21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2017 Grid of the Future Symposium

Cybersecurity Strategy – Active Defense

J. PACK
POWER Engineers, Inc.
USA

SUMMARY

As today's industrial control systems (ICS) become more connected and intelligent, the security threats and risk correspondently rise. This shift in ICS design and implementation requires a strategic shift in how ICS are protected and defended. Active defense measures including an increased focus on situational awareness is required to provide our ICS with a fighting chance of survival during an attack. Operational information and analysis to provide views different than traditional network and system security monitoring are required. Data analytics will play an increasing role in active defense, including predicting cybersecurity incidents and providing a head start in defending the ICS.
This shift in strategy will take time and resources, so good planning is critical for success. Use tools from the North American Electric Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST) to help plan the overall action plan and ensure that all levels of executive management understand the change and support the effort. The result should be a cybersecurity organization that is prepared for the dynamic nature of threats and vulnerabilities, with the structure to detect, respond and recover when bad things happen.

KEYWORDS

Cybersecurity, Strategy, Defense, Situational Awareness.

jeff.pack@powereng.com

History

As cybersecurity has progressed as a profession over the past thirty years, there has been a general approach [1] to developing an effective cybersecurity program. The process starts with understanding the scope of the overall program. Normally, the first step is an inventory of all systems and devices that fall within scope and the cybersecurity posture of each device or system. Next, most organizations perform or contract with a consultant to perform an initial cybersecurity risk assessment, based on one of several risk frameworks commonly used in the industry. Once the inventory and overall risk assessment is complete, a list of gaps and opportunities for improvement is developed, and then prioritized with the budget and resources available in the organization. Finally, continuous monitoring and testing determines if the risk posture has improved.

As the cybersecurity program matures, the cycle of assessment, implement, test and monitor is ongoing. This includes an occasional audit or regulatory compliance exercise to keep the organization alert and test for the ability to get the most out of the available budget and resources.

Threats Change

Through all of these cycles, the threats to the organization have changed from the assumptions made in the original risk assessment, with the greatest amount of threat change currently focused on ICS [2]. Mostly obscure compared to information technology (IT) systems, ICS are responsible for monitoring and operating critical infrastructure such as electric power, natural gas, water, sewer and transportation. ICS have been targeted in several nation-state attacks in recent years against the electric grid in Ukraine, and the success of those attacks has spawned a new family [3] of malicious code focused on ICS for the electric power sector.

Strategy Shift

In order to adequately prepare and recover from the dynamic threat changes, organizations with critical infrastructure ICS need to review their strategic direction for cybersecurity and ensure that they are dedicating budget and resources to the proper areas. The ICS of even ten years ago does not resemble where future ICS are moving [4]. The advent of virtualization and increasingly powerful hardware has enabled the software-defined world of ICS. In this world, all devices are connected with high speed networks and the analog world of CT/PT interfaces to the electrical protection system are replaced by digital merging units and sampled values. Widespread connectivity of increasingly intelligent end devices dramatically increases the complexity of ICS and, in turn, the ability to defend and protect the ICS [5].

Preventative controls such as access control, network traffic controls, authentication and authorization are effective and necessary. However, they are limited in their ability to defend against the current and future threats faced by modern software-defined and interconnected

ICS. These threats use multiple mechanisms to bypass the preventative controls and move directly into the system, including zero day exploits (previously unknown vulnerabilities in operating systems and applications), network traffic obfuscation and other attack methods.

In general, the ability to detect intruders on a network is becoming more and more difficult because of these new attack methods. The overall sophistication and capability of the attackers is increasing exponentially because of disclosure of advanced tools and techniques from nation-states [6]. Detection avoidance intelligence and techniques are becoming more commonplace in the ICS attacker space.

Cybersecurity programs need to shift towards more active defense controls and start implementing self-defending ICS applications and hardware. As the end devices become more intelligent, they also need to increase their ability to defend and sound alarms or alerts when malicious activity is detected. This effort will take time and investment, but we are starting to see related movement in the ICS space with software defined networking, where Ethernet switches are driven by very specific instructions and not just moving packets between switch ports.

