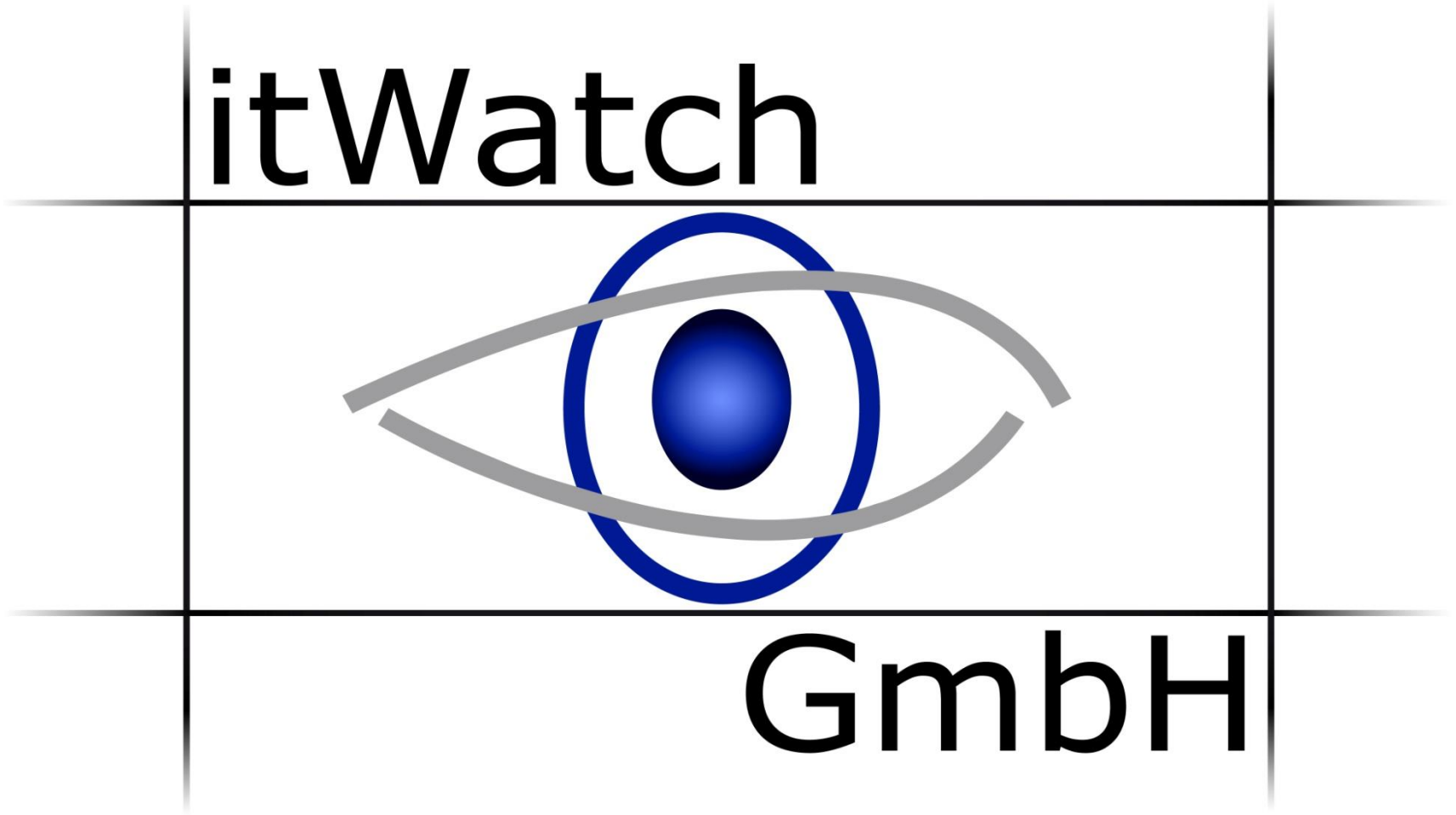
Ihre Sicherheit …
… unsere Mission



DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Anforderungen des IKT-Mittelstand an Normung und Standardisierung (Aus Sicht der IT-Sicherheit)

Donnerstag, den 30. Oktober 2014
11:40 – 12:00 Uhr
BMWi, Scharnhorststraße 34 – 37
Konferenzzentrum, Eichensaal

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Kurzvorstellung Ramon Mörl

- 25 Jahre Erfahrung als Berater in der IT-Sicherheit
- Leitende Tätigkeiten in Projekten für Firmen wie HP, IBM, Siemens, ICL und Bull in Belgien, Deutschland, Frankreich, Italien, Österreich, Schweiz und USA
- Als unabhängiger Evaluator und Berater der Europäischen Union vor allem im Bereich der ECMA und ISO-Standards für die IT-Sicherheit tätig
- Seit 2002 **Geschäftsführer der itWatch GmbH**

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Das Spannungsfeld

Nutzbarkeit ...

