Security advice

A few simple things are essential for the security of any network connected to today?s hostile Internet.

Up-to-date patches

All software, operating systems and applications, needs regular updates to remove vulnerabilities as they are discovered. These patches should be installed as promptly as possible after they have been properly tested. Particular care needs to be paid to applications for which automatic updating is not practicable; for example, most Web-based applications. You should contact your software vendor for details of when updates are released.

Up-to-date anti-virus

Everyone should use anti-virus software, both on their servers and desktops, to protect themselves from viruses, trojan horses, spy ware and other malicious software. It is essential to keep the product up to date; otherwise it quickly becomes useless and before long provides only an illusion of protection. It is always useful to be familiar with a number of alternative anti-virus software packages and tools in case your primary software fails. You may wish to consider under what circumstances it is no longer useful to attempt to remove malicious software and instead reinstall the system.

Firewall

A firewall partitions one network from another, enforcing a policy on precisely what traffic is allowed to pass between the two networks. More sophisticated (and expensive) firewalls are able to enforce more sophisticated policies and handle higher levels of traffic. Although all do some good, there are many options to be researched when choosing a firewall.

Backup

Not only does a backup of your data protect you from hardware failure but it also protects you from human error and data corruption. Backups should be made often and regularly and tests scheduled so that data can easily be recovered when a real problem occurs.

Network Segmentation

A prudent approach to developing and deploying a network should focus on three steps: learn, segment, and protect. Securing network hosts requires understanding what devices can be trusted and managed, and what devices cannot be trusted, and therefore not allowed to access certain segments of the network.

Network segmentation is the act or practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.

Logging

Log records of activity on your systems are essential tools for the investigation of an incident after it has occurred. You should configure appropriate, manageable levels of logging and ensure that you have procedures for storing and accessing them while they are current and destroying them after that. Janet CSIRT regularly encounter organizations who have difficulty tracing the origins of network traffic because they do not log network address translations or cannot read the logs, effectively allowing anonymous use (and misuse) of their networks.

Ideally logging would be centralised, held for a collection period of at least 90 days and include events such as logon events and security events.

Regular examination of logs (which can be partly automated) will often draw attention to issues before they become a serious incident.

There is a separate page of advice on log files:

- Keeping logs of network activity [1].

Links
[1] http://community.ja.net/library/janet-services-documentation/logging-network-activity