I/O Management

- oder -

Die Schattenseiten des Plug‘n‘Play

Martin Burri

IT-Sicherheitsbeauftragter

Visana Services AG

martin.burri@visana.ch

IT - Security Forum #5

Agenda

- Einstieg
- Was ist Plug‘n‘Play?
- Sicherheitsrisiko PnP-Devices
- Projekt I/O Management
- Fazit
- Fragen

Einstieg

Zwei Fragen an Sie:

Wo sind Ihre Memory Sticks im Moment?
Welche Daten sind darauf gespeichert?

IT - Security Forum #5

5

Visana

- Visana ist die fünftgrösste Schweizer Krankenversicherung. An ihrem Hauptsitz in Bern, in ihren 23 hauptamtlichen und 235 neben-amtlichen Geschäftsstellen sowie den 10 Leistungszentren beschäftigt sie insgesamt 1450 Mitarbeiterinnen und Mitarbeiter.
- Umgang mit „besonders schützenswerten Personendaten“ (nach DSG)…
- … erfordert eine stetige Sensibilisierung der MA und Umsetzung von technischen und organisatorischen Massnahmen

IT - Security Forum #5

6

2002 – neue PC Infrastruktur

Direktionsprojekt mit u.a. folgenden Zielen:

- Evaluation einheitlicher PCs und Notebooks
- Migration von NT und Office 95 auf *XP-Plattform*

Microsoft Windows xp Professional bringt neue Funktionalitäten:

- Plug and Play (PnP)
  PnP-fähige Geräte (Devices) können am PC/ Notebook ohne grosse Interaktion des Benutzers angeschlossen und in Betrieb genommen werden.

IT - Security Forum #5

7

Was ist Plug‘n‘Play ?

Automatische Ressourcenzuteilung durch das BIOS und Betriebssystem

Was ist Plug & Play?
Wenn ein Computer und seine Software (BIOS und Betriebssystem) für die Funktion Plug & Play gerüstet ist, kann der Computer automatisch erkennen, welche Geräte an ihm angeschlossen sind und die richtige Konfiguration selbst vornehmen. Dabei wählt der Computer ohne Ihr Eingreifen die optimale Einstellung des Modems, und die Software passt sich automatisch an diese Einstellung an. (Quelle: 3Com)

IT - Security Forum #5

8

Das ist Plug‘n‘Play !

Windwos XP – HCL (Hardware Compatible List)
Stand März 06:

- Wireless Devices: über 1500 Typen
- Removable Media Drives: über 2600 Typen
- Flash Memory Storage: über 2200 Typen
- Modems: über 1050 Typen
- …

Plug‘n‘Play ?

Sicherheitsrisiko PnP-Devices

Problematische PnP-Geräte:

Memory Stick, externe Festplatte, CD/DVD-Brenner, PDA, MP3 Player, Modem, Bluetooth- und Wireless Adapter etc.

- Jeder kann ein Gerät in Betrieb nehmen und die Daten lesen
- Daten sind in der Regel nicht genügend gesichert
- Grosse Datenmengen können ohne Probleme kopiert werden
- Keine Datensicherung
- Keine Kontrolle über fachgerechte Nutzung
- Gefahr von Verlust / Diebstahl (kleine Bauteile)
- Was passiert bei Verlust eines Gerätes?

Die Presse

InfoWeek 08/2004: News & Meinungen

USB: Flexibilität kostet

von David Rosenthal, erschienen am 19. April 200

Sicherheitsrisiko USB - Datenschützer schlagen Alarm

Von CW-Redakteur Jürgen Hill.

MÜNCHEN (COMPUTERWOCHE) - Auf ein häufig übersehenes Schlupfloch in modernen PCs weist der Landesbeauftragte für Datenschutz in Baden-Württemberg in seinem jüngsten Tätigkeitsbericht hin: die USB-Schnittstelle. Mit dem entsprechenden Know-how kann ein Eindringling auf diesem Weg die Schutzfunktionen des Betriebssystems umgehen und Kontrolle über den Rechner erlangen.

Schotten dicht

Fraunhofer Magazin 2.2004

Hacker, Datendiebe, Viren, Würmer – die Angriffe auf die Informationstechnologie von Firmen nehmen zu. Mobile Geräte wie Handys, PDAs und Memory Sticks eröffnen uner-
nschten Eindringlingen
ıe Einfallstore. Wie Unter-
ımen ihre Daten schützen
ınen, zeigen Fraunhofer-
scher auf der CeBIT.

Datenklau über USB-Schnittstelle binnen Sekunden

22.01.2004 um 11:11 Uhr

MÜNCHEN (COMPUTERWOCHE) - Die PC-Schnittstelle Universal Serial Bus (USB) erweist sich als oft vernachlässigte Gefahr. Ein Eindringling kann über USB die Schutzfunktionen des Betriebssystems umgehen und die Kontrolle über den Rechner erlangen. Bei der USB-Version 2.0, von der mittlerweile in fast jedem PC gleich mehrere Anschlüsse verbaut werden, ist der Datenklau sogar binnen Sekunden möglich.

Datenschützer warnen vor Angriffen über Memory-Sticks und WLAN-Adapt

USB-Schnittstelle läd zum Missbrauch ein

www.computerwoche.de

stern shortnews

Spionagegefahr durch USB-Schnittstelle

Die USB-Schnittstelle ist die einfachste Möglichkeit, Peripheriegeräte an seinen PC anzuschließen. Diese Möglichkeit kann von findigen Datendieben schnell missbraucht werden.

