# Hohe Sicherheit für sensible Daten

Autor(en): **Collenberg, Gian**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **111 (2020)**

Heft 7-8

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-914742

# Hohe Sicherheit für sensible Daten

**Intelligente Messsysteme** | Beim Smart-Meter-Rollout dürfen nur überprüfte intelligente Messsysteme (IMS) eingesetzt werden. Diese schützen aber nicht automatisch vor allen Cyber-Angriffen. Entscheidend ist, wie das IMS im Betrieb eingesetzt und ins Gesamtsystem eingegliedert wird. Nur durch umfassende technische und organisatorische Massnahmen kann ein gutes Sicherheitsniveau erreicht werden.

GIAN COLLENBERG

Im Rahmen der Energiestrategie 2050 hat der Bund die Grundlagen für ein flächendeckendes Smart-Meter-Rollout gesetzt. Gemäss der aktuellen Stromversorgungsverordnung Art. 31e «Einführung intelligenter Messsysteme» müssen bis am 1. November 2027 80 % aller Messeinrichtungen den Anforderungen intelligenter Messsysteme entsprechen. Die meisten Verteilnetzbetreiber (VNB) sind sich bewusst, dass das Stromnetz als ihr «Kronjuwel» besondere Schutzmassnahmen benötigt. Gehört das Stromnetz doch zur kritischen Infrastruktur eines jeden Landes.

Durch die steigende Vernetzung und Digitalisierung verschiebt sich der Schutzbedarf immer mehr in den Cyberraum. Dazu trägt auch der Smart-Meter-Rollout bei, verschmelzen doch damit die Welten von IT und OT (Operation Technology) immer stärker, was gesamtheitlich betrachtet neue Angriffsflächen generiert. Jeder Verteilnetzbetreiber ist in der Verantwortung und muss seinen Teil zum Schutz der kritischen Infrastrukturen beitragen.

## «Security by Design» allein reicht nicht aus

Die StromVV schreibt in Artikel 8b Datensicherheitsprüfung im Absatz 1 vor, dass nur intelligente Messsysteme eingesetzt werden dürfen, deren Elemente erfolgreich auf Gewährleistung der Datensicherheit hin geprüft wurden. Diese Datensicherheitsprüfung ist ein guter Ansatz, um die Hersteller zu verpflichten, bestimmte Sicherheitsmechanismen in ihre Systeme einzubauen.

Doch der Einsatz eines zertifizierten Systems allein reicht nicht aus; die Zer-

Bilder: Esolva AG

tifizierung bestätigt nur die Datensicherheit des geprüften Systems. Entscheidend für die Sicherheit ist, wie dieses System eingesetzt, sprich betrieben, wird. Jedes Unternehmen besitzt bereits eine IT-Infrastruktur, welche unterschiedliche Ausprägungen annehmen kann. Ein intelligentes Messsystem wird daher in eine bestehende Umgebung mit entsprechend vorhandenen Schwachstellen integriert. Für den sicheren Betrieb ist jedoch dieses Gesamtsystem mit all seinen Komponenten entscheidend.

Flächendeckend eingesetzte Smart Meter bringen für das EVU einige Vorteile mit sich. Viele Abläufe können damit effizienter gestaltet werden, was wiederum weitere Begehrlichkeiten weckt. Damit diese genutzt werden können, sind diverse Schnittstellen vom und zum IMS notwendig. Cyber-Angriffe setzen in der Regel am schwächsten Glied der Kette an, um sich initialen Zugang zu einem Unternehmen zu verschaffen. Einmal drin, können sich die Angreifer meist unter dem Radar bewegen und sich von einem System zum nächsten ausbreiten. Als klassisches Beispiel dient der gezielte Phishing-Mail-Angriff auf einen Mitarbeiter mit Zugriff zum IMS. Ist der Computer des Mitarbeiters infiziert, lassen sich weitere Informationen (zum Beispiel Zugangsdaten, genutzte Applikationen, besuchte Webseiten) sammeln **(Bild 1)**.

