

1 Problem / Ziel

Es ist derzeit unbestritten, dass die verschiedenen Geräte und Technologien, die die Mobilität der Mitarbeiter unterstützen, ein nicht vernachlässigbares Security-Problem darstellen.

Über die mit Notebook über PDA bis hin zum Mobiltelefon verbundenen Risiken gibt es inzwischen diverse Veröffentlichungen. Laut einer Studie von Ernst & Young (Quelle: Computerwoche 50/2005) betrachten 53 % der IT-Manager das Mobile Computing als die größte Herausforderung der nächsten Zeit im Bereich IT-Sicherheit. (Basis: Manager in 1.300 Organisationen weltweit, Angaben in Prozent).

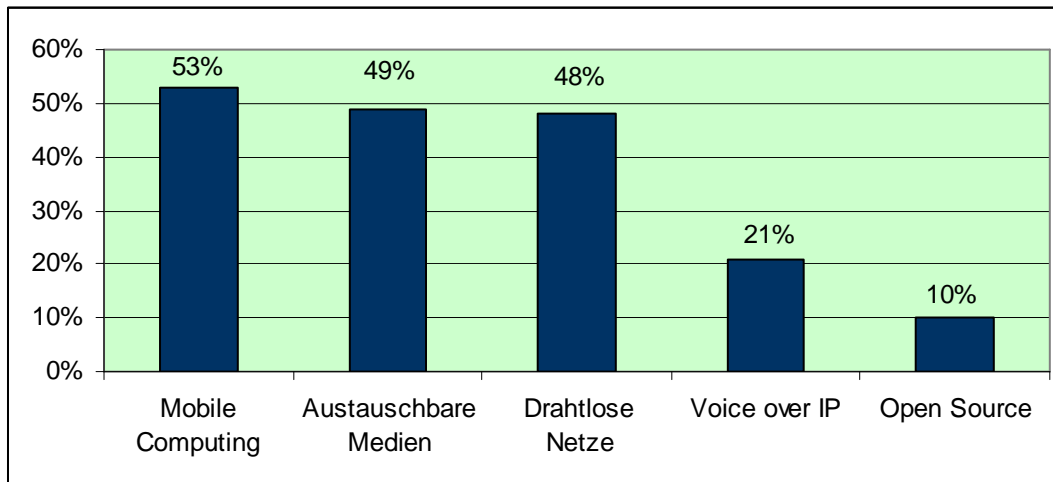


Bild 1: Welche Technologien bereiten Ihnen hinsichtlich Sicherheit Kopfzerbrechen? (Basis: Manager in 1.300 Organisationen weltweit, Angaben in Prozent)
Quelle: Ernst & Young Computerwoche 50/2005

Hier werden einige Anforderungen und Vorschläge zu einer angenäherten Lösung zusammengefasst, die helfen, einen unautorisierten Zugriff auf Daten durch folgende Richtlinie zu verhindern:

1. Es werden nur vom Unternehmen beschaffte und vergebene Geräte eingesetzt.
2. Es werden nur solche Geräte eingesetzt, die durch entsprechende Verfahren „steuerbar“ s.u. sind.
3. Die Geräte sind personen- und rollengebunden
4. Es wird ein unterschiedliches Berechtigungsprofil (Zugang im Unternehmen oder von außerhalb) bereitgestellt.
5. Jedes aktive Gerät verlangt eine eigene Authentifizierung und alle passiven (z.B. USB-Memo-Stick) eine gesteuerte Nutzungsberechtigung.

Bei aller Leichtigkeit, in der diese Richtlinien formulierbar sind, ist es keine triviale Aufgabe diese auch umzusetzen und vor allem technisch abzusichern. Im Grundsatz sollen diese Richtlinien so weit als irgend möglich technisch abgesichert und personenbezogen variierbar sein. Nur dann, wenn es keine technischen Möglichkeiten gibt, bzw. der Aufwand unvertretbar hoch ist, werden organisatorische Maßnahmen ergänzend eingesetzt.

Die Notebook-Thematik wird hier ausgeklammert, da diese Geräte in der Regel im Netzwerk und Security-Konzept des Unternehmens bereits hinreichend berücksichtigt sind.

