

# Lessons Learned aus einem Industrie-4.0-Security-PoC

«Industrie 4.0» ist ein Buzzword, das mit grossen Erwartungen, aber auch mit Unsicherheit aufgeladen ist. Ein Proof of Concept (PoC) für den Einsatz eines modernen VPN-Protokolls auf Industriesteuerungen zeigt die konkreten Chancen und Hürden in spezifischen Einsatzszenarien.



Wireguard ist ein modernes Open-Source-VPN-Protokoll mit steigender Adaption in der IT. Dies führt in einer zunehmend digitalisierten Industrie zur Frage, ob sein Reifegrad eine Anwendung in der Industrie zulässt und ein mittelfristiger Wechsel sinnvoll wäre. Aufbau und Ziele unseres PoC leiteten sich auf einem konkreten Anwendungsszenario wie folgt ab: Das VPN-Protokoll soll direkt auf einer Industriesteuerung eingesetzt werden, mit minimalen Infrastruktur-Abhängigkeiten. Erfolgskriterium war der sichere, stabile und einfache Remote-Zugriff auf die Steuerung über LTE.

Bei der ersten PoC-Durchführung kam es zu Stabilitätsproblemen bei der Verbindung. Diese konnten mit der Anpassung von Offloading-Funktionen der Netzschnittstelle im Betriebssystem behoben werden. Die zweite Iteration war mit Änderungen an Architektur und Aufbau des VPNs erfolgreich. Eine robuste, sichere Remote-Verbindung auf die Steuerung und Wartungstätigkeiten waren reibungsfrei möglich. Da Wireguard auf OSI Layer 3 ansetzt, waren Discovery-Funktionen basierend auf OSI Layer 2 wie vorhergesehen in dieser Konfiguration nicht mehr einsetzbar.

Da der PoC einen scharf definierten Scope mit viel Umsetzungsfreiheit hatte, muss nun Rücksicht auf Business,

Architektur und Anforderungen aus dem Betrieb genommen werden. Die Wahl eines sicheren Kommunikationsprotokolls ist dabei nur ein Aspekt von wesentlich umfassenderen Überlegungen. Generell verlangt die Einführung neuer Technologien und Geschäftsanwendungen Anpassungen bei den technischen Kompetenzen im Betrieb. Dies muss in den Prozessen der Organisation berücksichtigt werden, insbesondere bei der Sicherheitsorganisation von Unternehmen, da traditionelle Schutzmechanismen wie die Netzisolation durch Industrie 4.0 immer praxisuntauglicher werden.

« Industrie 4.0 ist die Chance, prozessual und organisatorisch standardisiert vorzugehen. »

In allen Fällen ist es vorteilhaft, auf bestehende Standards wie die ISA/IEC 62443, die ISO-27000-Serie, die NISTIR 8228, den Schweizer IKT-Minimalstandard oder dessen Branchenstandards zurückzugreifen. Die Auswahl sollte bezüglich der Anforderungen und der zu definierenden Massnahmen möglichst spezifisch ausfallen und im Unternehmen bestehende Standards berücksichtigen.

Ein PoC prüft immer die Machbarkeit innerhalb von Businessvorgaben, technischen Limitationen und Security. Die zunehmende Verschränkung von Funktionen, die Industrie 4.0 mit sich bringt, erweitert den Kreis der Stakeholder, die in den zunehmend länger werdenden Lieferketten zu verorten sind. Lifecycles von Systemen müssen nun miteinander abgestimmt sein, geteilte Infrastruktur und «Ownership» können bei der Definition, Finanzierung und Umsetzung von Sicherheitsmassnahmen unvorhergesehene Hürden bergen.

Industrie 4.0 ist ein grosses Buzzword. Es ist aber auch die Chance, prozessual und organisatorisch standardisiert und von Grund auf vorzugehen. Man soll sich daher seiner Ziele, dem Anwendungsfall und den Businessaspekten bewusst sein, damit die eine Sache richtig, nicht mehrere halb umgesetzt werden.

