RED DA: Vorgehensweise beim Risk Assessment

Ob Sie nun als Hersteller die RED DA Compliance durch eine Selbsterklärung dokumentieren, weil Sie mit ihrem Funk-basierten Produkt einen harmonisierten EN 18031-Standard vollumfänglich erfüllen oder ob Sie die Dienstleistung einer benannten Stelle zur Konformitätsbewertung nutzen, es ist in jedem Fall eine umfassende Risikobewertung (Risk Assessment) erforderlich. Dabei muss man häufig auch eine Lösung für völlig unsichere Kommunikationsbeziehungen finden.

Davon gibt es z. B. in der vernetzten industriellen Automatisierungstechnik sehr viele. Ein Beispiel ist Modbus TCP. Dieses Protokoll wird sogar in unzähligen Energieanlagen (also auch in „kritischer Infrastruktur“) nach wie vor sehr gerne genutzt. Daran ändert auch der wirklich hervorragende „Secure by Demand“-Leitfaden für Operational Technology (OT)-Betreiber der US-Cybersicherheitsbehörde CISA erst einmal nichts [1].

Man kann im Rahmen des Risk Assessment in einem solchen Fall wohl nur von der Annahme ausgehen, dass geeignete physische oder logische Maßnahmen in der Zielbetriebsumgebung einer Funkanlage den Zugang entsprechend koordinieren und nur autorisierte Entitäten einen Zutritt haben (bei einer Wireless-Modbus-Lösung hilft das allerdings auch nur teilweise).

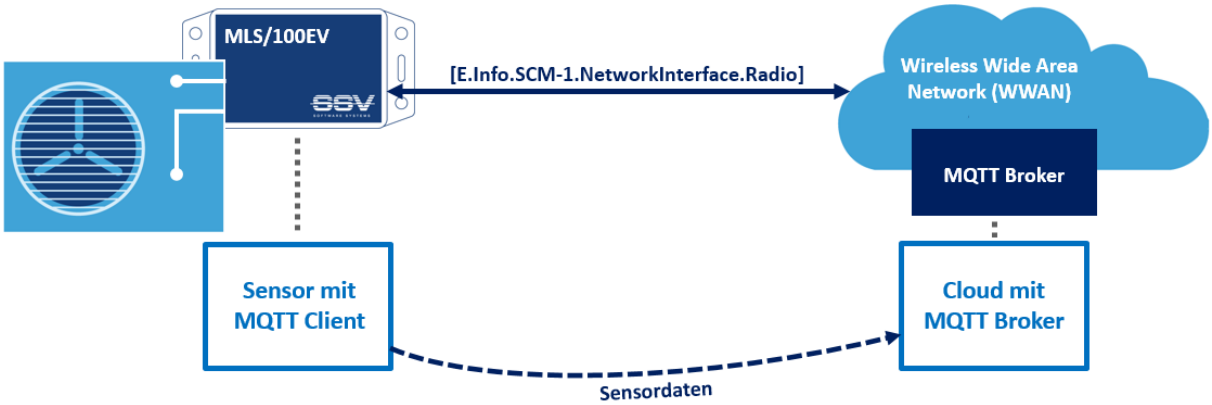

Abbildung 1: In einem ersten Schritt werden die Internet-basierten Funkverbindungen ermittelt und visualisiert. In diesem Beispiel existiert nur die (WWAN) LTE-M-basierte Mobilfunkkommunikation des MLS/100EV, um die jeweiligen Softsensor-Zielgrößen per MQTT an einen Broker zu übertragen. Für diese Datenverbindung ist eine dem Stand der Technik entsprechende Vertraulichkeit, Authentizität und Integrität sicherzustellen.

Unabhängig von den Altlasten der Praxis: Eine zielführende Vorgehensweise für ein Risk Assessment ist, zunächst einmal alle Kommunikationsbeziehungen einer Funkanlage zum Internet zu identifizieren und in entsprechenden Datenflussdiagrammen zu visualisieren: also z. B. den MQTT-basierten Nutzdatenfluss zu einem Cloud-Server und die automatischen Software-Updates aus der Cloud zum Funk-basierten Produkt. Des Weiteren ist auch für die lokale Benutzerschnittstelle zur Änderung der Konfigurationsdaten ein Datenflussdiagramm hilfreich. Zu jedem einzelnen Datenfluss sollte man dann ein STRIDE-Bedrohungsmodell (Thread Modelling Process, siehe [2]) anfertigen.

Abschließend fasst man das Ergebnis in einer Tabelle zusammen (siehe Tabelle 1). Dabei werden jedem Datenfluss die erkannten Bedrohungen und die möglichen Auswirkungen zugeordnet. Zusätzlich bewertet man die Eintrittswahrscheinlichkeit der Bedrohung und das jeweilige Risiko in der Praxis. Abschließend wird für jede Bedrohung eine geeignete Gegenmaßnahme bestimmt. So lassen sich z. B. die Bedrohungen „Man-in-the-Middle, Abhören, Spoofing“ für eine MQTT-Sensordatenübertragung in die Cloud durch den Einsatz einer TLS-basierten Verbindung mit Zertifikat und Server-Authentifizierung sehr deutlich abmildern.