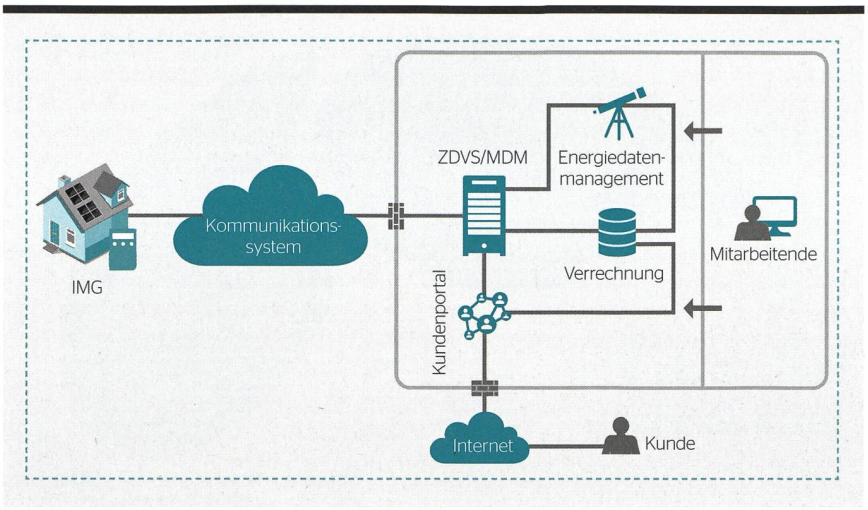


**Bild 1** IMS-Komponenten mit Schnittstellen und Umsystemen als Gesamtsystem mit möglichen Angriffspunkten.

## Anforderungen an den IMS-Betrieb

Die Wichtigkeit des Betriebs ist auch dem VSE bewusst. Daher hat er neben den Richtlinien zur Datensicherheitsprüfung im Anhang 2 «Betriebliche Anforderungen an IMS für die Datensicherheit» auch Anforderungen für den sicheren Betrieb eines IMS erlassen. Diese Anforderungen decken wichtige Bereiche, wie zum Beispiel Inventarisierung, Zugriffskontrolle, Lieferantenbeziehungen und Kommunikationssicherheit, ab. Die Anforderungen halten sich dabei an gängige internationale Standards und etablierte Empfehlungen. Wie genau und in welcher Tiefe eine Anforderung umgesetzt wird, liegt jedoch in der Verantwortung des Betreibers.

Es gibt aber auch Bereiche, welche der Anhang 2 explizit nicht abdeckt, die aber wichtig für das Sicherheitsniveau des Gesamtsystems sind. Darunter fallen beispielsweise organisatorische Aspekte wie eine unternehmensweite Informationssicherheitspolitik, die Personalsicherheit oder auch das Business Continuity Management. Entwickelt ein Unternehmen selbst Schnittstellen oder Tools, die im IMS-Betrieb helfen, müssen auch Anforderungen für die sichere Softwareentwicklung betrachtet werden.

Die betrieblichen Anforderungen an ein IMS sind sicher ein gutes Hilfsmittel und beleuchten einige smart-metering-spezifische Punkte. Doch die Erfüllung dieser Anforderungen allein reicht nicht aus, um das Gesamtsystem ausreichend zu schützen.

## Sicherheitskonzept vor dem Rollout festlegen

Um ein gutes Schutzniveau zu erreichen, ist eine Vielzahl verschiedener Massnahmen nötig. Kein Unternehmen ist in der Lage, alle Massnahmen umzusetzen. Umso wichtiger ist, dass diese priorisiert betrachtet werden. Wichtige Kenngrössen zur Priorisierung sind dabei die Effektivität und Effizienz einer Massnahme. Die Effektivität gibt an, wie gut eine Massnahme zum Schutz beitragen kann. Bei der Effizienz geht es um die Wirtschaftlichkeit. Die Umsetzung einer Massnahme, die in der Implementierung sehr aufwendig ist, aber nur wenig zum Schutz beiträgt, sollte gut überlegt werden.

