeichert.
Darum muss man je Benutzer fragen: Wie eigenständig 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. Alles zusammen spiegelt dann die Sicherheitskultur des Unternehmens wieder.

Bestimmung des Freiraumes

Ein Datentypist, der einen Arbeitsüberhang, evtl. in einem Zeitarbeitsverhältnis, abarbeitet, wird weniger Verständnis für die Vertraulichkeit der Daten haben als ein 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 in der Firma verbleiben sollten, z.B. durch eine Verschlüsselung mit einem Unternehmensschlüssel.

Abb. 1: Echtzeit-Kommunikation zwischen Nutzer und Sicherheitsprogramm

Bei Benutzern mit einer hohen Bindung an das Unternehmen, ausgereiftem technischen Wissen 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.

Im Dialog mit dem Anwender – nicht gegen ihn

Natürlich kann es einen guten Grund dafür geben im Hotel spontan ein sicherheitskritisches USB-Gerät einzusetzen. Für solche Ausnahmen lohnt es sich natürlich nicht, einen 24/7-Service zur Gerätefreigabe oder Richtlinienänderung vorzuhalten. Lösungen der Endgerätesicherheit sollten hier verschiedene kosteneffiziente Verfahren anbieten. Eine einfache Möglichkeit für den selbstverantwortlichen Benutzer liegt z.B. im folgenden Dialog:

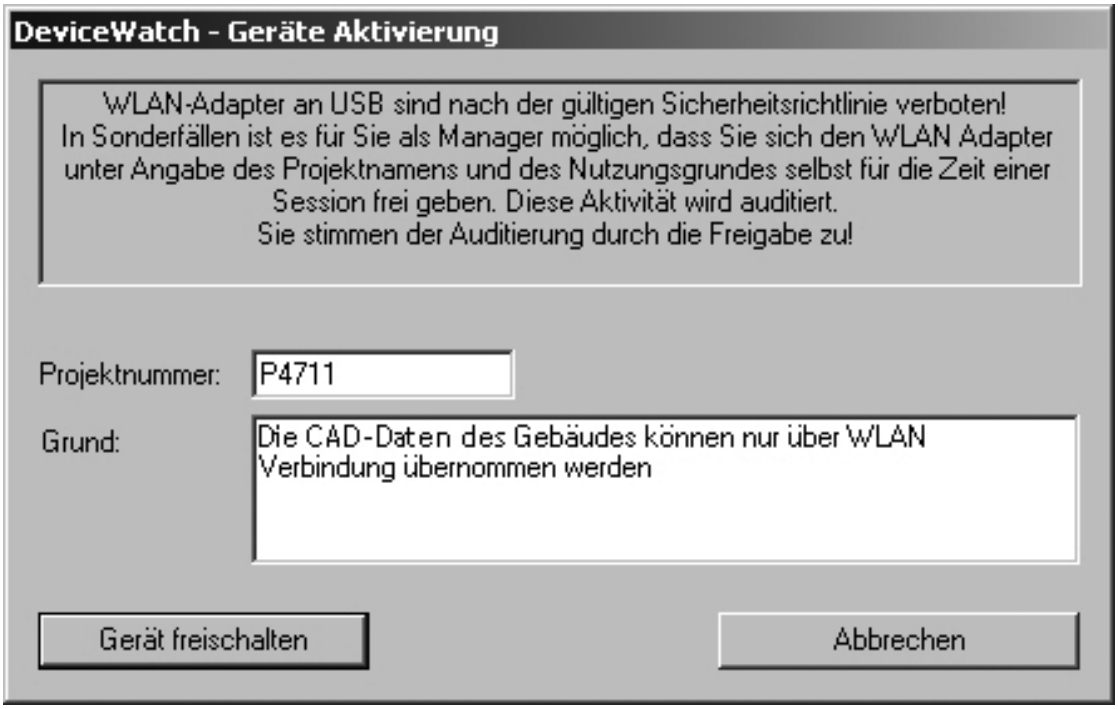

Abb. 2: In vielen Fällen ist für die VIP Anwender oder den Außendienst eine Selbstfreigabe gegen Monitoringauflage der beste Weg.