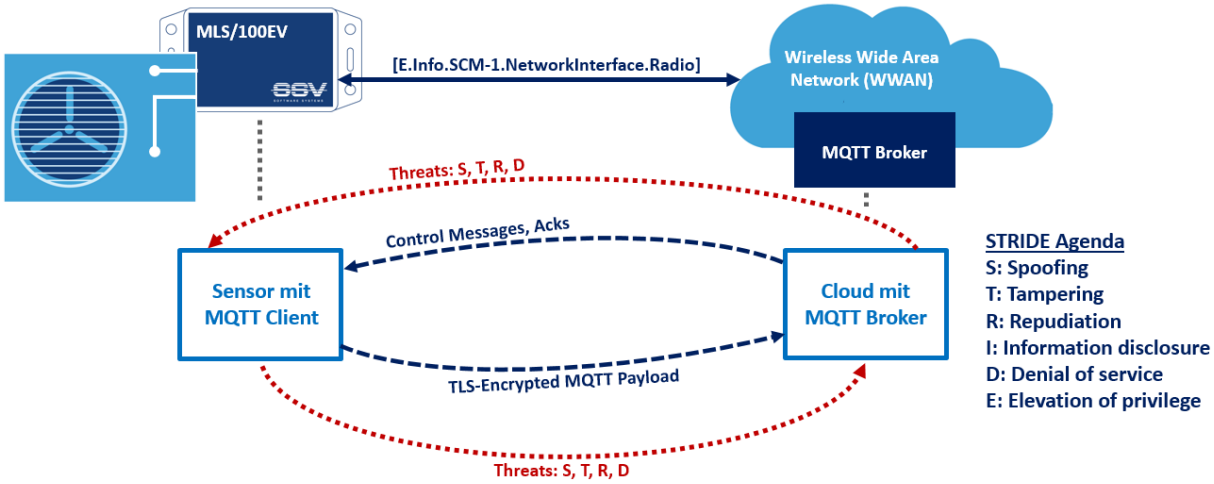

Abbildung 2: Mit Hilfe des STRIDE-Bedrohungsmodells werden einzelne Cybersicherheitsrisiken für die MQTT-Sensordatenübertragung identifiziert. Dafür wird im Rahmen einer Bedrohungsanalyse jede einzelne Kommunikationsbeziehung aus der Perspektive eines möglichen Cyberangreifers betrachtet.

Übrig bleiben in der Regel ein paar Dinge, gegen die es keinen wirkungsvollen Schutz gibt. Beispielsweise der Jamming-Angriff auf einen Funkkanal. Damit muss man leben können. Am Ende der Attacke sollte die betreffende Funkanlage aber ohne menschliches Einwirken wieder den Normalbetrieb aufnehmen.

ID	Funktion	Bedrohung	Auswirkung	Wahrscheinlichkeit	Risiko	Maßnahme(n)
1	MQTT-Kommunikation mit Broker.	Man-in-the-Middle, Abhören, Spoofing.	Falsche bzw. nicht vertrauenswürdige Sensordaten.	Mittel	Hoch	TLS-Einsatz mit Zertifikat und Server-Authentifizierung. Modem-IMEI als Geräte-Identifier (Geräte-ID).
2	Funktion des Firmware-Update.	Einschleusen manipulierter Software.	Systemübernahme durch Dritte.	Hoch	Hoch	Gerät wird in zutrittsgesicherter Profi-Umgebung betrieben. Update nur durch Experten vor Ort möglich. Image-Signatur wg. Secure Boot notwendig.
3	Geräteidentität	Geräte-Cloning. Daten-Spoofing durch Geräte-Clone. Entwenden der SIM-Karte.	Vortäuschen falscher Identitäten, Verbreiten von Fake-Daten.	Niedrig	Mittel	Als Geräte-ID wird die IMEI des internen Mobilfunkmodems genutzt. Da sich das Gerät in einer zutrittsgesicherten Profi-Umgebung befindet, ist die IMEI/SIM-Karte nur mit sehr großem Aufwand auslesbar bzw. entfernbar.
4	Cloud-Anbindung	Datenmanipulation durch Spoofing.	Fehlverhalten der Gesamtlösung.	Hoch	Hoch	TLS-basierte Cloud-Verbindung. In der Hardware verankerte Geräte-ID.
5	Verfügbarkeit der Internet-Verbindung.	Jamming, DoS-Angriff.	Funktion der Gesamtlösung gestört.	Mittel	Mittel	Frequenzbandüberwachung durch Mobilfunkbetreiber. Automatisches Geräte-Recovering durch Watchdog.

Tabelle 1: Übersicht der Ergebnisse zum MLS/100EV-Risk Assessment. Aus dem RED DA-Blickwinkel trifft auf einen MLS/100EV der Artikel 3.3 (d) zu. Daher muss die Fragestellung „Wie stelle ich sicher, dass von dieser Funkanlage keine Schäden im Internet verursacht werden?“ lauten (also beispielsweise durch die missbräuchliche Nutzung der MLS/100EV-Ressourcen durch eine Botnet-Firmware).

Externe Quellen

[1] Link zum „Secure by Demand“-Leitfaden der CISA: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Secure_by_demand_OT_250116.html

[2] Link zum „OWASP Thread Modelling Process”: https://owasp.org/www-community/Threat_Modeling_Process