GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Smith, Travis

"20 CIS Controls: Control 13 – Data Protection"

Tripwire.com

URL: https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-13-data-protection/

Accessed: 09 July 2019

Synopsis: Key Takeaways for Control 13

- **A wide array of difficulty**. Some of these recommendations can be considered quick wins, such as blocking access to cloud storage providers. Others such as creating an inventory of sensitive information can be a never-ending process. This is one of the more difficult controls to fully implement and for good reason. Protecting data is the primary goal of everyone in information security.
- **Rely on hardening standards**. Both CIS and DISA have hardening guidelines for mobile devices. These guidelines have recommendations on encrypting the drive as well as locking down USB access.
- **Look to control 6**. DLP can be expensive to roll out. By collecting audit logs across devices, you can achieve some level of insight into data exfiltration of sensitive data with existing tools. Tag the assets with sensitive data and monitor those more carefully. Leverage baselines for both network and file data so anything suspicious can quickly be flagged.

20 CIS Controls: Control 13 – Data Protection

TRAVIS SMITH (HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/TRAVIS-SMITH/)
FOLLOW @MRTRAV (HTTPS://TWITTER.COM/MRTRAV)
(HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/)
IN SECURITY AND DATA PROTECTION (/STATE-OF-SECURITY/TOPICS/SECURITY-DATA-PROTECTION/)

Today, I will be going over Control 13 from version 7 of the top 20 CIS Controls (https://www.tripwire.com/state-of-security/security-data-protection/security-controls/cis-top-20-critical-security-controls/) – Data Protection. I will go through the nine requirements and offer my thoughts on what I've found.

Key Takeaways for Control 13

- **A wide array of difficulty**. Some of these recommendations can be considered quick wins, such as blocking access to cloud storage providers (https://www.tripwire.com/state-of-security/security-data-protection/cloud/google-cloud-platform/). Others such as creating an inventory of sensitive information can be a never-ending process. This is one of the more difficult controls to fully implement and for good reason. Protecting data is the primary goal of everyone in information security.
- **Rely on hardening standards**. Both CIS and DISA have hardening guidelines for mobile devices. These guidelines have recommendations on encrypting the drive as well as locking down USB access.

- **Look to control 6**. DLP can be expensive to roll out. By collecting audit logs across devices, you can achieve some level of insight into data exfiltration of sensitive data with existing tools. Tag the assets with sensitive data and monitor those more carefully. Leverage baselines for both network and file data so anything suspicious can quickly be flagged.

Requirement Listing for Control 13

1. MAINTAIN AN INVENTORY OF SENSITIVE INFORMATION

Description: Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems including those located onsite or at a remote service provider.

Notes: Creating an initial list of where sensitive information is stored can be simple enough. The difficult task comes with maintaining the list and continually hunting for that data. This requirement is important since it will feed many requirements both for this Control as well as control 14.

2. REMOVE SENSITIVE DATA OR SYSTEMS NOT REGULARLY ACCESSED BY ORGANIZATION

Description: Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Notes: One of the reasons it is important to continually update the list of where sensitive information is stored (previous requirement) is that in some cases it will need to be removed. Having sensitive information in a powered-off virtual machine still caries risk since the virtual machine file can still be stolen. Ensure the proper virtualization monitoring tools are in place to both harden and monitor the virtual infrastructure.

3. MONITOR AND BLOCK UNAUTHORIZED NETWORK TRAFFIC

Description: Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

Notes: This is data loss prevention in a nutshell. Even though there are great tools at your disposal which can specialize in DLP, classifying the data to begin with will help reduce the loss rate of sensitive data.

4. ONLY ALLOW ACCESS TO AUTHORIZED CLOUD STORAGE OR EMAIL PROVIDERS

Description: Only allow access to authorized cloud (https://www.tripwire.com/solutions/maintain-control-in-the-cloud/) storage or email providers.

Notes: There is much less visibility into third party cloud/email providers than there is for internally owned assets. Because of this, it's important to at least have a policy to prohibit access to these providers. The next step is to block access to them entirely at the network perimeter.

5. MONITOR AND DETECT ANY UNAUTHORIZED USE OF ENCRYPTION

Description: Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

Notes: For the same reason that encryption is used for legitimate services, hackers will use encryption to hide what data is being stolen. This helps them evade detection to reach their ultimate goal. Not only look for anomalous encryption on the network but also for computer generated domain names.

6. ENCRYPT THE HARD DRIVE OF ALL MOBILE DEVICES

Description: Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.

Notes: Even well-intending users lose a laptop or phone from time to time. Make sure the encryption is configured properly to prevent attacks against stealing decryption keys from memory when the system is in hibernation or sleep mode.

7. MANAGE USB DEVICES

Description If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

Notes: USB input devices are pretty much standard these days, or maybe I am dating myself by thinking PS/2 keyboard and mice are still around. Either way, blocking mass storage devices or only whitelisting input devices can reduce the attack surface for data exfiltration.

8. MANAGE SYSTEM'S EXTERNAL REMOVABLE MEDIA'S READ/WRITE CONFIGURATIONS

Description: Configure systems not to write data to external removable media if there is no business need for supporting such devices.

Notes: The USB drive (https://www.tripwire.com/state-of-security/security-data-protection/danger-usb/) is more at risk of being an attack vector than a medium for data exfiltration. However, in some environments data exfiltration will be a major concern. In that case, blocking USB access completely is the best choice. If there is a business case for USB access, a per user exception can be made quite easily just by managing permissions to DLL files in Windows.

9. ENCRYPT DATA ON USB STORAGE DEVICES

Description: If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

Notes: This one to me seems like it is difficult to enforce. Provide the training to employees so they are aware of the risks of data on USB drives. Then provide them with the tools to secure your organization's critical data.

READ MORE ABOUT THE 20 CIS CONTROLS HERE:

Control 20 – Penetration Tests and Red Team Exercises (https://www.tripwire.com/state-of-security/security-data-protection/security-controls/20-critical-security-controls-control-20-penetration-tests-red-team-exercises/)

Control 19 – Incident Response and Management (https://www.tripwire.com/state-of-security/security-data-protection/security-controls/20-critical-security-controls-control-19-incident-response/)

Control 18 – Application Software Security (https://www.tripwire.com/state-of-security/security-data-protection/security-controls/20-critical-security-controls-control-18-application-software-security/)

Control 17 – Implement a Security Awareness and Training Program (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-17-awareness-training/)

Control 16 – Account Monitoring and Control (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-16-account-monitoring/)

Control 15 – Wireless Access Control (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-15-controlled-access/)

Control 14 – Controlled Access Based on the Need to Know (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-14-controlled-access/)

Control 13 – Data Protection

Control 12 – Boundary Defense (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-12-boundary-defense/)

Control 11 – Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-11-secure-configuration-network-devices/)

Control 10 – Data Recovery Capabilities (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-10-data-recovery/)

Control 9 – Limitation and Control of Network Ports, Protocols, and Services (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-9-limitation-control-network-ports/)

Control 8 – Malware Defenses (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-8-malware-defenses/)

Control 7 – Email and Web Browser Protections (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-7-email-web-protections/)

Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-6-audit-logs/)

Control 5 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-5-secure-configurations/)

Control 4 – Controlled Use of Administrative Privileges (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-4-controlled-privileges/)

Control 3 – Continuous Vulnerability Management (https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-3-vulnerability-management/)