Qualifizierte Mobile Security

2 Geräteauswahl

Bei der Geräteauswahl müssen verschiedene Kriterien betrachtet werden:

- Lässt sich die Geräte-ID mit Windowsmitteln (Gerätemanager) ermitteln?
- Ist ein Installationsprogramm zur Integration des Devices erforderlich?
- Sind spezielle Grätetreiber erforderlich?
- Handelt es sich um ein Gerät mit eigener Intelligenz oder nur um ein reines Speichermedium (Memo-Stick, Digitalkamera, MP3 Player,...)?
- Mit welcher Technologie wird dieses Device angekoppelt (USB, Bluetooth, Infrarot, WLAN,...)?
- Hat das Gerät eine eigene Authentifikation?

Als aktive Geräte sind PDAs (Personal Digital Assistant) und in gewissem Rahmen auch Mobiltelefone bzw. die Kombinationen aus bei dem Gegenstand der Betrachtung.

PDA

Es sollten hier Geräte zum Einsatz kommen, deren Geräte-ID im Windows Device-Manager identifiziert werden kann. Außerdem ist für PDAs zur Synchronisation ein entsprechendes Programm erforderlich, was ebenfalls für Kontrollstrukturen nutzbar ist.

Memory-Sticks

Auch hier sollten möglichst Hersteller gewählt werden, die eine eindeutige Identifikation des Gerätes ermöglichen.

Alle anderen Geräte (Externe Festplatten Kameras, MP3 Spieler, etc.) lassen sich im Prinzip auf diese beiden Typen zurückführen.

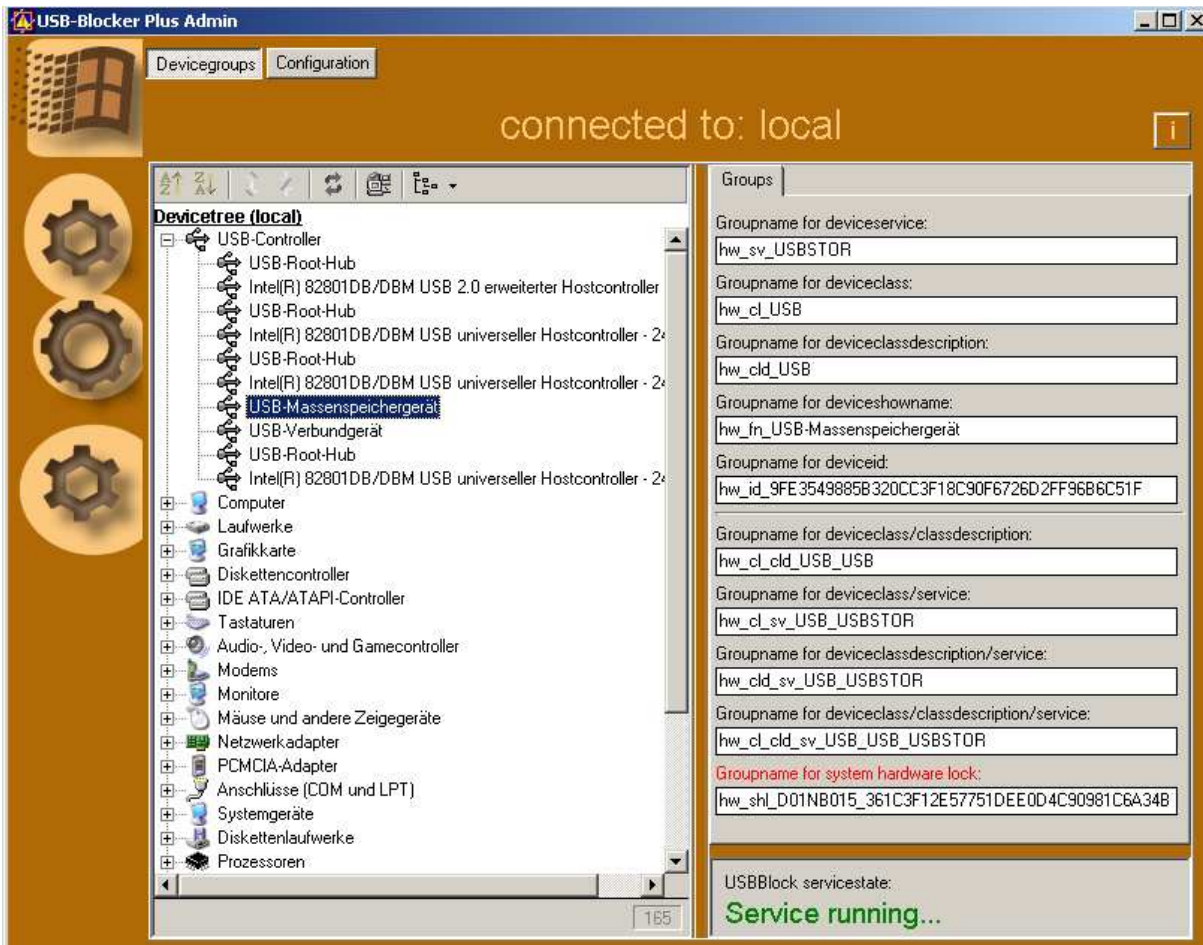


Bild2: Analyse der Daten eines Memo-Sticks und die automatische Generierung eines Gruppennamens im Directory im USB-Blocker PLUS

