HM Government

CYBER ESSENTIALS

Cyber Essentials Scheme

Requirements for basic technical protection from cyber attacks

June 2014

Contents

Introduction

A primary objective of the UK Government's National Cyber Security Strategy is to make the UK a safer place to conduct business online. However, determining the benefits of cyber security and knowing where to start are a significant challenge for many organisations.

This document presents requirements for mitigating the most common Internet based threats to cyber security. Firstly specific types of attack are identified and secondly the most basic technical controls an organisation needs to have in place are described. Deploying these controls will assist every UK organisation in defending against the most common forms of cyber attack emanating from the internet using widely accessible tools which require little skill from the attackers. Organisations implementing these controls can benefit by gaining confidence that basic technical security measures are in place and that important steps are being taken to protect its information and the information of its customers.

The document was developed in collaboration with industry partners, including the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institution (BSI), and is endorsed by Government. The technical controls within this document focus on five essential mitigations within the context of the '10 Steps to Cyber Security'. They reflect those covered in well-established and more extensive cyber standards, such as the ISO/IEC 27000 series, the ISF's Standard of Good Practice for Information Security and the IASME Standard.

Who should use this document?

The control themes set out in this document are relevant to organisations of all sizes.

Large organisations would already be expected to have some knowledge or experience of Cyber security. However, like smaller companies, many still have limited capability to implement the full range of controls necessary to achieve robust cyber protection.

Small organisations (including single employee businesses), and even some medium-sized organisations, may need to obtain further guidance and support to ensure the technical controls presented in these requirements can be implemented adequately. Further details can be found on page 13 of this document.

What can these requirements help an organisation protect?

An organisation's exposed technology to common cyber attacks will typically include computers that are capable of connecting to the internet, including desktop PCs, laptops, tablets and smartphones, and internet connected servers including email, web and application servers.

Understanding and using this requirements document

Of the basic but successful cyber attacks against UK businesses and citizens of which Government has detailed knowledge, the large majority would have been mitigated by full implementation of the controls under the following, selected categories:

1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

To implement these requirements, organisations will need to determine the technology in scope, review each of the five categories and apply each control specified. Where a particular control cannot be implemented for a sound business reason (e.g. is not practical or possible) alternative controls should be identified and implemented.

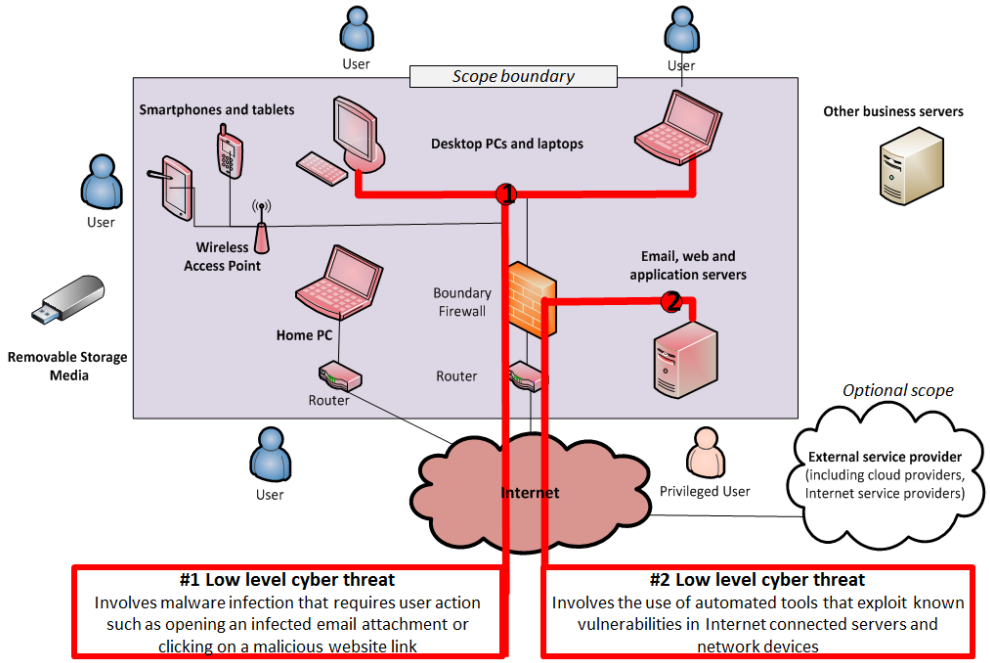


Figure 1: Scope of the requirements for basic technical protection

Many organisations allow employees to use their own computers for business purposes, often referred to as Bring Your Own Device (BYOD). As a result, such computers that handle sensitive information are in scope of this document.

