Schwachstellen-Management in der OT BKW Power Grid

Studiengang: MAS Cyber Security

Ein Konzept für das Schwachstellen-Management mit Scannern im industriellen Netzwerk (OT) der BKW Power Grid wurde unter der Berücksichtigung der Anforderungen für kritische Infrastrukturen entwickelt. Dabei ist ein Testaufbau mit Tenable-Produkten realisiert worden. Dieses Konzept wird in den nächsten Monaten umgesetzt und so die Cybersicherheit dieser kritischen OT-Infrastruktur erhöhen.

Ausganglage

Die Problematik des Schwachstellen-Scanning in der OT der BKW Power Grid besteht darin, dass die OT-Infrastruktur mit sehr vielen Zonen in verschiedenen Purdue-Levels aufgebaut ist und sich gewisse Geräte während des Scans blockieren können. Grundsätzlich findet sich wenig Literatur und Software für diese Thematik in der OT.

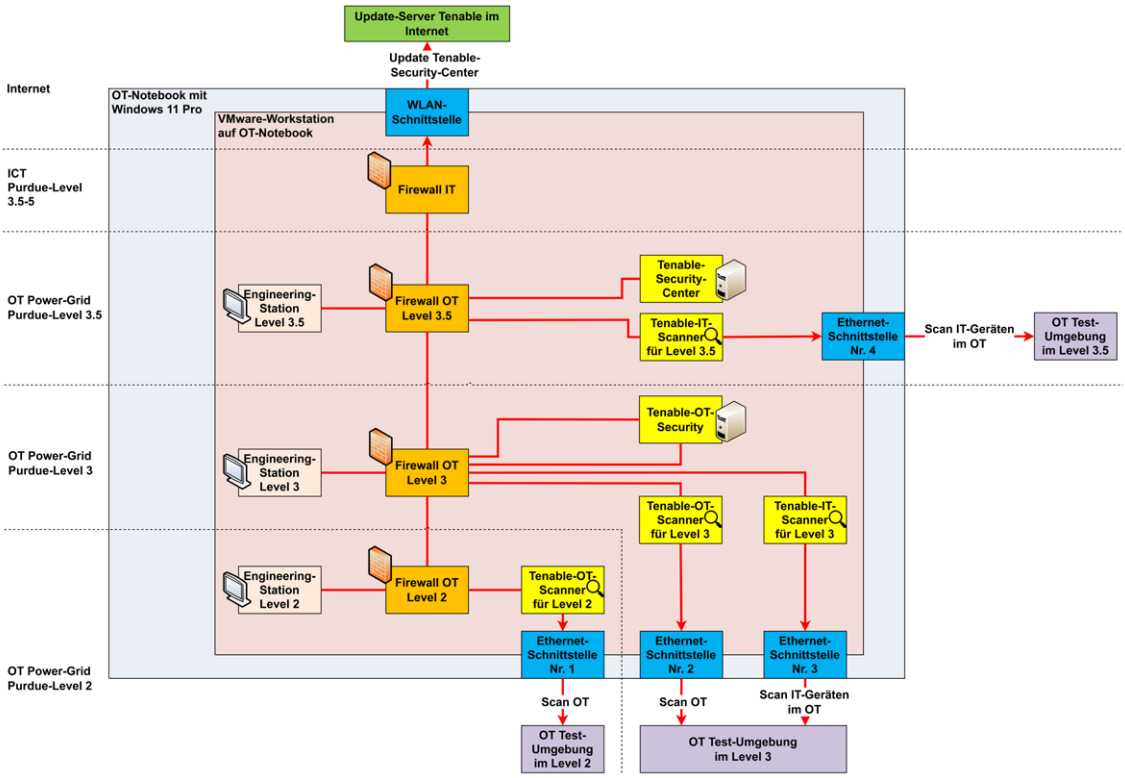
Vorgehen

Zuerst erfolgte die Auflistung der Geräte-Typen mit Scanfreigabe oder Verbot und die Analyse des Markts von OT-Schwachstellen-Software. Danach ist ein entsprechendes Konzept für das Scanning erstellt worden. In der OT-Testumgebung wurde dann ein Test mit einem Schwachstellen-Manager und vier Scannern aufgebaut und durchgeführt.

Ergebnisse

Das Konzept und der Testaufbau haben die Komplexität des Scans in der OT aufgezeigt. Die Geräte antworten mit zu wenig Informationen auf die Anfragen mit den IT-Protokollen, auch haben die Abfragen mit den OT-Protokollen, die durch Reverse-Engineering im OT-Scanner implementiert worden sind, nicht immer funktioniert. Zudem dürfen die meisten OT-Geräte, auf Grund von Betriebsrisiken oder Herstellerverbot, nicht in der produktiven Umgebung gescannt werden.

Rénald Marmet
renald@marmet.li



Konzept Testaufbau