Der Benutzer kann durch Eingabe eines gültigen Projektnamens das benötigte Gerät eigenverantwortlich frei geben – unterliegt dann aber einer detaillierten Protokollierung, der er selbst per elektronischer Willenserklärung revisionssicher zustimmt. Was für den angemeldeten Benutzer als »gültiges Projekt« gilt, kann der Kunde jeweils selbst definieren. Dazu ist die Einbringung eines eigenen Algorithmus als Plug-In ein guter Weg. Natürlich erscheint der vom Benutzer eingegebene Text im zentralen Logging, welches die Revisionssicherheit und Compliance garantiert. Der Text im Dialogfeld ist ebenfalls frei vom Kunden definierbar. So können zum

Beispiel auch Daten für die Abrechnung von Services in Echtzeit erfasst werden. Der Dialog ist dabei schon etwas für fortgeschrittene Anwender, die nach vorab definierten Prozessen vorgehen. Natürlich sind auch selbst definierte Nachrichtentexte, Links auf Online-Schulungen oder Awareness-Informationen wie etwa hinterlegte Videos denkbar. Der Kunde entscheidet zudem, ob die Freigabe der kritischen Aktion sofort oder auch abhängig von der Situation bzw. dem Kenntnisstand des Benutzers verzögert werden soll. So kann z.B. der Einsatz eines Massenspeichers so lange herausgezögert werden bis der Benutzer die Datenschutz-Information gelesen hat und dieser zugestimmt hat. Natürlich will man dem Benutzer nicht vor jedem Einsatz seines Memory Sticks die gleiche Nachricht oder denselben Videoclip als Info anbieten. Darum sollte die Häufigkeit der Aktion je Benutzer, je PC oder nach anderen algorithmischen Parametern beliebig frei definierbar sein. Einer automatischen und beweissicher gespeicherten, vierteljährlichen Belehrung, wie sie z.B. in HIPAA gefordert ist, steht dann nichts mehr im Wege.

Die Herausforderungen

Wir übernehmen die vorgenannte Unterteilung der Angriffspunkte und diskutieren deren wirksamen Schutz in heutigen Infrastrukturen.

1. Netzwerkübergangspunkte zwischen privaten (eventuell auch besonders zu schützenden) Netzen und öffentlichen oder einfach angreifbaren Netzen
2. Kommunikationsanwendungen
3. Kommunikationsgeräte
4. Mobile Datenträger

1. Netzübergänge

Die Netzwerkübergabepunkte werden heute mit mehrstufigen Firewallsystemen sehr gut abgesichert. Da diese Technik seit vielen Jahren stabil ist und zu der Umsetzung in fast allen Unternehmen Know-how vorhanden ist, sollte man auf diese Technik bauen. Das heißt natürlich zum einen die Schutzmaßnahmen immer aktuell an die bekannte Bedrohungslage anzupassen und diese Disziplin im Risikomanagement des Unternehmens zu verankern. Zum andern sollte man sich aber genau dieses Vorgehen als »Vorbild« oder Blaupause für alle anderen Kommunikationsbeziehungen nehmen. Daraus resultiert dann, dass man die auf den Firewalls etablierten Regeln an allen anderen Schnittstellen umsetzt, aber auch, dass man alle Bedrohungsszenarien an diesen Schnittstellen in das Risikomanagement des Unternehmens mit aufnimmt.

2. Kommunikationsanwendungen

Die Anwendungen, die über IP kommunizieren, wie z.B. Browser oder Email, laufen meist über die Firewall und werden dort durch Applikationsfilter geeignet geschützt. Kritisch sind verschlüsselte Daten, da diese zum einen wegen der geltenden Datenschutzrichtlinien nicht entschlüsselt werden dürfen oder es zum anderen auch technisch oft ohne Kenntnis des geeigneten Schlüssels und des angewendeten Verfahrens gar nicht möglich ist. Dieses verbleibende Restrisiko kann man über eine geeignete Endgerätesicherheit schließen, da auf dem Endgerät direkt vor der Verwendung der Daten diese auf jeden Fall entschlüsselt und somit im Klartext vorliegen werden.

3. Kommunikationsgeräte und Kommunikationsschnittstellen

Die Sicherheitsdefizite durch die generische Plug&Play-Pforte für kommunizierende Peripheriegeräte wie Modems, WLAN, externe Netzwerkkarten etc. an den Geräteschnittstellen wie USB, PC-Card, Firewire, Bluetooth, Infrarot etc. sind seit langem bekannt. Unerwünschte Geräte bedrohen nicht nur die Integrität der Netze, sondern es kann auch entscheidendes Unternehmenswissen unerkannt abgezogen und vervielfältigt werden. Zu den Interessen aus der IT-Sicherheit kommen zudem noch die Anforderungen des Betriebes nach Effizienz und Kostensenkung sowie die Notwendigkeit, den Benutzer bei komplexeren Einsatzszenarien zu unterstützen. Diese als Gerätekontrolle oder Device Control bezeichnete Thematik ist ein Teil der gesamten Endgerätesicherheit.

