Automatisierung von X.509-Zertifikaten

Einsatz von Netzwerkagenten zur Automatisierung von X.509-Zertifikaten

Praktikumsbericht

ausgearbeitet von

Suleiman Odeh
Matr. Nr.3391757

vorgelegt an der
Rheinische Friedrich-Wilhelms-Universität Bonn
Institut für Informatik IV
Arbeitsgruppe für IT-Sicherheit

im Studiengang
Cyber Security (B.Sc.)

Erstprüfer:	Prof. Dr. Michael Meier Universität Bonn
Zweitprüfer:	Dr. Matthias Frank Universität Bonn
Betreuer:	Dr. rer. nat. Marc-Philipp Ohm Universität Bonn

Universität Bonn

Bonn, 15. April 2024

Inhaltsverzeichnis

1 Einleitung

Heutzutage spielt die Automatisierung von X.509 Zertifikaten eine große Rolle. Insbesondere können durch diese Zertifikate das Identitätsnachweis und der Authentisierung der Benutzer erreicht werden [Bis22].

Aufgrund der großen Anzahl von X.509 Zertifikaten in einem Unternehmen ist es schwierig, alle diese Zertifikate manuell zu automatisieren. Sectigo Certificate Manager (SCM) bietet die Möglichkeit, die X.509 Zertifikate zu automatsieren.

SCM ist eine cloudbasierte Plattform von *Sectigo*, die die Möglichkeit bietet, Zertifikate vollständig zu kontrollieren. Dadurch können die Risiken im Zusammenhang mit Zertifikaten reduziert werden. [Sec18]

SCM bietet die sogenannten Network Agents, die für die Erkennung und Automatisierung aller Zertifikate, die über einen Server laufen. Ziel der Agenten ist es, Zertifikate zu erkennen und nach der Erneuerung automatisch auf dem Zielserver zu installieren. Dadurch wird Zeit gespart und das Risiko durch ablaufende Zertifikate vermieden.

Ziel dieses Praktikums ist es, zwei Netzwerk-Agents zu implementieren, wobei im ersten Agent lokal-Server unter Windows und im zweiten Agent ein Remote-Server unter Linux konfiguriert wird. Der Grund dafür wird später im Abschnitt `Abteilung und Projekts Beschreibung` erklärt.

2 Abteilung und Projekts Beschreibung

In diesem Kapitel wird das Unternehmen Westdeutscher Rundfunk (WDR) beschrieben, in dem ich mein Praktikum absolviert habe. Außerdem wird die Abteilung Cyber Security des WDR kurz vorgestellt. Zuletzt wird das Projekt genauer beschrieben, einschließlich der verwendeten Werkzeuge.

2.1 Abteilung Cybersicherheit beim Westdeutschen Rundfunk

Die Abteilung Cybersecurity des WDR befindet sich in Köln. Sie ist in vier Competence Center unterteilt. Das Praktikumsprojekt wurde im Competence Center Security Services durchgeführt. Dieses Competence Center beschäftigt sich mit der Bereitstellung von zentralen Security Services. Dazu gehören CloudSecurity, E-Mail-Schutz und Zertifikatsmanagement.

2.2 Projektsbeschreibung

Für dieses Projekt wurden zwei Netzwerkagenten verwendet. Beide Agents läufen lokal auf einem Windows-Rechner

Für den ersten Agenten wird nur ein lokaler Server unter Windows konfiguriert, da es zeitlich nicht möglich war, für den Agenten auch ein remote Server zu konfigurieren. Der entsprechende Server für den ersten Agenten ist Internet Information Services (IIS). Dieser Server läuft auf Port 80 und muss auf Port 443 umgestellt werden, damit die Zertifikate im SCM erkannt werden.

Für den zweiten Agenten wird nur ein Remote-Apache-Server unter Linux konfiguriert, da Apache auch auf Port 80 laufen will. Und die WDR Laptops sind Windows und daher ist Port 80 bereits für IIS reserviert und daher kann kein lokaler Server für den zweiten Agenten konfiguriert werden. Der verwendete Remote-Apache läuft bereits auf Port 443.

Es gibt drei Schritte damit die Agents erfolreich eingesetzt werden:

1. Installation des Agenten: Der Agent muss auf dem Computer des Benutzers installiert werden.
2. Konfiguration des Agenten: Der Server für den bereits installierten Agenten muss hinzugefügt und lokal oder remote konfiguriert werden
3. Zertifikate für die automatische Installation konfigurieren: Im letzten Schritt wird der Agent so konfiguriert, dass er die Zertifikate automatisch auf dem Server installiert, wenn diese erneuert werden.

