DESIGN UND INBETRIEBNAHME EINER SICHEREN ARCHITEKTUR FÜR ANLAGENNETZWERKE

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1] OMICRON electronics GmbH, Klaus, Österreich (andreas.klien@omicronenergy.com)
[2] Centralschweizer Kraftwerke (CKW) AG, Luzern, Schweiz (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Luzern, Schweiz (stefan.mattmann@ckw.ch)

Suchwörter: CYBER-SECURITY, IEC 61850, ANGRIFFSERKENNUNG, ANLAGENAUTOMATISIERUNG

Zusammenfassung

Für immer mehr Versorgungsunternehmen und Cyber-Security-Auditoren ist nicht nur die Leitstelle ein kritischer Angriffsvektor, sondern sie betrachten auch Schaltanlagen als potenziellen Eintrittspunkt für Cyberangriffe auf das Stromnetz. Wichtige Risikofaktoren dabei sind die Prozesse, die Art und Weise, wie die Wartung der Schutz- und Leittechnik erfolgt und wie der Fernwartungszugriff realisiert ist. Daher ist es erforderlich, die Cyber-Security der Sekundärtechnik zu prüfen. Zu diesem Zweck startete der Schweizer Energieversorger Centralschweizer Kraftwerke AG (CKW) 2016/2017 ein Projekt zur Entwicklung einer neuen Referenzarchitektur für seine Sekundärtechnik. Das Design der CKW begegnet diesen Angriffsvektoren mit entsprechenden Gegenmaßnahmen, bietet aber trotzdem ein vernünftiges Gleichgewicht zwischen Wartbarkeit und Sicherheit. Es enthält mehrere Sicherheitsebenen, darunter auch mehrere Firewall-Zonen. Außerdem kommt ein Intrusion Detection System (IDS) zum Einsatz. Die Auswahl eines geeigneten IDS für Anlagen hat sich als nicht ganz einfach erwiesen, da viele IDS die Anforderungen von Anlagennetzwerken nicht unterstützen. In diesem Artikel werden zunächst die für Anlagen wichtigsten Angriffsvektoren angeführt; daran schließt sich eine Beschreibung der Sicherheitsarchitektur an, die erstmalig in einem neu errichteten 110-kV-Anlagenprojekt der CKW implementiert wurde. Der Artikel schließt mit den Erfahrungen, die bei der Auswahl eines geeigneten IDS für Anlagen gemacht wurden, und den Lehren, die aus der Werksabnahmeprüfung dieses Projekts gezogen wurden.

1. Einführung

1.1. Angriffsvektoren bei Anlagen

Für den Rest dieses Artikels definieren wir den Begriff „Cyberangriff“ als ein Ereignis, bei dem ein Gegner den Dienst von mindestens einem Schutz-, Automatisierungs- oder Steuergerät in der Anlage ändert oder deaktiviert oder dessen Funktion beeinträchtigt. Um dies zu erreichen, kann ein Angreifer einen der in Bild 1 dargestellten Angriffswege nutzen [1].

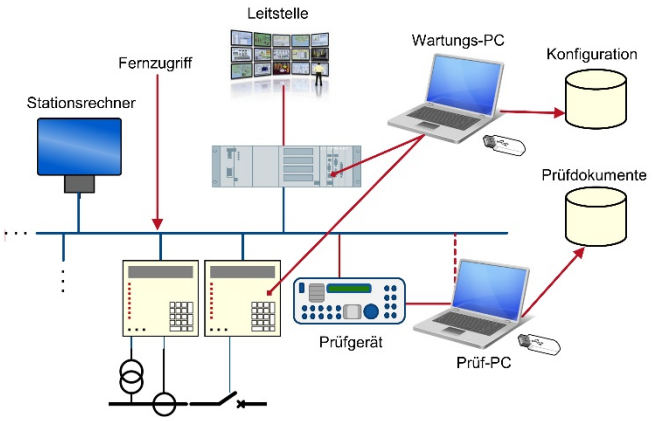

Bild. 1: Angriffsvektoren von Schaltanlagen [1]

Ein Angreifer könnte über die Leitstellenverbindung (**A**) eindringen, so wie es beim ersten Cyberangriff auf das Stromnetz der Ukraine passiert ist, bei dem die Firmware von Gateway-Geräten verändert wurde (wodurch die betreffenden Geräte zerstört wurden) [2], oder er könnte über eine Remote-Access-Verbindung (**B**) eindringen, wie es 2016 beim zweiten Cyberangriff in der Ukraine [3] und beim TRITON-Cyberangriff auf kritische Infrastruktur-PLCs [4] der Fall war.

