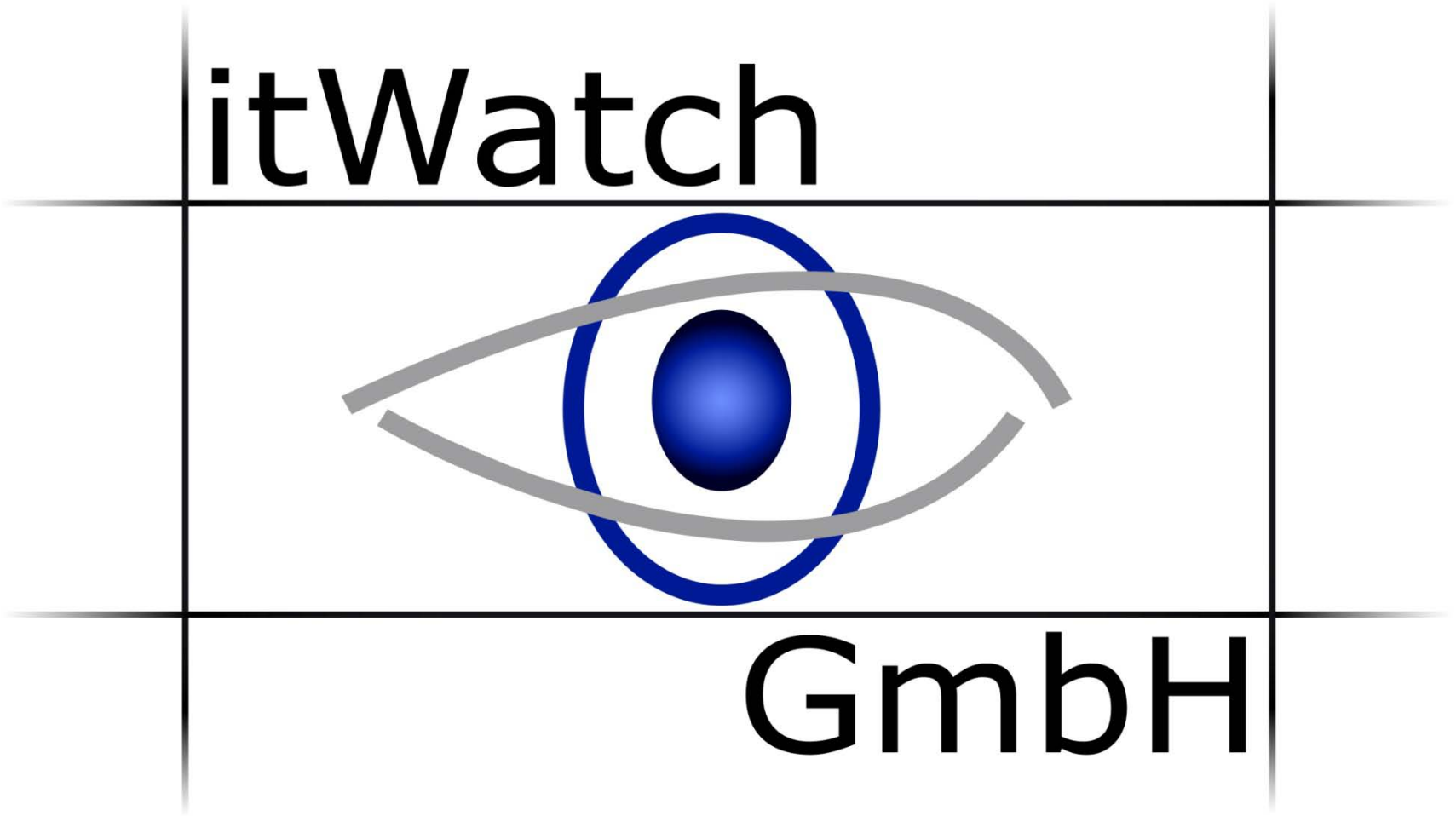
Ihre Sicherheit …
… unsere Mission



DLP & Verschlüsselung und Endgeräte Sicherheit –

Was braucht man wirklich?

it-sa
Nürnberg, 19. – 21. Oktober 2010

Ihre Sicherheit …
… unsere Mission

Wo treten Verstöße auf?
Welche Themen sind zu berücksichtigen?

Verstöße bei Netzkontakten
zum ISP – geregelt durch Firewall?
auf den Notebooks, PDAs ...

