CIS Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Why is this CIS Control Critical?

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing the risk to the enterprise. Since email and the web are the main means that which users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering. Additionally, as enterprises move to web-based email or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication, and phishing reporting buttons.

9.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

Asset Type	Security Function	Implementation Groups
Software	Protect	1, 2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV5`: Authorized software inventory
2. Authoritative source of information indicating supported/unsupported details by product.

Operations

1. Use `GV5` to identify and enumerate web browser and email client software (M1)

2. Compare each software identified in Operation 1 to Input 2

    1. Identify and enumerate software labeled as "supported" that is currently supported (M2)

2. Identify and enumerate software labeled as "supported" that is currently unsupported (M3)
3. Identify and enumerate software labeled as "unsupported" that is currently unsupported (M4)
4. Identify and enumerate software labeled as "unsupported" that is currently supported (M5)

Measures

- M1 = Count of authorized web browser and email client software
- M2 = Count of software labeled as "supported" and currently supported
- M3 = Count of software labeled as "supported" and currently unsupported
- M4 = Count of software labeled as "supported" and currently unsupported
- M5 = Count of software labeled as "supported" and currently supported

Metrics

Percentage of Unsupported Web Browser/Email Client Software in Use

Metric	**The percentage of unsupported web browser and email client software in use**
Calculation	`(M3 + M4) / M1`

Rate of False Positives

Metric	**The percentage of authorized web browser and email client software labeled as "supported" but found to be unsupported**
Calculation	`M3 / M1`

Rate of False Negatives

Metric	**The percentage of authorized web browser and email client software labeled as "unsupported" but found to be supported**
Calculation	`M5 / M1`

9.2: Use DNS Filtering Services

Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standards

Operations

1. Use `GV1` to identify and enumerate assets that support DNS filtering (M1)

2. Use `GV5` to identify and enumerate authorized DNS filtering services

3. For each asset identified in Operation 1, check to see if it is configured properly `GV3` to support authorized DNS filtering services from Operation 2

    1. Identify and enumerate assets properly configured (M2)

    2. 1. Identify and enumerate assets not properly configured (M3)

Measures

- M1 = Count of enterprise assets capable of supporting DNS filtering
- M2 = Count of assets properly configured to support DNS filtering
- M3 = Count of assets not properly configured to support DNS filtering

Metrics

DNS Filtering Coverage

Metric	The percentage of assets configured to use authorized DNS filtering services
Calculation	`M2 / M1`

9.3: Maintain and Enforce Network-Based URL Filters

Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Processs

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards
3. `GV5`: Authorized software inventory

Operations

1. Use `GV1` to identify and enumerate enterprise assets capable of supporting network-based URL filters (M1)

2. Use `GV5` to identify authorized web browsers/clients

3. For each asset identified in Operation 1 check to see if it is configured properly `GV3` to support authorized web browsers/clients from Operation 2

    1. Identify and enumerate assets properly configured (M2)
    2. Identify and enumerate assets not properly configured (M3)

Measures

- M1 = Count of enterprise assets capable of supporting network-based URL filters
- M2 = Count of assets properly configured to support network-based URL filters
- M3 = Count of assets not properly configured to support network-based URL filters

Metrics

Coverage

Metric	**The percentage of assets configured to use authorized network-based URL filters**
Calculation	`M2 / M1`

9.4: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

Asset Type	Security Function	Implementation Groups
Software	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory

Operations

1. Use `GV1` to identify and enumerate assets subject to browser/email plugin restrictions (M1)

2. Use `GV5` to identify authorized browser and email plugins

3. For each asset listed in Operation 1, collect the list of installed browser plugins and compare to the output of Operation 2

    1. Identify and enumerate assets with only authorized browser plugins installed or enabled (M2)
    2. Identify and enumerate assets with one or more unauthorized browser plugins installed or enabled (M3)

4. For each asset listed in Operation 1, collect the list of installed email plugins and compare to the output of Operation 2

