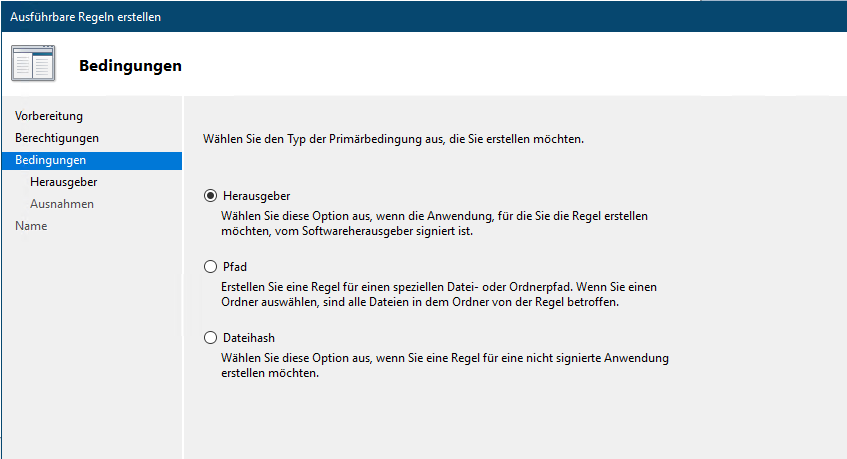


Nachdem der Dienst konfiguriert ist müssen die beiden Standardregelgruppen erstellt werden. Einmal für Ausführbare Dateien und einmal AppPaketregeln da sonst das Benutzerprofil unwiderruflich zerstört wird, oder das StartMenü sich nicht mehr benutzen lässt.

Jetzt wird die Ausführung sämtlicher Dateien welche nicht unter „Programme“ oder unter „Windows“ liegt oder nicht von einer elevated Session ausgeführt werden blockiert.

Will man jetzt gezielt Anwendungen freigeben kann man diese mit einer weiteren Regel freigeben.

Hier empfiehlt sich die Verwendung von „Herausgeber“ wenn die Anwendung signiert ist. Sollte die Anwendung nicht signiert sein muss man auf andere Kriterien ausweichen wie zb. Eine Pfad freigabe oder auf Basis des Datei Hashes.

Bevor der Applocker getestet werden kann sollte überprüft werden das der Dienst „Andwendungsidentität“ auf dem Client gestartet ist. Dazu ist nach einem „gpupdate /force „ ein Neustart notwendig.