OMNETRIC
A Siemens Company

DATENBLATT

Cyberbedrohungen: Vorbeugung und Schutz für Versorgungsunternehmen

Ein integrierter Ansatz, um Risiken zu erkennen und das Versorgungsnetz zu schützen

Das Sicherheitsgebot

Cyberangriffe – von nicht zielgerichteter Ransomware bis hin zu ausgereiften landesweiten Attacken – können die Netzleistung bedrohen oder sich auf den individuellen Datenschutz auswirken. Dies kann ernste Folgen für Versorgungsunternehmen, ihre Kunden und verbundene Wirtschaftszweige haben.

Cybersicherheit hat heutzutage für die meisten Betriebe hohe Priorität, doch Unternehmen, die kritische Dienstleistungen erbringen, wie beispielsweise Energieversorger, sind mit mehr Herausforderungen konfrontiert als die meisten anderen. Eine zuverlässige und stabile Stromversorgung ist für den Energienetzbetrieb das A und O. Wenn eine Attacke stattgefunden hat, können Versorgungsunternehmen nicht einfach Systeme abschalten oder isolieren. Ihr Hauptanliegen ist es, das System ohne Versorgungunterbrechung weiterzubetreiben.

Eine verbesserte Integration zwischen den Energiebetriebsabläufen von Versorgungsunternehmen und IT kann ihnen helfen, wertvolle Daten zu identifizieren und nutzbar zu machen, um den neuen Herausforderungen eines komplexen Energienetzes besser zu begegnen.

Sicherheitsbedenken halten Versorgungsunternehmen jedoch davon ab. Das Gebot, dass das Licht nicht ausgehen darf, kann sie zögern lassen, Integrationsinitiativen voranzutreiben und den Netzbetrieb weiter für die IT zu öffnen.

Diese vorsichtige Vorgehensweise ist zwar verständlich, die disruptiven Herausforderungen des neuen Energiesystems erfordern jedoch ein Handeln. Die Führungskräfte im Energiesektor müssen einen goldenen Mittelweg finden, bei dem sich Nutzen und potenzielle Risiken die Waage halten.

Was wir bieten

Um das Netz von Versorgungsunternehmen zu schützen, bedarf es der richtigen Technologie, der richtigen Prozesse und vor allem der richtigen Leute.

OMNETRIC hat es sich zum Ziel gesetzt, die Performance von Energieversorgern durch die IT-Integration ihrer operativen Prozesse zu verbessern, um ihre Geschäftsziele zu unterstützen. Wir sind im IDC MarketScape als führendes Unternehmen anerkannt: EMEA Service Providers Digital Grid Enablement 2019, Anbieterbewertung*

Den Herausforderungen der Versorgungsunternehmen in Sachen Cybersicherheit hat OMNETRIC Folgendes entgegenzusetzen:

- CISSP-qualifizierte Cybersicherheitsexperten mit umfassendem Wissen, was die besonderen Erfordernisse des Energienetzes angeht, und Zugriff auf Energieingenieure und Produktspezialisten.
- Langjährige Erfahrung in den Bereichen IT, Sicherheit und Energienetze.
- Die seltene Kombination aus fundierter Erfahrung mit Betriebstechnologien über die Übertragung und Verteilung hinweg und Expertise in den Bereichen IT-Consulting und Systemintegration.
- Zugang zur Recherche und Marktanalyse unseres Gesellschafters Siemens – und unserer anderen Ökosystempartnern –, um unsere Methodik mit den neuesten Einsichten anzureichern.

* Dok.-Nr. #EUR143345019, Juni 2019

Das Ziel: Nachhaltiger Schutz

Wir unterstützen Versorgungsunternehmen durch eine Reihe von Maßnahmen (siehe nachstehende Abb. 1) bei der Identifikation bestehender und künftiger Sicherheitsrisiken, bei der Implementierung und Integration von Sicherheitslösungen und bei Betrieb und Optimierung des Schutzes und der Prozesse ihrer Systeme.
Unsere Lösungen berücksichtigen technische, organisatorische und Prozesszusammenhänge. Wir können zwar mit Einzellösungen, wie speziellen Härtungstests, Verschlüsselungssystemen für intelligente Zähler (Smart Meters) und Log-Integration, helfen, unser Ziel ist jedoch stets ein umfassender, nachhaltiger Schutz.