It's also important to note that cybersecurity programs need to have a relatively stable and mature stance towards cybersecurity risk management for this shift in strategy to be successful. If a cybersecurity program is still struggling to implement the top five Center for Internet Security (CIS) Critical Security Controls [7], the shift towards active defense should be delayed until the program is able to identify scope and maintain an accurate configuration management system, including vulnerability assessment and patch management.

Situational Awareness

One of the major components associated with the shift towards active defense is the need for improved situational awareness. For ICS there are several areas that require integration into a traditional security information and event management (SIEM) environment.

Operational Information

There are opportunities to gather operational information normally focused on ICS such as status, temperature, pressure, speed and other indicators. When correlated with other information they may indicate an attack, either physical or electronic, on operational equipment [8]. For example, a low oil level in a transformer oil tank may indicate that the transformer cooling system may be damaged from sabotage (shooting holes in the transformer radiator). This was the attack method used on the Metcalf station in 2013.

Another indicator might be using the SCADA system to detect and report rapid operation of several remotely controlled circuit breakers over a short time period. In normal operations with no remedial action schemes or special protection schemes, this circumstance would not happen, so chances are that this activity is malicious. This pattern was used in the attack on Ukraine in 2015.

Selection of operational information is highly dependent on each ICS in service, but several characteristics are common for successful integration into the cybersecurity continuous monitoring program.

1. Focus on high-priority, high-importance assets. Similar to categorizing cyber assets for NERC Critical Infrastructure Protection (CIP) compliance, the most effort should be spent protecting high-value assets.
2. Use relevant information that already exists, or can be easily created or calculated. Complexity is the enemy of security, so don't make gathering operational information hard. The less complex, the easier it is to troubleshoot or debug during an incident or recovery action.
3. Pilot the operational information collection at a limited subset of devices or systems to gain implementation experience before launching a system-wide implementation.
4. Reach out to equipment vendors to see if there is interest in collaboration to implement capabilities on classes of equipment, such as fault recorders, protective relays, etc.

Analytics

The ability to process large data sets has improved dramatically over the past ten years with the advancement of "big data" tools such as Hadoop and commercial versions such as Microsoft Azure and IBM's Watson. Nearly any organization can now leverage existing analytical tools with virtual processing and storage (Amazon Web Services, Microsoft Azure) and scale their solutions to take on advanced analytics in network security monitoring, SIEM implementations and others. The overall goal would be to predict security issues before they grow into actual events [9].

Predictive analytics is gaining momentum in the domain of cybersecurity, helping to determine the probability of attacks against organizations so they can set up defenses before cybercriminals reach their perimeters. But predictive analytics isn't the only tool – some vendors believe that the right machine learning solution coupled with analytics provides its full potential. In short, predictive analytics is bound to change the future of cybersecurity programs.

Action Plan

The following sections define an overall action plan to shift strategy towards active defense, response and recovery. While each organization will need to define its own priorities and scope, the overall steps required should follow this action plan to some degree.

Update Threat Assessment

Get a current threat assessment from the Electricity Information Sharing and Analysis Center (E-ISAC) or a commercial firm to determine which threats are most relevant and critical, as well as projections on future threats. Consider keeping a threat intelligence service as a permanent service or subscription to maintain a current understanding of the dynamic threat environment. Threat intelligence can provide valuable insight into decision making for the organization [10].

Update Risk Assessment
Based on the changes identified in the updated threat assessment, the appropriate changes should be incorporated into the organization's cybersecurity risk assessment. As with the threat assessment, outside assistance on the risk assessment may bring additional relevant risks to light and improve the overall risk stature of the organization.

Prioritize Funding and Resources
Look at the overall budget and resources available and determine the best way to address the threats identified in the threat assessment and reduce or maintain overall residual risk levels. Include the future projections from an Integrated Resource Planning (IRP) effort in the process so the organization has a strategic map of threats, vulnerabilities and important assets.

This is a good time to verify support from executive management and develop a business case to request an increase in budget or resources if the threat and risk assessments support that position. The business case should include the average cost of responding and recovering from a cybersecurity incident compared to the amount of the requested increase in funding. The Poneman Institute conducts an annual "Cost of Data Breach" report on behalf of IBM [11] that may provide some insight in determining the cost estimates.

Communicate Direction to Staff
Communicate the shift in direction with cybersecurity staff so they are prepared to take on new roles or additional responsibilities as the strategy starts to shift direction. Organizational change management concepts [12] should be utilized to minimize the churn associated with changes.

