CYBER ESSENTIALS

AN INTRODUCTION

STEVE CAST, MD REDBOURN BUSINESS SYSTEMS

CYBER ESSENTIALS

This presentation introduces the topic and looks at the essential elements of the framework and explores the relevance for IBM i.

Attendees will leave with a clearer understanding of the Cyber Essentials program, the five technical controls and how to start the certification process for their organisation.

INTRODUCING:
STEVE CAST, MD REDBOURN BUSINESS SYSTEMS

Technical background as an RPG and CA:2E (Synon) developer

Formed Redbourn Business Systems in 1994, now 20+ staff and £3M turnover

After several years on the i-UG committee, joined the i-UG board in 2020 as Marketing Director

Recently appointed as IT Director of Bruni Erben

CYBER ESSENTIALS…

the

WHAT,
WHO,
WHY,
WHERE,
HOW
AND
WHEN

WHAT IS CYBER ESSENTIALS?

Cyber Essentials is a United Kingdom government information assurance scheme that is operated by the National Cyber Security Centre.

It encourages organisations to adopt good practice in information security.

Cyber Essentials also includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.

National Cyber Security Centre
a part of GCHQ

WHAT IS CYBER ESSENTIALS?

Cyber Essentials is a United Kingdom government information assurance scheme that is operated by the National Cyber Security Centre.

It encourages organisations to adopt good practice in information security.

Cyber Essentials also includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.

WHAT IS CYBER ESSENTIALS?

The Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials

WHAT IS CYBER ESSENTIALS?

It is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations which are offering incentives for businesses.

WHAT IS CYBER ESSENTIALS?

The full scheme, launched in 2014, enables organisations to gain one of two Cyber Essentials badges.

WHAT IS CYBER ESSENTIALS?

- A self-assessment option that gives you protection against a wide variety of the most common cyber attacks. This is important because vulnerability to simple attacks can mark you out as target for more in-depth unwanted attention from cyber criminals and others.
- Certification gives peace of mind that your defences will protect against the vast majority of common cyber attacks.

  Attackers are looking for targets which do not have the Cyber Essentials technical controls in place.

WHAT IS CYBER ESSENTIALS?

- Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same,

  but

  for Cyber Essentials Plus a hands-on technical verification is carried out.

CYBER ESSENTIALS WHO IS IT FOR?

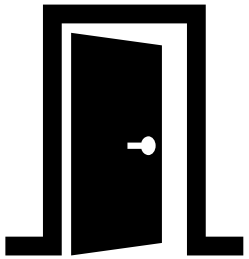
Cyber Essentials is suitable for all organisations, of any size, in any sector.

WHY CYBER ESSENTIALS?

The vast majority of cyber attacks are very basic in nature, carried out by relatively unskilled individuals.

The digital equivalent of a thief trying your front door to see if it's unlocked.

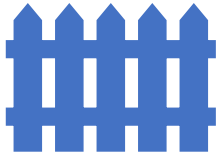
The guidance provided under Cyber Essentials is designed to protect your organisation from these attacks.



WHY CYBER ESSENTIALS?