4. Mobile Datenträger

Gerätekontrolle ist natürlich nicht nur auf die kommunizierenden Geräte beschränkt, sondern beschäftigt sich auch mit denen, die lokale Dienste erbringen, allen voran mobile Datenträger wie (gebrannte) CDs/ DVDs, Memory Sticks, USB-Platten, ZIP-Drives, externe Festplatten an S-ATA oder SCSI , SD- und sonstige Speicherkarten und viele mehr.

Endgerätesicherheit

Das Thema der Endgerätesicherheit (Endpoint Security) ist viel breiter als nur eine effiziente Zugangskontrolle für jedwede Geräteschnittstelle zu realisieren. In der Folge führen wir eine Bestandsaufnahme durch, was eine umfassende Lösung für die Endgerätesicherheit heute alles leisten muss:

• **Antivirus** – die klassische Disziplin ist auf fast 100% aller Endgeräte heute bereits implementiert und muss nicht weiter im Detail behandelt werden.

• **Gerätekontrolle** – Wer darf welches Gerät, egal ob Peripheriegerät oder fest verbaute Hardware wann, wo und wofür nutzen? Natürlich darf für eine neue Geräte- oder Schnittstellenklasse kein Update vom Hersteller nötig werden, da zu beliebigen Zeitpunkten neue Geräte in Betrieb genommen werden sollen, ohne, dass ein Softwareupdate nötig wird.

• **Verschlüsselung mobiler Datenträger** – Die Verfahren der Vergangenheit, wie etwa Partitionsverschlüsselung, haben zunehmend ausgedient, da der Bedarf an Vertraulichkeit immer mehr von den Dateiinhalten und ihrer Sensitivität abhängt und damit nicht mehr alle Daten einheitlich klassifiziert und behandelt werden können. Auch die einfache Verwendbarkeit auf beliebigen Drittsystemen ist eine wesentliche Anforderung, weshalb aus Sicht der Sicherheit ein einziger Schlüssel für alle Daten auf einem Datenträger wegen der Existenz sogenannter USB-Dumper kritisch ist – wie generell die vollständig transparente Entschlüsselung auf unsicheren Systemen ein Sicherheitsrisiko darstellt. (Siehe auch Infografik rechts)

• **Personalisierung von Datenträgern** – Günstige Datenträger verfügen über keine eigenen Merkmale wie Seriennummern. Die Nutzung von Datenträgern in besonders kritischen Bereichen (Vorstand, Akquisition, Stabsabteilungen etc.) erfordert aber aus Gründen der Compliance wesentliche Datenbewegungen beweisbar abzulegen. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier also Voraussetzung.

Info:

Anforderung Verschlüsselung mobiler Datenträger

Je nach Sicherheitskultur des Unternehmens und des angemeldeten Anwenders gilt es eine optionale oder zwangsweise Verschlüsselung anzubieten, die für jeden Benutzer einfach zu bedienen, also am besten gleich ins Betriebssystem integriert ist. Noch geschickter ist es zu prüfen, welchem Nutzer 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 nach extern
  - Schlüssel nur für die interne Nutzung (Firmenschlüssel)
- auf welchen mobilen Datenträger
  - ein digitales Imaging System,z.B. verstehen Digitalkameras keine verschlüsselten jpg-Dateien)
  - ein selbstverschlüsselnder Datenträger benötigt evtl. keine weitere Verschlüsselung
- mit Protokollierung
- nur auf persönlichen Datenträger

• **Kontrolle der Anwendungen** – Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von Whitelists und Blacklists. Exploits von Kommunikationsanwendungen können nur dann sinnvoll unterbunden werden, wenn diese Anwendungen in einem eigenen, restriktiven Rechteraum laufen und die Rechte des Anwenders nicht missbrauchen können.

• **Protokollierung aller sicherheitskritischen Aktionen** – Unabhängig davon, ob es um die Verwendung risikobehafteter Hardware oder Geräte, um den Austausch sensibler Dateien oder das Verwenden von problematischer Software geht, 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 zudem zwingend; insbesondere, wenn die gesamten Dateninhalte und nicht nur die Dateinamen protokolliert werden müssen, um beispielsweise Auflagen der Langfristarchivierung trotz der Verwendung von mobilen Datenträgern zu erfüllen.
• **Kontrolle der verwendeten Netze** – Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung alle 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 oder Prozesse, 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. Im besten Fall lässt sich ein Sicherheitsbenchmark der Endgeräte als Ausgangspunkt für das Risikomanagement darstellen.