Verstöße auf den Endgeräten
Data Loss Prevention

Gegen die Anwender ist Datenschutz unmöglich

Wo sind wir noch „ungeschützt“?

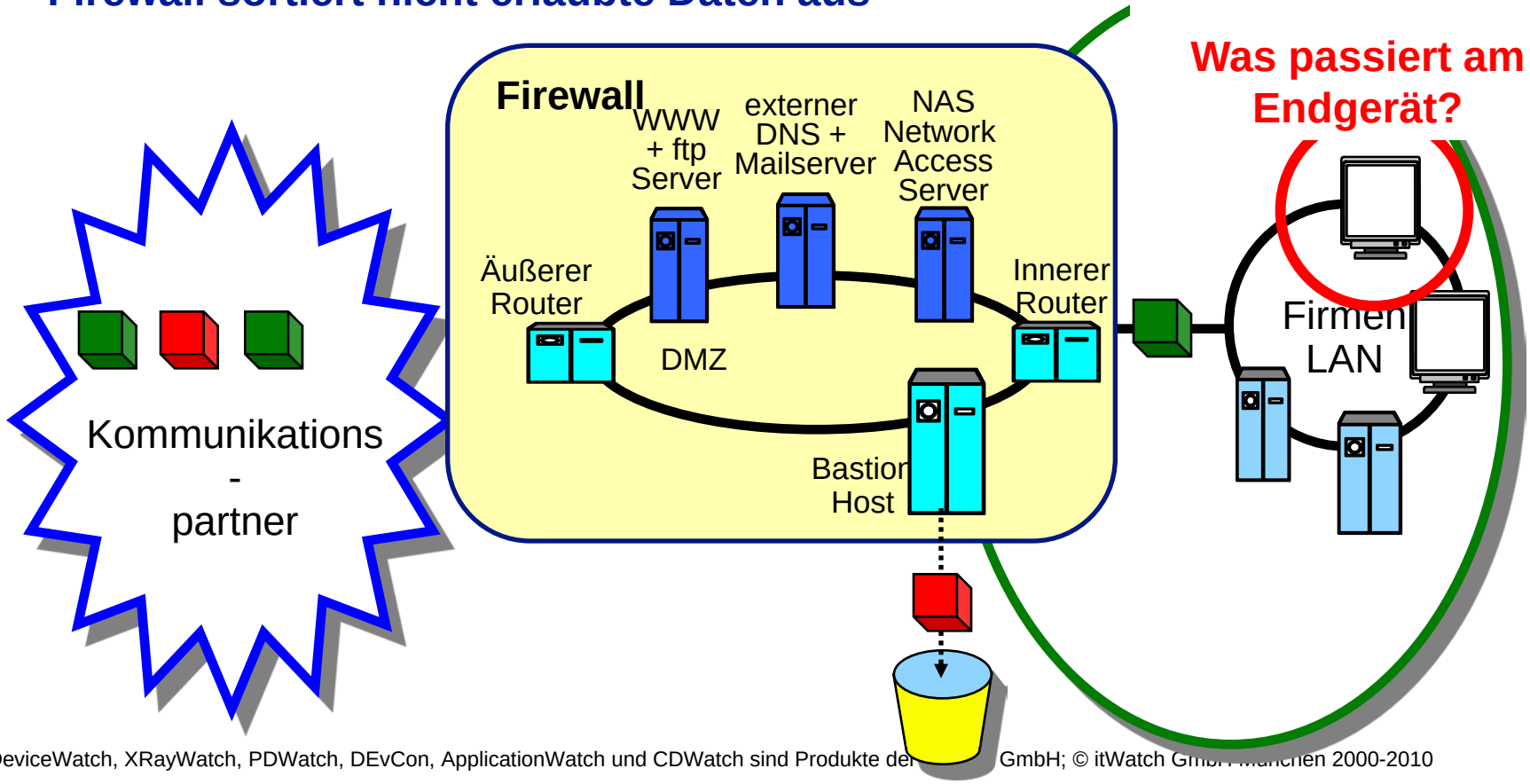
Protokoll fest: IP

Kontaktpunkte sichtbar, statisch und zentral betrieben

Firewall sortiert nicht erlaubte Daten aus

Problemzone Client

Was passiert am Endgerät?

