CyberTalk.org

Critical National Infrastructure, Cyber Security Preparedness

TABLE OF CONTENTS

INTRODUCTION

For any nation, attacks on critical national infrastructure pose an all-to-real, deeply disturbing cyber security threat. When critical national infrastructure experiences disruptions, national economies can collapse, lives are acutely affected, and our social fabric is degraded.

Attacks on critical infrastructure systems have the potential to impact access to drinking water, availability of energy, transportation modalities, financial accounts, healthcare, fire brigade availability, and other essential services that affect the quality of everyday life for hundreds of millions of people. To convey the gravity and gruesomeness of infrastructure attacks, infrastructure attack consequences include extreme physical duress and loss of life.

Cyber attackers frequently plan and execute compromises against critical infrastructure and control systems, although the vast majority of them are stopped and the issues solved. These attackers generally intend to curry political favor, gain financial advantages or simply wish to engender destruction.

In 2021, nearly **90%** of US-based critical infrastructure entities experienced attempted ransomware attacks, according to the US Federal Bureau of Investigation (FBI). "It's a dismal and harrowing reality," wrote *Fortune Magazine*.[1]

Nearly 90% of US-based critical infrastructure entities were hit with ransomware attacks in 2021.

Many existing infrastructure security systems lack the capacity and capabilities to effectively control for attacks in our current hyper-connected and demanding infrastructure ecosystems. Industrial control systems, such as SCADA, Programmable Logic Controllers (PLC) and Distributed Control Systems pose some of the greatest unprecedented risk.

The way in which we approach national cyber security strategy development and resilience planning must change. Organizations need to evolve their technology management best practices, work across government agencies and private groups, and implement stronger risk management solutions in order to safeguard critical national infrastructure systems

[1] The U.S. is Overdue for a Dramatic Shift in its Cybersecurity Strategy – but Change is Finally Coming, Fortune, Andrew Rubin, September 19, 2022

RECENT CRITICAL NATIONAL INFRASTRUCTURE EVENTS

The Water Industry

In the United States alone, there are as many as 70,000 separate water utilities, which encompass both potable and wastewater systems.[2] A large number of these operations are small, use older infrastructure, and have limited resources for cyber security investments. As a result, water systems both in the US and elsewhere are chronically under-protected.

The need to rehabilitate water infrastructure is urgent. In a well-known example, in 2021, the water treatment facility in Oldsmar Florida, a town of 15,000, experienced a security breach involving a hacker who attempted to poison the drinking water with lethal levels of sodium hydroxide. An administrator identified the issue and alerted authorities, but effective and rapid assessment of this type of sinister behavior is not guaranteed.

> More than 1,100 ransomware attacks have hit critical infrastructure systems to date.[3]

The Energy Sector

Global energy infrastructure is uniquely vulnerable to cyber attacks on account of the fact that networks include both physical and cyber infrastructure, and involve a large number of distributors, suppliers, storage facilities, other third-parties and assets, many of which are scattered across multiple countries.

The May 2021 attack on Colonial Pipeline exemplified how cyber attackers could leverage a single compromised password to stop the flow of fuel across an entire section of a country. The fuel disruption resulted in reduced third-party business services, promoted panic buying among motorists and increased the price of gasoline.

When pipelines shut down, the lights can go out, natural gas wells can stop operating, an entire economy can lose momentum, and people lose access to goods and services. Ultimately, Colonial Pipeline paid nearly $5 million to ransomware attackers in order to regain access to systems.

---

[2] U.S. Water Supply System Being Targeted by Cybercriminals, Forbes, Jill Magill, July 25, 2021

[3] www.securityweek.com/university-project-cataloged-1100-ransomware-attacks-critical-infrastructure

Log4j

Towards the end of 2021, a vulnerability in a commonly used software code library, known as Log4j, rocked and shocked the engineering and cyber security worlds. As you probably know, the implications of this vulnerability were far-reaching. Still today, the vulnerability persists in some systems and it continues to present a threat.

Since its discovery, Log4j has resulted in several relatively minor critical national infrastructure attacks. Experts believe that advanced hacking groups have already compromised intended infrastructure victims and are simply waiting for IT departments to relax defenses before triggering a large-scale disruption.

DYNAMIC TRENDS

Targeted Sponsored Attacks

As geopolitical tensions escalate, authoritative entities from around the world are urging critical infrastructure network defenders to prepare for and mitigate potential threats. State-sponsored entities have previously proven their ability to compromise IT networks, maintain persistent access to resources, exfiltrate sensitive data, and disrupt critical control systems.

