Dr. Mohammad M. R. Chowdhury
Senior Engineer, Cyber Security & Infrastructure
Advanced Services & Products
Process Automation – Oil, Gas & Chemicals, ABB AS
Oslo, NORWAY

Title:

Anatomy of Critical Infrastructure Protection

Abstract

The critical infrastructure of a nation provides essential services that serve as backbone of a nation's economy. The US Home Security department identifies 16 critical infrastructure sectors such as energy & utility, chemical, nuclear, healthcare, financial services and transportation, communication, manufacturing, other government facilities etc. In the critical infrastructure, the security breaches and the resulting service interruptions may cause catastrophic consequences such as environmental hazards, loss of lives, assets and reputation.

Both governments and private entities around the world are gravely concerned about the recent attack incidences on the critical infrastructure. In December 2015, major parts of Ukraine suffered power cuts following a series of cyberattacks on three local energy companies. In early 2016, a Los Angeles hospital has paid ransom to regain the access to its network which was taken down by hackers. In the past, a number of Malware/Trojan such as Shamoon, Duqu, Slammer, Stuxnet caused significant damages to the critical infrastructure. Lately Kaspersky Lab CEO Eugene Kaspersky rightly warned that cybersecurity of critical infrastructure is a 'mess' and nations must cooperate to fix it [in an interview to ZDNet published on April 15, 2016].

The security threat landscape for critical infrastructure is continuously evolving as it is moving from a stand-alone isolated network regime towards connected networks. Instead of proprietary protocols, adoption of open and common standards and protocols have made the once limited attack surface in the critical infrastructure easy to access.

No nation is immune to such cyber security attacks. Technologies are not enough to mitigate these attacks. Strong policies, awareness and continuous development of skills are also necessary. Moreover, sectors such as Industrial Automation and Control System have different requirements compare to the conventional IT systems. How can we prepare to counter all these attacks? How

can we reduce the possible impacts? This talk will shed light on some of the common holes in the systems, fundamentals of mitigation strategies and technologies, and the importance of policies, guidelines and awareness.