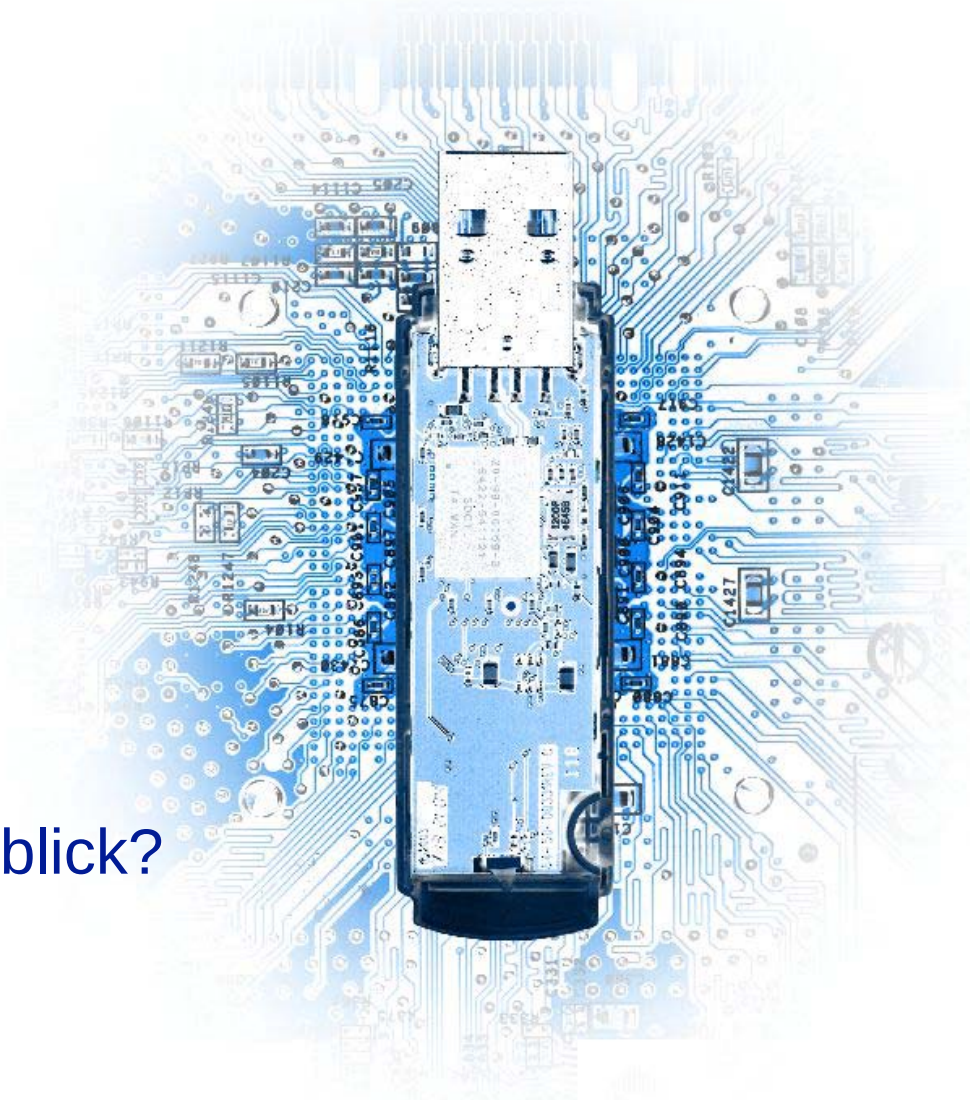


Angriffe auf Daten

- Datendiebe sind die Piraten des 21. Jahrhunderts
- Berechtigte
  - Mit bewussten Zugriffen
    - Risiko Datendiebstahl
  - Unbewussten Zugriffen
    - Schadsoftware
    - Trojanern
    - USB-Dumper
- Sichtbare Kontaktpunkte
  - Datenträger
  - Gebrannte Medien
- Unsichtbare Kontaktpunkte
  - Verschlüsselter Upload zu gemietetem Plattenplatz im Internet
  - Funkkontakte, Wireless
- Auf dem Client liegen die Daten „noch prüfbar“ vor – ein optimaler Wirkungspunkt