According to the Cybersecurity and Infrastructure Security Agency (CISA), the US government, the government of Canada, and the UK government, SVR cyber threat actors were responsible for the large-scale supply chain attack known as SolarWinds Orion, which affected dozens of US government agencies, critical infrastructure groups and private sector firms around the world.[4]

Possible state-sponsored cyber threats could include destructive malware, ransomware, DDoS attacks, intellectual property theft and espionage.

Broadly speaking, contemporary trends indicate that organizations need to take significantly more initiative when it comes to protecting the critical technologies that power governments, economies, livelihoods and lives. Winning cyber battles requires that organizations engage in proactive cyber security planning - developing multi-layered cyber prevention, defense, detection and remediation systems.

[4] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, CISA, April 20, 2022

PREVENTION

1 **Design phase.** If possible, critical national infrastructure organizations should consider security during the design phase of the critical infrastructure components. The reality is that a lot of architecture is legacy, and that this isn't always possible, but brand new initiatives should address cyber security from the get-go.

2 **Visibility.** Critical National Infrastructure organizations can start cyber security acceleration initiatives by increasing visibility into systems and data. Organizations that lack visibility into networks and processes will struggle to ensure security of systems. By leapfrogging this security fundamental, and focusing on more complex security concepts or architecture, well-intentioned efforts to modernize security architecture are liable to fail. Further, security programs will not return an optimal level of value.

3 **Inventory assets.** It's impossible to protect something if you don't know that it exists. Maintain a real-time inventory of all network assets, allowing security teams to pursue comprehensive visibility efforts into devices, connections, communications and protocols.

4 **Conduct simulations.** Rehearse and improve responses to cyber crises, including ransomware attacks. Simulations are most beneficial when they include third-parties, law enforcement, key customers and suppliers. Within simulation scenarios, decision-makers should discuss when to isolate or shut down network components, and whether or not to communicate with hackers.

5 **Partnerships.**.Critical infrastructure partnerships can significantly enhance understanding of the current threat landscape and assist with knowledge transfers around the finer details pertaining to securing cyber and physical resources. Perspectives from relevant stakeholders within partner groups can help shape security decisions in positive ways.

6 **Qualify vendors.** Ensure that the infrastructure vendors you work with or wish to work with can provide robust, consistent security and offer transparency around vulnerabilities in their products. This is critical for effective resilience. Ideally, government regulations would require a thorough evaluation and inspection process for all technologies deployed within critical infrastructure organizations.

7 **Secure remote access.** Cyber attackers can use drive-by malware, credential theft, multi-factor authentication fraud and a host of other easy options to compromise or deceive one of your remote employees. Take steps to secure remote access. These include providing employees with VPNs, securing remote access gateways and portal servers, and isolating remote work environments for organization-issued, third-party controlled and BYOD client devices

8 **Zero trust.** A zero trust approach offers a way to implement access controls. In the U.S., government agencies are required to achieve certain zero trust goals by the end of the fiscal year 2024, highlighting the utility and efficacy of zero trust.[5] Consider a zero trust architecture that includes a built-in Privileged Access Management solution.

9 **Conduct simulations.** Critical national infrastructure networks are comprised of thousands of OT and IoT devices from an assortment of different vendors. The vast majority of these devices lack the security needed for the CNI environment. In turn, organizations should leverage tools that identify system vulnerabilities to determine which devices are at risk. Updates should be installed as-needed.

10 **Endpoint security.**.Your endpoint security should function autonomously, and should be able to prevent unauthorized access without manual patches or updates. It really goes without saying, but focus on endpoint solutions that have been rigorously tested and that meet the highest standards

[5] How Zero Trust Can Stop the Catastrophic Outcomes of Cyber Attacks on Critical Infrastructure, Technative, July 3, 2022

DEFENSE

1 **Detection capabilities.** Detection and response for industrial environments is complex. Ensure that your organization retains detection and response capabilities that are specifically tailored to industrial environments. Implement security tools that can detect the full range of potential threats, that can provide analytics information allowing for strong risk-mitigation decisions, and deploy automated tools that augment the capabilities of existing resources, including administrators. Update tools as needed to ensure that your teams can keep pace with the latest threats.

2 **CDR.** Consider a Content Disarm and Reconstruction (CDR) solution, which deconstructs and reconstructs files as they travel across a network. The technology extracts the legitimate code from a file and then builds a new, functional and malware-free version of the file. The original file, along with any malware within the file, is quarantined or destroyed.

3 **Innovative ecosystem.** To continually prevent and defend against cyber security threats, your technology leaders must continually innovate within and adapt the existing cyber security ecosystem to meet emerging challenges, become more competitive and, of course, to keep hackers at-bay.