Diese Anforderungen an die Endgerätesicherheit sind darüber hinaus immer alle in Echtzeit, an allen Geräteschnittstellen, 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 innovativer mobiler Lösungen rund um die Peripheriegeräte ausrichten. Mobile Datenträger haben darum in den IT-Umgebungen auf Basis von Innovationsdruck und Kosteneffizienz mittlerweile ihren festen Platz. Doch diese unüberschaubare Anzahl neuer Geräte im Netzwerk will geplant, verwaltet, organisiert und nicht zuletzt in die Standardprozesse der IT integriert werden. Windows-Bordmittel sind für die IT-Abteilungen der Unternehmen

keine große Hilfe und so gibt es im Markt zunehmend mehr Produkte zur Security und zum Systems Management, die allerdings häufig jeweils nur einen Teil der Problematik abdecken. Auch die von Microsoft vorgestellten Betriebssysteme Windows 7 oder Windows 2008 Server bieten hier noch keine zufriedenstellende Lösung an, da bestimmte Verfahren vollständig fehlen und andere in der zentralen Steuerung nicht granular genug sind.

Spannungsfeld der IT-Manager

Um sich der Materie zu nähern, muss man zunächst das Spannungsfeld verstehen, in dem sich der IT-Manager befindet. Diese zuvor beschriebenen »volatile« Peripheriegeräte und die wachsende Anzahl kabelloser Schnittstellen kommen zu den »festen« Geräten wie Maus, Tastatur und Drucker in einem Ausmaß hinzu, wie es 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 in der Vergangenheit. Abgebrochene Installationen und Konfigurationsfehler müssen ebenso leicht erkennbar und vor allem behebbar sein wie die Integration in die Standardprozesse wie z.B. Beschaffung, Auslieferung, Freigabe, Validierung, Berechtigung. Der Helpdesk, nun mit einem deutlich höheren Aufkommen an

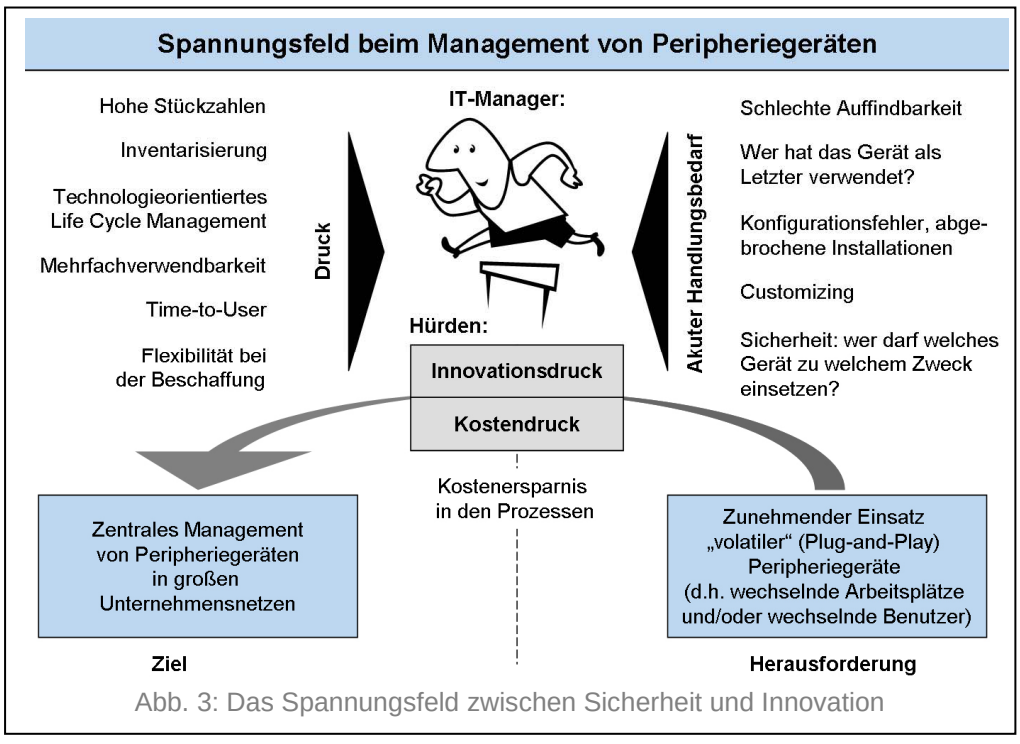

Abb. 3: Das Spannungsfeld zwischen Sicherheit und Innovation

Anfragen konfrontiert, muss seine Beantwortungszeit entscheidend verkürzen und ist dabei auf die Mehrfachverwendbarkeit von automatisierten Lösungen angewiesen, wie z.B. die »on-demand« Treiber-(Nach-)Installation.

