baramundi

Leitfaden

Microsoft Update Management

Whitepaper

Empower your IT

INHALT

1 Vom schnellen Pflaster zur monatlichen Routine

1.1 Vom Patch zum Update

Über die vergangenen zwei Jahrzehnte wurden Admins und IT-Verantwortliche hervorragend konditioniert: Die eingesetzte Software muss regelmäßig aktualisiert werden. Mit zunehmender Digitalisierung und Vernetzung durfte ein Endpoint nicht mehr isoliert, sondern musste als Teil eines schützenswerten Kollektivs betrachtet werden. Sicherheitslücken an einem Endpoint beeinträchtigten nicht mehr nur die Sicherheit des einzelnen Geräts, sie schwächten die Sicherheit des gesamten Unternehmens.

Die Softwarehersteller reagierten mit der Bereitstellung von Patches für einzelne Sicherheitslücken – die Verantwortlichen konnten so selbst entscheiden, ob und welche Lücken sie schließen möchten. Im Laufe der Zeit wurden immer schneller immer mehr Patches in unregelmäßigen Abständen bereitgestellt. Damit wurde es schwer, den Überblick zu behalten. Um diesem Umstand zu begegnen, führten immer mehr Unternehmen – allen voran Microsoft – den sogenannten „Patch Day“ ein. An einem festgelegten Tag im Monat wurde eine bunte Mischung von Sicherheitspatches veröffentlicht. Die IT-Abteilung hatte dann regelmäßig die Aufgabe, diese Patches zu testen und im Unternehmen zu verteilen. Die teils aufwendigen Tests waren nötig, denn ein Patch konnte u.U. auch ein System lahmlegen und dauerhaft unbrauchbar machen. Im Laufe der Zeit wurden am Patch Day zusätzlich zu den sicherheitsrelevanten Patches auch Updates für Funktionen im Betriebssystem verteilt. Nun mussten die Admins nicht mehr nur Sicherheitspatches testen, sondern auch die zahlreichen Updates. Das erzeugte zusätzlichen Aufwand und kostete Zeit. Auch nach einer Neuinstallation von Windows mussten alle benötigten Patches in der entsprechenden Reihenfolge – häufig auch mit zahlreichen Neustarts – installiert werden.

Die IT-Abteilungen zogen ihre Konsequenzen und gingen teils dazu über, nur noch selektiv zu aktualisieren. Besonders kritische Patches wurden getestet und installiert, weniger kritische Patches und Funktionsupdates wurden ausgelassen.

Microsoft begegnete dieser Problematik mit einer Veränderung der Aktualisierungsstrategie und führte kumulative Updates ein. Diese monatlich erscheinenden Updatepakete beinhalten neben den aktuellen Sicherheitspatches und Funktionsupdates auch die Patches und Updates der vorhergehenden Pakete. So muss bspw. nach einer Neuinstallation nur noch das aktuellste kumulative Update installiert werden, statt einer mittleren dreistelligen Anzahl an Patches. Das spart Zeit, bedeutet aber auch das Ende der selektiven Installation einzelner Patches (s.g. „Cherry picking“).

1.2 Das Microsoft Update Paradigma

Wie jeder verantwortungsvolle Softwarehersteller empfiehlt natürlich auch Microsoft, die verwendeten Endpoints möglichst vollständig aktuell zu halten. Gleichzeitig ist aber auch nachvollziehbar, dass nicht alle Endpoints zur selben Zeit mit denselben Updates versorgt werden können und sollten. Schließlich gibt es immer Endpoints, welche kritischer sind als andere. So wird ein Standard Office-PC in der Regel weniger kritisch für den Unternehmensbetrieb als bspw. ein Messrechner oder speziell konfigurierter CAD-Rechner eingestuft. Ersterer könnte im Problemfall deutlich unkomplizierter ausgetauscht werden als die beiden spezialisierten Geräte.

1.3 Das Ring-Konzept von Microsoft

Auf diesem Prinzip basiert auch das Ring-Konzept von Microsoft[1]. Ein Ring umfasst Geräte, welche ein Update zur selben Zeit erhalten. Diese Geräte sollten einen möglichst breiten und repräsentativen Querschnitt des Unternehmens – kategorisiert nach Kritikalität – abbilden. Typische Ringe könnten sein:

- **Preview – Vorschau und erste Tests**
  Der Vorschau-Ring ist nicht für die breite Verwendung im Unternehmen vorgesehen und dient der Auswertung von neuen Features eines Updates. In diesem Ring befinden sich vornehmlich die Geräte von technisch versierten Personen. Diese verlieren nicht automatisch an Produktivität, wenn etwas nicht nach Plan verläuft – ebenso die klassischen Test-Clients.
- **Early Adopters – Piloten und Überprüfung**
  Die Zusammenstellung dieses Rings erfordert eine gute Planung. Er sollte sich aus repräsentativen Geräten des Unternehmens zusammensetzen. Das bedeutet, dass hier alle Hardware und Anwendungen vertreten sein sollten. Selbstverständlich sollten diese Geräte auch regelmäßig genutzt werden, um eventuelle Probleme schnell aufzufinden.
  Insbesondere die IT-Abteilung und Testgeräte gehören nicht in diesen Ring, da sie meist nicht die breite Masse der Unternehmensgeräte repräsentieren.
- **Broad – Breite Verteilung im Unternehmen**
  In diesem Ring befinden sich nun alle restlichen Geräte, welche nicht in den zuvor benannten Ringen zu finden sind.

