HighConsulting

Customized Remote Service Manager
-
Sicherheitskonzept

HighConsulting GmbH & Co. KG
aiti-Park / Gebäude 09a
Werner-von-Siemens-Str. 6
86159 Augsburg

Tel: +49 (0) 821 450 788 0
Fax: +49 (0) 821 450 788 20
E-Mail: order@high-consulting.de

Geschäftsführer:
Gerd Pauli
Dr. Walter Hafner

HRA 16021 Amtsgericht Augsburg
St. Nr. 102/162/79803
Id. Nr. DE 256906131

Einleitung

Der HighConsulting Customized Remote Service Manager (CRSM) dient der sicheren Fernwartung von Industrieanlagen und anderen entfernten Netzwerken.

Die Fernwartung an sich stellt eine sicherheitskritische Komponente innerhalb des Unternehmensnetzwerks dar und sollte vor dem Einsatz entsprechend evaluiert werden. Grundlage für die Sicherheit einer Fernwartungsumgebung ist neben der Absicherung gegen Social-Engineering Angriffe die Sicherheit der dafür eingesetzten Software an sich.

Im Gegensatz zu Angriffen mit Methoden des Social-Engineering, bei denen immer Menschen beteiligt sind, lassen sich Angriffe auf technischer bzw. kryptographischer Ebene durch ein gut gewähltes, leistungsfähiges Sicherheitskonzept der Fernwartungssoftware vermeiden. Der CRSM wurde daher von Anfang an mit Blick auf die einschlägigen Empfehlungen des BSI und anderer Gremien entwickelt. Insbesondere finden die folgenden Dokumente Verwendung:

- Grundschutzkatalog Kapitel M 5.33 des Maßnahmenkatalogs - Absicherung von Fernwartung (1)
- Technische Richtlinie TR-02102-1 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen (2)
- Technische Richtlinie TR-02102-2 - Verwendung von Transport Layer Security (TLS) (3)
- Empfehlung BSI-CS 067 - Anforderungen an industriefähigen Netzwerkkomponenten (4)
- Empfehlung BSI-CS 054 - Grundregeln zur Absicherung von Fernwartungszugängen (5)

Alle sicherheitsrelevanten Komponenten wurden unter Verwendung von geprüften, quelloffenen Algorithmen implementiert. So wird sicher gestellt, dass keine Fehler durch eigene, inhärent unsichere Algorithmen eingeführt werden. Zusätzlich dazu werden alle Protokolle im sichersten empfohlenen Modus betrieben.

Im Folgenden werden die einzelnen Komponenten des CRSM Sicherheits-Frameworks detailliert beschrieben.

(1)
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05033.html

(2)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.pdf?__blob=publicationFile

(3)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf?__blob=publicationFile

(4) https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_067.pdf?__blob=publicationFile

(5) https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/anwender/dienste/BSI-CS_054.pdf?__blob=publicationFile

Gesamtkonzept

Wie die meisten modernen Fernwartungslösungen baut der CRSM auf verschlüsselten Virtual Private Network (VPN) Verbindungen, sog. Tunneln auf. Dabei wird im offenen, unverschlüsselten

Internet ein verschlüsseltes, lokales Intranet abgebildet. Im Unterschied zu vielen anderen Lösungen verbindet der CRSM die Endpunkte einer Kommunikation – etwa Wartungstechniker und Industrieanlage – nicht direkt miteinander. Die Kommunikation wird stattdessen immer über einen zentralen Rechner, den CRSM Server geleitet.

Verbindungen werden grundsätzlich vom Wartungstechniker bzw. dem VPN Gateway der Anlage hin zum CRSM Server initiiert. Soll vom CRSM Server aus eine Verbindung zu einer nicht permanent verbundenen Anlage initiiert werden, wird lediglich ein Verbindungswunsch übermittelt und das Öffnen der eigentlichen Verbindung dem Anlagen-Gateway überlassen (Callback).

Der CRSM Server bildet den Endpunkt für jeden VPN Tunnel im CRSM Gesamtverbund. Er nimmt Verbindungswünsche entgegen, analysiert und erlaubt sie je nach Berechtigung.

Eine Kommunikation zwischen Wartungstechnikern oder zwischen Anlagen ist grundsätzlich nicht möglich!

VPN Tunnel

Jegliche Kommunikation zum und vom CRSM Server erfolgt verschlüsselt. Die verwendete Verschlüsselungstechnologie ist OpenVPN (1). OpenVPN basiert auf dem TLS Protokoll (2), welches auch für die verschlüsselte Kommunikation mit Webservern eingesetzt wird (HTTPS).