In Zeiten organisierter Angriffe auf Firmeninformationen aus Drittstaaten darf neben der Betrachtung des reinen System Management der Sicherheitsaspekt nicht vernachlässigt werden, der wichtiger ist als je zuvor, um das Risiko von Datenlecks 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.

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 reines Blockieren und Protokollieren hinausgehen. Die Produkte aus der Sicherheitswelt haben aber fast alle keine Mehrwerte im Systems Management.

Fehler in DLP Projekten vermeiden

Wie kann man also effizient den Abfluss von Daten unter Einhaltung aller Vorschriften und der Unternehmens-Compliance unterbinden? Endpoint Security Produkte, die die aufgezeichneten Herausforderungen zu Gunsten der Produktivität des Unternehmens lösen sind ein Schlüsselelement. Es ist hier notwendig zu erkennen, dass eine Lösung des Problems »Datenverlust durch Mitarbeiter oder Außentäter« immer aus mehreren Komponenten besteht:

1. Dem Mitarbeiter, der die Unternehmensinteressen kennt und in adäquate Handlungen umsetzt,
2. einem technischen Werkzeug, welches die Bewusstseinsbildung beim Mitarbeiter unterstützt, die potentiellen Leckagepunkte am Endgerät blockieren, monitoren und verschlüsseln kann und
3. Definitionen über die Sensitivität von Dokumenten.

Viele Projekte scheitern daran, dass man im ersten Schritt zu viel will, weil eine Projektlaufdauer von mehreren Jahren ohne signifikante schnelle Gewinne für das Unternehmen in der heutigen Zeit kaum akzeptabel ist. Außerdem können die »Ausnahmen« zu häufig und damit zu teuer in der manuellen Administration werden oder die Sicherheitsrichtlinie nur aus Schlupflöchern bestehen und damit ihr Geld nicht wert sein.

Fallen vermeiden – Die häufigsten Fehler in DLP-Projekten

1. Alle vorhandenen Daten nach deren Kritikalität zu markieren kostet viel Zeit und Energie – und man muss lange auf positive Resultate warten. Das eigentliche Ziel, den unerlaubten Datenabfluss unterbinden, rückt in weite Ferne.
2. Die systembedingten Ungenauigkeiten in der Klassifikation führen im Betrieb zu falschen Entscheidungen (false positive und false negative) auf. Entweder bessert man im Betrieb häufig nach und generiert somit hohe administrative Kosten, oder stellt die Schutzkriterien so lax ein, dass das Ergebnis den Aufwand nicht mehr lohnt. Der Unmut über diese Ungenauigkeiten steigt über die Zeit und gefährdet den Erfolg des Projektes.
3. Häufig wird erst über die oben erwähnten Angriffe auf Schwachstellen von Standardanwendungen (Internet-Explorer Exploit) oder –formate (PDF-Exploit) ungewollt ein Datenkanal nach außen geöffnet. Der Angriff kommt aber von außen, weshalb es zu einer Aufgabe des DLP gehört den »Import von schädlichen ausführbaren Objekten« zu kontrollieren oder ganz zu verbieten (z.B. Java-Skript in PDF, DLL-Download über Browser etc.).

Best Practice, Phase 1

Einfache, weil im Betrieb unkritische Sicherheitsmaßnahmen, werden zuerst implementiert und schaffen schon nach wenigen Wochen schnelle Erfolge, sogenannte Quick Wins. Dazu protokolliert man – ohne die Daten der handelnden Benutzer zu erheben – die potentiellen Leckagepunkte, wie etwa Netzkontaktpunkte und lokale Kontaktpunkte über Kabel oder Luftschnittstelle (Bluetooth, WLAN...), kommunizierende Anwendungen (Email, Browser...) und mobile Datenträger (Memory Sticks, Firewire-Platten, gebrannte DVDs...). Die Schutzmaßnahmen im ersten Schritt beeinflussen den Betrieb nicht: Benutzersensibilisierung, Monitoring und damit verbunden das Alerting stehen an erster Stelle. Diese Maßnahmen erlauben die Kritikalitätseinschätzungen im weiteren Verlauf iterativ zu verfeinern. Die Untersuchung der statistischen Auswertungen des Monitorings zeigt die realen Risiken und pragmatische Verstöße gegen die bestehenden Vorschriften auf. Bereits nach dieser ersten Phase, die mit wenigen Arbeitsstunden erledigt ist, kann man klare Antworten auf die drängende Frage »Wie sicher sind wir?« geben.

