CIS Top 20 #7

Email & Web browser Protections
CIS Top 20 Critical Security Controls

Am I doing the right things?
CIS Top 20 Critical Security Controls

ICS Cyber Security Control Framework

- Procedural Security Controls
- Operational Security Controls
- Technological Security Controls
- Physical Security Controls
- Regulatory & Compliance Controls
CIS Top 20 Critical Security Controls

CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks.

These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. (www.cisecurity.org)
CIS Controls™

Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises
CIS Top 20 Critical Security Controls

CSC # 7   Email & Browser:

• The most common methods of attack on browsers are malicious browser extensions, exploiting known vulnerabilities, and using vulnerable add-ons such as Flash.
CIS Top 20 Critical Security Controls

• Email the primary method is phishing.

From: brettd1@just81.jushtost.com
Sent: Wednesday, November 19, 2014 4:52 PM
To: 
Subject: Shipment Status ID#000884027

Dear 

Courier was unable to deliver the parcel to you. Shipment Label is attached to email.

Yours sincerely,
Mathew Gorman,
Sr. Delivery Manager.

Pretty sure this isn't an official FedEx email address... lol

(C) 2014 FedEx. The content of this message is protected by copyright and trademark laws. All rights reserved.
CIS Top 20 Critical Security Controls

- Spear phishing – targeted phishing
- Whale phishing – targeted at high-profile Execs
CIS Top 20 Critical Security Controls

• Phishing can be reduced through technical controls but it will never be eliminated.
CIS Top 20 Critical Security Controls

• Solution Approach
  – Standard email and web configuration
  – Remove any ability to install browser toolbars and extensions
  – URL filtering
  – Sandboxing
  – Software patches up to date
  – HIPS / App whitelisting
CIS Top 20 Critical Security Controls

• There is the second part to this, which is the most difficult to control.......The people
CIS Top 20 Critical Security Controls

Human error is still the major source of most breaches and incidents.

<table>
<thead>
<tr>
<th>Causes</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing/Hacking/Malware</td>
<td>31%</td>
</tr>
<tr>
<td>Employee Action/Mistake</td>
<td>24%</td>
</tr>
<tr>
<td>External Theft</td>
<td>17%</td>
</tr>
<tr>
<td>Vendor</td>
<td>14%</td>
</tr>
<tr>
<td>Internal Theft</td>
<td>8%</td>
</tr>
<tr>
<td>Lost or Improper Disposal</td>
<td>6%</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

Browser Anatomy

- Rendition
- Scripting (e.g., JavaScript, VBScript)
- Java
- ActiveX
- Plug-ins
- HTML Parsing (or other ML)
- HTTP

Render
Interpret
Parse
Transport
CIS Top 20 Critical Security Controls

Technology Related Risks

- Portable Document Format (PDF)
- JavaScript and VBScript
- New Media Plug-ins
- Java
- PostScript
- ActiveX

- Low
- Medium
- High
## CIS Top 20 Critical Security Controls

For browser protections, start with filtering

<table>
<thead>
<tr>
<th>WebServers</th>
<th>Network</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>-MFA</td>
<td>-NGFW/URL</td>
<td>-AV/HIPS</td>
</tr>
<tr>
<td>-No browsing</td>
<td>-Sandbox</td>
<td>-App whitelist</td>
</tr>
<tr>
<td>-AV/HIPS</td>
<td>-SIEM</td>
<td>-GPO</td>
</tr>
<tr>
<td>-Harden</td>
<td>-Proxy</td>
<td>-Training</td>
</tr>
<tr>
<td></td>
<td>-Patching</td>
<td>-Patching</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

For email protections

**Email Servers**
- No emailing
- MFA
- AV/HIPS
- Patch

**Network**
- NGFW/URL
- Sandbox
- SPF
- Email gateway
- SPAM

**Client**
- AV/HIPS
- App whitelist
- GPO
- Training
- Patch
CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.
2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress
### CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.</td>
</tr>
<tr>
<td>7.2</td>
<td>Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.</td>
</tr>
<tr>
<td>7.3</td>
<td>Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.</td>
</tr>
<tr>
<td>7.4</td>
<td>Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.</td>
</tr>
<tr>
<td>7.5</td>
<td>Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.</td>
</tr>
<tr>
<td>7.6</td>
<td>The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.</td>
</tr>
<tr>
<td>7.7</td>
<td>To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.</td>
</tr>
<tr>
<td>7.8</td>
<td>Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

• 7-1 - Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.

• Tools
  – US-Cert browser hardening guides
  – Vulnerability management scanners
  – Thycotic – browser cached passwords
  https://thycotic.com/company/blog/2013/09/09/securing-web-browsers-through-group-policy/
CIS Top 20 Critical Security Controls

• 7-2 - Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

• Free Tools
  – NIST Email 800-45 guide
  – CIS Hardening guides per clients, app, server, OS

• Commercial Tools
CIS Top 20 Critical Security Controls

• 7-3 - Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.

• Free Tools
  – NIST Email 800-45 guide
  – CIS Hardening guides per clients, app, server, OS
CIS Top 20 Critical Security Controls

• 7-4 - Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

• Tools:
  – Proxy
  – Firewalls
  – SIEM
CIS Top 20 Critical Security Controls

7-5 - Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.
CIS Top 20 Critical Security Controls

• 7-6 - The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
CIS Top 20 Critical Security Controls

• 7-7 To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.
At the same time, implementing Sender Policy Framework at a DNS level and on the mail servers should cut down on the amount of spam and malicious traffic that is coming in to the system. It should be noted that while SPF is not an anti-spam measure, it's effective as a control for malicious mail traffic. It's important that the SPF records and implementation include receiver-side verification (this is actually directly mentioned in sub-control7.7).
CIS Top 20 Critical Security Controls

• 7-8 - Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.

• Tools:
  – Sandboxing
  – PaloAlto Wildfire, Fortinet, Fireeye, and many more
CIS Top 20 Critical Security Controls
Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC

Tuesday May 1st

CIC CSC # 8
Malware Defenses