Nicht nur sicher, sondern nützlich

Siem für Smart Metering | Security-Information-and-Event-Management-Systeme (Siem) sind Best Practice in der IT und sollten aus Sicherheitsgründen auch bei Smart-Metering-Systemen verwendet werden. Siems bieten nicht nur Schutz, sondern können auch als Investition in den Netzbetrieb gesehen werden.

TOBIAS MOHRHAUER

Der Smart-Meter-Rollout ist im vollen Gange. Dies ist auch notwendig, da bis 2027 80 % aller Zähler Smart Meter sein sollen. Die Vorteile des Smart Metering sind allgemein bekannt. Neben direkten Vorteilen, wie der Abschaffung der Handablesung und der Vereinfachung der Rechnungsstellung und von Wechselprozessen, soll die Transparenz den Stromverbrauch allgemein reduzieren. Ausserdem finden Smart-Meter-Daten immer mehr Anwendung in der Netzplanung. Das ist ein grosser Vorteil, um zukünftige herausfordernde Netzsituationen zu bewältigen.[1]

Nichtsdestotrotz werden weiterhin andere Nutzen für Smart-Meter-Daten gesucht. Es gibt immer wieder gute Ansätze, wie zum Beispiel das Potenzial, pflegebedürftige Menschen passiv zu überwachen [2] oder Wärmepumpenzyklen im Feld zu kontrollieren. Bisher fehlen aber Mehrwerte, die den Betriebsalltag eines Energieversorgungsunternehmens (EVU) tatsächlich vereinfachen. Dabei existiert dieser Mehrwert bei Daten, welche Smart-Metering-Systeme generieren; allerdings nicht bei den Lastgangdaten, die immer im Fokus sind, sondern bei den Log-Dateien des Systems.

Log-Dateien entstehen bei allen Komponenten eines Smart-Meter-Systems. Zähler, Datenkonzentratoren, Head-end-Systeme und Messdatenmanagement-Systeme loggen eine Reihe an Ereignissen und bilden so eine Historie. Diese Log-Dateien werden im Smart Metering heute, wenn überhaupt, nur sporadisch betrachtet und oft nicht in einem weiteren Kontext

Bild: jarmoluk/pixabay

gesehen. Das ist ein Sicherheitsrisiko, denn Log-Dateien weisen auf Manipulationsversuche und Cyber-Angriffe hin. Aber nicht nur das: Im Kontext eines Stromnetzes können Log-Dateien auch Einsichten bieten, die das EVU in betrieblicher Hinsicht unterstützen.

Warum «Siem»?

Ein erster Schritt, um diese Potenziale zu nutzen, ist die Einführung eines «Security Information and Event Managements» (kurz Siem) für Smart Metering. Siems sind nichts Neues. [3] In der IT ist es schon länger Best Practice, um ein hohes Sicherheitsniveau zu halten. In einem Siem werden die Log-Dateien aus allen relevanten Systemen zusammengeführt und gesamthaft betrachtet **(Bild 2).** Es können dann Ereignisse definiert werden, die aus einem oder dem gemeinsamen Auftreten mehrerer Log-Dateien bestehen. Es wird bestimmt, wie auf ein gewisses Ereignis reagiert wird. Typischerweise wird ein automatischer Alarm ausgelöst, der einem sogenannten «Security Operation Center» (SOC) weitergeleitet wird. Das SOC unternimmt daraufhin die notwendige Reaktion auf das Ereignis.

Ein Vorteil eines Siem ist, dass es lernen kann. Muster aus Log-Dateien, die auf ein Problem hingewiesen haben, können in Zukunft als ein Ereignis definiert und die dazugehörige Reaktion kann gleich hinterlegt werden. Auch die umgekehrte Logik kann abgebildet werden. Log-Dateien, die in erster Betrachtung auf einen Manipulationsversuch hinweisen, in Tat und Wahrheit aber keinen Einfluss auf den Betrieb haben, werden so gekennzeichnet und können ignoriert werden.