Mit diesen drei Ringen ist eine sehr zeitnahe Verteilung möglich. Erfahrungsgemäß reichen drei Ringe in der Praxis nicht aus, um komplexere Strukturen abzubilden. Daher ist die Anzahl der Ringe von Microsoft nicht begrenzt um eine weitere Unterteilung in Standorte oder auch Funktion (Client/Server) zu ermöglichen. In großen Unternehmen ist es zudem ratsam, bei der Größe der Ringe auch die Kapazität des Helpdesks zu berücksichtigen. Die konfigurierten Ringe können nacheinander aber auch überlappend mit Updates versorgt werden. Hierbei ist es sinnvoll, den Automatismus der baramundi Management Suite zu verwenden um nur im Fehlerfall manuell eingreifen zu müssen. Das bedeutet, dass die Geräte innerhalb der Ringe mit einem, von den Admins definierten, zeitlichen Versatz automatisch aktualisiert werden.

[1] https://docs.microsoft.com/de-de/windows/deployment/update/create-deployment-plan

2 Funktionsweise des baramundi Microsoft Update Managements

2.1 Updateprofile

Das Update Management der baramundi Management Suite setzt konsequent auf das Ring-Konzept von Microsoft und erweitert es um die Möglichkeit, einzelne Updates, aber auch ganze Produktlinien und sogar komplette Kategorien vom Updateprozess auszuschließen. Mithilfe einer Sperrliste entfällt die manuelle Freigabe der Updates. Neue Updates sind automatisch freigegeben und werden mit einem konfigurierten zeitlichen Versatz zum Veröffentlichungsdatum installiert, beginnend mit dem unkritischsten Ring.
Die Einteilung in die verschiedenen Ringe sowie die Konfiguration der Sperrlisten erfolgt durch Updateprofile – jeder Ring bekommt ein eigenes Updateprofil. Ebenso werden die Einstellungen im Updateprofil bei der Bewertung des Updatestatus eines Endpoints berücksichtigt. Die Verwaltung der Updateprofile wird in Kapitel 5.1 beschrieben.

2.2 Klassifizierungen

Alle Updates von Microsoft sind in Klassifizierungen eingeteilt, welche Microsoft wie folgt beschreibt[2]:

- **Security Updates**
  Eine allgemein freigegebene Korrektur für eine produktspezifische Sicherheitslücke. Sicherheitsrisiken werden anhand ihres Schweregrads im Microsoft-Sicherheitsbulletin als kritisch, wichtig, moderat oder niedrig eingestuft.
- **Critical Updates**
  Ein allgemein veröffentlichter Fix für ein bestimmtes Problem, das einen kritischen, nicht sicherheitsrelevanten Fehler behebt.
- **Definition Updates**
  Ein häufig veröffentlichtes Softwareupdate, das Ergänzungen zur Definitionsdatenbank eines Produkts enthält. Definitionsdatenbanken werden häufig verwendet, um Objekte mit bestimmten Attributen zu erkennen, z. B. bösartigen Code, Phishing-Websites oder Junk-E-Mails.
- **Updates**
  Ein allgemein veröffentlichter Fix für ein bestimmtes Problem. Ein Update behebt einen nicht kritischen, nicht sicherheitsrelevanten Fehler.
- **Upgrades**
  Inplace Aktualisierung von Windows 10 (z.B. von 1909 auf 2004). Diese werden über das Modul baramundi OS-Install durchgeführt, da nur so eine Anpassung der Windows-Installation an Unternehmensrichtlinien möglich ist.
- **Service Packs**
  Ein getesteter, kumulativer Satz aller Hotfixes, Sicherheitsupdates, kritischen Updates und Updates. Service Packs können zudem weitere Korrekturen für

[2] https://docs.microsoft.com/de-de/troubleshoot/windows-client/deployment/standard-terminology-software-updates

Probleme enthalten, die seit der Veröffentlichung des Produkts intern gefunden wurden, aber auch eine begrenzte Anzahl an vom Kunden geforderten Designänderungen oder Features.

- **Tools**
  Ein Hilfsprogramm oder Feature, das beim Ausführen einer Aufgabe oder einer Gruppe von Aufgaben hilft.
- **Feature Packs**
  Neue Produktfunktionalität, die zuerst außerhalb des Kontexts einer Produktversion verteilt wird und häufig in der nächsten vollständigen Produktversion enthalten ist.
- **Update Rollups**
  Ein getesteter, kumulativer Satz von Hotfixes, Sicherheitsupdates, kritischen Updates und Updates, die für eine einfache Bereitstellung gepackt sind. Ein Rollup zielt im Allgemeinen auf einen bestimmten Bereich ab.
- **Drivers**
  Software, die die Interaktion mit Geräten steuert.

2.3 Microsoft Update for Business (ab Windows 10)

Mit Microsoft Update for Business hat Microsoft eine neue Nomenklatur für Updates eingeführt.

