Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

Ready to respond? A look at continuous risk analysis in cyber security plans for nuclear power plants.

Fleurdeliza de Peralta
Pacific Northwest National Laboratory
Richland, WA, USA

Kim Lawson-Jenkins
U.S. Nuclear Regulatory Commission
Rockville, MD, USA

ABSTRACT

Nuclear power plants (NPPs) that implement strong security measures to detect suspicious network activities and effective strategies to respond upon detection of a cyber incident can help minimize the consequences of malicious activity involving software exploited through the supply chain or software vulnerabilities. Recent software compromises, such as the 2020 SolarWinds Orion attack and the 2021 attacks at a U.S. water treatment facility and major pipeline operator, did not directly target or affect the nuclear facilities. However, analysis of such attacks should be incorporated in continuous threat and vulnerability management processes implemented at NPPs within their cyber security plans. These events demonstrated how timely detection of malicious activity and effective mitigations can minimize the impact to an organization. This paper discusses the different security measures identified in U.S. Nuclear Regulatory Commission (NRC) cyber security guidance and international cyber security standards for nuclear facilities that could assist NPP operators with preventing, detecting, and responding to these types of malicious activities involving software and vendor services.

INTRODUCTION

A cyber incident could be the result of accidental or intentional acts by actors that are internal or external to the affected organization. The threat actor could also be motivated to infiltrate the information and operational technology systems in a nuclear power plant (NPP) for various reasons, such as making a political statement, interrupting energy infrastructure, impacting an organization's operation or financial business, or gathering data by surveilling organization's routine and systems operation. Since 2001, organizations have increased awareness of cyber security in nuclear power plants and have implemented comprehensive cyber security measures to protect from potential cyber threats. Vulnerabilities in legacy systems and development of new techniques by cyber actors have introduced new types of cyber threats to nuclear power plants. Recent cyber incidents, such as the compromise of the Solar Winds Orion software, the unauthorized remote access of water treatment facility's control systems and the ransomware inserted into a major pipeline operator's network, have demonstrated that threat actors are still successful in infiltrating an organization's systems. This paper discusses vulnerabilities exploited by the cyber threat actor in recent cyber incidents, the importance of vigilant awareness of cyber security vulnerabilities, and elements of an NPP's cyber security program (CSP) that would be effective in preventing and mitigating similar incidents. This paper specifically discusses CSP protections applied to devices that affect safety, security, and emergency preparation (SSEP) functions at an NPP. Cyber security attacks on NPPs devices that may affect the business network and non-SSEP energy production are not addressed in this paper.

INSIGHTS FROM RECENT CYBER INCIDENTS

Cyber threat actors are continuously devising sophisticated ways to hack into an organization's network for nefarious purposes. The events leading to recent cyber attacks provide insights on tactics and techniques used by the threat actors [18]. The events provide an opportunity for NPP licensees to assess the effectiveness of their cyber security program (CSP) and identify any vulnerability of digital assets based on assessing the tactics and techniques used by the threat actors to compromise a network. The cyber incidents discussed in this paper highlight the importance of managing cybersecurity risks associated with the supply chain, unauthorized access and malware.

SolarWinds Orion Software

SolarWinds develops software for businesses to help manage their networks, systems and information technology infrastructure. In December 2020, FireEye, a cybersecurity company and one of their customers, discovered malicious activity while investigating a compromise of their own network. Investigations determined that an advanced persistent threat (APT) actor inserted malicious code into SolarWinds' Orion platform creating a backdoor that was later used to access a customer's networks. Upon insertion of the software update, the malicious code infiltrated the networks of over 18,000 organizations, including U.S. government agencies, private sector organizations, and critical infrastructure entities [1][17]. A smaller subset of the affected organizations then became a target for follow-on exploitation [15]. Initial investigations determined that the Orion software may have been compromised in March 2020; however, forensic evidence indicated that files associated with the attack were compiled as far back as December 2019 [16]. The compromise went undetected for several months allowing the APT actor to create new accounts with privileged authorizations [1]. The cyber incident resulted in issuance of an emergency directive that required affected agencies to take immediate actions, such as forensically imaging system memory and/or host operating systems, analyzing stored network traffic for indications of compromise, disconnecting or powering down the software product from their network, isolating affected networks, and re-installing data from back-up storage sites [1][7].

APT actors or groups have the expertise, resources, and patience to access an organization's network and can remain undetected for an extended period [8]. The compromised software update allowed authentication to be bypassed, so that an APT actor could continue to execute unauthenticated Application Programming Interface commands [16]. With the "privileged access," the APT actor was able to obtain sensitive, but unclassified communications and identify other opportunities to compromise the IT supply chain [17].