Encourage feedback and adopt suggestions that improve focus or accelerate changes positively. Be prepared for some pushback associated with changes – encourage engagement but don't be pressured in keeping staff who become toxic to the strategic direction or other staff.

Don't forget to include other staff members who support the cybersecurity mission in meetings – operations staff who monitor the ICS 24/7 are usually the first ones to see potential malware infections. HR onboarding is the perfect time to start training new employees on cybersecurity threats and their responsibilities.

Review Charter, Policy and Areas of Responsibility
In coordination with changing the strategic direction, review the charter of the cybersecurity program and ensure that areas of responsibility haven't either expanded or contracted based on the shift in strategy. Areas that may not have considered before, such as employee code of conduct (insider threat) or legal/sustainability (environmental threats) may bring additional issues or opportunities to manage cybersecurity risk.

Review Risk Management Framework and Organization
The Risk Management Framework (RMF) provides an abstract structure for effective ICS risk management. The RMF process includes well-defined risk-related rolls and tasks within an

organization, including management, staff and other support roles. RMF tasks are executed as part of system development life-cycle processes.

Categorize ICS Assets and Systems

Review the inventory and cybersecurity posture of the applications, hardware and firmware included in the ICS and adjust system categorizations based on the updated threat and risk assessments. For example, information from a fault recorder may now be used to define an operational information input into the SIEM and therefore raise the overall importance of the fault recorders at each substation.

Select ICS Security Controls

Based on the updated categorization of ICS assets and systems, the set of security controls may require adjustment. To include the previous example, since the fault recorders will provide input to a cybersecurity process, increased access controls may be required to protect the integrity and availability of the fault recorder information.

Implement ICS Security Controls

Finally, implementing the adjusted controls will likely require a separate project similar to updating operational equipment in the ICS. As with all cybersecurity projects, ensuring that documentation is complete and impact on operations is minimized are top priorities.

Summary

As today's ICS becomes more connected and intelligent, the security threats and risk correspondently rise. This shift in ICS design and implementation requires a strategic shift in how ICS are protected and defended. Active defense measures including an increased focus on situational awareness is required to provide our ICS with a fighting chance of survival during an attack. Operational information and analysis to provide different views than traditional network and system security monitoring are required. Data analytics will play an increasing role in active defense, including predicting cybersecurity incidents and providing a head start in defending the ICS.

This shift in strategy will take time and resources, so planning the change in strategy is critical for success. Use tools from NERC and NIST to help plan the overall action plan and ensure that all levels of executive management understand the change and support the effort. The result should be a cybersecurity organization that is prepared for the dynamic nature of threats and vulnerabilities, with the structure to detect, respond and recover when bad things happen.

.

BIBLIOGRAPHY

[1] NIST Special Publication 800-39, "Managing Information Security Risk," March 2011.
[2] NIST Special Publication 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security," May 2015.
[3] Dragos, Inc., "CRASHOVERRIDE - Analyzing the Threat to Electric Grid Operations," June 2017.
[4] North American Electric Reliability Corporation, "Emerging Technology Roundtable – Substation Automation/IEC 61850," http://www.nerc.com/pa/CI/Documents/roundtable%20-%20IEC%2061850%20slides%20%20(20161115).pdf – visited 7/23/2017.
[5] Assante, M., "Digital Ghost: Turning the Tables," SANS Institute InfoSec Reading Room, February 2017.
[6] Shane, S., Rosenberg, M., and Lehren, A., "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents," https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html - visited 7/23/17.
[7] Center for Internet Security, "The CIS Critical Security Controls for Effective Cyber Defense," Version 6.1, August 2016.
[8] Pack, J., "Situational Awareness for SCADA Systems," University of Idaho Cybersecurity Symposium, April 2017.
[9] Dickson, Ben, "How predictive analytics discovers a data breach before it happens," https://techcrunch.com/2016/07/25/how-predictive-analytics-discovers-a-data-breach-before-it-happens/ - visited 7/21/2017.
[10] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/intel/ds-cti-services.pdf - visited 7/23/2017.
[11] https://www.ibm.com/security/data-breach/ - visited 7/21/2017.
[12] https://www.prosci.com/change-management/what-is-change-management - visited 7/21/2017.