# Cyber-Sicherheit für kritische Infrastrukturen

## (KRITIS)

Mit dem Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung von Netzwerk- und Informationssicherheit (NIS2) für kritische Infrastrukturen die für die Grundversorgung der Bevölkerung essentiell sind, werden Maßnahmen für ein hohes Sicherheitsniveau für kritische Infrastrukturen (KRITIS) definiert.

*Die im Mai 2023 vom BSI veröffentlichte Neufassung von KRITIS, spezifiziert unter anderem die Protokollierung von Netzwerkdaten (OPS.1.1.5 Protokollierung)*

WEITERE INFORMATIONEN ERHALTEN SIE VON:

Dabei müssen zur Angriffserkennung entsprechende Daten gespeichert und zur Auswertung durch geeignete Systeme bereitgestellt werden. Mit Hilfe von forensischen Untersuchungen muss eine Beweisführung, auch nachdem ein Angriff auf IT-Systeme oder Anwendungen bekannt wurde, möglich sein.

Um eine aussagekräftige Analyse durchführen zu können, ist es essenziell lückenlos alle relevanten Daten zu erfassen, zu speichern und durch eine zentrale Analyselösung auszuwerten.

DATACOM SYSTEMS INC

VIAVI Solutions

## DATENERFASSUNG

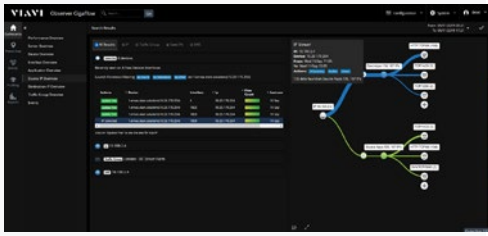
Zur Erfassung aller relevanten Paketdaten, eignen sich Aggregations TAPS, welche den Datenverkehr unterschiedlicher IT-Systeme auf nehmen und korreliert an eine zentrale Analyselösung weiterleitet.

Datacom Systems bietet dazu mit der Single Stream Lösung, die Möglichkeit 4-8 FDX Verbindungen (1-10G) zu aggregieren.

## DATENSPEICHERUNG / ANALYSE

Die **Gigastor** Hardware von Viavi Solutions ist eine Lösung zur Aufzeichnung, Analyse und Speicherung von Paketdaten, um tiefgehende und detaillierte Einblicke in die Netzwerkkonversationen zur effizienten Sicherheitsuntersuchung zur Verfügung zu stellen. Es lassen sich bis zu 1,2PB an Paketdaten ohne Verluste speichern und analysieren. Die Verschlüsselung der gespeicherten Daten (Data-at-Rest) nach AES-256 gewährleistet die Einhaltung der regulatorischen Vorgaben zum Datenschutz.

**GigaFlow** eignet sich, um die Einfallstore und die Bewegung von Angreifern im Netzwerk besser identifizieren zu können. Als Datenquellen dienen hierbei alle erdenklichen IT-Systeme. GigaFlow macht lokale Kommunikation sichtbar, auch in Netzwerkbereichen in der keine GigaStor platziert ist. Ein weiterer Vorteil von GigaFlow ist, dass ein längerer Rückblick auf Basis der Metadaten möglich ist.



Zur detaillierten Datenerfassung eignet sich die Kombination von GigaFlow und GigaStor perfekt.

VIAVI Solutions

## PROTOKOLLIERUNG / FORENSISCHE ANALYSE

Die zentrale Analyselösung von Viavi Solutions APEX, korreliert, analysiert und erstellt entsprechende Reports basierend auf verschiedenen Datenquellen, die Paket-, Meta-, Enriched-Flow-Daten. Beim Auftreten von potenziellen Sicherheitsverletzungen, versetzen effiziente Workflows die SecOp-Teams in die Lage, in kürzester Zeit umfangreiche Analysen durchzuführen und zu protokollieren.