Cybersecurity experts have assessed the incident and recommended methods to mitigate the impact of a similar attack in an organization's supply chain, such as continuous monitoring and intrusion detection of the organizations network [16]. Other security practices that would reduce the risk of this type of attack is applying the principle of least privilege and implementing continuous awareness training on threats posed by visiting untrusted websites or following links from unknown or untrusted sources, such as hypertext links contained in emails or attachments [16]. Other proactive security measures include improving security of cloud environments and endpoints (e.g., servers and workstations), increasing data analytics, and increasing situational awareness of intrusion threats and real-time identification of malicious cyber activity [17].

Water Treatment Facility

The water treatment facility in the city of Oldsmar, Florida, provides drinking water to the local community. In February 2021, unidentified cyber actors obtained unauthorized remote access to the supervisory control and data acquisition (SCADA) system of the water treatment facility [2]. The adversaries exploited cybersecurity weaknesses, including poor password security to remotely access a desktop sharing software that was running on an outdated operating system. The threat actor was able to manipulate plant system, such that dangerous levels of sodium hydroxide could have resulted in the drinking water [2]. Fortunately, the malicious activity was immediately detected by plant personnel knowledgeable in system operations who corrected the system changes and mitigated the attack before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change [2]. Cyber criminals have targeted and exploited desktop sharing software and computer networks with end-of-life status to gain unauthorized access [2].

In this incident, an outdated Windows operating system enabled a cyber actor to find an entry point and leverage the remote desktop protocol (RDP) exploits [2]. Continuing the use of outdated operating systems introduce a vulnerability because the software may no longer be supported by the developer (e.g., Microsoft) [2], Cyber actors will exploit known weaknesses to older operating systems. Security measures that could be taken to reduce the risk associated with RDPs include auditing the logs and network for systems that use RDP, closing unused RDP ports, applying multi-factor authentication, and logging RDP login attempts [2]. Without proper security measures, remote access tools could be used to control computer systems and drop files into the compromised computer. Other good security practices include isolating computer systems with outdated operating systems, using strong passwords, using properly configured fire walls, and using up-to-date anti-virus and spam filters.

Colonial Pipeline

Colonial Pipeline manages the largest pipeline system in the United States, which carries gasoline and other refined oil products to supply the east coast. In May 2021, malicious actors gained unauthorized access to the company's IT network and inserted a ransomware, which forced the fuel pipeline company to temporarily shut down operations and freeze its network [14]. Colonial Pipeline proactively disconnected certain OT systems to ensure the system's safety, as there was no indication that the threat actor moved laterally to the OT systems [14]. The attack vector on this critical infrastructure's network is still being investigated to determine the vulnerability in the system. Adversaries accessed the organization's network through a virtual private network account that was no longer in use and inserting a ransomware [11]. This incident impacted the availability of a critical infrastructure and resulted in the development of new cybersecurity requirements for critical pipeline owners and operators.[9]

With nuclear power contributing 20% of our nation's electricity capacity [3], a cyber attack impacting an NPP would not only affect a critical infrastructure but could potentially result in a radiological consequence if the intrusion affected safety systems that were designed to shut the plant down and maintain the fuel in a safe condition.

CONTINUOUS MONITORING AND RISK MANAGEMENT AT U.S. NPPs

In 2021, the NRC completed inspection of the fully implemented CSP at all licensed NPP in the United States. Implementation of a cyber security plan protects CDAs that perform SSEP functions at an NPP. The NPP operator's assessments of identified CDAs - including information regarding attack surface, attack pathways, vulnerabilities, and threats – provide the basis for selection of security controls applied to the CDAs or to the environment in which the CDAs operate. The security controls applied by the CSP are required to implement defense in depth protections that will ensure the capability to detect, respond to, and recover from cyber attacks. Once applied, the security controls should be continuously monitored for effectiveness. Implementation of continuous monitoring is an element of a CSP that supports timely detection of a cyber attack as required by 10 CFR 73.54 (e)(2)(i). This overview of a CSP implementation process is illustrated in Figure 1.

