

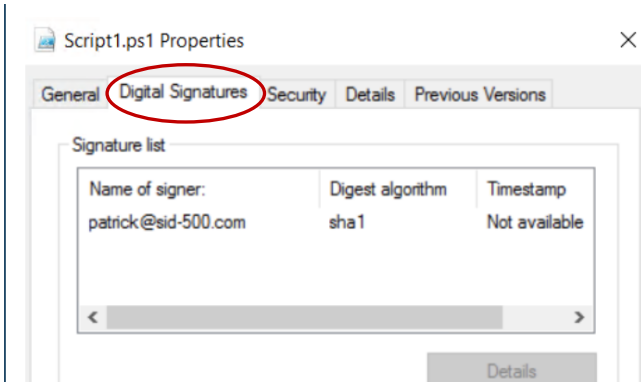
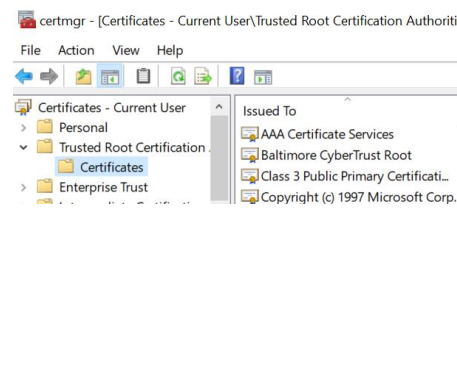
# Execution Policy

- ... verhindert das **unabsichtliche Ausführen** von PowerShell Codes (**\*.ps1**)

C:\Temp\script.ps1 : Die Datei "C:\Temp\script.ps1" kann nicht geladen werden, da die Ausführung von Skripts auf diesem System deaktiviert ist. Weitere Informationen finden Sie unter "about\_Execution\_Policies"

- Einstellungen:

- **Restricted** → Windows 10/11 (default)
- **Unrestricted**
- **RemoteSigned** → Windows Server (default)
- **AllSigned**
- **Bypass (ohne Prompts, Warnungen ...)**
- ...

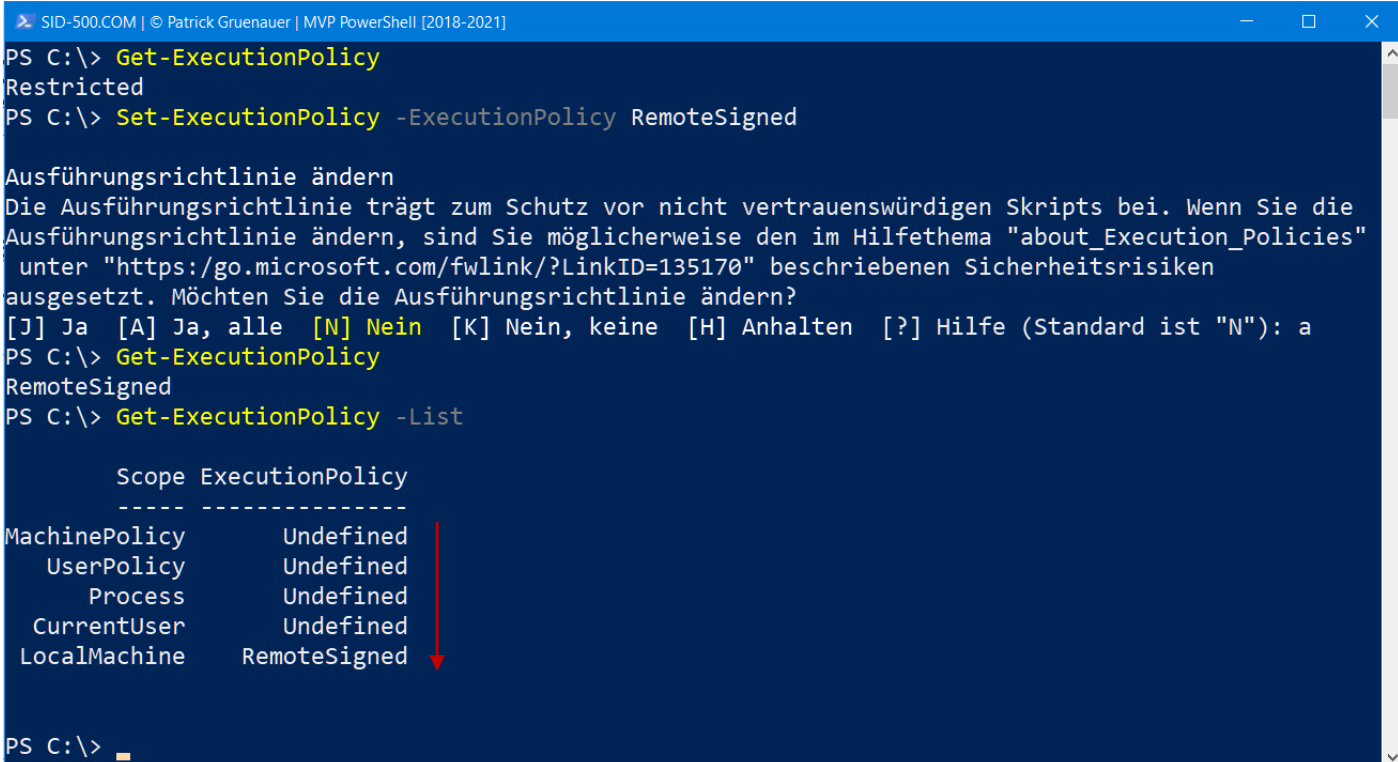


- Beispiel RemoteSigned: Wenn eine Datei aus dem Internet heruntergeladen wird, dann muss diese von einem vertrauenswürdigen Herausgeber (Zertifikat) digital signiert sein, eigens erstellte Skripts dürfen ausgeführt werden (Standard Windows Server BS)

# Execution Policy

- ... verhindert das **unabsichtliche Ausführen** von PowerShell Codes (\*.ps1) aber **NICHT** das Ausführen von **einzelnen Zeilen** im Skript (**F8 vs. F5**)

- Cmdlets:
  - **Get-ExecutionPolicy**
  - **Set-ExecutionPolicy**



```
SID-500.COM | © Patrick Gruenauer | MVP PowerShell [2018-2021]
PS C:\> Get-ExecutionPolicy
Restricted
PS C:\> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripts bei. Wenn Sie die
Ausführungsrichtlinie ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies"
unter "https://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken
ausgesetzt. Möchten Sie die Ausführungsrichtlinie ändern?
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): a
PS C:\> Get-ExecutionPolicy
RemoteSigned
PS C:\> Get-ExecutionPolicy -List

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine RemoteSigned
```

# Exkurs: Security Zonen

- Woher weiß PowerShell dass eine Datei vom Internet heruntergeladen wurde ? → IE Zonen

```
security_zones.ps1 X
1 Get-Content C:\temp\cortana.ico -Stream Zone.Identifier
2
3 [enum]::GetValues([System.Security.SecurityZone]) + [enum]::GetValues([System.Security.SecurityZone]).value__
4

PS C:\> C:\Users\patri\OneDrive\PowerShell\PowerShell Kurs\Codes\01 . Codes . Einführung in PowerShell\security_zones.ps1
[ZoneTransfer]
ZoneId=3
HostUri=https://icoconvert.com/files/download/home2015/20200613/20/XhuFjK1wyEmj2aKj/tGF/cortana_1280x720_tIX_icon.ico
MyComputer
Intranet
Trusted
Internet
Untrusted
NoZone
0
1
2
3
4
-1

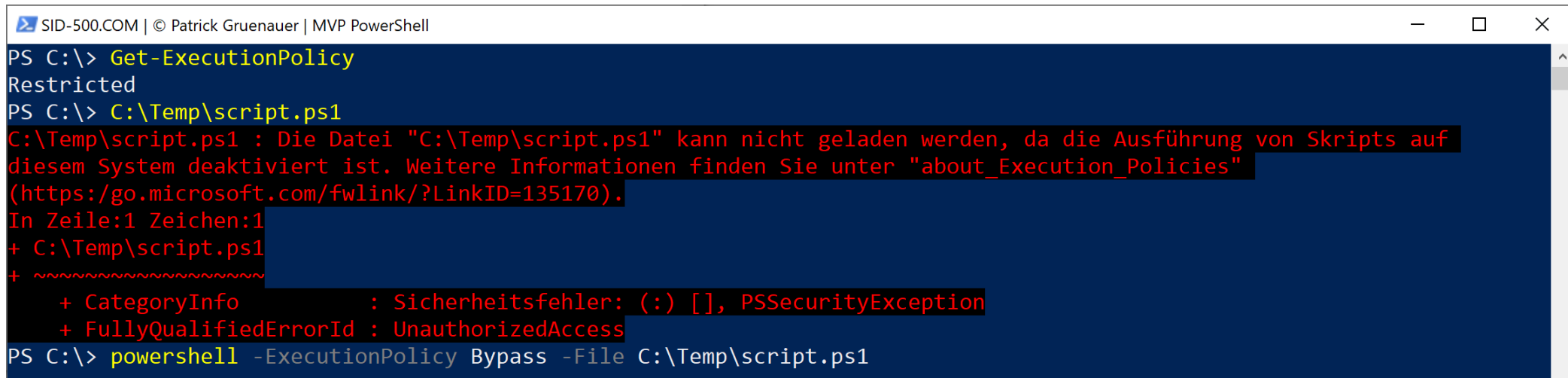
PS C:\> |
```

security\_zones.ps1

# Execution Policy

- Die Execution Policy ist **kein Sicherheitsfeature!**, sie ist ein **Fallschirm** für Administratoren
- Umgehen der Ausführungsrichtlinie

```
powershell -ExecutionPolicy Bypass -File Yourfile.ps1
```

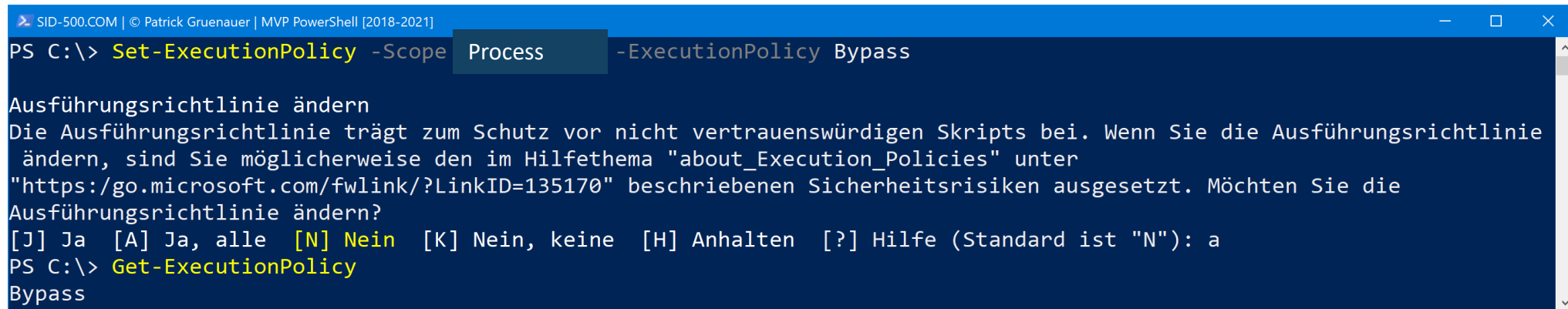


The screenshot shows a PowerShell console window with the title bar 'SID-500.COM | © Patrick Gruenauer | MVP PowerShell'. The command 'Get-ExecutionPolicy' is entered, returning 'Restricted'. Then, the command 'C:\Temp\script.ps1' is entered, resulting in an error message in red text: 'C:\Temp\script.ps1 : Die Datei "C:\Temp\script.ps1" kann nicht geladen werden, da die Ausführung von Skripts auf diesem System deaktiviert ist. Weitere Informationen finden Sie unter "about\_Execution\_Policies" (https://go.microsoft.com/fwlink/?LinkID=135170). In Zeile:1 Zeichen:1 + C:\Temp\script.ps1 + ~~~~~ + CategoryInfo : Sicherheitsfehler: (:) [], PSSecurityException + FullyQualifiedErrorId : UnauthorizedAccess'. Finally, the command 'powershell -ExecutionPolicy Bypass -File C:\Temp\script.ps1' is entered.

```
PS C:\> Get-ExecutionPolicy
Restricted
PS C:\> C:\Temp\script.ps1
C:\Temp\script.ps1 : Die Datei "C:\Temp\script.ps1" kann nicht geladen werden, da die Ausführung von Skripts auf
diesem System deaktiviert ist. Weitere Informationen finden Sie unter "about_Execution_Policies"
(https://go.microsoft.com/fwlink/?LinkID=135170).
In Zeile:1 Zeichen:1
+ C:\Temp\script.ps1
+ ~~~~~
+ CategoryInfo          : Sicherheitsfehler: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\> powershell -ExecutionPolicy Bypass -File C:\Temp\script.ps1
```

# Exkurs: Scopes

- Die Execution Policy ist **kein Sicherheitsfeature!** → Umgehen im Context des Users oder Prozess
- Ausführbar als „**normaler**“ **Benutzer** !
  - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass**

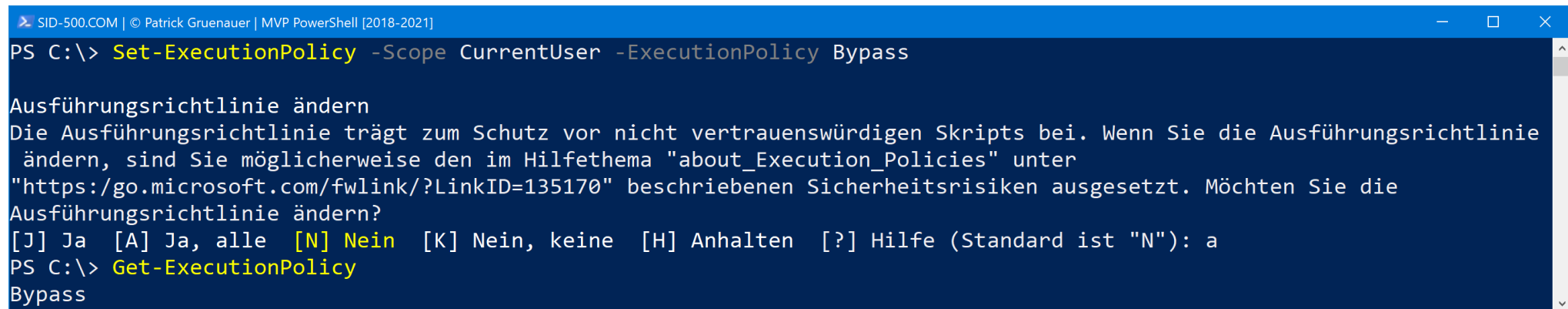