Standard

Transparenz	Kontrolle
API	Proprietär
Klartext	Verschlüsselung
Vertrauen	Authentisierung
...	...

Sicherheit

... Vertraulichkeit

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Was ist echte Sicherheit?

Ein sicheres Auto hat:

- Sicherheitsgurte
- Mehrere Airbags
- Rückspiegel
- ABS
- Licht
- …

nicht sicher

Der pragmatische Weg

- Nicht das sicherste Produkt setzt sich durch.
- IT-Sicherheit gilt als Verhinderer
- Häufig wird das Produkt mit dem “geringsten Impact” im Businessprozess aus Sicht des Betriebes bevorzugt
- Denötigt werden IT-Sicherheitsprodukte, die als Business Enabler wahrgenommen werden.

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Anforderungen des IKT-Mittelstand an Normung und Standardisierung (Aus Sicht der IT-Sicherheit)

Ist-Stand?

Wo sind die Probleme?

Welche Lösungen sind sinnvoll und notwendig?

Eingabe Geräte

- Hübsche Maus ist zusätzlich eine gefälschte Tastatur – siehe Heise Teensy Board Angriff oder BadUSB auf der Black Hat 2014 in Las Vegas

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

BadUSB

- Black Hat Konferenz im August 2014 in LasVegas stellten Karsten Nohl und Jakob Lell eine besondere Qualität der IT-Sicherheit dar:
  BadUSB - On Accessories that Turn Evil

- Verwendung eines USB-Sticks mit einem Controller von Phison, der so umprogrammiert wird, dass weitere Funktionen hinzu kommen ➡

  - USB-Stick gibt sich zusätzlich als Tastatur aus

  - Für die Funktionen werden vom Betriebssystem gelieferte Treiber verwendet

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

BadUSB

- Die “neue” schädliche Tastatur würde eigenständig Daten, die auf dem reprogrammierten Controller hinterlegt sind, Tastatureingaben an den Rechner schicken
- Kommandos in Form von Zeichensequenzen werden über die Tastatur gesendet, ohne dass es bemerkt wird.
- Der auf dem Rechner hinterlegte Schadcode
  - greift nun alle an diesen Rechner angesteckte USB Geräte (mit gleichartigen Controllern) an und reprogrammiert den Controller
  - Und treibt noch sonst so was Schadcode so treibt
- Ein Wurm mit Schadcode über die Reprogrammierung eines Controllers …

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

HID – Human Interface Devices

- HID ist eine Abstraktionsschicht inkl. Treiber, um Geräte an das OS zu koppeln, unabhängig von Kanal und Gerät selbst.
  - Kanäle können sein: usb, bluetooth, 12C, …
  - Geräte können sein: KBD, Mouse
- Standartgeräte, wie Tastatur und Maus koppeln direkt an die Standard HID Treiber des OS
- Daher ist für die Basisfunktionalität kein eigener Treiber notwendig
- Wenn sich ein Stück Hardware als HID zu erkennen gibt, wird das folglich vom Betriebssystem bedient.

⇒ Alle Eingaben landen via HID in den Message-Queues von Windows als „Keystroke-Messages“ oder „Mouse-Messages“

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

HID – Human Interface Devices

- Nachrichten in den Message-Queues (= Keystrokes) sind durch beliebige Anwender und beliebige Anwendungen konsumierbar
- Eine Anwendung kann normalerweise alle Keystrokes mithören, auch wenn sie nicht den Eingabefokus hat

⇒ Die Eingabe ist momentan nicht selbst bestimmt

- Oberhalb der HID kursieren alle Eingaben als Messages im System
  ⇒ Möglichkeit Keystroke-Messages zu generieren
  Ohne dass die Quelle ein echtes physikalisches Gerät ist.
- Sie brauchen die Möglichkeit Ihre Eingaben für Passworte, PINs, etc. sicher zu schützen

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Anforderungen des IKT-Mittelstand an Normung und Standardisierung (Aus Sicht der IT-Sicherheit)

Ist-Stand?