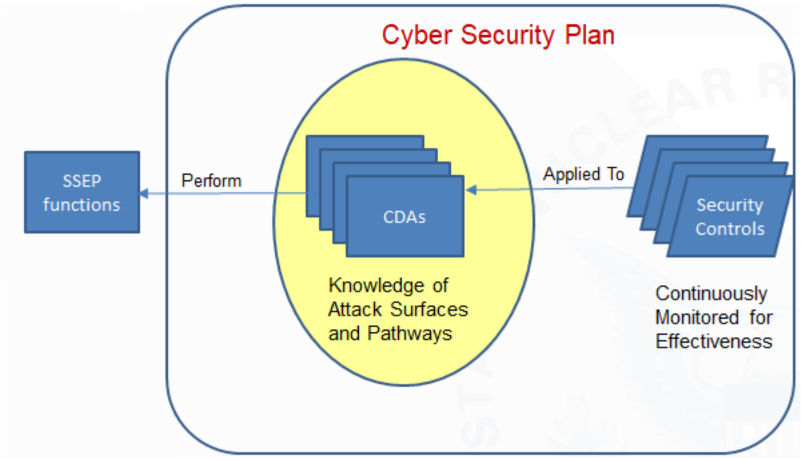
Cyber Security Plan
SSEP functions
Perform
CDAs
Applied To
Security Controls
Knowledge of Attack Surfaces and Pathways
Continuously Monitored for Effectiveness

Figure 1. Mapping CSP Effectiveness to SSEP Function Protection

Continuous monitoring (generation of log data and audit records) and assessments (review and analysis of data and records) ensure that the implemented security controls remain in place and that changes in the system, network, environment, or emerging threats do not diminish the effectiveness of these controls, processes, or procedures. Implementation of security controls in NRC-approved CSPs address protection of the five attack pathways for CDAs – physical presence, wired communications, wireless communications, portable media and mobile devices, and supply chain. Additionally, NPP operators have established and documented procedures for screening, evaluating, mitigating, and dispositioning threat and vulnerability notifications received from credible sources.

Dispositioning includes possible changes in the implementation of security controls to mitigate newly reported or discovered threats and vulnerabilities. These changes - documented in a corrective action program – are implemented with the goal of maintaining adequate defense-in-depth protection and to prevent CDA compromise or exploitation.

Specific cyber security controls to monitor login activities, directory access, changes to security services, baseline configuration changes, and other activities identified in recent notable cyber attacks are contained in the RG 5.71 [4] and NEI 08-09 [6] Appendices and are implemented in U.S. nuclear power plants' CSPs. Threat monitoring activities required in CSPs include

- Contact with selected security groups to remain informed of newly recommended security practices, techniques, and technologies and to share current security-related information, including threats, vulnerabilities, and incidents
- Use of credible information sources to receive prompt information about security threats and vulnerabilities and the use of that information to take prompt and appropriate action to mitigate any potential security effects to CDAs.
- Adjustment of monitoring tools and techniques as threat agents constantly change and adapt their tactics to circumvent defenses and countermeasures; adjusting the events to be audited within the CDAs based on current threat information and effectiveness analysis of the security controls.

INCIDENT RESPONSE AT U.S. NPPs

In the instance of a cyber security attack affecting a CDA, the NPP operator must notify the NRC in accordance with the provisions of 10 CFR 73.77 [19]. A cyber security event must be reported within the timeframe specified in 10 CFR 73.77(a). In addition, consistent with the requirements stated in 10 CFR 73.54(e)(2), the NPP's CSP must include incident response and recovery measures by describing how to accomplish the following:

- Maintain the capability for prompt detection and response to cyber attacks.
- Mitigate the consequences of cyber attacks.
- Correct exploited vulnerabilities.
- Restore affected systems, networks, and equipment associated with safety, security, and emergency preparedness functions affected by cyber attacks.

As of July 2021, no NPP licensee has notified the NRC of a cyber attack affecting a CDA. In the unlikely event of a cyber attack affecting CDAs, a nuclear reactor may always be shut down and maintained in a safe shutdown condition until the affected CDAs have been repaired.

All CSPs contain development, documentation, and deployment of policies and associated implementing procedures to address contingency planning and the NPP's ability recover from a cyber security attack as required by 10 CFR 73.54 (c)(2). Contingency planning includes testing and drills to verify the effectiveness of the contingency plan, CDA backup procedures, and mechanisms with supporting procedures that allow CDAs to be recovered and reconstituted to a known secure state following a disruption or failure. These contingency plans should be verified using CDAs associated with safety, security, and emergency preparedness functions as all of these areas could be subjected to cyber security attacks.