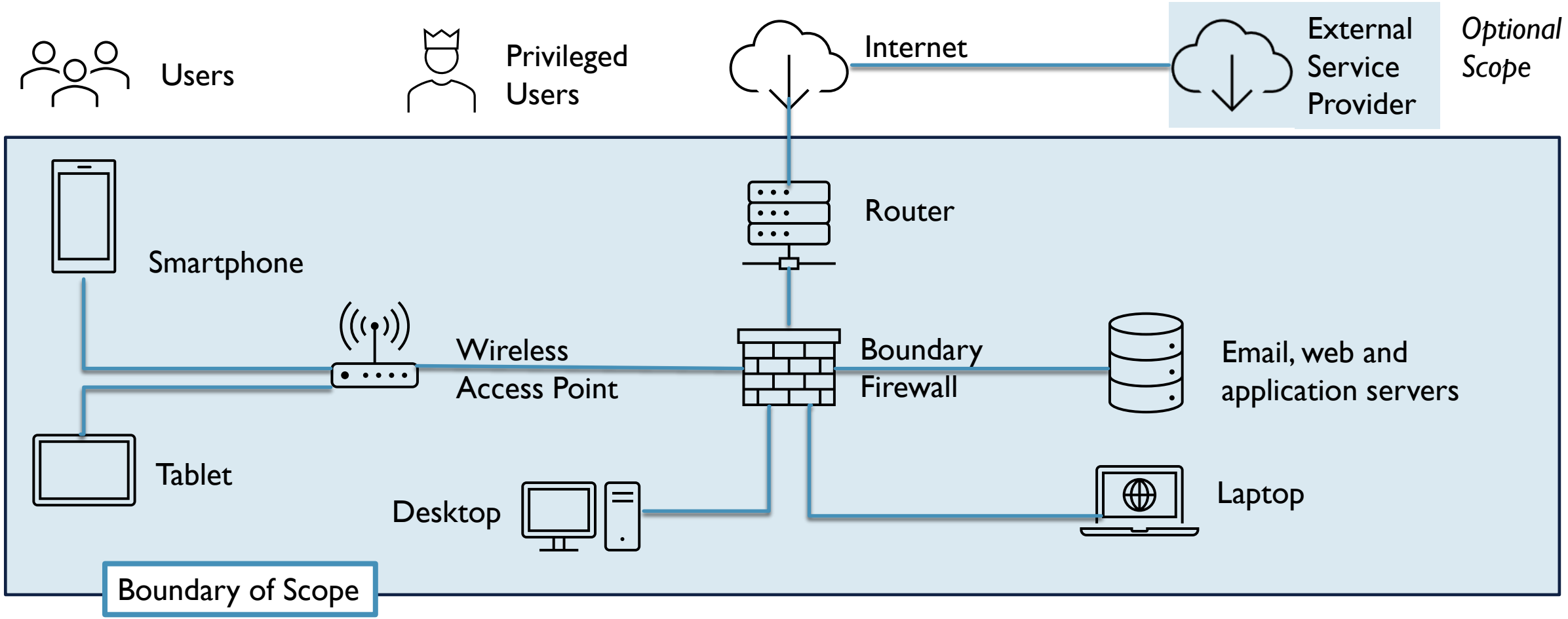
- Reassure customers that you are working to secure your IT against cyber attack
- Attract new business with the promise you have cyber security measures in place
- You have a clear picture of your organisation's cyber security level
- Some Government contracts require Cyber Essentials certification
- Be listed on the directory of organisations awarded Cyber Essentials

CYBER ESSENTIALS WHERE DOES IT APPLY?

