Paris Session 2022

EThekwini Electricity experience on cybersecurity regulations and the strategy that has been implemented

D2 Information Systems and Telecommunication

PS2 : Q2.1 What experiences can be shared on the adopted cyber security standards to support migration of legacy OT protocols to IP based protocols?

Lethukuthula Gumede
(South Africa)
Presented by Thuthukani Nduduzo Biyela

Background and problem statement

- Problem:
  - EThekwini Electricity required to extend grid visibility to 800+ geographically dispersed substations where fibre communications was not readily available.
  - The business decided to leverage third party mobile networks as a TCP/IP solution to service this communication need.
- Solution:
  - Migrating to IP based protocols increased the vulnerability exposure on the OT side of the business.
  - Operational requirements of ICT solutions to secure communications traffic differed in terms of key operational objectives.
  - IEC 62351 was found to be relevant as it dealt with communication network security and more specifically for profiles that included TCP/IP for power systems.

Challenges that were experienced

- Management of VPN certificates
  - Manual effort in generating certificates for each substation proved to be cumbersome .
  - Revocation of certificates for sites that were vandalised and/or decommissioned also proved to be administratively demanding.
  - Logistics around certificate handling
- Product support
  - Vendors did not readily support the TLS protocol as specified in the IEC standard.
  - Leveraging open-source technologies as a solution may have increased the overall risk profile of the intended solution. This raised its own security concerns.
- Complying with the mandatory requirements of the specification
  - The specification called for unique requirements that were not well received by solution providers.
- Unforeseen challenges
  - The cost of mobile communication traffic is based on the amount of data transferred across the network. The use of a VPN increased the overall data overhead.
  - Incorrect parameter settings for VPN channels resulted in poor communications availability.
- Organisational factors
  - Staff had to rapidly upskill themselves to support the custom solution.
  - Contracts had to be amended to cater for unique requirements of custom solution

Lessons Learnt

- Draft Standards should be evaluated in the marketplace before being promulgated
- Leveraging open-source technologies may increase the risk profile of an organisation. This should be carefully managed.
- More guidance on configuration options should be provided within standards
- Best practices on security hardening for common OT protocols should be investigated and be made available for EPU consumption.
- It is recommended that an independent authority be established to test for EPU conformance to IEC62351-3.
- A certificate authority for machine-to-machine devices that make up the smart grid should be centrally maintained.
- The automated test tools that check for compliance with specific standards are not well developed for the OT environment.

The solution has been live since 2010. Over the years, the business has gained operational confidence in the solution and feels that it is meeting the security operational objectives set out initially