Microsoft unterscheidet hier nicht anhand der genannten Klassifizierungen, sondern wie folgt:

- **Feature Updates**
  Wird zweimal pro Jahr veröffentlicht, in der ersten und zweiten Hälfte jedes Kalenderjahrs. Feature Updates fügen neue Features und Funktionen zu Windows 10 hinzu.
- **Qualitätsupdates (Kumulative Updates)**
  Bieten sowohl Sicherheitsupdates als auch nicht sicherheitsrelevante Fixes für Windows 10. Qualitätsupdates umfassen Sicherheitsupdates, wichtige Updates, Wartungsstapelupdates und Treiberupdates. Sie werden in der Regel am zweiten Dienstag jedes Monats veröffentlicht, können jedoch jederzeit veröffentlicht werden. Die Zweite-Dienstag-Version ist die Version, die sich auf Sicherheitsupdates konzentriert. Qualitätsupdates sind kumulativ, sodass die Installation des neuesten Qualitätsupdates ausreicht, um alle verfügbaren Fixes für ein bestimmtes Windows 10 Feature Update zu erhalten, einschließlich aller Out-of-Band-Sicherheitsupdates und aller Wartungsstapelupdates, die möglicherweise zuvor veröffentlicht wurden.
- **Treiberupdates**
  Diese Updatetreiber gelten für Ihre Geräte. Treiberupdates sind in Windows Server Update Services (WSUS) standardmäßig deaktiviert, für cloudbasierte Updatemethoden können Sie jedoch steuern, ob sie installiert sind oder nicht.
- **Microsoft Produktupdates**
  Diese aktualisieren andere Microsoft-Produkte, z. B. Office. Sie können Microsoft-Updates mithilfe von Richtlinien aktivieren oder deaktivieren, die von verschiedenen Wartungstools gesteuert werden.
- **Definition Updates**
  Ein häufig veröffentlichtes und häufiges Softwareupdate, das Ergänzungen zur Definitionsdatenbank eines Produkts enthält. Definitionsdatenbanken werden häufig verwendet, um Objekte mit bestimmten Attributen zu erkennen, z. B. bösartigen Code, Phishing-Websites oder Junk-E-Mails.
- **Wartungsstapelupdates (SSU)**
  Diese Updates nehmen eine Sonderrolle ein und sind nicht automatisch über das Update Management installierbar. Sie aktualisieren die Updatekomponenten, welche für die eigentlichen Updates benötigt werden. Diese SSUs erscheinen unregelmäßig und deutlich seltener als die regulären Updates.

2.4 Voraussetzungen

Das baramundi Microsoft Update Management unterstützt Windows ab Version 8.1 ohne weitere Anpassungen. Für Windows 7 SP1 und Windows Server 2008 R2 SP1 müssen mindestens folgende Voraussetzungen erfüllt sein:

- Unterstützung der SHA-2-Codesignierung vom September 2019 (KB4474419[3])
- Servicing Stack Update vom März 2019 (KB4490628[4])

Bei Windows Server 2008 SP 2 müssen mindestens folgende Voraussetzungen erfüllt sein:

- Unterstützung der SHA-2-Codesignierung vom September 2019 (KB4474419[3])
- Servicing Stack Update vom April 2019 (KB4493730[5])

Ältere Windows-Versionen werden nicht unterstützt.

2.5 Konfiguration der Gruppenrichtlinien

Da Microsoft empfiehlt, die Endpoints stets aktuell zu halten, wird auch Windows mit einer dementsprechenden Standardkonfiguration ausgeliefert. Um nun das volle Potenzial des Ring-Konzepts und baramundi Updateprofile nutzen zu können, muss diese Standardkonfiguration abgeändert werden.
Besonders hervorzuheben sind dabei die folgenden Konfigurationen:

- **Automatische Updates**
  Sowohl bei Verwendung der Online Quellen, als auch bei Einsatz des WSUS, müssen die automatischen Updates deaktiviert werden. Andernfalls aktualisiert sich Windows selbstständig und die Kontrolle liegt nicht mehr beim zentralen Management System.
- **Dualscan**
  Bei Verwendung des WSUS muss darauf geachtet werden, dass der Dualscan deaktiviert wurde. Andernfalls gibt es funktionale Einschränkungen beispielsweise bei der Verzögerung von Updates.
- **Updatequelle**
  Wird ein WSUS als Quelle für die Updates verwendet, muss die URL zum entsprechenden System per Gruppenrichtlinie vorgegeben werden.

Eine detaillierte Auflistung der benötigten und empfohlenen Einstellungen sowie eine Anleitung zur Konfiguration finden Sie in der baramundi Knowledge Base[6].

---

[3] https://support.microsoft.com/de-de/topic/unterst%C3%BCtzung-der-sha-2-codesignierung-f%C3%BCr-windows-und-wsus-2019-64d1c82d-31ee-c273-3930-69a4cde8e64f
[4] https://support.microsoft.com/de-de/topic/servicing-stack-update-ssu-f%C3%BCr-windows-7-sp1-und-windows-server-2008-r2-sp1-12-m%C3%A4rz-2019-b4dc0cff-d4f2-a408-0cb1-cb8e918feeba
[5] https://support.microsoft.com/de-de/topic/ssu-servicing-stack-update-f%C3%BCr-windows-server-2008-sp2-9-april-2019-8f49b928-2090-0cce-3ed6-21b6dc8c494b
[6] https://feedback.baramundi.de/knowledge-base/article/KB10911-EN

3 Microsoft Update Online

Microsoft stellt alle relevanten Updates über den eigenen Service „Microsoft Update“ zur Verfügung. Eine weiterer Onlinedienst ist „Windows Update“ – dies ist im Grunde dieselbe Quelle, allerdings mit reduziertem Umfang. Während „Microsoft Update“ Updates für alle unterstützten Microsoft Produkte (Exchange Server, MSSQL-Server, etc.) bereitstellt, sind per „Windows Update“ nur Updates für das eigentliche Betriebssystem zu finden.
Die Verwendung einer Onlinequelle bietet verschiedene Vor- und Nachteile. Zur Auswahl der für Ihre Umgebung passenden Quelle ist es wichtig, diese zu kennen.

