WIRKSAMES ECHTZEIT-SICHERHEITSMANAGEMENT

von System- und Geschäftsprozesswelten im KRITIS-Sektor

Datenzentrische KRITIS-Infrastrukturen, höchste Sicherheit und Stabilität

Heutige und zukünftige OT/ICS/PIT-Infrastrukturen verzeichnen ein massives Wachstum an IP-basierenden Netzwerkinfrastrukturen und darauf betriebenen Diensten. Die zunehmende Digitalisierung, welche auf einer immer granularer werdenden Datenakkumulation und -verarbeitung (Smart Grid) sowie der Bereitstellung von Daten in Echtzeit an verschiedene Nutzer- und Interessengruppen basiert, erfordert adäquate Betriebsführungs- und Managementlösungen für diese kritischen, hochverfügbaren System- und Geschäftsprozesswelten.

Die Komplexität und der Umfang des fachlichen, technischen und organisatorischen Ökosystems nimmt stetig zu. Gleichzeitig müssen wir uns aber auch verändernden Rahmenbedingungen stellen, welche durch endliche Fachressourcen und eine weiter steigende Geschwindigkeit, bei hoher Geschäftsprozessverantwortung, gekennzeichnet sind.

Komplexität bewältigen

Wir verfügen heute über Technologien zum Umgang mit diesen anstehenden und sich verändernden Herausforderungen, welche in der Vergangenheit nur großen Serviceprovidern, Institutionen oder Forschungseinrichtungen vorbehalten waren. Werden diese Technologien und Tools sinnvoll mit einem auf die jeweilige Struktureinheit angepassten Betriebskonzept kombiniert, dann kann die zunehmende Komplexität, durch gezielte Informations- und Aufgabenzuleitung an hochspezialisierte Fachstellen bzw. involvierte Partner sowie durch intelligente Verarbeitungen, Automatismen und Visualisierungen handhabbar gemacht werden.

Häufige Umsetzungsfehler

Eigene Ziele sowie auch die Forderungen aus einem Informationssicherheitsmanagementsystem (ISMS gemäß ISO/IEC 27001, 27019 u.ä.) führen häufig, gepaart mit einem überschaubaren Personalstamm dazu, dass aktionistische, isolierte Produktentscheidungen im Hinblick auf in Kürze beizubringende Ergebnisse getroffen werden. Auch sind eigene Startlösungen, auf Basis bestehender Tools oder durch Griff in den „Open Source-Baukasten“ anzutreffen. Nach einiger Zeit werden die Defizite dieser motiviert angedachten Konzepte aber sichtbar, indem benötigte Nutzergruppen nicht einbezogen sowie entsprechende Systemkopplungen und Exportfunktionen nicht oder nur mit hohem Aufwand bereitgestellt werden können. Ein solches Projekt wird immer eine „Baustelle“ und dementsprechend unvollständig bleiben. Zudem werden Zeit- und Personalressourcen gebunden, welche mit hoher Kompetenz und Effizienz die anstehenden Betriebsführungsaufgaben der KRITIS-System- und Geschäftsprozesswelten wahrnehmen sollten. Daraus entsteht eine nicht zielführende Bindung an die defizitäre Bestandslösung, welche dann häufig, in Respekt vor einem Veränderungsprozess unvollständig und zunehmend unwirksam weiterbetrieben wird. Einen kompetenten, erfahrenen und langfristig verfügbaren Hersteller und Fachpartner hier aufgabenteilig und effektiv einzubinden, stellt das probate Mittel dar und sichert die Wettbewerbsfähigkeit.

IT-Sicherheit ist kein geschlossenes Produkt, sondern ein dauerhafter Prozess

Wir empfehlen von Beginn an, das Ziel einer Betriebsführungslösung zur Aufrechterhaltung der IT/IS-Sicherheit und Systemstabilität zu verfolgen. Dieser Ansatz wird auch als SIEM-Konzept bezeichnet. Er zielt darauf ab, eine ganzheitliche Sicht auf die Sicherheit und Stabilität der Informationstechnologie (OT/ICS/PIT), in Echtzeit zu erhalten. Ein dauerhafter und wirksamer Prozess zur Erkennung von Schwachstellen der OT-, IT- und ICS-Systeme ist herbei verpflichtend und Grundlage für ein gesteuertes Patchmanagement sowie für das Risikomanagement. Die Erkennung bisher unbekannter Bedrohungen kann durch eine SIEM-Lösung erreicht werden. Hierzu sind einige potentialreiche und nutzbringende Lösungen insbesondere für verteilte Infrastrukturen von KRITIS-Netzbetreibern und Versorgungsunternehmen verfügbar. Eine solche Lösung sollte sich an F-C-A-P-S-Funktionen (siehe Kasten unten) orientieren und die ISMS-relevanten Kernprozesse umfassend unterstützen. Damit kann ein praktikabler „Umbrella“-Management-Ansatz umgesetzt werden, mit welchem die Funktionen „F-P-S“, im Sinne eines PDCA-Konzeptes und mit einem nutzbringenden Reporting, bereitgestellt werden. Eine solche Lösung kombiniert die Funktionen Asset-Erfassung, Schwachstellen-Detektion, Monitoring, Alarmierung, Infrastruktur-Visualisierung inklusive der Generierung ISMS-relevanter Dashboards und Reports.

Begriffe

F-C-A-P-S	Fault-, Configuration-, Accounting-, Performance- and Security-Management (CCITT-Empfehlung M.30)
OT	Operational Technology (ITK-Technologie für die Steuerung und Automation), umfasst auch ICS- und PIT-Infrastrukturen
ICS	Industrial Control System
PIT	Process IT (häufig dem Leitstand nahe IT)
SIEM	Security Information and Event Management

SIEM wurde auf Grund seiner Wirksamkeit in den Referentenentwurf zum „IT-SiG 2.0“ eingebracht

Wir empfehlen das Produkt „Continuous Threat Detection“ von Claroty Inc. Es stellt eine erweiterbare, nicht intrusive Lösung für das Echtzeit-Betriebsführungs- und Sicherheitsmanagement (SIEM), auf Basis der Flow basierenden Verkehrsdatenanalyse, bereit und ist prädestiniert für sensible KRITIS-Umgebungen.

CONTROLNET

CONTROLNET GmbH
Bauhausstraße 7c, 99423 Weimar
Central: +49 (0) 3643 9085 051
Fax: +49 (0) 3643 9085 052
CRITICAL INFRASTRUCTURE PROTECTION
ENERGY | KRITIS | UTILITY | INDUSTRY
www.controlnet.de info@controlnet.de

Stand: 10-11/2020