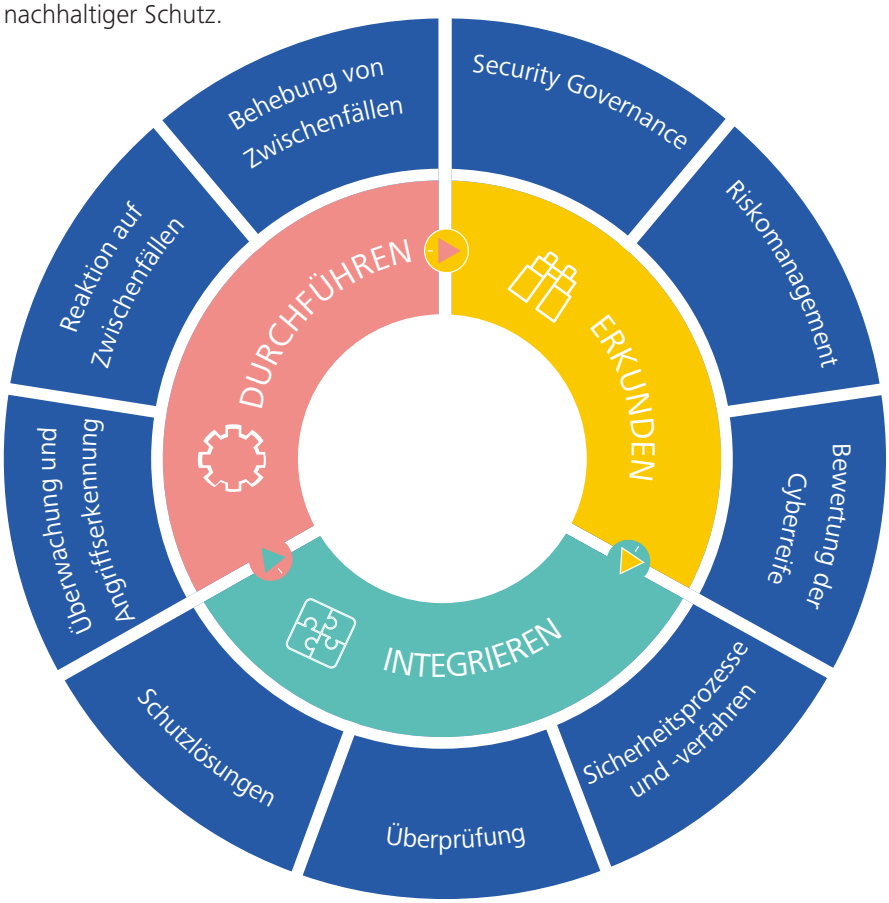

Abb. 1: Integrierter Cybersecurity-Ansatz

Wie wir Versorgungsunternehmen helfen, Cyberbedrohungen zu bewältigen

- Security Governance: Einbeziehen von Cybersicherheitsüberlegungen in alle Geschäftsentscheidungen.
- Risikomanagement: Erkennen und Verstehen der Cybersicherheitsrisiken und Einrichten der bestenmöglichen Überwachung, um sie zu mindern.
- Schutzlösungen: Auswählen und Umsetzen der richtigen Sicherheitsmaßnahmen, wie beispielsweise Firewalls und Identitätsmanagement, um Angreifer am Hacken von Systemen zu hindern.
- Überprüfung: Testen der Schutzmaßnahmen, um einen optimalen Betrieb zu gewährleisten.
- Sicherheitsprozesse und -verfahren: Sicherstellen der kontinuierlichen Effektivität bestehender Sicherheitsmaßnahmen.
- Überwachung und Angriffserkennung: Erkennen von Schwachstellen und Angriffen.
- Reaktion auf Zwischenfälle: Erstellen eines Plans bzgl. des Umgangs mit Sicherheitszwischenfällen.
- Behebung von Zwischenfällen: Wiederherstellungsmaßnahmen nach einem Angriff und Lernen aus Fehlern.

Die besten Ergebnisse erzielen

Die Effektivität einer Sicherheitsstrategie wird deutlich verbessert,

... wenn passende Talente am Werk sind

Versorgungsunternehmen sollten hinsichtlich der Cybersicherheitsbedrohung relevante Spezialisten engagieren, z. B. Informatiker und Ingenieure sowie Sicherheitsexperten mit Hintergrundwissen im Bereich Versorgungsunternehmen. Diese Fachleute kennen sich mit den Abläufen im Zusammenhang mit dem Netzbetrieb sowie den komplexen zugrunde liegenden Systemen aus.

... wenn Sicherheit im Unternehmen auf der Tagesordnung steht

Bei Sicherheitsentscheidungen geht es um das Abwägen von Risiken. Sie müssen entsprechend in Zusammenarbeit mit gut informierten Vertretern der Unternehmensführung getroffen werden, die eine ganzheitliche Perspektive einbringen können. Die Einbindung der Unternehmensführung ist entscheidend, um effektive Vorbeuge- und Schutzmaßnahmen zu etablieren und in Krisenzeiten die Mobilisierung und den Fokus geeigneter Personen sicherzustellen.

