Senior Airman Corey Clements

Senior Airman Aaron Markell, a tech controller assigned to the 437th Communications Squadron, keeps routine watch over the Firewall, ensuring incoming and outgoing correspondence flows correctly.

437 CS maintains vigilant watch

By Staff Sgt. Pamela Smith
437 AW Public Affairs

Members of the 437th Communications Squadron Information Systems Flight spend their days, and sometimes nights, vigilantly keeping watch over the wall – the firewall that is.

"Firewall is more of a concept than an individual item," said Master Sgt. James Kincheloe, chief of Information Protect Operations.

The firewall is the name given to the electronic equipment that monitors all incoming and outgoing computer traffic to Charleston AFB.

"When you think of the firewall, think of Swiss cheese," said Kincheloe. "There are holes in the wall that only certain numbered codes can get through." That is what determines who can access internal programs.

For instance, from a home computer someone can log onto the Charleston AFB web page via the Internet because it's outside our security perimeter, but only certain computers can access Intranet sites from off base.

Individuals seeking access to the Intranet from off base must request it in writing with proper justification. After a technical review, IPO recommends approval or disapproval to the Network Control Center chief or superintendent.

The base deals with an average of five to 10 attempted unsuccessful invasions monthly,

"Hackers attempt to crack the code and each time they attempt, a warning goes off at the Automatic Secondary Intrusion Management site," said Kincheloe. The ASIM, which is monitored 24 hours a day, seven days a week at Scott AFB, Ill., sets off a signal. The crew at Scott calls through to the IPO office here and lets them know that someone is attempting to gain entry.

Once members from the IPO office are alerted, they begin to track down the hacker by their Internet Protocol address, which is a unique, numeric identifier used to specify a particular host on a particular network and is part of a standardized scheme for identifying machines that are connected to the Internet.

Once a hacker is identified, IPO turns the information over to off base authorities.

The firewall is the main line of defense against disaster.

"If a hacker gains access, the damage can go undetected," said Alvin Green, 437 CS Chief, Network Control Center. "It can be fixed if changes are noticeable, but some changes may go undetected if they're not obvious."

If a hacker were to gain access to medical records, they could change a blood type or something like that and that may go undetected until its too late, he said. IPO ensures the availability, integrity, and confidentiality information on our network.

February is Information Awareness Month and is a good time to remind people to take proper security measures when using their computers. "It's just as important to be vigilant on the computer," Green said.

Some suggested precautions are:

- Apply AFCERTS service as soon as they're received
- Only load approved software
- Never give your password out

IPO has been successful in preventing hackers access to the Charleston AFB system and recently passed their inspection with flying colors.

"We received a vulnerability assessment from the Air Force Information Warfare Center and they were unable to break through our firewall," Green said.

Maintaining the firewall is an ongoing process that includes regularly backing up the system. Weekly, base computer systems are shut down and reconfigured. At that time, no information leaves the base or comes in.

Green and Kincheloe agree the biggest threat to computer security comes from the inside. "That's why people are encouraged to use "good" passwords and password protected screensavers," said Green. When talking about security people must think broader than the flightline. The protection of our mission critical network must be an absolute priority.

"It's just as important to be vigilant on the computer."

Information Awareness Month

Tip of the week

- Always scan disks, e-mail attachments, and downloaded files using the latest updated anti-viral product and signature file
- Clear/sanitize appropriate processing and storage devices
- Report incidents and vulnerabilities to your unit Computer Systems Security Officer