Note

This document does not cover supporting detective and recovery controls or the management of information risk. Further guidance on comprehensive approaches to cyber security can be found in the standards referenced in Annex A.

Organisations wishing to demonstrate a level of assurance by implementing these requirements can do so using the Cyber Essentials Assurance Framework document

Threats Requiring Mitigation

By implementing Cyber Essentials, organisations are mitigating against the following common types of cyber attack::

1. Phishing: malware infection through users clicking on malicious e-mail attachments or website links.

2. Hacking: exploitation of known vulnerabilities in Internet connected servers and devices using widely available tools and techniques.

Controls required for basic technical cyber protection

To mitigate the threats identified above, Cyber Essentials requires implementation of the following controls.

1. Boundary firewalls and internet gateways

Objectives

Information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Introduction

Without a correctly configured boundary firewall, internet gateway or equivalent network device, between the organisation's network of computers and the internet, cyber attackers can often gain access to these computers with ease and access the information they contain.

A boundary firewall can protect against commodity cyber threats – that is, attacks based on capabilities and techniques that are freely available on the internet – by restricting inbound and outbound network traffic to authorised connections. Such restrictions are achieved by applying configuration settings known as firewall rules.

Basic technical cyber protection for boundary firewalls and internet gateways

One or more firewalls (or equivalent network device) should be installed on the boundary of the organisation's internal network(s). As a minimum:

1. The default administrative password for any firewall (or equivalent network device) should be changed to an alternative, strong password.

2. Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall) should be subject to

approval by an authorised individual and documented (including an explanation of business need).

3. Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), should be disabled (blocked) at the boundary firewall by default.

4. Firewall rules that are no longer required (e.g. because a service is no longer required) should be removed or disabled in a timely manner.

5. The administrative interface used to manage boundary firewall configuration should not be accessible from the internet.

A strong password is typically one that: comprises a minimum number of characters in length (e.g. eight characters); differs from the associated username; contains no more than two identical characters in a row; is not a dictionary word; includes a mixture of numeric and alpha characters; has not been reused within a predetermined period of time (e.g. six months); and has not been used for another account.

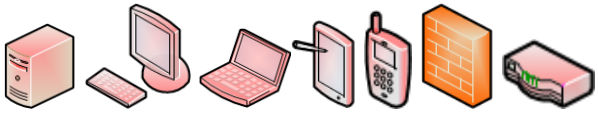
Alternative controls

In situations where the administrative interface needs to be accessible from the internet (e.g. because it is supported by a remote administrator or external service provider) the interface should be protected by additional security arrangements, which include using a strong password, encrypting the connection (e.g. using SSL), restricting access to a limited number of authorised individuals and only enabling the administrative interface for the period it is required.

2. Secure configuration

Objectives

Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.



Introduction

Computers and network devices cannot be considered secure upon default installation. A standard, 'out-of-the-box' configuration can often include an administrative account with a predetermined, publicly known default password, one or more unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications (or services).

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information, often with ease. By applying some simple security controls when installing computers and network devices (a technique typically referred to as system hardening), inherent weaknesses can be minimised, providing increased protection against commodity cyber attacks.

Basic technical cyber protection for secure configuration

Computers and network devices (including wireless access points) should be securely configured. As a minimum:

1. Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled.

2. Any default password for a user account should be changed to an alternative, strong password.

3. Unnecessary software (including application, system utilities and network services) should be removed or disabled.

4. The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).

5. A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.

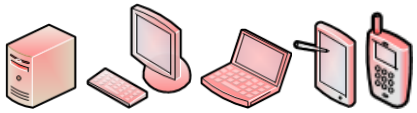
A personal firewall (sometimes referred to as a host-based firewall) is software that is

typically installed on a computer (often as part of the operating system) to restrict inbound and outbound network connections to and from authorised applications, such as a web browser or email.

3. User access control

Objectives

User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.



Introduction

User accounts with special access privileges (e.g. administrative accounts) typically have the greatest level of access to information, applications and computers. When privileged accounts are compromised their level of access can be exploited resulting in large scale corruption of information, affected business processes and unauthorised access to other computers across an organisation.

