Preventing a Stuxnet like Attack on Indian Soil

Rishabh Arijeet

Indian Institute of Technology Kanpur

Abstract

Critical infrastructure protection is vital to the day-to-day operation of any country, and those systems need to be protected to the fullest extent possible. Cyber security can be referred to as the protection of data and systems in networks, both wired and wireless, from unauthorized access or attack.

Having an advanced nuclear system is important for national security. Hence, countries are spending billions of dollars for gaining momentum in their nuclear plans. But as nuclear power is proving to be authoritative, the nuclear system is becoming prone to cyber-attacks. Over the past twenty years, five deadly cyberattacks compromised the national security in five countries. Not only affecting the internal security of any country, but cyberattacks have proven perilous for the privacy of the citizens. As new technological innovations are permeating the industry, the incidence of security breaches and possibility of cyberattacks has heightened. That's why scaling-up cybersecurity in nuclear institutes and models, become important.

A cybersecurity breach has several implications. Due to a cyber malware, the confidential documents associated with cyber security can be leaked. It can increase the vulnerabilities of nuclear systems. With a disrupted nuclear system, the adversaries can take advantage by corrupting the communication, and preventing the flow of information. Moreover, cyber-attacks are a direct threat to the integrity of any nation.

In September 2019, the cyber-attack at Kudankulam Nuclear Power Plant only exposed the dearth of cyber-security management in India. The attack was caused by the DTRACK Virus, which was developed by a group of hackers from North Korea. It was a direct attack on the administrative framework of India and was confirmed by ISRO. The confidentiality of a large amount of data was threatened due to this attack.

In nuclear power plants, assessments of cyber security are critical to ensuring the safe and reliable operation of the systems used. And the biggest threat today is STUXNET.

The Stuxnet virus set off alarm bells all over the world when it was discovered in 2010. Many observers viewed this unprecedented cyber-attack on a nuclear facility as the dawn of the age of cyber war - “the keystroke heard ’round the world.” Stuxnet also had significant implications for nuclear security. The attack revealed a troubling reality: in the future, cyber weapons could be used against nuclear facilities to achieve consequences far more serious than those observed at the Natanz uranium enrichment facility in Iran.

Stuxnet was an extremely precise weapon deployed against a highly secure facility for a very limited purpose. At no point were human lives or the environment in danger. However, this will not always be the case. With the code for Stuxnet now widely available online, it may only be a matter of time before a group intending to cause harm deploys a less discriminate weapon against a less secure, higher-consequence target like a nuclear power plant or nuclear materials storage facility.

Introduction

The reliance on digital technologies in modern weapons systems – particularly in nuclear weapons systems – has led to growing concerns that cyberattacks may pose additional risks at a time of escalating conflict, which could undermine the confidence needed to make reliable decisions. Cyber risks in nuclear weapons systems have thus far received scant attention from the nuclear weapons policy community. The potential impacts of a cyberattack on nuclear weapons systems are enormous. Data hacks can reveal sensitive information on facilities’ layouts, personnel

details, and design and operational information. Cyber interference could destroy industrial control systems within delivery platforms, such as submarines, causing them to malfunction. In addition, clandestine attacks could be conducted on targeting information or operational commands, which may not be discovered until the point of launch.

As defined by the International Atomic Energy Agency (IAEA), nuclear security is "the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities." [1]

So, if such an attack happens on a nuclear power plant in India, it may lead to another world war and who knows what. Stuxnet also had significant implications for nuclear security. The attack revealed a troubling reality: in the future, cyber weapons could be used against nuclear facilities to achieve consequences far more serious than those observed at the Natanz uranium enrichment facility in Iran. In this paper, we discuss how to prevent such a Stuxnet-like attack on Indian soil.

Methodology and Assumptions

Methodology

This paper is based on the problem statement that Many Critical Infrastrucure entities are managed by PLCs which runs on Windows OS and this is a paper to be submitted to NCIIPC detailing how to prevent a Stuxnet like attack on India's soil.

This is a mixed data type research paper which means the research done used both qualitative as well as quantitative data from secondary sources i.e. using secondary data. Since this paper has taken into consideration all the available data about an attack like Stuxnet , this is the most suitable approach for preventing the attack. Since new technologies are constantly evolving , in no way, this research assures 100% relevance and accuracy after a good amount of time.

For the quantitative and qualitative study purposes, sources have been taken from the official research papers provided in the problem statement.

