FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre

D-52425 Jülich, Tel. (02461) 61-6402

Beratung Netzwerk, Tel. (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0416

Dr. F. Mohr, JSC

22.01.2019

Notwendige Maßnahmen für Betriebssysteme im Status End-of-support

Informationen für Systemadministratoren

1. Einführung

Zum 08. April 2014 hat Microsoft den erweiterten Support für Windows XP eingestellt, wodurch der Produktlebenszyklus dieses Betriebssystems beendet wurde[(1)]. Dies schließt auch alle weiteren auf XP basierenden Varianten ein, also z.B. Windows XP 64-Bit oder Windows XP Media Center Edition.

Diese weitreichende Veränderung in der Palette der verfügbaren Betriebssysteme dient als Anlass, auf den generellen Umgang mit Betriebssystemen hinzuweisen, die das Ende ihrer Produktpflege (End-of-support) erreicht haben. Die jeweilige Plattform (Windows, Linux, Mac OS etc.) spielt dabei keine Rolle, die Überlegungen entsprechen sich.

Gemäß IT-Grundschutzregel H3[(2)(3)] dürfen Betriebssysteme im Status End-of-support nicht am JuNet betrieben werden, da notwendige sicherheitsrelevante Updates nicht mehr zur Verfügung stehen. Dies betrifft ausdrücklich auch den Einsatz in virtuellen Maschinen, Umsetzungsverfahren wie NAT (Network Address Translation) oder PAT (Port and Address Translation) sowie beispielsweise den in Windows 7 integrierten Windows-XP-Modus.

Alle Administratoren von Systemen im JuNet mit veralteten Betriebssystemen sollten daher für deren Migration auf eine aktuelle Version sorgen. Gibt es zwingende Gründe gegen eine solche

Umstellung, so sind die betroffenen Systeme über den zuständigen IT-Beauftragten dem IT-Sicherheitsbeauftragten mitzuteilen.

2. Migration auf aktuelle Betriebssysteme – möglich oder nicht?

Die Migration auf eine aktuelle Version des verwendeten Betriebssystems ist grundsätzlich immer durchzuführen, sofern keine zwingenden Gründe zum Weiterbetrieb veralteter Soft- und/oder Hardware in der Form vorliegen, dass sonst relevante Funktionalitäten verloren gingen. Dies könnte z.B. in Experimentumgebungen der Fall sein, für deren Komponenten keine Softwareupdates vorliegen oder keine Unterstützung durch modernere Hardwareplattformen gegeben ist. Veraltete Hardware allein ist kein Grund zum Weiterbetrieb, wenn die benötigten Anwendungen auch unter noch unterstützten Versionen des Betriebssystems verfügbar sind.

Sollte der Weiterbetrieb veralteter Betriebssysteme in Einzelfällen zwingend notwendig sein, so wird JSC zum Schutz der JuNet-Teilnehmer Maßnahmen zur Abschottung dieser Systeme treffen, wie es die IT-Sicherheitsrichtlinie vorsieht[(4)]. Diese Maßnahmen werden im Folgenden beschrieben.

3. Weiterbetrieb von Sonderlösungen im Status End-of-support

3.1. Das JuRassic-Netz

Betriebssysteme im Status End-of-support dürfen mit Anbindung an das JuNet nur weiterbetrieben werden, nachdem sie durch JSC in ein zu diesem Zweck eingerichtetes, stark beschränktes Netzwerk *JuRassic* verschoben wurden. Für dieses Netz gelten folgende Kommunikationsregeln:

- JuRassic ➔ öffentliches Netz: Nicht möglich.
- Öffentliches Netz ➔ JuRassic: Nicht möglich.
- JuRassic ➔ JuNet: Nur DHCP, DNS, NTP, SMTP zum zentralen Mailrelay und SSL-Kommunikation zu Kaspersky-Security Center möglich.
- JuNet ➔ JuRassic: Möglich mit Ausnahme des SMB-Protokolls, siehe unten.

Demnach können JuRassic-Systeme nicht auf das JuNet zugreifen, lediglich die Dienste DHCP, DNS, NTP und SMTP sowie Kaspersky-Updates werden zur Verfügung gestellt. Allerdings können JuNet-Teilnehmer auf JuRassic-Systeme zugreifen, um beispielsweise VNC-Sitzungen aufzubauen oder FTP-Übertragungen anzustoßen. Datenübertragungen per SMB-Protokoll (Server Message Block, z.B. NetBIOS oder Samba-Shares) sind grundsätzlich nicht möglich.

Für den Weiterbetrieb in JuRassic wird dem System eine private IP-Adresse nach RFC 1918 zugewiesen; die bisherige Host-ID und alle DNS-Aliase bleiben erhalten, um die Institutszuordnung zu erleichtern.

3.2. Voraussetzungen zur Teilnahme an JuRassic

Wie bereits in der Einleitung beschrieben, sind Endgeräte für das JuRassic-Netz über den IT-Beauftragten an den IT-Sicherheitsbeauftragten zu melden.

