Topic: Network Security Management

Enterprise Network Administration & Management

By Abdallah Ibrahim Nyero

Department of Computer Science & Engineering

Makerere University Business School

Topic: Network Security

Learning Objectives: To

1. Show need for network security
2. Identify Key Tenets of security
3. Distinguish between Vulnerabilities, Threats and Attacks
4. Show different vulnerabilities and methods of Attacks
5. Develop measures to secure the network
6. Develop Network security plan

Need for Network Security

- Network security is a core area that network administrators need to pay attention to
- Information Assets need to protected from both internal and external attacks
- Securing the network protects it from Information theft, identity theft,data loss and manipulation, disruption of service etc
- Thus confidentiality, Integrity, Availability and non repudiation have to be supported

Key Tenets of Network Security

- Confidentiality: Ensures there is privacy
- Integrity: Ensures message is not altered in any way
- Availability: Ensures the network resources and services are available whenever users need them:
- Non repudiation: Ensures non deniability of occurance of a transaction
- Authentication: Tests whether you are the one you purport to be

Vulnerabilities, Threats & Attacks

- Vulnerabilities: Weak points in our system that can be exploited
- Threats: possible danger that may exploit a vulnerability to breach security and cause harm
- Attack: Actual exploitation of the threats

Vulnerabilities

- ✓ Weak or Blank System Admin Password
- ✓ Sensitive Information Transmitted Unencrypted
- ✓ Weak or Blank Database Password
- ✓ BYOD (Bring your own device) policy
- ✓ Open ports, backdoors and unhardened devices
- ✓ The Trojan Human Wireless WEP in Use
- ✓ Misconfigured Firewall Allows Internal Access
- ✓ Wireless WEP in Use
- ✓ Misconfigured Firewall Allows Internal Access
- ✓ Etc

Common Methods of Attacks

- ✓ Use of social engineering
- ✓ Viruses, worms and Trojan horses
- ✓ Tracking cookies
- ✓ Phishing
- ✓ Spyware, adware (pop-ups and pop-unders)
- ✓ Denial of service (DoS) and DDoS attacks
- ✓ Brute force: guessing of passwords Physical threats and misuse
- ✓ Botnets
- ✓ SQL injection hacks of web servers and databases

Measures to Secure the Network

- Protecting/securing the network is a very important aspect
- This requires carefull planning
- It is not a one-off event
- The core of protecting the network is designing a network security plan
- Stakeholders in network security have to be guided by the network or IT security plan

Network Security Plan (NSP)

- Network or IT security plan is designed to protect information and other critical resources from all kinds of threats
- This ensures that risks are minimised, business continuity is upheld while ensuring that the goals of the organisation are achieved
- This plan is comprehensive to cover all aspects of security
- It ensures that all tenets of security are considered
- Varies from organisation to another due to diversity in business processes and what needs to be protected
- It should conform to IT best practices and laws of the land

Network Security Plan (NSP) Components

NSP may contain the following sections

- Risk analysis and assessments
- Roles/duties of different stakeholders
- Information Assets Classification
- Information handling
- Identity and Access Management
- Logical security Measures
- Physical security Measures
- Business Continuity
- Information Security incidence response
- Maintenance and Testing

NSP- 1.Risk analysis and assessments

- ✓ Determine information resources that need protection and all possible sources of risks that can affect it
- ✓ Look at the business processes and determine how they can affect network security
- ✓ Show what happen when these risks are not mitigated or minimised

NSP- 2. Roles/duties of different stakeholders

- ✓ All stakeholders who will be affected by the plan should be identified and roles/duties related to network and resources should be clearly specified
- ✓Responsible Departments/sections should also be identified
- ✓ This will help eliminate blame game as a result of negligence or non-compliance

NSP: 3. Information Assets Classification

- Anything that has value to the agency that can be communicated or documentary material, regardless of its physical form or characteristics.
- Includes, but is not limited to, paper, electronic, digital, images, and voice mail.
- Information technology hardware and software are not information assets for classification purposes.

Why Classify Information Assets ???