Ein gutes Beispiel einer sinnvollen Massnahme ist die Geräte- und Systemhärtung. Die meisten Geräte und Systeme verfügen von Haus aus über mehr Funktionalitäten, als im Betrieb benötigt werden. Um die Angriffsfläche zu reduzieren, sollten nicht benötigte Funktionen deaktiviert werden; darunter fallen zum Beispiel nicht verwendete Schnittstellen des Zählers. Des Weiteren werden ab Werk Standardpasswörter gesetzt, die gemäss den EVU-eigenen Komplexitätsanforderungen angepasst werden müssen. Bei einem anstehenden Smart-Meter-Rollout ist wichtig, diese «sichere» Zählerkonfiguration vor dem Rollout festzulegen. Eine nachträgliche Anpassung der im Feld installierten Zähler wird sehr aufwendig. Diese Härtung muss zwingend auf alle Komponenten ausgeweitet werden. Dazu gehören auch alle Bestandteile des Kommunikationssystems und des Zählerdatenverarbeitungssystems (ZDVS).

Eine weitere weitverbreitete technische Massnahme ist die Nutzung von Kryptografie zur Verschlüsselung der Daten während der Übertragung. Damit wird die Vertraulichkeit der Daten gewährleistet, weil die Daten nicht mitgelesen werden können. Je nach eingesetztem Verfahren wird so auch die Datenintegrität sichergestellt. Das bedeutet, dass die Daten während der Übertragung nicht verändert wurden. Die Verschlüsselung sollte End-to-End also vom Zähler bis zum ZDVS aufgebaut werden. Heutige Verschlüsselungstechnologien sind bei entsprechender Schlüssellänge kaum zu knacken. Ist ein Angreifer aber im Besitz der entsprechenden Schlüssel, können


**Bild 2** Nist-Kreis mit konkreten Aufgaben pro Bereich.

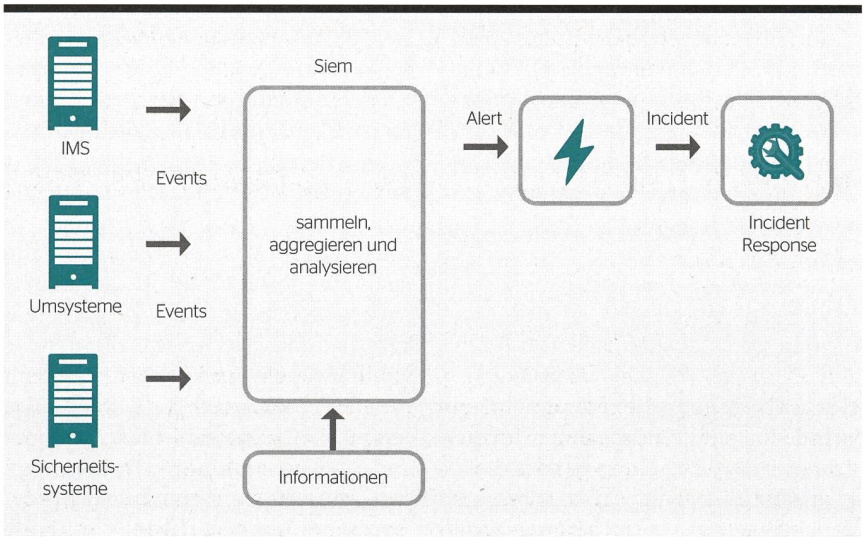


**Bild 3** Events -> Alert -> Incident – was wo wie geschieht.

die Daten problemlos entschlüsselt und gelesen werden. Damit kommt dem Schlüsselmanagement eine entscheidende Rolle zu. Die sichere Ablage der Schlüssel, aber auch das periodische Ändern müssen am Anfang des Rollouts definiert werden.