Wo sind die Probleme?

Welche Lösungen sind sinnvoll und notwendig?

Standard-Probleme

- Controller lassen sich von jedem über eine „standardisierte API“ patchen – ohne Authentisierung
- USB Geräte werden nicht authentisiert, weil der Standard „nur“ eine Identifizierung kennt
- Passworte müssen – für alle Anwendungen im Klartext zugänglich – über eine standardisierte Schnittstelle
- …
- Hauptgründe : Offene APIs (ohne Security), Kosten und Commodity

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Freiheit von Hintertüren

- Was macht ein institutioneller Angreifer mit viel Geld, der gerne an Ihre „heiligsten Daten“ kommen möchte?

- Er baut eine Sicherheitssoftware, die
  - von Ihnen so konfiguriert wird, dass sie die „heiligsten Daten“ erkennt und schützt und
  - Baut eine Hintertüre ein, welche die geschützten Daten über einen verdeckten Kanal ausschleust

- Technisch z.B. für einen hochsicheren Kryptoalgorithmus nachgewiesen in Bruce Schneiers kryptografischen Werken

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Anforderungen des IKT-Mittelstand an Normung und Standardisierung (Aus Sicht der IT-Sicherheit)

Ist-Stand?

Wo sind die Probleme?

Welche Lösungen sind sinnvoll und notwendig?

Gelöste Probleme (?)

- Kryptografie
  - Trennung von
    - Schlüssel und
    - Algorithmus
  - Ermöglicht Standardisierung von sicheren Algorithmen
- Sicherer Schlüsselspeicher – z.B. Smart Card
  - PIN Eingabe zum Aufsperren des Schlüsselspeichers?
- Authentisierung
  - Standardisiertes Vorgehen
  - (Geschütztes?) Ergebnis (Credential)
- Der letzte Meter?

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Vertrauenskette

Was ist eine Lückenlose Vertrauenskette?

Sie besteht aus:

- Technik
- Organisation
- Haftung
- Rechtssicherheit

Kann die Vertrauenskette standardisiert werden?

Vertrauensketten herstellen

- Vertrauensketten
  - Vom Anwender an der Tastatur
  - Über die
  - Hardware und
  - Die Services
  - Zu den Daten
  - Und bis zum Hersteller der Hard und Software.
- durch unabhängige Organisationen wie das BSI – *Bundesamt für Sicherheit in der Informationstechnologie*
- Freigaben oder Zulassungen für „Verschlusssache“
- Prüfungen im proprietären Rahmen
- Auch nach Rechtssicherheit & Haftung – z.B. Patriot Act

DeviceWatch, XRayWatch, PDWatch, DEvCon, AppWatch, CDWatch, ReCAPS, PrintWatch, DataEx, DataExSafe sind Produkte der itWatch GmbH; © itWatch GmbH, München 2000-2014
Produkte der itWatch GmbH; © itWatch GmbH, München 2000-2014

Sichere Tastatur?

- Starke Authentisierung der richtigen Tatstatur
- Verbot für Doppelte Tastatur
  bei Bedarf Echtzeiterkennung und Freigabe der zweiten Tastatur durch den Anwender
- Hardwarekomponenten bei Auslieferung „einfrieren“
  Echtzeitmeldung bei Veränderungen
- keine unbekannten Prozesse
- Sichere Maustastatur
- Sichere Übergabe von Passworten bis in die Anwendung, das Login etc.
- Schutz vor dem Ausspähen auf den Mausbewegungen
- …

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Die weitere Entwicklung

Robuste Cyber Sicherheits-Architektur:

- Sicherheit in den APIs
- Authentisierung von Anwendern UND
  - Devices, Hardware, PCs, …
  - Anwendungen, Prozessen von Anwendungen
  - …
- Trennung von Sicherheitssystem und Anwendungen
  - Microkernel Technologie
  - Virtualisierung
  - …

