Abu Shahid, 2022

Cyber Deterrence of Critical Infrastructure

Protecting Indian Oil

IndianOil

Why is Indian Oil as Important as it is?

- Indian Oil has a pipeline network of 90,000 kilometers and a throughput capacity of 94.56 MMT/ year for oil and 21.96 MMT/year for gas.
- It operates through 7 business divisions with most important ones being Refinery and Pipelines Division.
- Indian Oil accounts for nearly half of India's petroleum products market share.
- Indian Oil also happens to be the most profitable PSU.
- IndianOil has refineries at strategic locations for fueling the entire India

Challenges in Cyber Deterrence

- Many Critical Infrastructure use legacy systems
- Physical Redundancies are getting abandoned as reliance on virtual systems is increasing.
- Increasing reliance on IOT and mobile devices make an infrastructure more vulnerable.
- Every day, more gadgets are connecting to the internet, but there are no effective laws or governance in place

Legal Altar

- **Dealing with friendly states**: Existing Extradition Policy between the two states can be honored. Assistance can be sought from the accused country's National Cyber Law Enforcement body.
- **Dealing with neutral states**: they can be asked to cooperate in the investigation as per international treaties. A new Treaty and/or Extradition Policy can be signed if the other country meets our terms.
- **Dealing with hostile states**: India can ask other countries with vest the same interest as India to impose sanctions on the enemy state. Aggressive retaliation can be proposed.
- **Dealing with domestic culprits**: IT Act 2000, Companies Act 2013, Nist Compliances, IPC

Solution Architecture:

Securing IT Layer

- Firewalls, IDSs and IP Tables must be critically configured.
- Traffic Thresholds should be setup to reduce risk of DDoS attacks.
- Proper education program should be set in place to teach the staff about good cyber security practices.

Securing ICS Layer

- Use of Portable Storage Media should be heavily regularized.
- Air Gaps should be set in place between different divisions.
- Uni-directional gateways should be setup between IT and ICS layers.
- PLC message and signal should be authenticated for the source.

Benchmarks for Success

Protection metrics: In times of normalcy

- IP Blocks/month
- Phishing attempts averted/month
- Anomalies Detected/Month

Incident Metrics: When an attack is successful

- Number of server downtimes over the period
- Average server downtime.

THANK YOU

:)