ERGEBNISSE DER SICHERHEITSBEWERTUNG

IN SCHALTANLAGEN UND KRAFTWERKEN

Unser Experte erzählt, welche Risiken weltweit häufig auftreten

Über den Autor

Ozan Dayanç ist OT Security Engineer, Product Specialist und Mitarbeiter des Technischen Supports bei OMICRON. Zu seinen Aufgaben gehört die Bewertung von OT-Netzwerken weltweit. Hier berichtet er von seinen Erfahrungen beim Schutz von Netzwerken zur Automatisierung von Energieanlagen.

Ende 2020 meldete sich eine Kollegin bei mir und bat mich, mit unserem Angriffsüberwachungssystem (IDS) StationGuard einen Sicherheitsbewertungsbericht für eine:n unserer Kund:innen zu erstellen. Ich bekam vom Unternehmen entsprechende Engineering-Dateien und wurde über dessen Netzwerkarchitektur informiert. Diese Unterlagen bilden die konventionelle Grundlage für jede Sicherheitsbewertung, bevor meine Kolleg:innen und ich unsere Prüfung vor Ort fortsetzen.

Die Daten meiner ersten Sicherheitsbewertung haben sowohl für die Schaltanlagentechniker:innen als auch für die IT-Spezialist:innen völlig unerwartete Ergebnisse erbracht. Zu den Risiken, die unsere Bewertung zutage

gefördert hatte, gehörten mehrere unbemerkt gebliebene Verbindungen nach draußen, unerwartete Geräte im Netzwerk, veraltete Firmware, fehlgeschlagene RTU-Operationen, Konfigurationsfehler und Probleme mit dem Netzwerk und seinem Redundanzprotokoll (RSTP).

Seitdem haben wir weltweit viele Sicherheitsbewertungen durchgeführt (und Verbesserungen daran vorgenommen), und zwar nicht nur für Schaltanlagen, sondern auch für Kraftwerke und Control Center, darunter Anlagen mit IEC 61850-, IEC 608705104-, DNP3-, Modbus TCP/IP und vielen anderen IT-Protokollen.

Die Ergebnisse unserer Sicherheitsbewertungen waren immer interessant, manchmal aber auch alarmierend. Im Folgenden gehe ich auf einige häufig auftretende Risiken ein, die mir in den letzten Jahren begegnet sind:

Sie interessieren sich für unsere Sicherheitsbewertungen? Dann scannen Sie den Code oder schreiben Sie uns an

✉ info.puc@omicronenergy.com

VERALTETE FIRMWARE

mit bekannten Sicherheitslücken

26 Updates verfügbar

Bei jeder Sicherheitsbewertung stoße ich auf veraltete Firmware-Versionen. Im Rahmen unserer Bewertungen übergeben wir den Techniker:innen und IT-Expert:innen des Unternehmens ein passiv ermitteltes Bestandsverzeichnis. Wir ergänzen die Angaben zum Bestand um weitere Details, wie die Software-Version, die Hardware-Konfiguration und Seriennummern, indem wir Engineering-Dateien importieren.

Dieses Bestandsverzeichnis stellt eine solide Basis für die Analyse der Schwachstellen und Risiken dar.

EXTERNE VERBINDUNGEN

Kraftwerke und Control Center mit Remote-Verbindungen zum IT-Netzwerk des Unternehmens sind für einen Cyberangriff immer am anfälligsten. Bei der Bewertung des Netzwerks einer Schaltanlage in Südamerika stellten wir die Aktivität mehrerer Clients mit externen IP-Adressen fest. Das Unternehmen hatte seinen Techniker:innen erlaubt, sich über eine Remote-Verbindung (VPN-Tunnel) von zu Hause aus mit den IEDs zu verbinden und sie zu konfigurieren. Viele Funde beunruhigten die Verantwortlichen für die IT-Sicherheit. Einer davon waren eine IP-Adresse und eine MAC-Adresse, die niemand im Team kannte und die auch nirgends dokumentiert waren. Wir konnten die IP-Adresse zurückverfolgen und herausfinden, woher diese Verbindung stammte. Das ermöglichte es uns, ihren Zugriff auf das System zu blockieren. Achten Sie genauer auf potenzielle Sicherheitsrisiken, indem Sie alle Verbindungen in Ihrem Netzwerk sichtbar machen.