To protect against misuse of special access privileges, the principle of least privilege should be applied to user accounts by limiting the privileges granted and restricting access.

Basic technical cyber protection for secure configuration

User accounts should be managed through robust access control. As a minimum:

1. All user account creation should be subject to a provisioning and approval process.

2. Special access privileges should be restricted to a limited number of authorised individuals.

3. Details about special access privileges (e.g. the individual and purpose) should be documented, kept in a secure location and reviewed on a regular basis (e.g. quarterly).

4. Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the internet.

5. Administrative accounts should be configured to require a password change on a regular basis (e.g. at least every 60 days).

6. Each user should authenticate using a unique username and strong password before being granted access to applications, computers and network devices.

7. User accounts and special access privileges should be removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a pre-defined period of inactivity (e.g. 3 months).

4. Malware protection

Objectives

Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software.

Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform unauthorised functions on one or more computers.

Introduction

Computers are often vulnerable to malicious software, particularly those that are exposed to the internet (e.g. desktop PCs, laptops and mobile devices, where available). When available, dedicated software is required that will monitor for, detect and disable malware.

Computers can be infected with malware through various means often involving a user who opens an affected email, browses a compromised website or opens an unknown file on a removable storage media.

Basic technical cyber protection for malware

The organisation should implement robust malware protection on exposed computers. As a minimum:

1. Malware protection software should be installed on all computers that are connected to or capable of connecting to the internet.

2. Malware protection software (including program code and malware signature files) should be kept up-to-date (e.g. at least daily, either by configuring it to update automatically or through the use of centrally managed deployment).

3. Malware protection software should be configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed (via a web browser).

4. Malware protection software should be configured to perform regular scans of all files (e.g. daily).

5. Malware protection software should prevent connections to malicious websites on the internet (e.g. by using website blacklisting).

The scope of malware protection in this document covers desktop PCs, laptops and

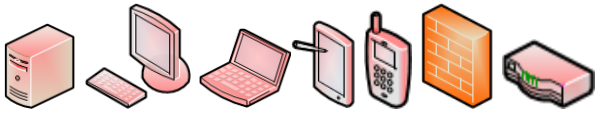
servers that have access to or are accessible from the internet. Other computers used in the organisation, while out of scope are likely to need protection against malware as will some forms of tablets and smartphones.

Website blacklisting is a technique used to help prevent web browsers connecting to unauthorised websites. The blacklist effectively contains a list of malicious or suspicious websites that is checked each time the web browser attempts a connection.

5. Patch management

Objectives

Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.



Introduction

Any computer and network device that runs software can contain weaknesses or flaws, typically referred to as technical vulnerabilities. Vulnerabilities are common in many types of popular software, are frequently being discovered (e.g. daily), and once known can quickly be deliberately misused (exploited) by malicious individuals or groups to attack an organisation's computers and networks.

Vendors of software will typically try to provide fixes for identified vulnerabilities as soon as possible, in the form of software updates known as patches, and release them to their customers (sometimes using a formal release schedule such as weekly). To help avoid becoming a victim of cyber attacks that exploit software vulnerabilities, an organisation needs to manage patches and the update of software effectively.

Basic technical cyber protection for patch management

Software should be kept up-to-date. As a minimum:

1. Software running on computers and network devices that are connected to or capable of connecting to the internet should be licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available.

2. Updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner (e.g. within 30 days of release or automatically when they become available from vendors).

3. Out-of-date software (i.e. software that is no longer supported) should be removed from computer and network devices that are connected to or capable of connecting to the internet.

4. All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner (e.g. within 14 days of release or automatically when they become available from vendors).

Where to go for more information

The guidance provided in this document represents a small yet essential part of defending against cyber threats. It does not present all of the security controls an organisation needs to have in place to protect against a broad range of threats, particularly those that are sophisticated threats (i.e. a threat with significant capability, funding and resource, typically known as advanced persistent threats).

Responding to and managing the vast range of cyber threats that UK organisations continue to face is a significant undertaking, involving the investment of people, money and time. Regardless of their size, use of technology, the industry sector in which they operate and their global presence, every organisation needs to implement a robust and effective approach to cyber security.

To be successful, such an approach to cyber security requires direction to be set by executive management, effective planning and decision making across the organisation and a comprehensive programme of activities based on key principles for managing cyber risk. These activities are covered in the supporting standards shown in the table below.

