Zertifikatsfehler im Browser - Zugriff verweigern

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

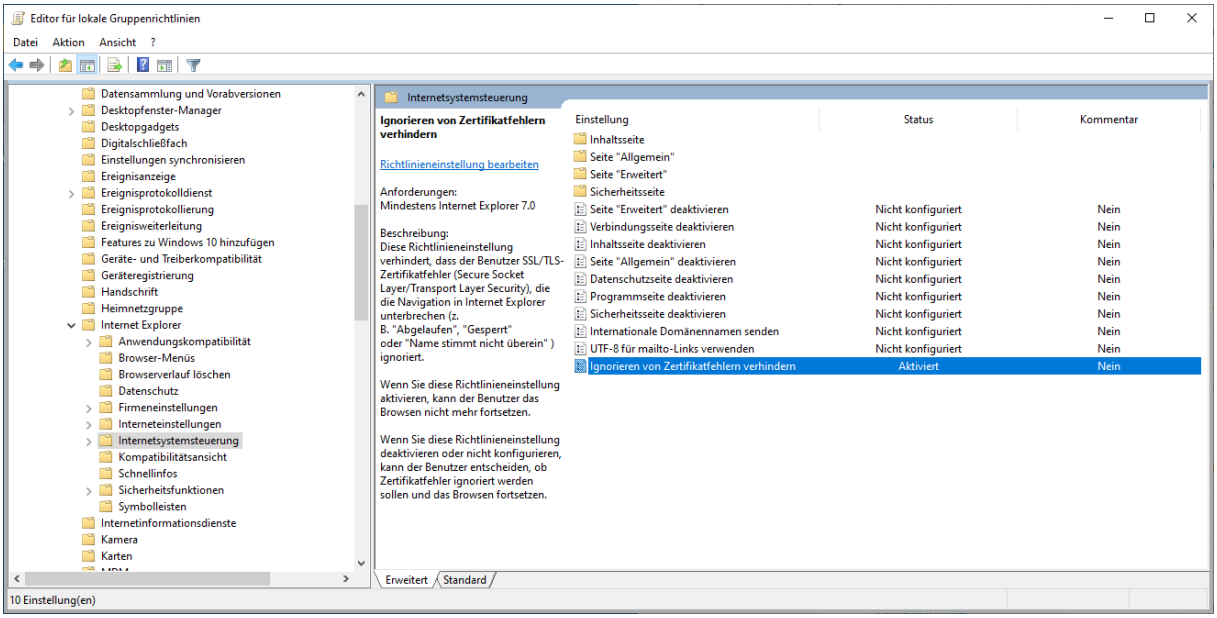
Die Browser überprüfen mit verschiedenen Mechanismen, ob der Name der aufgerufenen (geschützten) Webseite (SSL/TLS) auch im Zertifikat an den entsprechend Stellen Subject, SAN vorkommt. Wird keine Übereinstimmung gefunden sollte der Browser die Verbindung ablehnen, um vor einer möglichen Gefahr zu schützen.

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:

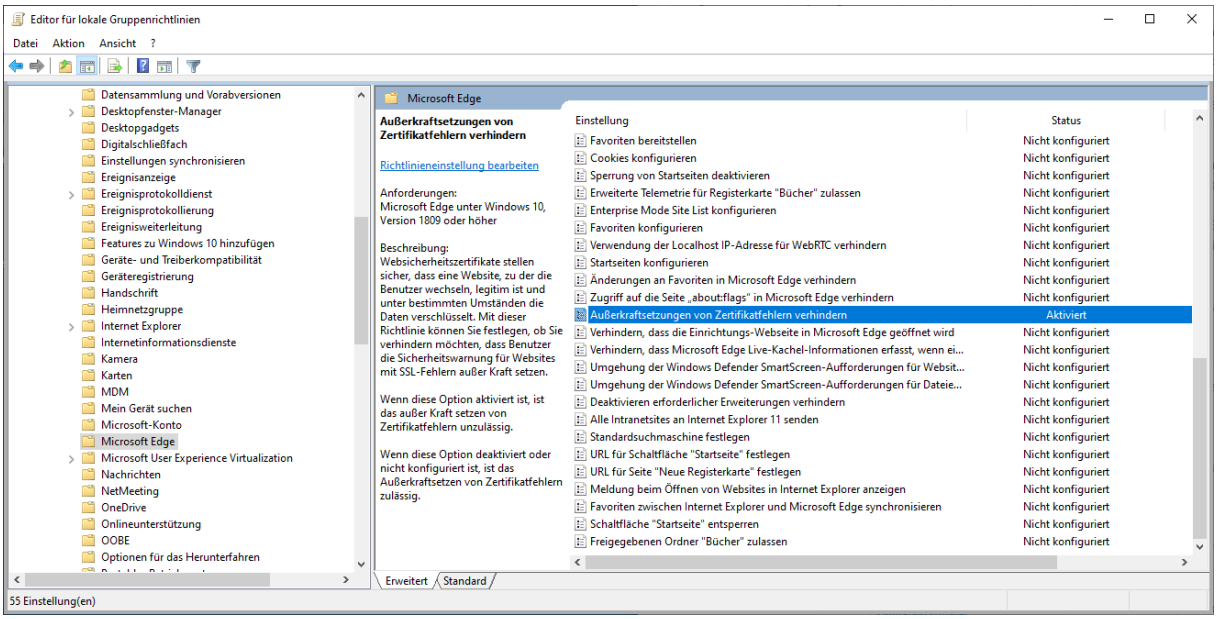
Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Internet Explorer/Internetsystemsteuerung



