Protect: No Exploitable Services on the Internet

`

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

2.W: Does the WWS ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol)?

Recommendation: Eliminate unnecessary exposed ports and services on public-facing assets and regularly review.

Why is this control important?

This control is important because closing ports and services to the public Internet helps prevent attackers from accessing the network. If your WWS connects a port or service (i.e., program) to the Internet, then a pathway exists for a cyberattack and you need to implement security measures to address it . A network perimeter is the secured boundary between the WWS's side of a network (the intranet) and the public Internet-facing side of the network. The perimeter contains the ports or "entrances" that attackers attempt to use to gain access to a WWS's intranet.

Additional Guidance

- ✓ You can search for Internet-exposed ports and services by using Shodan (a "search-engine" for Internet-facing assets) for assets on their network. Additionally, DHS CISA offers free vulnerability scanning services that scan for Internet-exposed services and alert the WWS of results.
- ✓ Sometimes your WWS must connect and therefore expose a service or port to the public Internet due to operational requirements. In these cases, the WWS should use an MFA service (e.g., Duo, Okta, RSA) to restrict access to authorized users and a firewall to filter out unusual traffic, and the WWS should monitor network access and activity logs for unusual actions that may indicate a cyberattack.

Implementation Tips

Implement appropriate compensating controls (e.g., firewalls, multi-factor authentication, or activity logging and monitoring) to all services (e.g., remote access, web hosting) connected to the public Internet to prevent common forms of attack.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AC-17 (page 48) and SC-7 (page 297) for more information on "Remote Access" and "Boundary Protection". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Management Template Guide: See Vulnerability Scanning Standard: Vulnerability Scanning SOP template. *https://www.cisecurity.org/wp-content/uploads/2020/06/Vulnerability-Scanning-Standard.docx*

DHS CISA Alert AA21-042A & AA21-287A: See these resources for information on various water system breaches from 2019-2021.

https://www.cisa.gov/uscert/ncas/alerts/aa21-042a

https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

DHS CISA Cyber Hygiene Services: See this resource for more information on DHS's free vulnerability scanning service. *https://www.cisa.gov/cyber-hygiene-services*

Shodan: See this resource to search for Internet-connected assets on the WWS's network. *https://www.shodan.io/*

CISA's Top Cyber Actions for Securing Water Systems: See item 1 on page 1 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*