Research methods include content analysis: categorizing and discussing the meaning of words, phrases and sentences

Assumptions

The power plant uses Cyber Physical System (CPSs) with

main components SCADA, DCS and PLC.

- The PLCs are controlled by computers with Siemens

  SIMATIC WinCC/Step 7 controller software.

- Internal hard drive in a computer and/or USB storage devices

  are acceptable ways for staff to do their work.

- The process control network (PCN) and control system

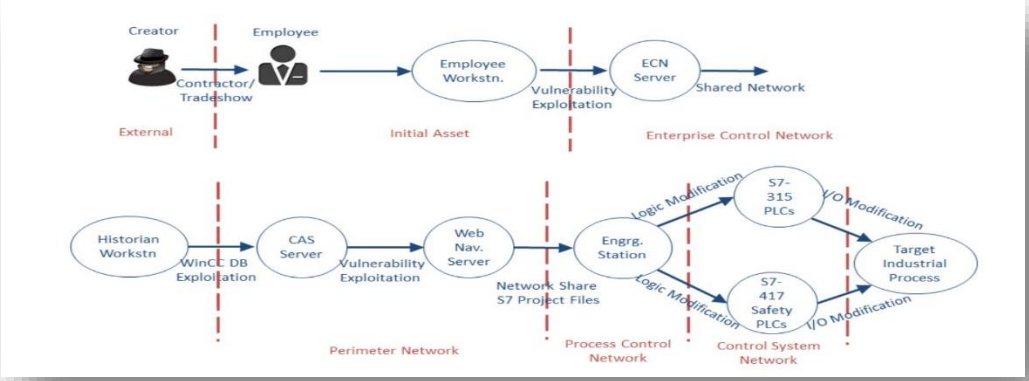
network (CSN) are hosted in the same security zone.

- The nuclear facility is located away from the central hub and

professionals. It is required that a proper security system is

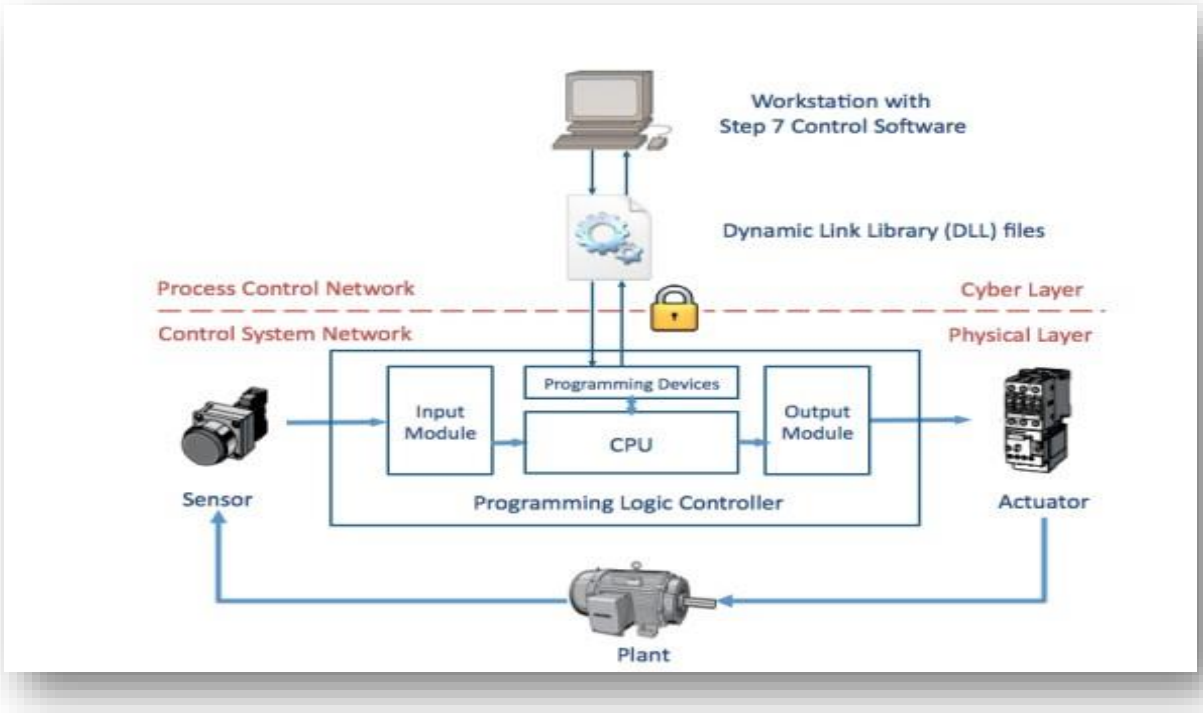
established.