Zertifikatsfehler im Browser - Zugriff verweigern

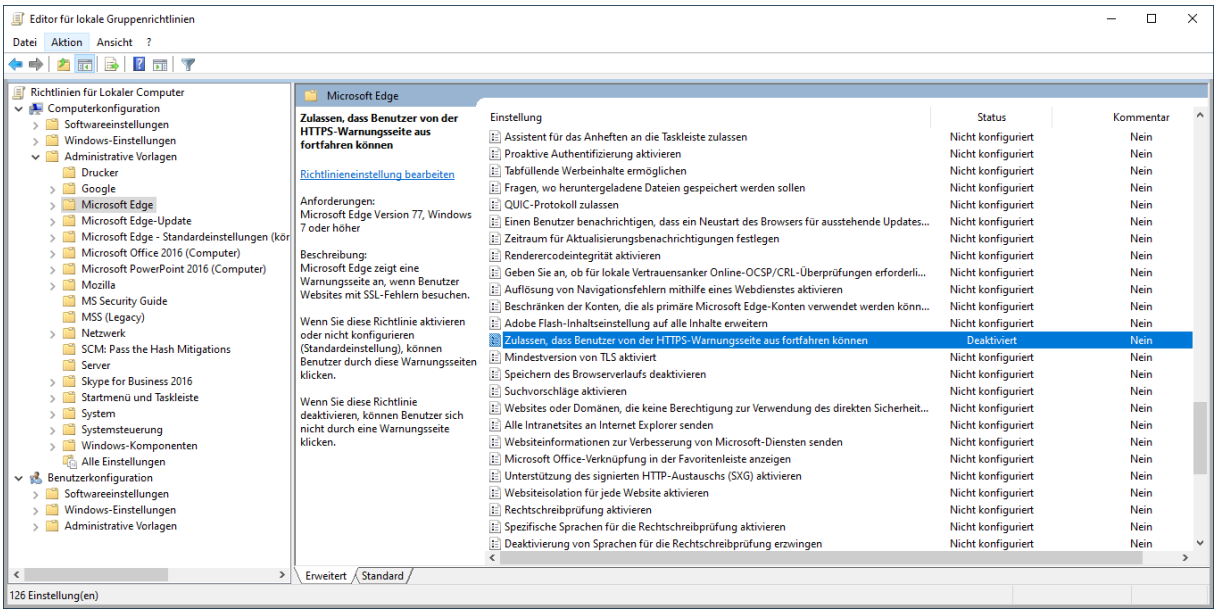
Die Einstellungen für den Microsoft Edge finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Microsoft Edge