Beispielsweise weist das ungeplante Öffnen eines Zählerdeckels auf einen Manipulationsversuch hin. Eine Reihe an Zählerdeckelöffnungen in kurzer Zeit am gleichen Zähler weist hingegen auf einen nicht-relevanten Wackelkontakt hin.[4] Ohne Siem kann der erste Wackelkontakt schnell dazu führen, dass man in Zukunft Log-Dateien zu Zählerdeckelöffnungen allgemein ignoriert: Das wäre ein grosses Sicherheitsrisiko. Die richtige Unterscheidung zwischen Manipulationsversuch und Wackelkontakt durch das Siem trennt Wichtiges von Unwichtigem und reduziert somit auch die Häufigkeit von «False Positives», also Fehlalarmen.

Mehr als nur Übersicht

Bekannte Siem-Plattformen, wie LogPoint [5], Splunk [6] oder Elastic Stack [7], sind offen und dynamisch aufgebaut, sodass Log-Dateien aus allen möglichen Systemen integriert werden können. Es werden Standardformate verwendet und Schnittstellen angeboten, die Integrationen vereinfachen. Gerade jetzt während des Smart-Meter-Rollouts ergibt das Sinn. In der bestehenden Übergangsphase wird oftmals mehr als ein Metering-System eingesetzt. Neben dem neuen Smart-Meter-System läuft eine bestehende Zählerfernauslesung für Grosskunden. Eine diversifizierte Systemumgebung macht es schwierig, die Übersicht zu halten. Die Zusammenführung von Logdateien auf dem Siem wirkt dem in dieser unübersichtlichen Situation entgegen. Das hat aber auch Vorteile für die Zukunft. Systemumgebungen sind im ständigen Wandel. Mit einem Siem hat man die Sicherheit, auch bei zukünftigen Systemeinführungen die Übersicht zu behalten.[4]

Bild 1 Der Smart-Meter-Rollout ist im vollen Gange. Kann man noch mehr aus den Daten von Smart Metern rausholen?