Mechanism of Stuxnet



The Stuxnet worm leverages known and previously unknown vulnerabilities to install, infect and propagate, aiming to sabotage industrial processes operated by Siemens SIMATIC WinCC and PCS 7 control systems. Figure above uses an example sequence of attacks to illustrate how the worm propagates through the enterprise control network (ECN) to the control system network (CSN). The worm first propagates via infected removable drives (such as flash drives and external portable hard disks), and then local area network communications (such as shared network drives and print spooler services), and finally infects Siemens project files, including both WinCC and STEP 7 files, which are used to program the PLC.

In conventional ICS network architectures, the process control network (PCN) and control system network (CSN) are hosted in the same security zone. The PCN hosts plant operators on their human-machine interface (HMI) workstations. The CSN is dedicated to traffic specifically related to automation and control such as traffic to and from PLCs. This has created potential security hazards for CSN once the worm penetrates the perimeter network and PCN since no firewalls are used to separate the two networks.



The figure above illustrates the interactions between PCN and CSN. The connection between the PCN and CSN is managed by a library file, which calls different routines to read and write to memory on the PLC. By replacing the library files, Stuxnet can tamper with commands from the PCN without being detected by the PLC or system operator, since there are no integrity checks used to verify the source of a message. In the 2010 Iranian Natanz nuclear facility incident , a function block DP_RECV for receiving network frames on the Profibus, a standard industrial

network bus used for distributed I/O, is replaced by a malicious block. Each time the function is used to receive a packet, the malicious Stuxnet block takes control and does post-processing on legitimate packet data, hence affecting the PLC and the control system.

Cyber Deterrence Challenges

The issue with creating cyber deterrence in this case, as opposed to deterrence in the traditional domains of warfare, is that cyber weapons are not displayed. In many cases, cyber weapons remain secretive projects known only to their creators. Without the ability to showcase weapons and capabilities, true deterrence cannot be generated. Nation-states may believe their enemies do not possess the ability to retaliate or attribute cyber-attacks and thus the nation appears weak to that form of warfare. By not displaying cyber capabilities, there is a small level of deterrence between nation-states created in that nations may assume other governments have better capabilities than they actually have. In the same way, though, a nation-state may inaccurately assume itself superior to another. Stuxnet left no doubt that a pair of nation-states possessed unprecedented cyber power.

A deterrence strategy depends on the ability of a state to restrain an opponent by threats, coercion, or incentive. There is a great deal of debate on whether the nature of threats in cyberspace can actually be deterred and whether we are considering applying a strategy that works well in the nuclear domain to an entirely different type of threat. Some of the challenges to the idea of cyber deterrence are discussed here.

Attribution is perhaps the biggest challenge. Nations must be clear about the identity of the perpetrator of a cyber-attack so that their counteractions are not

misdirected. This is not easy because locations can be spoofed, identities hidden, and the nature of cyberspace ensures that attacks can be launched from any geographical location. In addition, false flags could be used to deceive or misguide attempts to identify the attackers. The 2018 Winter Olympic Games opening ceremony in South Korea was hit by a cyber-attack that resulted in the official website being taken offline for 12 hours. *The Washington Post,* quoting intelligence officials, reported that the hacking was done by Russian spies who tried to make it look as if North Korea conducted the intrusion.[7]

Even if hacking groups are identified as belonging to a particular country, it is often not possible to prove that they are state-sponsored. Where the fingerprint of a state is found, there could be a reluctance to openly declare this because it could compromise intelligence operations. However, any hesitation to respond would weaken both credibility and deterrence.

Another challenge to cyber deterrence is the uncertainty of the effect. Nuclear deterrence worked because the capabilities of each side were known, as was the destructive potential of atomic weapons. National cyber capabilities are zealously guarded, and there is no certainty about how a cyber response would impact the adversary.

There is also the danger of unintended collateral damage. A joint U.S.-Israeli cyber-attack on the Iranian Uranium enrichment facility at Natanz started in 2009.

Although the malware, now known as Stuxnet, was designed to affect only the Siemens supervisory control and data acquisition systems at Natanz, it spread beyond its intended target. It is estimated that Stuxnet infected more than 200,000 computers around the world. NotPetya, considered the most devastating cyberweapon, is widely assessed as having been launched by a Russian state group called Sandworm. While it primarily targeted Ukraine, NotPetya disrupted businesses and supply chains worldwide, causing approximately $10 billion in damage. These considerations surrounding the uncertainty of effect could sometimes delay decisions on taking cyber deterrence actions.

Deterrence is a strategy based on the threat of use of force and fails if force is applied. Fischerkeller and Harknett contend that cyber deterrence is not a credible strategy because cyberspace is perpetually contested. They write, “The combination of interconnectedness and constant contact with cyberspace’s ever-changing character… encourages operational persistence in order to secure and leverage critical data and data flows.” They suggest that “in operational reality, operational persistence/engagement (not operational restraint)” is the “appropriate strategic choice."

‘Cyber persistence ’as defined by Fischerkeller and Harknett, is "a strategy based upon the use of cyber operations, activities and actions (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in

cyberspace”. They feel that this will “allow greater freedom of maneuver to impose tactical friction and strategic costs." Whether cyber persistence can also be considered a component of deterrence is open to interpretation.

Notwithstanding these challenges, the absence of a clear deterrence strategy could result in continuing cyber attacks from hostile players with impunity. According to Indian government data presented in the Parliament, nearly 1.16 million cases of cyber attacks were reported in 2020, up almost three times from 2019 and more than 20 times compared to 2016. This trend is likely to continue.

In crafting a cyber deterrence strategy, India will have to start almost from scratch. A 2013 Cyber Security Policy exists (and is now being updated), but it is a set of general guidelines. A cyber deterrence strategy will have to lay down a specific action plan to respond primarily to state-sponsored attacks that threaten national security.

LEGAL AND TREATY

Cyberattacks pose a growing threat to the integrity of sectors that are critical to our economic and social well-being. Cybersecurity threats have increased by over 358% in recent years, outpacing societies’ ability to effectively prevent or respond to them. There is an urgent need for cooperation between government and business leaders to align global cyber regulations that safeguard data and privacy.

To create a cyber-secure world, we must be as fast and globally integrated as the criminals. Facing a global threat with local resources will not be enough. Countries need to do more internally and internationally to coordinate their efforts.

However, a global cybersecurity and privacy regulations – while well-intentioned and seeking to contribute positively to the daily onslaught of emerging cyber threats – give limited consideration to harmonization between countries. The result, unfortunately, is discordant and confusing, like each section of an orchestra playing in a different key.

There are three areas where global harmonization of cybersecurity regulations could make us safer and enhance our access to innovative products and services:

1) Developing Consistent and Enhanced data protection

- Global standards ensure a common understanding of requirements rather than jurisdictional interpretations of law.
- Consistent application of data protection methods and procedures reduces risk and builds trust across borders and supply chains.
- Data duplication can be minimized by having fewer national data residency laws – less data proliferation means lower risk of data compromise.

2) Increasing Innovation and Interoperability

- Global inclusion is fostered when technical hurdles are lowered, allowing more interoperability.
- Inclusion feeds innovation by engaging the great minds and entrepreneurs around the world to participate in the global technological ecosystem.
- Interoperable architectures enable and facilitate privacy and security by design.

3) Reducing Cost

- Alignment with global standards will reduce the complexity of implementing security and privacy controls.
- Compliance exams could be streamlined through standard artifacts that meet the needs of all interested parties.
- The need for costly data residency requirements driven by security or privacy will be lessened.

CYBERSECURITY ASSESSMENT AROUND THE GLOBE

- The Convention on Cybercrime or the Budapest Convention, 2001

The Convention on Cybercrime or the Budapest Convention is the first international treaty which seeks to address the issue of Cyber Crime. It was drafted by the Council of Europe along with active participation of Canada, Japan, South Africa and the United States of America. It is the only legally binding international instrument on this issue. It was opened for signature in Budapest from 23 November 2001 and it entered into force on 1 July 2004. The convention was formed with an aim to harmonize national laws, improving investigative techniques, and increasing cooperation among nations. It acts as a guideline for any state developing national legislation against cybercrime. India has not adopted the convention and declined to ratify it as it was not a participant in its drafting.