3 Implemntierung der Automatisierung in Sectigo Certificate Manager

Dieses Kapitel beschreibt die Implementierung des Projekts. Es werden die Schritte für den Einsatz des Agenten sowohl für Linux-Agent als auch für Windows-Agent beschrieben.

3.1 Network-Agent für Windows

In diesem Unterkapitel werden die Schritte für die Installation und auch für Kofugration der Agents unter Windows erklärt.

3.1.1 Installation der Agent

Im SCM loggt man sich ein und fügt einen neuen Agenten hinzu. Nach dem Einfügen erscheint ein neues Fenster, in dem der Agent heruntergeladen werden kann. Man klickt auf Windows, damit der Agent auf das System heruntergeladen wird. Zusätzlich sollte das angezeigte Token kopiert werden. Dieses Token wird benötigt, um den Agenten zu identifizieren. Nach dem Download klickt man auf die Datei, um die Installation zu starten. Zunächst wird man aufgefordert, die Endbenutzer-Lizenzvereinbarung (EULA) zu akzeptieren und einen Installationsort für den Agenten auszuwählen. Anschließend muss das Token eingegeben werden. Der wichtigste Schritt ist dann die Eingabe der Proxy-Informationen. Alle Anfragen im WDR-Netzwerk gehen über den WDR-Proxy und damit der Agent den Status connected erhält, müssen die WDR-Proxy-Informationen eingegeben werden. Anschließend wird kurz gewartet und der Agent automatisch gestartet. Der Agent erhält dann im SCM den Status connected, wie in Abbildung 1 dargestellt.

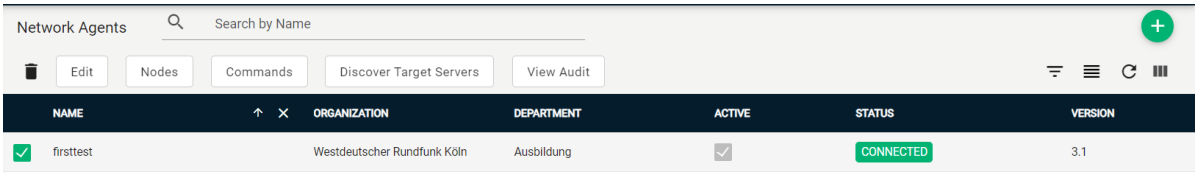

Abbildung 1: *Der Windows Agent mit dem Namen Firsttest erhält nach erfolgreicher Installation den Status connected.*

3.1.2 Konfiguration der Agent

Da ich beim WDR mit dem Betriebssystem Windows gearbeitet habe, wird sich der Agent nach der Installation automatisch mit dem IIS-Server verbinden. Für die Konfiguration ist es aber noch notwendig, den Server auf https zu bringen, damit der Agent die Zertifikate, die über IIS laufen, automatisieren kann.

Um IIS auf https zu bringen, erhaltet man ein Zertifikat von WDR. Dieses Zertifikat muss dann in den IIS Manager importiert werden. Danach muss man das Zertifikat einer IP-Adresse zuordnen, indem man unter Bindung die IP-Adresse und zusätzlich Port 443 auswählt.

Im letzten Schritt muss die entsprechende Domain im Zertifikat durch die zuständige Person im WDR der gewählten IP-Adresse zugeordnet werden, damit das Zertifikat als gültig betrachtet wird. In Abbildung 2 kann man nun sehen, dass die Serverzertifikate im SCM zu sehen sind und bereit für den Schritt Auto-Installation sind.

