

OT-Securitymanagement für NIS2 & Co. mit IRMA® einfach gemacht:

Implementierung von IRMA® im Bereich des Kraftwerkparkes der KELAG



Die Digitalisierung kritischer Infrastrukturen wie beim Kraftwerkspark der KELAG stellt Betreiber vor neue IT-Sicherheitsanforderungen. Die Umsetzung der NIS-2-Richtlinie und die Absicherung gegen Cyber-Angriffe machen eine effektive Überwachung nötig.

„Geringer Aufwand bei gleichzeitig unmittelbarem Nutzen für den Betreiber – das war unser Fokus bei der Einführung eines neuen Tools“, erklärt Günther Joham (Anlagen-Betriebstechnik). **Die heterogene Netzwerkinfrastruktur erschwerte eine zentrale Sicherheitsüberwachung, weswegen speziell auf Effizienz und schnellen Mehrwert Wert gelegt wurde.**

Die Kraftwerksgruppe Fragant, Herzstück der KELAG-Stromerzeugung, beeindruckt durch ihre Komplexität und einzigartige Bauweise mit einem Netzwerk aus Speichern, Stollen und Kraftwerken, das sich über 700 bis 2.500 Höhenmeter erstreckt. Sie versorgt jährlich rund 225.000 Haushalte mit Strom und ist seit Jahrzehnten ein zentraler Pfeiler der Kärntner Energieversorgung.

Die Kraftwerksgruppe nutzt das Wasser der Hohen Tauern in einem europaweit einzigartigen System aus Hochgebirgsspeichern, Speicher- und Laufkraftwerken sowie einem komplexen Netzwerk aus Stollen und Beileitungen. Dieses ermöglicht sowohl die Stromproduktion als auch das Pumpen in höher gelegene Speicherseen.

Als "grüne Batterie" reagiert die Anlage flexibel auf Netzschwankungen durch erneuerbare Energien oder Lastwechsel. Ihre Fähigkeit, große Energiemengen aufzunehmen und abzugeben, macht sie unverzichtbar für die Energiewende und die Klimaschutzziele.



Systematischer Implementierungsansatz:

Die Implementation erfolgte in einem **systematischen, zweistufigen Prozess**.

„Zunächst schufen wir die Grundlagen, bevor wir in die kontinuierliche Überwachung übergingen“, erklärt Joham. „Dieser Ansatz half uns, die Komplexität zu beherrschen und den laufenden Betrieb nicht zu gefährden.“

In der ersten Phase lag der Fokus auf einer soliden Infrastruktur. „Eine einheitliche Zeitbasis ist essenziell, um alle Netzwerkzugriffe und Aktivitäten nachvollziehen zu können“, betont Joham. Die Installation eines zentralen Zeitservers bildete hierfür das Fundament.

Ein weiterer entscheidender Schritt war die Einführung der automatischen Asset-Erkennung.

„Mit dieser Bestandsaufnahme erhielten wir erstmals einen **vollständigen Überblick über alle Komponenten, Firmware-Versionen und Patch-Stände**“, so Joham.

„Wir haben nun Online einen guten Überblick, welche Endgeräte wir im Netzwerk haben und wie diese miteinander kommunizieren.“



Technische Umsetzung und Asset-Management

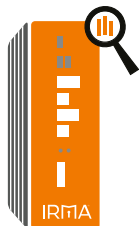
Die technische Realisierung basiert auf einer durchdachten Segmentierung der Netzwerke. „IRMA® überwacht als passiver Network Monitor unsere Systeme mit einer Kapazität von bis zu 250 Mbps“, erläutert Joham die technischen Details. „Die vier Monitoring-Schnittstellen ermöglichen uns eine granulare Überwachung aller kritischen Bereiche, ohne den laufenden Betrieb zu beeinträchtigen.“

Ein besonderer Fokus lag auf dem **strukturierten Asset-Management**.

„Diese klare Trennung ermöglicht uns eine präzise Abstufung der Sicherheitsmaßnahmen“, erklärt Joham. „**Prozesssysteme unterliegen naturgemäß höheren Sicherheitsanforderungen als administrative Systeme**.“ Die automatische Asset-Erkennung durch IRMA® XL war hierbei ein Game-Changer: „Innerhalb kürzester Zeit konnten wir eine vollständige Asset-Datenbank aufbauen. Das System erkennt nicht nur neue Geräte automatisch, sondern kategorisiert sie auch entsprechend ihrer Funktion und Kritikalität.“

Die Implementierung umfasste auch die Einrichtung spezifischer Regelwerke für jeden Standort. „**Jedes Kraftwerk hat seine eigenen Besonderheiten und Anforderungen**“, betont Joham. „IRMA® ermöglicht uns, diese individuellen Aspekte zu berücksichtigen und gleichzeitig einen konzernweit einheitlichen Sicherheitsstandard zu gewährleisten.“

IRMA®
SO EINFACH. SO SICHER!