Best Practice, weitere Schritte

Auf dieser Information basieren die regelmäßigen Verfeinerungen der technischen Sicherheitsmaßnahmen, z.B. Blockade und Zwangsverschlüsselung, die erst sukzessive in die jeweils adäquate Reaktion münden. Je nach Applikation, Netzwerk, Datenträger, handelndem Benutzer und natürlich identifiziertem Dateninhalt werden folgende Maßnahmen erzwungen: Verschlüsselung mit Firmenschlüssel oder

persönlichem Schlüssel, bewusstseins- oder wissensbildende Informationen über das konkret identifizierte Risiko an den Anwender in Echtzeit, revisionssichere Beweiserhebung – bei Bedarf mit gespeicherter elektronischer Willenserklärung für einen Haftungsübergang – oder auch eine Blockade der Aktion. Eigene algorithmische Prüfungen und solche von Drittprogrammen sollten eingebunden werden können, so dass eine Sequenz voneinander abhängiger Prüfungen nach unterschiedlichen Kriterien entsteht.

Alternativen zur Klassifikation einzelner Dateien

Wie oben beschrieben ist das Ziel jede einzelne Datei in allen »Daseinsformen – auch auszugsweise – mit dem richtigen Etikett zu versehen, was in größeren Netzen unrealistisch ist, da sich die Durchmischung der Daten nicht sinnvoll einschränken lässt. Eine bessere Lösung ist die Virtualisierung in Subnetzen. Mit klassischen Verfahren wie CITRIX® oder Terminalserver lassen sich Daten von höherem Schutzbedarf zu Datenclustern zusammenfassen, die in separierten Netzen liegen. Der Zugriff in diese Netze kann nach dem Verfahren »Read up – No write down« gesteuert werden. Die Zugriffsroutinen in diese Netze finden dann authentisiert statt. Mit den in diesem Artikel beschriebenen Verfahren des Applikationsschutzes sind dann die Zugriffsclients in diese Netze geeignet geschützt, so dass weder deren Konfiguration verändert werden kann noch die sensiblen Daten unerlaubt ausgelesen oder kopiert werden können.

Die Lösung

»Dynamische Security«
So flexibel wie Ihr Unternehmen ist, so sollte sich auch Ihre Security Policy in Echtzeit Ihren Bedürfnissen anpassen. Kenntnisstand des Mitarbeiters, Verwendung des Notebooks im Haus, offline, an WLAN oder im Home Office beeinflussen den gültigen Freiraum. Wird die Situation in Echtzeit erkannt, kann die gültige Richtlinie ereignisgetrieben vollautomatisch gewechselt werden und die Risiken sind gebannt. So werden verschiedene Welten für den Kunden gewinnbringend zusammengeführt:

1. Das Wissen des Endanwenders um die Sensitivität einer Datei,
2. das Wissen der zentralen IT um Richtlinien, die Sicherheit von Datenträgern und Prozessen, sowie vertrauenswürdige Benutzergruppen und eigenverantwortlich handelnde Mitarbeiter,
3. die Investitionen in Security Awareness Maßnahmen kommen in Echtzeit an den Nutzungspunkt,
4. die intern geklärte Haftungsfrage und Haftungsübergänge,
5. die aktuelle Gesetzeslage,

6. technisch umgesetzte Compliance-Anforderungen, die mit geeigneter Information in Echtzeit an den Benutzer kommuniziert und dabei revisionssicher abgelegt werden.

Sicherheitsziele können also durch

1. proaktiven Schutz mit Verboten,
2. 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. Die Sicherheitsziele binden immer alle Leckagepunkte gleichermaßen ein.

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.

Abb. 4: Das Spannungsfeld des IT-Managers zwischen Gesetz,

Compliance, Vertrauen und Wünschen

Wir möchten eine mögliche Lösung mittels eines konkreten Produktes in Stichpunkten skizzieren. Die Endpoint Security Suite der itWatch, die wir hier für eine exemplarische Lösungsumsetzung gewählt haben, um mit zentral definierbaren, aber dezentral gültigen security policies eine reibungslose, einfache Nutzung sowohl für den Anwender als auch den Administrator zu garantieren, kann die gültige Sicherheitsrichtlinie bei Bedarf zudem in Echtzeit an die Situation anpassen. In verschiedenen Umgebungen erbringt die Security Suite die angegebenen Leistungen schon seit Jahren und bietet so auch Handlungssicherheit. KMU als auch Großunternehmen sowie das Militär und viele staatlichen Institutionen vertrauen seit Jahren auf dieses Werkzeug aus deutscher Produktion.