    1. Identify and enumerate assets with only authorized email plugins installed or enabled (M4)
    2. Identify and enumerate assets with one or more unauthorized browser plugins installed or enabled (M5)

Measures

- M1 = Count of assets subject to browser/email plugin restrictions
- M2 = Count of assets with only authorized browser plugins installed or enabled
- M3 = Count of assets with unauthorized browser plugins installed or enabled
- M4 = Count of assets with only authorized email plugins installed or enabled
- M5 = Count of assets with unauthorized email plugins installed or enabled

Metrics

Browser Plugin Enforcement Quality

Metric	**The percentage of assets compliant with authorized browser plugins**
Calculation	`M2 / M1`

Email Client Plugin Enforcement Quality

Metric	**The percentage of assets compliant with authorized email plugins**
Calculation	`M4 / M1`

9.5: Implement DMARC

To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. DMARC Policy
2. TXT record published in DNS
3. The Mail Transfer Agent used by the enterprise
4. The Mail User Agent used by the enterprise

Assumptions

1. The DMARC configuration policy includes instructions to produce either Aggregate (rua) or Forensic (ruf) reports.
2. The enterprise has access to these reports either daily (for Aggregate) or in real-time (for Forensic).

Operations

1. Check if enterprise has a DMARC policy

    1. If the enterprise has a DMARC policy, M1 = 1
    2. If the enterprise does not have a DMARC policy, M1 = 0

2. Examine Input 2 for a value indicative of the use of DMARC

    1. If a value for DMARC is identified, M2 = 1
    2. If a value for DMARC is not identified, M2 = 0

3. Examine Input 2 for a value indicative of the use of SPF

    1. If a value for SPF is identified, M3 = 1

    2.
        1. If a value for SPF is not identified, M3 = 0

4. Examine Input 2 for a value indicative of the use of DKIM

    1. If a value for DKIM is identified, M4 = 1
    2. If a value for DKIM is not identified, M4 = 0

5. Check if enterprise uses a Mail Transfer Agent

    1. If the enterprise uses a Mail Transfer Agent, M5 = 1
    2. If the enterprise does not use a Mail Transfer Agent, M5 = 1

6. Check if enterprise uses a Mail User Agent

    1. If the enterprise uses a Mail User Agent, M6 = 1
    2. If the enterprise does not use a Mail User Agent, M6 = 1

Measures

- M1 = Output of Operation 1
- M2 = Output of Operation 2
- M3 = Output of Operation 3
- M4 = Output of Operation 4
- M5 = Output of Operation 5
- M6 = Output of Operation 6

Metrics

DMARC Usage

Metric	**Usage and configuration of DMARC/SPF/DKIM**
Calculation	`(M1 + M2 + M3 + M4 + M5 + M6) / 6`

9.6: Block Unnecessary File Types

Block unnecessary file types attempting to enter the enterprise's email gateway.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

Operations

1. Use `GV1` to identify and enumerate assets configured as email gateways (M1)

2. Using `GV3` check the attachment blocking configuration for every asset identified in Operation-1

    1. Identify and enumerate email gateways properly configured to block unnecessary attachments (M2)
    2. Identify and enumerate email gateways not properly configured to block unnecessary attachments (M3)

Measures

- M1 = Count of email gateways
- M2 = Count of properly configured email gateways
- M3 = Count of improperly configured email gateways

Metrics

Coverage

Metric	The percentage of properly configured email gateways
Calculation	`M2 / M1`

9.7: Deploy and Maintain Email Server Anti-Malware Protections

Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standard

Operations

1. Use `GV1` to identify and enumerate all email servers within the enterprise (M1)

2. For each email server identified in Operation 1, use `GV3` to check if native or external anti-malware protections are configured

    1. Identify and enumerate email servers with configured anti-malware protection (M2)
    2. Identify and enumerate email servers without configured anti-malware protection (M3)

Measures

- M1 = Count of email servers
- M2 = Count of properly configured email servers
- M3 = Count of improperly configured email servers

Metrics

Coverage

Metric	The percentage of properly configured email servers
Calculation	`M2 / M1`