3.1 Vorteile

- Sofortige Verfügbarkeit nach Freigabe durch Microsoft.
- Sicherheit, stets das korrekte Update in der richtigen Revision zu erhalten.
- Kein zentraler Speicherplatz nötig – Endpoints beziehen Installationsquellen direkt von Microsoft oder per Peer-to-peer (P2P).
- Aufwand für den Betrieb eines WSUS entfällt.

3.2 Nachteile

- Internetverbindung notwendig – Somit nicht nutzbar, wenn die Endpoints keinen Internetzugriff haben.

4 Windows Server Update Services

Mit dem Produkt „Windows Server Update Services“ kurz „WSUS“ stellt Microsoft eine Softwarekomponente zur Verfügung, welche es u.a. ermöglicht, die Microsoft Online Dienste im eigenen Firmennetzwerk zu spiegeln. Das ermöglicht die lokale Bereitstellung der zur Aktualisierung der Endpoints notwendigen Daten.
Selbstverständlich gibt es auch hier Vor- und Nachteile.

4.1 Vorteile

- Endpoints benötigen keine Internetverbindung.
- Updates werden nur einmal heruntergeladen und lokal vorgehalten.

4.2 Nachteile

- Zusätzlicher Aufwand für die Pflege der benötigten Infrastruktur.
- Verzögerte Verfügbarkeit der Updates möglich.
- Abweichende Daten zwischen lokalen und online Quellen, da am WSUS stets die Zeitstempel der lokalen Bereitstellung herangezogen werden.

5 Arbeiten mit dem baramundi Microsoft Update Management

5.1 Verwalten von Updateprofilen

Zunächst werden die für das eigene Unternehmen relevanten Ringe anhand eigener Kriterien definiert. Anschließend werden die zur Abbildung der Ringe benötigten Updateprofile in der baramundi Management Suite angelegt. Hierbei sollten aussagekräftige Namen und ggf. ergänzende Kommentare verwendet werden. Ebenso wird die Verzögerung der Updates in Tagen angegeben.

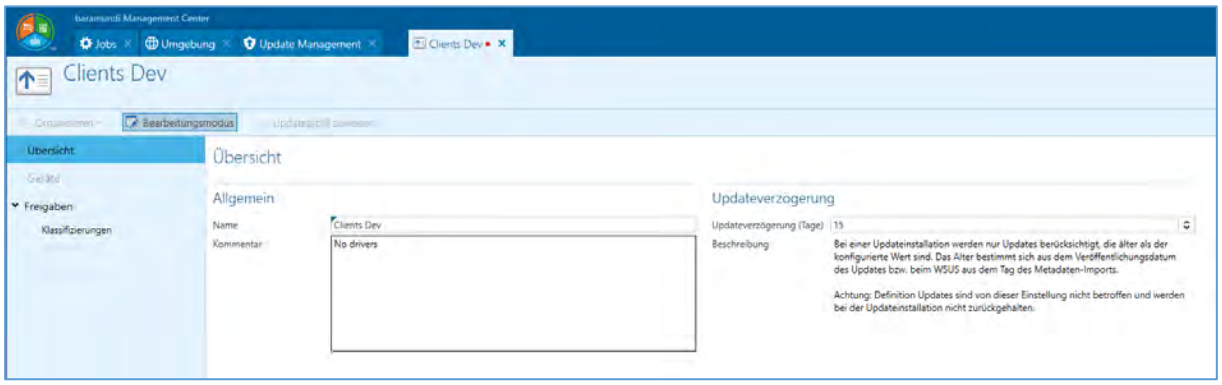

Abbildung 1 - Erstellung eines Updateprofils

Zu beachten ist hier, dass Definition Updates von der baramundi Management Suite grundsätzlich nicht verzögert werden, da dies die Funktion des Windows Defender Antivirus beeinträchtigen würde.

Im nächsten Schritt werden die generell freizugegebenen Klassifizierungen bestimmt. Aus Gründen der Sicherheit – und um ein möglichst durchgehend aktuelles System zu gewährleisten – sollten nach Möglichkeit alle Klassifizierungen freigegeben sein. Eine Ausnahme stellen bei dieser Empfehlung die Klassifizierungen „Upgrades“ und „Drivers“ dar (siehe Abschnitt 2.2).

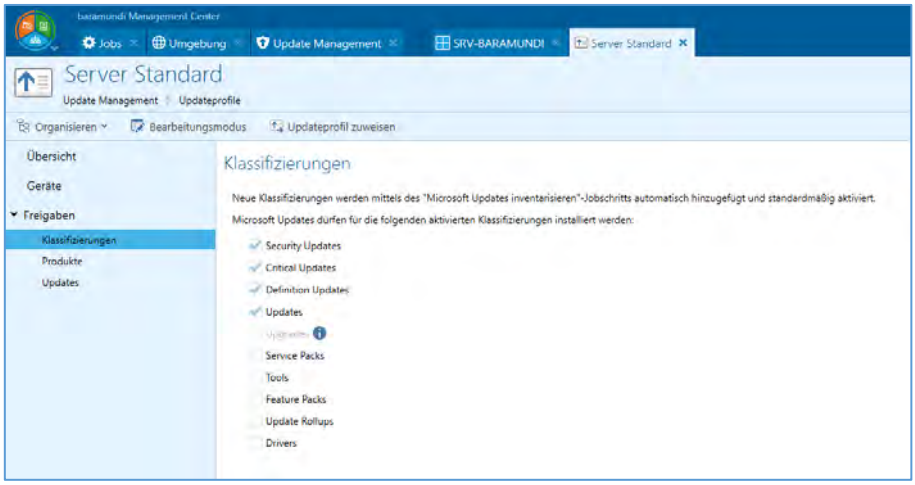

Abbildung 2 - Freigegebene Klassifizierungen eines Updateprofils

Je nach Anforderung können im Updateprofil auch komplette Produkte oder granular einzelne Updates blockiert werden.

Sollte beispielsweise „Microsoft Silverlight“ grundsätzlich nicht auf Unternehmensrechnern installiert und aktualisiert werden, so kann dieses Produkt im Updateprofil als geblockt markiert und somit von der Verteilung ausgenommen werden.

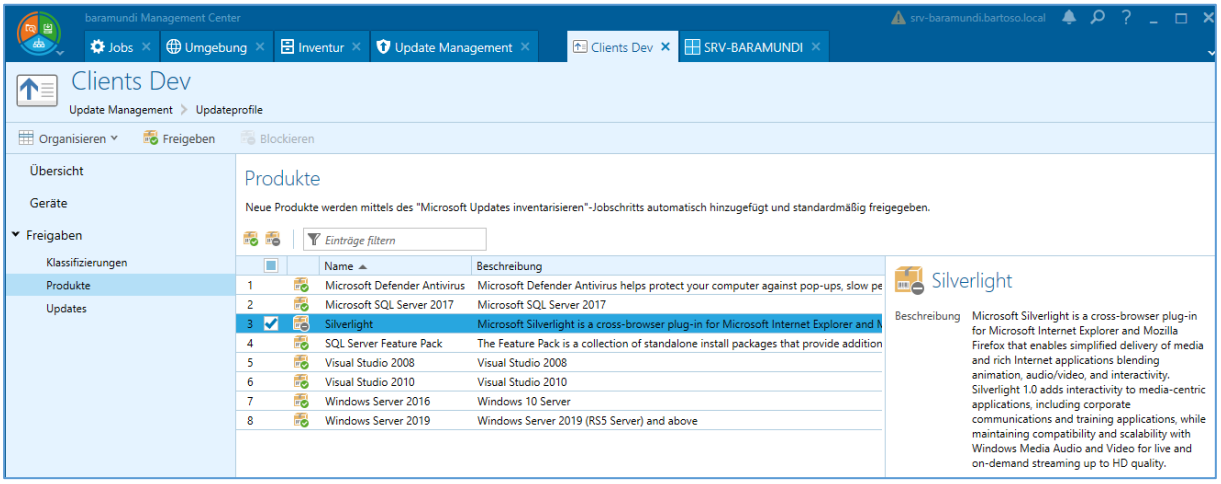

Abbildung 3 - Freigabe und Blockierung von Produkten im Updateprofil

Selbstverständlich wirken sich diese Freigaben nicht nur auf die Verteilung, sondern auch direkt auf die Inventarisierung aus. So ist jederzeit am Endpoint ersichtlich, ob Updates fehlen und ob diese verzögert oder blockiert sind.

5.2 Konfiguration der Jobs

Alle am Endpoint relevanten Aktionen sind im Jobschritt „Microsoft Updates verwalten“ zusammengefasst. Dort kann sowohl eine Inventur als auch die Aktualisierung ausgewählt werden.
In beiden Fällen stehen drei Quellen zur Auswahl zur Verfügung:

- Microsoft Update Online[7]
  Enthält Updates sowohl für Windows als auch für zahlreiche weitere Microsoft Produkte.
- Windows Update Online[7]
  Enthält nur Updates für Windows. Weitere Produkte werden nicht abgedeckt.
- Windows Server Update Services (WSUS)[8]
  Enthält alle Updates, welche auch über Microsoft Update Online zur Verfügung stehen. Der den Endpoints angebotene Umfang kann vom Admin konfiguriert und angepasst werden.

Eine Inventur sollte regelmäßig, mindestens einmal pro Woche durchgeführt werden. Hierbei wird lediglich der aktuelle Updatestatus des Endpoints ermittelt, es werden keine Updates installiert o.ä.

Obgleich die Wahl der Quelle im Jobschritt die größtmögliche Flexibilität ermöglicht, sollte man sich im Vorfeld für eine Quelle entscheiden und diese beibehalten. Von einem Mischbetrieb mit Online- und Offlinequellen wird dringend abgeraten. In der Praxis weichen die Daten des WSUS teils von den Daten der Onlinequellen ab. Dies führt zu Inkonsistenzen und gerade in Bezug auf das Veröffentlichungsdatum kann das problematisch werden – die Verzögerung funktioniert nicht korrekt.

Zur Installation der Updates dient die Aktion „Microsoft Updates verteilen“. Hier sollte stets dieselbe Quelle ausgewählt werden, welche zuvor auch für die Inventarisierung verwendet wurde.

[7] Der Endpoint benötigt eine Internetverbindung.
[8] Der WSUS muss in der eigenen Infrastruktur installiert, konfiguriert und betrieben werden.

