



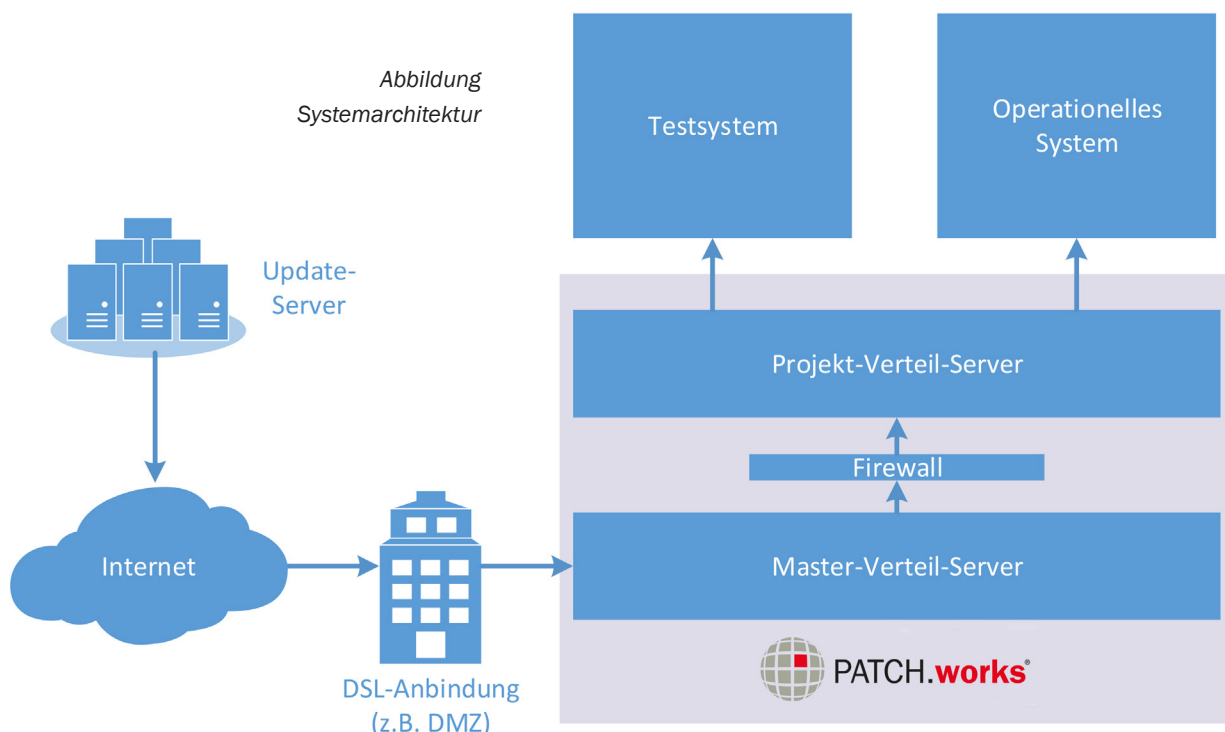
PATCH.works®

Patch Managementsystem für IT-Systeme der Bw

IT-Systeme in den verschiedenen Vorhaben der Bundeswehr werden häufig als geschlossene Systeme ohne Zugang zum Internet betrieben. Die in diesen „grünen“ Systemen enthaltenen Softwareprodukte bedürfen – ebenso wie in offenen Systemen – einer kontrollierten und speziell für die Virenschutzsoftware einer permanenten Aktualisierung. Aufgrund der fehlenden Internetverbindung müssten die zur Aktualisierung von den Produktherstellern zur Verfügung gestellten Patches ggf. über eine Drehstuhlschnittstelle eingespielt werden. Dieses Verfahren ist zeit- und ressourcenaufwendig sowie fehleranfällig. Die Aspekte *Automatisierung, Vereinheitlichung und Entlastung der Administratoren* werden nicht adäquat berücksichtigt. PATCH.works® bietet für diese Problemstellung die richtige Lösung.

Systemkonzept

Das Patch-Managementsystem PATCH.works® stellt Software Updates in geschlossenen Systemen ohne Internetzugang bereit und erlaubt eine problemlose Integration in unterschiedliche Einsatzumgebungen durch eine generische Systemarchitektur. Das am Internet angeschlossene System, welches Updates von den Servern der Produkthersteller empfängt, ist der Master-Verteil-Server; nach ihm, durch eine Firewall getrennt, folgt der Projekt-Verteil-Server, welcher die Rechner im Projektbereich versorgt. Hierbei wird die absolute Trennung des operativen Systems zum Internet sowie ein zusätzlicher Virenschutz – unter Wegfall der Drehstuhlschnittstelle – gewährleistet.



Master-Verteil-Server

- Automatisches Beziehen von Updates der Hersteller, über Internet/Intranet (z.B. via WANBw, Strausberg)
- Integritätsprüfung durch Virens Scanner
- Update-Bereitstellung auf Download-Servern (passiv)



Projekt-Verteil-Server

- automatisches Herunterladen vom Master-Verteil-Server
- getrennte Bereitstellung für Test- und Produktionsumgebung
- Bereitstellung auf unabhängigen (passiven) Download-Servern
- manueller Test im Testsystem, dann Freigabe für Produktionsumgebung
- Steuerung durch automatisierten Zeitplan möglich

Administration

Die Administration der verschiedenen Komponenten im Master- und den Projekt-Verteil-Servern erfolgt über ein webbasiertes Portal, in dem alle Funktionen gebündelt sind.

Systemeigenschaften

PATCH.works® erfüllt die folgenden Anforderungen:

- Technologieunabhängige und generische Lösung, bestehend aus Hardware und Software
- Trennung in zwei „Hälften“ für Netzflusskontrolle oder Schutzbereichsübergang
- Automatisierung, Vereinheitlichung, Administrationsentlastung
- Kontrolle und Steuerung der Update-Freigabe durch die Administratoren

Folgende Softwareprodukte werden aktuell von PATCH.works® unterstützt:

- Windows Betriebssysteme
- Linux Debian, Redhat (centos) und OpenSUSE
- Virenschutz Symantec Endpoint Protection
- Anwendungssoftware: Acrobat Reader, Adobe Flash, Mozilla Firefox und Java Runtime

Patch Management in unterschiedlichen Sicherheits-Domänen

Existieren unterschiedliche Sicherheits-Domänen, so kann beispielsweise der Projekt-Verteil-Server über das **SDoT**® Security Gateway mit dem Master-Verteil-Server verbunden werden.

- Updates werden von Download-Servern des Master-Verteil-Servers über das **SDoT**® Security Gateway heruntergeladen
- Getrennte Bereitstellung für Test- und Produktionsumgebung
- Manueller Test im Testsystem, anschließend Freigabe für Produktionsumgebung
- Steuerung durch automatischen Zeitplan