CONCLUSIONS

NPPs are considered among the most secure of our nation's critical infrastructure. However, recent high profile cyber attacks on critical infrastructure, such as water and fuel, have raised concern with the security at all critical infrastructure facilities. Malicious actors successfully gained access to the affected organization's networks by exploiting weaknesses within critical infrastructure and/or systems. Investigation of these incidents identified that malicious actors exploited vulnerabilities involving the organization's supply chain security and management of assets, accounts, and access. These types of cyber attacks, however, could be mitigated by CSPs implemented at U.S. NPP licensees. Use of one-way data diodes and implementation of effective portable media and mobile device security protect the critical systems and digital assets from cyber attacks. The NPP operators perform monitoring of CDAs and the effectiveness of their CSP implementations to maintain the capability for timely detection and response to cyber attacks. Threat monitoring activities include incorporating knowledge of attackers TTPs and anomaly detection within their CSP defensive strategy. Continuous monitoring of critical systems should look for indicators of attack such as exfiltration of data, privilege escalation, execution of new and unknown processes, and unusual communication between processes. Execution of CSP incident response drills, exercises, and backup CDA procedures prepare the licensees to respond to and recover from cyber security attacks. NRC licensees of NPPs completed full implementations of their CSPs in 2017 and the NRC recently completed inspections of these CSP implementations. The CSP implementations provide assurance that the NPPs are ready to respond to evolving threats and malicious cyber activities.

REFERENCES

[1] DHS. 2021. Department of Homeland Security. Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise,* dated December 13, 2020 accessed on February 15, 2021 from https://cyber.dhs.gov/ed/21-01/

[2] Cybersecurity & Infrastructure Security Agency (CISA) Alert AA21-042A, *Compromise of US Water Treatment Facility,"* released on February 11, 2021, accessed on February 15, 2021 from https://us-cert.cisa.gov/ncas/alerts/aa21-042a

[3] U.S. Energy Information Administration, "FAQS - What is U.S. electricity generation by energy source?" Last updated: March 5, 2021, accessed on June 7, 2021.

[4] U.S. Nuclear Regulatory Commission, "Protection of digital computers and communication systems and networks," Web page. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html, accessed June 11, 2021.

[5] U.S. Nuclear Regulatory Commission, "U.S. NRC 2019–2020 Information Digest," August 2019, https://www.nrc.gov/ML1924/ML19242D326.pdf .

[6] Nuclear Energy Institute 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, April 2010.

[7] M. Miller, "Officials say executive order with a 'dozen actions' forthcoming after SolarWinds Microsoft breaches," dated March 30, 2021, The Hill, Washington D.C.,

accessed on June 25, 2021 at https://thehill.com/policy/cybersecurity/545631-officials-say-executive-order-with-a-dozen-actions-incoming-after

[8] Cybersecurity & Infrastructure Security Agency Alert, AA20-352a, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure and Private Organizations," dated April 15, 2021, accessed on June 25, 2021 at https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[9] Cybersecurity & Infrastructure Security Agency, "Pipeline Cybersecurity," Accessed on June 25, 2021 at https://www.cisa.gov/pipeline-cybersecurity-initiative .

[10] Cybersecurity & Infrastructure Security Agency, "Ransomware Guidance and Resources," Accessed on June 25, 2021 at https://www.cisa.gov/ransomware .

[11] Cybersecurity & Infrastructure Security Agency Fact Sheet, "Rising Ransomware Threat to Operational Technology Assets," Accessed on June 25, 2021 at https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf .

[12] Cybersecurity & Infrastructure Security Agency, "Supply Chain Compromise," Accessed on June 25, 2021 at https://www.cisa.gov/supply-chain-compromise.

[13] National Institute of Science and Technology Report, "Defending Against Software Supply Chain Attacks, Cybersecurity & Infrastructure Security Agency," dated April 2021, Accessed on June 25, 2021 at https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf .

[14] Cybersecurity & Infrastructure Security Agency Alert, AA21-131a, "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks", revised May 20, 2021, accessed on July 6, 2021 at https://us-cert.cisa.gov/ncas/alerts/aa21-131a .

[15] CISA Insights, "Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders; accessed on July 8, 2021 at https://www.cisa.gov/sites/default/files/publications/CISA_Insights_SolarWinds-and-AD-M365-Compromise-Risk-Decisions-for-Leaders_0.pdf .

[16] Center for Internet Security, "The SolarWinds Cyber-Attack: What You Need to Know", updated March 15, 2012, accessed on July 6, 2021 at https://www.cisecurity.org/solarwinds/.

[17] Letter from U. S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA) to United States Senate, the Honorable Ron Wyden, dated June 3, 2021

[18] MITRE ATT&CK for Industrial Control Systems Web page https://collaborate.mitre.org/attackics/index.php/Main_Page accessed on June 7, 2021

[19] U.S. Nuclear Regulatory Commission, "Cyber security event notifications," Web page. https:// https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0077.html, accessed June 15, 2021.