MIDLANDCOMPUTERS

Security Review 2017

Sections 1-5 are from the Cyber Essentials scheme.

1. 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.

2. 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.

3. User access control

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).
8. Is full administrative access to computers given only to those users who really need it?

4. Malware protection

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).
6. Malware protection software should be configured to scan incoming email automatically

5. 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)

6. Other topics

These are not part of Cyber Essentials, but our own (standard) suggestions / recommendations:

1. BYOD (Bring Your Own Device): review policy regarding staff using their own devices on the company network (e.g. smartphones on Wi-Fi). Restrict this if appropriate.
2. User Education: users are now the first line of defence against ransomware and other malware. Consider implementing policy to educate users on risks of malware, e.g.:
    - how to spot phishing / spear phishing email
    - not to click links or open attachments unless certain of source
    - what to do if infected
    - if in doubt, ask IT before doing anything
3. Written policies: if they don't already exist, consider adopting official company IT policies.
4. Recommended password policy for standard users: this is not mentioned in the Cyber Essentials scheme (only admin accounts are).
    - Do not select "password never expires" on standard user accounts; instead, configure the password policy (even if policy states passwords never expire)
    - Implement policy agreed with management, considering:
        - Risks of insecure password policies
        - User impact of more stringent policies
        - Effect on IT support workload of stricter policies

- Suggested example policy settings:
    - History: 24 passwords remembered
    - Max age: 180 days
    - Min age: 7 days
    - Min length: 7 characters
    - Complexity: Enabled
    - Account lockout: After 10 failed attempts (account must then be unlocked by admin)
- Immediately disable a user account when staff member leaves

5. Other password recommendations:
    - Use separate accounts with strong passwords and least required privilege rather than domain admin to run:
        - application services, e.g. SQL
        - scheduled tasks
    - Set up new account for domain admin use, disable built-in administrator account
    - Optionally, use different admin accounts for each admin user (e.g. MidlandAdmin, JoeBloggsAdmin, etc.) with no shared knowledge of passwords
6. Folder permissions: review and apply least privilege, i.e.:
    - read-only access where nothing more is required
    - modify access (rather than full control) if read/write/delete access required (because users don't need to be able to change the permissions on files)
7. Group membership:
    - review semi-regularly
    - apply access by group, not individual

MIDLANDCOMPUTERS

Our Services

We are a Telford-based business to business IT support company, specialising in a range of services from cloud hosting, virtualisation, business continuity and more. We are a Microsoft Gold Partner and pride ourselves in delivering the best IT solutions for your business with our comprehensive technology services, hardware, data centre and ongoing support.

With over 15 years' experience serving clients both in the Shropshire and West Midlands area and further afield, we have long standing relationships with a diverse mix of customers covering different sectors across the globe building on an excellent reputation and offering an exceptional range of services which extends well beyond basic hardware and software.

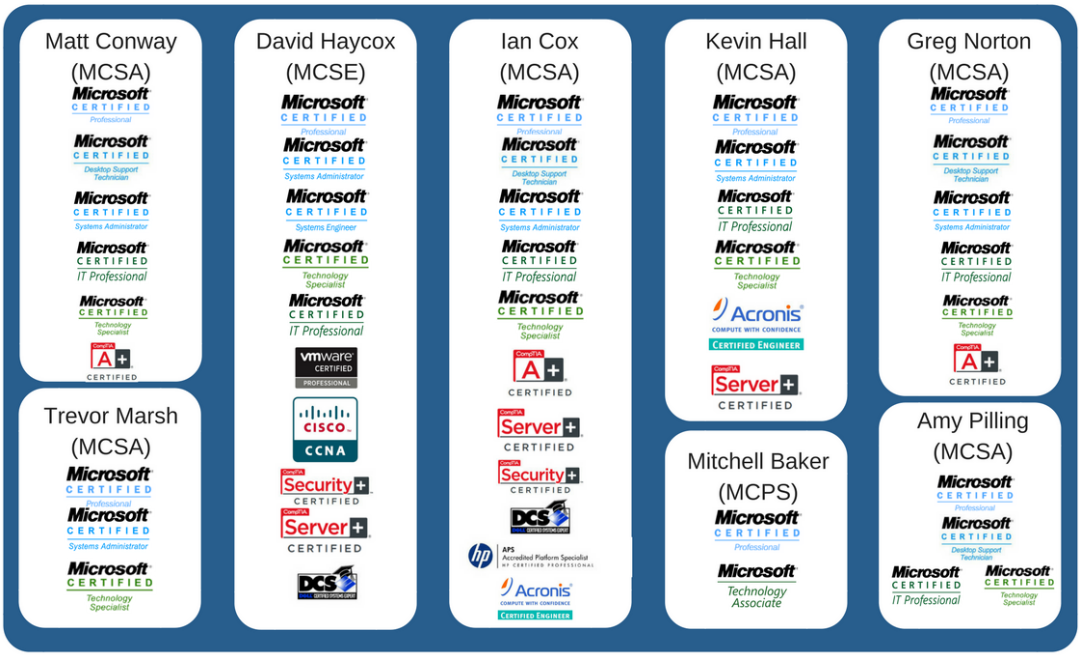
Our Accreditations and Partners

Midland Computers values business partnerships with industry leaders, and is proud to have achieved official reseller status with companies such as Microsoft, HP, F-Secure, Intel, Sage and Dell. Our partnerships with some of these companies require us to buy products exclusively through official UK distribution channels. Others do not, but our purchasing policy is to do this whenever possible anyway, as this way we ensure that you receive legal products with full warranty and manufacturer support, should you need it. We are partnered with a broad range of suppliers, giving us the ability to supplement our own comprehensive stock holding with an enormous variety of products from most well-known IT equipment manufacturers, usually available for delivery within a few days.

The Midland Computers engineers are highly qualified and certified to the highest standards. Many of the companies that Midland Computers provides services to are so impressed with our dedication and support that they move all of their IT provision from their previous suppliers to us. They then enjoy the many advantages of us being their sole IT supplier.

In summary, Midland Computers can troubleshoot any problem you encounter, has full understanding of your IT infrastructure to support you quickly and efficiently, is always looking at how to improve product offerings, and gladly takes on board new advancements or suggestions and rolls them into the company's portfolio.

MIDLANDCOMPUTERS



MIDLANDCOMPUTERS