Owl’s Role in Achieving the 7 Steps

The seven steps recommended by the DHS include specific recommendations on the use of data diodes. As the global leader in data diode technology, with power grid implementations around the world, Owl has a wealth of experience in implementing cybersecurity in grid systems. This document is intended to show how each of the DHS’s seven steps can be accomplished through the use of Owl intelligent data diodes to help operators dramatically reduce cyber risk.

1. APPLICATION WHITELISTING
   Only allow predesignated applications to run and access data. Owl solutions only accept data from whitelisted data sources, restricted to a unique IP address, port, and protocol. This prevents malware from communicating over the data diode.

2. CONFIGURATION / PATCH MANAGEMENT
   Ensure systems are up to date and that a secure method for introducing authenticated software patches is used. Owl solutions authenticate software patches and updates, then securely transfer them into control centers without using potentially contaminated laptops or portable media.

3. REDUCE ATTACK SURFACE AREA
   Isolate control system networks from untrusted networks, lockdown unused services and ports, and use a data diode to provide network segmentation. Owl solutions provide hardware-enforced network segmentation and support the DHS recommendations for isolating control networks, reducing the attack surface to zero.

4. BUILD A DEFENDABLE ENVIRONMENT
   Segment networks and restrict host-to-host paths to prevent the spread of infection. Owl data diodes are purpose built as the most effective network segmentation devices available.

5. MANAGE AUTHENTICATION
   Implement “least privilege”, increase password length, change passwords regularly, and require separate credentials for corporate and control network zones. Owl solutions provide an intrinsic separation of corporate and control network zones, as well as authentication on all transfers, and allow for long passwords requiring regular changes.

6. IMPLEMENT SECURE REMOTE ACCESS
   Implement monitoring-only data access enforced by data diodes, remove backdoors, and any persistent remote connections. Owl data diodes are specifically designed to facilitate secure remote monitoring without enabling remote access or any remote connections.

7. MONITOR & Respond
   Monitor traffic at and within control system boundaries, perform login analysis, and watch for access control manipulation. Owl solutions provide real-time monitoring, display & analysis of all connections, and allow offsite auditing of all network activity.

Guidance from the DHS, NSA, and NERC to improve cybersecurity in power substations, microgrids, and transmission infrastructure.

CYBERSECURITY GUIDANCE FOR THE GRID

The power grid and its associated bulk electric systems represent millions of disparate systems connected in networks that range from a single building to thousands of square miles. From substations and transmission equipment, to new microgrids and small scale power generation, these systems all face the growing threat of cyberattack from increasingly sophisticated adversaries.

Beyond the regulations put in place by NERC CIP, the US Department of Homeland Security (DHS), in collaboration with the FBI and the NSA, put together a list of seven concrete steps that grid operators can take to create a layered, defense in depth architecture and mitigate cyber incidents.

Call 203-894-9342 or email info@owlyberdefense.com

Our team is always available to meet your cybersecurity needs
Defense-in-Depth

A “defense in depth” approach prevents a cybersecurity architecture from relying on a single strategy or element to defend a network. Data diodes, a hardware-based network cybersecurity technology designed to protect critical networks while allowing secure, one-way-only data sharing, play an integral part in this layered cybersecurity approach. These multiple layers create a matrix of protection which greatly reduces risk by blocking possible threats across different vectors.

OPDS-100D

Entry level data diode for affordable, effective network confidentiality and assurance.

The OPDS-100D allows operators to deploy more targeted and precise cybersecurity controls at a dramatically lower TCO. The 100D is a highly reliable, single-box data diode solution in a DIN rail form factor which supports multiple data flows and data types, with a maximum throughput of 104 Mbps.

The 100D can be used to create network micro-segments, protecting individual devices (e.g. a PLC), historians, databases, substations, monitoring stations along transmission lines, or any other environment with either one or more data sources and low bandwidth requirements.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com