Operative Vorteile und Planungssicherheit – eine klare Empfehlung der KELAG

„Ein entscheidender Vorteil ist unsere neue **Planungsfähigkeit**“, betont Joham. „Durch die genaue Kenntnis über End-of-Life-Daten, Wartungszyklen und Firmware-Stände können wir jetzt vorausschauend budgetieren. Ob Hardware-Tausch oder Firmware-Updates – wir haben nun alle relevanten Informationen zur Hand, um Investitionen und Wartungsarbeiten optimal zu planen.“

Die Reaktionszeit bei Sicherheitsvorfällen wurde signifikant verkürzt. „Wo wir früher Stunden oder gar Tage brauchten, um potenzielle Sicherheitsvorfälle zu erkennen und einzuordnen, haben wir heute **innerhalb von Minuten einen klaren Überblick über die Situation**“, erklärt Joham. „Das System generiert dabei keine Flut von Fehlalarmen, sondern liefert präzise, aktionsrelevante Informationen.“

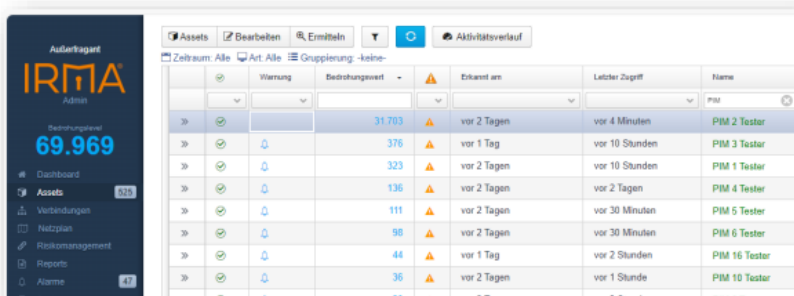
Validierung und Zukunftsperspektiven

Die Wirksamkeit der implementierten Maßnahmen wurde durch umfangreiche externe Tests bestätigt. *„Der durchgeführte Penetrationstest durch das Unternehmen CANCOM, hat die **Robustheit** unserer Sicherheitsarchitektur eindrucksvoll unter Beweis gestellt“,* berichtet Joham. *„Besonders die Integration von IRMA® XL wurde von den Sicherheitsexperten sehr positiv bewertet. Diese **externe Validierung bestätigt, dass wir mit unserem Sicherheitskonzept auf dem richtigen Weg sind.**“*

4.2 Aktivierte Anomalie-Erkennung

Alarmsysteme helfen dem verantwortlichen Team, schnell zu reagieren, sollte es zu einem Sicherheitsvorfall kommen. Das Monitoring und die Anomalie-Erkennung von IRMA bietet umgehend Informationen zum Zustand der vernetzten Automatisierung.

Im Zuge des Assessments wurde der Schwachstellenscanner, sowie mehrere Anomalien von einem Pentest erkannt.



Warnung	Betroffenes	Erkannt am	Letzter Zugriff	Name
	31.703	vor 2 Tagen	vor 4 Minuten	PIM 2 Tester
	376	vor 1 Tag	vor 10 Stunden	PIM 3 Tester
	323	vor 2 Tagen	vor 10 Stunden	PIM 1 Tester
	136	vor 2 Tagen	vor 2 Tagen	PIM 4 Tester
	111	vor 2 Tagen	vor 30 Minuten	PIM 5 Tester
	98	vor 2 Tagen	vor 30 Minuten	PIM 6 Tester
	44	vor 1 Tag	vor 2 Stunden	PIM 16 Tester
	36	vor 2 Tagen	vor 1 Stunde	PIM 10 Tester

Für die Zukunft sind bereits weitere Optimierungen vorgesehen. *„Wir werden die Sicherheit weiter stärken und gleichzeitig die Effizienz unserer Systeme optimieren,“* erklärt Joham. *„Das Ziel ist es, einen noch besseren Überblick über alle Prozesse zu erhalten und unsere Infrastruktur zukunftssicher auszubauen.“*

Fazit und Ausblick

Die erfolgreiche Implementation von IRMA® XL beim Kraftwerkspark der KELAG demonstriert eindrucksvoll, wie moderne Sicherheitstechnologie effektiv in kritischer Infrastruktur eingesetzt werden kann. „Der Schlüssel zum Erfolg lag in der systematischen Herangehensweise und der engen Zusammenarbeit aller Beteiligten,“ resümiert Joham. *„Wir haben nicht nur ein Sicherheitssystem implementiert, sondern eine nachhaltige Basis für die digitale Zukunft unserer Kraftwerke geschaffen.“*

Die Kombination aus automatischer Asset-Erkennung, kontinuierlicher Überwachung und schneller Reaktionsfähigkeit bildet ein robustes Sicherheitssystem, das den steigenden Anforderungen an die IT-Sicherheit entspricht. *„Mit IRMA® sind wir bestens für aktuelle und künftige Herausforderungen gerüstet,“* schließt Joham. *„Das System wächst mit unseren Anforderungen und bietet uns die Flexibilität, die wir in einem sich ständig wandelnden Umfeld benötigen.“*

INFOBOX: Auf einen Blick

Projektumfang

- Standorte: 82 Lauf- und 11 Speicherkraftwerke
- Jährliche Stromerzeugung: 1.442 GWh Strom
- Energiemix aus Wasserkraft, Photovoltaik und Windenergie

Technische Spezifikationen IRMA® XL

- Monitoring-Kapazität: bis zu 250 Mbps
- Monitoring-Schnittstellen: 4
- Asset-Management: bis zu 300.000 Assets
- Reaktionszeit: < 5 Minuten bei Sicherheitsvorfällen
- Netzwerksegmente: Video- und Prozessnetzwerk getrennt

Hauptfunktionen

- Automatische Asset-Erkennung
- Echtzeit-Anomalie-Erkennung
- Zentrale Zeitserver-Synchronisation
- Automatisierte Bestandsaufnahme
- Kontinuierliches Compliance-Monitoring

Erreichte Verbesserungen

- Lückenlose Nachvollziehbarkeit aller Zugriffe
- Automatische Erkennung nicht-autorisierter Aktivitäten
- Vollständige Asset-Datenbank mit Echtzeitaktualisierung
- NIS-2-Richtlinien-Konformität
- Verkürzte Reaktionszeiten bei Sicherheitsvorfällen

Validierung

- Penetrationstest durch Fa. Cancom
- Schwachstellenscanner-Analyse
- Kontinuierliches Security-Monitoring