

Network Security: Issues for Online Education

Steven Hatch
MultiMedia CBT Systems Australia

Abstract

With the expansion of the Internet in the 90's and its uptake by business, education and personal users, as a means of transferring data and communicating using the computer, security of data and its protection from viruses, hackers and others, has been of growing concern.

Over the last year in my work as a consultant on online learning I have seen a number of examples of security measures impacting on students and teachers using online technologies. This paper will use a series of small examples to highlight network security issues and their impact on online education.

Introduction

With the expansion of the Internet in the 90's and its uptake by business and personal users as a means of transferring data and communicating using the computer in the office, home or on the move, security of data and its protection from viruses, hackers and others has been of growing concern. Paralleling the expansion of the Internet has been the development and uptake of online forms of teaching and learning. Universities, schools, technical colleges, private training companies and corporations have all begun to adopt online learning technologies and resources to expand the flexibility of and access to education and training. Networked "systems have become the norm for the successful operation of any business" including those in education (Khandelwal & Natarajan, 2002, p39).

Over the last year in my work as a consultant on flexible and online learning I have seen a number of examples of security measures within educational institutions themselves impacting on students and teachers using online technologies for learning and assessment, and have learnt of many more from students and their institutions, of problems associated with security measures.

Security Cases

1. A teacher at an educational institution clicked on an attachment from a student after reading in the body of the email that the final assessment was attached, to find that the attachment is a text message that read, "The attachment to this email was automatically deleted due to it not being of a type allowable". The subject was databases within an IT degree and the attachment deleted was a Microsoft Access Database file.

2. An institution was the subject of a series of attacks by Hackers, and the IT department installed a new firewall that excluded all students and staff from accessing the network from the Internet. All access to library records and online learning systems were denied for one week.
3. Students at a major regional university were attempting to access a CHAT room as part of their online course. Only 3 of over 20 students were able to successfully access the chat session from their workplace.
4. Some students attempting to use the website construction feature in Blackboard found that while they could login to the course management system, they could not login to the website feature.
5. Students from many universities have complained that they are unable to access various websites from within the institutions computer network.
6. At a major institution the IT Administrator informed all staff that he had noticed an increase in emails with attachments that appeared to be students assignments and the practice of allowing students to submit any work electronically had to stop.
7. Teachers trying to run educational CD ROMs for their students found that they were unable to get the CDs to run and gave up.
8. Students and staff at a large institution were unable to log-on to any online learning materials or to complete forms, as the network prevents any data being sent out.

Discussion

Prior to computers and in the early days of computers, security consisted mainly of keeping records and later computers, behind locked doors (Lierley, 2001). Today with computers on every desk, in schools, universities, libraries and homes, security has become a much more complicated issue. Security, which was once considered to be just a consideration for governments computer systems, is now one of the major issues for all IT administrators and computer users (Fisch & White, 2000).

Fisch & White, (2000) point out that a good security system provides confidentiality and integrity by confirming the identity of the people who are attempting to access the computer or network, and protects against inappropriate access by users, while providing availability for those that need to be able to access the systems to use them in an authorized manner. The idea is that computer security should keep out the bad guys while allowing the authorized users to do their job. The problem is that many of the security problems that occur, are instigated or caused by those that are authorized to use the system, that is, by authorized users using the system to commit fraud, spy on records, steal customer lists, load unauthorized programs, play games,

download programs, watch TV, view videos, or surf the web for non business related matter. This makes the job of the IT administrator very difficult. Not only is there a need to protect the system from those on the outside, but also from those on the inside, while always having an eye on the budget and network capacity.

A quality security system involves the following principles:

- Identity – each user, program, object, and resource is uniquely identified.
- Accountability – users can be held accountable for their actions.
- Monitoring – a record is maintained of user's actions.
- Authorization – rules exist that govern access to systems.
- Least privileges – users are restricted to the resources needed to perform their job.
- Separation – areas of greater risk or security need are separated from interfering with the other systems.
- Redundancy – duplicate hardware and copies of data are maintained to allow for failure and to provide timeliness access to information (Fisch & White, 2000, p37).

Why, if a good security system allows users access to the tools that they need to do their job, have the institutions in the case studies instituted policies that make it harder for people using Internet resources, CD-ROMs and online learning products? The simple answer is that it is usually easier and cheaper to bar everything. The real issue lies in the fact that a lot of IT Administrators neither fully understand all the new technologies that come along, nor why, and if, they are needed for the efficient running of the organisation, parts of the organisation or an individuals job or study requirements. Often when an IT Administrator is approached by a single individual wanting, say Flash™ or JavaScript™ to run on a computer, the request is ignored or refused, as it is very time consuming to support a single installation that is different from the standard, and even more so when you do not understand how the technology works.