Damit Endgeräte in JuRassic verschoben werden können, müssen sie zwei Voraussetzungen erfüllen:

1) Die Migration auf ein noch unterstütztes Betriebssystem (im Fall von Windows XP etwa Windows 7) ist nicht möglich, siehe Abschnitt **2.**
2) Das System teilt sich den Netzwerkanschluss NICHT mit anderen Teilnehmern, die in ihrem bisherigen Netz verbleiben sollen (z.B. über Office Switches).

Ist Bedingung 1) verletzt, ist ein Upgrade auf ein aktuelles Betriebssystem durchzuführen bzw. das Endgerät abzulösen. Wenden Sie sich bei Fragen dazu bitte an Ihren IT-Beauftragten oder PC-Dienstleister.

Ist Bedingung 2) nicht erfüllt, kann das System aus technischen Gründen erst in JuRassic verschoben werden, sobald der Konflikt z.B. durch eine Nachverkabelungsmaßnahme bereinigt wurde. Wenden Sie sich bei Fragen zu diesem Bereich an die Ansprechpartner im JSC (Tel. 6440), die eigentliche Verkabelung des Endgeräts und dessen Anbindung an JuNet führt JSC dann nach Stellen eines Verkabelungsauftrags[(5)] kurzfristig für Sie durch.

Da die Systeme in JuRassic auch weiterhin potentiell verwundbar sind, wird dringend zum Einsatz einer Firewall geraten; der Betrieb eines aktuellen Virenscanners ist auch in JuRassic obligatorisch.

3.3. Konfiguration der JuRassic-Teilnehmer

Passen Sie als Administrator von Endgeräten im JuRassic-Netz deren Konfiguration an die in Abschnitt **3.1** beschriebenen Kommunikationsbeziehungen an. An dieser Stelle sollen beispielhaft einige Einstellungen erwähnt werden, die erfahrungsgemäß oft zu Problemen bzw. unnötigem Datenverkehr führen und daher verbessert werden sollten:

- *WINS*: Der WINS-Server des JSC (134.94.80.84) ist für JuRassic-Teilnehmer nicht erreichbar. Entfernen Sie ihn daher aus der IP-Konfiguration.
- *DNS-Server*: Die korrekten DNS-Server sind 134.94.32.3, 134.94.32.4 und 134.94.32.5. Entfernen Sie alle anderen DNS-Server (sowohl intern als auch extern) aus der IP-Konfiguration.
- *Öffentliches Netz*: Das Internet ist aus JuRassic heraus grundsätzlich nicht erreichbar. Daher sollten Sie jegliche Kommunikation auf den Ports 80 und 443 unterbinden.
- *Windows Update*: Da das öffentliche Netz nicht erreichbar ist, kann auch Windows Update nicht auf die entsprechenden Microsoft-Server zugreifen. Eventuelle Microsoft-Updates (MS Office etc.) müssen auf anderem Weg eingebracht werden, deaktivieren Sie daher den Windows Update-Dienst.
- *Kaspersky*: Aus JuRassic erreichbar sind nur die zentralen Kaspersky-Server im JuNet, nicht die http-Server im öffentlichen Netz. Konfigurieren Sie Kaspersky daher so, dass nicht versucht wird, Updates aus dieser Quelle abzurufen.
- *TeamViewer*: Beachten Sie, dass Teilnehmer im JuRassic-Netz keine TeamViewer-Verbindungen aus dem JuRassic-Netz heraus aufbauen können.

Mit diesen Anpassungen tragen Sie spürbar zur Entlastung des Datenverkehrs im JuRassic-Netz bei, die JuNet-Administration bittet daher um Beachtung.

4. Schlusswort

Im Fall des Weiterbetriebs von Endgeräten mit einem nicht mehr unterstützten Betriebssystem außerhalb von JuRassic behält JSC sich deren sofortige Sperrung vor, um den Grundschutz im

JuNet für alle Teilnehmer aufrecht zu erhalten. Ebenso ist es nicht zulässig, auf Systemen in JuRassic weitere Interfaces in anderen Netzen zu betreiben.

Systeme ohne Netzwerkverbindung werden dagegen nicht weiter betrachtet: Gegen deren Weiterbetrieb bestehen keine Einwände, solange sie nicht mit dem JuNet verbunden werden.

5. Dokumente

(1) Informationsblatt zum Lebenszyklus von Windows:
https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet

(2) IT-Sicherheitsregeln für den Grundschutz:
http://intranet.fz-juelich.de/ITSicherheitsregeln_Grundschutz

(3) Gesamt-Rahmenbetriebsvereinbarung Informations- und Kommunikationssysteme:
http://intranet.fz-juelich.de/SharedDocs/Downloads/GR/DE/recht/betriebsvereinbarungen/IuK_Systeme.pdf

(4) IT-Sicherheitsrichtlinie des Forschungszentrums Jülich:
http://intranet.fz-juelich.de/ITSicherheitsrichtlinie

(5) Verkabelungsauftragssystem des JSC:
https://junet-portal.fz-juelich.de/cgi-bin/public/start_cable.cgi