Cybersecurity Safeguards and System Recommendations Report

**To:** NAME, CIO - Defense Department of the United States of America

**From:** Your name, Cybersecurity Analyst - Red Cell 637 Defense

**Subject: Task 3 Cyber Defense Report**

Recommended Safeguards

There is a great importance in defending the critical infrastructure services at the power grid located at Western Interconnection in America, the focus that we will have will be on all safeguards we can find for our ICS (Industrial Control Systems), and or the ICS security. Technicians and engineers are allowed the ability to adjust and to review the key infrastructure process because of the control systems within the manufacturing of power generation, water treatment, general manufacturing, sewage and transmission. Below is a table that I have created in hopes of showing my safeguards to the vulnerabilities that are CIS along with an explanation on how my safeguards can aid in the protections of the critical infrastructure services:

* Developing a policy that is formal along with procedures of the preset baseline software and hardware baseline configurations. Due to the system of CIS having vulnerabilities that already known this safeguard will most definitely protect it. when we do have procedures and policies that are formal it helps by preventing any errors that could be looked at as critical by all employees involved thus not having to worry about compromising the network. One known example would someone opening an attachment that had come from an unknown email and the attachment having some sort of code that is malicious and not good. This just the start of it when it comes to the configurations baseline.
* A huge physical Security increase - the use of storage device that are portable would not be allowed at within the area of work. The access of USB within the group policy known as the Linux and or windows security settings would have to be disabled. This is a safeguard that can in the protection of the CIS due to the attack of Stuxnet on the Centrifuges Iranian became introduced by contractors who were Iranian that had introduced the device of the USB while it was loaded with codes that were known to be malicious. This would be a recommendation in helping to prevent an alike attack within the CIS (Kushner, 2013).
* Intrusion Prevention System (IPS) – we need to ensure that there is an installation of IPS devices within the networks. I would advise this with a strong and stern recommendation rather than having the detection system of intrusion (IDS). This one safeguard will work by protecting the CIS in way of the ICS security police being enforced to not have an external exchange of data and with the restriction of access while still being able to protect it from threats that would come from the outside in. With that there could be data that may get loss and it could get carried out faster than we think once there is access gained by the APT. with this we see that the intrusion prevention system will be able to take an action that is instant and right away which would be based on rules that was set by policies. (Stouffer, et al. 2015).
* Enterprise Level Anti-Virus Software – with this we can learn to have an acquirement and an investment of software that is in the form of Anti-malware/ and anti-virus which would include a signature that was partial and full for the capabilities of signature matching. This can help in protecting the CIS due to the capabilities that come from the exploit detection, sandboxing and behavioral analysis from the AV software package which is known as being robust. With this we will be better able to will help to recognize, malware and block and remove them if it comes from an email that could be missed or not seen by the IPS and or firewall. The over the counter software’s that are available for ordinary consumers are just not that strong. There should be some Memory and Data Injection Prevention in order to not allow overflows from the buffer and the injection of the SQL (Ohlhorst, 2014).

Safeguards of Evolutions

* Configuration and formal policy evolution of safeguard - this type of police will be one that will need a review that will be constant and on call. This is because of the standards that come from the ISO and the vastly changing of technologies that are new and are emerging quickly. There is a suggestion that come from firms such as Independent consulting ones stating that there should be a review taking place annually in reviewing things such as timeliness, accuracy and completeness. (Flick, 2012). There is a constant update when it comes to the technology of software and hardware. While there are threats that come in which are new there is always some sort of update being revised and or made.
* Evolution for Physical Security – while there is an improvement in the hardware capabilities of hardware we are better abled at looking at how we can increase the security that is physical with ending nodes that contain biometrics. We see that scanners that are for finger printing will aid in making it harder to access machines.

Recommendation for systems and functions

Because we have already gotten an establishment that an APT is what was mapping and also probing our network I have listed some recommendations which are in the process in means of enabling a detection that is fast for threats coming from cybersecurity:

* In order to detect any threats that are coming cyber security I would suggest a detection system of intrusion. For this should be a multi layered IDS. It needs to be signature based in order to know and identify attacks as it come. There should be capabilities coming from the IDS of anomaly detection. This recognizes activities which are not normal at all. (Stouffer, et al. 2015).
* Another suggestion and or recommendation would be using the “back-door” detecting algorithms. This can put a disguise on making it look legitimate. We would simply have to eliminate it by making look like there are different patterns in traffic. (Paxon, 2003).
* Another one would be to frequently check on the DNS servers for IP addresses that could injected. APTs more than likely use such values as 127.0.0.2 and 1.1.1.1 as holders. They also most often register domains which are looked at as random ones. Another one would be them completing with emails.
* Avoiding the tendency in ignoring any warnings when it comes to programs that are known to be not-malicious from an anti-virus. We see that Anti-viruses will sometimes put a flag on some harmless looking programs and with that the staff within the IT will most likely not look into it. with this the security software, can flag them especially if it has never been used. This may mean that there was access gained from the APT. The IT staff must be more on it. (Chang, 2014).
* We could also install monitoring tools that are from the open source network which would be able to scan and also monitor any network on a level that is non-virus which would be able to bypass the IDS/IPS system. There are some tools like the security Onion that can be used in this. This too comes from Linux. (Higgins, 2015).

Evolution of Functions or Systems

Of course, we see the need in evolving and adjusting the function system over time. With that here are some examples on how we would evolve and change in moving ahead.

* We would need to update the intrusion detection system. Especially within the signature data base. There would be a need to check to see if the technologies that are new has been created which could lead to a choice for new products rather than the one we have.
* There needs to be a frequency in the auditee of the DNS servers. Looking ahead the IT staff must be able to do research that is constant in making sure there are no new known domains added which are spoofed.
* Program warnings that are Non-malicious- the staff will have to monitor logs of the scans for anti-viruses regularly. They will also have to compare and do a cross reference with them and with the machines and all employees involved. They need to keep in mind that there will be new malwares using different file names and they have to be on top of that.
* Network monitoring tools that are open sourced- These tools are in the Linux operating system distributions. A lot of the operating systems don’t automatically update due to reasons of security so they would have to be manually updated or needs to be configured. The Security Onion distribution aims at the staff being vigilant with running the Sudo apt-get dist-update command on a basis that will be regular.

In conclusion, all the in place which detect an APT on the system are not at all what we know as a static method, they involve things such as the staff always there auditing the operating systems, logs, software and the knowledge in ensuring that we can detect all intrusions that come our way in a manner that is fast and efficient.

References

Chang, Z. (2014, August 15). 7 Places to Check for Signs of a Targeted Attack in Your Network - TrendLabs Security Intelligence Blog. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/7-places-to-check-for-signs-of-a-targeted-attack-in-your-network/

Chapple, M., & Seidl, D. (2015). *Cyberwarfare: Information operations in a connected world*. Jones & Bartlett Learning.

Energy Sector Control Systems Working Group. (2011). *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. Retrieved from http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap\_finalweb.pdf

Flick, S. (2012, May 22). How Often Should You Review Your Policies and Procedures? Retrieved from https://q9cqualityconsulting.com/2012/05/22/how-often-should-you-review-your-policies-and-procedures/

Higgins, K. J. (2015, August 1). Using Free Tools to Detect Attacks On ICS/SCADA Networks. Retrieved from http://www.darkreading.com/perimeter/using-free-tools-to-detect-attacks-on-ics-scada-networks/d/d-id/1318527

Kushner, D. (2013, February 26). The Real Story of Stuxnet. Retrieved from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

McLARTY, T. F., III, & RIDGE, T. J. (2014). SECURING THE U.S. ELECTRICAL GRID. *Securing Pension Provision*. doi:10.1057/9781137453976.0004

Paxson, V. (2003). Detecting material defects in real time. *NDT International,* *22*(2), 128. doi:10.1016/0308-9126(89)90913-9

Security for Industrial Control Systems. (2015). *Manage* Industrial Control Systems *Lifecycle*. Retrieved from https://www.cpni.gov.uk/Documents/Publications/2015/12-May-2015-3.%20Manage%20ICS%20Lifecycle%20Final%20v1.0.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. doi:10.6028/nist.sp.800-82r2

Trends in sector-specific aid, 1971-2010. (2012). doi:10.1787/dcr-2012-graph65-en

United States Department of Energy Energy Sector-Specific Plan An Annex to the National Infrastructure Protection Plan. (2010). *Securing Pension Provision*. doi:10.1057/9781137453976.0004

Virus:DOS/EICAR\_Test\_File . (2015, September 20). Retrieved from https://www.microsoft.com/en-us/security/portal/threat/encyclopedia/Entry.aspx?Name=Virus%3ADOS%2FEICAR\_Test\_File

Zhang, Y. (n.d.). *Detecting Backdoors*. Retrieved from http://ouah.org/backdoor-sec00.pdf