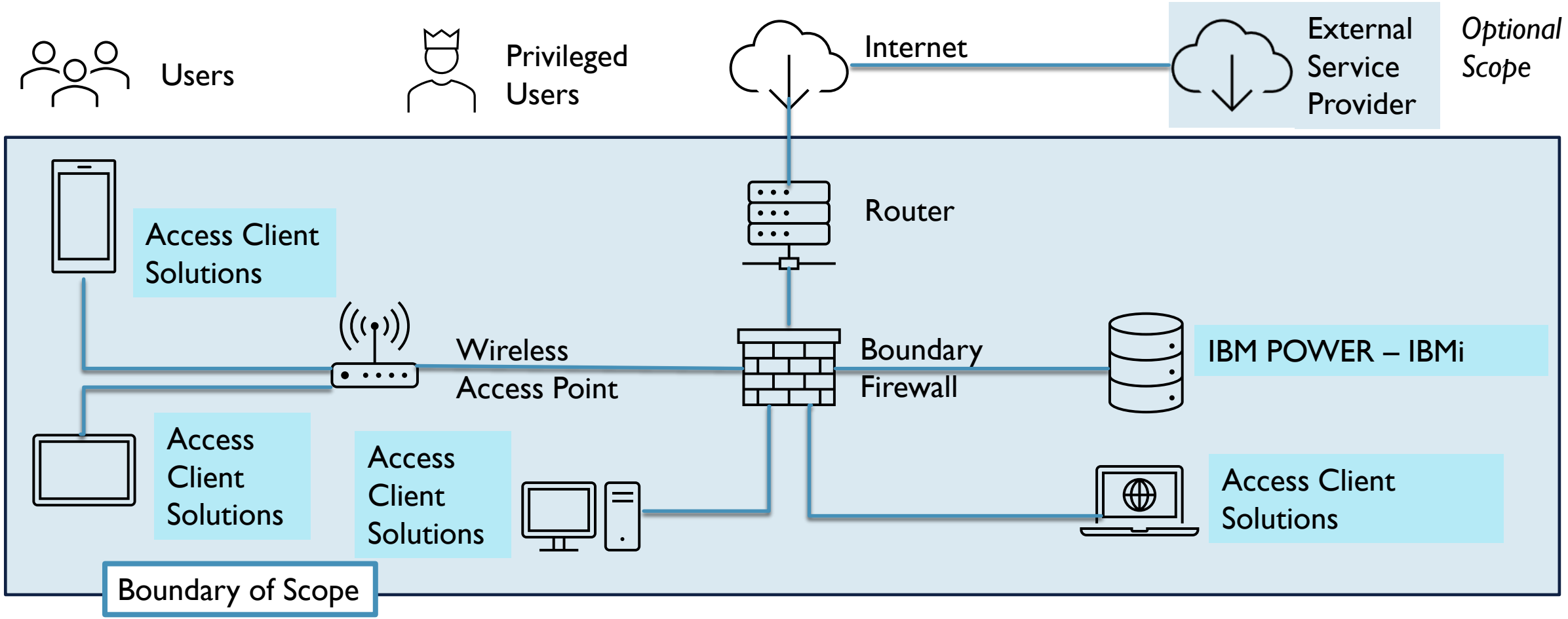


Establish the boundary of scope.

Determine what is in scope within this boundary.



DETERMINING THE SCOPE BOUNDARY – *CAN BE COMPLEX!*



DETERMINING THE SCOPE BOUNDARY – IBM POWER - IBMi CONTEXT

CYBER ESSENTIALS THE FIVE CONTROL THEMES

Review each of the five technical control themes and the controls they embody as requirements

CYBER ESSENTIALS - WHERE MUST YOU INTRODUCE CONTROLS?

Firewalls

Secure Configuration

User Access Control

Malware Protection

Patch Management

FIREWALLS

CYBER ESSENTIALS - CONTROL THEMES

FIREWALLS

Applies To:

Boundary firewalls; desktop computers; laptop computers; routers; servers (including IBMi)

Objective:

Ensure that only safe and necessary network services can be accessed from the Internet.

FIREWALLS

Introduction

All devices run network services, which create some form of communication with other devices and services.

By restricting access to these services, you reduce your exposure to attacks. This can be achieved using firewalls and equivalent network devices.

A boundary firewall is a network device which can restrict the inbound and outbound network traffic to services on its network of computers and mobile devices.

It can help protect against cyber attacks Cyber Essentials: Requirements for IT infrastructure by implementing restrictions, known as ‘firewall rules’, which can allow or block traffic according to its source, destination and type of communication protocol.

FIREWALLS

Introduction

Alternatively, a host-based firewall may be configured on a device. This works in the same way as a boundary firewall but only protects the single device on which it is configured.

This approach can provide for more tailored rules and means that the rules apply to the device wherever it is used.

However, this increases the administrative overhead of managing firewall rules.

An IBMi option

REQUIREMENTS UNDER THE FIREWALL CONTROL SCHEME

Every device that is in scope must be protected by a correctly configured firewall (or equivalent network device).

REQUIREMENTS UNDER THE FIREWALL CONTROL SCHEME

Change any default administrative password to an alternative that is difficult to guess, or disable remote administrative access entirely.

REQUIREMENTS UNDER THE FIREWALL CONTROL SCHEME

Prevent access to the administrative interface (used to manage the Firewall configuration) from the Internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:

- A second authentication factor, such as a one-time token
- An IP allow list that limits access to a small range of trusted addresses

REQUIREMENTS UNDER THE FIREWALL CONTROL SCHEME

Block unauthenticated inbound connections by default

REQUIREMENTS UNDER THE FIREWALL CONTROL SCHEME

Ensure inbound firewall rules are approved and documented by an authorised individual.

The business need must be included in the documentation

REQUIREMENTS UNDER THE FIREWALL CONTROL SCHEME

Remove or disable permissive firewall rules quickly, when they are no longer needed.

Use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

SECURE CONFIGURATION

CYBER ESSENTIALS - CONTROL THEMES

SECURE CONFIGURATION

Applies To:

email, web, and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers

(including IBMi)

Objective:

Ensure that computers and network devices are properly configured to:

- Reduce the level of inherent vulnerabilities.
- Provide only the services required to fulfil their role.

