SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Azure AD: *Federated* Authentisierung für Subdomain, *Managed* Authentisierung für Parent-Domain: so wäre es möglich

Dieses Dokument beschäftigt sich mit der Frage, ob man im Azure Active Directory die Authentisierung einer Domain (hier `mydomain.ch`) auf `Managed` setzen kann, während sie für eine Subdomain (hier `sub.mydomain.ch`) auf `Federated` gestellt wird, um sich beispielsweise über die SWITCH edu-ID zu authentisieren. Das Gegenstück zu Subdomain wird im Folgenden als Parent-Domain bezeichnet (`mydomain.ch` ist die Parent-Domain von `sub.mydomain.ch`).

Vorweg sei gesagt: Ja, es ist im Prinzip möglich, jedoch, falls der Azure Active Directory bereits konfiguriert ist, bedingt ein solcher Umbau längere Unterbrüche für die Endbenutzenden und der zu treibende Aufwand ist beträchtlich.

Die Voraussetzungen

Um eine Domain unabhängig von den anderen zu behandeln, darf bei ihr das Attribut `RootDomain` keinen Wert haben. Dies kann in der Powershell überprüft werden:

```
$sub = Get-MsolDomain -DomainName "sub.mydomain.ch"
$sub.RootDomain
```

Der Output sollte leer sein, in diesem Fall besitzt sie keine `RootDomain`. Falls dies für eine Subdomain der Fall ist, so kann sie mit `Set-MsolDomainAuthentication` auf `Federated` gesetzt werden, und die Parent-Domain auf `Managed`. Falls die Subdomain eine `RootDomain` besitzt (Output der obigen Kommandoreihe ist `mydomain.ch`), so übernimmt sie jeweils automatisch die Authentication-Einstellungen von dieser und kann selbst nicht separat bearbeitet werden. Es gibt leider keinen einfachen Mechanismus, diese Abhängigkeit aufzulösen, wenn sie mal besteht.

Das Problem

Damit eine Subdomain nicht von ihrer Parent-Domain abhängig ist, muss sie im Azure AD *vor* ihrer Parent-Domain hinzugefügt und verifiziert werden. Wenn danach die Parent-Domain hinzugefügt wird, wird die Subdomain nicht an diese geknüpft und kann somit separat behandelt werden. Wenn die Parent-Domain bereits vorhanden ist, so wird für die Subdomain beim Hinzufügen gleich (ohne Verifikation) für das Attribut `RootDomain` der Name der Parent-Domain gesetzt und sie kann für die Authentisierung nicht separat betrachtet werden.

Die Lösung

Einfach gesagt: im Azure AD die Subdomain *vor* der Parent-Domain hinzufügen. Da in den meisten Fällen jedoch beide Domains bereits in der falschen Reihenfolge hinzugefügt wurden, müsste die Parent-Domain wieder komplett entfernt und beide neu hinzugefügt und verifiziert werden. Um die Domain zu entfernen, dürfen aber keine User unter dieser Domain existieren, was das ganze Vorhaben unter Umständen sehr komplex machen kann.

Wer das `RootDomain` Attribut von der Subdomain entfernen will, ohne die Parent-Domain komplett neu hinzuzufügen, muss dies mit Hilfe des O365 Supports abklären.