PSW GROUP

Telefonischer Support
+49 661 480 276 10

über 17 Jahre

OCSP-STAPLING:
Der aktuelle Stand der Sperrlisten

TECHNISCHE ANLEITUNG

PSW GROUP GmbH & Co. KG

Flemingstraße 20-22
36041 Fulda
Hessen, Deutschland

So haben gesperrte oder widerrufene Zertifikate keine Chance mehr.

INHALTS-VERZEICHNIS

OCSP

Wie Theorie und Praxis auseinander gehen

OCSP – Kurz erklärt

„Online Certificate Status Protocol“, kurz auch OCSP genannt. Dieses Protokoll dient dem Feststellen, ob ein SSL/TLS-Zertifikat gesperrt oder widerrufen wurde. Sogenannte OCSP-Responder werden von Zertifizierungsstellen ("Certificate Authority", CA) betrieben, die das Zertifikat für Ihren Webserver ausgestellt haben. Dieses Zertifikat enthält die URL des OCSP-Responders Ihrer CA.

Wird eine https-Website mit der URL aufgerufen, findet über den Webbrowser eine Prüfung statt, ob eine Sperrung oder ein Widerruf des Zertifikats vorliegt. Achtung: ausschließlich bei den Browsern Mozilla Firefox und Microsoft Internet Explorer ist das OCSP aktiviert, in Googles Chrome-Browser ist das OCSP deaktiviert.

100%-IGE ERREICHBARKEIT KANN KEINER GEWÄHRLEISTEN

Praxis-Probleme mit OCSP

Um die Gültigkeit des Zertifikats zu prüfen, fragen diese beiden Browser, nachdem der Verbindungsaufbau zur Website stattgefunden hat, beim CA-eigenen OCSP-Responder an, dessen URL Teil des Serverzertifikats ist. Der Betreiber des OCSP-Responder erkennt die IP-Adresse, von der der Webserver aufgerufen wurde. Nun erhöht das zusätzliche Verbinden zum OCSP-Responder leider die Latenz; und inwieweit die IP-Adresse geloggt wird und dadurch Datenschutzprobleme entstehen erscheint zuweilen nicht nachvollziehbar. Blockiert man Verbindungen zum CA-Server, können sich zudem Angreifer einschleichen, um mittels geklautem Private Key eine Man-in-the-Middle-Attacke durchzuführen.

Ein weiterer Nachteil ergibt sich durch die Erreichbarkeit der CA-Server. Die Gültigkeitsprüfung via OCSP bedingt, dass die Server der jeweiligen CA immer zuverlässig auf die Anfragen reagieren; 100-prozentige Erreichbarkeit kann jedoch niemand gewährleisten. Erreicht der Browser nun aufgrund von Wartungsarbeiten oder sonstigen Ausfällen den Server der CA nicht, müsste das Zertifikat eigentlich als ungültig eingestuft und in der Folge die https-Verbindung verweigert werden.

Browser-Konfigurationen für erhöhte Sicherheit

Heißt: diese strenge Gültigkeitsprüfung ist einfach nicht praxistauglich. Um mehr Praxistauglichkeit zu erreichen, haben die Browserentwickler OCSP unsicher implementiert: erhält die Anfrage keine Antwort, sieht der Browser das Zertifikat einfach als gültig an, womit der eigentliche Sinn von OCSP verpufft.

Das ist auch der Grund, warum Google in Chrome auf OCSP verzichtet: bietet OCSP nicht die gewünschte Sicherheit, ist das Feature sinnlos. Manuell können Sie die Prüfung auch in Chrome wieder einschalten, indem Sie in den erweiterten Einstellungen den Punkt "Serverzertifikate auf Sperrung prüfen" aktivieren. Jedoch wird Ihnen das lediglich das Gefühl von Sicherheit vermitteln: es existiert keine uns bekannte Möglichkeit, Googles Browser so zu konfigurieren, dass Zertifikate bei Nichterreichbarkeit des OCSP-Servers als ungültig erklärt werden.

Mozillas Browser Firefox unternimmt den OCSP-Check per Default unsicher. Sie können Firefox jedoch unter "Erweitert" – "Zertifikate" – "Validierung" so konfigurieren, dass Zertifikate abgelehnt werden, wenn die Verbindung zum OCSP-Responder fehlschlägt.

Auch Microsoft hat sich für die unsichere OCSP-Prüfung im Internet Explorer entschieden. Zwar wurden ursprünglich Nutzer gewarnt, das Feature schaltete Microsoft jedoch im Jahre 2011 ab und begründet dies in einem Blogbeitrag damit, dass viel zu viele Warnungen auftraten, ohne dass dem Nutzer gesagt werden könne, wie er damit umzugehen hat.