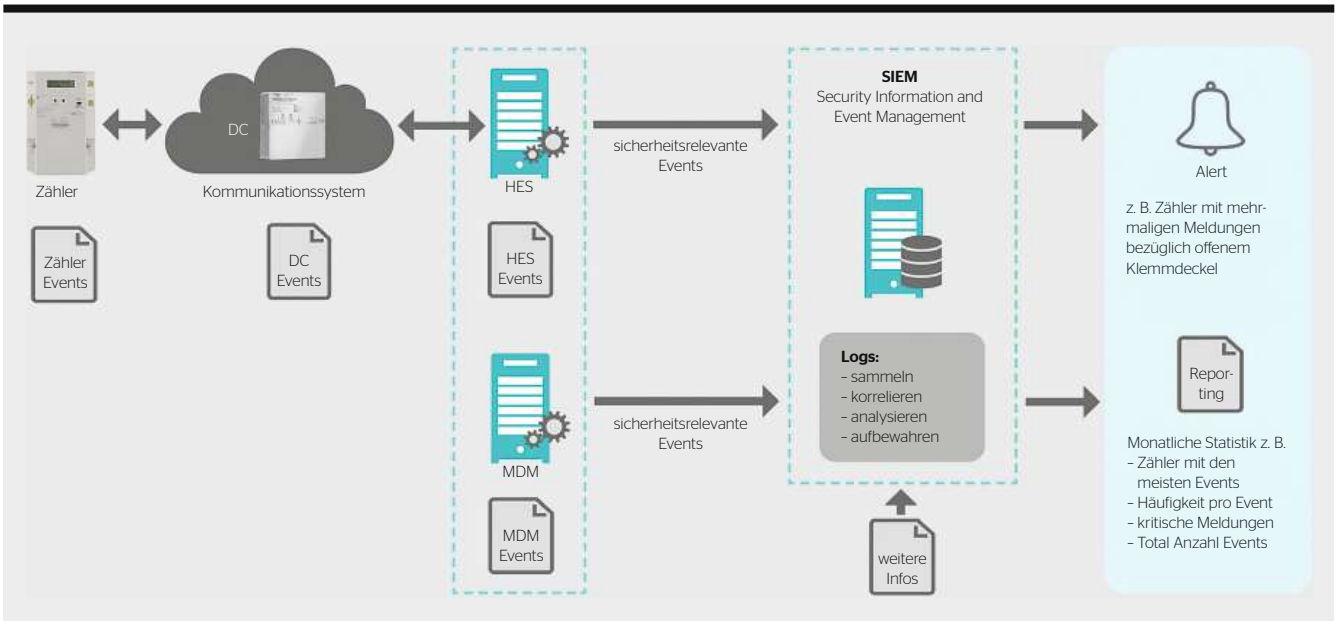

Bild 2 Grundlegende Funktionsweise eines Siem für Smart Metering.

Bilder: Esolva AG

Die Einführung einer Siem-Plattform ist somit der logische nächste Schritt nach dem Smart-Meter-Rollout, oder besser noch während des Rollouts. Das Sicherheitsniveau wird auf die Ebene von State-of-the-art-IT-Systemen gehoben. Die sicherheitstechnischen Vorteile sind direkt und mit einem Siem offensichtlich gegeben. Doch wo ist der eingangs erwähnte betriebstechnische Mehrwert? Zwar ist die Erhöhung des Sicherheitsniveaus ein echter Mehrwert, aber hier wird mit Smart-Meter-Daten ein Problem gelöst, das ohne Smart Meter gar nicht bestände. Gibt es einen Mehrwert für den Netzbetrieb allgemein? Das Potenzial ist sicherlich vorhanden.

Da Log-Dateien in einem universellen, schnell filterbaren, zusammengeführten System vorhanden sind, lassen sich allgemeine Fragen aus dem Betrieb viel schneller untersuchen als bisher. Wie viele Zähler eines EVUs sind beispielsweise wegen Baustellen nicht erreichbar? Wann und welche Zähler nicht erreichbar waren, auch weit zurück in der Historie, kann man mit nur wenigen Klicks in Erfahrung bringen und gegen eine Liste der Baustellen vergleichen. Gibt es eine statistisch höhere Wahrscheinlichkeit von Wackelkontakten bei einem bestimmten Zählermodell? Die Beantwortung solcher Fragestellungen, kann ohne Siem Wochen in Anspruch nehmen, wenn spezielle SQL-Abfragen auf unterschiedlich aufgebaute Datenbanken gemacht werden müssen, deren Ergebnisse anschliessend miteinander verbunden und ausgewertet werden müssen.

Aufgrund der universellen Natur bekannter Siem-Datenbanken sind auch Daten aus Nicht-Zählersystemen integrierbar. Wenn zum Beispiel Informationen zu Baustellen allgemein integriert werden, kann die oben aufgeworfene Frage nicht nur schneller beantwortet werden, sondern es können auch Regeln definiert werden. Nicht erreichbare Zähler nahe Baustellen sind beispielsweise tiefer zu priorisieren, weil der Ausfallgrund bekannt ist. Die Integration von Daten aus Dispatch-Management-Systemen reduziert False Positives bei abgenommenen Zählerdeckeln, wenn es sich um ein geplantes Ereignis handelt. Lassen sich auch Zusammenhänge zwischen Unterspannungen bei Zählern und der Auslastung von Ladestationen sehen? Hängen Überspannungen und Wetterdaten zusammen? Und wenn ja, wie? Es ist nur ein kleiner Schritt weiter, um auch diese Fragen zu beantworten, die keinen direkten Zusammenhang mit dem Betrieb des Smart-Metering-Systems haben.