NICHT GENUTZTE DIENSTE

Offene/unbenutzte Dienste bieten unverhältnismäßig viele Möglichkeiten für Hacker, Automatisierungs- oder Leittechniksysteme anzugreifen. Glücklicherweise lassen sich diese ungenutzten Dienste durch Netzwerküberwachung leicht erkennen. Zu den ungenutzten Diensten, die wir bei unseren Bewertungen am häufigsten antreffen, gehören die folgenden:

- IPv6: Das Protokoll war auf den meisten PCs aktiviert, manchmal aber auch auf IEDs. IPv6 wurde nie wirklich genutzt, bot aber verschiedene Angriffsvektoren im Netzwerk.
- Windows-Dateifreigabe: Der Dateifreigabedienst war auf PCs und Windows-basierten RTUs und Gateways immer aktiviert, wurde aber nicht genutzt.
- PTPv2: Dieses Protokoll war standardmäßig auf einigen industriellen Switches aktiviert, wurde aber fast nie genutzt.

Allein durch Deaktivieren dieser Dienste lässt sich die Zahl der Cyberrisiken für die Geräte im Netzwerk deutlich senken.

ERKENNEN VON ÄNDERUNGEN AN DER KONFIGURATION

In einer Schaltanlage in den USA stellten wir eine Fehlkonfiguration bei den GOOSE-Nachrichten fest. Zu diesem Problem war es gekommen, weil die Geräte von zwei verschiedenen Engineering-Stellen konfiguriert worden waren. Die fehlende Absprache zwischen den Techniker:innen hatte Kommunikationsprobleme zwischen den OT-Geräten zur Folge. Wir fanden heraus, dass bestimmte Remote-Befehlsaktivitäten in der Schaltanlage aufgrund ungültiger Verriegelungsbedingungen nicht richtig funktionierten. Die Konsequenz war, dass es in dringenden Fällen nicht möglich gewesen wäre, die Schaltgeräte aus der Ferne zu bedienen. Das hat mir gezeigt, wie solche kleinen Probleme in der GOOSE-Kommunikation zu größeren Problemen für das Kraftwerk führen können. Aus diesem Grund und um unser Wissen zu erweitern und mit anderen Kraftwerken, Schaltanlagen und Control Centern in Kontakt zu kommen, bieten wir diese Sicherheitsbewertungen weiter kostenlos an.

FEHLER IN DER KONFIGURATION DER LEITTECHNIK-KOMMUNIKATION

Falsch konfigurierte RTU- und Leittechnikgeräte können die Kommunikation verlangsamen und dazu führen, dass bei kritischen Vor-Ort-Ereignissen Übertragungen fehlschlagen. Ich erinnere mich an einen Fall in einer Schaltanlage in Europa, wo die MMS-Reports wegen eines Konfigurationsfehlers an die falsche Client-IP-Adresse gesendet wurden. Durch die Behebung dieses Fehlers konnte die Kommunikationsgeschwindigkeit der IEDs messbar verbessert werden.

Die Untersuchung von Verzögerungen bei der Kommunikation reduziert das operative Risiko behinderter Reaktionsprozesse.

DIE HÄUFIGSTEN SICHERHEITSRISIKEN

in Netzwerken von Kraftwerken

Nicht dokumentierte externe Verbindungen, die direkt auf IEDs und Switches zugreifen
Veraltete Firmware mit bekannten Sicherheitslücken
Nicht genutzte Dienste
Nicht autorisierte Zugriffe

Normalerweise werden diese Sicherheitsprobleme durch funktionale Probleme begünstigt, wie z. B.

Konfigurationsprobleme in IEDs, RTUs und Netzwerk-Switches
Fehler bei der Zeitsynchronisation
Probleme mit der Netzwerkredundanz