Zur Implementierung des TLS Protokolls wird die quelloffene Bibliothek OpenSSL (3) verwendet.

OpenSSL 1.2 wurde 2006 vom NIST nach dem Standard FIPS 140-2 zertifiziert, die im CRSM eingesetzte Version OpenSSL 2.0.1 im Jahr 2012 (4). FIPS 140-2 „Security Requirements For Cryptographic Modules“ (5) ist der Standard, den Kryptographie-Module für den Einsatz in öffentlichen Einrichtungen der USA erfüllen müssen. Detailliert dargelegt ist die OpenSSL FIPS 140-2 Security Policy in (6).

Da TLS sehr viele verschiedene, unterschiedlich sichere Verschlüsselungsalgorithmen zulässt, ist es wichtig zu wissen, welche Algorithmen eingesetzt werden. Für den CRSM sind dies:

- Key Hashing (HMAC) (7): RSA SHA3-512
- Verschlüsselung der IP Pakete: AES-256-CBC
- Diffie-Hellman Parameter für den Schlüsselaustausch (8): 2048 bit
- Schlüssellängen: 4096 bit

Diese Parameter definieren mithin die sicherste Variante einer TLS/OpenVPN Verbindung. Es werden ausschliesslich diese Parameter im CRSM Verbund verwendet. Ein Fallback auf unsichere Parameter ist nicht möglich.

Der Aufbau der Tunnel ist zertifikatsbasiert. Selbstverständlich findet eine Zwei-Wege Authentifizierung statt. D.h., der Server muss sich am Client authentifizieren und der Client am Server. Dabei muss das Client-Zertifikat beim Verbindungsaufbau folgenden Bedingungen genügen:

- es muss vom CRSM Server signiert sein (siehe auch nächstes Kapitel)
- es muss gültig sein, d.h. es darf nicht abgelaufen sein und nicht in der Revocation List stehen
- es darf nicht temporär durch den CRSM Administrator gesperrt sein
- der Zertifikatsname muss mit einem im CRSM angelegten Objekt (Anlage/Techniker) übereinstimmen

Wird eine der Bedingungen nicht erfüllt, ist kein Verbindungsaufbau möglich. Da die Client-Zertifikate ausschliesslich auf dem CRSM Server generiert werden, ist sicher gestellt, dass keine unauthorisierten Verbindungen aufgebaut werden können. Sollte ein Client-Zertifikat entwendet

werden, lässt es sich leicht zentral sperren. Diese Sperrung kann auch ein Wartungstechniker vornehmen, der einen Missbrauch seines Zertifikats festgestellt hat.

Durch die Verwendung dieser sicheren Parameter war der CRSM zu keiner Zeit anfällig für die kürzlich bekannt gewordenen SSL Sicherheitslücken wie Heartbleed und Poodle!

(1) http://openvpn.net/

(2) http://de.wikipedia.org/wiki/Transport_Layer_Security

(3) https://www.openssl.org/

(4) https://www.openssl.org/docs/fips/fipsvalidation.html

(5) http://www.nist.gov/itl/upload/fips1402.pdf

(6) http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf

(7) http://cseweb.ucsd.edu/~mihir/papers/hmac.html

(8) http://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch

Zertifikatsmanagement

Ein x.509 Public-Key Zertifikat identifiziert die Kommunikationsteilnehmer eindeutig und fälschungssicher. Wikipedia schreibt dazu (1):

> Um beim Einsatz von asymmetrischen Kryptosystemen falsche (z.B. untergeschobene) von echten Schlüsseln zu unterscheiden, wird ein Nachweis benötigt, dass der verwendete öffentliche Schlüssel auch zum designierten Empfänger der verschlüsselten Nachricht bzw. zum Sender einer digital signierten Nachricht gehört. Außerdem muss bei der Verschlüsselung und Prüfung der digitalen Signatur sichergestellt werden, dass der Schlüssel auch mit diesem kryptographischen Verfahren und für den gedachten Anwendungsbereich verwendet werden darf. Diese Nachweise werden durch digitale Zertifikate geleistet.
>
> …
>
> Der Aussteller eines Zertifikates wird als **Zertifizierungsinstanz** bezeichnet. Die Zertifizierungsinstanz sollte von einer vertrauenswürdigen Organisation oder Stelle (z.B. eine Behörde) betrieben werden, damit die Anwender sich auf die in den Zertifikaten enthaltenen Informationen verlassen können. Durch die digitale Signatur über das Zertifikat lässt sich die Authentizität und Integrität des digitalen Zertifikates überprüfen. Für diese Prüfung wird jedoch wiederum eine Zuordnung des Signaturschlüssels des Ausstellers zu seiner Identität, d.h. ein weiteres Zertifikat, benötigt. Diese Hierarchie von Zertifikaten bildet eine Public-Key-Infrastruktur (PKI).