Einen weiteren Eintrittspunkt stellen die Engineering-PCs (**C**) dar, die entweder direkt an die Anlagenausrüstung oder an das Anlagennetzwerk angeschlossen sind. Verbindet ein Schutztechniker seinen Computer mit einem Relais, um die Parametrierung zu ändern, könnte Malware auf dem PC wiederum Malware auf dem Relais installieren, wie es etwa beim berühmten Stuxnet-Cyberangriff 2010 mit SPS-Steuerungen geschehen ist [5].

Für die Prüfung von IEC-61850-Systemen verwendete Laptops (**D**) werden oft direkt an den Anlagenbus angeschlossen, was ebenfalls als

potenzielle Möglichkeit für das Infizieren von IEDs gilt. Aus diesem Grund gibt es neue IEC-61850-Prüflösungen, die eine den Standards für Cyber-Security entsprechende Trennung zwischen dem Prüfcomputer und dem Anlagennetzwerk sicherstellen. Somit ist das Prüfgerät selbst (**E**) der einzig verbleibende potenzielle Eintrittspfad. Deshalb müssen Anbieter von Prüfgeräten in die Abhärtung ihrer Geräte investieren, um zu verhindern, dass dieser Eintrittspfad für Angreifer nicht attraktiv ist.
Der Ort, an dem Einstellungen (**F**) und Prüfdokumente (**G**) gespeichert werden, kann ebenfalls eine Infektionsquelle sein. Daher gehört der Standort des Servers oder Speichergeräts ebenfalls zum kritischen Kreis. Er sollte sich nicht in der IT-Zone des Büros befinden. Aus diesem Grund ist es sinnvoll, für diese Daten eine getrennte, isolierte und geschützte Datenmanagementlösung einzuführen.

2. Vorschlag für eine neue Anlagenarchitektur

2.1. Was ist der aktuelle Stand bei der OT-Cyber-Security?

Die Arbeitsgruppe zur Sicherheit in der Operational Technology (OT) des Verbandes Schweizerischer Elektrizitätsunternehmen (VSE) hat unter dem Titel „Handbuch Grundschutz für Operational Technology in der Stromversorgung“ ein Dokument mit Empfehlungen für die Branche veröffentlicht. Dieses Handbuch verweist auf das „Cyber Security Framework for Critical Infrastructure“ des US-amerikanischen National Institute of Standards (NIST) [7], das ständig angepasst und verbessert wird (die neueste aktualisierte Fassung stammt aus dem Jahr 2018). Das NIST-Framework basiert auf der Annahme, dass es nie einen hundertprozentigen Schutz vor Cyberangriffen geben wird. Mit genügend Wissen und Mühe können alle Sicherheitsmaßnahmen ausgehebelt werden. Darauf aufbauend empfiehlt das NIST-Framework einen Prozess, der sich aus diesen fünf Schritten zusammensetzt: „Identifizieren“, „Schützen“, „Erkennen“, „Reagieren“ „Wiederherstellen“. Wie bereits im vorherigen Abschnitt dieses Artikels ausgeführt, besteht der erste Schritt daher in der Identifizierung von Angriffsvektoren (Schritt „Identifizieren“). Anschließend können im nächsten Schritt Gegenmaßnahmen implementiert werden (Schritt „Schützen“). Wenn es einem Angreifer dennoch gelingt, diese Hürden zu überwinden, muss der Angriff erkannt (Schritt „Erkennen“) und bestenfalls sofort bekämpft werden (Schritt „Reagieren“), um schnellstmöglich den Normalzustand wiederherzustellen (Schritt „Wiederherstellen“). Anhand der Lehren, die in den Schritten „Erkennen“ und „Reagieren“ gezogen werden, können neue Angriffsvektoren identifiziert und neue Gegenmaßnahmen implementiert werden, bevor der ganze Prozess von vorn beginnt.

