Brian Sowers

08/11/2022

Threat Intelligence and Intelligence Sharing

1. Identify two specific cybersecurity threat intelligence sources you should monitor and explain why they are valuable to the industry as a whole.

Two sources of intelligence sources that should be monitored in the energy sector are Tech Intelligence (TECHINT) and Cyber Intelligence (CYBINT). TECHINT is defined as "intelligence gathered on equipment and material to assess the capabilities of adversaries" (Secure Business Systems Operations Module 2, 9). Prior to the rapid modernization of Operational Technology (OT) networks, OT consisted mainly of large equipment to generate and distribute power. They still do, of course, by they are controlled and maintained by an increasing number of digital equipment that provides for automation and remote monitoring. An attack on the energy sector can now result in lasting physical and cyber damage, since the "the modern electric grid is dependent upon cyber-physical systems" (Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 5). TECHINT, I argue, is just as important as identifying which equipment the adversary has as it is to properly identify which equipment a utility provider has. For example, security researchers purchased a SCADA server on eBay "that contained poorly protected configuration files, diagrams, operational substation data and other sensitive information" (Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 19). Further, due to the digitalization of OT networks, the attack surface of OT networks has expanded to IT vulnerabilities, and many adversaries are now able to use many of the same methods to access OT networks as they would in IT networks. CYBINT, which is defined as "the collection of data via signals intelligence, open-source intelligence, and electronic intelligence," (Secure Business Systems Operations Module 2, 11) ties in closely with the above example concerning the SCADA server. Security researchers used eBay, a public marketplace falling under OSINT, to purchase a SCADA server housing utility information (ELINT).

2. Describe some of the regulatory or compliance standards for your sector that would impact the types of information you would share with your intelligence community in the future.

Due to the critical nature of resources in the U.S. energy sector, "the confidentiality of the information shared between … entities is a primary concern for utilities as well as the government" (Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 30). Various efforts have been initiated to facilitate the sharing of information between utilities and the government, but some issues still remain. For example, the establishment of the Electricity Information Sharing and Analysis Center (E-ISAC) in 1998 helped to disseminate "declassified cyber threat information to utilities," (Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 31) but failed to address the inaccessibility of classified information to utilities or the low number of personnel with security clearances at these utilities. The Protected Critical Infrastructure Information Program (PCII) helps to facilitate information sharing between utilities and the government but this information is tightly controlled and accessed by "trained … government employees and contractors" and that the "lack of a bidirectional information flow may delay other utilities' efforts to remedy connected of similar vulnerabilities in a timely manner" (Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 30). Federal legislation, however, has begun to recognize the need for increased information sharing while also maintaining a high degree of information restriction to preserve its confidentiality. Utilities wish to be able to quickly pass information to others, yet they do not want to suffer legally from the information they provide and share. In 2015, “the Cybersecurity Information Sharing Act of 2015 (CISA 2015) was passed, providing greater liability protections to utilities that voluntarily share cyber threat information with the government and aims to facilitate better real-time sharing of threat information with participating entities. There is a careful balance to information protection and information sharing in the energy sector that has not yet been realized due to the rapid modernization of OT networks. In the future, I believe legislation will allow for utilities to freely share information to the energy sector quickly and securely.

Works Cited

“Secure Business Operations Module 2, https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_1.pdf. Accessed: 08 November 2022.

“Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.” *Mission Support Center Analysis Report. “*https://www.paloaltonetworks.com/CourseFiles/Cyber_Threat_Vulnerability_Analysis_U.S._Electric_Sector.pdf. Accessed: 08 November 2022.