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

Computerkonfiguration/Administrative Vorlagen/Microsoft Edge

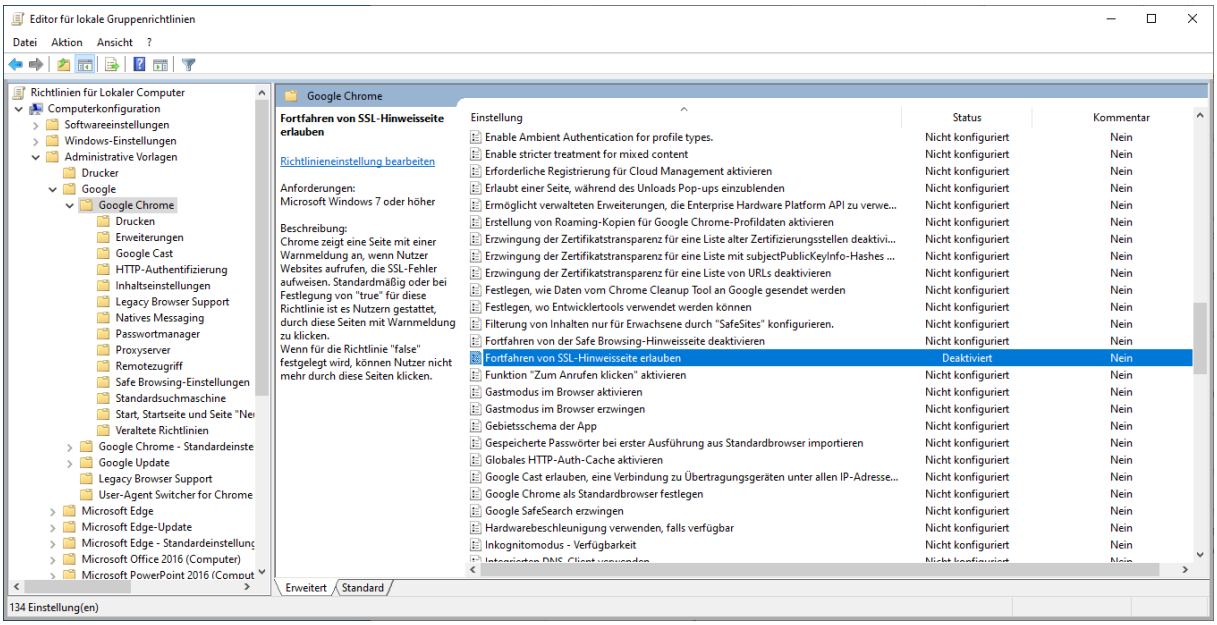


Erstellt von Jörn Walter **03.02.2020**

Zertifikatsfehler im Browser - Zugriff verweigern

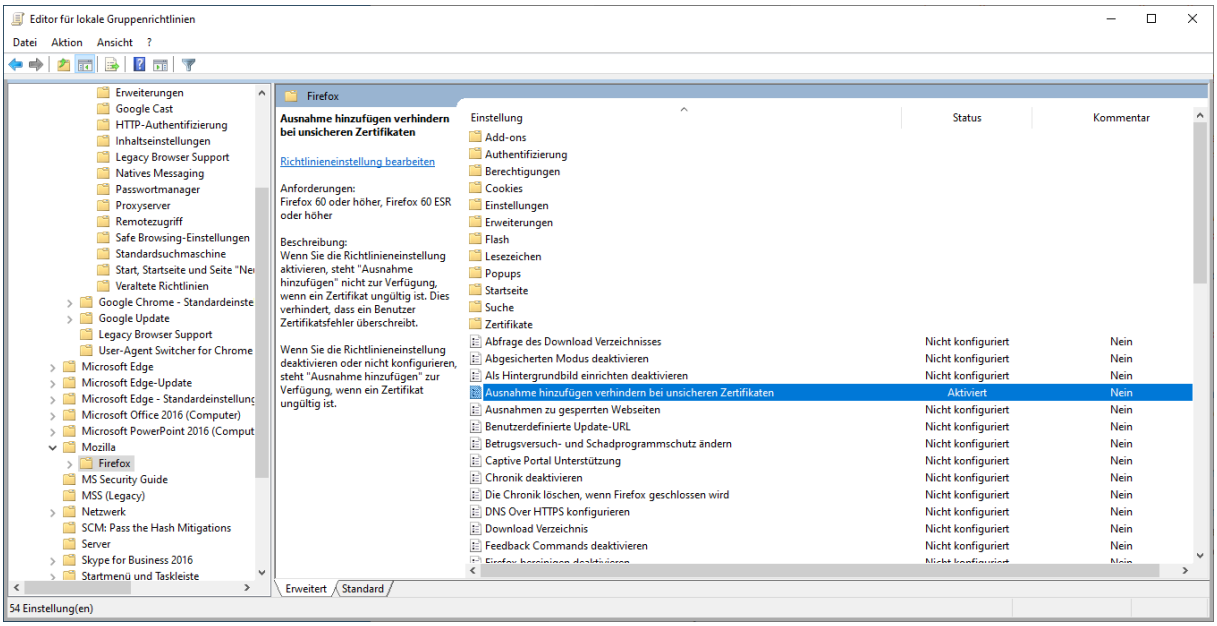
Die Einstellungen für den Google Chrome finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Google/Google Chrome