Die VSE-Empfehlung legt großen Wert auf das Zusammenwirken von Mensch, Technologie und Prozessen innerhalb der Organisation. So ist beispielsweise eine fortlaufende Überwachung oder eine kontinuierliche Angriffserkennung (Schritt „Erkennen“) nur sinnvoll, wenn auf Alarmmeldungen angemessen reagiert wird. Dazu ist es erforderlich, dass die Alarmmeldungen für alle am Reaktionsprozess Beteiligten, also sowohl die OT-Techniker als auch die IT-Sicherheitsspezialisten, verständlich sind. Anderenfalls wird der Reaktionsprozess ineffizient. Außerdem ist Fakt: Wenn das IDS zu viele falsche Alarme liefert, werden schlussendlich alle Alarme ignoriert.

2.2. Initiativen zur OT-Cyber-Security bei CKW [6]

Das Thema OT-Sicherheit – insbesondere was die Steuerungs- und Schutzsysteme angeht – ist für die CKW in den letzten Jahren immer wichtiger geworden. Der Grund dafür waren die erwähnten Branchenempfehlungen in der Schweiz und vor allem auch die von den CKW in den vergangenen Jahren vorgenommenen Bewertungen der OT-Sicherheit ihrer Anlagen. Diese Bewertungen haben Schwachpunkte sowohl in den Netzwerken als auch in der Steuerungstechnologie aufgezeigt, die in den Anlagen verwendet wird. So wurden beispielsweise unsichere Zonenübergänge und einige kritische Methoden für den Fernzugriff auf die Steuerungscomputer in den Anlagen gefunden. Darüber hinaus war es nicht möglich zu beurteilen, ob im Anlagennetzwerk gerade ein Angriff stattfindet oder ob es im Netzwerk verdächtige Aktivitäten gibt, die auf einen drohenden Angriff hindeuten könnten.

Die CKW haben diese Erkenntnisse zum Anlass genommen, sich selbst das Ziel zu setzen, die essenziellen Schwachpunkte zu eliminieren und die Anforderungen an die zukünftige Anlagenarchitektur zu verschärfen. Daher wurden diese Erkenntnisse in den neuen Designstandard der CKW für die Sekundärtechnik integriert.
Neben der Arbeit an diesem Designstandard konnte die CKW sich auch aktiv in die Arbeit der VSE-Arbeitsgruppe für das erwähnte Handbuch zur OT-Sicherheit einbringen. Durch diesen Informationsaustausch konnten sie die Erkenntnisse aus der Arbeitsgruppe kontinuierlich in den eigenen Designstandard einfließen lassen.

2016/2017 begann ein Projektteam der CKW mit der Planung der neuen Unterstation (US) Rothenburg, die 2020 in Betrieb gehen wird. Bei diesem Projekt kamen der neue Standard der CKW für eine sichere Architektur und die neuesten Empfehlungen aus dem Handbuch zur OT-Sicherheit zur Anwendung. Um diese neuen und tiefgreifenden Sicherheitsmaßnahmen umsetzen zu können, entschieden sich die CKW, die Netzwerkarchitektur und die Switch-Konfiguration selbst zu implementieren.

2.3. Netzwerkdesign

Im Netzwerkdesign der Unterstation (US) Rothenburg wurden in jeden Bereich Hürden eingebaut, um Angreifern das Leben so schwer wie möglich zu machen. Bild 2 zeigt das Netzwerk der US Rothenburg.

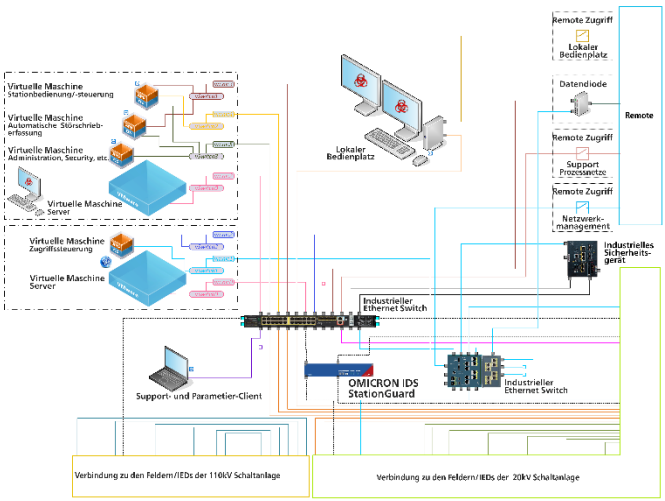

Bild 2: Netzwerkarchitektur der US Rothenburg [6]

