NETWORK SECURITY

Network security is the ability to put in place policies and tools designed to protect valuable assets of an organization from potential threats that are as a result of interconnectivity of computing devices. This may originate from hackers and crackers from interconnected devices, unauthorized access to confidential information through unauthorized means such as spoofing and to a larger extend genuine organization users (employees). In network administration and management, this refers to the loss of data or compromised system integrity or denial of access to the computing system services.

To enforce security, certain levels of convenience and stringent measures of discipline have to be enforced. This creates routine management tasks that are easily noticeable whenever there are breaches. This in turn enables the administrator to put in place mechanisms to safeguard the system with the help of the very users that can be great sources of threats.

There are various ways in which a system can be compromised:

- Physical threats: physical intrusion like in the server room, weather, natural disaster, bombs, power failures, etc.

- Human threats: Hacking, cracking, stealing, trickery, bribery, spying, sabotage, accidents.
- Software threats: bugs, viruses, Trojan horses, logic bombs, denial of service.

To mitigate against the three threats, three tasks have to be put in place as both preventive and damage control measures.

- Identify what to protect.
- Evaluate sources of threats and how to enforce trust.
- Establish elaborate cost-effective counter-measures to threats and attacks.

Network Systems Attackers

A network systems attacker is an individual who obtains, or tries to obtain, unauthorized access to networked system. These attackers can be insiders or outsiders. Insiders are legitimate organizational users who attempts to gain unauthorized access to certain network resources they are not entitled to access. Outsiders are individuals who do not have authorized access to network resources but tries to gain access through system vulnerabilities.

Categories of network systems attackers

Though there are several types of network system attackers, the two main types of network system attackers are:-

i) Hackers

ii) Crackers

Hackers

These are individuals with excellent technological skills and knowhow who exploits holes and vulnerabilities in designed network systems. They are helpful and useful personnel since they put the organizational management on it toes in ensuring that all security lapses and vulnerabilities are well taken care of.

Crackers

These are individual who unethically utilize their technological skills and knowhow to defeat network system protection in an attempt to unlawfully gain access to organizational resources.

Causes of insecurity of networked systems

Four types of fundamental weaknesses causes insecurity to networked systems, though the fourth in the context of what a network administrator is supposed to

do shift that responsibility to the system, and not necessarily the network administrator. They are:-

i) Policy Weaknesses
ii) Configuration Weaknesses
iii) Technology Weaknesses
iv) Human Weaknesses

Policy Weaknesses

This is an attribute that reflects the short comings of organizational management. It exploits the capability and capacity of the management to enact and/or enforce policies regarding aiding or safeguarding organizational networked systems. Sample the following:-

i) Written security policy – lack of documentation and adaptation work plan simply infers that security efforts are entrusted on knee-jack philosophy and guesswork capabilities of the personnel in charge at the respective times.

ii) Disaster recovery plan. Lack of a detailed data recovery plan is a recipe for disaster when danger such as a fire, flood, or earthquake strikes. In such a scenario, everything is delegated to the mercies of the personnel in charge in terms of judgment, experience and knowledge to handle the situation. Here, even the best trained and most experienced personnel can make makes the most stupid mistakes.

iii) Policy for software and hardware maintenance. Lack of policy on maintenance of digital devices such as additions, changes and/or upgrades introduces unexpected security vulnerabilities. For example,

any unguided addition of a wireless access point to a network can open up the network to security threats and render the organizational resources vulnerable. In a similar way, any unauthorized upgrade of software can introduce unauthorized third party software capabilities that can leak organizational data to third party entities. Such kinds of upgrades must always be guided through a policy.

iv) Security surveillance. A lack of this kind of a policy from management is tantamount to failure by the management to execute its responsibilities. Logs, audit trails and track of running processes must be constantly surveyed to thwart any chances of vulnerability. The worst case scenario is for the management not recognizing and/or realizing that a breach had occurred and/or was continuing.

v) Hiring policies. High staff turnover and lack of training opportunities for staff can all impact on network security by introducing untested, inexperienced and/or less skilled personnel into positions of authority and responsibility.

vi) Organizational policies. Internal organizational policies must be explicit to all staff and be enforced at all times by management because any slackness creates and environment where opportunists

might easily strike. For example, office politics such as power struggles might lead to undetected security breaches and render the network vulnerable.

Configuration weakness

There is need for management to enact and enforce configuration policies because, in most cases, digital devices and software accept installation with default settings. This default setting features always creates vulnerabilities and can be disastrous to organizational resources.

Common configuration issues that management needs to forcefully grapple with include but not limited to the following:

i) Implement effective access control measures to limit, track and monitor traffic flow within the network.
ii) Implement measures to discourage use of default and/or missing passwords, ensure password expires and never to reuse old passwords.
iii) Shut down all unused running services and processes as well as deactivating all unused active ports.

iv) Encrypting traffic across the network especially User IDs and passwords.

v) Disable all remote access features and only enable when extremely required and with necessary security measure in place.

It is worthy if the management can monitor digital device and software vendor announcements and advisories, and government and industry news agency information and warnings, to identify emerging vulnerabilities and mitigation measures.

Technology Weakness

Every technology in existence has uncertainties and inherent vulnerabilities that can be exploited by hackers and/or crackers. Therefore it is imperative that the management is ever updated through trainings, consultancy and other channels of communication to identify emerging threats, their impact on the network and the respective mitigation measures. By virtue that no one has brought out the vulnerabilities in your area of concern does not allow the administrator to comfortably sit on his/her laurels and assume they are home and dry security wise. The following are some of the weaknesses associated with technology:-

i) Protocols that create, facilitate and/or sustain connected device intercommunication were not originally designed for security hence can be sources of vulnerabilities. Therefore management must be aware and put in place measures to support those protocols with some of the security best practices and services, and link them with other products that work cohesively together to reduce the risks inherent in the environment.

ii) Network device Operating Systems have own inherent weaknesses and vulnerabilities whether open standard or proprietary, that need attention through patches, upgrades, and best practices.

iii) Network devices have vulnerabilities, often referred to as “holes,” that are exploitable by hackers and crackers. Patches, upgrades, and best practices can easily mitigate known vulnerabilities and threats associated with these holes.

Human Weakness

These are faults committed by genuine system users who are either unaware, are ignorant and/or blatantly stubborn that some activities they engage in expose the network to danger. These weaknesses can easily be mitigated by enacting and enforcing policies at system administration level given that at network

administration level, the administrator mainly deals with devices and their respective interconnectivity.