Network Segmentation Based on Sensitivity

Network Segmentation is the practice of splitting a network into multiple sub-networks. These networks are usually designed around business needs, for example, having sub-networks for executives, finance, operations, and human resources or by keeping election functions separated from other county functions. Networks can also be separated by data sensitivity, keeping more sensitive election data separated from every day communications.

Keeping information segmented can shrink the attack surface: successful attacks on one part of a network are less likely to impact the other parts. It can also lead to performance improvements within each sub-network. Users are often required to re-authenticate in order to access other, particularly more sensitive, areas of the network. This can limit how much damage a threat actor can do if they gain access to any given part of a network.

Network segmentation can be physical or logical. Physical segmentation keeps network traffic separate through devices such as firewalls and switches. Logical segmentation uses virtual networks and addressing schemes to keep traffic on its intended sub-network. Additional segmentation can be achieved through network isolation, where an entirely separate network is created. This is often performed in the field of elections for sensitive election data like tabulators. There are often other portions of the election management system that may be connected to an isolated network.

Additionally, organizations may wish to segregate high-risk applications from the general network. For instance, multiple employees may need to access applications used to design ballots, and they all may need to push and pull data from the same election datastore (e.g., fileserver).

Organizations should leverage their data inventories to understand what systems have the most sensitive data. High-risk data, and assets hosting or processing high-risk data, are likely candidates for some form of network segmentation.

Goals

1. Know whether your election environment needs to segmented and understand the best ways to do so (Level 1 maturity)
2. Deploy appropriate network segmentation tools (Level 1 maturity)
3. Manage network segmentation appropriately (Level 1 maturity)

Actions

For Network Segmentation Based on Sensitivity, the necessary actions are the same for all maturity levels.

1. Take simple steps to segment traffic, like creating a guest wireless network and a voice network.
2. Leverage the data inventory for identifying high risk assets that should be segmented.
3. Determine your network segmentation strategy, including whether to employ physical segmentation, logical, or both.
4. Deploy a network segmentation tools appropriate for your environment, including establishing policies for firewalls and related devices.
5. Monitor and adjust policies to meet the changing needs of your organization.

Cost-Effective Tools

- Many states and localities deploy governance, risk, and compliance (GRC) tools to help manage security on their networks. Find out what tools you are currently using and whether they have network segmentation capabilties.
- Exising firewalls, switches, and their associated software can also be used to improve network segmentation.

Mapping to CIS Controls and Safeguards

- 3.12: Segment Data Processing and Storage Based on Sensitivity
- 12.2: Establish and Maintain a Secure Network Architecture
- 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work
- 13.4: Perform Traffic Filtering Between Network Segments

Mapping to CIS Handbook Best Practices

- 6