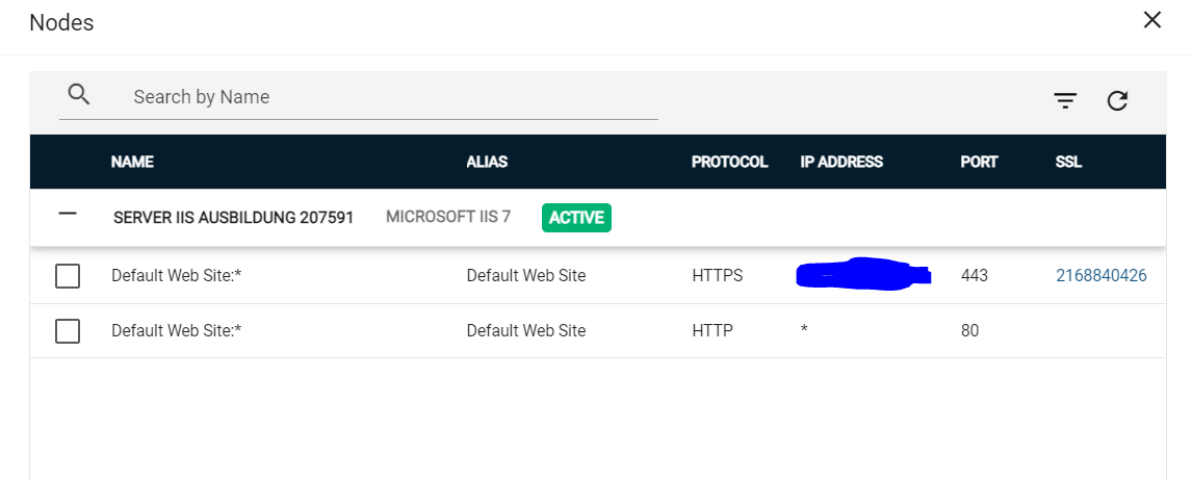

Abbildung 2: *Die IIS-Serverzertifikate mit den zugehörigen Ports und Protokollen werden nach erfolgreicher Konfiguration im SCM angezeigt.*

3.2 Network-Agent für Linux

In diesem Unterkapitel werden die Schritte für die Installation und auch für Kofugration der Agents unter Linux erklärt. Für Sowohl die Installation als auch die Konfiguration werden Windows Subsystem for Linux (WSL) verwendet. Wichtig zu beachten, dass alle Befehle sudo Rechte brauchen.

3.2.1 Installation der Agent

In SCM meldet man sich an und fügt ein neue Agent hinzu. Nach dem Einfügen erscheint ein neues Fenster, in dem der Agent heruntergeladen werden kann. Man klickt auf Linux, damit der Agent auf das System heruntergeladen wird. Zusätzlich sollte man das angezeigte Token kopieren. Dieses Token wird zur Identifizierung des Agenten benötigt. Nach dem Download öffnet man WSL und erteilt Ausführungsberichtugng für Datei. Danach wird aufgefordert, die EULA zu akzeptieren. Anshcließend wird das Token eingegeben. Der wichtigste Schritt ist dann die Eingabe der Proxy-Informationen. Alle Anfragen im WDR-Netz gehen über den WDR-Proxy und damit der Agent den Status connected erhält, muss die WDR-Proxy-Information eingegeben werden. Im Vergleich zum Windows-Agent muss der Agent manuell gestartet werden.Der Agent bekommt dann den Status connected in SCM angezeigt.

3.2.2 Konfiguration der Agent

Der bereitgestellte Remote Server läuft bereits auf https. Es muss aber noch eine Verbindung zum Remote Server aufgebaut werden. Dies geschieht, indem man die WSL öffnet. Danach stellt man eine SSH-Verbindung zum Remote-Server her. An dieser Stelle meldet man sich im SCM an und fügt dem Agenten einen Apache Server hinzu. Bei der Einstellung gibt man den Zertifikatspfad an, damit die Serverzertifikate sowohl gefunden als auch automatisch in SCM importiert werden können. man muss auch die Zugangsdaten für den Server eingeben. Schlißlich speichert man die Einstellung und wartet kurz dann werden alle Server Zertifikate angeziegt werden.

3.3 Die Zertifikate für Auto-Installation konfigurieren

Zuerst muss ein neues Zertifikat für die automatische Installation im SCM angefordert werden. Abbildung 3 zeigt, welche Antragsoption zu wählen ist. Die alte Domain muss angegeben werden, damit das alte importierte Zertifikat in SCM ersetzt wird. Außerdem muss der Server angegeben werden, auf dem das Zertifikat installiert werden soll. Nachdem dieses Zertifikat erstellt wird, wird das Serverzertifikat automatisch durch das neue Zertifikat in SCM ersetzt, da beide Zertifikate die gleiche Domain enthalten.