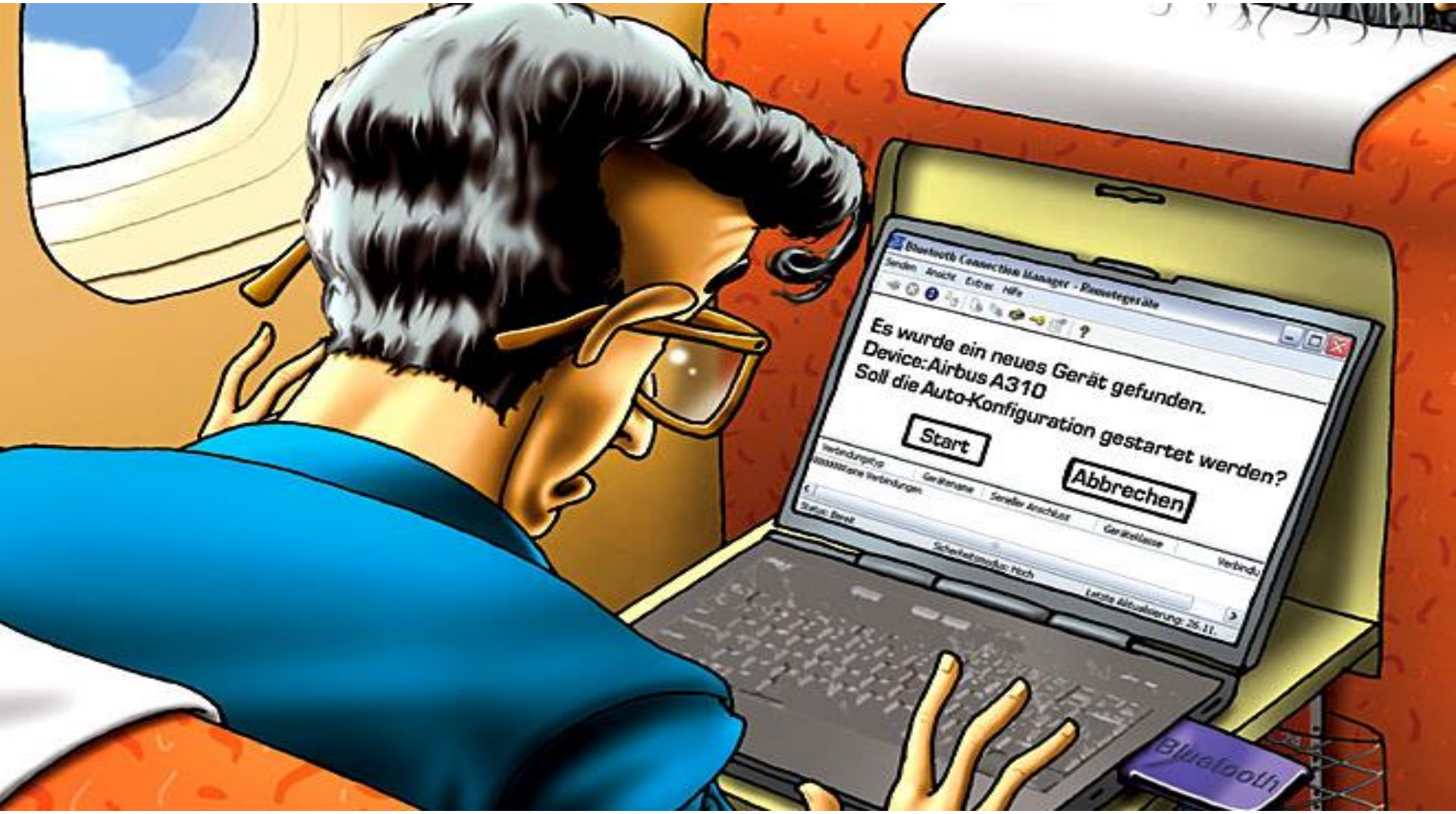
DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Was braucht nun der Mittelstand?

- Der Mittelstand kann es nicht leisten die komplexen Evaluierungen, die notwendig sind, um echte IT-Sicherheit zu erreichen, selbst durchzuführen
- Die öffentlichen, vertrauenswürdigen Stellen sehen sich aus Gründen der befürchteten Wettbewerbsverzerrung nicht in der Lage konkrete Lösungen zu nennen
- Der Markt (und nicht nur der Mittelstand – auch die Kommunen und viele andere sind betroffen) brauchen einen katalytischen Effekt, in welchem Ross und Reiter genannt werden

DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014

Besten Dank für Ihre Aufmerksamkeit



DeviceWatch, XRayWatch, PDWatch, DEvCon, ApplicationWatch, CDWatch , ReCAppS, PrintWatch, DataEx, AwareWatch, ReplicationWatch und CryptWatch sind Produkte der itWatch GmbH; © itWatch GmbH München 2000-2014