

Logical Security

The nature of computer crime has changed over the years as the technology has changed and the opportunities for crime have changed. Although external threats, such as Trojans, Worms, Spam, and DDOS attacks are still common (30%), the field is increasingly dominated by professionals who steal information for sale and disgruntled employees who damage systems or steal information for revenge or profit.

Surveys have shown that most damage is done by insiders (70%). Many insiders have the access and knowledge to compromise or shut down entire systems and networks. However these percentages are not accurate as most companies do not report computer crimes to avoid damage to the company reputation.

Results of a recent survey done by European countries and the USA shows the following as the most common threats faced by companies:

1. Malware
2. Phishing
3. Pharming
4. SPAM
5. Distributed Denial of Service (DDOS)
6. Unauthorized access by outsiders
7. Vandalism/sabotage
8. Extortion
9. Fraudulent Transactions
10. Physical loss
11. Unauthorized access by insiders
12. Insiders misuse

Unfortunately statistics on network attacks for South Africa are not available yet, to date South Africa does not have an established national Computer Security Incident Response Team (CSIRT). However the process of educating and forming a CSIRT team started in March 2010.

“The main object of the company as an association not for gain, is to carry on, establish, promote, manage and control, various interest and user groups, for the promotion of education, and awareness of information security.” (Source: ISG AFRICA MEMORANDUM OF ASSOCIATION)

IP Logical/Network Security

In the field of networking, the specialist area of **network security** consists of the provisions made in an underlying computer network infrastructure policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access.

The terms Network Security and Information Security are often used interchangeably. Network Security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information Security, however, explicitly focuses on protecting data resources from malware attack by use of Data Loss Prevention (DLP) techniques.

Network security starts from authenticating the user, commonly with a username and a password. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Anti-virus software or an Intrusion Prevention System (IPS) helps detect and inhibit the action of malware such as computer Worms, Trojans and SPAM.

Network Access Control aims to do exactly what the name implies, control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

A **firewall** is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit,

deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both.

Antivirus (or anti-virus) software is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.

Unified Threat Management (UTM) is a comprehensive solution that has recently emerged in the network security industry, and has gained widespread currency as a primary network gateway defence solution for organizations. In theory, it is the evolution of the traditional firewall into an all-inclusive security product that has the ability to perform multiple security functions in one single appliance: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing and on-appliance reporting.

Wireless Security

Wireless networks are very common, both for organizations and individuals. The ability to enter a network while mobile has great benefits, however the risks to users of wireless technology have increased as the service has become more popular.

Types of unauthorized access:

- Accidental association
- Malicious association
- Identity theft (MAC spoofing)
- Man-in-the-middle attacks
- Denial of service
- Network injection

In a wireless network, an access point, AP, sends and receives signals to any number of other, local wireless devices .It is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.

Fat AP

An AP with sufficient program logic and processing power to allow it to enforce policies relating to access and usage, rather than working under the supervision of a centralized controller.

Thin AP

An AP intended to act under the supervision of a centralized controller that configures, manages, and secures the environment .The centralized controller provides a single point of administration for all APs.

Wireless security standards such as, WEP (Wired Equivalent Privacy),TKIP (Temporal Key Integrity Protocol) with MIC (Message Integrity Check), WPA (Wi-Fi Protected Access), 802.1x EAP (Extensible Authentication Protocol) and WPA2 (Wi-Fi Protected Access 2) are all possible whether you are using fat or thin access points, however, the real differences exist in security implementation and management

Fat access points require that security settings be configured on each individual access point and because there is security information stored on the flash memory of the access point there is the potential for a network breach in the event that an access point is stolen.

In contrast, thin access points do not contain or process any security configuration information. The wire-less controller processes and manages security for each access point as opposed to replacing access points

In addition to basic security standards, some vendors are offering integrated value-added security software designed specifically for WLAN security. The integration of additional features such as "stateful packet inspection" firewall, VPN termination, and IDS (intrusion detection system) into one platform makes WLAN deployment as secure as a wired network.