... wenn Sicherheit in die Kernlösung integriert ist

Die Sicherheitserfordernisse sollten idealerweise während der Ausarbeitung der Lösungen bewertet werden und nicht erst später, wenn die Lösung schon im Einsatz ist. Wenn die grundlegende Energietechnologie in eine sichere Umgebung implementiert werden kann, die die Menschen, den Prozess und die technischen Sicherheitsaspekte berücksichtigt, werden die Risiken minimiert. Ist hingegen Sicherheit nicht von Anfang an in das Lösungsdesign integriert, wird das spätere Vorgehen gegen eine Attacke in der Regel schwieriger, kostspieliger und disruptiver, und Gegenmaßnahmen weniger effektiv.

Wie legt man los?

Um Versorgungsunternehmen zu helfen, Sicherheitsprobleme zu erkennen und zu bewerten, bieten wir eine **Bewertung der Cyberreife** (Cyber Maturity Assessment) an – einen Ansatz, der Versorger bei der Einschätzung und Festellung der vorliegenden Sicherheitslage hinsichtlich ihrer Energielösungen unterstützt und bessere Entscheidungen bezüglich künftiger Sicherheitsinvestitionen ermöglicht.

Unser Ziel ist es, Versorgungsunternehmen zu helfen, nicht mehr die Rolle der Feuerwehr spielen zu müssen, sondern eine strategische Verbesserung der Sicherheitssituation zu erreichen. Unsere Bewertungsmethodik basiert auf ES-C2M2 und kann die Cyberreife anhand von Standards und Normen wie NERC CIP, ISO 27001, ISF Good Practice und NIST 800 bewerten.

Die Sicherheitslandschaft verändert sich

Digitalisierung:
Früher war angemessener Schutz gegeben, wenn man wesentliche Ausrüstungen und Anlagen mit physischen Schlössern gesichert hat. Heutzutage erfordern die zunehmende Zahl von Geräten, steigende Konnektivität zwischen Netz und anderen Systemen sowie verteilt vorliegende Energiesysteme neue Ansätze.

Erweiterter Einfluss und Zugang:
Inzwischen wirken Geräte über das Umspannwerk hinaus und sind häufig – beispielsweise im Fall von intelligenten Zählern (Smart Meters) – für Personen außerhalb des Versorgungsunternehmens zugänglich. Mehr Personen, Organisationen und Geräte – insbesondere solche, die sich außerhalb der Firewall des Versorgungsunternehmens befinden – bedeuten mehr Risiko. Ein höherer Automatisierungsgrad erschwert es dem Betriebspersonal, ungewöhnliches Verhalten oder Anomalien zu erkennen, wodurch das Risiko weiter erhöht wird.

Verfügbarkeit von Angriffstools:
Da erforderliche Tools direkt als Download zur Verfügung stehen, wird es für böswillige Akteure wie Hacker, Terroristen, und Kriminelle entsprechend einfacher, das Netz anzugreifen.

Vorschriften und Regulierung:
Regulierungsbehörden gehen mit der Zeit und reagieren auf die Bedenken der Kunden. Die Datenschutzgrundverordnung (DSGVO) beispielsweise verbessert die Sicherheitsvorkehrungen hinsichtlich personenbezogener Daten in der EU. Die Entwicklung der nordamerikanischen Vorschriften (NERC CIP) geht weiter, und immer mehr Länder setzen lokale Vorschriften um. Diese Vorschriften auf Länderebene verändern die Sicherheitslandschaft für Versorgungsunternehmen.

OMNETRIC hilft

Wir verfügen über das nötige Branchenwissen, die Ingenieurs-, Daten- und Sicherheitskompetenzen sowie über die Erfahrung, um geeignete Sicherheitslösungen für Energieversorger und Netzbetreiber zu entwerfen und zu etablieren. Wir kennen die Herausforderungen, die sich beim Umgang mit kritischer Infrastruktur stellen, und die Bedeutung von Zuverlässigkeit und Effizienz im Netzbetrieb. Wir sind uns auch der Auswirkung von Sicherheitsbedrohungen bewusst und der Geschwindigkeit, mit der neue Bedrohungen zutage treten.

Kontakt

Geschäftliche Anfragen
request@omnetric.com

Marketing und Unternehmenskommunikation
pr@omnetric.com

Stellenangebote
www.omnetric.com/vacancies

Über OMNETRIC – A Siemens Company

OMNETRIC ermöglicht es Energieversorgern durch die IT-Integration ihrer operativen Prozesse, die Vorteile digitaler Energiesysteme für ihr Geschäft zu nutzen.

Das globale OMNETRIC-Team, bestehend aus Ingenieuren, Informatikern, sowie Sicherheits- und Datenexperten, verfügt über langjährige, branchenspezifische Erfahrung in der Datenanalyse und -verwertung. OMNETRIC hilft seinen Kunden dabei, nachhaltig von Veränderungen im Energiesektor zu profitieren und neue Geschäftsmodelle zu etablieren.

OMNETRIC steht seinen Kunden seit 2014 als innovatives, lösungsorientiertes Technologieunternehmen zur Seite. Besuchen Sie uns auf www.omnetric.com.