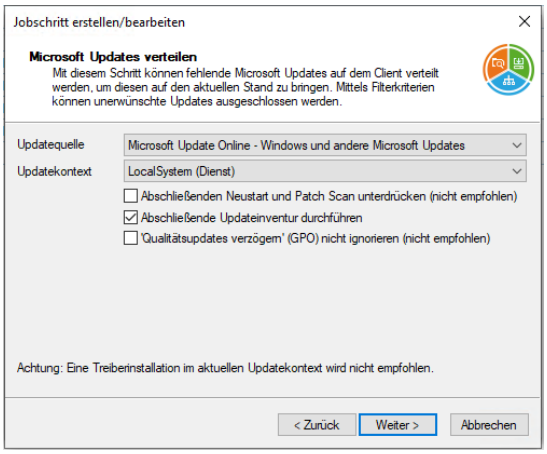

Abbildung 4 - Konfiguration der Aktion "Microsoft Updates verteilen" im Jobschritt "Microsoft Updates verwalten"

Für Sonderfälle ist es hier ebenfalls möglich, den von den Updates im Normalfall benötigten Neustart zu unterdrücken. Dies ist nicht empfohlen und führt dazu, dass einige Updates bis nach dem nächsten Neustart nicht korrekt erkannt werden können – Systemupdates werden i.d.R. erst beim Neustart vollständig installiert.

Die abschließende Inventur hingegen wird dringend empfohlen und sorgt dafür, dass der durch den Updatevorgang hergestellte, aktuelle Updatezustand auch korrekt an den baramundi Management Server gemeldet und somit in den Auswertungen berücksichtigt wird.

Im nächsten Schritt kann ausgewählt werden, nach welchen Vorgaben ein Endpoint im Rahmen dieses Jobs aktualisiert werden soll:

- **Manuelle Konfiguration**
  Sämtliche Einstellungen wie Klassifizierung, ein- und ausgeschlossene Produkte/Updates und zeitliche Verzögerung sind granular einstellbar.
- **Updateprofil**
  Der Updatevorgang richtet sich nach den Einstellungen im Updateprofil, welches dem Endpoint zugewiesen ist. Sollte kein Updateprofil zugewiesen sein, bricht der Jobschritt ab – der Endpoint wird nicht aktualisiert.

Für eine konsistente und vorhersehbare Updatestrategie wird die Verwendung von Updateprofilen dringend empfohlen. Die manuelle Konfiguration sollte nur in Einzelfällen oder zu Testzwecken verwendet werden.

5.3 Auswertung am Endpoint

Der aktuelle Updatezustand eines Endpoints wird zum einen als farbiger Statusbalken für einen schnellen Überblick, aber auch als detaillierte Liste der betreffenden Updates angezeigt.

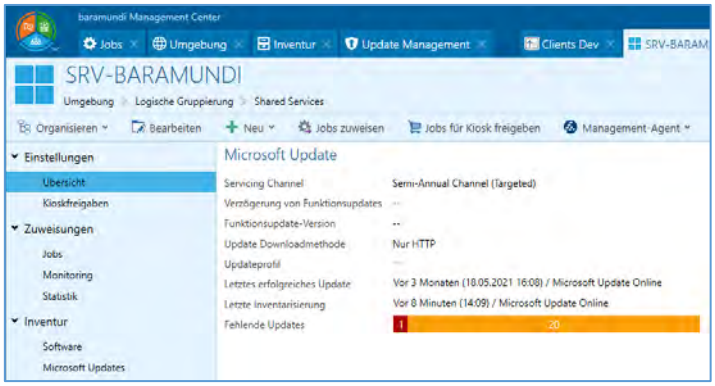

Abbildung 5 - Updatezustand auf der Übersichtsseite eines Endpoints

Die Auswertung des Updatezustands basiert auf den Einstellungen des Updateprofils – sofern zugewiesen. Ein Endpoint wird erst dann als aktuell gewertet, wenn die benötigten Updates installiert, blockiert oder verzögert sind. Ohne Updateprofil kann weder die Blockierung noch die Verzögerung von Updates berücksichtigt werden.

