2-3 Security Controls

György Kálmán
Critical Infrastructure Protection Group, CCIS
mnemonic AS

Overview of the module

- Definitions
- The 20 most important security controls by CIS
- Conclusion

Definitions

- Security control: a safeguard or countermeasure to avoid, detect, counteract or minimize security risk to an asset
  - Preventive: try to avoid something to happen
  - Detective: try to find out if something is happening right now
  - Corrective: limit the extent of damage if something has happened
- By their nature, security controls can be:
  - Physical : guard, fence, wall
  - Procedural: definied processes, training and awareness
  - Technical: access control, traffic analysis, cryptographic functions
  - Legal: prison, fine etc.

Principles

- Controls should:
  - Focus on addressing the most important risk sources
  - Should be consistent along the organisation
  - Automated where feasible
  - Root causes shall be identified and eliminated if possible
  - Measureable.

The 20 critical controls

1. Inventory of authorized and unauthorized hardware.
2. Inventory of authorized and unauthorized software.
3. Secure Configurations for Hardware and Software For Which Such Configurations Are Available.
4. Continous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance and Analysis of Complete Security Audit Logs
7. E-mail, web and other online service protection
8. Malware Defenses
9. Limitation and Control of Ports, Protocols and Services
10. Data Recovery Capability
11. Secure Configurations of Network Devices Such as Firewalls And Routers.
12. Boundary Defense
13. Data Protection
14. Controlled Access Based On Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Training To Fill Gaps
18. Application Software Security
19. Incident Response Capability
20. Penetration tests and Red Team Exercises

1. Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why is this important:

- Only authorized systems shall get access to the network
- Avoid mapping of the system by an attacker
- Access of externals to the system

1. Inventory of Authorized and Unauthorized Devices

Defenses:

- Install a discovery tool to have an updated view of the current state of the system
- Log relevant services, like DHCP, ARP or others
- Differences from actual and previous inventory should be evaluated (e.g.: replacement of old devices should be updated automatically)
- Implement network-level authentication

Sensors:

Active discovery service, passive discovery service, asset inventory, network level authentication, log management, alert console

2. Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why is this important:

- Only authorized software should be installed on the systems
- Avoid possibility of unauthorized software
- Protection against malware

2. Inventory of Authorized and Unauthorized Software

Defenses:

- File integrity checking
- Application whitelisting
- Software inventory
- Isolated environments for unsafe but required software

Sensors:

Inventory, whitelisting system, virtualization, log management, alert console

3. Secure Configurations for Hardware and Software

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why is this important:

- Directory of standard baseline security configurations
- Configuration management with integrity checks
- Only use secure remote management

3. Secure Configurations for Hardware and Software

Defenses:

- File integrity checking
- Automated configuration management
- Directory of secure configs

Sensors:

Baseline security configurations, configuration enforcement, file integrity checking services, logging and alerting

4. Continous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Why is this important:

- Updated picture on vulnerabilities in the system
- Can focus maintenance on the assets in most critical status
- Correlate vulnerability scans with event logs

4. Continous Vulnerability Assessment and Remediation

Defenses:

- Deployed vulnerability scan agents
- Patch management
- Log monitoring
- Comparison of vulnerability scans in time
- Patch directory/intelligence service

Sensors:

Vulnerability scanner, patch management, logging and alerting.

5. Controlled use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Why is this important:

- To protect key system components
- Protect sensitive data
- Keep the effect of other controls

5. Controlled use of Administrative Privileges

Defenses:

- Minimize the use of administrative privileges
- Inventory of all privileged accounts
- Control on default usernames and passwords
- Two/multi factor authentication for privileged accounts
- logging

Sensors:

Identity management, centralised authentication system, dedicated systems for administration, logging and alerting

6. Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Why is this important:

- Be able to reconstruct what has happened
- Supports root cause analysis
- Can be used for validation and evaluation of controls

6. Maintenance, Monitoring and Analysis of Audit Logs

Defenses:

- Independent time sources for stamping
- Validate logging settings for all sources
- Storage with integrity protection for the logs
- Periodic anomaly checks
- Deploy Security Information and Event Management (SIEM) solution

Sensors:

Time distribution, logging and alerting.

7. E-mail and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

Why is this important:

– E-mail and web are used as spearheads for initial compromise of a system

7. E-mail and Web Browser Protections

Defenses:

- Whitelisting of allowed browsers
- Limit the use of extensions, script languages
- Logging
- Network-based URL filters
- Secure DNS

Sensors:

Configuration enforcement, URL and content filters, secure DNS, email checking, logging and alerting

8. Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Why is this important:

- Prevent execution of unauthorized code
- Avoid possibility of unauthorized software
- Protection against malware

8. Malware Defenses

Defenses:

- Anti-virus, anti-malware, host-based IPS
- Centralised management of these solutions
- Enable anti-exploit technologies like data execution prevention, EMET
- Secure DNS

Sensors:

Anti-virus and anti-malware endpoint protection, logging, SIEM, configuration service, alerting.