Die Einstellungen für den Mozilla Firefox finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Mozilla/Firefox

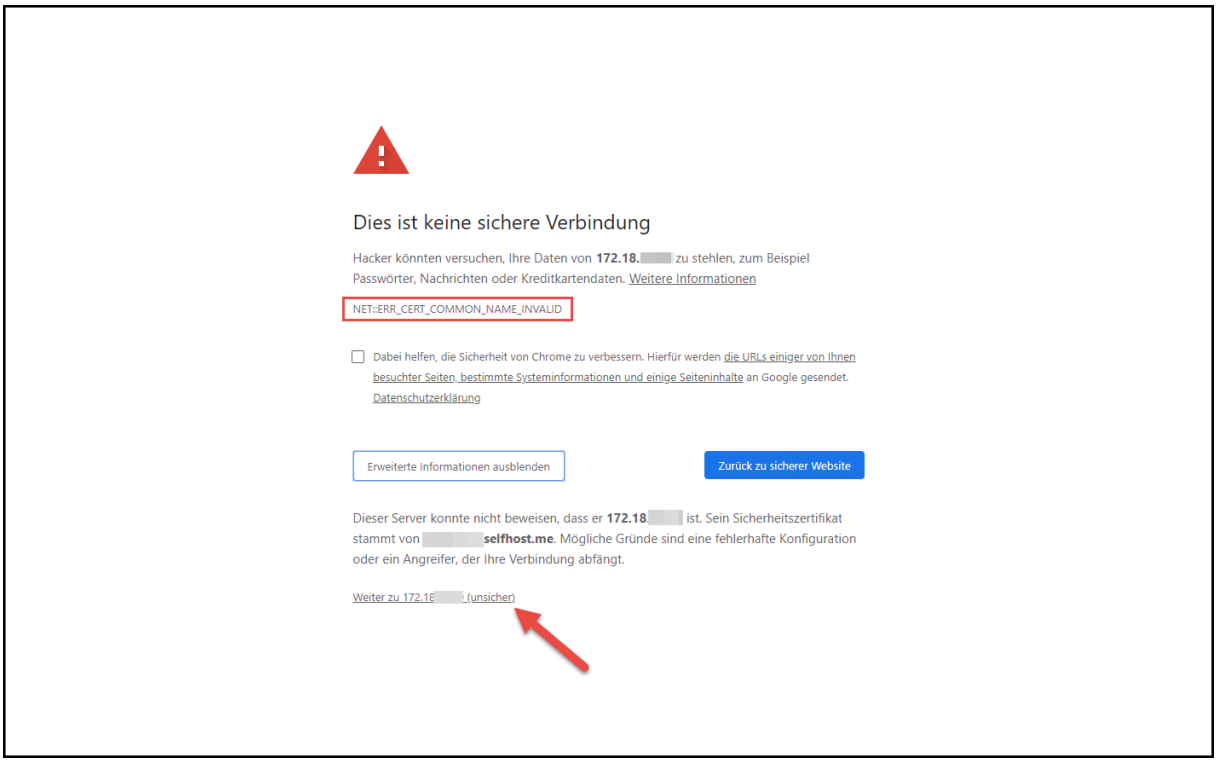


Erstellt von Jörn Walter **03.02.2020**

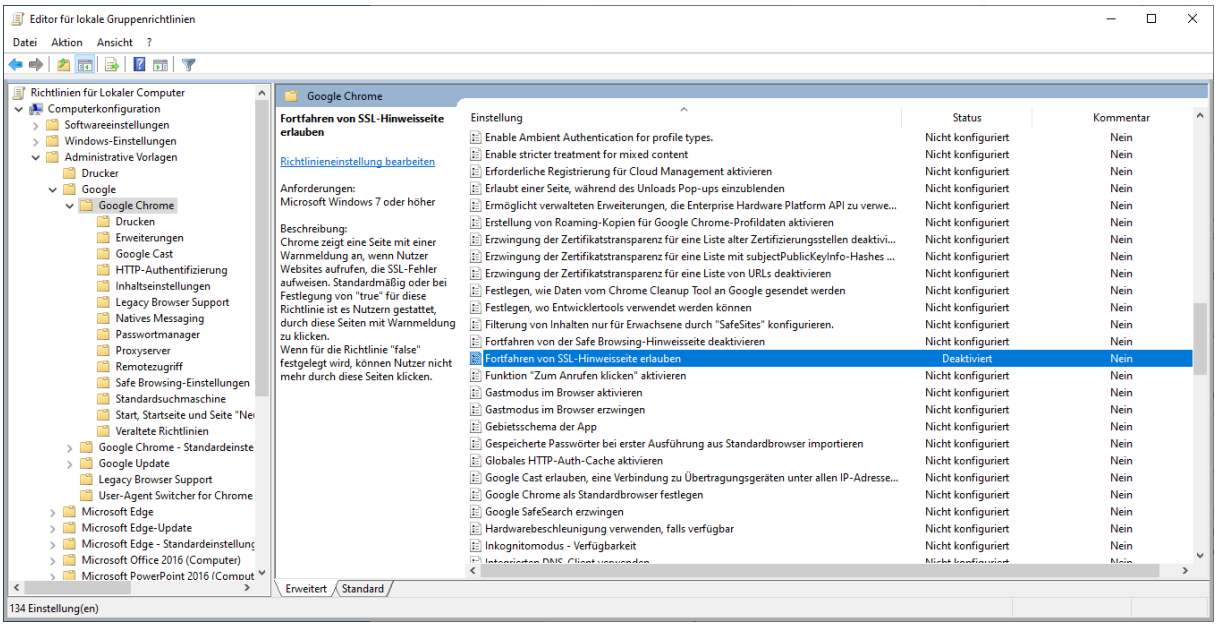
Zertifikatsfehler im Browser - Zugriff verweigern

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.

