SYNERCOMM

SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #18

Application Software Security

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # # 18

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CIS Top 20 Critical Security Controls

Why Is This Control Critical?

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

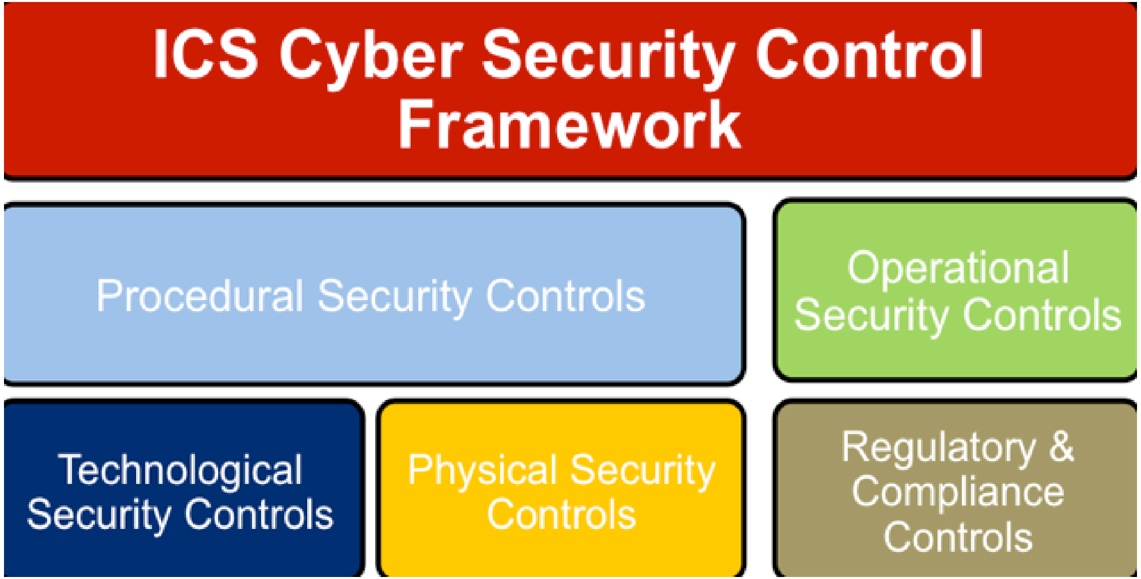
17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Understanding the Control types



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

- 1ST AND FOREMOST
- ESTABLISH SECURE CODING PRACTICES
  - The first step in writing secure code is following best practices.
  - OWASP has a great cheat sheet for the secure software development life cycle. Additionally, developers can study for the ISC2 Certified Secure Software Lifecycle Professional (CSSLP) certification.

CIS Top 20 Critical Security Controls

- **The Solution**
  - The security of applications (in-house developed or acquired) is a complex activity requiring a complete program encompassing enterprise-wide policy, technology, and the role of people. These are often broadly defined or required by formal Risk Management Frameworks and processes.

CIS Top 20 Critical Security Controls

- Now that you have an idea of which components you should have in place, let’s take a look at the process of implementing these controls, keeping in mind that it will look very similar across companies of various sizes and industries.

CIS Top 20 Control #18

Step 1: Foster a Relationship with Your Application Development and Procurement Groups

CIS Top 20 Control #18

Step 2: Implement Security Gates to Address the Controls Instead of Having a Pass/Fail at the End of the Software Development Lifecycle

CIS Top 20 Control #18

Step 3: Ensure You Have the Proper People and Tools in Place

CIS Top 20 Critical Security Controls

Key Takeaways for Control 18

- Understand your risk.
- Layered security is important

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 CSC # 18

- Sample Gap questions

1. Are clear business requirements defined each time custom business applications are developed or implemented?
2. Is appropriate security always defined as a business requirement for business application systems?
3. Does the organization utilize a documented software development lifecycle when developing all applications?
4. Does the organization utilize code review tools when developing custom code for the enterprise?
5. Are Web Application Firewalls (WAFs) used to protect all web-based applications?

CIS Top 20 Critical Security Controls

18.1	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.
18.2	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
18.3	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
18.4	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.
18.5	Do not display system error messages to end-users (output sanitization).
18.6	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.
18.7	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.
18.8	Ensure that all software development personnel receive training in writing secure code for their specific development environment.
18.9	For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.

CIS Top 20 Critical Security Controls

- *18-1 - For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security hardening recommendations.*
- Free Tools
  - Spiceworks - Though not a notifier for versioning, it does detect software versions, and you can build reports using this information, and auto email reports on a schedule, it can help.
  - Secunia - Free online tool that can be downloaded for personal use to detect and update out-of-date software.
  - AppUpdater - Small list of supported software, but updating can be automated without interaction. Supports Windows, Linux, Mac, and lots more features.
- Commercial Tools
  - Secunia - Enterprise grade software compliance suite
  - See tools listed in control 3-2

CIS Top 20 Critical Security Controls

- *18-2 - Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks.*
- Tools
  - Barracuda
  - F5
  - Citrix

CIS Top 20 Critical Security Controls

- *18-3 - For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.*
- This is more of a process than a tool. But if you know of any tools, let me know.

CIS Top 20 Critical Security Controls

- *18-4 - Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis.*
- Free Tools
- OpenVAS - An open source vulnerability scanner that can be configured to scan web applications for things like XSS (among others).
- Metasploit - A tool for the everyday pen-tester and security enthusiast.
- OWASP has published a list of tools (Free and Commercial), so without further

CIS Top 20 Critical Security Controls

- *18-5 - Do not display system error messages to end-users (output sanitation).*
- More of a process per application.

CIS Top 20 Critical Security Controls

- *18-6 - Maintain separate environments for production and non-production systems.*
- This is more of a process than a tool. Essentially, you must create both a physical and a logical divide between your production systems and dev environment. I have always done this via VLANs, keeping the Dev VLANs completely off the production networks. Also, many people are of the mindset of adding the dev environment as sub-domains of your production domains. DON'T DO THIS. I have been successful at gaining access to higher domains from sub domains by exploiting a Kerberos weakness known as "forging a golden ticket". Complete separation, with an implicit block on your network firewall. That being said, I do allow explicit production traffic to enter the dev environments.

CIS Top 20 Critical Security Controls

- *18-7 - For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.*
- **Free Tools**
- STIGs Currently, there are STIGs for MSSQL and Oracle, but the same concepts of these two platforms can be applied to other DB vendors.

CIS Top 20 Critical Security Controls

- *18-8 - Ensure that all software development personnel receive training in writing secure code for their specific development environment.*
- This all comes down to training and who you hire, unfortunately :)

CIS Top 20 Critical Security Controls

- *18-9 - For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.*
- I have seen in house tools that scan in house code, but do not know of any free or commercial.

CIS Top 20 Critical Security Controls

- You are invited!!
  - SynerComm IT Summit
  - October 22-23rd
  - Milwaukee @ Potawatomi
  - Enabling Secure Digital Transformation
  - Registration

CIS Top 20 Critical Security Controls

Thank you for Attending.

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

Tuesday October 2nd

CIC CSC # 19

Incident Response and Management