In dieser Architektur werden alle in Abschnitt 1.1 dieses Artikels beschriebenen Angriffsvektoren angegangen, wobei eine ganze Palette von Sicherheitsmaßnahmen zum Einsatz kommt Die Fernverbindungen der Anlage hatten bei der Absicherung die höchste Priorität. Diese Fernverbindungen werden nicht nur durch Firewalls und Tunnellösungen gesichert, sondern sie sind auch standardmäßig deaktiviert. Verbindungen für den Fernzugriff werden nur dann aktiviert, wenn es nötig ist. Das bedeutet, dass für die Aktivierung des Fernzugriffs mehrere Personen benötigt werden, was dem Prozess einer Zwei-Faktor-Authentifizierung ähnelt.

Die Kommunikation mit der Leitstelle erfolgt über das serielle Protokoll nach IEC 60870-5-101. Der Zugriff auf die Anlagengeräte zu Wartungszwecken erfolgt immer ausschließlich über spezielle Arbeitsstationen, die speziell gesichert sind. Diese Arbeitsstationen sind virtualisiert und an einem zentralen Standort untergebracht. Dieser Fernzugriff für die Wartung muss ebenfalls aus der Ferne aktiviert werden.

Die Leittechnik, das Störschreibererfassungssystem sowie das Sicherheitssystem werden virtualisiert und auf einem lokalen Host-Computer in der Anlage betrieben. Selbst die lokale HMI-Station greift nur über eine Remote-Desktop-Verbindung und eine zusätzliche lokale Firewall auf diese Systeme zu. Es wird mit rollenbasierter Zugriffssteuerung (Role-Based Access Control, RBAC) gearbeitet. Das bedeutet, dass es nicht ein Passwort pro Gerät, sondern ein Passwort pro Benutzer gibt. Der Vorteil dabei ist, dass ein Techniker für alle Anlagen nur ein Passwort, nämlich sein eigenes, benötigt. Wenn ein Mitarbeiter das Unternehmen verlässt, reicht es, dessen Benutzernamen zu entfernen – das Ändern von Passwörtern ist nicht nötig. Diese Benutzerverwaltung wird mithilfe eines zentralen Active-Directory(AD)-Servers und eines lokalen RADIUS-Servers in der Anlage implementiert. Benutzer müssen sich über das AD anmelden, das ihm die notwendigen Berechtigungen zuweist. Wenn nötig, kann der Zugriff auf das zentrale AD von einem zentralen Standort aus aktiviert werden. Außerdem müssen sich die Benutzer bei jedem IED mit einem eigenen Benutzernamen und einem eigenen Passwort anmelden. Die IEDs nutzen dabei

den lokalen RADIUS-Server, um die Authentifizierung des Benutzers und das Passwort zu überprüfen und um die diesem Benutzer zugewiesenen Berechtigungen abzurufen. Dies gilt sowohl für den Zugriff auf die Geräte mit den Hersteller-Tools als auch für die Bedienung auf dem IED-Display. Dabei werden keine Standardpasswörter verwendet.

Alle mit dem Anlagennetzwerk verbundenen PCs sind speziell gehärtet. Diese Abhärtung erfolgt unter anderem dadurch, dass die Windows-Firewall entsprechend der Kommunikationsmatrix der Anlage konfiguriert wird. Außerdem werden die Funktionen des Betriebssystems gesperrt, die für die Rolle dieses Clients nicht benötigt werden.
Als zusätzliche Sicherheitsmaßnahme wird die Netzwerkzugriffskontrolle über MAC Authentication Bypass implementiert, was bedeutet, dass nur registrierte Geräte eine Verbindung zum Netzwerk-Switch herstellen können.

Im Falle einer Fehlfunktion muss der Switch auch die Reservegeräte aus dem Bestand erkennen und akzeptieren. In den Netzwerk-Switches der Anlage und in der Firewall werden ACLs (Access Control Lists) konfiguriert, um festzulegen, welches Gerät mit welchem anderen Netzwerkteilnehmer über welches Protokoll und welchen Switch-Port kommunizieren darf.

