CyberSecurity: Top 20 Controls

ISACA Kampala Chapter CPD Event - 30 March 2017

By Bernard Wanyama - CISA, CGEIT, CRISC, CISM

Assume breach……

The CIS Top 20 Critical Security Controls

CIS, SANS, NSA and US Gov’t pioneered the concept of the Top 20 Critical Security Controls in 2008

Offense must inform defense approach

In essence, guidance for implementing cybersecurity controls

Pareto Logic: 80/20

Hygiene concept

Technical Coverage: Systems, Networks and Applications

Security Thinking

Organisational Security is best viewed as a continuum and not an end-state

Continuous Improvement

The Concept of Organisational Maturity

Hygiene concept

CSC #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.

Tools
Endpoint Security
Asset Management Tool
MDM

CSC #2: Inventory of Authorized and Unauthorized Software.

Tools
Endpoint Security
MDM
Asset Management

CSC #3:
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

Tools
Active Directory Policy
Orchestration Software
Network Config Management (Rancid, etc)

CSC #4: Continuous Vulnerability Assessment and Remediation

Tools
OpenVAS
Nessus
Qualys

CSC #5: Controlled Use of Administrative Privileges.

Tools
Logging & Alerting
Sudo for UNIX, Run As for Windows

CSC # 6: Maintenance, Monitoring and Analysis of Audit Logs

Tools
Logging software, SIEMs
Syslog, Event Log
Log Rhythm, Splunk, syslogD

CSC #7: Email and Web Browser Protections

Tools
Latest versions of browsers and email clients
Patch Management Tools

CSC #8:
Malware Defenses

Tools
Endpoint Protection
Network Malware Scanning (NGFW, NGIPS)
SIEMs

CSC #9: Limitation and Control of Network Ports, Protocols, and Services

Tools
Lockdown, SCAP, Configuration Management
Nmap & other port scanners

CSC #10:
Data Recovery Capability

Tools
Backup, backup, backup
Business Continuity Plans

CSC #11: Secure Configuration of Network Devices such as Firewalls, Routers and Switches

Tools
Lockdown - recommendations from CIS, vendors, Team Cymru
Configuration Management tools to track current vs baseline

CSC #12: Boundary Defense

Tools
Perimeter firewall, IPS, HoneyPot, Honey Net
Insider threat
Layered defenses - defence-in-depth

CSC #13: Data Protection

Tools
Access Control - Mandatory for sensitive information
File Integrity Monitoring, Database Integrity Monitoring
Data Leakage Prevention

CSC #14: Controlled Access based on the Need to Know

Tools
User rights matrix - regularly reviewed and signed off
Access Reports on daily, weekly basis

CSC #15: Wireless Access Control

Tools
PSK, WPA2, VPN, SSL-certificate based authentication
Wireless IPS, SIEM
Logging

CSC #16: Account Monitoring & Control

Tools
Logging & alerting - logrotate for UNIX
Database Activity Monitoring

CSC #17: Security Skills Assessment and Appropriate Training to Fill Gaps

Tools
Training & Staff Development

CSC #18: Application Software Security

Tools
Code reviews, black and whitebox testing, DevSecOps
App scanning (Accunetix, Qualys, etc)

CSC #19: Incident Response & Management

Tools
Incident Response Plan
Monitoring & Alerting
IPS, SIEM

CSC #20: Penetration Tests and Red Team Exercises

Tools
Simulations
Pen Tests, Issues Remediation

Implementation Guidance

Strategic, Board-level Initiative

Long term programme - 3 to 5 years

Phased approach - top 3 - top 5

Accountable Executives

Embed in organisational policies

Internal & External Auditors should make use of CIS benchmarks

Implementation Guidance

Top 5 Controls - Foundational Cyber Security Hygiene

Prioritisation is the key benefit

Implementation Guidance

Additional Resources

Current information about the CISControls as well as numerous working aids to assist in your implementation may be found at:

https://www.cisecurity.org

Includes FAQs, Posters, Spreadsheets, Measures of Success, etc

80%

The Top 5 controls will mitigate approximately 80% of the Internet-based attacks.

Assume breach.
Start the journey and keep going

Thanks!

Follow us online

Facebook: IsacaKampalaChapter

Twitter: @ISACAKampala

Web: www.isaca.or.ug