Theorie und Praxis gehen ordentlich auseinander. Wenngleich auch einige Browser die Prüfung vornehmen bleibt sie nutzlos – auch ohne Antwort vom Server werden Zertifikate akzeptiert. Eben dieses Problem sowie diverse weitere Nachteile, wie die erhöhte Latenz, löst das Verfahren OCSP-Stapling.

OCSP - STAPLING

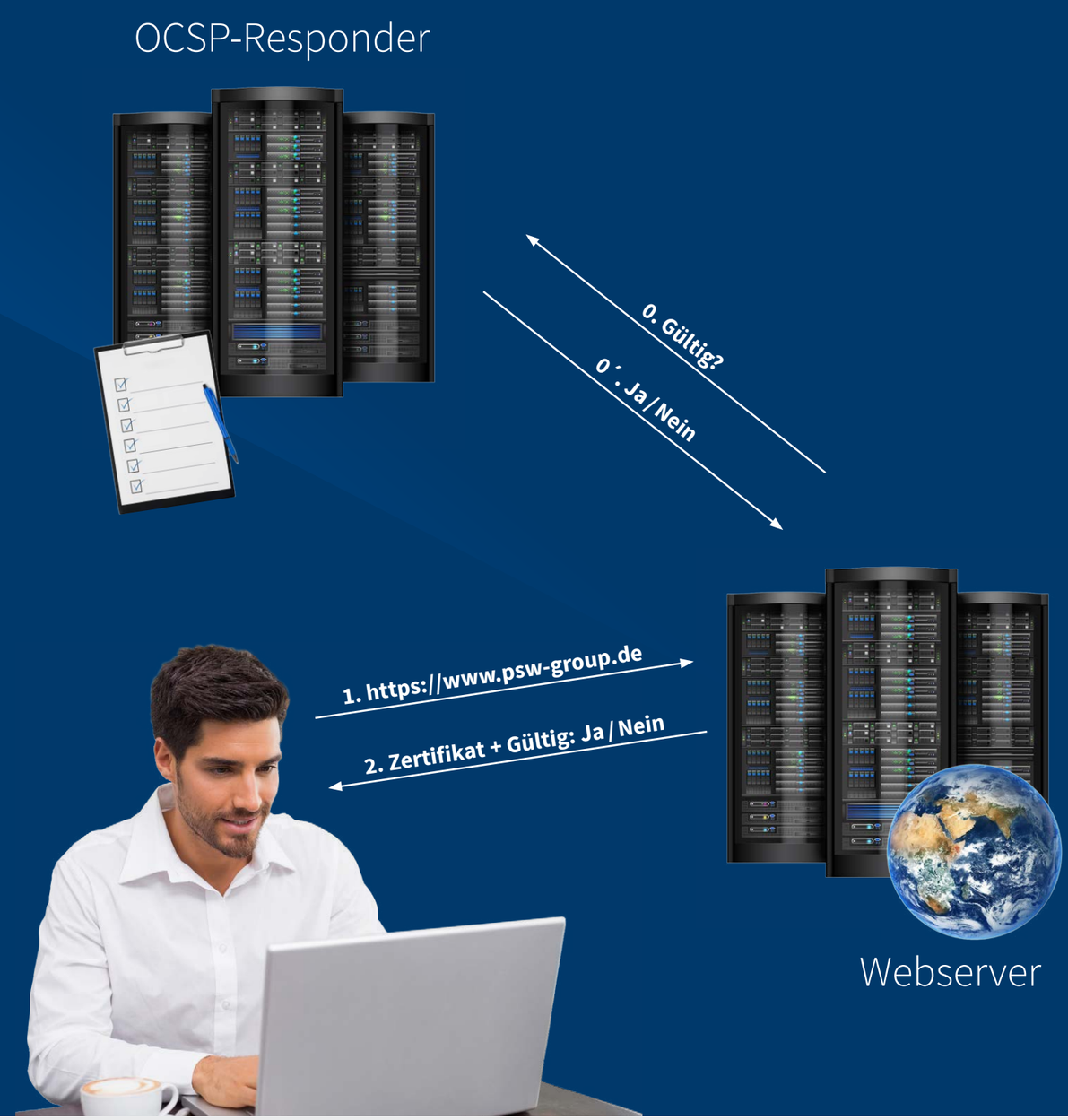
Bringen Sie Ihren Webserver auf Touren
und erhöhen Sie die Privatsphäre

Prüfen ohne OCSP-Responder-Verbindung

Die Internet Engineering Task Force (IETF) hat das Verfahren OCSP-Stapling seit geraumer Zeit standardisiert. Die Grundidee: nicht mehr der Nutzer selbst bzw. dessen Browser fragt bei der CA an, sondern der Webserver selbst bekommt diese Aufgabe zugeteilt. Die Antwort der Zertifizierungsstelle ist signiert, was die Authentizität gewährleistet und sie gilt nur für einen bestimmten Zeitraum, beispielsweise eine Stunde. Der Server speichert die Antwort und dem Nutzer wird sie während des TLS-Handshakes mitgeliefert. Auf diese Weise gelingt es dem Verfahren OCSP-Stapling, diverse Probleme von OCSP zu lösen:

Die Zertifikate selbst sind seit Dezember 2014 OCSP-fähig. Weiter ist es wichtig, dass Ihre Serversoftware das Feature unterstützt; zuweilen sind separate Konfigurationen notwendig.