Das Busnetzwerk der Anlage und das Netzwerk für die Konfiguration und Wartung sind logisch (VLAN) und physisch voneinander getrennt. Das bedeutet, dass auf jedem IED die MMS- und GOOSE-Nachrichten nach IEC 61850 über eine andere Netzwerkschnittstelle als der Wartungszugriff laufen. Außerdem ist das gesamte Anlagenbusnetzwerk segmentiert, wobei u. a. die folgenden Segmente durch die Firewall (ACLs) voneinander getrennt sind:

- 110 kV (GOOSE und MMS)
- 20 kV (GOOSE und MMS)
- lokale HMI-Station
- Protokoll-Gateway
- Nebenanlagen
- Wartungsnetzwerke für IEDs und Clients
- Verwaltungsnetzwerk, VM, RADIUS

Die Kommunikation von der Anlage zu den Netzwerkbereichen höherer Ebene ist zusätzlich durch eine Datendiode gesichert. Diese Datendiode gewährleistet, dass nur ausgehende Kommunikationssitzungen initiiert werden können, und bietet damit eine zusätzliche Sicherheitsschicht. Der gesamte Netzwerkverkehr im System wird durch ein IDS überwacht, das nach dem Whitelist-Prinzip funktioniert: Jeglicher Datenverkehr, der nicht auf der Whitelist steht, erzeugt standardmäßig einen Alarm. Das IDS kann Alarme über die RTU an die Leitstelle und über spezielle Protokolle für die Alarmsignalisierung (Syslog) an ein Security Operation Center (SOC) senden.

3. Angriffserkennung

Die Sicherheitsarchitektur der CKW basiert auf der Einrichtung von Netzwerksegmenten, die jeweils durch die Firewall (ACLs) voneinander getrennt sind. Über die Konfiguration der Firewall ist genau festgelegt, welche Protokolle für die Kommunikation zwischen den Segmenten genutzt werden können. Allerdings können auch die von der Firewall erlaubten Protokolle wie die in IEC 61850 verwendeten Protokolle MMS/GOOSE und anbieterspezifische Engineering-Protokolle dazu genutzt werden, Geräte anzugreifen und sie zu infizieren. In Szenarien wie diesen wollte CKW in der Lage sein, unerlaubte Aktivitäten schnell zu erkennen. Zu diesem Zweck entschied man sich, in der Referenzarchitektur ein IDS vorzusehen.

Um den kritischsten Datenverkehr, also die Kommunikation zwischen dem Gateway und den IEDs analysieren zu können, sollte zumindest der gesamte Verkehr des Protokoll-Gateways zur Analyse in das IDS gespiegelt werden. Die Switches auf Feldebene müssen in der Regel nicht überwacht werden, da von dort typischerweise nur Multicast-Verkehr (GOOSE, Sampled Values) ausgeht. Um sicherzustellen, dass auch der gesamte Unicast-Verkehr in allen Netzwerkzweigen analysiert wird, wird empfohlen, alle Switches in das IDS zu spiegeln.

In der CKW-Architektur ist das IDS mittels Mirror Ports an allen Switches im Netzwerk verbunden. Das bedeutet, dass das IDS den Verkehr auf dem Anlagenbus und auch den von außen eingehenden

Verkehr analysiert, bevor und nachdem dieser die Firewalls passiert hat.

3.1. Anforderungen an ein Schaltanlagen-IDS

Die Auswahl eines für Schaltanlagen geeigneten IDS hat sich als nicht ganz leicht erwiesen. Eine wichtige Anforderung war, dass sich das IDS von den Schutz- und Leittechnikern, die für alle IEDs und die gesamte Netzwerkausrüstung zuständig sind, einfach bedienen lässt. Um die schnelle Reaktion auf Alarme zu ermöglichen, sollte es einfach sein, die IDS-Alarme mit Ereignissen in der Anlage und Ereignisprotokollen im HMI zu verknüpfen. Zu diesem Zweck sollte das IDS statt einfach nur IT-Security-Fachjargon konkrete anlagenbezogene Informationen anzeigen.

Bis vor Kurzem gab es beim IDS nur zwei Hauptansätze: den signaturbasierten und den „lernbasierten" Ansatz.