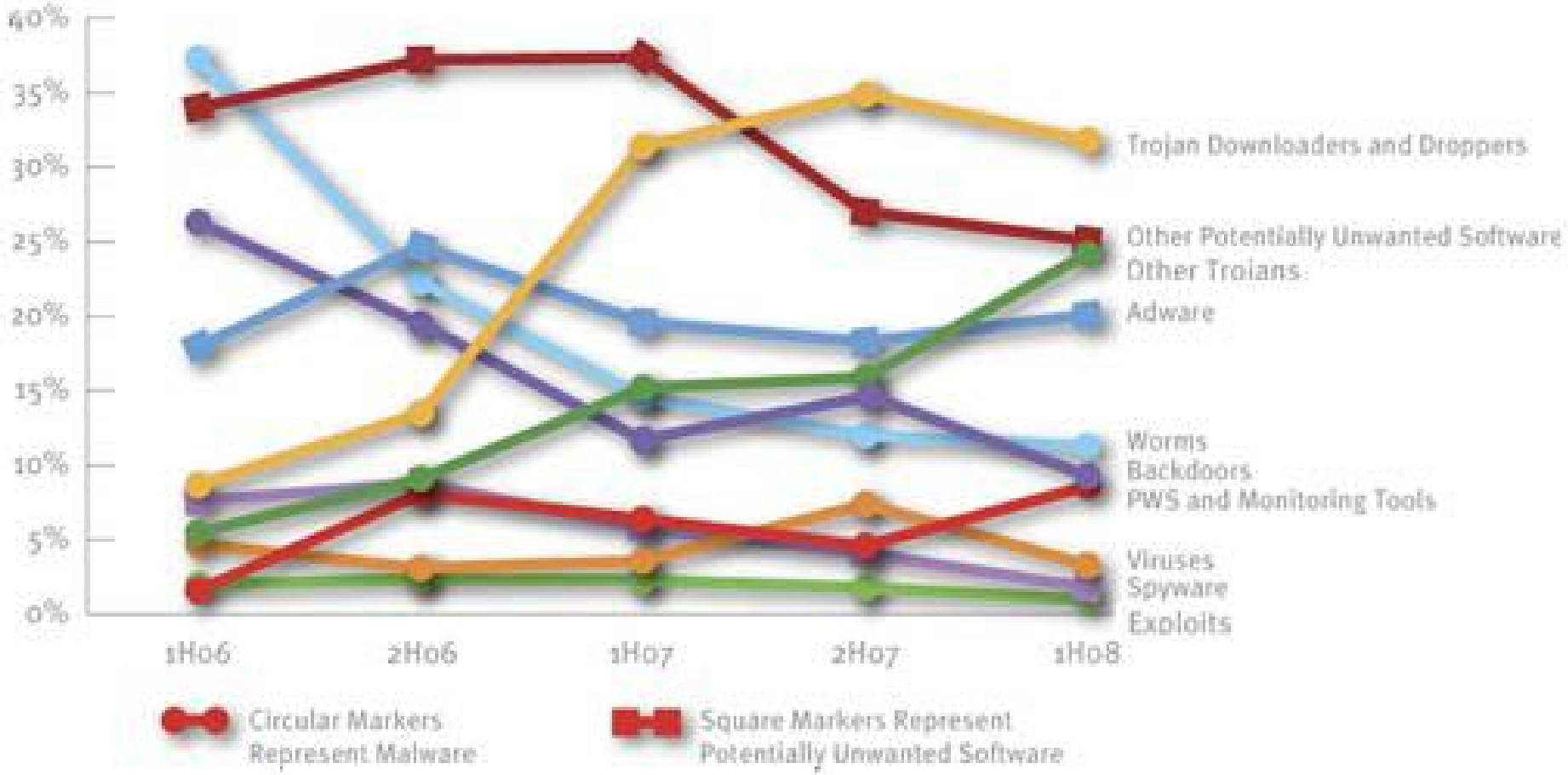
Welche „Daten“ bergen Risiken

- Archive - geschachtelt
- Verschlüsselte Objekte
- Eingebettete Objekte
- Applikationsdaten
  - Skype
  - Teamviewer
- Modifizierte Applikationen
  - Plug-Ins
  - Patches
- Wie erhält man den Durchblick?



Anwendungen: Microsoft Report

- Microsoft Security Intelligence Report 5 (Auszug)
- Bedrohungslage durch Schadsoftware und nicht erwünschte Anwendungen



Applikationskontrolle

- Inventar – alle Anwendungen in Echtzeit mit Eigenschaften (Version etc.) einsammeln. Jede Anwendung eindeutig Authentisieren
- **Monitoring** – Anwendung Start und

  kritische Dateizugriffe der Anwendung
- **Blocking** –White- und / oder Black List

  mit Echtzeit-Umschaltung der gültigen Policy.
- **Verwendung** der Anwendung abhängig vom Systemzustand (Skype)
- Content Filter für Anwendungen, so werden
  - Restriktionen (z.B. für Browser) und
  - erweiterte Anwendungs-Rechte
- unabhängig von den Rechten des Anwenders umgesetzt
- Kommunikationsanwendungen
  - Lese-Verbot für sensible Dateien
  - Schreibverbot für ausführbare

