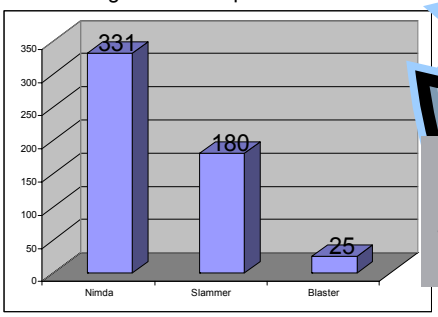
3A03 – Security Löcher schnell und effizient schließen mit HP OpenView Radia

Alexander Meisel

HP OpenView

Patch Management *Why do I need it?*

Time in days from issue of Bulletin to acknowledgement of Exploit



Just in…

- Bulletin MS04-011 issued April 13th 2004
- Sasser Exploit acknowledged 1st May 2004
- 18 days!

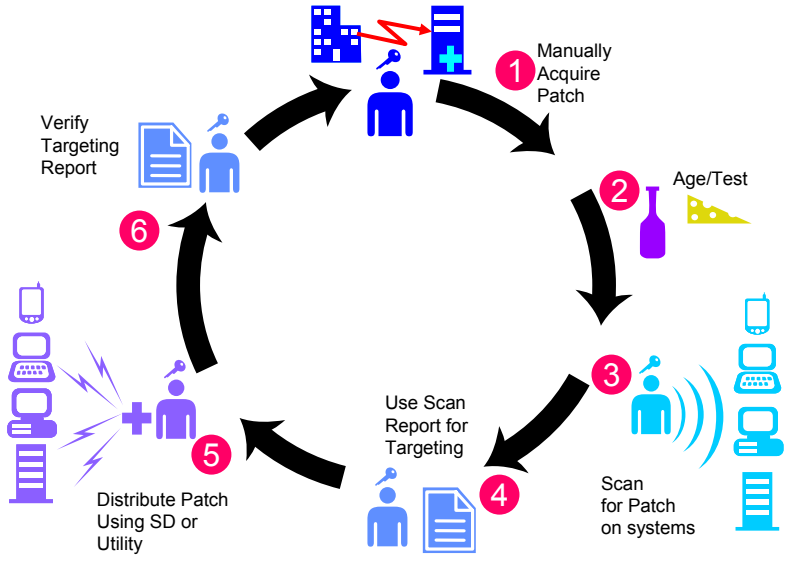
Patch Management

- Risikominimierung
  - Sicherheitslücken schaden dem Geschäft
    - *"The SQL Slammer worm caused between $950 million and $1.2 billion in lost productivity in it's first five days worldwide. (cnet news)"*
  - Anpassung an Veränderungen mit hoher Zuverlässigkeit wird benötigt
  - 95% der Lücken sind durch proaktives Patchmanagement vermeidbar*
- Kosten
  - Implementation von automatisierten Patchmanagementlösungen reduzieren die Helpdesk-Calls und damit die Kosten
- Hohe Effektivität
  - IT muß 24/7 Service unterstützen und trotzdem hohe Skalierbarkeit, niedrige Kosten, Flexibilität erreichen

