CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

PS2

Reducing cyber-attack actual damage by Controlled Degradation of the control system to less vulnerable network configuration and isolating infected system components

MAXIM NIKANDROV
Intelligent Grids (iGRIDS), Ltd
Russian Federation
nikandrov@igrids.ru

In the modern World, the risk of becoming a victim of cyber-attack is constantly increasing. There are many malicious by design as well as non-malicious legitimated software that can be used for malicious purposes, e.g. like remote access tools (RDP), screen capture tools, etc. Irrelevant to classification, they can be a real danger to control networks and related technological process.

One has to admit that it is not enough to protect the organization network by securing only the Control network perimeter. There are many known penetration techniques and, possibly, many unknowns that will be discovered in the future. From other hand, the nature of modern cyber defense technologies for Control networks is monitoring behavior only with very little preventative techniques. This limitation of the cyber defense technology is a result of unpredictability of industrial devices located in the Control network. They are so fragile so no one can predict their reaction on change in network traffic pattern or abrupt loss of control data stream. What can we do if even having security technologies will not help us to be more secure?

Let’s us propose a concept of "Controlled Degradation of the control system”. Concept reduction of cyber-attack damage by isolating infected system components. The core idea is similar to human body resistance to infection, and in particular, isolating infected cells from the rest of the healthy ones to save entire body. In our case, we propose to abandon some control functions or disable network communication with components that maybe infected or suspected to be compromised to reduce potential attack surface and to protect most critical assets in the Control network. E.g. we will fall back to smaller network by disconnecting or separating all unnecessary network segments if some anomaly is detected in the control network. This is the first stage of defense that can be executed by operation personnel as soon as attack is detected or as a preventive measure.

Next level is total reduction of operating units and network communication to possible minimum, necessary for the normal protection devices job functions. Most operations are done manually. Should be used in areas where serious cyber incidents are detected.

The proposing process must include 2 modes:

1. control of all physical and logical connections to the information network (not just the outer perimeter as in classical Firewall) by controlling industrial switches and IEEE 802.1x connection and MAC, IP authorization;
2. The automated fallback to pre-determined less vulnerable configuration of the control network/process when cyber-attack or suspicious behavior is detected in the control network. This should significantly reduce the attack surface, isolate and stop the infection on the earlier stage of the process, minimize damage to the control process. Although, some insignificant parts of the system may be considered as damaged/lost.

The cyber defense system, control system and the operating personnel should be well trained and be ready to act responsibly when attack is identified in the Control network.