Module 11 - Network Security | Goals and Threats

Contents

1. Objectives

- Explain the importance of network Security
- Outline major threats to network security
- Assess the major security goals of business organizations today
- Describe how to conduct a risk assessment
- List the risk assessment frameworks commonly used today
- Describe 5 common steps associated with risk assessment
- Identify major threats to ensuring business continuity and describe ways to effectibely counter these threats

---

2. Importance of Network Security

The rise of the Internet has redefined the nature of information security. More and more people are starting using the internet.

The number of security incidents grows by about 30% per year. In 2016, about 50 million passwords were stolen, and 51% of adults from a survey of 1,500 people claimed they experienced some cyber security incident.

Laws have been made to try to improve the crime rate over the internet, but they have been slow to catch up. There is still much left to learn about the true depth of the internet

3. Organizations Focused on Cyber Crime

Many organizations, private and public, focus on helping individuals, organiztions, and governments to protect themselves from cyber crime.

- CERT (Computer Emergency Response Team) at Carnegie Mellon University
- APWG (Anti-Phishing Working Group)
- McAfee
- Symantec

4. Rise of Cybercrime

Cyber crime has now become a "profession" that is done for profit. Another type of cyber crime is hacktavism, which is hacking to bring attention to a larger political or social goal.

Not only that, but cyber crime has gone up because of the rise in mobile devices as well. Since mobile devices, such as cellphones and iPads, are so widely available

5. The Need for Network Security

Network security has become increasingly important because of a few things. There is more potentail vulnerability for organization's assets. There have also been more well-publicized security break-ins.

A company can experience huge losses when security failures occur. Companies are obligated to protect customer privacy and prevent the risk of identity theft.

Lastly there is a lot of value in the data stored on most organizations' networks and a lot of value provided by the application systems in use (far exceeding the cost of the networks themselves)

6. Security Threats

- Threats to Business Continuity
  - Disruption - Ex: switch failure, cut cable
  - Destruction of Data - Ex: virus destroys failures
  - disasters - Ex: fire burns down data center
- Threat of Unauthorized Access/Intrusion
  - External attackers gaining Access
  - Most unauthorized access incidents involve employees
    - principle of least privilage (only have as much access as you need)