* Source : CERT

3

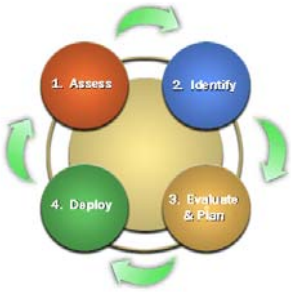
Patch Prozess



Patch Process*

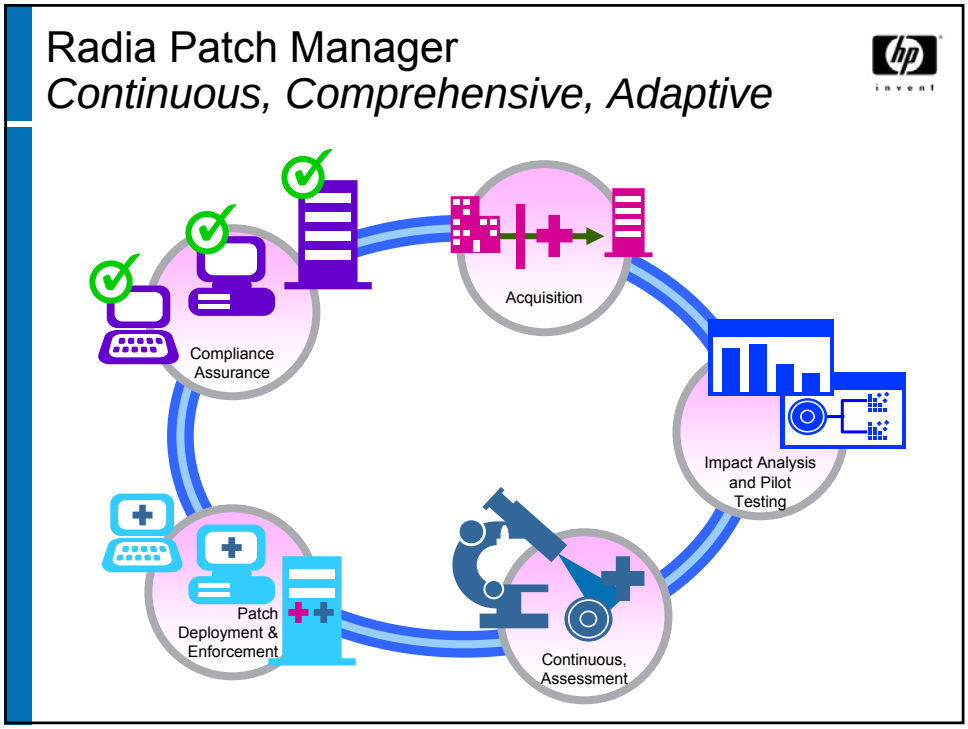
1. **Audit machine** production environment to determine operational baseline (daily for servers, weekly for workstations)
2. **Confirm** that the **audit** has taken place and identify machines that have not been audited. (daily for servers, weekly for workstations)
3. **Check security web** sites to determine whether new patches are available. (Daily).
4. **Scan production environment** for required patches. (weekly).
5. **Assess patch prerequisites**, sequences and conflicts. (per required patch)
6. **Pilot patch release** in production environment. (per required patch)
7. **Deploy patch** release to production environment. (per patch)

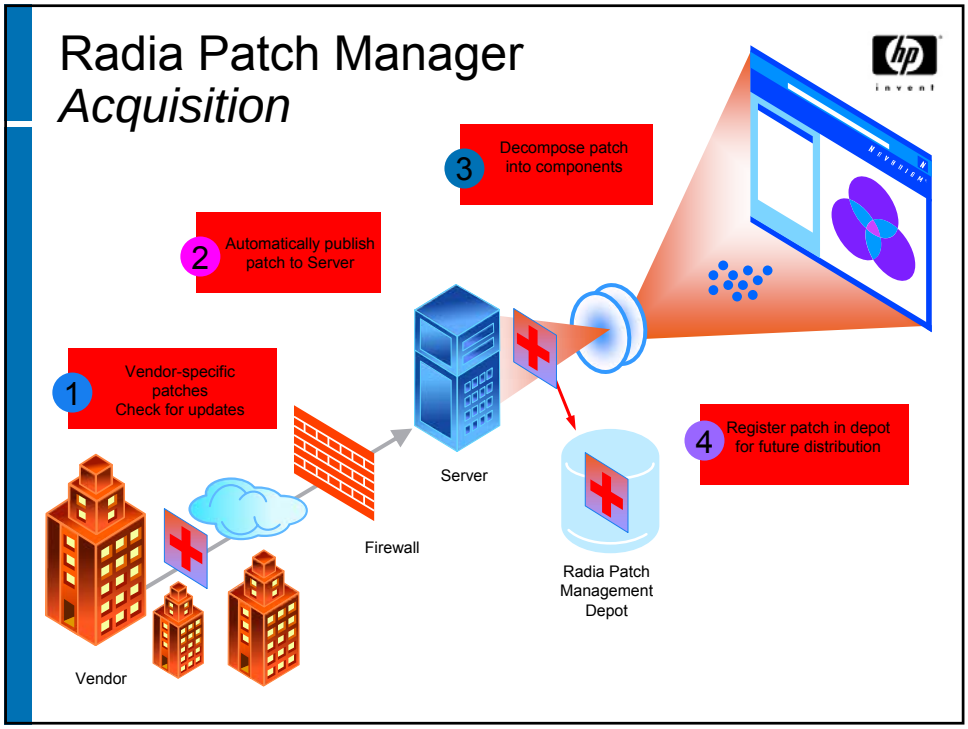
*see Microsoft TechNet Patch Management Prozess