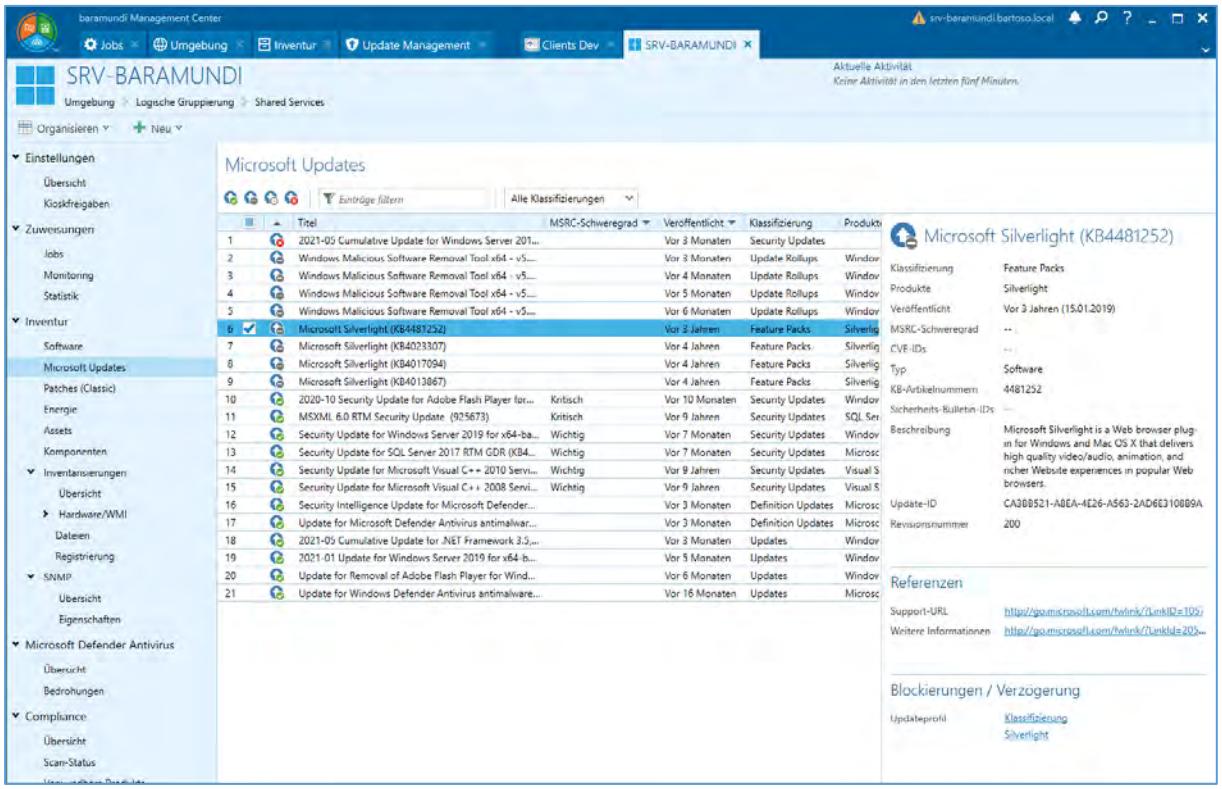

Abbildung 6 - Updateinventur am Endpoint

5.4 Auswertung für Gruppen

Updateprofile dienen nicht nur der Freigabe/Blockierung und Verzögerung von Updates, sondern auch der Auswertung des Updatezustands – So lässt sich schnell erkennen, ob ein Endpoint die Vorgaben des Updateprofils erfüllt bzw. ob alle dem Updateprofil zugeordneten Endpoints konform sind oder Handlungsbedarf besteht.

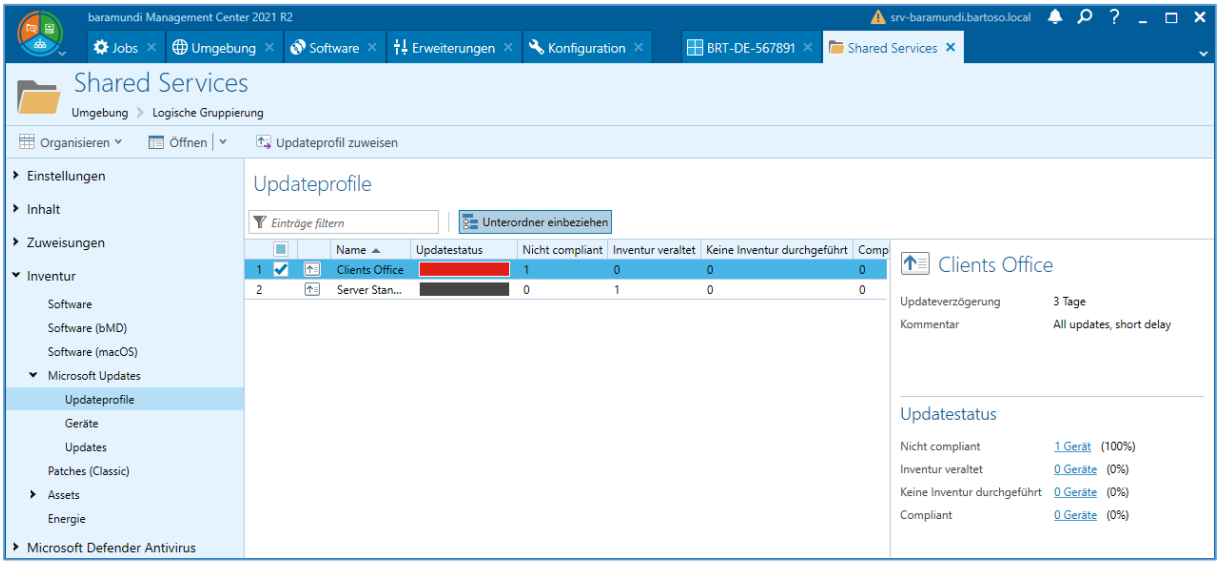

Abbildung 7 - Erfüllungsgrad der Updateprofile

Über Links in der Detailview kann auch direkt an die Liste mit den entsprechenden Endpoints gesprungen werden. Sämtliche Listen lassen sich natürlich auch direkt exportieren und weiterverarbeiten.

5.4.1 Detaillierte Übersicht über Updatezustände

Die Updatezustände der Endpoints lassen sich nach Gruppenzugehörigkeit anzeigen.