Dateninhaltskontrolle

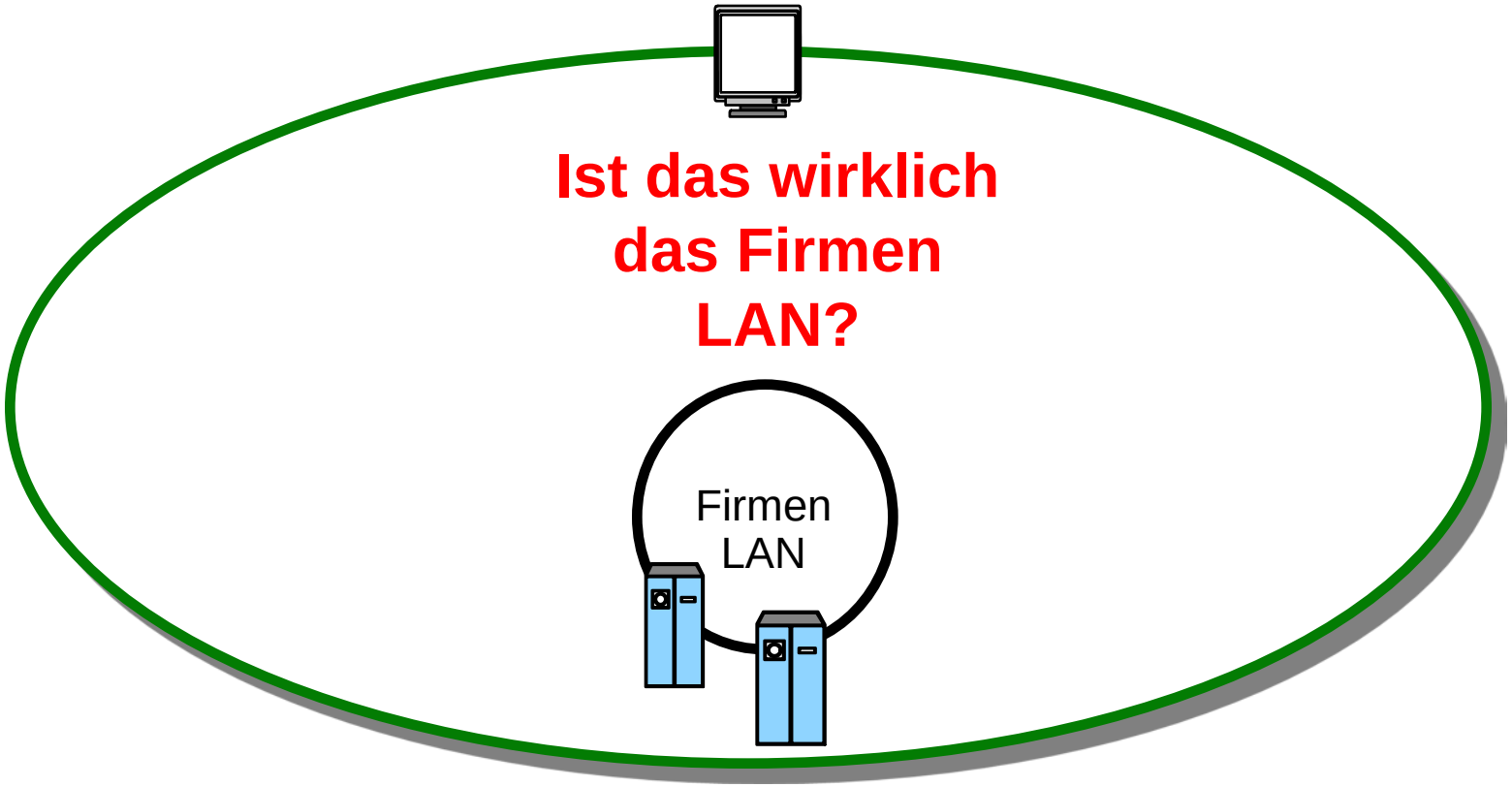
- Kontrolle des Datei-Austausches mit
  - Devices
  - Medien
  - Netz-Laufwerken
  - Citrix Terminalserver
  - Über Anwendungen
- Content Filter kontrollieren jeweils beim Lesen oder Schreiben jede einzelne Datei, komprimiert, verschlüsselt oder zu Archiven gepackt nach bestimmten Dateitypen oder Inhalten (Pattern) individuell
- Pattern Prüfung
  - Schutz vor vorgetäuschten Namen
  - Kontrolle besonderer Inhalte z.B. „firmenvertraulich“.
- Shadowing - Protokollierung kritischer Inhalte