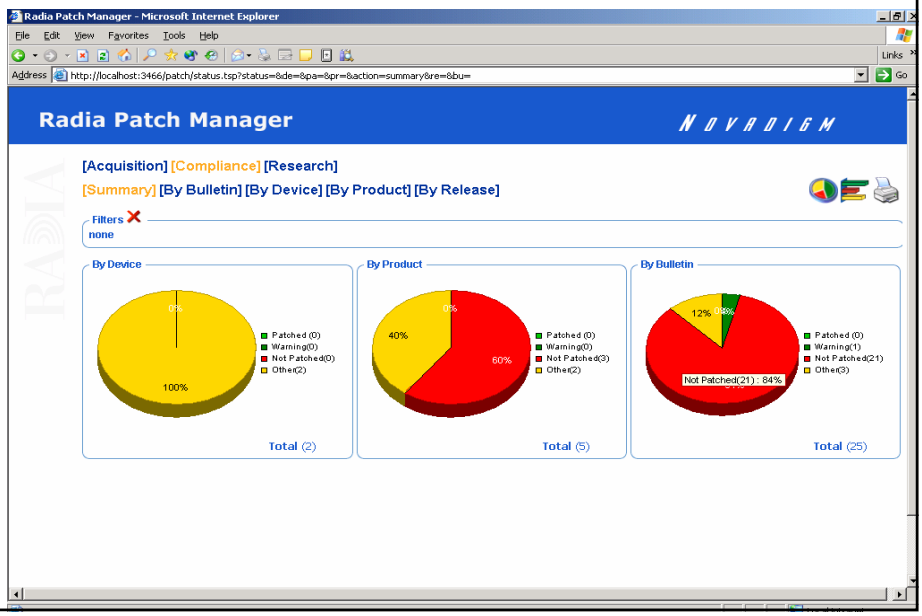
Patch Management Prozess

- Viel Automatisierungspotential
- Lösungen für Client und Server Bereich notwendig
- Windows, Linux, UNIX ???

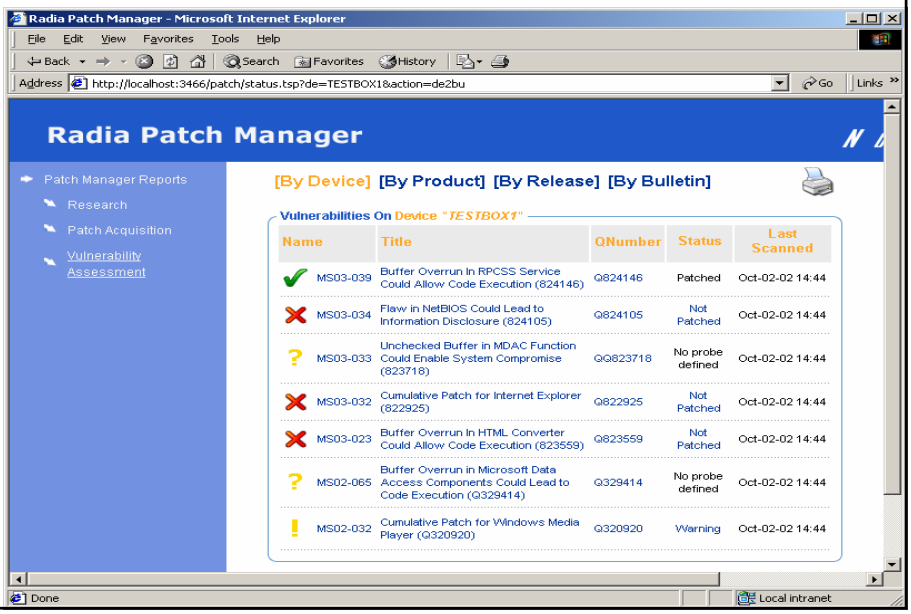

Radia Patch Manager
Continuous, Comprehensive, Adaptive
Acquisition
Impact Analysis and Pilot Testing
Continuous, Assessment
Patch Deployment & Enforcement
Compliance Assurance


Radia Patch Manager
Acquisition
3 Decompose patch into components
2 Automatically publish patch to Server
1 Vendor-specific patches Check for updates
4 Register patch in depot for future distribution
Server
Firewall
Radia Patch Management Depot
Vendor

