CISA
CYBER+INFRASTRUCTURE

CISA INSIGHTS CYBER

Enhance Email & Web Security

AT-A-GLANCE RECOMMENDATIONS

- Adopt a Minimum DMARC Policy of "p=none"
- Implement HTTPS With HSTS Across All External-Facing Domains
- Disable Weak Encryption Standards for Web and Email
- Maintain Ongoing Visibility of DMARC Findings and Reports

CYBERSECURITY THREAT

Phishing emails and the use of unencrypted Hypertext Transfer Protocol (HTTP) remain persistent channels through which malicious actors can exploit vulnerabilities in an organization's cybersecurity posture. Attackers may spoof a domain to send a phishing email that looks like a legitimate email. At the same time, users transmitting data via unencrypted HTTP protocol, which does not protect data from interception or alteration, are vulnerable to eavesdropping, tracking, and the modification of the data itself.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages its State, Local, Tribal and Territorial (SLTT) government partners, as well as private entities, to use this guide to learn more about this threat and associated mitigation activities. This guidance is derived from Binding Operational Directive 18-01 – Enhance Email and Web Security and includes lessons learned and additional considerations for non-federal entities seeking to implement actions in line with federal civilian departments and agencies, as directed by CISA.

ATTACK BREAKDOWN

How It Works

Email

- An attacker spoofs the domain of a reputable organization, and sends an email that looks to be a legitimate email.

Web

- Data sent over HTTP is susceptible to interception, manipulation, and impersonation. This data can include browser identity, website content, search terms, and other user-submitted information.

Why It's Effective

Email

- Other organizations or members of the public might receive spoofed emails, perceive them to be from an authoritative source, and act on them.
- Internal employees may assume spoofed emails are legitimate and act upon them.
- If an attacker is successfully spoofing a domain in order to send malicious emails from it, this can significantly harm the affected organization's reputation.

Web

- Unencrypted HTTP connections create a privacy vulnerability and expose potentially sensitive information about the users of unencrypted websites and services.

NEAR-TERM RECOMMENDED ACTIONS

To address the significant risks to organizational information and information systems posed by phishing emails and use of the unencrypted HTTP protocol, CISA directed federal civilian agencies to undertake the following series of near-term actions and encourages non-federal organizations to do the same:

Actions to Mitigate Phishing Email Attacks

1. When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes passive man-in-the-middle attacks more difficult.
2. SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) allow a sending domain to effectively "watermark" their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect. When an email is received that does not pass an organization's posted SPF/DKIM rules, DMARC (Domain-based Message Authentication, Reporting & Conformance) tells a recipient what the domain owner would like done with the message.
3. Setting a DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an organization to be made aware of the source of an apparent forgery, information that they would not normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

Actions to Enhance Web Security

1. HTTP connections can be easily monitored, modified, and impersonated; Hypertext Transfer Protocol Secure (HTTPS) remedies each vulnerability. HTTP Strict Transport Security (HSTS) ensures that browsers always use an https:// connection, and removes the ability for users to click through certificate-related warnings.
2. Organizations should consider progress on HTTPS and HSTS deployment, such as removing support for known-weak cryptographic protocols and ciphers.
3. According to CISA vulnerability scanning data, 7 of the 10 most common vulnerabilities seen across observed networks at the time of issuance of Binding Operational Directive 18-01 would be addressed through implementing the recommended actions in this guidance related to web security.

Where to Get Started

1. Recommendations for enhancing email security:
    a. Configure all internet-facing mail servers to offer STARTTLS, and all second-level organization domains to have valid SPF/DMARC records, with at minimum a DMARC policy of "p=none" and at least one address defined as a recipient of aggregate and/or failure reports.
    b. Ensure that Secure Sockets Layer (SSL) v2 and SSLv3 are disabled on mail servers, and 3DES and RC4 ciphers are disabled on mail servers.
    c. Ensure that organizations add the centralized body location as a recipient of DMARC aggregate reports.
    d. Set a DMARC policy of "reject" for all second-level domains and mail-sending hosts.
2. Recommendations for enhancing web security:
    a. Ensure that all publicly accessible websites and web services provide service through a secure connection (HTTPS-only, with HSTS), SSLv2 and SSLv3 are disabled on web servers, and 3DES and RC4 ciphers are disabled on web servers.
    b. Identify and provide a list of second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains to the centralized body charged with managing these recommendations.
    c. Consider drafting a report to the leadership of the centralized body charged with managing these recommendations on the status of implementation.
    d. Collect feedback and input from partner equities before release to avoid vendor constraints during implementation.
    e. Ensure validating authority and its mechanisms are sound and in place before release to track compliance to successful implementation.
    f. Send all sub-organizations a weekly scorecard to drive competition amongst the participants.