```
SID-500.COM | © Patrick Gruenauer | MVP PowerShell [2018-2021]
PS C:\> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripts bei. Wenn Sie die Ausführungsrichtlinie
ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter
"https://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten Sie die
Ausführungsrichtlinie ändern?
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): a
PS C:\> Get-ExecutionPolicy
Bypass
```

# Exkurs: Scopes

- Die Execution Policy ist **kein Sicherheitsfeature!** → Umgehen im Context des Users oder Prozess



```
SID-500.COM | © Patrick Gruenauer | MVP PowerShell [2018-2021]
PS C:\> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripts bei. Wenn Sie die Ausführungsrichtlinie
ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter
"https://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten Sie die
Ausführungsrichtlinie ändern?
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): a
PS C:\> Get-ExecutionPolicy
Bypass
```

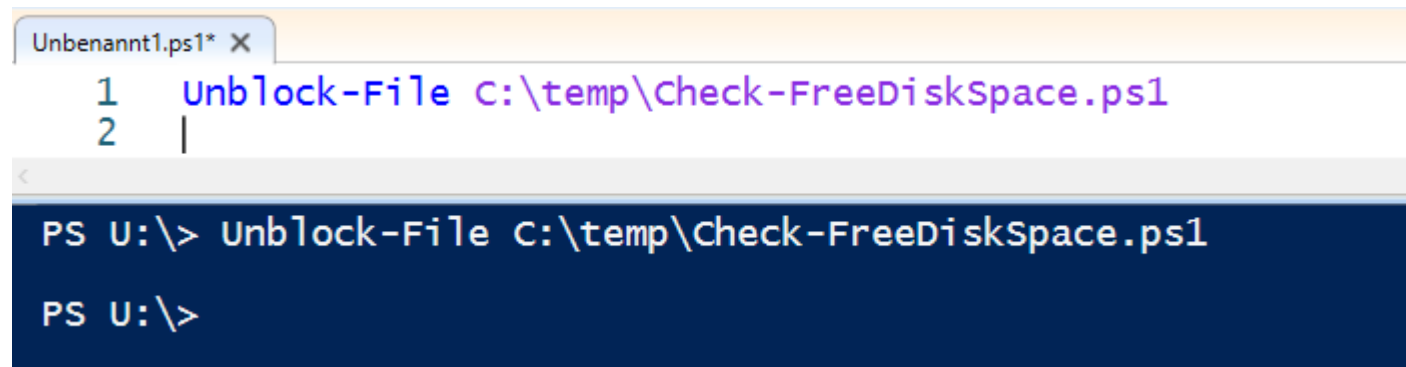
**Unrestricted.** Loads all configuration files and runs all scripts. If you run an unsigned script that was downloaded from the Internet, you are prompted for permission before it runs.

**Bypass.** Nothing is blocked and there are no warnings or prompts.

# Unblock-File

---

- Die Execution Policy ist **kein Sicherheitsfeature!**, sie ist ein **Fallschirm** für Administratoren
- Mit **Unblock-File** können Dateien, welche aus dem Internet heruntergeladen wurden geöffnet werden, auch dann wenn die Execution Policy (**RemoeSigned!**) dies nicht erlauben würde



```
Unbenannt1.ps1* X
1 Unblock-File C:\temp\Check-FreeDiskSpace.ps1
2 |
PS U:\> Unblock-File C:\temp\Check-FreeDiskSpace.ps1
PS U:\>
```