Powershell

Sicherheit und Integration

Inhaltsverzeichnis

1 Sicherheitsvorschriften für den Einsatz von Skripts

Obwohl die auf den Betrieb individuell angepassten Skripte sehr nützlich sind, können sie auch gleichzeitig zur Verbreitung von bösartigem Code verwendet werden. Unbedarfte Anwender erhalten E-Mails mit der Aufforderung, den Anhang zu öffnen. Der Anhang entpuppt sich stattdessen als VBS-Skriptdatei, welche dem System mächtig zusetzen kann.

Daher sind Sicherheitsvorschriften bei der Handhabung zu beachten:

- Über die Sicherheitsrichtlinie in Windows PowerShell (auch als Ausführungsrichtlinie bezeichnet) kann festgelegt werden, welche Skripts ausgeführt werden dürfen und ob diese über eine digitale Signatur verfügen müssen. Um unnötige Risiken zu vermeiden, ist es in keiner der Ausführungsrichtlinien in Windows PowerShell zulässig, ein Skript durch Doppelklicken auf dessen Symbol auszuführen. So führt Windows in der Grundeinstellung überhaupt keine Skripte aus. Das muss explizit vom Systemadministrator freigeschaltet werden. Die Freischaltung erlaubt dabei unterschiedliche Abstufungen, welche alle mit der Signierung von Skipten zusammenhängen. Zusätzlich ist die Endung „*.ps1“ mit Notepad verknüpft. Selbst wenn ein Rechner Skripte zulässt, würde ein unbedarfter Doppelklick auf einen Anhang oder eine Datei lediglich Notepad öffnen und den Quelltext anzeigen.
- Um Skripte auszuführen, muss man die Sicherheit der Windows PowerShell anpassen. Hierzu gibt es die zwei Cmdlets:

  get-executionpolicy: Wert wird abgefragt.
  set-executionpolicy: Der untenstehende Wert wird gesetzt.

Sicherheit	Policy Wert	Beschreibung
hoch	Restricted (Default)	Es werden keine Skripte ausgeführt.
	Allsigned	Nur signierte Skripte werden ausgeführt.
	Remote Signed	Lokal erstellte Skripte sind erlaubt, aber andere Skripte müssen signiert werden.
niedrig	Unrestricted	Jedes Skript wird ausgeführt.

- Um die Einstellung zu ändern, kann in einer PowerShell-Konsole, die unter administrativen Rechten läuft, der folgende Befehl eigegeben werden:

  set-executionpolicy RemoteSigned

  Alternativ können die Einstellungen auch über eine Gruppenrichtlinie (GPO) gesetzt werden.

- Nutzt man die PowerShell z. B. nur für die Serveradministration, kann auf allen Standardrechnern die PowerShell auf Restricted gesetzt werden, auf allen Servern hingegen auf Allsigned. Die Rechner der Serveradministratoren, die eigene Skripte schreiben und testen, werden hingegegen auf RemoteSigned gesetzt. Damit können lokal erstellte Skripte zum Testen direkt ausgeführt werden, jedoch wird verhindert, dass man Skripte, die man von Kollegen erhalten hat oder aus dem Internet heruntergeladen hat, versehentlich ausführt. So wird sichergestellt, dass nur die gewünschten Skripte, die nach der Erstellung und dem Testen signiert werden müssen und somit nicht mehr verändert werden können, ausgeführt werden.

2 Integrationsmöglichkeiten im eingesetzten Betriebssystem

Zwei Möglichkeiten, wie PowerShell-Skritps automatisch ausgeführt werden können, sind nachfolgend aufgeführt:

- Aufgabenplanung: Mit der Aufgabenverwaltung („Scheduled Tasks“) werden beliebige Programme zu einem festgelegten Zeitpunkt und/oder in festgelegten Intervallen gestartet. Zu den zahlreichen Einstellungen einer geplanten Aufgabe gehört u. a. der Name eines Benutzerkontos. Da hier auch die Namen von Systemkonten eingesetzt werden können, stellt eine geplante Aufgabe eine Möglichkeit dar, Programme, z. B. unmittelbar mit der Anmeldung, unter einem Systemkonto auszuführen.

  Für den Umgang mit geplanten Aufgaben bietet die PowerShell zwei Module:

  ScheduledTasks
  PSScheduledJob

- GPO-Objekt: Es bei den Skripten in Gruppenrichtlinien die Möglichkeit, explizit PowerShell-Skripte für folgende Fälle zu hinterlegen:
  - Systemstart (Computer Configuration/Windows Settings/Scripts/Startup)
  - Systemende (Computer Configuration/Windows Settings/Scripts/Shutdown)
  - Benutzeranmeldung (User Configuration/Windows Settings/Scripts/Logon)
  - Benutzerabmeldung (User Configuration/Windows Settings/Scripts/Logoff)

  Die auszuführenden PowerShell-Skripte sind in den entsprechenden Sysvol-Ordner der Domäne zu kopieren. Den Pfad dahin findet man über die Funktion „Show Files“ auf der Registerkarte „PowerShell Scripts“ der oben genannten Gruppenrichtlinieneinträge. Nach dem Ablegen der Skriptdateien sind diese zusätzlich über „Add“ in den Dialog einzubinden.

Historie

Dokument erstellt	R. Müller	03.11.2016