Security Awareness – Sicherheitsbewusstsein schaffen

- 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 aktuellen 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
    - Bestätigungen des Anwenders sind revisionssicher als elektronische Willenserklärung hinterlegt
- 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 darüber hinaus an beliebige »Zusatzqualifikationen« (z.B. Token-Authentisierung) geknüpft werden.

Sicherheits Management

- Der Kunde möchte eine Risikoeinschätzung der Ist-Situation für den Einsatz und die Nutzung aller Geräte 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 »Risiko-Inventar« 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
    - Geräte nach Schnittstellenart, Geräteklassen, etc.
    - Dateien, Quotas, etc.
- 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 nach DICOM Standard 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, z.B. auf denen des Außendienstes oder der Stabstellen. Für diese steht ein Blacklisting zur Verfügung, welches in Echtzeit neue Anwendungen an eine zentrale Stelle und zur sofortigen Entscheidung meldet. Die »Latenzzeit« kann also durch ein SLA definiert werden.
- Die Anwendung für einen bestimmten Einsatzzweck, wie etwas das CDBrennen, kann so 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 ITAbteilung.
-

Abb. 5: So oder ähnlich könnte der VIP-Nutzer die Selbstfreigabe erleben

- Selbstfreigaben für den selbstverantwortlichen Nutzer gemäß 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 (n-Mal Nutzung oder Übergangszeit) mit den im Intranet beschriebenen Nutzungsalternativen ausgegeben. So kann man auch kritische Sicherheitsrichtlinien mit Standardprojektorganisation umsetzen.
- So gibt es bei der Projektkapazität keine »Spitzenbelastungen« durch unerwartete Benutzerreaktionen.

Automatisierung

- Fehlerbehebung bei Plug&Play-Fehlern erfolgt vollautomatisch auf dem PC beim Auftreten des Fehlers, sogar, wenn der PC offline ist. Administration und Help Desk sollten zeitnah Zugriff auf alle relevanten Infos haben, aber Standardfehler können direkt und automatisch behoben werden.
- Automatische Synchronisation mit PDAs, z.B. beim Dienstbeginn des Chefarztes: 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 erhält in Echtzeit alle Plug&Play-Fehler
- Frei definierbare Reaktion auf Ereignisse
- Policy-Wechsel & Veränderung der Policy in Echtzeit, abhängig von der Situation wie z.B. Stand-Alone-Nutzung oder im Netz, werktags oder feiertags
- Permanenter Überblick über alle Geräte im Einsatz durch Inventory/Asset Schnittstelle
- Gerätehersteller liefern oft kleine Mehrwertpakete, die in Echtzeit durch einen Event Filter genutzt werden können, um z.B. Fehlersituationen sofort zu beheben
- Polizei Bayern setzt die Sicherheitsanforderungen aus der Justiz für die digitalen Fotografien der Tatorte durch einen sicheren Prozess um: siehe http://www.kes.info/archiv/online/BayPolDiFo.html
- Monitoring & Statistik – statistischer Überblick über sich stets wiederholende Fehlermeldungen oder Fragestellungen wie »Wie viele Calls pro 1000 Mal anstecken eines Plug&Play Devices?«
- 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 itWatch Endpoint Security war ganz einfach: Auf einem speziellen Datenträger werden die Messdaten nun vollautomatisch, außerhalb der Benutzeranmeldung, sprich ohne Login auf den Messstationen, aufgebracht. Die Zeit der unerlaubten Spiele ist vorbei.
- Das automatisierte Einsammeln von verschlüsselten Protokolldateien ohne Zugriffsrechte auf Stand-Alone-Systemen ist ein häufiger auftretendes Lösungsszenario, z.B. auf Schiffen (die Rechner sind meist nicht vernetzt – trotzdem besteht Bedarf nach Auditing etwa wegen der Abrechnung der Satelliten-Kommunikation).

Kostensenkung

- Polizei Bayern erzielt 1,2 Mio. EUR Einsparung pro Jahr durch Automatisierung von Geschäftsprozessen
- Reduktion der Call Kosten durch
    - weniger Anrufe,
    - bessere Information,
    - kürzere Reaktionszeiten,
    - Reduktion der Managementkosten und
    - Qualitätsverbesserung der Services.
- Zentrale 24/7-Services – 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 Erzeuger der MP3-Datei ein Leserecht auf den Datenträgern hat – automatisch per Email an eine Zentrale übermittelt, bearbeitet und zurückgesendet. Der Kunde kann damit seine Kosten deutlich senken und erhält zusätzlich detaillierte Auswertungen und beweissichere Ablaufberichte.
- CDWatch erwirtschaftet eine Aufwandsrendite von über 200% bei einem ROI von über 160%.