Verschlüsselung

- Die Entnahme von personenbezogenen Daten aus dem Firmennetz nur verschlüsselt erlauben
- Wer darf vertrauliche Daten aus Ihrem Netz unverschlüsselt mitnehmen?
- Firmenschlüssel beschützen die Daten sicher bei Lagerung außer Haus
- Erlauben Sie einzelnen Benutzern
  - eigene Schlüssel zu vergeben oder
  - bestimmte Dateien unverschlüsselt mitzunehmen
  - steuern Sie, abhängig von den Datei-Inhalten, die Vertraulichkeit der Information
  - Schlüsselhinterlegung
    - zur Reduzierung der Help Desk Kosten – lokal und
    - Für den Notfall zentral
- Identische Vertraulichkeits-Richtlinien auf mobilen Datenträgern (auch CD/DVD), der lokalen Platte oder bei Netzkommunikation

Erkennung freundlicher Netze

Schreibrechte auf Y:\<User>\...



Was wäre, wenn der Angreifer „das Netz“ nachgebaut hätte.

Die letzte Bastion: der Anwender

- Einbinden des Anwenders in die Endpoint Security – zusammen ist man stärker
- Dialoge in Echtzeit ermöglichen – in Anwender-Sprache
  - Selbstfreigabe für den „erwachsenen selbstverantwortlichen Nutzer“
  - Sensibilisierung für besondere Zusammenhänge
    - Technik – besonders schützenswerte Daten (z.B. Passworte)
    - Gesetz ...
  - Elektronische Willenserklärung ermöglicht Zustimmung zu
    - Protokollierung
    - Haftungsübergang ...
  - Inhaltliche Schulung mit „elektronischer Prüfung“ als Freigabevoraussetzung
  - Compliance – Nachweis der rechtssicheren Nutzung
- Definierte Freiräume schaffen Kooperation
- VIP: Unsicherheit darf nicht Privileg werden

Kontakt

Ihre Ansprechpartner

Technische Fragen:

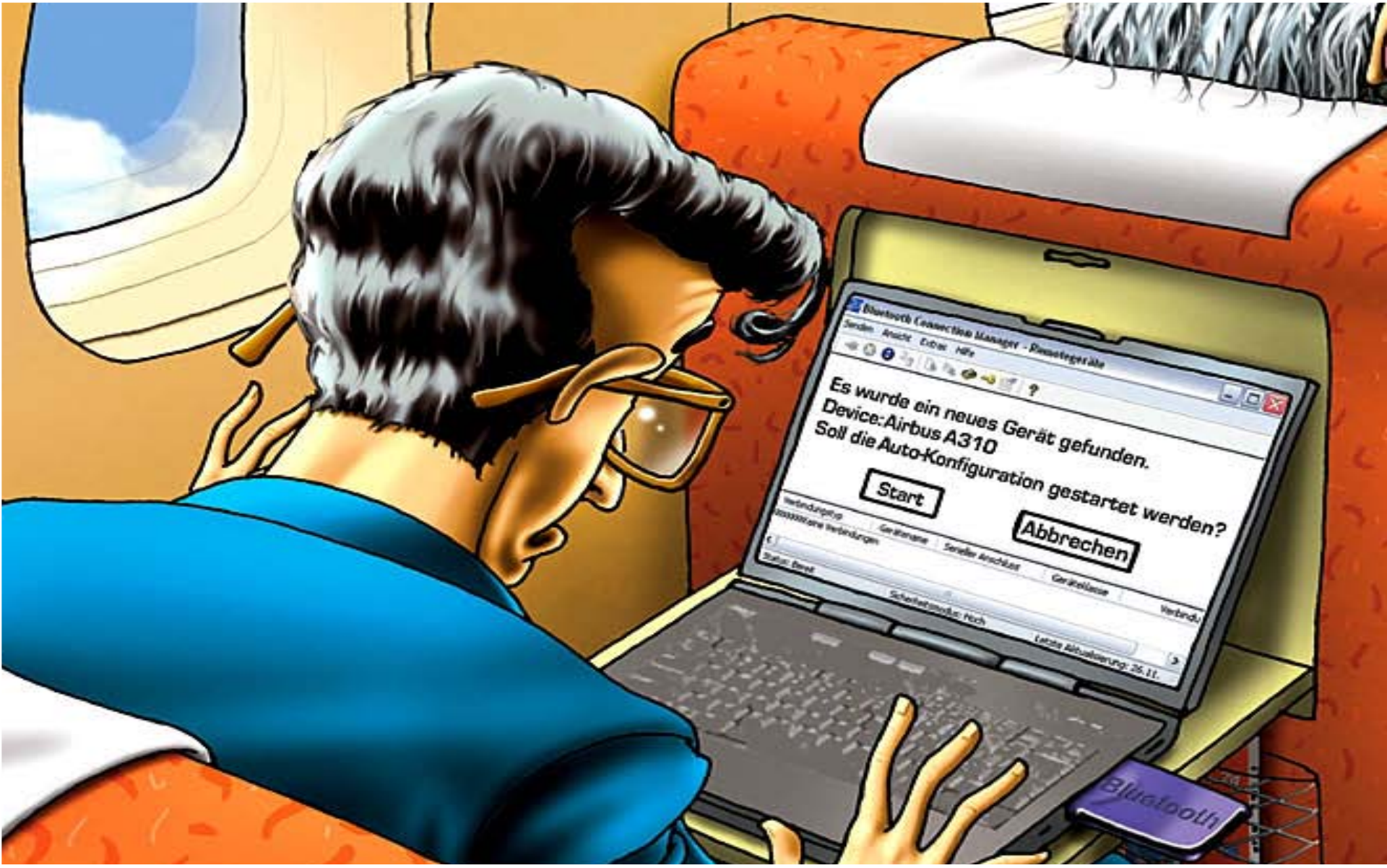
Hotline: +49 1805-999984

DeviceWatch@itWatch.de

Organisatorische Fragen:

Telefon: +49 89-620 30 100

info@itWatch.de



Besten Dank für Ihre Aufmerksamkeit

ct 1/2003

Ihre Sicherheit …
… unsere Mission

Die Endpoint Security Suite der itWatch beinhaltet:

DeviceWatch – Gerätekontrolle

XRayWatch – Dateien, Inhalte blockieren und auditieren

PDWatch – Verschlüsselung Mobil, lokal und zentral

CDWatch – Medienbasierter Schutz

ApplicationWatch Applikationskontrolle

DEvCon – kaskadierende Device Event Console

Automatisierung – Scanner – Drive Mapping

Echtzeit Monitor – Reporting

alle Module - ein einziger Agent

Funktionen

DeviceWatch

- **Devices** sind alle eingebauten oder externen Geräte wie Memory Sticks, Modems, Drucker, Scanner, PDAs, Handys etc.
- **Schnittstellen** sind alle Ports, über welche moderne PCs verfügen: USB, PCMCIA, Bluetooth, WLAN, Firewire, Infrarot etc.
- Sie definieren, welcher Benutzer welches Device wann und wo **unter welchen Umständen** einsetzen darf
- Sicherer Einsatz aller Geräte, Devices und Schnittstellen, Benutzer-, Gruppen- und PC-spezifisch – natürlich **U3**-ready!

Funktionen

XRayWatch - Austausch mit (Netz)-Laufwerken und Citrix kontrollieren

Content Filter
- Dateiaustausch kontrollieren

- Jeweils beim Lesen oder Schreiben können Sie einzelne Dateien oder bestimmte Dateitypen (mit Wildcards) individuell
  - Freigeben, sperren oder
  - Verschlüsseln (zwangsweise oder optional)

Pattern Prüfung
- Schutz vor vorgetäuschten Namen

- Erweiterung des Content Filters um beliebig genaue **inhaltliche Prüfungen** (semantisch und syntaktisch);
- Standardformate werden mitgeliefert und auch mit gewartet,
- kundenspezifische Erweiterungen sind in wenigen Minuten erledigt, z.B. „firmenvertraulich“.

