OAKLAND UNIVERSITY

Thursday, November 18, 2004

Team works long hours to recover from cyber attack

*By **Dawn Pauli**, contributing writer*

A message Theresa Rowe, assistant vice president of University Technology Services, received the morning of Nov. 6 was the first hint something was wrong with Oakland University's computer system.

"The initial call reported a problem with the Kresge Library network. After a network problem was ruled out, we had to figure out what happened before we could fix it," Rowe explained.

Sometime early Nov. 6, an intruder working from a remote computer hacked into one of Oakland University's campus domains, Opennet.

"By all appearances, the hacker was trying to be as malicious as possible and destroy what they could destroy," Rowe said. "It was the most invasive attack on the computer system we have experienced."

Rowe gathered a team of key system administrators, including Steve Glowacki, John Coughlin, Dan Fryer, Shaun Moore, Mike Cojocari, Shajan Kay, Aaron Wyatt and the HelpDesk team, including Chris Condie and his staff of OU students, to work on restoring computers.

Security measures were able to contain the damage, however, about 40 desktop computers and 15 servers were stricken.

"On any given day, about 5,000 devices connect to our network. Only about 55 computers and servers were affected by this. Percentage-wise, we did a good job in stopping what the hacker was attempting to do," Rowe said.

Most importantly, data was not accessed from the Banner Servers or other non-Opennet programs. The SAIL system was not affected, and winter registration began on schedule Nov. 8.

OU team members worked long hours to reformat computers affected by the attack, rebuild operating systems and restore backup files.

"Our biggest challenge was helping people restore information who did not back up their desktop computers," Rowe said. "We're working to try to help people recover data and are using special tools that can read deleted data."

Mary Otto, dean of the School of Education and Human Services, found herself without a computer for four days. Fortunately, all her data was recovered.

"I think people like me who lost use of their computer for several days learned the importance of the old fashioned ways of communicating – the telephone, meeting in person and mail," Otto said.

Investigation under way

Despite the many security measures built into computer systems, unauthorized entry into a computer system to cause damage, commonly known as hacking, is still widespread among U.S. businesses.

With the assistance of the University Technology Services Department, the Oakland University Police Department and Computer Crime Squad of the FBI in Detroit are conducting a joint investigation.

"The intrusion was malicious and perpetrated with the intent to damage the system. Every effort will be made to identify the responsible person or persons and seek prosecution to the fullest extent of the law," said Sam Lucido, chief of the OU Police Department.

Rowe acknowledges it will be difficult to find the perpetrator of the attack. “These people are pretty smart and usually take steps to cover their tracks. But, we have a lot of tools in place to track things like this, and we are reviewing all of that data with the police department.”

Future security

It’s the responsibility of each member of the OU community who uses the network to ensure its safety and security.

UTS will be distributing information to faculty, staff and students about how to secure their desktop computers and why it is critical to backup data on a regular basis.

“Once the dust settles, we’ll analyze all the data and create new strategies for protecting assets,” Rowe said. “We’ll examine it very closely and put new safeguards in place. We’re always looking at new threats. We try to stay one step ahead, but there are many computers all over campus that different groups are responsible for maintaining. We’re as good as our weakest link.”

SUMMARY
Sometime early Nov. 6, an intruder working from a remote computer hacked into one of Oakland University’s campus domains, Opennet. Security measures were able to contain the damage, however, about 40 desktop computers and 15 servers were stricken. OU team members worked long hours to reformat computers affected by the attack, rebuild operating systems and restore backup files.

Created by CareTech Administrator (webservices@caretechsolutions.com) on Thursday, November 18, 2004
Modified by CareTech Administrator (webservices@caretechsolutions.com) on Thursday, November 18, 2004
Article Start Date: Thursday, November 18, 2004