Network Fort

Strengthening Network Security with NetworkFort

Feb 2021

Business Background

The enterprise was at constant risk of cyberattacks as well as its network was susceptible to internal and external security vulnerabilities. It required a one-stop solution to cater needs of both its cyber environment as well as internal and external network.

Challenge

- Discovering any external or internal security vulnerabilities
- Identifying if a combination of lower-risk vulnerabilities could be exploited in a particular sequence to create a high-risk weakness
- Identifying security vulnerabilities in application, file, and database servers
- Auditing and measuring the size of potential impacts of successful attacks both inside and
- from outside of the company
- Testing the viability of network defenders to detect and to respond to attacks
- Providing evidence to support increased network security
- Providing a solution to ensure 100% threat-free cyber environment.
- Ensuring autonomous response upon detection of crucial threat.

Solution

To ensure cyber protection across endpoints of the network of the enterprise, NetworkFort deployed its product, NetworkFort, in the network that helped the enterprise to maintain its competitive edge in the market. NetworkFort not only provided an enabled solution to detect intrusions but also provided a way to block them from entering the network.
Since, the enterprise security system lacked in identifying crucial threats in their earliest stages, so, NetworkFort assessed their network for security checks particularly for
Vulnerability assessment and penetration testing.

- Vulnerability Assessment

Our team assessed the security of the network from both the inside and outside of the network and reports were produced based on the weaknesses of parts of the network, as well as the network as a whole. This assessment highlighted the areas of risk and accordingly advised the changes that were needed to be made.

- Penetration Testing

Our team conducted penetration test that included comprehensive external, internal, and social testing. (The social testing in itself explores, as the expression implies, examination and discussion of staff methodologies and habits). The penetration test found vulnerabilities in the network, so, our team proposed to run a software that delivers a 'payload'; this helped to reveal weak links in the system. It is a known fact that if a hacker deploys a payload with harmful code, they can easily take control of segments and potentially expose the entire network. The penetration test that we performed prevented this from happening, by finding out such vulnerabilities first and then, with the client's permission, we actively exploited them.

Below are the initial phases of network security assessment:

- Assessing the Vulnerabilities of Networks, Applications, and Other IT Resources. Our team documented and analysed entire IT infrastructure to find the weaknesses and potential issues.

- Conducting Comprehensive Scanning Of Ports, Vectors, and Protocols.

  We conducted a comprehensive scan of all ports on network to identify the IT equivalent of open windows and unlocked doors. The most common malicious network scanned search for vulnerabilities in a standard range of 300 ports on a network where the most common vulnerabilities were found. However, there may be over 60,000 ports on the network that can be suspected.

- Probing Internal Network Weaknesses.

  We assessed the outside interaction with internal networks. Unfortunately, it cannot be assume that all threats will originate from outside the network. Internal people can pose a threat too.

- Reviewing Wireless Nets, Including Wi-Fi, Bluetooth, RFID, Rogue Devices.

  Wireless nets, rogue devices, and removable media all were found to have vulnerabilities.

Security Flaw Detected

There were many issues related to the security of network infrastructure. Some issues were more technical and required the use of various tools to assess them properly. Some issues

were easy to see from outside the network, and others were easier to detect from inside the network.

Major security flaws detected were:

- Configuration of devices such as firewall or IPS was not correct.
- There were vulnerabilities in network hosts, which made the network susceptible to exploitation.
- Problem in network design, such as Internet connections, remote access capabilities, layered defence s and placement of hosts on the network
- Interaction of installed security devices such as firewalls, IDSs, antivirus and so on was not properly done. Commonly attacked ports were unprotected.
- Network host configuration was not rightly done
- Network monitoring was poor and there were no means to predict future attacks.

Deployment of NetworkFort in the Network

With integration of NetworkFort in the network, the enterprise was able to identify critical threats as well as the existing vulnerabilities. NetworkFort provided a way to keep enterprise a step ahead of attackers via its predictive behavioral analytic's feature. The machine learning techniques were applied to identify traditional trends or patterns in data. It helped the enterprise to detect even a minor deviation from present data pattern. In this way, NetworkFort helped them to identify any intruder in their network.

Company Info

Website https://www.networkfort.com

Phone number 1-410-603-4767

E-mail address: info@networkfort.com