LOGPOINT

SIEMENS

INTERVIEW MIT SIEMENS

# NIS2 erfüllt: Electrification X schützt Energieversorger mit Logpoint

# SIEMENS

**Im Gespräch mit mit Wolfgang Keiner**
**Global Product Manager Cybersecurity bei SIEMENS**

## WAS WAREN DIE GRÖSTEN HERAUSFORDERUNGEN, DENEN SICH SIEMENS-KUNDEN VOR DER IMPLEMENTIERUNG EINER SIEM LÖSUNG IN BEZUG AUF CYBERSICHERHEIT UND NETZWERKTRANSPARENZ STELLEN MUSSTE?

“Die Kunden der Siemens Smart Infrastructure verwalten kritische Energienetzinfrastrukturen. Der steigende Strombedarf und die Integration erneuerbarer Energien erfordern die Modernisierung und Digitalisierung der Automatisierungstechnik. Die Digitalisierung ermöglicht zwar einen fortschrittlichen Betrieb der Stromnetze, erhöht aber auch die Anfälligkeit für Cyberattacken. Die Gewährleistung robuster Cybersicherheitsmaßnahmen zum Schutz kritischer Infrastrukturen hat oberste Priorität und wird durch verschiedene Vorschriften wie die NIS2 (European Network and Information Security Directive 2) durchgesetzt.

Die Vorschriften verlangen von den Betreibern kritischer Energienetze, dass sie Vorfälle im Bereich der Cybersicherheit wirksam erkennen und darauf reagieren, was sowohl moderne als auch ältere Systeme vor Herausforderungen stellt. Moderne Systeme sind komplex, während traditionelle Systeme mit veralteter Technologie und Integration zu kämpfen haben. Die Absicherung mit robusten Cybersicherheitsmaßnahmen und die Einhaltung von Vorschriften sind wichtige und anspruchsvolle Aufgaben für unsere Kunden.”

## WARUM HABEN SIE SICH FÜR LOGPOINT ALS PARTNER ENTSCHIEDEN UND WELCHE FAKTOREN HABEN IHRE ENTSCHEIDUNG BEEINFLUSST?

“Für seine Kunden aus dem Energieversorgungssektor wählte Siemens Logpoint aufgrund mehrerer Vorteile. Logpoint bietet eine umfassende Sicherheitsplattform, die SIEM, Automatisierung und Case-Management integriert und einen ganzheitlichen Ansatz zur Identifizierung von und Reaktion auf Cybersicherheitsvorfälle bietet.
Logpoint war in der Lage, das Fachwissen von Siemens über Umspannwerke, Automatisierungsarchitekturen für Umspannwerke und IoT-Konnektivität zu nutzen. Die Kombination dieser Stärken mit Logpoint schafft ein starkes Wertversprechen für Siemens-Kunden.
Die Plattform ermöglicht die Einhaltung wichtiger Vorschriften wie der DSGVO und NIS2 und bietet sofort einsatzfähige Compliance-Unterstützung und vorkonfigurierte Dashboards. Die Plattform ist hochgradig skalierbar, flexibel und erfüllt die Anforderungen mit Bereitstellungsoptionen wie SaaS, On-Premises und Private Cloud für sowohl kleine als auch große Netzwerke.
Logpoint bietet einen starken Partner- und Kundensupport, der sicherstellt, dass Siemens und seine Kunden effektive Fähigkeiten aufbauen können, um Cybersicherheitsvorfälle in kritischen Energiesysteminfrastrukturen zu identifizieren und darauf zu reagieren. Diese Faktoren machen Logpoint zu einer robusten und zuverlässigen Wahl, wenn es darum geht, die Cybersicherheitslage der Kunden von Siemens im Bereich der Energieversorgung zu verbessern.”

## WELCHE AUSWIRKUNGEN HAT LOGPOINT SIEM AUF DIE ANGRIFFSERKENNUNG UND DIE NIS-2-KONFORMITÄT BEI SIEMENS ELECTRIFICATION X?

“Electrification X ist eine umfassende IoT-Suite für Umspannwerke. Sie ist darauf ausgelegt, die Herausforderungen der Energiewende durch die Verbindung der physischen mit der digitalen Welt zu meistern. Sie ist Teil des Siemens Xcelerator Portfolios und bietet eine Internet-of-Things (IoT) Software as a Service (SaaS) Plattform für Elektrifizierung und Automatisierung. Durch den Einsatz fortschrittlicher digitaler Technologien unterstützt Electrification X die Modernisierung und
Optimierung von Energieversorgungssystemen und ist damit ein wertvolles Werkzeug für das Management von modernen und komplexen Energieinfrastrukturen.

Logpoint verbessert die Identifizierung von Cybersicherheitsvorfällen und die NIS2-Konformität für Electrification X-Kunden erheblich:
Erhöhte Sichtbarkeit: Durch das Sammeln und Anreichern von Protokolldaten aus verschiedenen Quellen bietet Logpoint detaillierte Einblicke in das Netzwerk und die IT-Infrastruktur. Diese Transparenz ist entscheidend für die Erkennung von und die Reaktion auf Cybersicherheitsvorfälle.
Verbesserte Erkennung von Cybersicherheitsvorfällen: Logpoint zentralisiert die Datenüberwachung und übersetzt komplexe Protokoll- und Ereignisdaten in eine einzige Sprache. Dies bietet einen umfassenden Überblick über die Sicherheitslage und ermöglicht eine schnellere und genauere Erkennung von Cybersicherheitsvorfällen.
Einhaltung gesetzlicher Vorschriften & Compliance: Logpoint ermöglicht die Einhaltung der NIS2-Anforderungen durch die Bereitstellung von Compliance-Unterstützung und Dashboards für das Access Management, das Incident Management und das Monitoring der Perimeter-Sicherheit. Dies hilft den Kunden von Siemens, die strengen gesetzlichen Anforderungen zu erfüllen und ein hohes Maß an Cybersicherheit zu gewährleisten.”

## LOGPOINTS PERSPEKTIVE AUF DIE SIEMENS PARTNERSCHAFT

**Wettbewerbsvorteil durch integrierte Cybersicherheit**

Siemens bietet mit Logpoint integrierte Cybersicherheitslösungen, die speziell auf kritische Infrastrukturen zugeschnitten sind ein klarer Wettbewerbsvorteil.

**Beschleunigte Markteinführung sicherer Lösungen**

Durch die reibungslose Integration von Logpoint kann Siemens Sicherheitsfunktionen schneller implementieren und gesetzliche Anforderungen wie NIS2 effizient erfüllen.

**Mehrwert für Kunden durch transparente Sicherheitsarchitektur**

Transparente Sicherheitsarchitekturen und zentrale Überwachung schaffen Vertrauen und Mehrwert für Siemens Kunden.

**Effizienzsteigerung und Kostenersparnis**

Automatisierte Analysen und Compliance Prozesse sparen Zeit und Ressourcen bei gleichzeitig verbessertem Schutz.

**Zukunftssicherheit und Skalierbarkeit**

Logpoint unterstützt Siemens bei der Umsetzung skalierbarer Sicherheitslösungen, die mit steigenden Anforderungen wachsen können.