- **Das Protokoll zeigt sich wesentlich datenschutzfreundlicher, denn Verbindungen zwischen Nutzer & CA-Server bleiben aus, womit auch das loggen der IP-Adresse des Users ausbleibt**
- **Mögliche Ausfälle des OCSP-Servers sind seltener ein Problem**
- **Der Server nimmt wieder Geschwindigkeit auf; das Problem der erhöhten Latenz verschwindet**



OCSP – STAPLING

bei Apache, Microsoft & nginx

****

Apache:
Unterstützt OCSP-Stapling
seit Version 2.4

WICHTIG:
Der SSLStaplingCache
ist außerhalb eines virtuellen
Hosts zu definieren

Die Apache Einrichtung

Legen Sie unter "/etc/apache2/conf.d/" eine Datei, beispielsweise "OCSPStapling.conf", mit folgendem Inhalt an:

```
SSLUseStapling on
SSLStaplingCache 'shmcb:/tmp/sta-
pling-cache(102400)'
SSLStaplingReturnResponderErrors off
```

SSL-Server-Test

Der SSL-Server-Test von Qualys SSL Labs erlaubt es Ihnen, zu testen: geben Sie Ihre URL ein und prüfen Sie, ob im Punkt "OCSP Stapling" ein grünes "Yes" kommt. So sieht es idealerweise aus:

OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains; preload
HSTS Preloading	Chrome Edge Firefox IE Tor

****

Microsoft:
Unterstützt OCSP-Stapling
ab Windows 2008

Die Microsoft Einrichtung

Sie brauchen keine gesonderten Konfigurationen vornehmen, da seit Windows 2008 OCSP Stapling per Default aktiviert ist.

****

nginx:
Unterstützt OCSP-Stapling
ab Version 1.3.7

DIE 3 MÖGLICHEN STOLPERSTEINE

FIREWALL BLOCKIERT

Haben Sie Ihren Server so konfiguriert, dass Ihre Firewall ausgehenden Traffic verhindert, so stellen Sie für OCSP-Stapling bitte eine Ausnahme her.

EXTERNE DNS-SERVER

Die OCSP-Responder-Adresse wird per Default von nginx auf dem DNS-Server aufgelöst. Die Webserverkonfiguration unterbindet notwendige externe DNS-Server-Verbindungen, bis Sie diese mit Ihrer lokalen DNS-Server-Adresse für nginx angepasst haben.

VERSCHIEDENE
VIRTUELLE HOSTS

Haben Sie verschiedene virtuelle Hosts konfiguriert, aktivieren Sie OCSP-Stapling bitte mindestens im als "default_server" konfigurierten Host. So kann das Verfahren auf allen weiteren virtuellen Hosts ebenfalls angewendet werden.

Die nginx Einrichtung

In der SSL-Konfiguration Ihres nginx-Servers sieht der OCSP-Stapling-Teil dann so aus (IP-Adressen und Pfade tauschen Sie bitte entsprechend aus):

```
ssl_trusted_certificate /pfad/kette_mit_root
ssl_certificate /pfad/serverzertifikat_mit_kette_ohne_root
ssl_stapling on;
ssl_stapling_verify on;
resolver 192.0.2.1 valid=300s;
resolver_timeout 10sf
```

Testen können Sie wieder mit Qualys SSL Labs oder aber OpenSSL. Werfen Sie dafür gerne einen Blick in die nginx-Dokumentation.

OCSP-STAPLING FÜR DATEN-SCHUTZ & TEMPO

"Das Verfahren OCSP-Stapling löst die Probleme von OCSP auf, die Konfigurationen und Voraussetzungen gelingen relativ problemlos. Haben Sie Fragen oder Probleme beim Umstieg auf OCSP-Stapling, setzen Sie auf unsere Unterstützung: nutzen Sie unseren Support oder lassen Sie sich von uns zurückrufen – wir helfen Ihnen gerne bei der Umsetzung, denn unser Service geht über den Standard hinaus!"

Telefonischer Support
+49 661 480 276 10

Christian Heutger
CEO | PSW GROUP

OCSP-STAPLING:
Der aktuelle Stand der Sperrlisten

TECHNISCHE
ANLEITUNG

PSW GROUP

PSW GROUP GmbH & Co. KG
Flemingstraße 20-22
36041 Fulda
Hessen, Deutschland