SAPPHIRE™

Technical Security Review Service Definition

Classification: Public

Contents

Proprietary Notice

Overview

Considering the increasing importance of security, the number of organisations that allow for contingency in their Information Security budget is alarmingly low. Unexpected events can be a drain on both time and resource and can leave organisations with little finances to allocate to resolving the problem.

Sapphire can provide your company a technical network and general information security health check. The approach can be divided into the following areas:

1. **Perimeter Security**

Dealing with firewall, gateways and VPNs and technical entry points. Physical Access to your premises can also be reviewed.

2. **Internal Viewpoint**

Dealing with AD configuration (including structure and permissions etc), A/V, backups, and network access controls etc.

3. **External Viewpoint**

Dealing with mobile devices, their control, and the protection of the data on them (i.e. by the use of encryption etc).

4. **Policies**

Dealing with internal audit and user policies, including recommendations for required policies and review of current policy set.

Functional and Non-Functional Detail

The technical network security review will be carried out by a Sapphire Security Consultant and will include the following phases:

Perimeter Security Review

A full review of the existing perimeter firewall rule base will be carried out by a Sapphire Consultant. This review will ensure that the Cloud Customer's firewall policy is both secure and only allowing the required data to pass through and in the relevant direction.

The Sapphire Consultant will require a full high level network diagram if available, and a member of the firewall administrative team to help with the review. Also included within the perimeter review will be the following areas, all of which will be reviewed in their current state and

recommendations against Best Practice will be reported where applicable by the Sapphire Consultant.

- Checking Firewall set up and general configuration
- AV at both perimeter and on desktops
- Remote access policies
- VPN connectivity procedures

A physical security audit can also be included within this phase (at an additional cost), whereby a Sapphire Consultant will carry out a physical review of the Customer's premises. This can be to review the access controls in place for staff and/or contractors gaining access to the physical area where the network equipment is stored and also to ensure that these controls cannot be bypassed.

Internal Security Viewpoint Review

The following areas will be reviewed and compared to current security Best Practice, where applicable recommendations for improvement will be provided.

- Two Factor Authentication capabilities.
- Backup procedures
- Active Directory set up and associated access rights
- File structures and directories
- Data storage and access to central servers
- Web and Email filtering capabilities

External Security Viewpoint Review

The following areas will be reviewed and compared to current security Best Practice, where applicable recommendations for improvement will be provided.

- Portal access
- Mobile device usage
- Encryption
- Client access to company web site

Policy Review

Along with the technical reviews detailed above, Cloud Customer's current policy set can be reviewed, and recommendations can be made for amendment or addition where appropriate, examples of policy areas such as the following can be included within the review.

- Leaver and new starter policies
- Encryption of mobile devices
- Induction and training procedures
- Mobile device usage

Sapphire's Certifications and Associations