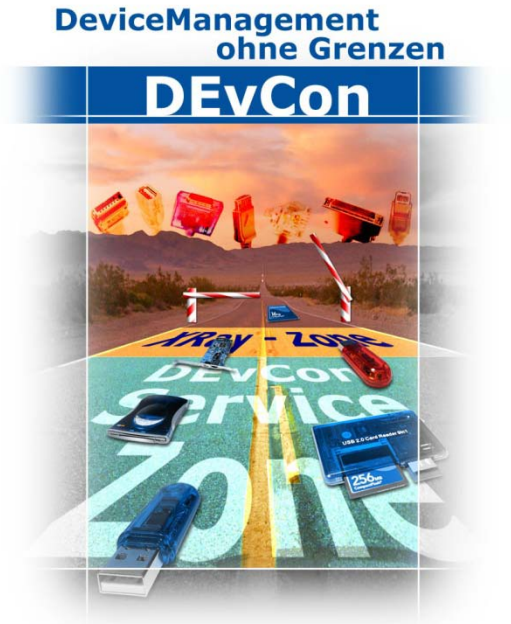
Shadowing - Protokollierung ohne Overkill!
- Alle Dateien oder nur vordefinierte Dateitypen werden je Device und Benutzer oder Gruppe protokolliert (Dateiname oder gesamter Inhalt)

Funktionen

System Management vom Feinsten:

SystemManagement im Netz mit vielen Mehrwerten:

- Kaskadierende Echtzeitkonsole aller Endgeräte Events im Netz,
- On Demand Device Treiber Management,
- Autostart des Virenscanners auf externen Laufwerken
- Überprüfung der Security-Einstellungen für Kommunikation oder Drittprodukte,
- Integration in Frameworks wie Tivoli oder OpenView ...
- erledigt alle Anforderungen bei dem Betrieb von Devices aus Sicht des System-Managements
- Unerwünschte Prozesse automatisch beenden
- Unerwünschte Netzwerke verbieten – oder in Echtzeit geeignete Vorkehrungen treffen
- Alerting nach Schwellwerten – auch netzwerkweit konsolidiert
- Reporting mit vordefinierten Reports



Funktionen

System Management

- **DeviceWatch Drive Mapping** - Kollisionsfreie Vergabe der Laufwerksbuchstaben zentral netzwerkweit – keine Überlagerung mit Ihren Netzwerklaufwerken.
- **DeviceWatch Scanner** – **Inventar**ermittlung und **Soll-Ist** Analyse. Ermittelt alle Devices, die angeschlossen sind – netzwerkweit – transparent für den Benutzer – ohne Client-Installation.
- **DCView** – Echtzeitviewer für Ereignisse im Netz (themenbasiert)
- **DCReport** – vordefinierte Reports und Anfragen in Echtzeit
  - Revision
  - Administration

Funktionen

ApplicationWatch

- **Inventar** – alle Anwendungen werden in Echtzeit mit Eigenschaften (Version etc.) eingesammelt. Jede Anwendung nur einmal an die Zentrale oder
- **Monitoring** – Anwendungsstart und -ende für statistische Auswertungen und Lizenzoptimierung
- **Blocking** –White- und / oder black List mit Echtzeit-umschaltung der gültigen Policy.

- **Verwendung** der Anwendung abhängig von Systemzustand
- Content Filter können für Anwendungen vergeben werden – unabhängig von den Rechten des Anwenders – Organisation von Plug-Ins - Verbot von sensiblen Dateien für Kommunikationsanwendungen

Funktionen

PDWatch

– **Verschlüsselung** und **Vertraulichkeit** über zentrale Richtlinien steuern

- Wer darf Daten aus Ihrem Netz unverschlüsselt mitnehmen?
- Geben Sie Firmenschlüssel zum firmen-internen Datenaustausch zentral vor
- Erlauben Sie einzelnen Benutzern
  - eigene Schlüssel zu vergeben oder
  - bestimmte Dateien unverschlüsselt mitzunehmen
  - steuern Sie, abhängig von den Datei-Inhalten, die Vertraulichkeit der Information
  - Schlüsselhinterlegung – lokal und zentral
  - Aufräumen
- Moderner Informationsschutz - zentral organisiert! **Auf mobilen Datenträgern (auch CD/DVD), der lokalen Platte oder im Netz**

Funktionen

CDWatch – medienabhängige Kontrolle von CDs und DVDs

- Zusätzlich zu den Content Filtern
- Nicht jede CD darf verwendet werden?
- Verwalten Sie freigegebene CDs und DVDs mit
  - Gültigkeitszeitraum,
  - automatischen Installations- und Deinstallations-Vorgaben.
  - Teilfreigaben für Benutzer
- Arbeitet für alle CDs / DVDs – gekaufte und selbstgebrannte auf Basis einer Inhalts Signatur der CD / DVD