



## Zertifikatsfehler im Browser - Zugriff verweigern

Ein Leser hatte mich gestern angeschrieben, mit der Bitte im zu zeigen, wo die Einstellungen im Gruppenrichtlinieditor zu finden sind.

Es geht darum, den Benutzern keine Möglichkeit einzuräumen, sofern der jeweilige Browser ein Problem mit einem Zertifikat erkannt hat, diesen Fehlerhinweis zu umgehen, und die Webseite trotz Hinweis auf eine Gefahr zu besuchen.

Dafür bieten die Hersteller in ihren ADMX-Vorlagen entsprechende Einstellmöglichkeiten an.

Die Browser überprüfen mit verschiedenen Mechanismen, ob der Name der aufgerufenen (geschützten) Webseite (SSL/TLS) auch im entsprechend Stellen Subject, SAN vorkommt. Wird keine Übereinstimmung gefunden sollte der Browser die Verbindung ablehnen, um vor einer möglichen Gefahr zu schützen.

Das machen aber nicht alle Browser aus dem Karton heraus! Um den Schutz zu aktivieren benötigt wir zuerst alle ADMX Dateien für die jeweiligen Browser.

<https://www.gruppenrichtlinien.org/downloads/>

**Die Einstellungen für den Internet Explorer finden wir hier:**

Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Internet Explorer/Internetsystemsteuerung

Einstellung	Status	Kommentar
Seite "Erweitert" deaktivieren	Nicht konfiguriert	Nein
Verbindungsseite deaktivieren	Nicht konfiguriert	Nein
Inhaltsseite deaktivieren	Nicht konfiguriert	Nein
Seite "Allgemein" deaktivieren	Nicht konfiguriert	Nein
Datenschutzseite deaktivieren	Nicht konfiguriert	Nein
Programmseite deaktivieren	Nicht konfiguriert	Nein
Sicherheitsseite deaktivieren	Nicht konfiguriert	Nein
Internationale Domänennamen senden	Nicht konfiguriert	Nein
UTF-8 für mailto-Links verwenden	Nicht konfiguriert	Nein
<b>Ignorieren von Zertifikatfehlern verhindern</b>	<b>Aktiviert</b>	<b>Nein</b>



## Zertifikatsfehler im Browser - Zugriff verweigern

Die Einstellungen für den Microsoft Edge finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Microsoft Edge

The screenshot shows the Local Group Policy Editor window. The left navigation pane lists various policy categories under 'Computerkonfiguration' and 'Administrative Vorlagen'. The right pane is focused on the 'Microsoft Edge' policy. Under 'Außerkraftsetzungen von Zertifikatfehlern verhindern' (Prevent certificate errors), there is a table of settings. One setting, 'Zugriff auf die Seite „about:flags“ in Microsoft Edge verhindern' (Prevent access to the 'about:flags' page in Microsoft Edge), is highlighted in blue and has the status 'Aktiviert' (Enabled). Other settings listed include preventing the opening of certain websites, disabling SmartScreen, and managing Intranet zones.

Die Einstellungen für den Microsoft Edge-Chromium Browser finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Microsoft Edge

The screenshot shows the Local Group Policy Editor window. The left navigation pane lists various policy categories under 'Computerkonfiguration' and 'Administrative Vorlagen'. The right pane is focused on the 'Microsoft Edge' policy. Under 'Zulassen, dass Benutzer von der HTTPS-Warnungsseite aus fortfahren können' (Allow users to proceed from the HTTPS warning page), there is a table of settings. One setting, 'Zulassen, dass Benutzer von der HTTPS-Warnungsseite aus fortfahren können' (Allow users to proceed from the HTTPS warning page), is highlighted in blue and has the status 'Deaktiviert' (Disabled). Other settings listed include enabling TLS 1.3, activating the renderer code integrity checker, and adjusting navigation error handling.



## Zertifikatsfehler im Browser - Zugriff verweigern

Die Einstellungen für den Google Chrome finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Google/Google Chrome

The screenshot shows the Windows Group Policy Editor with the path "Computerkonfiguration\Administrative Vorlagen\Google\Google Chrome". The selected policy is "Fortfahren von SSL-Hinweiseite erlauben". The right pane displays various configuration options for handling SSL certificate errors. One specific setting, "Fortfahren von SSL-Hinweiseite erlauben", is highlighted with a blue selection bar at the bottom.

Die Einstellungen für den Mozilla Firefox finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Mozilla/Firefox

The screenshot shows the Windows Group Policy Editor with the path "Computerkonfiguration\Administrative Vorlagen\Mozilla\Firefox". The selected policy is "Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten". The right pane displays various configuration options for handling SSL certificate errors. One specific setting, "Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten", is highlighted with a blue selection bar at the bottom.



## Zertifikatsfehler im Browser - Zugriff verweigern

Ein Beispiel in Aktion, wenn wir die Richtlinie für Google Chrome so einstellen, das der Browser dahingehend gehärtet wird.

Ohne Härtung, bekommen wir die Möglichkeit geboten, den Hinweis mit Weiter zu 172.18.xx.xx (unsicher) zu umgehen, um die Webseite zu dennoch besuchen.

Schalten wir die Richtlinie „Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten“ auf = Deaktiviert,



## Zertifikatsfehler im Browser - Zugriff verweigern

...ist ein Umgehen des Hinweises nicht mehr möglich und die Webseite bleibt im Zugriff verhindert.



### Dies ist keine sichere Verbindung

Hacker könnten versuchen, Ihre Daten von **172.18.██** zu stehlen, zum Beispiel Passwörter, Nachrichten oder Kreditkartendaten. [Weitere Informationen](#)

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

Dabei helfen, die Sicherheit von Chrome zu verbessern. Hierfür werden die URLs einiger von Ihnen besuchter Seiten bestimmte Systeminformationen und einige Seiteninhalte an Google gesendet. [Datenschutzerklärung](#)

[Erweiterte Informationen ausblenden](#)

[Neu laden](#)

172.18.██ schützt Ihre Daten in der Regel durch Verschlüsselung. Als Google Chrome dieses Mal versuchte, eine Verbindung zu 172.18.██ herzustellen, gab die Website ungewöhnliche und falsche Anmelddaten zurück. Entweder versucht ein Angreifer, sich als 172.18.██ auszugeben, oder die Verbindung wurde durch eine WLAN-Anmeldeseite unterbrochen. Da Google Chrome die Verbindung vor dem Austausch von Daten unterbrochen hat, sind Ihre Informationen weiterhin sicher.

Sie können 172.18.██ zurzeit nicht aufrufen, da die Website verschlüsselte Anmelddaten gesendet hat, die von Google Chrome nicht verarbeitet werden können. Netzwerkfehler und Angriffe sind in der Regel nur vorübergehend, sodass die Seite wahrscheinlich später wieder funktioniert.