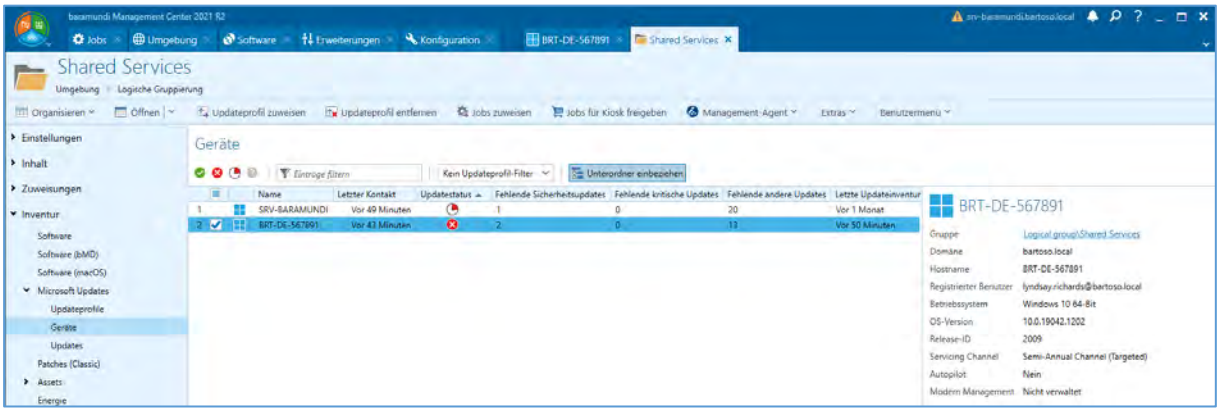

Abbildung 8 - Übersicht über die Updatezustände der Endpoints innerhalb einer Gruppe

So lassen sich einzelne Gruppen (z.B. Abteilungen) aber auch verschachtelte Zweige (z.B. Standorte) gezielt auswerten. Auf einen Blick ist erkennbar, ob die Geräte die Vorgaben des Updateprofils erfüllen, ob und wie viele Updates fehlen und auch wann zuletzt inventarisiert bzw. aktualisiert wurde. Selbstverständlich kann auch auf die verschiedenen Zustände und die Updateprofile gefiltert werden.

5.4.2 Detaillierte Übersicht aller Updates

Ebenso ist die Auflistung aller referenzierter Updates innerhalb einer Gruppe und darunterliegender Gruppen essenziell.

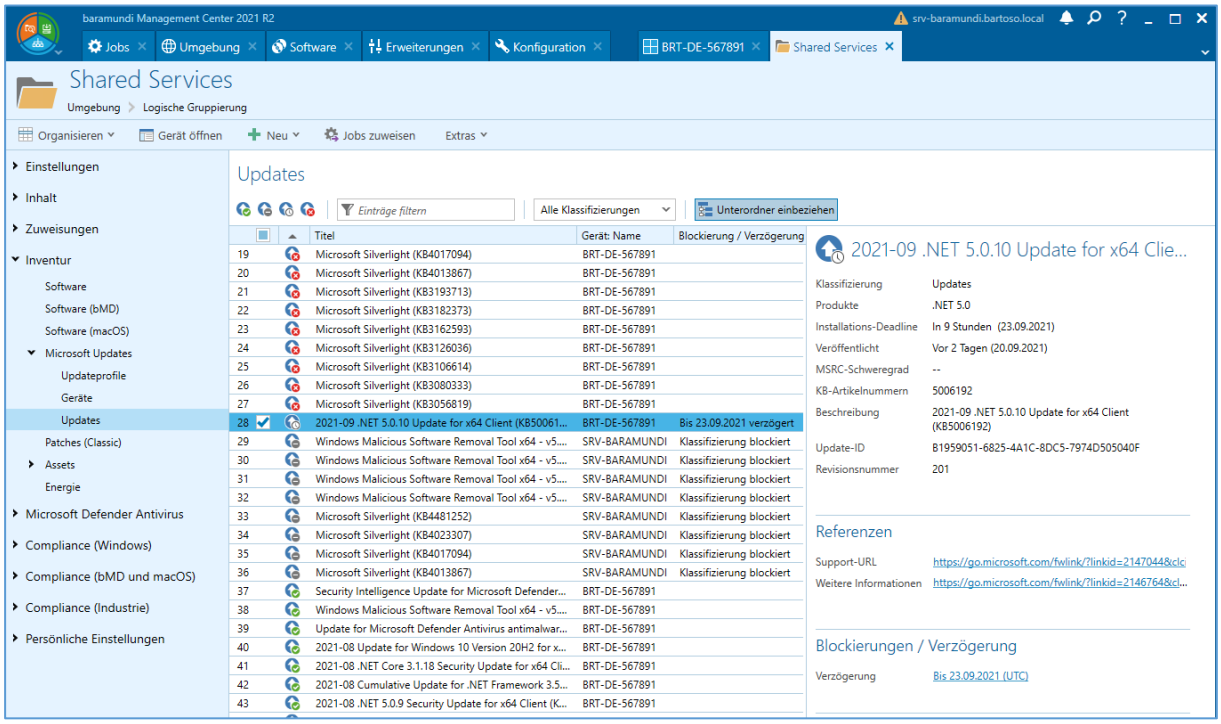

Abbildung 9 - Auflistung aller referenzierten Updates der Endpoints unterhalb einer Gruppe.

So werden alle installierten und fehlenden – damit auch die verzögerten oder blockierten – Updates der in der Gruppe enthaltenen Endpoints aufgelistet. Selbstverständlich auch hier mit der Möglichkeit zur Filterung nach Zustand, Name, KB-Nummer und weiteren Eigenschaften.

baramundi

Wir freuen uns, Sie kennenzulernen!

Kontaktieren Sie uns!

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

+44 2071 93 28 77
request@baramundi.com
www.baramundi.com

+48 735 91 44 54
request@baramundi.com
www.baramundi.com

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

+43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

+39 340 8861886
request@baramundi.com
www.baramundi.com

+41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

+1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com