SAPPHIRE™

IT Health Check – CHECK Testing

Service Definition

Classification: Public

Contents

Proprietary Notice

Overview

The IT Health Check Service, or CHECK, was developed by NCSC to enhance the availability and quality of the IT Health Check Services that are provided to government in line with HMG policy.

Sapphire is a long-standing member of this scheme, having maintained the 'Green Light' status since 2004. Sapphire is regularly measured against the high standards set by NCSC. As such, HMG and CNI customers can be assured that they will receive high quality testing service if the work is carried out under the Terms and Conditions of CHECK.

Sapphire has a team of Infrastructure CHECK Team Leaders and CHECK Team Members, as part of The Cyber Scheme.

Sapphire will conduct an on-site, remote or hybrid IT Health Check on specified hosts to provide an assessment of the effectiveness of deployed internal cybersecurity. It is designed to identify weaknesses in the security of computer systems connected to the environment, including workstations, servers and network equipment as well as applications and critical systems.

Functional and Non-Functional Detail

In today's connected world, organisations of all sizes in both the public and private sectors need to be aware of the limitations of their security technologies and procedures. If you have company and/or personal data either connected to the Internet or providing access to business-critical services, then you should regularly test the security of your infrastructure.

On completion of the engagement, Sapphire provides a management report and a full technical report. The deliverables include recommendations for technical countermeasures and other improvements as appropriate. The reports also make comparisons of previous test results to enable our customers to evaluate the effectiveness of ongoing patch management and configuration work.

Sapphire provides a range of testing services which offer peace of mind as well as being flexible to your business needs.

An IT health check is a mixture of vulnerability assessments, penetration testing, build and configuration reviews of a customer's network. The ITHC will prove to an accreditor or third party that their external and internal infrastructure is adequately protected and their data is secure and correctly segregated. An ITHC should include internal and external testing, including the following components:

External Testing

This should include systems that provide services on the Internet such as email servers, web servers and other systems such as the firewalls that are in place to prevent unauthorised access from the internet into your organisation. External testing should also include any systems you have in place to allow staff to connect into your organisation remotely. These remote access solutions normally involve Virtual Private Networks (VPNs) that should be tested as part of your external assurance. If your organisation is dependent on third-party suppliers and they have access to and from your systems from their own office locations this should also be considered as an external connection and tested.

Internal Testing

It should include vulnerability scanning of your internal network. At a minimum it should include:

- Desktop and server build and configuration
- Patching at operating system, application and firmware level
- Configuration of remote access solutions
- Build and Configuration of laptops and other mobile devices such as phones and tablets used for remote access
- Internal gateway configuration (including PSN gateway)
- Wireless network configuration

The PSN or any Code of Connection don't expect a full network test on all devices however it can be cycled provided it demonstrates compliance and importantly risk management – the organisation must show they aren't a risk to rest of the professional network. Due to this our clients can test on a 10% sample basis or base it on build types.

It is the organisations decision though what should be tested, and we simply need to know total numbers of systems, servers or hosts to define how long the test will take.

Collation of Findings and Report Generation

The deliverables will include recommendations for technical countermeasures and other improvements where appropriate. The reports will also make comparisons of previous test results to enable the G-Cloud Customer to evaluate the effectiveness of ongoing patch management and configuration work.

The reports include:

- Nature of vulnerability
- Assessment of risk
- Approaches that may be adopted to minimise or alleviate the vulnerability
- How secure is the Customer in terms of business
- Technical summary
- Management summary

Technical and management reports will be generated highlighting any vulnerabilities found and will include relevant technical countermeasures.

Findings are clearly marked in the report and are detailed in the technical report.

 Serious Risk

 High Risk Vulnerability

 Medium Risk Vulnerability

 Low Risk Vulnerability

Sample reports are available on request.

Sapphire's Certifications and Associations