SECURE CONFIGURATION

Introduction

Computers and network devices are not always secure in their default configurations. Standard, "out of-the-box" configurations often include one or more weak points such as:

- An administrative account with a predetermined, publicly known default password. (QSECOFR?)
- Pre-enabled but unnecessary user accounts (sometimes with special access privileges) (QPGMR?)
- 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 technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Computers and Network Devices

An Applicant must be active in its management of computers and network devices.

REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)

QPGMR/QUSER?

REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Change any default or guessable account passwords to something non-obvious.

QPGMR/QPGMR

QUSER/QUSER

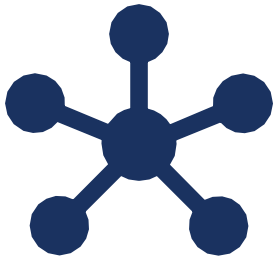
REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Remove or disable unnecessary software (including applications, system utilities and network services)

NETSERVER?

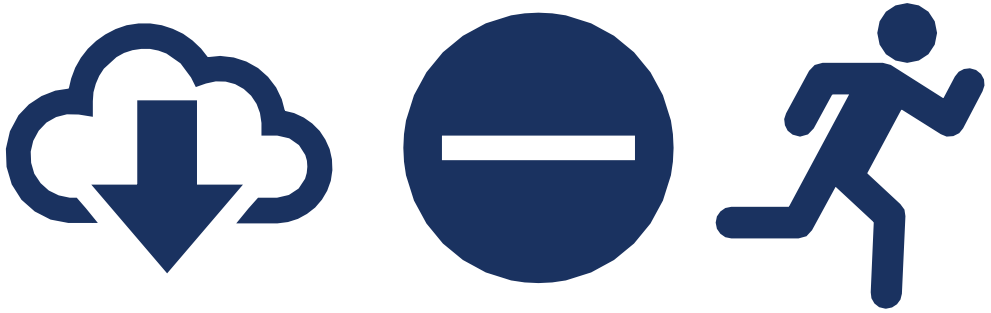
SSH?

FTP?



REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the Internet)



REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Authenticate users before allowing Internet-based access to commercially or personally sensitive data, or data which is critical to the running of the organisation.

REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

<u>Password-based Authentication</u>

An Applicant must make good use of the technical controls available to it on password-protected systems.

As much as is reasonably practicable, technical controls and policies must shift the burden away from individual users and reduce reliance on them knowing and using good practices.

Users are still expected to pick sensible passwords.

REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Protect against brute-force password guessing, by using at least one of the following methods:

- lock accounts after no more than 10 unsuccessful attempts
- limit the number of guesses allowed in a specified time period to no more than 10 guesses within 5 minutes

See System Values:

WRKSYSVAL SYSVAL(*SEC)

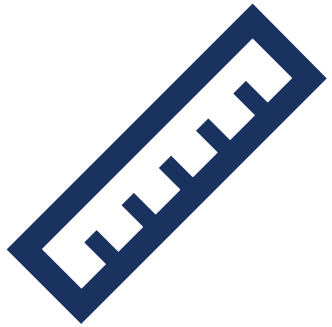
REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Set a minimum password length of at least 8 characters.

Do not set a maximum password length.

"Gotcha" QDSIGNON to QDSIGNON2,

or you cannot logon to a green screen



REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

Change passwords promptly when the Applicant knows or suspects they have been compromised.

REQUIREMENTS UNDER THE SECURE CONFIGURATION CONTROL SCHEME

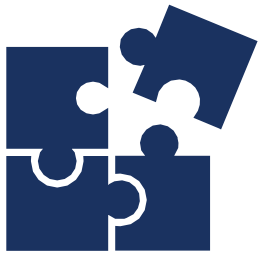
Have a password policy that tells users:

- How to avoid choosing obvious passwords (such as those based on easily discoverable information like the name of a favourite pet)
- Not to choose common passwords — this could be implemented by technical means, using a password deny list
- Not to use the same password anywhere else, at work or at home
- Where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard
- If they may use password management software — if so, which software and how
- Which passwords they really must memorise and not record anywhere

NOT REQUIRED UNDER THE SECURE CONFIGURATION CONTROL SCHEME

The Applicant is NOT required to:

- Enforce regular password expiry for any account
- Enforce password complexity requirements



USER ACCESS CONTROL

CYBER ESSENTIALS - CONTROL THEMES

USER ACCESS CONTROL

Applies To:

email, web and application servers; desktop computers; laptop computers; tablets; mobile phones.