Specific issues that are of particular importance for online and computer-mediated learning include the following.

- The Chat feature of the major learning management systems (LMS) such as Blackboard™ and WebCT™ rely on the use of Java script. With the advent of self launching viruses, many corporate have set the defaults on their web browsers to disable the use of Java scripts by the web browser. Some even go further to block Java access to the entire system, so that users cannot reset their browsers to accept Java applications such as Chat. Another problem is that many firewall products do not provide for CHAT programs and thus they are disabled (Enck, 1998). CHAT programs are often used by Hackers to transfer information into and out of the systems they have hacked. The ports opened by CHAT programs also provide a means by which hackers

can enter a system or scan it for Internet Protocol (IP) addresses (CIAC, 1998).

- The use of websites or CD-ROMs requiring plug-ins or the installation of programs or viewers. IT Administrator typically bar the installation of any plug-in or new program for a number of reasons. The first is licensing. It is an imperative that IT Administrators know exactly what software is installed on their computers to ensure that the organisation complies with copyright and licensing regulations and agreements. The second is to stop people installing games or other programs not related to the activities of the business, and with which people will waste time when they should be doing their job. Thirdly, hackers or people wanting to steal information could install some programs that collect information and transmit that information or save it for later use. Fourthly, some programs use up a lot of network capacity and thus slow the network down. Lastly, programs that contain viruses could be installed and spread throughout the network causing loss of data.
- Firewalls and software such as WebWasher™ and DynaBlock™ provide the ability to use a single solution to provide very broad ranging security protection (Hurwitz, 2002; Lawson, 2002). The advantages of these products are that they are reasonably priced and easy to set up. The disadvantage is that without spending time to analyse the business needs for various applications and access, most IT administrators are tempted to just set the Firewall to block everything without taking the time to manually configure the device. With programs such as WebWasher™ the IT Administrator is able to block applications such as shopping and subscription services. However, this is done by blocking the Internet browsers' ability to send information out of the network. This then stops people from being able to fill in forms or log-on to any service.
- The high cost of servers, storage, network bandwidth, Internet access and security issues all combine to allow IT administrators to restrict access to email attachments and image rich content in websites.

Conclusion

Security will continue to be a major issue for educational institutions and their students for the foreseeable future. What is now needed and will be required is a better understanding, by the IT people, of what is required in the way of network access, plug-ins, bandwidth and applications to conduct the educational aspects of the business and a better understanding of the security and cost issues of security, and bandwidth, by the teaching and administration staff. This will not happen until we get all the parties, including IT, Administration, Finance and Teachers, involved in a process of constructive dialogue. This process of constructive dialogue will need to involve a process of education for all those involved.

Research should also be conducted to determine the true extent of the problems that security and bandwidth issues are causing to teachers and their students.

Trademarks TM All Trademarks are the property of their respective owners.

References & suggested reading

Cameron, D (1996). Security issues for the Internet and the World Wide Web. Charleston, SC, USA. Computer Technology Research Corp.

CIAC (1998). What you really need to know about Internet relay chat. Livermore, CA, USA. Computer Incident Advisory Capacity, Lawrence Livermore National Laboratory.

Enck, J (1998). Administrator's survival guide: Systems management and security. Loveland, CL, USA. Duke Press.

Fisch, E A & White, G B (2000). Secure computers and networks: Analysis, design, and implementation. Boca Raton, FL, USA. CRC Press.

Hruska, J & Jackson, K M (1990). Computer security solutions. Boca Raton, FL, USA. CRC Press.

Hurwitz (2002). Protecting the perimeter. Framingham, MA, USA. Hurwitz Group.

Khandelwal, V K & Natarajan, R (2002). Quality IT management in Australia: Critical success factors for 2002. Penrith, NSW, Australia. University of Western Sydney.

Lawson, A (2002). Internet security research paper. East Yorkshire, UK. Butler Group.

Lierley, M (2001). Security complete. San Francisco, CA, USA. Sybex.

About the Author

Steven Hatch runs a consulting business in education specialising in Multimedia, Online and flexible delivery of education and training and professional development for teaching using technology. Steven clients include major corporations, registered training companies, schools, TAFE Institutes and Universities. Steven has a Diploma in IT, a Grad Dip in Computer Based Learning, a Master of Online Education and a Master of Education (Adult). Steven is currently completing a Doctorate in Professional Development for Online Teaching.

Steven may be contacted at steve@mmcbt.com