Scada Segmentation

Cyber-threats usually refer to external attack vectors. That is why most companies with critical infrastructure (Scada) have taken the approach to separate and isolate their real-time systems environment from the IT and corporate networks.
Scada Segmentation is a search & exploit process that targets potential "cracks" in the gap between the two networks.

Overview

Over the past several years, there is a recognition that Scada systems that were previously proprietary and isolated systems are now connected to corporate networks, and many contain connection points from the Internet. It is also common knowledge now that the electronic equipment controlling critical infrastructure is susceptible to failure through DoS (Denial of Service), malformed packets, and malicious code caused by viruses, Trojans and worms.
Cyber security vulnerability assessments performed on SCADA and process control networks have exposed a pattern in the approach that many companies take in securing their critical assets.
More than 80 percent of these electric, gas, water and energy companies mentioned that one firewall or equivalent cyber defense solution between their IT Corporate Network and process control network was sufficient for maintaining the security of their critical assets under control of SCADA and process control systems.
These companies typically considered the process control network as one large black box, and tended to approach securing these environments by attempting to isolate that environment as much as possible from any other network. While this is a good first attempt and a move in the right direction, there are additional cyber security solutions that should be taken under consideration given modern external and internal threats facing these critical assets that are connected through Ethernet and Internet-routable protocols.
Usually Scada network architecture have enterprise network (used for all the enterprise purposes), DMZ (used as a gateway from the enterprise network to the operational network) and operational network (used for Scada devices)

The Scada Segmentation Service

CybeRisk's experts will attempt to access the operational network from the enterprise network simulating a malicious user or an external attacker.

This service is performed as a "Grey Box", where CybeRisk's experts will have operational network credentials and without knowledge about the network architecture. The service includes:

- Enumerating the users of the operational network.
- Target machines within the operational network
- Identify active connections between enterprise network and operational network.
- Scan the DMZ / operational network (only with client permission)
- Use the operational network users' machines to access the operational network / Use vulnerability to access the operational network directly.

About CybeRisk

CybeRisk Security Solutions ("**CybeRisk**"), a Finjan Company (NASDAQ: FNJN), was founded in 2015 to deliver global advanced Cyber Risk and Security Advisory Services.

CybeRisk services range from strategy level down to highly technical and tactical consulting. Those services are backed by a suite of advanced Attack & Penetration, Defense Optimization, and diagnostic services to customers globally.

By bridging the gap between current cyber security and cyber risk practices, **CybeRisk** offers organizations an integrated cyber risk management process that aligns the processes of management, security and risk into one business-centric framework.

CybeRisk's comprehensive array of advanced services combine leading methodologies from across the cyber security and cyber risk spectrum in order to offer our customers a single, multifaceted process for the remediation of cyber risk and the management of cyber security.

For more information and/or a free consultation call, please contact inqueries@cyberisk.biz