SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #15

Wireless Access Control

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 15

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

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

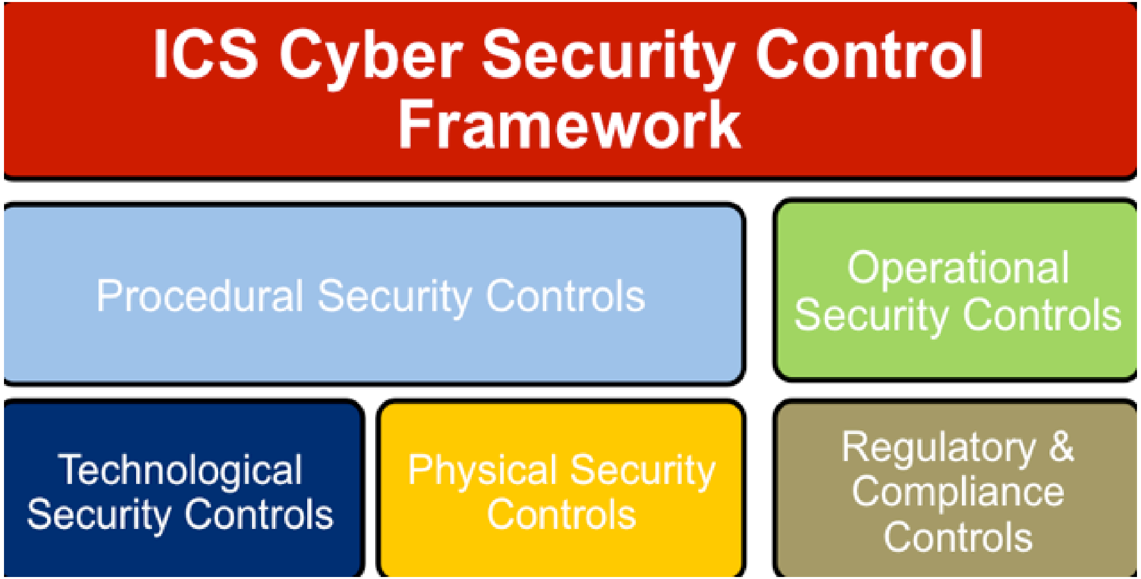
Foundational

- 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 15 Procedures and Tools

- Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.

How can you implement CIS Control 15?

Do not broadcast your SSID.

Deploy TLS certificates on your main/secure networks.

Use WPA2-Enterprise

Adjust and limit your radio broadcast levels

Perform Wireless (RF) site assessments

Create a guest network

Monitor

CIS Top 20 Critical Security Controls

- **Key Takeaways from Control 15**
  - Reduce your attack surface
  - Use your tools

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

When performing an audit of an organization’s wireless systems, auditors should consider at a minimum asking the following questions:

1. Are only appropriate users authorized to utilize wireless networking systems from the organization’s systems?
2. Is AES-CCMP used to encrypt all wireless data in transit on 802.11 wireless networks?
3. Is EAP/TLS used for authentication to each of the organization’s sensitive 802.11 wireless networks?
4. Is the use of Bluetooth or ad hoc networks explicitly denied on each of the organization’s systems?
5. Has the organization deployed a Wireless IDS (WIDS) solution to monitor for the use of inappropriate wireless systems?

CIS Top 20 Critical Security Controls

15.1	Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
15.2	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.
15.3	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.
15.4	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).
15.5	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
15.6	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.
15.7	Disable peer-to-peer wireless network capabilities on wireless clients.
15.8	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.
15.9	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.

CIS Top 20 Critical Security Controls

- *15-1* - Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.

- **Free Tools**
  - FreeRADIUS & 802.1x - How to setup 802.1x with FreeRADIUS. Just know that Windows, Linux, and Mac come built in with their own Supplicant. No need for a third party.
  - SANS guide to deploy 802.1x
  - Group Policy for Wireless 802.1x

- **Commercial Tools/Services**
  - **Forescout**

CIS Top 20 Critical Security Controls

- *15-2* - Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.

- **Free Tools**
  - RogueScanner
- **Commercial Tools**
  - Many WAP vendors offer these kind of detection tools. You may even have them, but aren't using them!

CIS Top 20 Critical Security Controls

- *15-3* - Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.

- Tools:
  - Again, these tools are heavily dependent on your WAP vendor. Make sure you go with a good vendor that offers these tools.

CIS Top 20 Critical Security Controls

- *15-4* - Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration

- Tools
  - Group Policy - How to whitelist SSIDs for wireless clients on your domain.

CIS Top 20 Critical Security Controls

- *15-5* - Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
- Tools:
  - This is in your SSID config
  - Do not leave your Guest un-secured use at least WPA2

CIS Top 20 Critical Security Controls

- *15-6* - Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.

- Tools:
  - This is in your SSID config

CIS Top 20 Critical Security Controls

- *15-7* - Disable peer-to-peer wireless network capabilities on wireless clients.

- **Tools**
  - GPO - you can find this setting at Computer Configuration > Policies > Administrative Templates > Network > Microsoft Peer-to-Peer Networking Services
  - Many wireless vendors offer this setting (performance as well)

CIS Top 20 Critical Security Controls

- *15-8* - Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

- Tools:
  - GPO - How to disable Bluetooth and other wireless beaming
  - Many wireless vendors have Bluetooth available for beacons, make sure it is disabled

CIS Top 20 Critical Security Controls

- *15-9* - Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.
- Tools:
  - 802.1x can aid in this situation, but it is not required. Small businesses should have the ability to configure their wireless routers/APs to provision clients on a segregated network and deny that network from accessing internal resources (don’t forget to block VPN access!).

CIS Top 20 Critical Security Controls

- *15-xx* - a few additional items
  - Back to CSC #1 – AP hardware inventory
  - Use tools from Vendor – Spectrum analyzer, WIPS
  - Strong auth, AES encryption, device certs or tokens
  - Harden mobile devices. Laptops to NOT REMEMBER wireless networks (easy spoof)**Pineapple

CIS Top 20 Critical Security Controls

Thank you for Attending.

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

Tuesday November 13th

CIC CSC # 16

Account Monitoring and Control