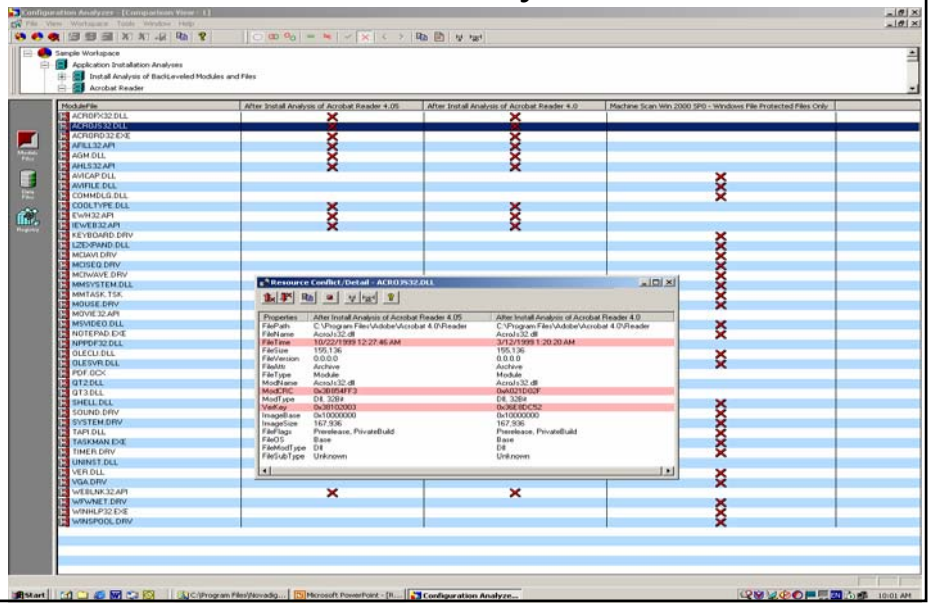
RADIA Patch Manager Reports



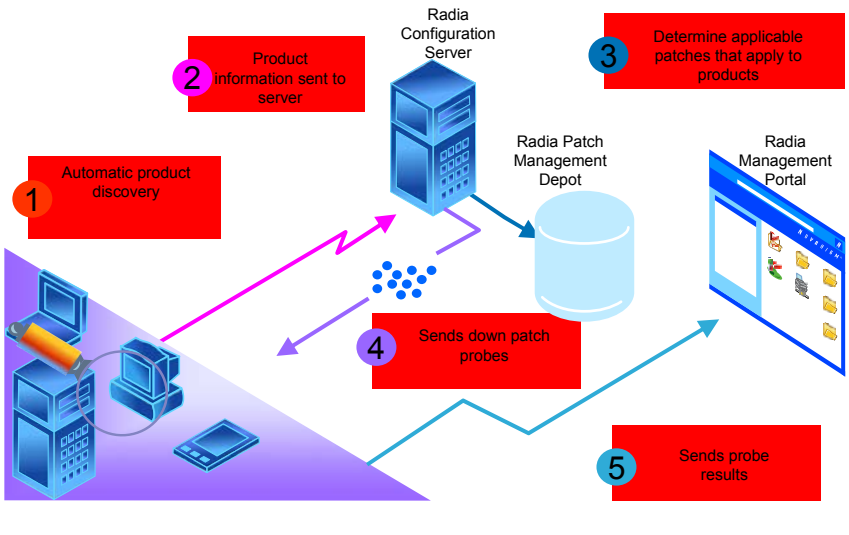
RADIA Patch Manager Reports



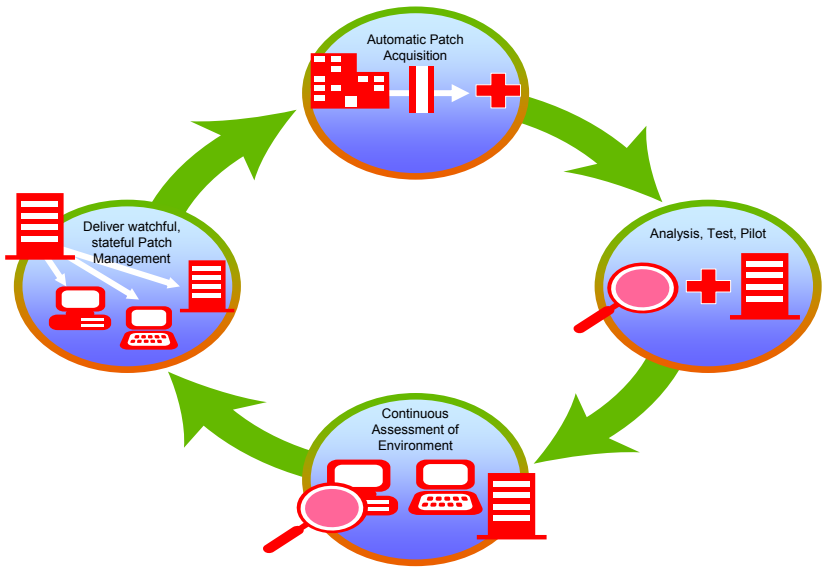
Erweiterte Konflikt Analyse



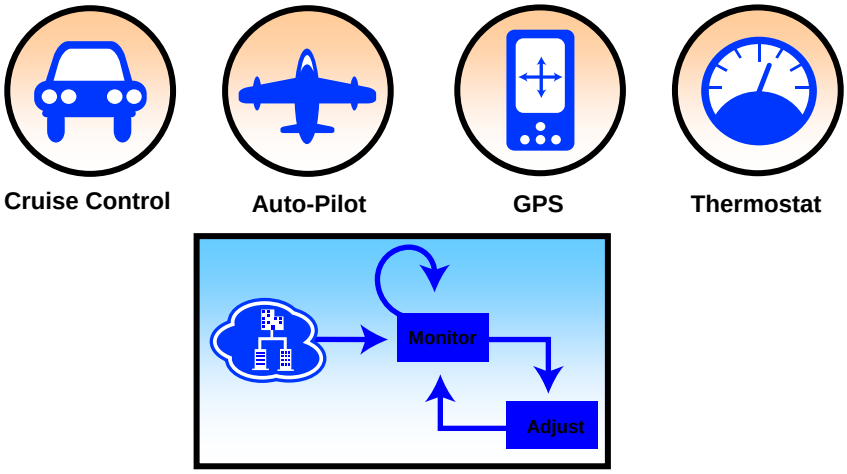
Radia Patch Manager
Automatic Assessment



Radia Patch Manager
Process Driven Patch Management



Was ist Desired State Management?



Zusammenfassung

- Patch Management in heterogener Client und Server Umgebung (Windows, Linux, Solaris*, HP-UX*) schließt schnell Sicherheitslücken (* later 2005)
- Automatische Akquise und Analyse der Verwundbarkeit
- Reduzierte Test-Aufwände durch Konflikt Analyse
- Desired State Management stellt dauerhaft sichere Umgebung sicher
- Objekt-orientiertes Modell ermöglicht Bandbreitensteuerung und einfachste Zuweisung auf Basis von Organisationsstrukturen (Verzeichnisse)