9. Limitation and Control of Network Ports

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Why is this important:

- Reduce attack surface
- Inventory of services
- Easier to spot configuration anomalies

9. Limitation and Control of Network Ports

Defenses:

- Only ports and services with validated need are run
- Automated port scans
- Reduce attack surface with only exposing hosts towards the internet with validated need
- Use of firewalls

Sensors:

Firewalls, endpoint protection, automated port scanners, logging and alerting

10. Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Why is this important:

- Restoration after incident
- Limit possible damage

10. Data Recovery Capability

Defenses:

- Automatic backup with appropriate frequency
- Test of backup functionality and media
- Protect backups with crypto and physical security controls
- Offline/isolated backups to limit 0day damage

Sensors:

backup system, logging and alerting

11. Secure Configurations for Network Devices

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why is this important:

- Actually utilize the security features of the devices
- Common security baseline
- Ensure effect of other controls

11. Secure Configurations for Network Devices

Defenses:

- Secure baseline config for devices
- Directory of configs with integrity protection
- Automated tool for checking differences to configurations
- Secure management solutions
- Keep software/firmware up to date

Sensors:

Network management system, config checking tool, SIEM, logging and alerting

12. Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Why is this important:

- Protect internal systems with building a hardened perimeter
- There are some systems we cannot protect with host-based functions

12. Boundary Defense

Defenses:

- Filter malicious or invalid addresses
- Analyze and log traffic passing the perimeter
- IDS+IPS
- Secure remote access with e.g. Two-factor auth
- Secure DNS

Sensors:

Firewall, secure routing, centralised authentication, configuration enforcement, network management, SIEM, logging and alerting

13. Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Why is this important:

- Avoid leaking sensitive/valuable information
- Limit damage with monitoring access to such information

13. Data Protection

Defenses:

- Identify sensitive/valuable information
- Deploy cryptograpic solutions for securing data at rest
- Network-based systems to monitor access to data
- Periodic host scans
- DLP
- Scan for unnecessary crypto

Sensors:

Encryption systems, DLP, endpoint protection, logigng and alerting

14. Controlled Access Based on Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Why is this important:

- Similar to restrictive use of privileged accounts: reducing attack surface
- Here focus on data access

14. Controlled Access Based on Need to Know

Defenses:

- Role-based Access Control
- Network segmentation, service zones
- Use of crypto for data in transit
- Use Access Control Lists
- Secure data at rest and audit access

Sensors:

Network management, cryptograpic solutions, DLP, logging and alerting

15. Wireless Access Control

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.

Why is this important:

- Prevent unauthorized access
- Prevent eavesdropping
- Reduce mapping possibilities

15. Wireless Access Control

Defenses:

- Enforced security profile and configuration
- Search for rouge devices and access points
- Check hardware configuration for unnecessary wireless interfaces

Sensors:

Network level authentication, network management, configuration enforcement, SIEM, logging and alerting

16. Account Monitoring and Control

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Why is this important:

- No orphan accounts
- Avoid disgruntled employee risk
- Implement need-to-know

16. Account Monitoring and Control

Defenses:

- Remove orphaned accounts
- Have all accounts set an expiration date
- Process for disabling accounts on role change/termination
- Inactivity monitoring, profiling
- Monitor access to disabled/expried accounts

Sensors:

Identity and access management, configuration enforcement, centralised authentication system, SIEM, logging and alerting

17. Security Skills Assessment and Training

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Why is this important:

- Important to enable effective operation of other technical controls
- Earn support from the organization

17. Security Skills Assessment and Training

Defenses:

- Gap analysis
- Training to close gaps
- Security awareness program with validation
- Identify skills for critical roles and validate

18. Application Software Security

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

Why is this important:

- In-house software can be effective but also finding the organization has larger responsibility to find security flaws
- Internal processes in place for communicating errors between different roles

18. Application Software Security

Defenses:

- Up to date software environment
- Firewalls
- Explicit error checking, input validation and sanitization
- Testing: periodic and/or after modifications
- Separate environments for test/preprod/prod

Sensors:

Patch management, firewalling, code review, SIEM, logging and alerting.

19. Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Why is this important:

- When there is a problem, the organization needs to know what to do.
- Well-designed response limits damage

19. Incident Response and Management

Defenses:

- Written, offline available incident response procedures
- Assign duties and titles
- Assign decision responsibilities
- Use global time to help timestamping
- Encourage reporting of anomalies
- Periodic exercises

20. Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Why is this important:

- Real challenge for the organization
- External and internal penetration tests reveal weaknesses which are hard or not possible to find with other checks

20. Penetration Tests and Red Team Exercises

Defenses:

- Regular tests
- Pentest accounts should be only used for this purpose and monitored/disabled if not in use
- Create testbed to train for the exercises

Sensors:

Pentest system, SIEM, logging and alerting.

Conclusion

- Not all of the controls are feasible to implement in all systems, but they give a good foundation for planning
- Generally: limit access to what is needed and only run, for there is a validated need.
- Periodic checks and exercises to make things easier and professionally executed when there is a real problem