- Not all information has the same value or importance to an agency, therefore information requires different levels of protection.
- Information asset classification is critical to ensure assets have a level of protection corresponding to the sensitivity and value of the information asset.
- An organisation can classify its assets as Confidential, Internal/private and Public
- Others classify as Published, Limited, Restricted and Critical

Confidential, Internal/private and Public

- ✓Confidential: Deemed extremely sensitive where unauthorised disclosure or compromise can lead to severe damage to the organisation
- ✓Internal/private: Information which is intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of organization employees, clients, partners or individuals who otherwise qualify for an exemption.
- ✓Public: Information that is accessible to the general public. It is not protected from disclosure

NSP. 4 Information handling

- This section stipulates how information should be handled depending on the level of classification.
- Records with highly sensitive information should be maintained where they must exist
- These areas should be clearly specified in the NSP such that responsible individuals will know where to take them

NSP. 5. Identity and Access Management

- This section ensures that users of network resources are accurately identified and given the right previleges
- No user should access what they are not previleged to
- These can be enforced through two key concepts i.e. Authorisation and Authorisation
- All rules regarding who should get into the system and access what resources and with what tools should be documented.
- System time-outs have to be implemented
- Authorisation and authentication provides for non-repudiation through audit trails

NSP. 6. Logical security Measures

- This section shows the different logical security measures that help protect network resources. These measures include but not limited to

- ✓ Use of firewalls, Intrusion Detection Systems and Intrusion Prevention Systems
- ✓ Port lockdown and minimising running services
- ✓ Use of Anti-virus software
- ✓ Software updates and patches
- ✓ Inventory of Authorised and Unauthorised devices and softwares
- ✓ Enable and Monitor Logging and Auditing on a 24x7 basis
- ✓ Encryption of sensitive information

Logical security Measures

- Under each measure, the NSP should show what it is and strategies to achieve it. For example incase of Software updates and patches: the policy can be as follows:
- Software updates and patches: This policy ensures that the company's softwares have the recent available signatures or versions. The systems administrator will check network applications for updates on a weekly basis. In case new version of the sofware is available, it will be downloaded and installed. However, only stable versions should be downloaded and installed in production network. Beta versions can be downloaded and istalled for testing purposes in a controlled environment. Users are also encouraged to install latest software patches and updates. In case the network senses that a certain user is using old applications which puts the whole network at risk, they will be notified immediately. Failure to adhere to the notifcations, the user will automatically be blocked from further accessing the network resources

NSP. 7. Physical security Measures

- These are physical access controls employed to protect network resources. These can include

- ✓ Video Surveillance Cameras (CCTVs)
- ✓ Locks
- ✓ Card Keys
- ✓ Biometric Authentications
- ✓ Guards

Physical security Measures

- NSP should as well address strategies to achieve each physical measure as well as best practices and principles. Taking an example of card keys, an organisation can have:
- Card Keys: These cards allow users to authenticate themselves to a room or facility. The card key contains details of the employee. All senstive areas of the building like server room and Accounts will be accessed by only those with card keys. In case of a new employee, a card key will be provided within 24 hours after receiving and accepting the appointment letter. Employees should securely keep their card keys. These card keys should not be shared. In case a card key is lost, the employee should immediately report the issue to systems admin office. The admin office should take necessary steps to handle the issue immediately to avoid cases of deniability of service access. When an employee leaves the company, the card key or all details relating to that account shall be deactivated. This is intended to stop a former employee from accessing the system

NSP. 8. Business Continuity

- NSP should ensure that the business can still have access to network resources even in cases of a disaster. Key aspects of this is carrying out impact analysis and developing backup/disaster recovery plans.
- Impact analysis will show the extent to which disruptive event will have on business operations. This will require looking at different scenarios e.g. Is it a virus attack, system hack, power outtages, fire, tornado, floods etc? This can be in terms of how long the system will be off in case of a problem
- Backup/ Disaster recovery plan shows strategies that will be put in place to ensure resumption of business in case of any occurance or outtages.
- Considerations for different site alternatives should be made e.g. cold, warm,mobile or hot sites
- For Backup Strategy, consider: Full, Incremental or Differential backups

NSP. 9. Information Security incidence response

- On a corporate network, a number of things/events can occur which can have an impact or potential to affect the confidentiality, Integrity and Availability of network resources
- During risk assessment and analysis, such incidents should be identified
- At this stage, NSP should address possible responses to these incidences.
- As a general rule, once an incidence happens, it should be reported immediately to the responsible officer
- Information about the incidence has to be gathered. This may include the time, nature of the problem, contact information, place/device which has been affected and any other information that is deemed relevant

NSP. 10. Maintenance and Testing

- We looked at software updates, upgrades and patches. But this is just a small part of network maintenance
- When a network is deployed, it has to be tested and maintained at certain predetermined times. Within NSP, frequency of maintenance and testing has to be specified, time in terms of days, week or months when maintenace will take place.

Time can also be in terms of Peak or Off-peak hours ie. day vs night. This will vary from business to business. Most maintenance and testing are done at off-peak hours.

- Users should be notified days before the d day. This is why we see banks and telecom companies sending users SMS about when they will perform upgrades of their systems. Such policy would have been covered in the NSP.
- Contracts regarding maintenance have to be in place. You may find that the testing and maintenance service has been out-sourced

References

- Michigan Technological University Information Security Plan

THANK YOU