NAME : Lethukuthula Gumede
COUNTRY : South Africa
REGISTRATION NUMBER : 6760

GROUP REF. :
PREF. SUBJECT : PS2
QUESTION N° : 2.5

Question 2.5: What experiences can be shared on the adopted cyber security standards to support migration of legacy OT protocols to IP based protocols?

Problem

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. This introduced a significant security risk as critical SCADA traffic would be traversing third party owned infrastructure.

Solution

The migration to IP based protocols increased the vulnerability exposure on the OT side of the business.

We found that the operational requirements of ICT solutions to secure communications traffic differed in terms of key operational objectives. Where ICT focussed on confidentiality and integrity as key objectives, the requirements of OT are generally optimised around availability and data integrity.

The business researched applicable standards that were available to help reduce the security exposure of SCADA traffic traversing third party networks. The 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.

Within the ICT domain, typically, TCP/IP traffic is secured through VPN tunnels using the IPsec protocol as the defacto standard. The IEC62351-3 specifically recommended the use of Transport Layer Security (TLS) for OT type traffic. The reason mentioned in the standard is that OT connections are typically of longer duration than that of ICT traffic which is generally characterised as being 'bursty' in nature. TLS maintains security throughout the duration of the TCP connection much better than other protocols.

Engaging with suppliers in the marketplace viz., modem suppliers and firewall solution providers, it was immediately apparent that support for TLS in the market was not as prevalent as that of other common ICT type protocols.

This then led the business to implement an in-house open-source solution to meet the technical requirements of the IEC62351 standard.

Some of the challenges that were experienced

1. **Management of VPN certificates**

a. The manual effort in generating certificates for each substation proved to be cumbersome from and administration point of view
b. Revocation of certificates for sites that were vandalised and/or decommissioned also proved to be administratively demanding

c. Logistics around certificate handling i.e., issuing to contractors, expiry of certificates, etc. was also time consuming.

Specific processes had to be developed to handle the administration of the above.

2. Product support

a. Vendors did not readily support the TLS protocol as specified in the IEC standard. This significantly limited the product options that were available
b. Off the shelf back-end solutions were not readily available and/or supported by existing service providers
c. Leveraging open-source technologies as a solution may have increased the overall risk profile of the intended solution. This raised its own security concerns.

3. Complying with the mandatory requirements of the specification

a. The specification called for unique requirements that were not well received by solution providers.

4. Unforeseen challenges

a. 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. An exercise to understand how best to optimise the VPN parameters to reduce data overhead is currently underway.
b. Incorrect parameter settings for VPN channels resulted in poor communications availability. More guidance on the configuration of the VPN parameters should have provided in the standard.

5. Organisational factors

a. Staff had to rapidly upskill themselves to support the custom solution. This involved upskilling on open-source technologies, server administration, and general ICT skills.
b. Contracts had to be amended to cater for unique requirements of custom solution.

Whilst the initial objective of this project was to extend grid visibility to the remote terminal units in the field, an added advantage of using the VPN solution was that technically, this solution also created the opportunity for protection engineers to remotely access their relays for engineering and diagnostic purposes.

Specific learnings

a. Draft Standards should be evaluated in the marketplace before being promulgated

b. Leveraging open-source technologies may increase the risk profile of an organisation. This should be carefully managed.

c. More guidance on configuration options should be provided within standards

d. Best practices on security hardening for common OT protocols should be investigated and be made available for EPU consumption.

e. It is recommended that an independent authority be established to test for EPU conformance to IEC62351-3.

f. A certificate authority for machine-to-machine devices that make up the smart grid should be centrally maintained.

g. 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.