

Don't pull your finger out

Mike Bromwich, Technical Director, PDMS

June 2001

IT security is a much broader subject than may at first be apparent. The reason for this is that the word 'security' can be applied to many different areas of IT and the business processes and structures it supports. In previous articles, we have covered issues such as encryption, authentication and privacy under the heading of security. In this article, I address the less glamorous but in many ways more important issue of network security, and its role in preventing (and detecting) unauthorised access to your systems.

The areas of security previously mentioned have grown largely from the increasing reach of the Internet. Now that everyone and everything is becoming 'joined-up', we can communicate, interact and transact electronically. This has introduced the requirement for encryption and authentication. Ironically, it is this growth in the Internet which has, to a large extent, introduced the requirement for network security. Although the issue has been addressed in many instances, it has recently been reported that 80% of corporate networks which are at some time connected to the Internet have nothing in place to hinder the progress of anyone maliciously attempting to gain access to their systems.

There are many approaches which would-be intruders can use to poke their noses where they are not wanted. Many can be explained via analogies with physical attacks which are already well understood.

Installing a firewall is akin to locking the door on the front of your house. It allows access for authorised individuals, but it has a letterbox to allow people to send you letters and messages. However, if you are careless, a burglar could use the letterbox to reach through and turn the key on the inside of your door. The burglar (and anyone else who is passing) can then have free access to your property, possessions and confidential information.

Only a small configuration or software flaw is required to provide the access required to apply this technique to your network. Typically, the letterbox is the inbound route to your mail or web server. A bug or misconfiguration in either of these is all that is required to gain enough access to your network to make your firewall as useful as a chocolate fireguard.

One way to minimise the risk posed by such attacks is to use a network design which includes a 'De-militarised Zone'(DMZ). This is similar to an air lock, and forms a double-skin around the critical sections of your network. E-Mail and Web access is allowed only into this restricted part of you network, and hence the next layer of security can be much stronger. It is still important to make sure that the outer layer of security is appropriate, otherwise your DMZ can act as a staging post from which a second attack can be launched.

Another common type of attack is known as a Denial of Service attack (DoS). This is similar to someone pushing a pipe through your letterbox and pumping in a few thousand gallons of treacle. Everything grinds to a halt, and you cannot get in or out of your house.

This type of attack can be difficult to address, since by the time a DoS attack is underway, it can become impossible to gain access to the firewall to make the necessary changes. If your house is full of treacle, it is difficult to get to your front door to close the letterbox.

Some means of entry can be more vicious. Posting a bomb through your letterbox that is disguised as a package is an efficient way to wreak havoc. Similarly, sending a virus or 'trojan' as an attachment to a message can cause similar devastation to your IT systems. Opening the attachment executes a program which can cause all manner of chaos, including deleting information, rendering your network open to further attack, and/or distributing itself to everyone in your address book.

There is sophisticated software available which analyses each message that arrives at your network, and quarantines any messages that contain such nasties. Ironically however, the increasing use of E-Mail encryption can make it impossible for such software to work efficiently, and it is therefore important to choose encryption and virus protection software which co-operate with one another or which is integrated into a single package.

We have already mentioned one tool that can be put to good use to further the cause of network security. A firewall is a device (or piece of software) that monitors connection attempts between the internal network and the outside world and decides which traffic should be permitted. There are, however, a couple of issues that must be considered when deploying a firewall. Firstly, having a misconfigured firewall is as dangerous as having no firewall at all. In fact, it may be more dangerous, since it can inspire a false sense of security that leads to dangerous working practices. Secondly, it is not necessarily the link to the outside world that poses the greatest risk. Traffic that the firewall permits since it matches criteria that it considers safe can do significant damage when it arrives at its destination. For example, a harmless-looking but carefully constructed web request can exploit deficiencies in the web server that receives it. It is therefore imperative that the purchase of a firewall is not considered as the only step required to secure your network - all your IT systems should at least be considered.

Physical security, internal procedures and training are also important aspects of IT security. Failing to secure access to servers, forgetting to disable the accounts of ex-employees and permitting the use of weak passwords are all easy to implement but are often neglected.

In most cases, however, many safeguards are in place there will still be some weaknesses in design, configuration or procedures. An Intrusion Detection System or IDS monitors your internal network and reports any suspicious activity. If it detects anything that appears threatening, it can respond by generating notifications or in some cases proactively making changes to network configuration to eliminate the threatening traffic.

If you've read this article so far, it should be apparent that securing IT systems is not a one-off task that must be performed. It is an ongoing mindset and activity that should be planned, monitored and managed. The more reliance we place on electronic communications, the more important it becomes that network security is addressed.

Legend has it that a young boy from the Netherlands once saved his town from flooding by spotting a small hole in the dam and plugging it with his finger. Network security is very similar. Problems need to be recognised and addressed before they become issues. Once the dam breaks, it may be too late.