(including IBMi)

Objective:

Ensure user accounts:

- Are assigned to authorised individuals only
- Provide access to only those applications, computers and networks actually required for the user to perform their role

USER ACCESS CONTROL

Introduction

Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information.

By ensuring that only authorised individuals have user accounts, and that they are granted only as much access as they need to perform their role, you reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information.

When such accounts are compromised, their greater freedoms can be exploited to facilitate large-scale corruption of information, disruption to business processes and unauthorised access to other devices in the organisation.

USER ACCESS CONTROL

Introduction

'Administrative accounts' are especially highly privileged, for example.

Such accounts typically allow:

- Execution of software that has the ability to make significant and security relevant changes to the operating system Changes to the operating system for some or all users
- Creation of new accounts and allocation of their privileges

All types of Administrator will have such accounts, including Domain Administrators and Local Administrators.

Now consider that if a user opens a malicious URL or email attachment, any associated malware is typically executed with the privilege level of the account that user is currently operating.

QSECOFR, QSECOFR, *SECADM, *SECOFR, *SYSOPR, *ALLOBJ

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

The Applicant must be in control of its user accounts and the access privileges granted to each user account. It must also understand how user accounts authenticate and control the strength of that authentication.

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Have a user account creation and approval process

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Authenticate users before granting access to applications or devices, using unique credentials

~~QUSER~~

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Authenticate users before granting access to applications or devices, using unique credentials

~~QUSER~~

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Remove or disable user accounts when no longer required

(when a user leaves the organisation or after a defined period of account inactivity, for example)

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Implement two-factor authentication, where available

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Use administrative accounts to perform administrative activities only

(no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)

REQUIREMENTS UNDER THE USER ACCESS CONTROL SCHEME

Remove or disable special access privileges when no longer required

(when a member of staff changes role, for example)

MALWARE PROTECTION

CYBER ESSENTIALS - CONTROL THEMES

MALWARE PROTECTION

Applies To:

desktop computers; laptop computers; tablets; mobile phones.

Objective:

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

MALWARE PROTECTION

Introduction

The execution of software downloaded from the Internet can expose a device to malware infection.

Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform malicious actions.

Potential sources of malware infection include malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

MALWARE PROTECTION

Introduction

If a system is infected with malware, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

You can largely avoid the potential for harm from malware by:

- Detecting and disabling malware before it causes harm (anti-malware)
- Executing only software that you know to be worthy of trust (allow listing)
- Executing untrusted software in an environment that controls access to other data (sandboxing)

REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

The Applicant must implement a malware protection mechanism on all devices that are in scope.

For each such device, the Applicant must use at least one of the three mechanisms that follow:

REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

ANTI-MALWARE SOFTWARE

The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily.

This may be achieved through automated updates, or with a centrally managed deployment.

REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

ANTI-MALWARE SOFTWARE

The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder. IFS

REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

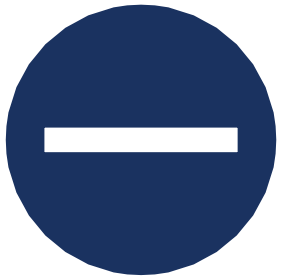
ANTI-MALWARE SOFTWARE

The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).

REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

ANTI-MALWARE SOFTWARE

The software must prevent connections to malicious websites on the Internet (by means of deny listing, for example) — unless there is a clear, documented business need and the Applicant understands and accepts the associated risk.



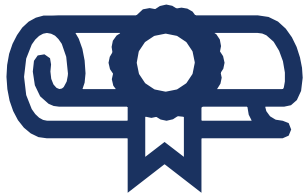
REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

APPLICATION ALLOW LISTING

Only approved applications, restricted by code signing, are allowed to execute on devices.

The Applicant must:

- actively approve such applications before deploying them to devices
- maintain a current list of approved applications. Users must not be able to install any application that is unsigned or has an invalid signature.