Um das volle Potenzial zu nutzen, braucht es Entdecker

Die Integration von Daten aus Smart-Meter-fremden Systemen ergibt somit die Möglichkeit, neue Fragen zum Betrieb zu beantworten. Die so gewonnenen Einsichten sind wiederum Regeln, von denen in Zukunft profitiert werden kann. Hierfür ist allerdings einiges an Neugier notwendig. Einsichten und Antworten kommen nicht direkt aus dem täglichen Betrieb, sondern müssen aktiv von sachverständigen Personen gesucht werden. Dieser Nutzen ist zugegebenermassen ein Stück weit spekulativ.

Noch weiter gedacht, sprich noch spekulativer, ist die Suche von Zusammenhängen mittels künstlicher Intelligenz. Ein Siem, das all diese Daten zusammenfügt, bietet die perfekte Ausgangslage zur Durchsuchung und zum Auffinden von Zusammenhängen, die nicht erwartet wurden. Hier steht dann die Antwort vor der Frage: Man sieht beispielsweise einen Zusammenhang zwischen Kommunikationsproblemen mit dem Fernwirksystem und einem anderen Ereignis. Kann der Zusammenhang ermittelt werden?

Es ist richtig, dass andere Datenbankstrukturen besser für solche Untersuchungen geeignet wären als ein Siem. Allerdings wären das dann separate Projekte, die keinen anderen Mehrwert mit sich bringen. Ein Siem bringt den Sicherheitsmehrwert in dem Moment, in dem es aufgebaut wird. Von hier aus sind Einsichten zum Smart-Meter-Betrieb relativ einfach, und mit verhältnismässig kleinem Aufwand können auch ganz spekulative Fragen beantwortet werden. Die für das Sicherheitsniveau praktisch notwendigen Investitionen in ein Siem haben das Potenzial, somit langfristig noch viel weitreichendere Vorteile zu haben: für Erkenntnisse, für den Smart-Meter-Betrieb und für den Netzbetrieb allgemein.

Referenzen

[1] «Smart Metering Roll Out – Kosten und Nutzen: Aktualisierung des Smart Metering Impact Assessments 2021», Ecoplan, im Auftrag des Bundesamts für Energie, 2015.
[2] «Siima», EWB, 2022, www.siima.ch.
[3] «Improve IT Security With Vulnerability Management», M. N. Amrit und T. Williams, 2005.
[4] «Security Monitoring im Smart Metering: Prüfung der Realisierbarkeit sowie Erarbeitung eines Konzepts zur frühzeitigen Erkennung von Cyberattacken», G. Collenberg, MAS-Thesis, Hochschule Luzern, MAS Information & Cyber Security, Landquart, 2020.
[5] www.logpoint.com.
[6] www.splunk.com.
[7] www.elastic.co.

Autor

Tobias Mohrhauer ist Teamleiter Marketing, Innovation & Produktmanagement bei der Esolva AG.
→ Esolva AG, 7302 Landquart
→ tobias.mohrhauer@esolva.ch

RÉSUMÉ

Sûr, mais aussi utile

Des SIEM pour le smart metering

Les systèmes de gestion de l'information et des événements de sécurité (ou SIEM en anglais) sont une meilleure pratique dans le domaine IT ; pour des raisons de sécurité, ils devraient également être utilisés au niveau des systèmes de smart metering. Étant donné que ces systèmes sont constitués de nombreux composants, remplaçables pour certains, un système supérieur qui rassemble les fichiers journaux augmente significativement le niveau de sécurité. Mais les SIEM présentent encore d'autres avantages pour le smart metering. Grâce à la structure claire des données dans les SIEM, il est possible de répondre plus facilement à des questions sur l'exploitation d'un système de smart metering, et l'intégration de données supplémentaires fournit même des réponses sur l'exploitation du réseau. Ainsi, non seulement les SIEM offrent une protection, mais ils peuvent aussi être vus comme un investissement dans l'exploitation du réseau. TOBIAS MOHRHAUER