Key Findings of the 2015 Ashburn, VA Data Center Resilience Project

Michael Thompson
Cyber Security Analyst
Argonne National Laboratory
thompsonm@anl.gov
Regional Resiliency Assessment Program

Argonne is supporting the U.S. Department of Homeland Security’s Regional Resiliency Assessment Program (RRAP) in exploring the resilience of the Ashburn Data Center Cluster

In looking at a problem of this scope, we found two central questions that bear a closer examination for Internet resilience:

• Assess the resilience and vulnerabilities of the lifeline infrastructure supporting data center operations and their collective interdependencies
• Assess the collective preparedness and protection capabilities of Ashburn Data Centers and Internet Infrastructure.

For more information on the Regional Resiliency Assessment Program contact: resilience@dhs.gov or on the Ashburn RRAP: kelly.wilson@hq.dhs.gov
Ashburn Study Footprint

Courtesy of Argonne National Laboratory
Ashburn, VA, Data Center Cluster RRAP

Why Ashburn?

Beyond Ashburn’s history as an interconnection point, there remain several factors that spur its current and continued growth:

- Abundant low cost energy
- Abundant water
- Abundant land
- Favorable tax incentives
- Proximity to Washington, D.C. and Transatlantic Fiber

Ashburn / Washington Fiber (Source: Zayo.com)

References:
- Interview with Buddy Rizer, 2015
Ashburn, VA, Data Center Cluster RRAP Findings

- The properties that make this infrastructure resilient also make it difficult to gather data and conduct data-driven analysis of potential failures.

- It is in part owing to this difficulty in data collection that the Ashburn, VA RRAP project’s Key Findings focus on improving communication and information sharing.

- The Ashburn, VA RRAP project identified vulnerabilities that may affect the Internet community’s ability to prepare for and recover from the impacts of a variety of natural and manmade threats to its infrastructure assets.

References:
- Facilitated Discussion, March 24, 2015
- Interviews with Private Sector Stakeholders, 2015
- Infragard Data Center EMP Workshop, May 28, 2015
Internet resilience is contingent on a limited number of centralized Internet exchange points (IXPs).

- A study should be conducted that simulates the outage of an IXP. Such a simulation would include modeling the traffic and Transmission Control Protocol congestion during an outage of IXP facilities in the greater Ashburn area.

References:

- Facilitated Discussion, March 24, 2015.

Source: Argonne National Laboratory
Modeling an IXP outage

References:
• Facilitated Discussion, March 24, 2015.
• Interview with Equinix, March 17, 2015.
Transparency in both network and data center infrastructure would enhance resilience planning.

- A workshop should be coordinated on the development of cloud and data center service taxonomies and assessments. Such taxonomies and/or assessments should allow for equal comparison of resilience features across providers and empower customers by fostering open, honest competition.

References:
• Facilitated Discussion, March 24, 2015.
• Interview with CenturyLink Communications, March 17, 2015.
Local law enforcement personnel would benefit from training and the exchange of information concerning how to recognize suspicious activity around IT infrastructure assets.

- Law enforcement personnel should engage industry stakeholders to facilitate training and education on fiber routes and suspicious activity. This training should also address how and when to approach maintenance personnel and how to confirm that they are authorized to work in a given area.

References:
- Facilitated Discussion, March 24, 2015.
- Interview with Virginia State Police and Loudoun County Sheriff’s Department, March 4, 2015.
Data center and content providers may not have a pathway to contribute to resilience efforts and/or communicate criticality during an emergency.

- A workshop should be conducted for the data center community so that all parties can communicate their needs for points of contact and access to emergency operation center (EOC) resources and for communication pathways during an emergency.

References:
- Facilitated Discussion, March 24, 2015.
- Interview with Virginia State Police and Loudoun County Sheriff’s Department, March 4, 2015.
Questions? Comments? Please Make Contact

Michael Thompson
Cyber Security Analyst
Argonne National Laboratory
thompsonm@anl.gov