

May 9, 2025

- Firewalls
- Secure Configuration
- Security Update Management
- User Access Control
- Malware Protections

- Network Fragmentation and Monitoring
- Honeypots
- Pentesting

Cyber Essentials

UK Cyber Essentials

- Main Goal: Protection against the **most common** cyber threats
- **Not effective** against more advanced attacks such as:
 - Zero-Day Vulnerabilities: A security flaw built into software that is unknown to developers
 - Social Engineering
 - Advanced Persistent Threats
 - ...

Basic Requirements to protect IT infrastructure

- Firewalls
- Secure configuration
- Security Update Management
- User Access Control
- Malware protection

Scope of Cyber Essentials

- A corporation using Cyber Essentials should define the scope of their protection
 - What are the boundaries of the IT infrastructure that is the company's responsibility to protect
- Cyber Essential requirements should apply to all devices within this boundary that:
 - Accept communication from the internet from untrusted hosts
 - Establish outbound connections via the internet
 - Control the flow of data between any device in the boundary and the internet

Firewalls

Overview

- Make sure that only secure and necessary network services can be accessed from the internet
- They are a **network security device**
- They reduced exposure to attacks over the whole system
- Firewalls rules allow to blacklist or whitelist traffics based on their source, destination, protocol, etc

Requirements for Safety - By Cyber Essentials

- Block all inbound connections by default
- Every inbound rule that accepts connections must be **motivated** and documented
- Remove or disable unnecessary firewall rules quickly when no longer needed

Secure Configuration

Overview

- Ensure that network devices are properly configured
- Ensures the reduction in vulnerabilities
- Each device should only provide the services required to fulfil their role
- **Default** configurations are not always secure
 - Administrative account tends to have a default password
 - Unnecessary applications, bloatware, and services are usually installed on systems by default

Requirements by Cyber Essentials

- Remove or Disable unnecessary software
- Disable auto-run features
- Change default passwords
- Ensure users are authenticated before allowing them access to organisational data or services

Security Update Management

Overview

- **Aim:** Ensure that devices and software are not vulnerable to known security issues for which **fixes are available**
- Set of best practices for the maintenance and updating of software

Vendor Patches

- Vendors release patches for products they still support:
 - As soon as new vulnerabilities are discovered
 - Periodically

Requirements by Cyber Essentials

- All software must be licensed and supported, otherwise removed
- Have automatic software updates enabled where possible
- Make sure updates are applied (manually, if required) within 14 days from release
 - Especially for high-risk vulnerabilities

User Access Control

Overview

- **Aim:** Ensure that user accounts are assigned to **authorised** individuals only
- Provide access to only the assets that a user **requires** to carry out their role
- Reduces the risk of information being stolen or damaged

Requirements by Cyber Essentials

- Setup a process to create and approve a new user account
- Always authenticate users before granting access to an application or device
- Remove or disable accounts when no longer required
- Remove or disable special access privileges when no longer required
- Implement MFA where available
- Use separate accounts for higher-ups - admin account for admin stuff only for better security
 - Reduces the likelihood that a higher privilege account is compromised

Malware Protections

Overview

- **Aim:** Restrict execution of known malware and unknown software
- Verify if software is malicious
- Reduce the risk of damage caused by malicious code

Requirements by Cyber Essentials

- Anti Malware software should be used in line with **vendor recommendations**
- Application whitelisting should be used:
 - Only approved applications are allowed to execute on devices

Additional Cyber Defences

Data Protection

- Understand the risk
- Use encryption
- Fragmentation
 - Split up data into multiple pieces, stored in diverse locations
 - Makes it more difficult for bad actors to reach the whole scope of the data
- Data Backup
- Privacy Protection

Segregation of Duties

- **Basics:** Have more than one person required to complete a **critical** task
- If N accounts are required to execute a security-critical task - N unique accounts should be compromised to undermine such task
- Example:
 - In banking, all sensitive orders should be signed off by at least 2 people from 2 different departments

Network Fragmentation and Monitoring

Fragmentation

- Split infrastructure based on different properties
 - Business processes
 - Necessary exposure
 - Risk levels
- Use firewalls at all boundaries of the fragmentation

Monitoring

- Use Intrusion Detection/Prevention systems (ID/PS)
 - Observe and record all traffic on a given network
 - Block malicious traffic
 - Two main approaches:
 - Signature-based: Match traffic patterns against known attack signatures
 - Anomaly-based: Detect deviations from normal traffic patterns
 - Alert on suspicious traffic
- Use machine learning techniques
 - Accuracy
 - Explainability
 - Adversarial learning

Honeypots

Honeypots Overview

- Using a **decoy** to lure attackers
 - Hardware, Software and data that simulates a real system but is actually isolated
 - Detects attacks, deflects the attackers, and **gathers info** on potential attacks on the *real system*
 - Can be used to study attacker behavior and techniques
- Types of honeypots:
 - **Research honeypots**: Used to gather intelligence about attack methods
 - **Production honeypots**: Deployed to protect organization
 - **Pure honeypots**: Full-scale production systems with sensors
 - **High-interaction**: Provide real operating systems for attackers to interact with
 - **Low-interaction**: Simulate only specific services
- Key considerations:
 - Must be effectively isolated from production systems
 - Should appear authentic to attackers
 - Need constant monitoring and maintenance
 - Legal implications of trapping attackers

Pentesting

What is Penetration Testing?

- An authorized simulated cyberattack on a computer system
- Performed to evaluate the security of the system by:
 - Identifying technical vulnerabilities
 - Testing security controls
 - Validating security policies
 - Verifying incident response capabilities
- Provides actionable recommendations for improving security

Types of Pentesting

- Black Box Testing:
 - Tester has no prior knowledge of the system
- White Box Testing:
 - Full system information is provided
- Gray Box Testing:
 - Limited information provided

Essential Pentesting Phases

- Planning:
 - Scope definition
 - Rules of engagement
 - Timeline and objectives
- Intelligence Gathering:
 - OSINT collection
 - Network/system mapping
 - Technology identification
- Vulnerability Assessment:
 - Automated scanning
 - Manual testing
 - Validation of findings
- Exploitation:
 - Proof of concept
 - Privilege escalation
 - Lateral movement
- Reporting:
 - Findings documentation
 - Risk assessment
 - Remediation guidance

- Prevented the attack
- Mitigated the impact of the attack
- Been ineffective

Second Attack : the attacker bribes an insider who has physical access to the data centre of the corporation and can steal customer personal data

- **Data Protection:** *Mitigated* - Encryption and fragmentation would limit data access
- **Segregation of Duties:** *Ineffective* - Single compromised machine still allows network scanning
- **Network Fragmentation & Monitoring:** *Prevented* - IDS would detect scanning, firewalls limit access
- **Honeypots:** *Mitigated* - Could detect and study attacker's scanning behavior
- **Pentesting:** *Prevented* - Would identify email vulnerabilities and network security gaps

- **Data Protection:** *Mitigated* - Encrypted, fragmented data harder to steal
- **Segregation of Duties:** *Prevented* - Multiple people needed for data access
- **Network Fragmentation & Monitoring:** *Mitigated* - Unusual access patterns detected
- **Honeypots:** *Ineffective* - Insider knows real from fake systems
- **Pentesting:** *Mitigated* - Could identify physical security weaknesses