- Internet Corporation for Assigned Names and Numbers (ICANN)

It is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

- International Telecommunication Union (ITU)

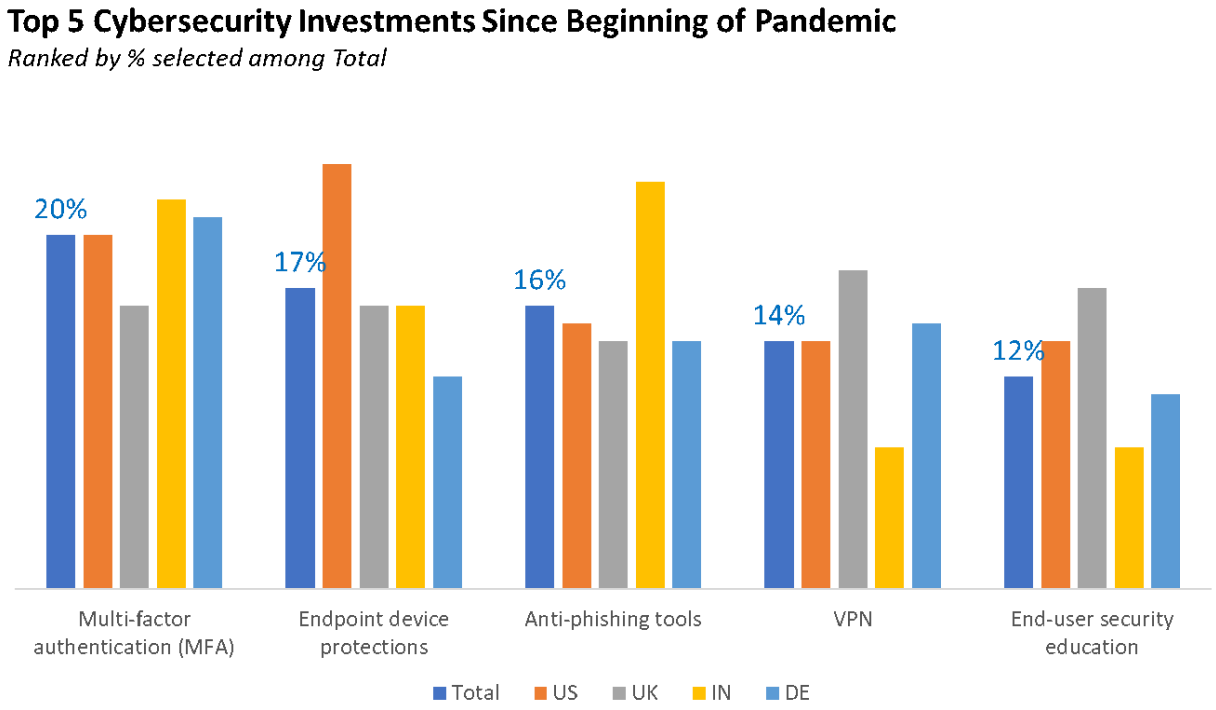
UN, to ensure connectivity in communication networks around the globe, established a body which would facilitate international connectivity in communications networks, develop the technical standards that ensure networks and technologies seamlessly interconnect and strive to improve access to ICTs to underserved communities worldwide, thus International Telecommunication Union (ITU) came into picture.

CYBERSECURITY INVESTMENT AROUND THE WORLD

The U.S. government spends $19 billion per year on cyber-security but warns that cyber-attacks continue to evolve at a rapid pace.

The rising tide of cybercrime has pushed information security spending to more than $86.4 billion in 2017.

But in India, two out of three companies spend less than 5% of their IT budget for beefing up their cyber security.



Solution Architecture

The methods for improving utility security to be covered are as follows:

● Restrict the use of USB media & other portable storage devices and enforce encryption of sensitive data

● Air gap control system networks where possible and restrict connection points to other networks using specialized firewalls and/or one-way data transmission devices

● Utilize a rigid and methodical procedure for moving code to and from production networks and control systems

● Make use of a dedicated source code management system for control system/PLC code allowing for version control and rollback to a known good version when unexpected/undesirable behavior occurs after a modification is made.

Even with the methodical application of defense in depth techniques and the thorough implementation of information security best practices, protecting systems from an advanced targeted threat such as the Stuxnet worm is a challenge for even the most skilled information security practitioners. Protecting critical infrastructure against a persistent and highly skilled adversary is extremely difficult at best and perhaps (arguably) impossible given enough time, expertise, and knowledge of the target environment.

