Computing

Wie kann ich mit der Windows PowerShell ein selbst ausgestelltes SSL-Zertifikat mit SHA256 erstellen?

- Mit Hilfe der PowerShell in Windows ist es möglich, für kleine Umgebungen ein gültiges **self-signed** SSL-Zertifikat **anzulegen**, welches unter anderem SHA256 verwendet.
- Bei SHA-256 handelt es sich um einen Algorithmus zur **Verschlüsselung**.
- Die Erstellung eines neuen SSL-Zertifikates mit SHA256 ist z.B. dann wichtig, wenn Sie bislang selbst ausgestellte SSL-Zertifikate mit dem **Algorithmus** SHA1 bzw. SHA-1 verwendet haben.
- SSL-Zertfikate mit SHA1 werden von Windows schon seit längerem als **unsicher** eingestuft und aktiv **blockiert**.
- Zudem verhindern die **Browser** Microsoft Edge und Google Chrome seit der Version 119 das Hinzufügen von Ausnahmen für mit SHA1 erstellte SSL-Zertifikate.
- Zudem ist **wichtig**, dass im SSL-Zertifikat neben dem Common Name (CN) auch der Subject Alternative Name (SAN) gesetzt ist.
- Der Common Name wird von Windows nicht mehr **verifiziert**.
- Um ein selbst ausgestelltes SSL-Zertfikat zu erstellen, welches die oben genannten Anforderungen erfüllt, öffnen Sie die Windows PowerShell mit **Administratorrechten**.
- Geben Sie den folgenden **Befehl** ein und bestätigen Sie mit Enter, um das Zertifikat zu erstellen (das Zertifikat aus dem **Beispiel** wird für drei Jahre ausgestellt, bitte passen Sie zudem im Befehl den Server-Namen und die Domain an):

  ```
  New-SelfsignedCertificate -DNSName "testserver", "testserver.ihr
  edomain.local" -CertStoreLocation "cert:\LocalMachine\My" -KeyLe
  ngth 4096 -KeyAlgorithm RSA -NotAfter (Get-Date).AddYears(3)?
  ```

- Sie können nun in der Microsoft Management Console (MMC) bei den Zertifikaten im Abschnitt Eigene Zertifikate **überprüfen**, dass das SSL-Zertifikat angelegt wurde.
- **Kopieren** Sie das Zertifikat und fügen Sie es zudem im Abschnitt Vertrauenswürdige Stammzertifizierungsstellen ein.
- Optional können Sie das neu erstellte Zertifikat über Ihren Domain Controller (DC) als Gruppenrichtlinienobjekt bzw. GPO **verteilen**.
- Wie Sie das **Binding** des Zertifikates mit dem neuen **Fingerabdruck** über den netsh-Befehl durchführen, erfahren Sie hier.
- Wie Sie Optional ein **Binding** eines bestehenden Zertifikates über den netsh-Befehl **löschen** bzw. **entfernen**, erfahren Sie hier.

Computing

Verfasser:
Letzte Änderung: 2024-03-11 17:16