Sonstige Speichermedien

Sowohl CD als auch DVD-Brenner können im Prinzip als mobile Geräte betrachtet werden. Dies zudem noch in zwei Richtungen, einmal die Brenner selbst um Datenträger zu beschreiben und dann letztlich die Medien mit den Daten. Obwohl diese Geräte relativ einfach mit „Bordmitteln“ des Betriebssystems über Policies in Richtung auf personenbezogene Freigaben gesteuert werden können, wird vielfach ein einheitliches Tool über alle mobilen Geräte und Medien gewünscht.

Authentifizierung / Kryptierung

Eine gerätebezogene Authentifizierung verbunden mit einer evtl. Kryptierung der Daten unterstützen die Personalisierung der Nutzung mobiler Geräte und damit die Absicherung gegen fremde Nutzung. Derselbe Effekt lässt sich auch mit „externer“ Intelligenz erreichen, indem das Notebook oder der PC die Daten so verschlüsselt, dass diese nur von der erzeugenden Person lesbar sind. Außerdem lassen sich diverse Geräte und Medien soweit personalisieren, dass sie nur von zugelassenen Personen genutzt werden können.

Eine bereits aus der Diskettenzeit bekannte Möglichkeit der Datenverschlüsselung mit einem Unternehmens-Key sollte auch heute wieder in Betracht gezogen werden. Damit kann erreicht werden, dass Daten die von einem Unternehmens-PC auf einem Memo-Stick gespeichert werden, wiederum nur von einem PC im Unternehmensnetz gelesen werden können.

Steuerung über Installationsprogramme

Diverse Geräte benötigen zur Kommunikation mit einem PC ein zu installierendes Programm. Hiermit ist eine weitere Möglichkeit der Steuerung und Kontrolle der Nutzung externer Geräte gegeben. Dazu gehören typischerweise PDAs (ActiveSynch) und auch intelligente Mobiltelefone (Phonetools). In einem gut verwalteten Unternehmensnetz haben die Nutzer (normalerweise) keine lokalen Adminrechte, so dass die Nutzung dieser Geräte über eine gesteuerte Software-Zuteilung (User- und Berechtigungsverwaltung) zugeordnet werden kann. Somit kann ein nicht-berechtigter Nutzer ein PDA im Synchronisationsmode auch *nicht* nutzen, da ihm die dafür erforderliche Software nicht bereitgestellt wird. In der weiteren Stufe kann die Steuerung dann auf das Gerät selbst ausgedehnt werden, soweit die USB-Control-Software (wie z.B. der USB-Blocker PLUS) dazu in der Lage ist.

