Cybersecurity in der Niederspannungsenergieverteilung

Von der Feldebene bis in die Cloud
siemens.de/lowvoltage/digitalisierung

Die Digitalisierung bringt viele Vorteile mit sich. Durch immer professionellere Cyberangriffe steigt allerdings auch das Risiko für hohe finanzielle Verluste. Bei Infrastruktureinrichtungen wie Stromnetzen drohen sogar Versorgungsengpässe. Was das speziell für die Niederspannungsebene bedeutet, zeigt Siemens mit einem ganzheitlichen Cybersicherheit-Ansatz zum Schutz und sicheren Betrieb entsprechender Komponenten und Anlagen.

Einen umfassenden Schutz gegen Cyberbedrohungen verspricht das Defense-in-Depth Konzept, wie es auch Siemens empfiehlt. Dabei handelt es sich um ein übergeordnetes und umfassendes Informationssicherungskonzept, das Anlagensicherheit, Netzwerksicherheit und Systemintegrität herstellt.

Ein wichtiges Element des Konzepts bildet die ganz unmittelbare Feldebene. Denn die Vernetzung mit dem Internet bedeutet für IoT-fähige Komponenten auch: Sie müssen dieselben hohen Cybersecurity-Standards erfüllen wie andere vernetzte Systeme. Nur dann können sie die Betriebssicherheit eines Unternehmens oder Gebäudes dauerhaft gewährleisten. Direkt in den Geräten integrierte Sicherheitsfunktionen gehören damit zu jedem durchgängigen Cybersecurity-Konzept. Konkrete Ansatzpunkte bieten u. a. ein systematisches Management möglicher Schwachstellen über den gesamten Lebenszyklus einer Komponente, Account Management, Schreibzugriff-Beschränkungen und signierte Firmware.

Cybersecurity ist die Grundlage für sicheren Betrieb

So setzt Siemens in seinen kommunikationsfähigen Produkten generell nur signierte Firmware ein. Damit kann ausschließlich von Siemens hergestellte Software auf dem jeweiligen IoT-Gerät installiert und betrieben werden. Das verhindert die Veränderung der Firmware durch Dritte.

Die Installation von Updates stellt zwar einen kritischen Vorgang dar, weil theoretisch Dritte mit manipulierten Updates schädlichen Code aufspielen können. Dagegen hilft aber die signierte Siemens-Firmware. Ein Manipulationsversuch am Code zieht automatisch eine Änderung dieser Signatur nach sich, wodurch das Update vom Gerät als nicht vertrauenswürdig erkannt und somit eine Installation verhindert wird. Zudem kann in vielen Geräten ein Passwortschutz gesetzt werden, der jede unautorisierte Veränderung an der Konfiguration verhindert. Zudem werden durch Konfiguration eines IP-Adressenfilters nur bestimmte, vom Anwender anerkannte IP-Adressen zur Kommunikation mit den Geräten freigegeben.

SIEMENS

Sicherheit auf allen Ebenen realisiert

Wie eine durchgängige Cybersicherheit von der Feldebene bis in die Cloud realisiert werden kann, zeigt zum Beispiel der offene Leistungsschalter 3WA: Am Gerät selbst schützen integrierte Sicherheitsmerkmale den Schalter gegen Manipulationsversuche. Das PROFINET-IO/Modbus-TCP-Modul COM190 etwa verfügt über einen integrierten Hardware-Parameter-Schreib- und Fernschaltschutz. Das bedeutet: Bei aktiviertem Hardware-Schreibschutz können keine Parameter mehr verändert werden, während bei aktiviertem Fernschaltschutz das Ein- oder Ausschalten über einen der Kommunikationswege unterbunden wird. Beide Funktionen sind werksseitig immer aktiviert und müssen manuell und somit bewusst am Kommunikationsmodul selbst ausgeschaltet werden. Sofern der offene Leistungsschalter 3WA in einem zugangsbeschränkten Betriebsraum installiert ist, stellen der Parameter-Schreib- und der Fernschaltschutz für unbefugte Dritte ein unüberwindbares Hindernis beim Versuch des Zugriffs dar, da der Schutz nur lokal am Leistungsschalter deaktiviert werden kann.

