Cyber Essentials Certification Checklist

www.thecyphere.com info@thecyphere.com

1 FIREWALLS

- [ ] Prevent access to the firewall administrative interface from the Internet. Ensure it is protected with MFA (multi-factor authentication) and IP white-listed access if required.

- [ ] Change default administrative passwords to a strong and unique password or disable remote administrative access entirely

- [ ] Block unauthenticated inbound connections by default

1 FIREWALLS

- [ ] Block unauthenticated inbound connections by default
- [ ] Ensure that inbound firewall rules are aligned with business requirements and follow a change management process
- [ ] Review firewall rules regularly and remove outdated or unnecessary rules
- [ ] Ensure firewall firmware is kept up-to-date with the latest security patches

2 SECURE CONFIGURATION

- [ ] Change all default passwords or guessable account passwords
- [ ] Remove or disable unnecessary software, unnecessary user accounts and services
- [ ] Implement security settings that are appropriate for your organisation
- [ ] Ensure all network devices are configured to lock after a period of inactivity

2 SECURE CONFIGURATION

- [ ] Disable the auto-run feature without user authorisation to prevent malware execution
- [ ] For physical access to devices, biometric, PIN or password-based authentication must be in place
- [ ] Protect your chosen authentication methods against brute-force attacks by throttling the rate of attempts and device lockout
- [ ] Use technical controls to manage the quality of passwords.

3 USER ACCESS CONTROL

- [ ] Your organisation must have a process to create and approve user accounts

- [ ] Authenticate users with unique credentials before authorising access to applications, systems, services or devices

- [ ] Remove or disable user accounts when not required, i.e. leavers, inactive user accounts

- [ ] Remove or disable special access privileges (or admin accounts) when no longer required

3 USER ACCESS CONTROL

- [ ] Cloud services authentication must utilise multi-factor authentication (MFA) and implement MFA where available

- [ ] Use dedicated admin account for privileged tasks and don’t allow corporate email, web browsing or standard user activities

- [ ] Support users in selecting unique passwords by educating staff and providing usable, secure password storage.

3 USER ACCESS CONTROL

- [ ] Ensure that there is an established process to change passwords if you know/suspect a password/account has been compromised.

- [ ] Ensure MFA for all administrative accounts and accounts accessible from the Internet.

4 MALWARE PROTECTION

- [ ] A malware protection mechanism (antivirus software solution) must be in place on all devices in scope

- [ ] Anti-malware software must be configured to
  - prevent malware from running (file execution)
  - prevent the execution of malicious codes
  - prevent connections to malware infected websites over the Internet
  - updated in line with vendor recommendations

4 MALWARE PROTECTION

- [ ] Your organisation should have an approved application process, maintain a current list and be restricted by code-signing.

5 SECURITY UPDATE MANAGEMENT

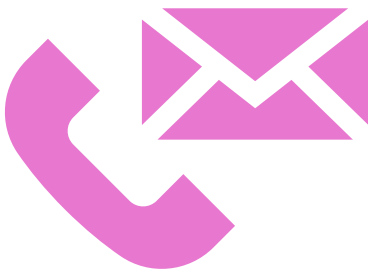
- [ ] All software on in-scope devices must:
  - be actively supported and licensed
  - be removed when it becomes unsupported software or removed from scope by using a defined subset (VLAN or firewall-based segregation) that prevents
  - have automatic updates enabled where possible

5 SECURITY UPDATE MANAGEMENT

- [ ] Ensure all patching updates, including manual configuration changes, are in place within 14 days of an update being released. This is applicable for critical or high-risk vulnerabilities (or CVSSv3 base score of 7 or higher)

Recap

1. Firewalls
2. Secure Configuration
3. User Access Control
4. Malware Protection
5. Security Update Management



Get in touch to discuss your CE+ plans