Die einzige praxisrelevante Angriffsmöglichkeit auf eine PKI besteht in der Vortäuschung einer vertrauenswürdigen Zertifizierungsinstanz und der Signierung von Zertifikatsanträgen mit dem vorgetäuschten Instanz-Schlüssel.

Um diese Angriffsmöglichkeit zu unterbinden, werden alle Zertifikate innerhalb der CRSM Infrstruktur auf dem CRSM Server generiert und gepflegt. Damit stellt der CRSM Server seine eigene Zertifizierungsinstanz dar. Die dazu eingesetzte Software ist easy-rsa (2), das als Teil des OpenVPN Pakets direkt auf OpenSSL aufsetzt.

Wie im vorigen Abschnitt „VPN-Tunnel“ angemerkt, werden die Client-Zertifikate, mit denen sich Anlagen und Techniker ausweisen vom CRSM Server nur akzeptiert, wenn sie bei der Erstellung auch von ihm signiert wurden.

(1) http://de.wikipedia.org/wiki/Public-Key-Zertifikat

(2) http://openvpn.net/index.php/open-source/documentation/miscellaneous/77-rsa-key-management.html

Zugangsberechtigungen

Mit gültigen Zertifikaten können VPN Verbindungen innerhalb des CRSM Verbunds hergestellt werden. Das bedeutet allerdings noch nicht, dass ein Zugriff der Techniker auf die Anlagen möglich ist.

Für einen erfolgreichen Anlagenzugriff eines Technikers sind mehrere Bedingungen nötig:

- grundlegendes Recht zum Zugriff auf die Anlage oder Komponente oder auch nur auf bestimmte Dienste einer Komponente
- die Wartungsfähigkeit einer Anlage oder Komponente. Diese kann z.B. bei Auslaufen eines Servicevertrags global entzogen werden
- durch den Workflow bestimmte Rechte: Der Workflow ist kundenspezifisch und kann z.B. ein geöffnetes Wartungsticket durch einen Kunden voraussetzen

Erst wenn alle Punkte zutreffen, ist ein Zugriff eines Technikers auf eine Anlage oder Komponente möglich. Je nach implementiertem Workflow kann also die Vergabe einer Fernwartungsberechtigung letztlich beim Endkunden liegen („Schlüsselschalter“).

Daneben können kundenspezische Firewall- oder Routingregeln aktiv sein, die mögliche Verbindungen noch weiter beschränken.

Gateway Sicherheit

Die Remote Service Gateways (RSGW), die als VPN Endpunkte in die Anlagen integriert werden, müssen einen sehr hohen Selbstschutz bieten, da sie weltweit unbeaufsichtigt betrieben werden und Missbrauch nicht ausgeschlossen werden kann.

Daher sind alle Gateways vollverschlüsselt nach dem AES-256 Standard:

- Die RSGW Hardware besteht aus einem Embedded-Board mit vollständig verschlüsseltem BIOS auf Flash-ROM
- Das verschlüsselte BIOS lädt das Betriebssystem von einer ebenfalls vollständig verschlüsselten CF-Karte als Massenspeicher.
- Das RSGW Betriebssystem prüft die Hardware Platform und startet nur auf RSGW Hardware

Ein Zugriff auf die RSGWs ist per Web-Frontend (HTTPS) und optional SSH möglich. Beides kann bei Sicherheitsbedenken ohne Einfluss auf den Betrieb deaktiviert werden.

Der Zugriff per SSH ist zusätzlich abgesichert: Erlaubt ist zunächst nur das Aufspielen einer Konfiguration per SCP. Die Authentisierung erfolgt per RSA Schlüssel. Optional ist der Zugriff auf eine eingeschränkte Kommandozeile möglich. Erlaubt sind hier nur spezielle Befehle mit ausgesuchten Argumenten. Der Zugang kann hier nach Kundenvorgabe über Passwort oder RSA Schlüssel erfolgen.

Über den CRSM Server ist es möglich, anlagenspezifische Firewall- und Routing-Einstellungen auf den RSGW zu übertragen. Somit ist eine sehr weitgehende Kontrolle über alle Kommunikationsströme einer Anlage möglich.