Network security planning

Technology, Information Technology

Network security planning Introduction Network security planning entails developing best practices and measures for protecting the network infrastructure. It entails establishing a security baseline for securing the main management planes in an organization. Furthermore, network security planning also aims at developing a strong foundation where more advanced security measures, techniques, and methods can be subsequently established. This is made possible through developing additional security design aspects that are inevitable for the enhancement of control, visibility, and general safety of the data panel.

The following areas have been identified as the key elements that require baseline security. This includes the following:

Network policy enforcement

Routing infrastructure

Network telemetry

Switching infrastructure

Infrastructure device access

Device survivability and resiliency

Over the year network infrastructure has always been suffering major threats and immeasurable attacks of the data panel. The following has been established as the major threats to the network infrastructure:

Intrusions

Routing protocol attacks

Spanning tree attacks

Botnets

Privilege escalations

Session hijacking

Denial of service i. e. DoS

Unauthorized access

Distributed Denial of service i. e. DDoS

Man in the middle attacks i. e. MITM

Network Infrastructure access best practices

In order to secure network infrastructure one must secure and manage the access of such infrastructure devices. Compromising with the infrastructure devise access, compromises the management and security of the entire network. This calls for the establishment of critical and suitable controls necessary to curb unauthorized invasion to the infrastructure devices. Network infrastructure devices aims at providing a wide range and different variety of access protocols. This includes asynchronous and console connections, In addition to protocols based on remote access such as HTTP, Telnet, rlogin and SSH. Therefore, every infrastructure device should be skillfully configured and reviewed to ensure that only allowed access procedures are enhanced and that they are thoroughly protected.

This has led to development of key measures aimed at protecting both management and interactive access to an infrastructure contrivance. This includes the following.

Authenticate access- make sure access is only permitted to authorized groups, users and services.

Account for all access activities- record whom and when accessed the infrastructure device and all the activities that occurred for auditing purposes.

Restrict the accessibility of the device- limit all the permitted methods of access, as well as the accessible ports and communicators.

Authorize actions- restrict the views and actions permitted by any group, user, or service.

Present legal notifications- exhibit legal information developed in conjunction with the company’s legal framework.

Enhance confidentiality of data- protect all the sensitive data stored from copying or viewing. Protect all the information in a communication channel from session hijacking, sniffing, and man in the middle attacks.

Cisco safe architecture, like any other network security system, is not immune to limitations. However, it has successfully developed threat mitigation and detection programs readily available on Cisco security agents, Cisco firewalls, Cisco network admissions control, and Cisco IPS and web safety appliances.

In addition, these devices alerts and generate information centrally gathered and correlated using the Cisco security monitoring, analysis and response system which recognize the source of threats, envisage the attack route, give the possible suggestions and sometimes optionally implements the response actions. The visibility of Cisco IPS reduces many instances of false positives thus allowing for dynamic quarantine impositions of unsecured hosts. In addition, Cisco security manager helps simplify the management of Cisco safe architecture, carryout threat mitigation, and troubleshooting.

References

Gregory, A. (2004). Cisco safe architecture. London: Oxford UP.

Kennedy, F. (2007, May 5). Newspaper classifieds contain Cisco safe architecture. Daily News, pp. F1, F9.

Mark, T. (2009). Cisco network systems. New York: Nerd Press.