Beim signaturbasierten Ansatz kommt – wie bei einem Standardvirenscanner für PCs – eine Blacklist zum Einsatz und es wird nach bekannten Viren und Malware gesucht. Das Problem dabei ist, dass es nur eine kleine Zahl von bekannten Cyberangriffen auf Schaltanlagen gibt, aber bereits das erste Auftreten eines neuen Angriffs schwerwiegende Folgen haben könnte. Deshalb muss das IDS Bedrohungen ohne Vorkenntnisse über den Angriff erkennen können.

Das ist der Grund, warum meistens ein „lernbasierter" Ansatz verwendet wird. Das IDS sieht sich generische Protokollparameter der Kommunikation an und „lernt" die Werte und die Häufigkeit der einzelnen Parameter. Auf diese Weise wird sichergestellt, dass im Normalbetrieb ein Alarm ausgelöst wird, sobald die Netzwerkkommunikation deutlich vom gelernten Durchschnitt abweicht. Das Ergebnis ist aber, dass bei allen Ereignissen, die während der Lernphase nicht aufgetreten sind, falsche Alarme ausgelöst werden. Beispielsweise bei Auslöse- und Schaltoperationen oder routinemäßigen Schutzprüfungen kann dies oft der Fall sein. Da das System die Bedeutung der Telegramme im Netzwerk nicht versteht, verweisen die Alarmmeldungen auf generische Protokollparameter wie „MMS confirmed-write-response failed". Das führt zu einer hohen Zahl falscher Alarme, die jeweils von IT-Spezialisten und IEC-61850-Spezialisten geprüft werden müssen. Ein solcher Aufwand im Reaktionsprozess war für CKW nicht hinnehmbar.

3.2. Verwendeter IDS-Ansatz

Bei IEC-61850-Anlagen wird das gesamte Automatisierungssystem mit allen IEDs, ihren Datenmodellen und ihren Kommunikationsmustern in einem standardisierten Format beschrieben – der Substation Configuration Language (SCL). Diese Informationen erlauben einen anderen Ansatz für die Erkennung von Angriffen: Das Überwachungssystem kann ein Systemmodell des Automatisierungssystems der Anlage erstellen und es kann jedes Paket im Netzwerk mit diesem Modell vergleichen. Selbst die in den übertragenen Nachrichten (GOOSE, MMS, SV) enthaltenen Variablen können mit den aus dem Systemmodell abgeleiteten Erwartungen verglichen werden. Damit basiert der Ansatz auf einer Whitelist, weil alle Pakete, die nicht zum Systemmodell passen, einen Alarm auslösen. Die CKW hat sich für ein IDS entschieden, das auf diesem Ansatz beruht – dem StationGuard von OMICRON.

Der Vorteil dieses Ansatzes besteht darin, dass nicht nur Cyber-Security-Bedrohungen, wie fehlerhafte Pakete und unzulässige MMS-Steuerungsvorgänge, sondern auch Kommunikationsfehler sowie Probleme mit der Zeitsynchronisation und damit auch bestimmte Geräteausfälle erkannt und als Alarm gemeldet werden.

Durch die Verwendung des „Substation"-Abschnitts in der SCL-Datei lässt sich automatisch ein Übersichtsdiagramm der Anlage erstellen, in dem dann die Alarme sogar grafisch dargestellt werden können. Solch eine Anzeige kann hilfreich sein, wenn es darum geht zu ermitteln, ob eine Aktion, die einen Alarm ausgelöst hat, mit Absicht durchgeführt wurde: Der Alarm könnte beispielsweise auf eine Prüfung durch einen Techniker zurückgehen oder es könnte unerlaubtes Verhalten durch einen infizierten Prüf-Laptop sein.

Dieser Artikel wurde geschrieben, nachdem die Werksabnahmeprüfung in der US Rothenburg abgeschlossen war und während die Inbetriebnahme

gerade lief. Bereits für die Werksabnahme musste fast die gesamte Netzwerkkonfiguration fertiggestellt sein, damit geprüft werden konnte, ob das Design funktioniert. Eine der Lehren war, dass das IDS Unterstützung für die Erstellung der Kommunikationsmatrix bieten kann. Weiter haben wir festgestellt, dass Pakete durch das Routing der Firewall mehrfach auftreten können, was ein IDS „verwirren“ könnte. StationGuard unterstützte dieses Szenario jedoch korrekt. Zusätzlich ist das Erstellen der Kommunikationsmatrix für die Firewall-Konfiguration mit einem beträchtlichen Aufwand verbunden, weil dies manuell erfolgen muss. Da das IDS auf die SCL-Whitelist zurückgreifen kann, könnte auch dieser Prozess zukünftig automatisiert werden.