Ref	Supporting standards and guidance
1	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems – Requirements ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
2	Information Security Forum – The Standard of Good Practice for Information Security (2013)
3	The IASME Consortium – The Standard for Information Assurance for Small and Medium Sized Enterprises – (2013)
4	HMG 10 Steps to Cyber Security

Further advice is available through the CESG Listed Advisor Scheme detailed at www.cesg.gov.uk/servicecatalogue/CLAS/Pages/CLAS.aspx.

Details of where corresponding controls, covered in this document, reside in supporting standards are presented in the following table.

Standard	1. Boundary Firewalls and internet Gateways	2. Secure Configuration	3. Access Control	4. Malware Protection	5. Patch Management
ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems – Requirements ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls	A.13.1 Network Security Management	A.12.1 Operational Procedures and Responsibilities	A.9.2 User Access Management	A.12.2 Protection from Malware	A.12.6 Technical Vulnerability Management
Information Security Forum – The Standard of Good Practice for Information Security (2013)	CF9 Network Management	CF7 System Management CF 9 Network Management CF14 Mobile Device Configuration	CF6 Access Management	CF10 Threat and Vulnerability Management	CF10 Threat and Vulnerability Management
The IASME Consortium – The Standard for Information Assurance for Small and Medium Sized Enterprises – (2013)	4.9 Malware and Technical Intrusion	4.8 Access Control	4.8 Access Control	4.9 Malware and Technical Intrusion	4.7 Operations and Management
10 Steps to Cyber Security	3 Network Security	2 Secure Configuration	4 Managing User Privileges	7 Malware Prevention 9 Removable Media Controls	2 Secure Configuration

Annex A: Where these requirements are covered in other cyber standards

Organisations wishing to understand or address how these requirements fit into a broader cyber risk framework or obtain further information about different aspects of managing cyber risk should consult the following standards.

ISO/IEC 27001/2	ISF SOGP	IASME	10 Steps
A.5 Information security Policies	CF1 Security Policy and Organisation	4.3 Policy and Compliance	1 Information risk management regime
A.6 Organisation of information security	CF1 Security Policy and Organisation	4.1 Organisation	1 Information risk management regime
A.7 Human resource security	CF2 Human Resource Security	4.5 People	5 User education and awareness
A.8 Asset management	CF3 Asset Management	4.4 Assets	2 Secure configuration
A.9 Access Control	CF5 Customer Access CF6 Access Management	4.8 Access control	4 Managing user privileges
A.10 Cryptography	CF8 Technical Security Infrastructure		
A.11 Physical and environmental security	CF19 Physical and Environmental Security	4.6 Physical and environmental protection	
A.12 Operations Security	CF10 Threat and Vulnerability management CF7 System Management CF 9 Network Management CF14 Mobile Device Configuration	4.7 Operations and management 4.8 Access Control 4.9 Malware and technical intrusion 4.11 Backup and Restore 4.10 Monitoring	2 Secure configuration 7 Malware prevention 8 Monitoring 9 Removable media controls
A.13 Communications Security	CF9 Network Management CF15 Electronic Communications	4.9 Malware and technical intrusion	3 Network security
A.14 System acquisition, development and maintenance	CF4 Business Applications CF13 Desktop Applications CF17 System Development Management CF18 Systems Development Lifecycle	4.7 Operations and management	
A.15 Supplier relationships	CF16 External Supplier Management	4.7 Operations and management	
A.16 Information security incident management	CF11 Incident Management	4.12 Incident Management	6 Incident management
A.17 Information security aspects of business continuity management	CF20 Business Continuity	4.13 Disaster Recovery/Business Continuity	

A.18 Compliance	SR2 Compliance	4.3 Policy and Compliance	
	SG1 Security Governance Approach	4.1 Organisation	1 Information risk management regime
	SG2 Security Governance Components	4.1 Organisation	1 Information risk management regime
	SR1 Information Risk Assessment	4.2 Assessing the risk	1 Information risk management regime
	CF7 System Management	4.7 Operations and Management 4.11 Backup and Restore	
	CF12 Local Environments		
	CF14 Mobile Computing	4.4 Assets	9 Removable media controls 10 Home and mobile working
	SI1 Security Audit		
	SI2 Security Performance	4.10 Monitoring	8 Monitoring

© Crown copyright 2014

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. Visit www.nationalarchives.gov.uk/doc/open-government-licence, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

This publication is also available on our website at www.bis.gov.uk

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/14/696