IT - Security Forum #5

Beispiel: USB Memory-Stick

- Plug'n'Play
- Grosse Datenspeicherkapazitäten
- Fehlende Datensicherheit
- Verlust (kleine Abmessung) / Diebstahl

- Haupt-Problematik: Finder hat Zugriff auf Daten

Erkenntnis vom Management:

- Sicherheitsproblematik nicht nur mit USB-Devices !
- fehlendes I/O Management

13

IT - Security Forum #5

Projekt I/O Management

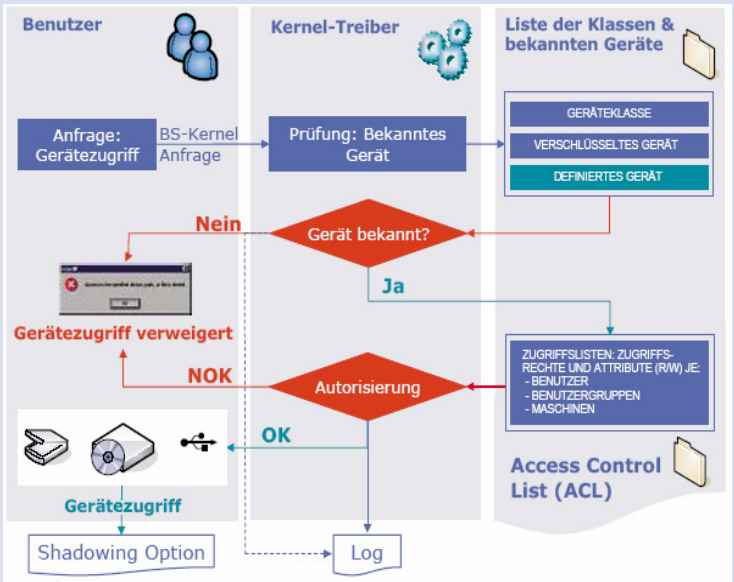
- Erstellung Security-Policy
  - Anforderungen an Firmen Memory-Stick
  - Anforderungen an Nicht-Standard-Devices (z.B. Digicams, Scanner etc.)
  - Handhabungskriterien für Entscheidungsträger
- Evaluation Software und Firmen Memory-Stick
- Freigabe durch Management
- Publikation Mitteilung
  - Richtlinie für die Nutzung von externen Devices
  - Antrag auf Firmen Memory-Stick
  - Antrag auf Nicht-Standard-Devices
- Prozess-Anpassungen
- Rollout pro Organisationseinheit

14

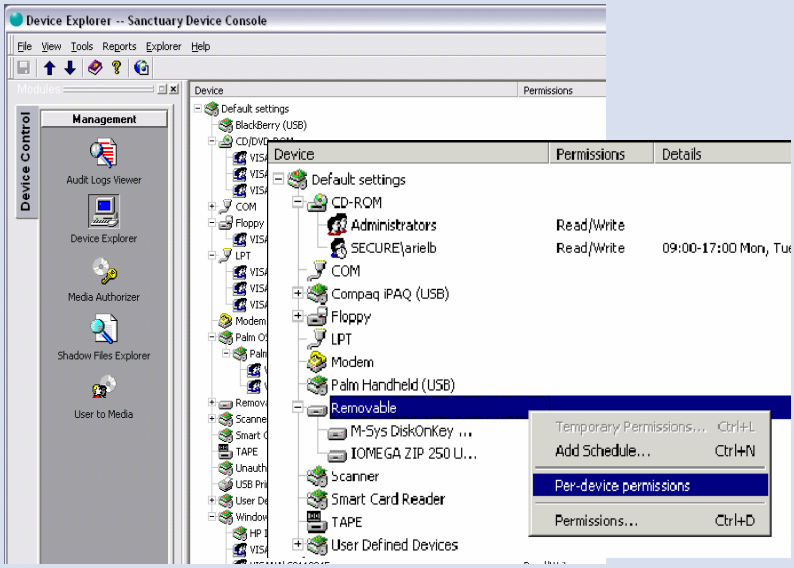
Lösung Software

- Zentrale Zugriffskontrolle über sämtliche Schnittstellen
- Device White List: Kontrolle über neue Geräte
- Änderungen der Zugriffsrechte im laufenden Betrieb
- Zugriffsberechtigungen: zeitlich, lesen/schreiben
- Zugriffsprotokollierung
- Shadowing
- Diverse Installationsmöglichkeiten für die Clients

Lösung Software 2



Lösung Software 3



Lösung Hardware: Memory-Stick

- „Firmen Memory-Stick“
- Daten sind durch Fingerprint geschützt
- Gesamter Speicherbereich ist verschlüsselt (no public area)
- Eigene, integrierte Verschlüsselungslogik
- Keine Software nötig
- Kein Treiber für Windows 2000/3, ME, XP, Linux, Solaris, Mac notwendig

IT - Security Forum #5

Fazit

- Awareness beim Management und bei den Mitarbeitenden
- Sich Zeit nehmen für Prozessdefinitionen und das Handling von Ausnahmen
- Ganzheitlicher Ansatz wählen (PDA, Notebooks, Telearbeitsplätze etc.)
- „Vertrauen ist gut – Kontrolle ist besser“

Minimierung des Sicherheits-Risikos „PC-Schnittstelle“ durch Einführung eines I/O Managements

Software-Produkte:

- Sanctuary Device Control, DriveLock, Universal Device Blocker, USB Access

19