inspired **solutions**

Security Architecture Review

In order to protect critical business services and assets, organisations today must be confident that their network security architecture provides a robust, comprehensive defence against both external and internal threats. As an organisations network architecture evolves over time, the network security technologies must follow suit.

Network security is no longer viewed as a product based strategy, but instead as an indepth system that incorporates all elements of the network infrastructure.

Network security risk is best managed through a systematic, architectural approach that encompasses the entire network lifecycle. Without effective security controls in place, an organisation places data integrity, information confidentiality and the availability of business-critical applications at greater risk.

As part of the Security Architecture Review, APSU will provide a detailed evaluation of the organisations network security architecture, technology policy and management practices. The service identifies vulnerabilities and recommends improvements to the security architecture in line with industry security best practices. The result of the service is a roadmap to achieving a strengthened security infrastructure providing multilayer "defence-indepth" network protection.

The Cisco Lifecycle Services Approach

The APSU Security Architecture Review is part of the Optimise phase of the Cisco Lifecycle Services Approach. The aim of Lifecycle Services is to provide a consistent and proven methodology for the adoption of advanced network technologies.

The aim of the Optimise phase is to achieve operational excellence through ongoing improvements to the network and provides a foundation for network upgrades and enhancements, implemented in the other stages of the Network Lifecycle.

Benefits

Following a Security Architecture Review, an organisation can:

- Effectively protect the network infrastructure by identifying vulnerabilities and deviations from best practices and policy.
- Act upon recommendations to mitigate security risks that threaten the confidentiality, integrity, and availability of business processes and information.
- Help to achieve compliance requirements by identifying improved internal controls and procedures needed to better protect data from unauthorised access.
- Extend the network investment by expanding the security capabilities of the existing network infrastructure without wholesale upgrades.
- Lower operating costs through the consistent deployment of security technology policy and procedures.
- Improve productivity by strengthening the ability of IT staff to prevent, detect, and respond to future security threats.

Methodology

APSU Security consultants conduct a detailed review of the organisations network security goals and requirements as well as evaluating any associated security technology policies. They then provide an indepth analysis of the network security architecture, including the network topology, solution components, device features and configurations. Security technology policies for remote access, network segmentation, server protection, authentication, and firewall design can all be included in the scope of the review. Additionally, the service can evaluate the overall security architecture for scalability, performance, and manageability.

Following the above analysis, APSU provide a detailed analysis of network security architecture vulnerabilities and operational risks and evaluate how closely the current security architecture aligns with industry network security best practices.

APSU then provides prioritised recommendations to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations and network and security management tools. By following a systematic and detailed approach to assessing network security, the service helps organisations reduce threats to the confidentiality, integrity, and availability of business processes and applications and helps to improve risk management and satisfy compliance needs.

APSU can also offer network penetration testing services via a specialist partner as a regular security check and balance.

The end product to the customer is the detailed Network Security Architecture Report containing:

- Analysis and prioritisation of discovered vulnerabilities and identification of the critical findings.
- Recommended actions to improve the network security architecture in order to meet the organisations security goals.

Why APSU?

APSU is a Cisco Premier Partner with specialisations in Advanced Security, Wireless and Unified Communications. APSU Consultants have broad knowledge and experience in network security design, implementation and optimisation backed up by professional industry leading qualifications.

Technical Considerations

The following are the agreed technical constraints for an APSU Security Architecture Review:

- Physical and logical access to network infrastructure and security devices must be made available to APSU Consultants.
- To facilitate some of the automated auditing processes, SNMP community strings may need to be configured on devices.
- The customer must be able to provide an IT representative to collaborate with the APSU Consultant whilst onsite.

For further **information** contact our sales team on **01285 862 100** or email **info@apsu.com**