Endpoint Security leicht gemacht...
...Risiko-Management von Anfang an

Risiken und das Inventar vollautomatisch kennen lernen und „beherrschen“

Sie kennen das…
Gerade in größeren Unternehmen und Organisationen existiert oft die Einsicht, dass **gegen „Sicherheits-löcher“ vorgegangen** werden muss. Nur, was sind die dringlichsten Aktionen gegen die gefährlichsten Risiken? Und wo soll man anfangen?
Wie Sie ganz **einfach und vollautomatisch** die echten Daten aus der Produktion erhalten, um alle tatsächlich **vorhandenen Risiken** und **potentielle Verstöße** gegen **gültige Dienstanweisungen** besser einschätzen und gegebenenfalls auch intern Ihren Handlungs- und möglichen Ressourcenbedarf untermauern können, möchten wir Ihnen an Hand der folgenden **Projektskizze**, aufgeteilt in Phasen, exemplarisch darstellen. Natürlich begleiten Sie unsere Produkte durch alle Projektphasen.

Phase	Aufwand ca. in PT	Erreichte Ziele, Positive Effekte
"Einsammeln"	**0,5 - 2**	**Vollständige Inventarisierung aller Devices, Anwendungen, Dateien und der damit verbundenen, potenziellen Risiken**
Für Freiräume, Sicherheits- und Systemsmanagement Ziele definieren	**1 - 2**	**Abbilden der Unternehmenskultur und technischer Schutz auf 100% der PCs möglich**
Weicher Roll-Out	**1 - 2**	**Akzeptanz beim Anwender – Feintuning der Use Cases ohne administrativen Aufwand; Security Awareness**
Scharf Schalten im Betrieb	**0,5**	**Compliance, Revisionssicherheit, Übersicht, effiziente Handlungsmöglichkeiten**

Projektphase „Einsammeln“ - Vorhandene Risiken identifizieren (IST-Analyse)

IST-Analyse folgender Aspekte - die meisten Facetten sind durch eine **itWatch** Standardpolicy abgedeckt und bereits in der Auslieferung enthalten[1]:

- Ermittlung von
  - verwendeten Geräten (Devices) und Schnittstellen (Ports) bzgl.:
    - Verwendungsdauer
    - Größe von Datenträgern (belegter Speicher / freier Speicher)
    - Seriennummern oder sonstiger individueller Eigenschaften von bestimmten Devices
  - kritischen Dateiarten im Austausch: *.exe, *.mp3, ...
    - Austausch zwischen
      - Netzwerkshares und lokalem PC
      - mobilen Datenträger und lokalem PC
    - Shadowing[2] kritischer Dateiarten
    - Dateigröße und/oder sonstige individuelle Eigenschaften von bestimmten Dateien
  - Anwendungen
    - Verwendungsdauer von Anwendungen
    - individuelle Eigenschaften von bestimmten Anwendungen
  - verbundenen Netzen
    - Verbindungsdauer zu den Netzen
    - Individuelle Eigenschaften von bestimmten Netzen
- Benchmarking von Abteilungen und/oder Standorte in Bezug auf Kriterien wie Datenexport
- Clientinstallationen auf der gewünschten Anzahl PCs
- Administrationsstationen, DEvCon Server, DCReport, DCView und Datenbanken

Auf Basis des Datenmaterials erfolgt ein Abgleich mit allen bestehenden Richtlinien und Dienstanweisungen. Eine Schluss-Präsentation der Ergebnisse (evtl. mit einem Auditbericht) zeigt dann die Auswertung der Daten und die daraus resultierende Risikobewertung auf.

---

[1] Es ist auch möglich, dass nur die Abweichungen von der bereits bestehenden Richtlinie oder Dienstanweisung erfasst werden und damit die Auswertung bereits deutlich übersichtlicher wird.
[2] Unter Shadowing versteht man die vollständige Protokollierung des Inhalts der Dateien

Projektphase 2: Ziele für Freiräume und das Sicherheits- und Systemsmanagement definieren

Freiräume behalten:

IT-Security muss nicht notwendigerweise kompliziert sein und die Kollegen an der Arbeit hindern. Auch eine zusätzliche Arbeitsbelastung im Betrieb oder in der Administratoren ist nicht notwendig. Im Gegenteil: mit **itWatch** wird das Konzept „Null Administration – volle Sicherheit“ Realität. Manche Anwender müssen in bestimmten Situationen (z.B. am Wochenende) eine Aktion durchführen können, obwohl diese gegen die allgemeine Richtlinie verstößt.

Kein Problem: Automatisch ist die Zustimmung zur Protokollierung per Dialog in Echtzeit eingeholt, zentral archiviert und schon schaltet sich das betreffende Gerät selbst frei – natürlich revisionssicher und compliant.

Sicherheits-Ziele:

- Benutzer dürfen keine ausführbaren Programme (*.exe, *.sys, *.dll ...) in das System einbringen – auch nicht als eingebettete Objekte in Word Dateien.
- Keine portablen Anwendungen ausführen – weder auf dem PC noch in der Terminal Server Session? Ausnahmen wie z.B. den firmeneigenen Tarifrechner über U3 über White List zulassen?
- Aushilfen, Azubis Trainees o.ä.dürfen Firmen-Dateien auf mobilen Datenträgern nur mit dem Firmensschlüssel verschlüsselt mitnehmen. So bleiben die Daten im Unternehmen und die Gefahr der unerwünschten Datenlecks (*Data Leakage*) ist gebannt.

Systems-Management-Ziele:

- Mit **itWatch** weiß der Help Desk von Gerätefehlern, schon bevor der Anwender zum Telefon greift.
- Treiberupdates dann, wenn sie gebraucht werden (on demand)? Kein Problem!
- Virenscanner automatisch über externe Medien laufen lassen
- Protokollierung nur dort wo es notwendig ist und keine Netzkillerapplikation durch Shadowing
- Personalisierte Datenträger
- PDAs mit Benutzerzuordnung und vollautoamtischer sicherer Synchronisation
- Aktualisierung des Inventars in beliebigen Drittprodukten

Mehr Ziele finden Sie in dem White Paper "USB-Sicherheit" unter www.itWatch.de/USB_Sich.pdf

Projektphase 3 - Weicher Roll-Out

Weicher Roll-Out:

Viele Administratoren fürchten den Tag an dem eine strengere Sicherheitsrichtlinie in Kraft tritt und bestimmte, bislang geläufige Aktionen unterbunden werden. Denn wenn etwa einem „VIP“-Nutzer bestimmte Berechtigungen entzogen wurden, dann ist mindestens ein Telefonat beim Admin vorhersehbar. Mit den Produkten der **itWatch** kommunizieren Sie mit dem User bereits während des weichen Roll-Out im jeweils gewünschten Detaillierungsgrad wie sich die Unternehmensrichtlinie hier auswirkt und wie sich der Anwender jetzt und in Zukunft verhalten soll und zwar immer genau dann, wenn die zukünftig gesperrte Aktion ausgeführt werden soll. Den Übergangszeitraum können Sie nach Zeit und/oder der Anzahl der „freien“ Aktionen je nach Benutzergruppe definieren.

Projektphase 4: - Scharfschalten

Scharfschalten:

Die Policy, die vorher „nur“ gemeldet hat, oder Daten über Art und Umfang von Transaktionen an die Zentrale geliefert hat, wird einfach scharf geschalten. Änderungen an der Policy werden selbstverständlich revisionssicher protokolliert.

Interessiert? Dann kontaktieren Sie uns

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
Aschauer Str. 30
D-81549 München

itWatch – Sicherheit, die mitdenkt!