AdviSec Ltd

IT SECURITY HEALTH CHECK

SECURITY CONSULTANCY

BACKGROUND

The requirement for undertaking an IT security health check is documented in standards such as the ISO 27001, PCI DSS, and various Codes of Connection[1]. Furthermore, and as important, it is now a 'main-stream' security requirement for the Government and Commercial sectors.

What isn't so well understood is the process for:

- Scoping 'health checks', e.g. network, web-application, WiFi, RAS dial-in
- Engaging a professional Provider
- Determining the number of days to complete a 'health check and the overall cost[2]
- Information exchange requirements
- Agreements to which Client and Providers need to comply
- Interpreting the results of a 'health check

ADVISEC LTD

AdviSec Ltd is an independent consultancy providing a range of services to secure Clients against the threats which arise from operating modern IT system and networks. Such services address the CONFIDENTIALITY, INTEGRITY and AVAILABILITY risks, in a cost effective manner, respecting constraints, supporting legal undertakings, and always ensuring that security solutions do not undermine the Clients' ability to deliver their business objectives.

In respect of IT security health checks, Advisec offers the following options for consultancy support:

- Option 1: Client managed service - Our consultant takes details of the requirement during a brief telephone call and thereafter contacts a provider who will liaise with the Client regarding their proposal for undertaking the project (FREE-service)
- Option 2: Advisec managed service – Our consultant manages the IT security health check from 'start to finish' (COST: £1600 for two-days consultancy)

[1] E.g. N3, GSi, PNN3, PSN
[2] Quotes vary from £450 - £1300 per day

CLIENT ENGAGEMENT

- Option 1: Client managed service - Our consultant takes details of the requirement during a brief telephone call and thereafter contacts a provider who will liaise with the Client regarding their proposal for undertaking the project.

- Option 2: Advisec managed service – Our consultant manages the IT security health check from 'start to finish'. Key points:
    - Client raises a P.O. for two days consultancy
    - Our consultant attends a short meeting with the Client to gain an understanding of their network and application infrastructure and to understand any concerns and constraints. At the same meeting the requirements for an IT security health check, and in particular the scope, shall be identified[3].
    - The requirements for the 'health check' shall be documented by our consultant in a Statement of Requirements (SoR).
    - Our consultant shall identify a suitable Provider, based on their capability, cost, security controls / vetting, accreditation, and availability, and will thereafter seek a proposal on behalf of the Client (using the SoR).
    - A tri-party telephone conference shall be held to discuss the proposal and identify a 'way forward'. Discussion shall also include the time slots for conducting the tests, facilities requirements, timescales for reporting 'vulnerabilities', the reporting method, points of contact, and the requirement to sign NDAs and other contractual documentation required by the CREST and/or CHECK accreditation schemes.
    - The Client shall raise a P.O. with the Provider for service delivery[4].
    - The Provider undertakes the 'health check', and returns details of 'high-risk' vulnerabilities immediately to the Client via secure means. Our consultant will confirm that this step has been undertaken.
    - Our consultant shall review the results of the 'health check' from the technical and quality perspectives and returns comments to the Provider via the Client.
    - Assistance in interpreting the results of the 'health check' for the Client – telephone call (or meeting at additional cost)
    - End of engagement

[3] Key considerations: (i) is the test internal or external, (ii) number of systems to be tested, (iii) type of systems to be tested, and (iv) 'sensitivity' of the 'test target' from a security perspective, including confidentiality, integrity and availability.
[4] Note a guidance sheet is available 'on request' which provides an indication of the numbers of days required to complete an IT security health check – useful for budgeting purpose.

BENEFITS TO CLIENT OF OPTION 2

Clients can be assured of high quality security advice provided by experienced security consultants, accredited under the CLAS and CISSP schemes.

Client can be assured of a properly scoped and professional 'IT security health check' which has been delivered at reasonable cost.

FURTHER DETAILS

Further details are available from Nigel Strutt. Contact details: 07780 526195 or 01869 388011 (telephone), nigel.strutt@advisec.co.uk (email) or nigel.strutt@advisec.cjsm.net (secure email)