Restriction of Portable Storage media

One possible method for risk reduction for portable storage media is to use WORM (write-once read many) storage for backups. For example, the use of DVD discs would be one method of accomplishing relatively safe backup storage from the control system network. Data stored on key assets could be burned to DVDs from one or more of the computers on the control system network and then the backup DVDs could then be taken off-site for storage.

Another possible procedure for minimizing the risks introduced by the use of USB storage media would be to perform a low-level format of all USB devices on a stand-alone computer running a boot-able operating system such as Knoppix Linux. A PC or laptop running a version of Knoppix (or another boot-able Linux distribution) is a technique used by a number of organizations for sensitive financial transactions and also by information security professionals to avoid the possibility of using a malware infected computer/operating system for performing certain computing activities in a secure manner. Once a USB or CD/DVD disc is created from an ISO image downloaded from a trusted/known good source repository the ISO can be validated using an MD5 or SHA-1 checksum to ensure the operating system image has not been tampered with. Then when a system is booted from the disc or USB drive that was also formatted fresh before making it bootable, the system can be trusted for use in formatting portable USB memory devices such as a hard drive and/or a flash memory stick/thumb drive. After formatting is complete the device(s) can be used on control system computers knowing that extensive precautions have been taken to minimize risks introduced by portable storage media.

Air Gap Control System Networks

The use of air gaps as a means of protecting systems and devices by separation from other systems and/or networks has been used for decades as a security precaution. Air gaps by definition are just what the name implies – separation from other networks and the risks and threats introduced by network connectivity. Network-borne and/or Internet-based threats can cause compromise of mission-critical software and/or hardware necessary for the uninterrupted delivery of utility services including electricity and clean water to homes and businesses as well as the transfer of waste water to treatment/processing facilities. Methods used to spread malicious software to victim systems include the use of compromised websites, email via file attachments or website links, or from one infected computer to another via wired or wireless networks including the Internet. Such methods have been utilized for nearly as long as systems have been inter-connected.

Precaution taken by Stakeholders and Employees

As in other cybersecurity practice, policy and procedures that are communicated and enforced effectively are one of the most significant methods necessary for protecting utility control systems. All of the mitigating controls and state of the art defense-in-depth gear in the marketplace today will not prevent a serious incident from occurring if we as utility employees and stakeholders do not take the appropriate level of caution and due diligence in our day-to-day work that directly impacts ICS and SCADA systems, devices and related/connected equipment. While beyond the scope of this paper, employee security awareness training and the precise,

methodical, repeatable implementation and enforced adherence to security-minded human behavior cannot be underestimated.

Securing the ICS/SCADA Systems

Securing network connectivity points and protecting control systems/networks through implementation of strictly configured firewalls and unidirectional security gateways are both useful methods for strengthening ICS security.

Unidirectional Security Gateways (given by Waterfall)

An extensive and broad base of solutions all utilizing their proprietary one-way diode technology to secure sensitive systems for implementations where air gaps are not possible and/or feasibly practical. The software and hardware operate a specialized fiber optic network that strictly controls the transmission and receiving of datagrams/packets. Using this approach, security concerns with regard to the protocol implementation and design of Ethernet and TCP/IP are avoided. Using one-way diode and/or patented fiber-optic communication technology, the gear handles the low-level network flow control, and the software takes care of everything happening on the wire; including but not limited to the OSI layers as well as offering completely customizable configuration of the application stack (Waterfall, 2013).

Using Specialized network gear

This method is used to secure the SCADA installations throughout the power plant using secure Ethernet switches with built-in firewall/VPN to reliably connect and safeguard SCADA equipment from “insider” attacks. Ruggedized Ethernet switches use highly secure firewall to monitor application traffic and stop unauthorized and potentially damaging activity.

Integrated firewall on each port provides a network-based distributed security solution equivalent to the use of personal firewalls on each system in the network, with service-aware inspection of traffic in every end-point and role-based validation of SCADA flows. It provides full security functions in a single switch: Service validation, remote access, inter-site VPN and access control.