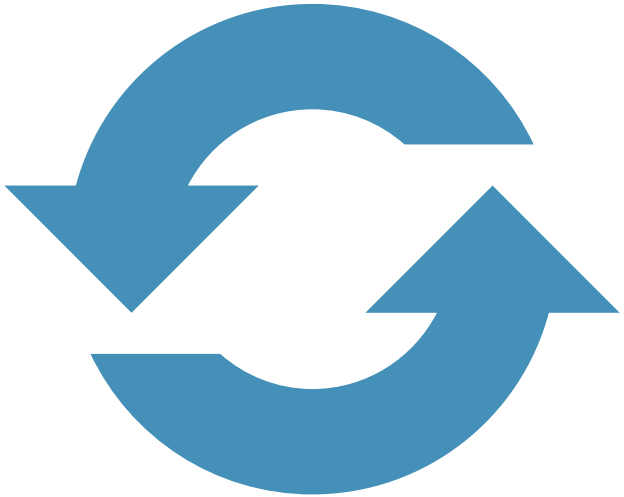
REQUIREMENTS UNDER THE MALWARE PROTECTION CONTROL SCHEME

APPLICATION SANDBOXING

All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user.

This includes:

- Other sandboxed applications
- Data stores, such as those holding documents and photos
- Sensitive peripherals, such as the camera, microphone and GPS
- Local network access



PATCH MANAGEMENT

CYBER ESSENTIALS - CONTROL THEMES

PATCH MANAGEMENT

Applies To:

Web, email and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

Including IBMi

Objective:

Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

PATCH MANAGEMENT

Introduction

Any device that runs software can contain security flaws, known as ‘vulnerabilities’.

Vulnerabilities are regularly discovered in all sorts of software.

Once discovered, malicious individuals or groups move quickly to misuse (or ‘exploit’) vulnerabilities to attack computers and networks in organisations with these weaknesses.

PATCH MANAGEMENT

Caution

Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of software updates known as ‘patches’.

Patches may be made available to customers immediately or on a regular release schedule (perhaps monthly).

REQUIREMENTS UNDER THE PATCH MANAGEMENT CONTROL SCHEME

The Applicant must keep all its software up to date.

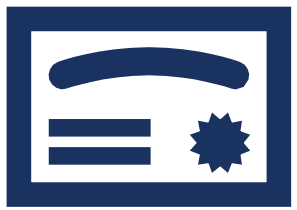
Software must be:

REQUIREMENTS UNDER THE PATCH MANAGEMENT CONTROL SCHEME

Licensed and supported

Operating System and Applications

!! V7R2 – 30th April 2021 !!



REQUIREMENTS UNDER THE PATCH MANAGEMENT CONTROL SCHEME

Removed from devices when no longer supported

REQUIREMENTS UNDER THE PATCH MANAGEMENT CONTROL SCHEME

Patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as 'critical' or 'high risk'

"Gotcha" - Some vendors release patches for multiple issues with differing severity levels as a single update. If such an update covers any 'critical' or 'high risk' issues then it must be installed within 14 days.

Subscribe to IBM notifications

HOW DO YOU GET CERTIFIED?

Cyber Essentials is a United Kingdom government information assurance scheme that is operated by the National Cyber Security Centre.

Cyber Essentials - NCSC.GOV.UK

Certification is available from the National Cyber Security Centre approved partner, the IASME Consortium.

Cyber Essentials Apply Now – Iasme

WHEN WILL YOU START?

Appling for a Cyber Essentials verified self assessment takes 10 minutes to do and costs £300.

Once you have applied you have 6 months to complete your self assessment questionnaire.

Cyber Essentials Apply Now – Iasme

You can review the questions and prepare your answers in advance:

Cyber Essentials only question booklet v11c (iasme.co.uk)

CYBER ESSENTIALS PLUS?

Remember -

Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same,

but

for Cyber Essentials Plus a hands-on technical verification is carried out.

QUESTIONS AND ANSWERS SESSION

THANK YOU

STEVE.CAST@REDBOURN.CO.UK

WWW.REDBOURN.CO.UK

REDBOURN BUSINESS SYSTEMS

THE PRIORY

HIGH STREET

REDBOURN

AL3 7LZ 01582 794229