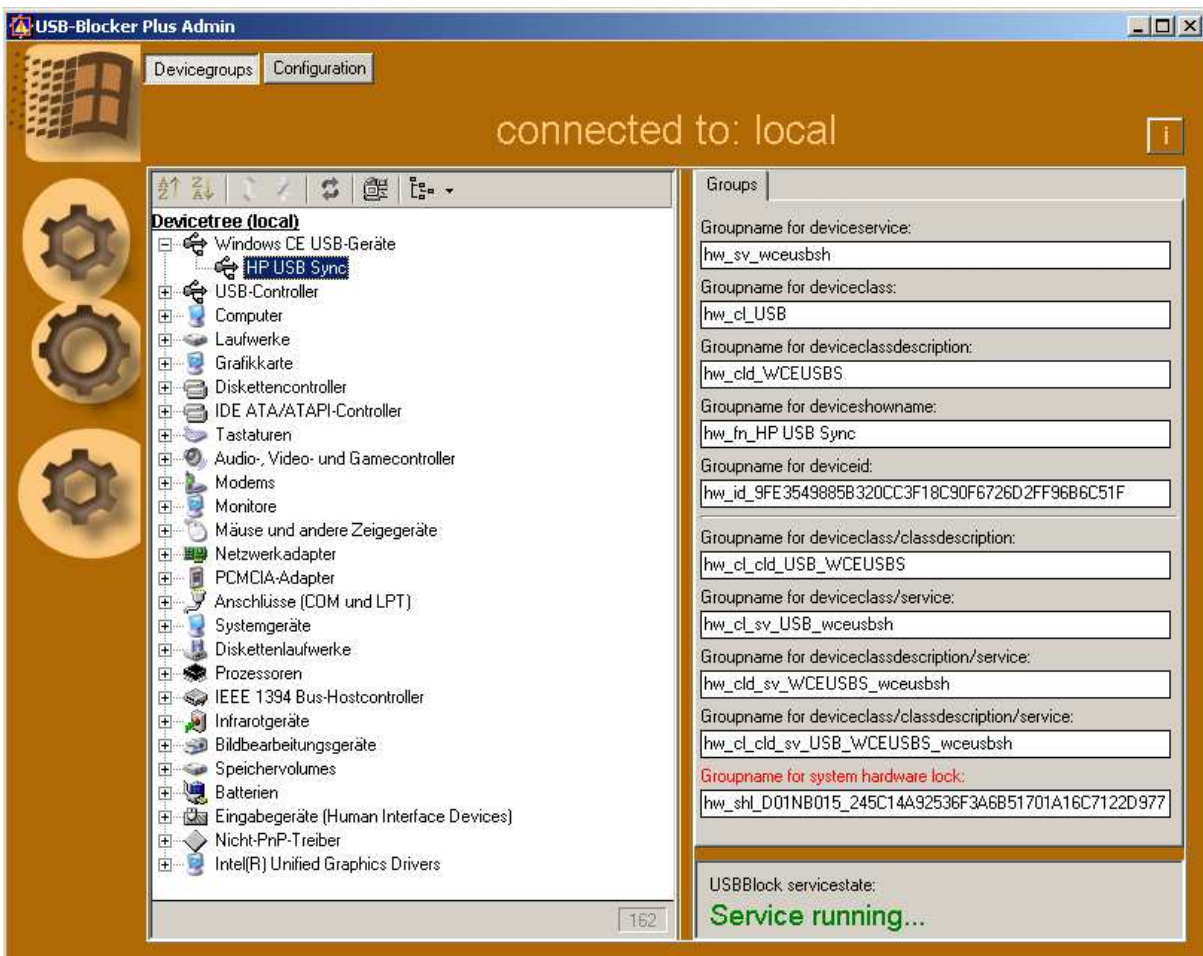


Bild 3: Erkennung des HP-PDA durch den USB-Blocker PLUS

Ein letzter möglicher Schritt wäre das aktive Auslesen der herstellerspezifischen Geräte-ID aus dem PDA und die Nutzung dieser Information zur Berechtigungssteuerung bezogen auf ein individuelles Gerät. Hierzu ist aber ein Programm erforderlich, das mit der Logik im PDA kommuniziert.

3 Benutzerverwaltung

Für die Benutzerverwaltung gibt es zwei, in der Effektivität und in der Einhaltung der Sicherheits-vorgaben grundsätzlich unterschiedliche, Möglichkeiten:

1. Verwaltung in einem der üblichen Directory-Systeme (ADS, NDS,...)
2. Verwaltung in einer Zentralen Nutzer- und Berechtigungsverwaltung über ein oder mehrere Director(y)ies.

Wobei die 2. Möglichkeit auf die 1. aufsetzt und insbesondere für große Unternehmen von Bedeutung ist.

3.1 Verwaltung der Nutzung in einem Directory

Eine relativ einfache Methode besteht darin, die Geräte bzw. ihre Geräteklasse durch ein geeignetes Tool (z.B. den USB-Blocker PLUS) zu identifizieren und daraus abgeleitet, im Directory eine entsprechende Gruppe anzulegen. User, die Mitglied dieser Gruppe sind, haben dann die Berechtigung dies Gerät bzw. Geräte dieses Typs zu nutzen. Die Qualität eines solchen Tools wird dadurch bestimmt, in welchem Maße es die einzelnen Verwaltungsschritte und die Sperrung bzw. Freigabe automatisiert unterstützt. Ein solches Tool sollte neben dem ADS als Directory auch NDS und LDAP unterstützen.

3.2 Verwaltung von Nutzungs-Berechtigungen mobiler Devices in großen Unternehmen

In großen Unternehmen mit vielen Nutzern und einer komplexer IT-Struktur wird die oben beschriebene Vorgehensweise schnell unhandlich, nicht in Abhängigkeit von der Tätigkeit des Users aktualisierbar und vor allem nicht eindeutig nachvollziehbar.

