**Case Study: CAMBRIDGE KINETICS**

How we helped Cambridge Kinetics become Cyber Essentials Plus Certified.

**The Challenge**

Our client, Cambridge Kinetics are software development experts. Jason, the Managing Director, approached Cambridge Support in need of ensuring that his organisations security configuration was compliant. David, our Cyber Security Specialist considered their enquiry and thought that a Cyber Essentials Plus certification would be the best route.

Cyber Essentials Plus is a government led scheme consisting of approximately 80 questions that help organisations assess their practices with regards to cyber security. There is a Cyber Essentials certification and in addition a 'Plus' certification. The Plus certification is a more robust analysis of a company's security practices.

Working with Jason, we carried out work on the following topics:

- End user computers – are they on a compliant OS version and the latest update patch?
- Servers – are they on a compliant OS version and the latest update patch?
- Tablets - are they on a compliant OS version and the latest update patch?
- Network equipment - are they still supported and not EOL, and on the latest update patch?
- Firewall checks.
- Password policy checks.
- Software patching – is supported software installed and is it on the latest update patch.
- MFA config – is it on for their main Microsoft platform, is it on for their other cloud services.

**The Solution**

The Cyber Essentials Plus certification consists of an audit conducted by our audit partners, to be compliant and pass the cyber essentials plus requirements. The audit is scheduled for one day and involves the auditors checking a sample of computers to ensure they are compliant. This is checked against the answers provided by Cambridge Kinetics in the CE standard certification.

Cambridge Support performed an audit consisting of 7 tests, shown below:

- **Test Case 1: Remote vulnerability assessment.** We require the external IP address that is in scope to run a vulnerability scan.

- **Test Case 2: Check patching.** Both OS and software were checked. We also checked for unsupported software. The most common that are missed are things like .NET, Visual C++

- **Test Case 3: Check malware protection on EUDs (End-user Device).** This is checking that an anti-malware solution is enabled and it is up to date.

- **Test Case 4: Check effectiveness of EUD defences against malware delivered by email. The Auditors will send various emails through to each person during the test which include various attachments.** This involves sending fake malicious attachments and checking if they are blocked. This test requires the user to be logged in and have access to their chosen method of email retrieval such as outlook.

- **Test Case 5: Check EUD defences against malware delivered through a website. The Auditors ask to visit websites that contain test files.** In this test we download fake malicious files and check to see if they are blocked either by the browser or the anti-malware solution.

- **Test Case 6: Testing separation between standard account and admin account. We do this by trying to run a single application as an admin. If a prompt for credentials comes up, the test has been passed.**

- **Test Case 7: 2 factor authentication is tested on cloud consoles. This is done by opening the admin console over the preferred browser in a clear incognito session. If, when a user tries to sign in, a prompt for MFA comes up, the test has been passed.** For this test we ask the user to attempt to login to the cloud service being used via an incognito browser session to prevent cached information being used. The user only needs to get as far as the authenticator message and does not need to go any further. Alternatively, a screenshot can be provided of the config.

**The Outcome**

After performing all the tests in the audit, Cambridge Kinetics were thrilled to achieve their Cyber Essentials Plus Certification. They can now display the Cyber Essentials logo on their website to show their commitment to cyber security. They also recently became ISO 9001 certified, so they are certainly a company committed to improving their company.