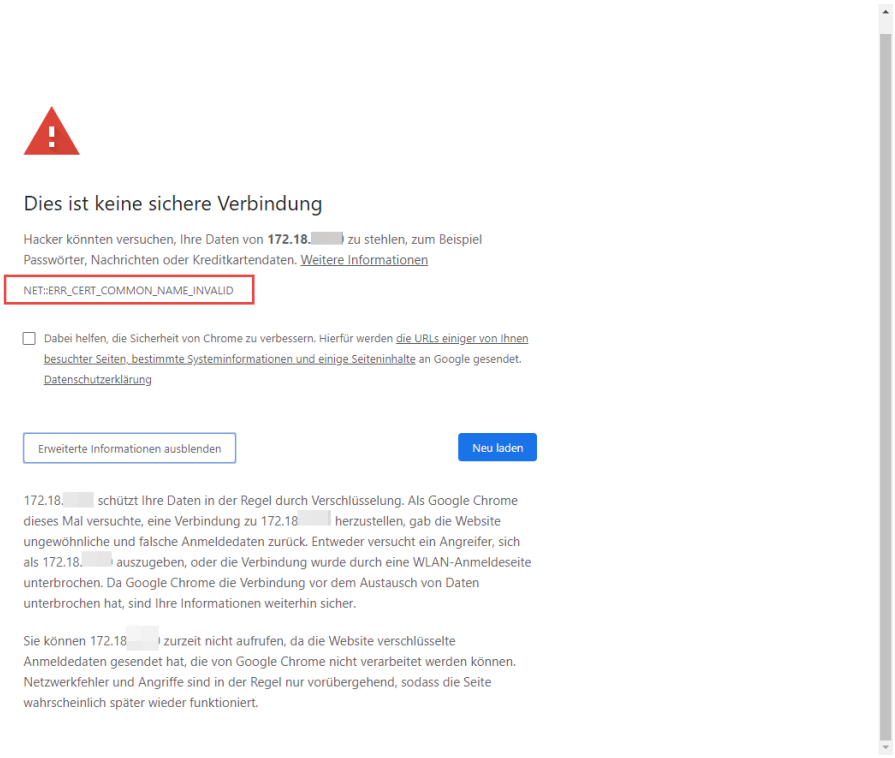


Schalten wir die Richtlinie „Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten“ auf = Deaktiviert,



Zertifikatsfehler im Browser - Zugriff verweigern

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



Erstellt von Jörn Walter **03.02.2020**