4 **Insights from MITRE.** The MITRE ATT&CK Framework aims to remove ambiguity and provide common vocabulary for defenders who are combatting attacks. MITRE provides extensive details around the exact steps and methods that hackers use for specific attack types, and describes possible remediation processess.

5 **NIST standards.**.Continue to follow standards and guidelines outlined by the National Institute of Standards and Technology (NIST) in order to implement and operationalize stronger resilience measures.

6 **Hire and train.**.Ensure that your organization has well-defined roles and responsibilities; an important element within an emergency. In addition, upskill and cross-train staff members, enabling them to perform tasks that are adjacent to current roles. Lastly, provide exceptional employee training that prevents employees from accidentally creating new vulnerabilities.

EXPERT INTERVIEW HIGHLIGHT

Deryck Mitchelson, Field CISO of the EMEA Region for Check Point Software

Combatting critical infrastructure threats and adversaries is tough. Determining where to start revising and upgrading your existing approach can be even more challenging. Discover what one of Check Point Software's experts has to say on the matter...

Deryck Mitchelson is the Field CISO of the EMEA region for Check Point Software. Previously, he served as the digital director for NHS National Services Scotland, and he has been named one of the UK's most influential CIOs.

See the complete article here.

The interconnected age

Attacks against Critical National Infrastructure are not new. From disrupting water supplies in besieged Constantinople during the 14th century, to the strategic Allied bombing campaign of WWII, throughout history, adversaries have continually used critical infrastructure as means through which to harm perceived opponents during times of political conflict. What is new is that critical infrastructure is more interconnected than ever before, increasing cyber security risk and complicating security measures.

Interconnected infrastructure sectors that are not bound to the same security policy requirements may be at risk of cascading cyber attack effects. The deliberate and malicious modification of data belonging to the water system, for example, could affect firefighters' abilities to respond to catastrophic fire events. Conversely, malicious modification of data belonging to firefighters could lead to poor or inaccurate decisions around regional water distribution. While interconnectivity can proffer new opportunities, if managed incorrectly, it can also create unnecessarily difficult outcomes.

The industrial IT/OT risk

If we look beyond cross-sector interdependencies, within individual industrial sectors, the convergence of Operational Technology (OT) and Information Technology (IT) massively intensifies cyber security risk. Historically, OT systems were designed with isolation in mind, operating a limited number of software programs, if any at all. Power stations were entirely isolated; requiring physical security alone. Gradually, isolated power stations were connected to one another. Today, OT systems are often connected to Information Technology networks, making these legacy systems uniquely vulnerable to an advanced generation of cyber security threats.

CASE STUDIES

UNITEL

As a first step, CISO Deryck Mitchelson recommends getting the visibility piece right.

While working to secure telecommunications company Unitel, Cybersecurity Analyst Dialungana Malungo highlighted the utility and effectiveness of this recommendation, drawing on his real-world experiences.

Unitel is a mobile telecoms and Internet provider with a 70% share of the Angolan market.

After adopting a centralized management, total visibility solution, the company is now better able to manage remote users and to create granular security rules for different user groups.

"You cannot protect what you cannot see," he says. "Check Point gives us visibility into our infrastructure. With Check Point, we're confident we can protect ourselves against emerging cyber security attacks."

Learn more here.

SINOPEC

For Sinopec, future-proofing security infrastructure represented a core business priority. The company set out to obtain unrivaled network protection, secure remote access, enhanced visibility and greater security control.

By using management software blades, such as SmartView Monitor, Sinopec centrally monitors all of its Check Point devices to get a complete visual picture of changes to gateways, remote users, and security activities. This enables administrators to immediately identify changes in network traffic flow patterns and to stop malicious activity.

Established in July 1998, China Petrochemical Corporation (Sinopec Group) is a large petroleum and petrochemical enterprise founded on the basis of the former China Petrochemical Corporation.

"...any disruption is unacceptable. The Check Point 12407 security appliance is the foundation for our network security strategy and provides us with reliable, high-performance protection in a scalable, integrated package." – Sinopec group spokesperson

Learn more here.

CONCLUSION

Threats to critical national infrastructure are increasing. Make the best decisions possible and optimize your cyber security strategies, tactics, and systems.

Pursuing the prevention and defense recommendations included in this e-book could literally help keep the lights on, the water systems running, or the mobile phones charged – for your enterprise, your clients, and your nation's general population.

Ensure that your organization creates a robust, scalable cyber security foundation that not only meets current needs, but that can also combat the cyber security threats of the future.

For more information and resources to ensure the integrity of OT and ICS environments, click here.

Discover more executive-level insights on CyberTalk.org.

Lastly, to receive cutting-edge cyber security news, insights, best practices and analyses in your inbox each week, sign up for the CyberTalk.org newsletter.