Damit während des Rollouts alle definierten Sicherheitsmassnahmen beachtet werden, empfiehlt es sich, vorgängig ein Sicherheitskonzept zu definieren, in welchem sämtliche Sicherheitsmassnahmen genau spezifiziert sind und der Umgang mit diesen festgehalten wird. Das Sicherheitskonzept muss allen in das Rollout und den IMS-Betrieb involvierten Personen bekannt sein. Am besten eignen sich dafür spezifische Informationssicherheitsschulungen, an denen die Risiken aufgezeigt werden und somit das Bewusstsein dafür geschaffen wird.

## Das Erkennen von Angriffen wird immer wichtiger

Die Bedrohungslage spitzt sich stetig zu und die Angreifer werden professioneller. Es reicht daher nicht mehr aus, möglichst viele präventive Massnahmen umzusetzen. Betreiber von kritischen Infrastrukturen müssen damit rechnen, Ziel solcher Angriffe zu sein. Umso wichtiger ist, diese Angriffe frühzeitig zu erkennen und entsprechend rasch zu reagieren, um den Schaden in Grenzen zu halten. Die Wichtigkeit von detektierenden Massnahmen nimmt laufend zu, das wird auch in den Anforderungen an den IMS-Betrieb herausgestrichen: «Das intelligente Messsystem muss mit Hilfe von präventiven und detektiven Massnahmen geschützt werden.»

Um diese Bereiche abzudecken, wird gerne das Nist-Framework als Alternative zum ISO-27001-Standard beigezogen. Darin wird grosses Augenmerk auf die Bereiche «Erkennen», «Reagieren» und «Wiederherstellen» gelegt **(Bild 2)**.

Im IT-Betrieb ist das Monitoring aller Komponenten, um Störungen frühzeitig zu erkennen, nicht mehr wegzudenken. Geht es um das Erkennen von sicherheitsrelevanten Vorfällen, spricht man daher auch vom Security Monitoring. Die Auswertung sicherheitsrelevanter Log-Meldungen (sogenannten Events) soll Auffälligkeiten aufzeigen, die Hinweise auf unrechtmässige Nutzungen oder Angriffe geben. Dafür kommt in der Regel ein Security-Incident- und Event-Management-System (Siem) zum Einsatz. Mit dem Abbilden von Erkennungslogiken durch die Kombination verschiedener Events können Auffälligkeiten erkannt werden. Moderne Siem-Systeme nutzen zusätzlich Machine Learning, um Anomalien effizienter erkennen zu können. Ein Siem ist abhängig von den generierten Events aller Systeme **(Bild 3)**. Die Anforderungen im Bereich Logging für ein IMS sind vage gehalten: «Für die Informationssicherheit relevante Events müssen aufgezeichnet und überwacht werden (Logging & Monito-

ring).» Somit muss jeder Betreiber eines IMS für sich selbst definieren, welche Events relevant sind und diese auswerten. Jeder Hersteller generiert andere Events. Somit müssten bei einem Einsatz verschiedener Produkte unterschiedlicher Hersteller unterschiedliche Events miteinander kombiniert werden. Einheitliche Richtlinien für IMS-Komponenten würden das Auswerten der Events und damit das Erkennen von Angriffen vereinfachen.

## Reaktion auf einen Vorfall vorbereiten

Wird im Security Monitoring ein Alarm generiert, muss klar definiert sein, wie darauf zu reagieren ist. Dazu muss sich ein IMS-Betreiber vorgängig mit dieser Frage auseinandersetzen und sich auf mögliche Vorfälle vorbereiten. Um rasch reagieren zu können, müssen Prozesse und Verantwortlichkeiten klar definiert sein; beispielsweise wenn auf mehreren Smart Metern Anzeichen für unrechtmässige Zugriffe entdeckt oder seit einigen Tagen aussergewöhnliche Steuerungsbefehle ausgelöst werden.