Je nach Anwendung des offenen Leistungsschalters 3WA kann es nützlich sein, ihn über die Kommunikationsschnittstelle ferngesteuert ein- oder auszuschalten. Dass ein Fernschalten nur möglich ist, wenn der Betreiber dies vorsieht, gewährleistet das Kommunikationsmodul COM190 mit seinem Fernschaltschutz. Dabei handelt es sich um zwei Klemmen, die zum Deaktivieren des Fernschaltschutzes überbrückt werden müssen. Wie der Parameter-Schreibschutz ist auch der Fernschaltschutz ab Werk aktiviert und muss bei Bedarf bewusst überbrückt werden.

Über einen separaten Kanal, beispielsweise eine speicherprogrammierbare Steuerung (SPS), wird das Fernschalten bedarfsgerecht freigeschaltet und anschließend wieder gesperrt. Die Fernschaltung selbst erfolgt über eine andere Anwendung, etwa ein Energiemanagementsystem. Eine Fernschaltung ist also nur bei Kontrolle über zwei voneinander unabhängige Wege möglich, was ein unbefugtes Schalten durch Hacker oder Malware deutlich erschwert.

Bluetooth-Zugriff sorgfältig abgesichert

Die Bluetooth-Funktionalität des offenen Leistungsschalters 3WA ermöglicht es, über die SENTRON powerconfig mobile App auf diesen zuzugreifen. Dabei finden umfangreiche Sicherheitsvorkehrungen Anwendung, zum Beispiel Verschlüsselung.

Zudem ist die Bluetooth-Schnittstelle werksseitig deaktiviert und muss bewusst über das Display der elektronischen Auslöseeinheit ETU600 eingeschaltet werden. Nach dem Gebrauch sollte die Bluetooth-Schnittstelle ausgeschaltet werden, um missbräuchlichen Zugriff zu verhindern. Für das Pairing mit dem offenen Leistungsschalter 3WA wird eine einmalige PIN verwendet, die von Siemens vergeben wird. Sie wird für jeden offenen Leistungsschalter 3WA neu generiert und während der Produktion auf die jeweilige Einheit geladen. Nach dem ersten Pairing sollte der Betreiber diese PIN ändern.

Als Gateway zur Cloud kann die IoT-Datenplattform 7KN Powercenter 3000 eingesetzt werden. Sie sammelt Informationen zu Energiewerten aus unterlagerten, kommunikationsfähigen Geräten. Diese Daten werden anschließend über cloudbasierte Anwendungen (z. B. MindSphere) visualisiert und ausgewertet. Die Kommunikation über ein einzelnes, mit Sicherheitsfunktionen geschütztes Gateway sorgt dabei für die Datensicherheit. Um die Sicherheitsfunktionen des 7KN Powercenter 3000 nutzen zu können, kann u. a. die Modbus-TCP-Whitelist des offenen Leistungsschalters 3WA genutzt und das 7KN Powercenter 3000 in die Liste der freigegebenen IP-Adressen aufgenommen werden.

Die Software SENTRON powerconfig dient zur Inbetriebnahme und Parametrierung von offenen Leistungsschaltern 3WA. Der Zugriff lässt sich dabei mithilfe der Modbus-TCP-Whitelist sowie dem Parameter-Schreibschutz am Kommunikationsmodul COM190 einschränken.

Cybersicherheit stets auf Höhe mit den aktuellen Bedrohungen

Mit diesen Maßnahmen hat Siemens die Weichen für cybersichere Produkte gestellt. Da sich die Bedrohung ständig verändert und weiterentwickelt, entwickelt auch Siemens neue Sicherheitstechniken, die stetig Risiken reduzieren. Kommunikative Geräte tragen dazu bei, dass in der Industrie 4.0 effizienter und ressourcenschonender gearbeitet werden kann. Die Anzahl der Anwendungen, die auf Kommunikation aufbauen, nimmt ständig zu. Ein starkes Cybersecurity-Konzept, das durch in den Geräten installierte Sicherheitsfunktionen unterstützt wird, stellt sicher, dass Betreiber diese Anwendungen sicher nutzen und von allen Vorteilen profitieren können.

Herausgeber
Siemens AG

Smart Infrastructure
Electrical Products
Siemensstraße 10
93055 Regensburg
Deutschland

Artikel-Nr. SIEP-B10219-00
TH S22-210537 DA 1221

SIEMENS