Dies liegt daran, dass die Rechte direkt dem User zugeordnet werden. Diese Zuordnung unterliegt keinerlei maschinellen Regel und vor allem nicht den Änderungsprozessen. Wenn ein User ein solches Device auf Grund einer geänderten Tätigkeit (z.B. vom Außendienst zum Innendienst) nicht mehr benötigt, erfolgt bei der personenbezogenen Zuordnung in der Regel keine Veränderung.

Außerdem werden die durch mobile Devices generierten Administrationstätigkeiten schnell so umfangreich, dass sie nicht mehr sinngerecht gehandhabt werden. Eine Nachvollziehbarkeit in Bezug auf die Beantragung eines solchen Rechtes ist in fast allen Fällen auch nicht gegeben.

Der Ausweg liegt hier in der Lösung der Berechtigung von der direkten personenbezogenen Zuordnung hin zu einer rollenbezogenen Zuordnung. Beispielsweise kann man, wie im Bild unten angegeben jedem internen Mitarbeiter das Recht geben, einen Memo-Stick zu benutzen.

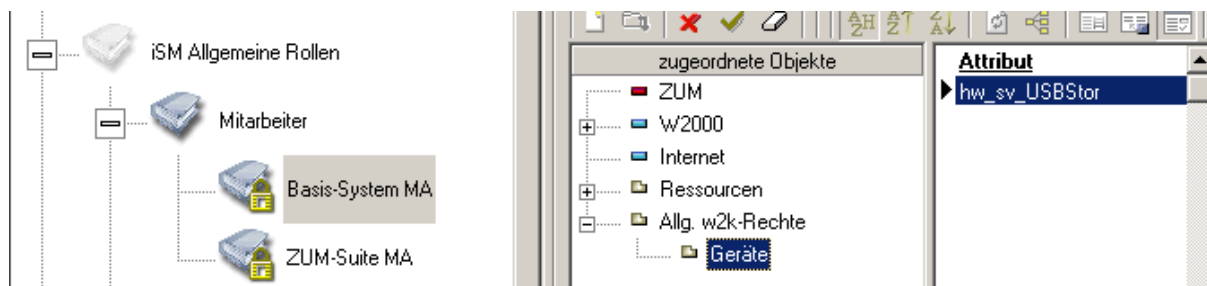


Bild 4: Zuweisung des Memo-Sticks zu jedem internen Mitarbeiter

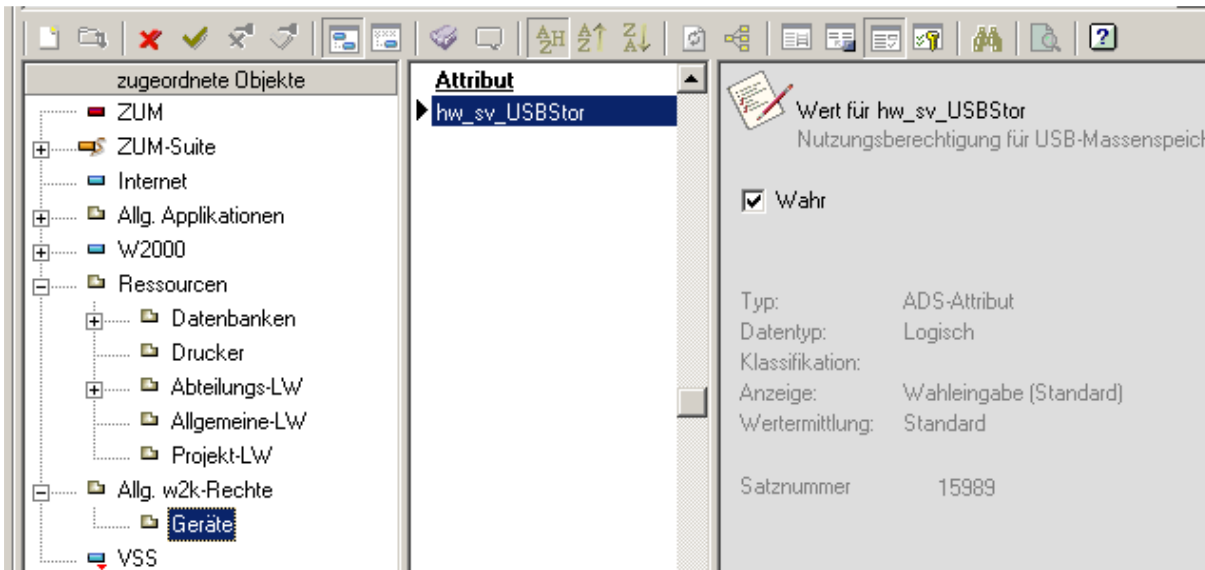


Bild 5: Zuweisung des Memo-Sticks zu jedem internen Mitarbeiter

