TIP 410: PNNL — Risk Management Tool — DOE CEDS Initiative*

Context

Cyber risk quantification is the process of evaluating the cyber risks that have been identified and then validating, measuring and analyzing the available cyber data using mathematical modeling techniques to accurately represent the organization's cybersecurity environment in a manner that can be used to make informed cybersecurity infrastructure investment and risk transfer decisions.

Chief Executive Officers, Chief Information Security Officers, and other executives in the energy sector need to have a means of prioritizing proposed cyber security initiatives based on the anticipated degree of improvement the proposed countermeasures will make.

Description

This project is a partnership with Pacific Northwest National Laboratory (PNNL) and the Bonneville Power Administration (BPA) to develop an initial generic substation architecture and associated attack tree that will enable a user to interact with a diagram of the architecture, identifying where and how each countermeasure will be implemented.

With this information the user is able to determine the potential relative change in risk posture for each proposed countermeasure. Results can then be fed into the organizations prioritization process to determine the relative benefit per dollar spent.

Once the methodology has been validated, this Risk Management Tool can be expanded to provide a library of common power distribution architectures and associated attack trees.

Benefits

This project demonstrated the capability to systematically and quantifiably determine the potential relative changes in risk, guiding utilities to avoid ending up with sub-optimal expenditures of scarce resources. While other risk quantification processes, methodologies and tools exist, they can be resource intensive to use.

Accomplishments

The primary goal was achieved. This study validates a capability that leverages knowledge of the implemented architecture, countermeasures that are in place and knowledge of the adversaries known tactics techniques and procedures (TTPs), to assess the relative changes in risk posture that can be achieved by the implementation of a list of countermeasures.

Deliverables

BPA provided the test bed for developing portions of the underlying attack tree representing BPA's environment. The BPA project team has been involved in the following:

- Participation in projects meetings and project reviews
- Support development of generic substation architecture.
- White papers on special assignments for the project's sponsor or internal efforts.
- Participation on project teams in the conduct of research and/or engagement with industry and external groups of sponsors, academics or industry representatives.

Although active participation has ended, BPA will monitor developments as the PNNL project proceeds and will receive and evaluate the Risk Management Tool for use by the Agency.

TIP 410: PNNL — Risk Management Tool — DOE CEDS Initiative*

Project Start Date: March 2019

Project End Date: September 2019

Reports & References

Risk Management Tool: A Research Project to Quantify Relative Changes in Cyber Risk;
Kristine Arthur-Durett, Bary Elison, Steve Unwin, Jeff Doty, Crystal Eppinger, Jonathan Lalo, Carl Miller, Matthew Sturtevant
Pacific Northwest National Laboratory

Participating Organizations

Pacific Northwest National Laboratory (PNNL)
Dominion Energy

For More Information Contact:

Technology Innovation Office:
TechnologyInnovation@bpa.gov

Conclusions

In light of the ever-changing cyber threat landscape and the limited resources that can be brought to bear to mitigate these threats, a significant challenge for organizations is determining how to compare mitigations in order to select those which provide the greatest benefit. To address this challenge for the Energy sector, the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response asked Pacific Northwest National Laboratory) to develop a method to compare the relative cyber risk reduction that could be achieved through the deployment of defensive countermeasures, including selected Cybersecurity for Energy Delivery Systems Research and Development funded tools and technologies.

The ultimate objective of the project was to provide a general, repeatable method for determining the relative benefits of proposed enhancements that can be applied by stakeholders without requiring deep expertise in the underlying attack tree model structure or extensive experience in using an attack tree modeling and analysis platform. This was accomplished in part by enabling the user to interact with a graphical representation (schematic) of an implemented architecture to identify where proposed countermeasures would be implemented. The using organization could then take the resulting relative changes in risk combined with the utility's costs associated with implementation and support of each proposed countermeasure to prioritize the proposed initiatives.

The methodology has shown itself to be viable using generalized architectures. Initial demonstrations with potential users have been positive and have suggested alternate uses for the Risk Management Tool in planning and operating their environments.

Moving forward, additional research and development to automate the attack tree creation as the architecture is modified by the user will enhance the benefit gained and usefulness of the Risk Management Tool.

***Cybersecurity for Energy Delivery Systems (CEDS)**
The Cybersecurity, Energy Delivery Systems (CEDS) division within the U.S. Department of Energy's (DOE's) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) invests in tools and technologies that help the energy sector secure existing infrastructure from cyber threats and design next-generation systems that can detect, reject, and withstand cyber incident.