Neben dem definierten Vorgehen müssen auch die entsprechenden Ressourcen mit dem nötigen Know-how bereitstehen. Cyber-Angriffe können von überall auf der Welt ausgelöst werden, folglich müssen die Systeme rund um die Uhr überwacht werden. Um diese Abdeckung zu gewährleisten, muss eine passende Betriebsorganisation – in der Regel ein Security Operation Center (SOC) – aufgebaut werden. Da diese Personen nicht in andere Betriebsaufgaben eingebunden sind, können sie auf einen Vorfall direkt reagieren. Ein Alarm wird durch einen SOC-Mitarbeiter (Security-Analyst) geprüft. Handelt es sich um einen Incident (Vorfall mit negativen Auswirkungen), werden sofort weitere definierte Schritte gemäss einem Playbook ausgelöst. Weitere Informationen oder Personen zur Bewältigung des Vorfalls werden hinzugezogen. Bei einem grossflächigen Vorfall mit Auswirkungen auf das ganze Unternehmen kommt unweigerlich auch das Notfall- und Krisen-Management ins Spiel. Cyber-Vorfälle können schnell mehrere Systeme betreffen und so den gesamten Betrieb des Unternehmens in Mitleidenschaft ziehen. Umso wichtiger ist, dass das Management bereits im Vorfeld seine Hausaufgaben erledigt und das Business-Continuity-Management erarbeitet hat.

Die Anforderungen für den IMS-Betrieb definieren auch Vorgaben für das Management von Informationssicherheitsvorfällen: «Eine konsistente und effektive Vorgehensweise im Hinblick auf die Handhabung von Sicherheitsvorfällen sicherzustellen, einschliesslich der Meldung von Sicherheitsereignissen und Schwachstellen.» **(Bild 3)**

## IMS-Betrieb «sicher» gestalten

Zum sicheren Betrieb eines IMS sind verschiedene Punkte entscheidend. Der Einsatz eines zertifizierten IMS bildet eine wichtige Grundlage. Entscheidend ist, wie sich das IMS in das Gesamtsystem einbettet. Jede Kette ist nur so stark wie das schwächste Glied. Die vom VSE definierten Anforderungen an den IMS-Betrieb sind eine gute Basis, müssen aber zwingend mit weiteren Sicherheitsmassnahmen ergänzt werden. Vor dem Rollout sollten alle Sicherheitsmassnahmen definiert und in einem Sicherheitskonzept festgehalten werden. Insbesondere den detektiven Massnahmen und der Reaktion auf Vorfälle sollte genügend Gewicht beigemessen werden. Durch die sich stetig ändernde Bedrohungslage steigt die Wahrscheinlichkeit eines Angriffs. Die richtige Vorbereitung ermöglicht, solche Attacken frühzeitig zu erkennen, zu stoppen und grösseren Schaden oder Ausfälle zu verhindern.

**Autor**
**Gian Collenberg** ist IT-Sicherheitsverantwortlicher bei Esolva AG.
→ Esolva AG, 8570 Weinfelden
→ gian.collenberg@esolva.ch

RÉSUMÉ

## Données sensibles, sécurité élevée

Systèmes de mesure intelligents

**Dans le cadre du déploiement des smart meters, seuls les systèmes de mesure intelligents (SMI) vérifiés peuvent être installés. Cependant, ceux-ci ne protègent pas automatiquement contre toutes les cyberattaques. La façon dont le SMI est utilisé et intégré dans le système global est déterminante. Seules des mesures techniques et organisationnelles étendues permettent d'atteindre un bon niveau de sécurité.**

**Pour exploiter un SMI en toute sécurité, différents points sont déterminants. L'utilisation d'un SMI certifié constitue une base importante, et la façon dont ce SMI est intégré dans le système global est décisive. En effet, une chaîne est aussi solide que son maillon le plus faible. Les exigences fixées par l'AES envers l'exploitation d'un SMI constituent une bonne base, mais doivent impérativement être complétées par d'autres mesures de sécurité. Avant le déploiement, toutes les mesures de sécurité devraient être définies, et un concept de sécurité consigné. En particulier, il faudrait accorder suffisamment de poids aux mesures de détection et à la réaction aux incidents. Avec la situation de menace en constant changement, la probabilité d'une attaque augmente. Une bonne préparation permet d'identifier de telles attaques suffisamment tôt, de les stopper et d'éviter les dommages et les pannes de grande ampleur.** MR