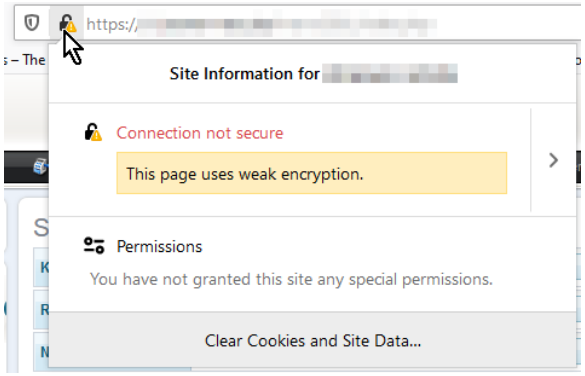
Abschaltung von SSLv3 und TLS 1.0

Wir schalten am 30.06.2020 den Support für SSLv3 und TLS1.0 in unserer Infrastruktur flächendeckend ab.

Warum schalten wir SSLv3 und TLS 1.0 **jetzt/bald** ab?

Anhand unserer Logfile-Überwachung können wir ermitteln, wie viele Verbindungen noch auf TLS1.0 setzen. In den letzten Monaten hat die Verwendung der veralteten Verschlüsselungsmethoden in unserer Infrastruktur stark abgenommen. Parallel dazu haben die populären Browser-Hersteller angekündigt, Webseiten deren Server TLS1.0 anbieten als unsicher zu kennzeichnen:



Wir sind daher der Meinung, dass wir nun im Interesse aller Kunden handeln, wenn wir diese veralteten Verschlüsselungsmethoden nicht länger anbieten.

Worum handelt es sich bei SSLv3 und TLS 1.0?

TLS1.0 und SSLv3 sind im weitesten Sinne Verschlüsselungsmethoden, die bereits (im Fall von TLS 1.0) im Juni 2018 von Großteilen der Industrie (PCI /DSS) abgekündigt wurden. Als Hoster ist man angehalten, diese aus heutiger Sicht unsicheren Verschlüsselungsmethoden nicht länger anzubieten. Stattdessen sollte man mindestens TLS1.2 verwenden.

Während moderne/aktuelle Betriebssysteme, E-Mail Clients oder Browser TLS1.2 problemlos nutzen können, ist ältere Software unter Umständen nicht in der Lage die neuen Methoden zu nutzen.

Welche Browser/Betriebssysteme können sich nach der Abschaltung nicht mehr verbinden?

Nutzer älterer Software, die seit langem keine Updates erfahren hat könnten Probleme erfahren. Beispielsweise:

- Mobiltelefon: Android 4.3 oder älter
- OS X 10.6.x mit Safari 5.x oder OS X 10.8.x mit Safari 6.x
- Windows XP, Vista, Version 7 mit Internet Explorer 8 oder älter
- Nutzer von OpenSSL 0.9.8y oder älter (z.B. ältere Linux-Systeme)

(Die oben aufgeführten Beispiele sind allesamt vom jeweiligen Hersteller abgekündigt und gelten als veraltet bzw unsupported)

Wie kann ich testen ob ich betroffen bin?

Sofern Sie die folgende URL problemlos aufrufen können, wird es auch nach dem 30.06.2020 für Sie keine Einschränkungen geben:
https://tlstest.power-netz.de/

Weiterführende Details liefert ein Besuch der Test-Seite von Qualsys:
https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html

Was ist, wenn ich die obige Webseite nicht problemlos aufrufen kann?

Bitte prüfen Sie, ob für Ihr Betriebssystem und für Ihren verwendeten Browser evtl ein Update des Herstellers verfügbar ist und spielen Sie dieses Update ein. Ggf müssen Sie sich beim Hersteller nach kostenpflichten Updates (z.B. Apple) erkundigen. Diese Updates müssten Sie bitte bis zum 30.06.2020 eingespielt haben.

Testlauf am 15.06.2020

Am 15.06.2020 werden wir einen Testlauf durchführen, in dem wir die Umstellungen für 2 Stunden testweise einspielen und danach wieder rückgängig machen.

Für Rückfragen stehen wir Ihnen gerne per Telefon oder E-Mail zur Verfügung.