A Szenario – Auftragsbeschreibung

Die meisten Anpassungen der Windows Client-Rechner wird man über Benutzerprofile und sogenannte *Gruppenrichtlinien* machen (siehe spätere Laborübung). Es gibt aber auch Einstellungen, die man über die *Windows Registry* direkt durchführen muss. Dafür ist es notwendig, den Aufbau der Windows Registrierungsdatenbank zu kennen. Sie finden eine Kurzerklärung der *Windows Registry* in den Zusatzblättern und -folien zu dieser Übung.

Achtung: Es ist stets gefährlich, schreibend in die Registrierung einzugreifen, da bei leichtfertigen Änderungen der Rechner unbrauchbar werden kann! Daher muss man die *Registry* und die Systemdateien vor den Änderungen sichern (nächster Punkt!).

Ihr heutiges Protokoll – das Sie während der Übung auf einer virtuellen Maschine mit Windows 11 erstellen – soll die jeweilige Aufgabenstellung, den Lösungsweg und Antworten auf etwaig gestellte Fragen enthalten. Wichtig sind insbesondere die *vollständigen Pfade* zu den einzelnen Werten in der Registry *(mit allen Schlüsseln dazwischen)*!

B VM

Erstellen Sie eine neue virtuelle Maschine:

- Windows 11,
- linked clone,
- Netzwerk: Host only – damit gibt es weniger Updates
- Snapshot zu Beginn (`init`) nicht vergessen!

C Sicherung des Systemzustandes

Hintergrund: Unter Windows 11 (sowie in den vorhergehenden Versionen auch) ist eine von Microsoft empfohlene Methode, die *Registry*-Dateien (und mehr) zu sichern, das Setzen eines *Wiederherstellungspunkts (Restore Point)*, der wichtige Dateien (inkl. Registrierungsdatenbank) des Systemlaufwerks (typisch C:) in einem reservierten Bereich (Verzeichnis) des Datenträgers in einem *Snapshot* abspeichert. Ab der Erstellung des Wiederherstellungspunktes führt Windows in diesem geschützten Verzeichnis dann auch ein Änderungsprotokoll *(Change Log)* mit, das im Falle einer Systemwiederherstellung auf einen früheren Wiederherstellungspunkt ein `Rollback` der vorgenommenen Änderungen erlaubt:

(1) Erstellen Sie einen Wiederherstellungspunkt mit dem Namen `before_registry_changes` (*wie?*) – aktivieren Sie ggf. vorher die Schutzeinstellung der Systemwiederherstellung für das Laufwerk `C:`!

(2) Wie groß ist die Platzverbrauch (“derzeitige Belegung”) der Wiederherstellungsdateien (nach Erstellen des WHP)? Dokumentieren Sie dies mittels Screenshots im Protokoll!

Zur Sicherung der Registry kann man alternativ mit dem Programm **regedit** (oder auf der Kommandozeile **reg**) einzelne oder alle Schlüssel in einer `.reg` -Sicherungsdatei abspeichern (und auch wieder einspielen, siehe letzter Punkt dieser Übung).

D Windows-Explorer Einstellungen professionalisieren

(3) Microsoft verpasst dem Windows-Explorer standardmäßig einige sehr ungünstige Einstellungen. Es empfiehlt sich daher, auf jedem Rechner folgende Einstellungen zu ändern:

- Dateinamenserweiterungen von bekannten Dateien werden nicht angezeigt: Warum ist das aus eigentlich aus Sicherheitsgründen sehr schlecht?

Lassen Sie daher die *Erweiterungen bekannter Dateien* anzeigen

- Zeigen Sie den "Vollständigen Pfad in der Titelleiste" an
- Lassen Sie *versteckte Dateien und Ordner* anzeigen
- Lassen Sie *geschützte Systemdateien* anzeigen
- Blenden Sie "leere Laufwerke" nicht aus
- Lassen Sie "Vorherige Ordnerfenster bei der Anmeldung wiederherstellen"
- Lassen Sie im "Navigationsbereich Alle Ordner anzeigen"

E Import von `.reg`-Dateien

Manchmal werden Dateien bereitgestellt, die man direkt in die Registry einspielen kann.

(4) Öffnen Sie den Explorer und erstellen Sie auf Ihrem Desktop eine Textdatei mit Ihrem Familiennamen als Dateinamen!

(5) Kopieren Sie die Datei `Altes Kontextmenü aktivieren.reg` aus der beigefügten `.zip`-Datei auf Ihrem Desktop!

- Öffnen Sie diese Datei mittels Doppelklick aus dem Explorer!
- Welche Warnungen werden angezeigt?
- Warum ist das Importieren von Registry-Einstellungen über ein `.reg`-File aus dem Internet gefährlich

(6) Diese Änderung ist nicht sofort wirksam – Dazu muss man sich entweder nochmals neu anmelden oder den Desktop neu starten. Wir starten den Desktop manuell neu – dies ist manchmal nützlich, wenn die Anzeige von Windows nicht korrekt funktioniert oder wenn Registry-Einträge nicht sofort wirksam sind:

- Starten Sie den Task-Manager (welche Tastenkombination?)
- Wählen Sie "Mehr Details" aus und danach den "Windows Explorer"
- Klicken Sie auf "Neustart"!

F Manuelle Änderungen in der Windows Registrierung

Diese Theorie-Frage kann man auch durch praktische Recherche beantworten:

(7) Welche Berechtigungen können Sie auf Registry-Elemente vergeben und wie? Auf welche Elemente der Registry können *überhaupt* Berechtigungen vergeben werden (*Tipp:* Vorbesprechung/bereitgestellte Unterlagen konsultieren oder einfach versuchen, die Berechtigungen von Elementen mit **regedit** zu ändern)?