Über die Rolle erhält ein Mitarbeiter das entsprechende Recht, ohne dass ein Administrator eingreifen muss. Wenn dieser Mitarbeiter dann z.B. zum Externen wird, wird ihm dies Recht automatisch entzogen.

Eine weitere Komponente kann dann diese Zuordnung aus Sicht des Standortes und der Abteilung verwalten.

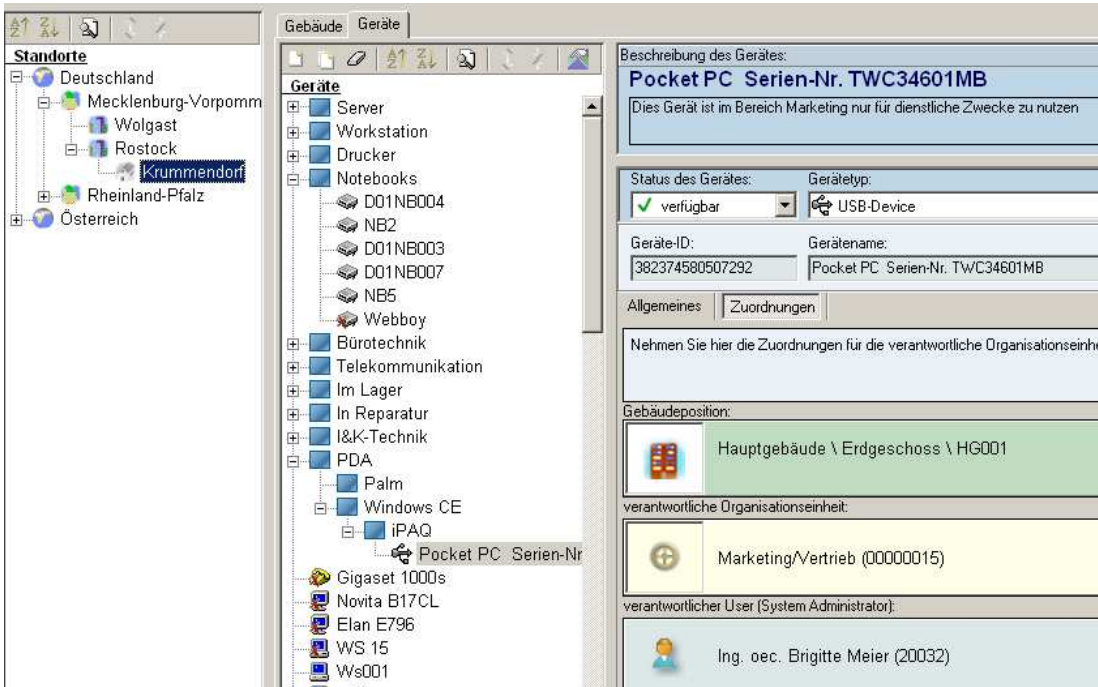


Bild 6: Verwaltung der Zuordnung aus Sicht des Standortes und der Abteilung

4 Zusammenfassung

In diesem Manuskript wird die Vielfalt der Steuerungsmöglichkeiten in Richtung Mobile Security dargestellt. Auch hier ist für jedes Unternehmen eine generelle Richtlinie zu erarbeiten, die ausgehend von der zu beeinflussenden Risiken die Zielstellung für den Technik-Bereich vorgibt. Diese Ziele richten sich auch nach den Notwendigkeiten der Nutzung mobiler Geräte und deren Nutzungsgrad und funktioneller Tiefe sowie den Funktionen bzw. Rollen der Mitarbeiter. Erst wenn diese Vorgaben erarbeitet wurden, ist das Technik-Team in der Lage aus der Vielfalt aller Geräte und deren Security-Möglichkeiten ein entsprechendes Einsatzkonzept zu erarbeiten.

Von besonderer Bedeutung ist hierbei die Größe und Komplexität eines Unternehmens, um die technisch vorhandenen Möglichkeiten auch sinnvoll organisatorisch einbetten zu können.