Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Security issues raised by connection to Janet

1.1 Connecting to the Internet

The rapid success of the Internet is largely due to the fact that its aims are kept very simple. The network is designed just to move packets of information from one computer to another, leaving it up to those computers to decide how to handle the packets and what their content may mean. This separation of roles means that the same basic network protocols used thirty years ago to carry text commands to mainframe computers from remote terminals can still be used today (though at much greater speed!) to video-conference between two smartphones. In principle an Internet communication can be established between any pair of more than a billion directly connected computers with no need to change or obtain permission from the underlying network.

While this openness has been a great success in facilitating the development and widespread adoption of applications that the network's designers could not have imagined, it also means that the network can do relatively little to either define or prevent unwanted uses of the computers it connects. As far as the network is concerned, every packet is alike: it is up to the receiving computer to handle appropriately whatever information it may contain. Since there is essentially no restriction on what a sending computer can put in a packet, any computer connected to the Internet needs to be able to cope with malicious packets and content as well as benevolent. Standards (known as RFCs) exist for how to use the network to carry an e-mail, a webpage or a video-conference, but computers can, and do, choose to ignore them for both good and bad reasons. The network does not, and cannot, check.

In particular the network cannot check whether the information it carries is accurate. A series of packets may claim to contain a plain text message but actually contain an executable program; an e-mail may claim to come from one address when in fact it comes from a different continent; even the source address of a packet can be forged. Computers, their programs and their users need to be aware of the possibility of such misrepresentations and take appropriate steps to defend against them.

1.2 Consequences of Insecurity

A user who responds to a deceptive e-mail or a computer that runs a malicious program can both give an intruder access to information or systems that was not intended. Such events are considered security breaches. The most common immediate results of a breach are either that an intruder obtains a copy of a legitimate user's username and password - thus enabling the intruder to do anything that user could on any system to which that username and password give access - or else the intruder gains the ability to install and run programs of their choice on the compromised computer.

The impact of such a breach can be experienced in three different ways:

- a loss of confidentiality - where information is disclosed to someone not authorised to see it;
- a loss of integrity - where information or computers cannot be relied upon to be or behave correctly;
- a loss of availability - where information, computers or services are not accessible to those who need them.

Clearly any of these can harm the operation of the affected organisation. Security breaches can also affect trust and reputation, both of the organisation and its services by its users, and of the organisation by external partners who it needs to work with. Ultimately an organisation that is not seen to be dealing effectively with security can find that other people and organisations are unwilling to share information with it, or accept communications from it. Such damage to reputation can last much longer than the security breach itself.

1.3 Motivation and methods

There are a wide range of different reasons why someone may wish to breach an organisation’s security. The most obvious is where a particular organisation is targeted, for example because the attacker wishes to protest against the organisation or its activities, or because the organisation has information the attacker wants. However it is probably more common for Internet-connected computers to be attacked merely because they are Internet-connected. Universities and colleges in particular may be seen as having large resources of bandwidth, storage and processing power that could be useful tools for a network attack against a different organisation, for unlawful storage or distribution of information, or merely to send large volumes of junk e-mail. Organisations with a high reputation may also be valuable for the trust that others have in them - scammers seem to gain additional value if they can send their mails ‘from’ a reputable e-mail domain.

Attacks seldom follow the movie stereotype of a lone attacker directly probing his ultimate target. More typical is an automated financially-motivated phishing attack where users at an organisation will be sent forged e-mails apparently from their IT service to try to persuade them to login to a site that appears to be within the organisation but is most likely to itself be hosted on compromised computers somewhere else. If users are fooled and give away their passwords these will then be used to log in to the organisation’s webmail service and used to send either bulk advertising mails (for which the advertiser will pay money) or yet more phishing e-mails. The contents of the compromised mailboxes may well be copied in case they contain other information of value. Such an attack can affect the confidentiality, integrity, availability and reputation of the organisation since mails may be sent in such bulk that the webmail service is overwhelmed and other organisations place it on a black-list from which all e-mails are rejected.

1.4 Achieving Security

The ideal would, of course, be to prevent all security breaches in the first place. This guide suggests ways that computers, networks and people can be made more resistant to the most common kinds of attack. However even high-security organisations still suffer security breaches and education organisations are unlikely to be able to widely deploy as strict preventive measures as they can. Organisations therefore need to also develop systems and processes to detect security breaches promptly, contain their effects, undo the damage as far as that is possible, and learn from each incident how to improve their security measures and reduce the likelihood of future incidents. Information on planning to respond to security incidents may be found in our guide to effective incident response [1] and on the Janet CSIRT [2] pages.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/security-issues-raised-connection-janet

Links
[1] https://community.ja.net/library/janet-services-documentation/effective-incident-response
[2] https://community.ja.net/library/janet-services-documentation/janet-csirt