Avecto Whitepaper

Compliance series

Guide to meeting requirements of the UK Government Cyber Essentials Scheme

Contents

Introduction to the scheme

Businesses are at greater risk than ever before from cyber attacks, but a lack of resources, expertise and awareness has left SMEs vulnerable. The increasing prevalence of security breaches in the headlines provides an indication of the changing threat landscape, and small businesses have largely considered themselves to be at less risk than large corporations or government, either because they don't believe they have any information of value, or that they are not high-profile enough to warrant interest from hackers.

Recognising the potential losses that a security breach can involve for SMEs, the UK government has launched a cut-down version of its 10 Steps to Cyber Security, providing five achievable goals that it believes both small and large businesses should implement to secure their IT systems.

The Assurance Framework provides two certifications, Cyber Essentials and Cyber Essentials Plus, that SMEs can obtain with minimum effort and at low cost. Cyber Essentials Plus offers greater assurance through external testing of the implemented controls, and both certifications involve completing a questionnaire that's approved by a company executive, and then verified by an independent certification body.

The five goals set out in the Cyber Essentials Scheme are as follows:

01 **Boundary firewalls and internet gateways** - these are devices designed to prevent unauthorized access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
02 **Secure configuration** – ensuring that systems are configured in the most secure way for the needs of the organization.
03 **Access control** – ensuring only those who should have access to systems to have access and at the appropriate level.
04 **Malware protection** – ensuring that virus and malware protection is installed and is up to date.
05 **Patch management** – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor have been applied.

Once a Cyber Essentials or Cyber Essentials Plus certification has

been awarded, the company can display the relevant badge, giving business partners and clients confidence that adequate measures have been taken to minimize the risk of data loss and downtime caused by security breaches.

Boundary firewalls and internet gateways

Devices that protect the network edge, such as routers and firewalls, can fail to provide adequate protection if configured incorrectly. Factory settings, such as blank or default administrator account passwords, can provide an easy point-of-entry for hackers. Additionally, network rules that allow inbound traffic should always be approved and documented by a qualified member of IT staff, and rules that are no longer required removed as soon as possible.

Access to the administrative interface, whether via a web GUI or command-line console, should be restricted to approved devices on the internal network. If external access to the admin interface is required, additional precautions should be used, such as SSL encryption and SSH with certificates to authenticate hosts and clients.

Secure configuration

Windows 7 is relatively secure out-of-the-box, but as soon as default settings are changed or third-party software installed, the potential attack surface may increase significantly. Following some simple best practices can ensure that Windows-based devices stay secure. Guest user accounts should be disabled, unnecessary administrative users removed, and accounts should be properly secured with strong, unique passwords. The Autoplay - or Autorun feature in earlier versions of Windows - should be disabled using Group Policy to make sure software on removable media can't automatically install.

Third-party software has long been considered the biggest threat to Windows devices, with the likes of Adobe Flash, Acrobat Reader and Java being among the top offenders. Java should be removed wherever possible, and Adobe applications always kept up-to-date with the latest versions. Application control, such as that provided by Windows AppLocker and Avecto Defendpoint, can also be valuable in preventing users from installing third-party software that might introduce vulnerabilities.

Windows PCs are often used outside the protection of the corporate network, so an endpoint firewall is critical for ensuring devices remain secure when connected to the public internet or untrusted network. Windows Firewall, or a third-party firewall that's part of an endpoint security suite, should always be enabled on each device, following the same advice about approving the addition of firewall security rules that applies to network-edge security devices.

Access control

The hardest goal to achieve on the list, the Cyber Essentials Scheme requirements state that administrative accounts should not be used on devices with internet access, or for reading email, which rules out assigning administrative privileges to most employees. But this can pose a challenge when running legacy applications, and sometimes admin rights are required to perform system tasks.

The use of a third-party least privilege solution such as Defendpoint by Avecto enables organizations to remove administrative privileges without impacting the user experience. Applications and processes can be assigned the necessary rights, while leaving logged in users with standard user privileges. This ensures a much higher level of security, meeting the scheme requirements as well as ensuring that users remain productive.

Additionally, exception-handling capabilities such as Challenge/Response codes can be used to ensure users have flexible options to request the access they need, with auditing and reporting options that can be used to ensure policy rules are created to suit individual users or groups.

Furthermore, the scheme requires all users have unique named accounts, that administrative accounts be limited to a few authorized employees, and forbids the sharing of administrative logins. Finally, the creation of user accounts must be subject to approval, and documented with a business case.

Malware protection

Just as is the case with firewalls, misconfiguration of antivirus software can render it ineffective. The Cyber Essentials Scheme necessitates that all devices connected to the internet be protected by malware protection software, and that the software and signature files should be updated at least daily. Disks should be scanned regularly for potential threats, files automatically checked when downloaded and opened, and webpages scanned as they're loaded.

Patch management

The Cyber Essentials Scheme requires that the operating system and third-party software be licensed, supported, and updated automatically, or within thirty days of a patch being released; with the exception of security patches, which must be installed within fourteen days of release.

Windows Update can be used to automatically update the operating system and some Microsoft products, but third-party software often requires its own update mechanism, or in the case of Windows Universal Apps, the Windows Store takes responsibility for automatically keeping apps up-to-date.

As SMEs don't always have the resources to automate the deployment and maintenance of applications, it may be that some applications will either need to be updated by IT staff manually, or patches distributed to users so they can be installed.

About Avecto

Avecto is an innovator in endpoint security.

Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software has been implemented at many of the world's most recognizable brands, with over 8 million licenses deployed.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

The company has placed in the top four of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK's fastest growing software companies as well on the global stage.

Deloitte. Technology Fast50 UK 2014

UKtech awards 2015

winner Cyber Security Awards

intel Security Innovation Alliance

Microsoft Partner Gold Application Development