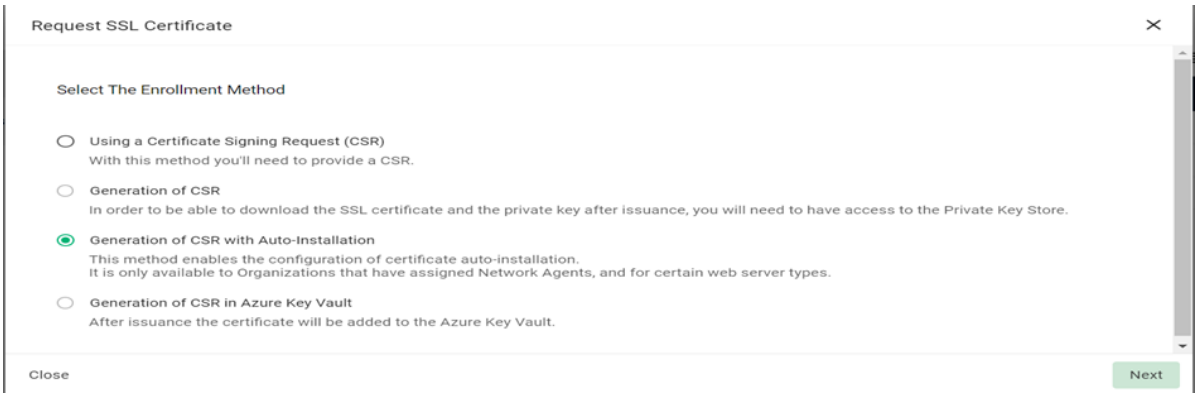

Abbildung 3: *Die dritte Option stellt die Zertifikatsanforderung mit Auto-Installation dar.*

Die beiden Zertifikate sind nun im SCM ausgetauscht, müssen aber noch auf dem Server ausgetauscht werden. Bevor dies geschieht, möchte das SCM den Apache neu starten, benötigt dafür aber sudo-Rechte. Es muss also ein Skript geschrieben werden, das den Apache mit

sudo-Rechten neu startet. Danach muss man sudo-Rechte für normale Benutzer vergeben, indem man die Datei sudoers ändert. Dies stellt ein großes Risiko dar, da normale Benutzer ohne Passwort auf alle root-Dateien zugreifen können. Dies wird nur einmal gemacht, das heißt bei der nächsten Installation muss der Apache nicht neu gestartet werden.Schließlich muss der Pfad zum Skript bei der Konfiguration des Apache im SCM angegeben werden. Der IIS muss nicht gestartet werden.

Um die beiden Zertifikate auf dem Server zu tauschen, geht man zuerst in das Serververzeichnis. Dort sind alle Zertifikate aufgelistet. Für den Port 443 muss das neu installierte Zertifikat ausgewählt werden. Ist das erledigt, wird bei der nächsten Installation automatisch das danach erstellte Zertifikat für Port 443 ausgewählt, da es den gleichen Namen wie das alte Zertifikat hat.

4 Zusammenfassung

Dieses Praktikum wurde beim Westdeutschen Rundfunk absolviert. Es wurde ein Projekt durchgeführt. Das Projektziel ist, zwei Network-Agents zu implementieren. Der Sectigo Certificate Manager der Firma Sectigo bietet die Möglichkeit, diese Network-Agents einzusetzen. Beide Network Agents dienen der Automatisierung von X.509 Zertifikaten. Für den ersten Agenten wird ein lokaler IIS-Server unter Windows konfiguriert. Für den zweiten Agenten wird ein remote Apache-Server unter Linux konfiguriert. Bei der Automatisierung wird zuerst der Agent auf einer Maschine installiert. Anschließend wird der Server konfiguriert, wobei für den Apache eine SSH-Verbindung erforderlich ist. Anschließend wird ein neues Zertifikat für die automatische Installation angefordert. Nach der Installation auf dem Server muss dieses Zertifikat für den Port 443 ausgewählt werden. Das Ergebnis ist, dass der erste Agent ohne Fehler und ohne Risiko funktioniert hat. Im Vergleich zum ersten Agenten bestand beim zweiten Agenten das Risiko, dass für den normalen Benutzer für kurze Zeit sudo-Rechte angegeben werden müssen, damit SCM den Apache neu starten kann.

Literaturverzeichnis

[Bis22] Biswas, Debarati: *Are You Still Managing X.509 Certificates Manually? Time to Embrace Automation*. 2022. URL: https://www.appviewx.com/blogs/are-you-still-managing-x-509-certificates-manually-time-to-embrace-automation/ (besucht am 07. 04. 2024).

[Sec18] Sectigo: *Sectigo Certificate Manager*. 2018. URL: https://www.sectigo.com/resource-library/sectigo-certificate-manager (besucht am 07. 04. 2024).

Abbildungsverzeichnis