So testet man auf Meltdown und Spectre

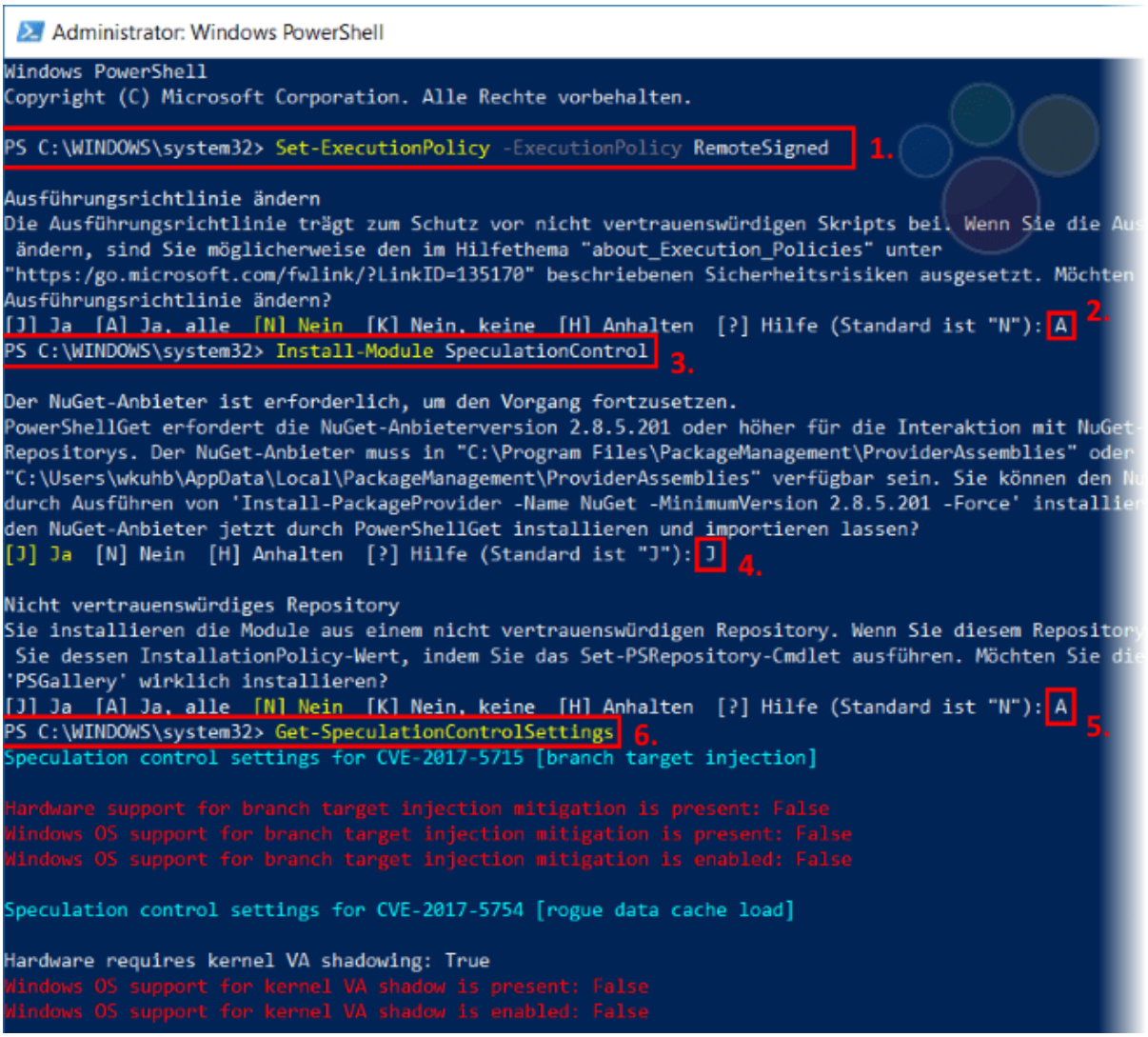
Bildquelle: TU Graz
Die aktuellen Sicherheitslücken, die bei Prozessoren von Intel, aber (teilweise) auch anderen Herstellern, auftreten, stehen derzeit im Blickpunkt der IT-Welt. Aktuell wird an der Schadensbegrenzung gearbeitet. Über die PowerShell von Windows kann man überprüfen, ob und welche Sicherheitsmaßnahmen installiert sind.

Die Schwachstellen, die Microsoft als "speculative execution side-channel vulnerabilities" bezeichnet, betreffen viele moderne Betriebssysteme und Prozessoren, darunter jene von Intel, AMD und ARM. Microsoft hat bereits erste Notfall-Patches dazu veröffentlicht, KB4056892 richtet sich an Windows 10 Fall Creators Update (Version 1709), KB4056891 an Windows 10 Creators Update (Version 1703), die komplette Übersicht aller gepatchten Windows-Systeme ist im Update-Katalog von Microsoft zu finden.

Nächsten Dienstag folgen am Patch-Day sicherlich weitere Fixes, auch die jeweiligen Hersteller werden hier noch tätig sein, die Behebung der Lücken wird jedoch insgesamt wohl noch Tage und vielleicht Wochen dauern.

Ob und welche Schutzfunktionen aktiviert sind, kann man mit Hilfe der PowerShell herausfinden. Dazu hat Microsoft einen Support-Beitrag veröffentlicht, in Folge findet ihr eine Anleitung, wie man vorgehen soll (via Deskmodder).

Und so sollte man vorgehen:



Schritt-für-Schritt-Anleitung in der PowerShell

- Windows-Taste drücken oder das Startmenü anklicken und **PowerShell** eintippen.
- PowerShell per Rechtklick als Administrator ausführen.
- In das aufgehenede Fenster **Set-ExecutionPolicy -ExecutionPolicy RemoteSigned** eingeben oder kopieren, Enter drücken und die Ausführung mit "A" bestätigen.
- **Install-Module SpeculationControl** eingeben oder kopieren, Enter drücken und mit "A" bestätigen. Nun wird per NuGet das Modul installiert.
- **Get-SpeculationControlSettings** eingeben oder kopieren und ausführen.

Bin ich geschützt?

Daraufhin bekommt man (abhängig von Soft- und Hardware) eine Liste, die angezeigt, ob und wie das System geschützt ist bzw. ob eine Schadensmilderung aktiv ist. In der Regel sollte hier möglichst häufig "True" erscheinen. Dabei ist der obere Bereich (CVE-2017-5715) Teil von Spectre, darunter (CVE-2017-5754) wird Meltdown angeführt. Die jeweiligen Zeilen erläutern, ob eine Schutzwirkung für Hardware sowie das Windows-Betriebssystem vorliegt. Ist sie grün markiert (True), dann ist der Schutz präsent bzw. aktiviert.

Siehe auch:

- Fast alle PCs betroffen: Schwere Lücken erschüttern die Hardware-Welt
- Intel: Nächste Security-Katastrophe ist im Anmarsch
- Microsoft mit Notfall-Patch für CPU-Sicherheitslücken
- Metdown & Spectre: Die wichtigsten Fragen und Antworten im Überblick