Alle folgenden Abfragen und Änderungen sind direkt über Einträge in der *Windows Registry* (z.B. mit **regedit** oder mit der *Powershell*) vorzunehmen. Bitte geben Sie *unbedingt* stets an, *welche Registry-Pfade*, z.B. `HKLM\Hardware\...` Sie verwenden, welche Dateneinträge für einen bestimmten *Wert* Sie vornehmen und wann diese Einstellung aktiv wird! Zeigen Sie jeweils anhand eines geeigneten Screenshots im Protokoll, was Ihre Änderungen bewirken!

(8) Nun stellen Sie ein Hintergrundbild mit eines Feldhamsters[1] in der Registry ein, indem Sie nachfolgende Schritte anwenden. *Hinweis:* Windows unterstützt für das Hintergrundbild allerdings nicht jedes Dateiformat – dann ist der Hintergrund schwarz. Daher empfiehlt es sich, einen Screenshot des gewünschten Bildes anzufertigen und diesen abzuspeichern.

[1] https://naturschutzbund.at/tier-des-jahres.html

- Mit welcher Tastenkombination können Sie das Snipping-Tool aufrufen?
- Wie lautet der absolute Pfad des gespeicherten Screenshots?
- Öffnen Sie diese Datei in Paint und schreiben Sie mit dem Text-Tool in großen Buchstaben "*Tiername* von *IhrVorname* am *heutiges Datum*".
- Wie aktivieren Sie dieses Hintergrundbild für den aktuellen Benutzer direkt in der Registry und wann wird das aktiv?

  Fügen Sie einen Screenshot in Ihr Protokoll ein!

(9) **Pimp your PC**: Beeindrucken Sie Ihre Freunde mit dem neuesten und tollsten Prozessor (über *Systemsteuerung* ⟶ *System* herauslesbar)! Ändern Sie dazu die Beschreibung Ihres Prozessors in der Registry auf etwas Eindrucksvolles, etwa einen flotten Serverprozessor mit 96-Kernen von Intel (`*IhrFamilienname* Intel Xeon 6972P`)…

Fügen Sie einen Screenshot in Ihr Protokoll ein!

(10) Welche Programme werden auf diesem Computer *automatisch gestartet* und *wann* passiert das? Nennen Sie zumindest zwei!

Relevante Registry-Einträge *(vollständiger Pfad – wie immer – ins Protokoll!)*?

Anmerkung: es gibt noch viel mehr Stellen, an denen automatisch gestartete Software gespeichert wird. Diese kann man sich mit dem Programm **autoruns** der Sysinternals-Suite ansehen.

(11) Fügen Sie den Taschenrechner **calc.exe** für den derzeit eingeloggten User zum Autostart über die Registry hinzu und testen Sie die Automatik (*wie?*).

Tipp: Schauen Sie sich z.B. ähnliche systemweite Einträge unter `HKLM` als Beispiel an und machen Sie den Analogieschluss für `HKCU`!

(12) Über die Registry kann man auch einen Ordner dauerhaft als Laufwerk einbinden: Im Schlüssel

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\DOS Devices
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\DOS Devices
```

Erstellen Sie eine neue Zeichenfolge namens `x:` und weisen Sie ihr als Wert

```
\??\c:\users\junioradmin\Desktop
```

zu. Das `\??\` am Anfang ist kein Tippfehler, sondern muss so sein. Nach einem Windows-Neustart zeigt der Explorer das zusätzliche Laufwerk[2].

Fügen Sie einen Screenshot in Ihr Protokoll ein!

(13) Erweitern Sie das Kontextmenü des Explorers um die Option "Öffnen mit Lieblingseditor von *IhrVorname*" (das könnte z.B. *Notepad* sein)!

Tipp: Schlüssel

```
HKEY_CLASSES_ROOT\*\shell\Öffnen mit Lieblingseditor von IhrVorname\command
```

anlegen und dort den `(Standard)`-Wert (das ist der "namenlose" Wert) auf `notepad.exe %1` setzen (*IhrVorname* steht für Ihren *tatsächlichen* Vornamen)! Funktioniert das bei Ihnen? Rechtsklick im Explorer auf eie Datei – dann "*Weitere Optionen anzeigen*" Fügen Sie einen Screenshot in Ihr Protokoll ein!

[2] Um es wieder zu entfernen, brauchen Sie nur die in der Registry erstellte Zeichenfolge wieder zu löschen

G Sichern und Einspielen eines Registry-Schlüssels

G.1 Sichern

(14) Exportieren Sie den Registry-Schlüssel `HKCU\Control Panel\Desktop` mit **regedit**

(15) Welches Format (was für ein Dateityp?) hat die **.reg**-Datei (*Tipp:* mit Lieblingseditor öffnen)?

G.1 *Bonus*: Einspielen

Testen der Backup-Funktion:

(16) Machen Sie nun eine passende Registry-Änderung (z.B. den Desktop Hintergrund) und verifizieren Sie diese *(⟶ Protokoll!).*

(17) Jetzt importieren Sie wieder den Schlüssel – wurde Ihre Änderung aus der **.reg**-Datei erfolgreich zurückgesetzt?

Testen der Änderungsfunktion:

(18) Ändern Sie den Registry-Eintrag (z.B. den Desktop Hintergrund) in der **.reg**-Datei und importieren Sie die Datei wieder (*Tipp für angehende Gurus:* Das geht auch mit

```
reg import dateiname.reg
```

auf der Kommandozeile).

Wozu kann man diese **.reg**-Dateien noch gut gebrauchen?

Viel Spaß!