Is CADR on Your RADAR?

Critical Infrastructure Operators Gain Actionable Knowledge of their OT Environment's Gaps

Ransomware attacks—and cybersecurity attacks in general—continue to dominate the headlines. According to a report released by SonicWall, a provider of advanced cybersecurity solutions, 2021 is an ominous signal that ransomware is here to stay as the attack vector-of-choice for threat actors looking to make money and cause disruption. Through September 2021, SonicWall logged around 500 million attempted ransomware attacks, a 148% increase as compared to 2020, projected to rise to 714 million attempts by year-end. Critical infrastructure operators have become a high-value target for ransomware attackers. Attacks on critical infrastructure not only provide revenue opportunities, but also a platform for invoking societal and political chaos, disrupting everything from supply chains to destabilizing currency.

Critical Infrastructure Operators were not Prepared to Handle Cyber Attacks

Recently, a number of high-profile ransomware attacks on critical infrastructure have occurred in manufacturing (Acer), food processing (JBS Foods), and energy pipeline operations (Colonial Pipeline) resulting in supply chain disruptions, financial losses, increased costs passed on to consumers, and a general destabilization of society that relies on dependable and predictable delivery of goods and services. In the largest-ever attack on an American energy system, the Colonial Pipeline hack rattled our collective consciousness of the potential effects of ransomware. The ensuing disruption in gasoline supplies invoked a throw-back to the energy crises of the 1970's where gas rationing had anxious consumers waiting in long lines on their designated day to purchase a limited quantity of fuel. Colonial Pipeline supply shortages resulted in sharp price increases and forced some panicked consumers into hoarding behaviors, buying as much fuel as possible and storing it in containers ill-suited for transporting a flammable liquid. And worse yet, they paid the attackers $4.4 million in bitcoin ransom, some of which the FBI later recovered. And why did this happen?

Post-attack reports point to poor cybersecurity hygiene practices that exposed the password to an old virtual private network (VPN) account, providing remote access to the company's servers. The account was not subject to two-factor authentication, thereby failing to further protect unauthorized use by an attacker. As a result, for a company that supplies nearly half of the fuel consumed on the East Coast, Colonial was forced to shut down parts of its operations to contain the threat. And it raised the question: what other vulnerabilities exist in energy systems that could result in similar or worse outcomes?

New Security Directives from Regulatory Agencies in Focus for 2022

Shortly after the Colonial hack, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) announced a series of security directives aimed at requiring owners and operators of TSA-designated critical liquids and natural gas pipelines to assess their cybersecurity exposure and implement several urgently needed protections against cyber intrusion. In their press release, the TSA specifically itemized requirements to review current practices, identify gaps, and develop remediation plans to address the gaps. This is especially relevant for critical infrastructure operators. Alongside traditional information technology (IT) environments, operators employ operational technology (OT) assets and networks that for example, control the flow of pipelines, automate the manufacturing process, and manage the cleaning and filtering of wastewater—and just about anything that uses hardware and software to monitor and control industrial equipment. Collectively, these assets and networks, sometimes referred to as the Industrial Control System (ICS), are target-rich environments that are game changers when attacked.

CADR: Going Further than a Standard Cybersecurity Assessment

The TSA directives point to a regulatory environment that is inching closer to mandatory cybersecurity requirements. This means that critical infrastructure operators must be adept at proactively assessing the cybersecurity posture of their OT environments, identifying gaps, and developing remediation plans. This requires

not only a review of cybersecurity practices but an in-depth critical review of how the OT environment is designed, architected, and implemented. And this is key to evaluating an organization's true exposure to ransomware and other attacks. Why? Because OT environments are complex. Their design is typically more evolutionary and additive, rather than starting from a clean sheet of paper. Many of the deployed digital assets are vendor-sourced, employ legacy technologies, and may come out-of-the-box with security limitations and vulnerabilities. And, it may be difficult if not impossible to shield these environments from the potential hazards of the Internet, especially if there isn't effective separation between the OT network and the traditional IT, Internet-facing network. Given the cybersecurity challenges posed by OT environments, finding the inherent weaknesses is paramount to mounting an effective defense against intrusion. Enter the Cybersecurity Architecture Design Review.

A Cybersecurity Architecture Design Review, or CADR, positions critical infrastructure operators to gain actionable knowledge of their OT environment's gaps. In short, the CADR process examines the design, implementation, operation, and resilience of the OT environment, including interaction with the IT environment, to not only fend-off attacks but to quickly respond and recover from attacks when needed.

CADR was Designed for Industrial Control Systems and Operational Technology

In collaboration with 1898 & Co., Axio has established a CADR assessment process built on reputable assessment methodologies and consistent with the recommended controls in NIST Special Publication 800-82 Guide to Industrial Control Systems Security. This process provides stakeholders with a clear evaluation of alignment to the TSA's security directives while establishing a baseline on which to build effective defense-in-depth strategies to improve the security posture of the OT environment. But the CADR assessment goes further than traditional assessments: in addition to reviewing current practices and controls, testing is performed to substantiate the effectiveness of these controls. This provides operators a real-world view of how well their cybersecurity strategy is actually performing.

The Core Components of a CADR Assessment

The assessment comprises four key components: a network architecture review, a system configuration and log review, network traffic analysis, and a comprehensive NIST-based controls review.

The network architecture review is the CADR core activity. Using available network artifacts (such as network diagrams, asset configurations, and third-party connections) the review extends across the organization's network boundaries—IT, OT, wireless, and emerging technologies such as SD/WAN—providing a comprehensive and holistic picture of the network's exposure to attack.

Complimentary to the network architecture review, the system configuration and log review is a deeper dive into the security configurations for critical assets that comprise the IT and OT environments. Because poor cyber hygiene is a major (and fixable!) contributor to poor attack resilience, practices for system hardening, patching, configuration management, and remote asset management are forefront. System log analysis is performed to identify suspicious activity that could exploit such gaps, including where unauthorized configuration changes may have been made. And because log analysis is only as good as the logs that are collected, the review focuses on the comprehensiveness and relevance of existing log collection activities.

To provide a real-time view of the environment's controls-in-action, network traffic analysis is performed to inform stakeholders about perceived or known anomalous activity or threats that affect critical assets. Using tools that monitor and collect network traffic data, activity is reviewed to establish desired traffic patterns, identify anomalous behaviors, and identify sources of undesirable traffic, further substantiating the effectiveness of current controls.

Finally, leveraging the NIST 800-82 Guide, the Axio/1898 & Co. team conducts interviews with key stakeholders to establish that leading practices for securing industrial control systems are in place as recommended. Identified gaps are examined with respect to the potential impact on the organization's cybersecurity posture and prioritized for improvement.

Supporting Critical Infrastructure to Ensure Optimal Resilience

While the regulatory environment is certainly evolving toward more mandatory directives for critical infrastructure security and resilience, the incentives for performing a CADR far outweigh any compliance requirements coming down the road. The ability to identify and understand key gaps, prioritize improvements, and test resilience under controlled conditions is an investment worth serious consideration. For risk managers, the decision is even more clear: investing in critical gap remediation before an attack far outweighs the potential cost of business interruption, lawsuits, fines and legal penalties, loss of life or injury, and reputational damage. For organizations in target-rich industries that are heavily dependent on industrial control systems to meet their mission, the investment might mean the difference between a minor inconvenience and major, costly disruption. And for some companies, that difference may decide whether they continue in business at all.

If you'd like to learn more about the CADR assessment and how to get started today, please contact us at sales@axio.com.