COST: **$**$$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

2.M: Does the WWS use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?

Recommendation: Ensure that email security controls are enabled on all corporate email infrastructure.

Why is this control important?

This control is important because using security controls can reduce the risk of email-based attacks to WWS operations by filtering out malicious emails before they reach employees.

The most common and successful methods for attackers to enter a network are through email-related attacks such as phishing, spoofing, and interception. Phishing is an attack method where employees are sent an email with a malicious file, link, or request. Once the employee opens the link, a malicious file may load malware onto your WWS network, which can lead to stealing employee credentials, or tricking an employee into providing credentials or WWS funds.

Spoofing is a method that attackers often use together with phishing, where an attacker designs a malicious email to look like it came from a reputable source, usually by copying the style and email address of a known company.

Interception is a method where an attacker can place themselves in between the sender and receiver of an email, giving them the opportunity to steal the email and its contents.

Implementation Tips

Enable STARTTLS (Start Transport Layer Security), SPF (Sender Policy Framework), and DKIM (DomainKeys Identified Mail) on all of your WWS email infrastructure. CISA recommends that you also enable DMARC (Domain-based Message Authentication, Reporting, and Conformance) and set to "reject."

Resources

DHS CISA BOD 18-01: See this resource for more information on how to configure various email security controls. https://www.cisa.gov/binding-operational-directive-18-01

Additional Guidance

- ✓ WWSs should conduct employee training and awareness campaigns to complement these recommended technical controls and reduce the overall risk of email-based attacks to the WWS network.
- ✓ While the WWS should avoid all connections between OT and the public Internet, if possible (see Factsheet 2.X), the WWS should not set up any OT asset to receive email since email attacks are common and often effective.

`

NIST 800-177 (Revision 1) Trustworthy Email: See sections 2.3.1, 5.2.4, 5.2.5 and 7.3.1 for more information on “Simple Mail Transfer Protocol (SMTP)”. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SI-8 (page 348) and SC-18 (page 311) for more information on “Spam Protection” and managing macros, referred to as “Mobile Code”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*