Citrix ADC SSL Bewertung optimieren – Stand Februar 2020

Im ursprünglichen Artikel bin ich auf die Basis-Schritte eingegangen, wie man bei Qualys die SSL Bewertung auf einen guten Stand bringen kann.

Da die Test-Routinen jeweils an die neusten Erkenntnisse angepasst werden, waren meine Bewertungen auf ein B gesunken, was für mich nicht hinnehmbar war. Hier möchte ich euch die Schritte beschreiben, wie ich wieder auf eine A+ Bewertung gekommen bin.

Der erste Schritt ist relativ einfach. Durch die aktivierten TLS 1.0 und TLS 1.1 wurde die Bewertung automatisch auf ein B heruntergestuft. Dazu kann man diese im virtuellen Server einfach in den SSL Parametern deaktivieren. Im gleichen Atemzug habe ich auch bereits TLS 1.3 aktiviert.

```
set ssl vserver nsgw-vsrv-gateway.domain.pit -tls1 DISABLED -tls11 DISABLED -tls13 ENABLED
```

Der nächste Schritt beinhaltet die Anpassung der Cipher Suites. Bei Qualys findet man einen direkten Link mit der Auflistung passender Algorithmen. Nebst dem bestehenden TLS 1.2 habe ich auch gleich diese für TLS 1.3 hinzugefügt.

Man kann einerseits die bestehende Gruppe anpassen oder wie ich eine neue Gruppe erstellen:

```
add ssl cipher CIPHER-PIT-AEAD
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 1
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384 -cipherPriority 2
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-ECDHE-ECDSA-AES128-SHA256 -cipherPriority 3
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-ECDHE-ECDSA-AES256-SHA384 -cipherPriority 4
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.3-AES256-GCM-SHA384 -cipherPriority 5
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.3-AES128-GCM-SHA256 -cipherPriority 6
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 7
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 8
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384 -cipherPriority 9
bind ssl cipher CIPHER-PIT-AEAD -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256 -cipherPriority 10
```

Anschliessend muss man nur noch auf dem vServer die alte Cipher Gruppe entfernen und die neue hinzufügen um in der Bewertung ein A+ zu sehen:

```
unbind ssl vserver nsgw-vsrv-gateway.domain.pit -cipherName CIPHER-PIT
bind ssl vserver nsgw-vsrv-gateway.domain.pit -cipherName CIPHER-PIT-AEAD
```

Zu guter Letzt müssen sämtliche Applikationen getestet werden, ob auch alle mit den verschärften Algorithmen umgehen können.

Viel Spass beim Nachbau :-)

ADC-IncreaseSSL-20200222Herunterladen