Controlling/Accounting

- Der Kunde möchte den Einsatz seiner Peripheriegeräte nach Nutzungsdauer abrechnen: Die Endpoint Security der itWatch kann die Nutzungsstrukturen und -häufigkeiten, z.B. außergewöhnlich teurer Geräte in der Medizin, statistisch erfassen und per Dialog die Eingabe einer Buchungs-/Rechnungsnummer o.ä. verlangen bzw. diese algorithmisch erzeugen, um automatisierte Abrechnungsverfahren zu unterstützen.

Schutz von Stand-Alone-Systemen

- In dem RFID-Ausweisleser »SwissDoc« schützt DeviceWatch das System vor Modifikationen der angeschlossenen Geräte wie Scanner etc.
- Bei einem Großprojekt im Automotive Bereich unter Führung der DEKRA werden die Prozesse bei dem digitalen Fahrtenschreiber mit der Endpoint Security der itWatch geschützt.

Verschlüsselung

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 – Die Lösung: 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 (Firmenschlüssel) – und die Daten bleiben im Unternehmen
- Trivialdaten, z.B. Wegbeschreibungen o.ä.
- können in Koexistenz zum verschlüsselten Datenmaterial unverschlüsselt auf mobilen Datenträgern gespeichert werden.

- Zielabhängige Wahl der Verschlüsselung: Etwa für »Bildverwertende Geräte« ist unverschlüsselte Auslagerung zwingend erforderlich.
- Benutzerfreundliche Bedienung für alle User: Kein Knowhow von Verschlüsselungssoftware nötig, keine Extraaktion und kein Zeitaufwand nötig, da automatisch in alle Funktionen des Betriebssystems integriert.
- Mit PDWatch kann jede geltende Firmenrichtlinie, egal ob freizügig oder restriktiv angelegt und 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.«

Compliance

- Vermeidung von 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-relevanter Information beweisbar protokollieren
- Schulungsinhalte, deren Kenntnis die (gesetzlichen) Vorgaben einfordern, können vor Nutzung beweisbar geprüft werden (siehe auch Datenschutzführerschein)
- Illegale DVD Kopierer erkennen, sperren und melden

Fazit

Entwickeln Sie in Ihrem Unternehmen eine Sicherheitskultur und halten diese in einfacher Weise mit zentral definierten Maßnahmen aktuell ohne die Benutzer zu »gängeln«. In Echtzeit und nur, wenn ein Bedarf am Nutzungspunkt besteht, durchläuft der Benutzer die gewünschten wissensbildenden und/ oder juristisch relevanten Vorgänge und erteilt bei Bedarf seine Zustimmung zu besonderen Maßnahmen, welche revisionssicher und in der Häufigkeit algorithmisch steuerbar sein sollten. Es resultiert ein Projektvorgehen, welches in kleinen Schritten sofort schnelle Erfolge aufzeigt und die aktuelle Risikomatrix gleich mitliefert, so dass die nächsten Schritte entlang der tatsächlich identifizierten Bedrohungen implementiert werden. 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: Ein einfacher Roll-Out mit der automatisierten Integration in alle vorhandenen Prozesse ermöglicht die kosteneffiziente Nutzung.

Quellenangabe

- Projektbericht Landespolizei Bayern »Sichere IT-Umgebung für digitale Tatortfotos«: 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; http://www.kes.info/archiv/ online/BayPolDiFo.html

- LANline 08/2006, S.66 ff. – Artikel »Daten sicher transportieren«
- LANline 11/2007, S 48 ff. – Artikel »Security Awareness in Echtzeit«
- Professional Computing 02/2008, S 16, Artikel »Null Administration – Volle Sicherheit«
- LANline 05/2008, S. 28 ff – Artikel »Gesetz und Compliance sind nicht alles: Unternehmenskultur als Faktor der IT-Sicherheit«
- itWatch White Paper 12/2009: »DLP – Ist jeder Anfang schwer?, Erfahrungen und kurzfristige Lösungsmöglichkeiten«
- eGovernment 03/2010, S. 17 – Artikel »Schutz der öffentlichen Daten: Schnelle Projekt-Erfolge – nachhaltige Risikominimierung«
- Peter Scholz: Unbekannte Schwachstellen in Hardware und Betriebssystemen. Handbuch der Telekommunikation, Wolters Kluwer Verlag, März 2005.