ONGOING RECOMMENDED ACTIONS

1. Perform extensive outreach and support for technical as well as implementation questions.
2. Host implementation events and technical exchanges to provide additional guidance on implementation.
3. Send out scorecards weekly to leadership for awareness and to motivate improvement.
4. Develop public-facing website to provide guidance and FAQs.
5. Identify non-compliance for follow-on conversations.
6. Develop a central reporting location for all DMARC reports, and provide analysis to all equities.

LESSONS LEARNED AND ADDITIONAL CONSIDERATIONS

Lessons Learned

1. Due to a general misunderstanding about how DMARC works, and the potential fear of "missing" emails, the centralized body charged with managing the recommendations should create guidance to share with non-technical staff.
2. Many organizations do not understand the need to protect non-sending email domains with DMARC. DMARC adoption helps organizations better understand email use and categorize mail sending domains.
3. Organizations need higher-level governance to guide their actions concerning these standards. Future changes in an environment could result in increased vulnerability.

4. Organizations should be cautious when entering records on DNS as it is sensitive to errors.
5. While the goal is to reach 100% adoption of mitigation best practices, an organization's environment can fluctuate, causing unevenness in maturity. Adoption progress tends to 'mature' at the 90-95% mark, on average.

Implementation Considerations

1. The challenges around "indirect email flows," where email is sent via intermediaries (mailing lists, account forwarding) is recognized as an issue and discussed further in the references below.
2. There is a significant vendor constraint in disabling 3DES in mail environments.
    a. Microsoft has stated that they will begin disabling in July 2019.
    b. Google has launched MTA-STS as a solution.
        i. Google Blog: https://gsuiteupdates.googleblog.com/2019/04/gmail-making-email-more-secure-with-mta-sts.html
3. Be aware of potential issues with scanning sites that require authentication.
4. Have a firm understanding of inventory/environment before release.
5. Establish internal success metrics before release.
6. Entities with consolidated IT organizations are more efficient at implementation.

Resource Considerations

1. Many organizations, particularly smaller ones, may lack DMARC expertise and require support in order to implement DMARC.
2. Reading and understanding DMARC reports is extremely difficult without a tool.
3. Implementing the actions recommended in this guide may result in budgetary and/or contractual/vendor implications.

HELPFUL LINKS AND REFERENCE MATERIALS

CISA Binding Operational Directive 18-01 - Enhance Email and Web Security and FAQ:
https://cyber.dhs.gov/bod/18-01/

UK National Cyber Security Centre (NCSC) MailCheck GitHub Repository:
https://github.com/ukncsc/mail-check

ElasticMARC - DMARC Aggregate Report Digest and Analysis for Windows Utilizing the Elastic Stack GitHub Repository:
https://github.com/wwalker0307/ElasticMARC

Dmarcian XML to Human Converter:
https://dmarcian.com/xml-to-human-converter/

DMARC.org + Code and Libraries Page:
https://dmarc.org/
https://dmarc.org/resources/code-and-libraries/

Global Cyber Alliance – Benefits of Email Authentication and DMARC TXT Records:
https://dmarc.globalcyberalliance.org
https://dmarc.globalcyberalliance.org/resource/dmarc-txt-records-what-we-discovered/

Authenticated Received Chain (ARC) Mail Forwarding Guidance:
http://arc-spec.org/

For further guidance, organizations should consult National Institute of Standards and Technology (NIST) Special Publication 800-177 Trustworthy Email:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf