System configuration and maintenance

General-purpose computer systems as supplied are not designed to be connected to hostile networks. The Internet outside the organisation should certainly be regarded as hostile and for some purposes parts of the internal organisation should also be viewed in this light. This means that many of the computers in the organisation need additional configuration and maintenance to reduce the likelihood of them falling victim to an attack across the network.

Most computers are configured to provide far more services than are required to perform their intended function. Workstations do not need to run web, database or nameserver programs; servers do not need to run web browsers or word processors. The first step in securing any computer is therefore to remove, or at least disable, any software or options that are not needed for its intended purpose. The software that is needed should then itself be configured to remove any unnecessary options that present an unacceptable risk. New threats are being discovered continually, so systems must also be maintained to take account of them. This should be a continuous process throughout the lifetime of the computer and may include installing new software versions or patches, enabling security options and disabling insecure functions. The JANET Factsheet Securing Networked Computers [1] provides more details.

Additional programs and services can be installed to detect and prevent attacks. One of the most effective of these is anti-virus software, which can be installed centrally, on end-user systems, or both. See the JANET Factsheet Computer Viruses - Don't Click Here [2].

Secure configuration and maintenance must be included in the organisation's security policy and procedures. Without guidance from these documents, this vital work will not happen. The first priority should be those computers that are intended to provide a service to an external network, for example web, mail and nameservers and proxies. These machines will appear in public directories so are likely to be the most obvious targets for attack. They will often also be less protected by firewalls than purely internal systems. Other computers that may connect directly to the untrusted Internet, for example laptops that connect from time to time to other networks, and computers that participate in Grids or other peer-to-peer systems, should also be a high priority since these cannot always be protected by an organisation’s gateway firewall. It may be appropriate to run host-based software firewalls on these machines. Internal systems that are particularly important, for example file servers or administrative machines, should also be secured as a high priority, and appropriate protective software installed on other computers that handle messages from the outside world. Nor should the threat from within the organisation be forgotten: students and staff are not always well-intentioned towards the organisation. In time the aim should be to have all computers on the network significantly better protected than when they came out of their packing cases.

Links
[1] http://community.ja.net/library/janet-services-documentation/securing-networked-computers

[2] http://community.ja.net/library/janet-services-documentation/computer-viruses-dont-click-here