4. Fazit und Ausblick

Wenn es einem Angreifer gelingt, eine oder mehrere Anlagen zu beeinflussen, kann dies schwerwiegende Folgen für das Netz haben. Anlagen bieten verschiedene Angriffsvektoren, bei denen die Firewall umgangen werden kann. In der neuen, sicheren Architektur der CKW stehen zahlreiche Gegenmaßnahmen für die in diesem Artikel genannten Angriffsvektoren zur Verfügung. Die Sicherheitsmaßnahmen bieten ein hohes Maß an Sicherheit, ohne dass dadurch auf effiziente Wartungs- und Engineering-Arbeiten per Fernzugriff verzichtet werden muss. Diese Architektur basiert auf der Erkennung von Angriffen im Kern des Netzwerks. Bei IEC-61850-Anlagen kann ein IDS-Ansatz genutzt werden, bei dem mithilfe der SCL automatisch eine Whitelist des gesamten zulässigen Netzwerkverkehrs erstellt wird. Dadurch ist es auch möglich, erkannte Ereignisse in der Sprache der Schutz-, und Leittechniker anzuzeigen, sodass diese in enger Zusammenarbeit mit Security-Verantwortlichen effizient die Ursachen von Alarmen ermitteln können.

Es liegt in der Natur der Cyber-Security, dass jedes Design immer noch verbessert werden kann. Eine mögliche Verbesserung ist beispielsweise die Implementierung einer zertifikatbasierten Netzwerkzugriffssteuerung gemäß 802.1X [8] anstelle des aktuell verwendeten MAC-basierten Ansatzes. Dafür müssen jedoch mehr IEDs den Standard 802.1X unterstützen, was momentan nicht der Fall ist. Folgeartikel sollten sich mit den Erkenntnissen aus der Inbetriebnahme dieses Projekts beschäftigen und die Ergebnisse zukünftiger Sicherheitsbewertungen und Penetrationstests dokumentieren, die in dieser Anlage durchgeführt werden.

5. Quellen

[1] Klien, A.: „New approach for detecting cyber intrusions in IEC 61850 substations“, PAC World Conference Europe, Glasgow, 2019

[2] „Analysis of the Cyber Attack on the Ukrainian Power Grid“, SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, abgerufen im November 2019

[3] „WIN32/INDUSTROYER – A new threat for industrial control systems“, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, abgerufen im November 2019

[4] „Threat Research – Attackers Deploy New ICS Attack Framework ‚TRITON‘ and Cause Operational Disruption to Critical Infrastructure“, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, abgerufen im November 2019

[5] Kushner, D.: „The Real Story of Stuxnet –

How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program“, IEEE Spectrum, Februar 2013

[6] Gosteli, Y., Klien A.: „Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg“, bulletin.ch, 2019, 6, S. 50–52

[7] NIST: „Framework for improving critical infrastructure cybersecurity“, Version 1.1, National Institute of Standards and Technology, April 2018

[8] IEEE: „802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control“, International Standard, Februar 2010

OMICRON ist ein weltweit tätiges Unternehmen, das innovative Prüf- und Diagnoselösungen für die elektrische Energieversorgung entwickelt und vertreibt. Der Einsatz von OMICRON-Produkten bietet höchste Zuverlässigkeit bei der Zustandsbeurteilung von primär- und sekundärtechnischen Betriebsmitteln. Umfassende Dienstleistungen in den Bereichen Beratung, Inbetriebnahme, Prüfung, Diagnose und Schulung runden das Leistungsangebot ab.

Kunden in mehr als 160 Ländern profitieren von der Fähigkeit des Unternehmens, neueste Technologien in Produkte mit überragender Qualität umzusetzen. Servicezentren auf allen Kontinenten bieten zudem ein breites Anwendungswissen und erstklassigen Kundensupport. All dies, zusammen mit einem starken Netz von Vertriebspartnern, ließ OMICRON zu einem Marktführer der elektrischen Energiewirtschaft werden.

Mehr Informationen, eine Übersicht der verfügbaren Literatur und detaillierte Kontaktinformationen unserer weltweiten Niederlassungen finden Sie auf unserer Website.

www.omicronenergy.com