Encryption of Data

The use of encryption for storage media is an inexpensive method for securing data. Three readily available methods include a PROTECTING CRITICAL INFRASTRUCTURE AGAINST THE NEXT STUXNET 31 commercially available USB flash drive product such as Iron Key which features AES 256-bit hardware encryption (Imation, 2013). Microsoft provides full-disk encryption known as BitLocker for Windows 7 and Windows 8. BitLocker provides either 128-bit or 256-bit AES encryption, and on systems with a supported TPM chip further security measures are available for key storage (Microsoft, 2012). A third option is to use properly vetted free and open-source encryption software such as TrueCrypt, which has been approved by cryptography expert Bruce Schneier. TrueCrypt has a wide variety of choices for encryption methods including AES, Twofish, and Serpent algorithms (TrueCrypt, 2013).

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and

event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Machine Learning for ICS Security

Specially designed IDSs use machine learning algorithms to detect threat activities that are anomalous to a particular system, using algorithms for pattern recognition. There are other IDSs, which use signature-based systems to compare the activities to a database of known threats (Yasakethu and Jiang, 2013; Maglaras and Jiang, 2014; Dua and Du, 2011). These functionalities can be combined together for a robust detection system and will provide a sufficient layer of protection for various attack scenarios.

Benchmarks for success

What does success look like when trying to prevent a cyber warfare attack on a critical infrastructure?

Cybersecurity never sits still. While you may have created a program that addresses the current cyber threats towards your organization, the chances are that it will not stay that way. New threats emerge, new techniques and technologies are put into play by cyber criminals.

PERFORMANCE METRICS:

The correct set of cybersecurity performance metrics will support the cybersecurity program, and help the organization make the right decisions when it comes to the future of the program. Tracking cybersecurity performance metrics over time will give early warning when tools or controls are no longer effective, when new tools need to be considered, or when additional resources are needed.

Below are just some examples of the many metrics that can be used to create a balanced report that will benefit the cybersecurity program.

- Average time to patch vulnerabilities – When vendors release security updates, how long does it take to update software? Delays to applying security patches leaves the organization open to cyber-attack through a known vulnerability. Best practice is to apply patches fast, and when patches are not available, to virtually patch in the interim.

- Number of systems with known vulnerabilities – Some systems may have known vulnerabilities. Knowing how many systems have known vulnerabilities, and what the vulnerabilities are in each system will enable your organization to manage risk.

- Mean time to detection – The longer it takes to detect attacks, the more damage attackers can cause. Average dwell time has dropped to 24 days, a significant improvement from 56 days in 2020, but it is still time for attackers to cause significant damage. The aim is to get as close to zero as possible.

- Cost per incident – Cyber incidents cost money, man hours, loss of productivity, and more. This cybersecurity performance metric will provide a picture of the resources used to clear up each incident. The aim is for this figure to be as low as possible.

What does success look like when under a cyber warfare attack?

An organization's impact measurements are used to monitor the potential impact of a cyber security breach and the damage conducted to organizational assets (both tangible and intangible assets). The key to maintain a high level of performance in regards to impact measurements is to manage the fallout from the breach effectively.

For successful assessment you need to ask questions like Total value of assets defended against a cybersecurity incident (Note: This is triggered only after a vulnerability is identified) and Total damage from cyber incidences including damage to assets and time to recovery.

What does success look like when asked to launch an offensive?

SUCCESSFUL CYBERATTACK

Exercising command and control:

The attacker can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees.

the hacker can lock a company’s IT users out of the organization’s entire network if they want to, perhaps demanding a ransom to restore access designating a successful attack.

Achieving the hacker’s objectives

Not all hackers are after monetizable data or incriminating emails that they can publish. Some simply want to cause chaos or to inflict pain on a company. Execution of the motives of the hacker is a sign of a successful cyberattack.

References

1. https://acehacker.com/microsoft/cybersecurity/resources/An-Impact-Aware-Defense-against-Stuxnet.pdf
2. https://acehacker.com/microsoft/cybersecurity/resources/After-Stuxnet-Acknowledging-the-Cyber-Threat-to-Nuclear-Facilities.pdf
3. https://acehacker.com/microsoft/cybersecurity/resources/Protecting_Critical_Infrastructure_Against_the_Next_Stuxnet.pdf
4. https://acehacker.com/microsoft/cybersecurity/resources/The-History-of-Stuxnet.pdf
5. https://unidir.org/sites/default/files/publication/pdfs//understanding-nuclear-weapon-risks-en-676.pdf
6. https://www.linkedin.com/pulse/how-do-you-measure-success-cybersecurity-gary-manley-ma-pmp/