

Heed the hackers

Is your computer system and network safe?

Cheryl Hentz

The more sophisticated our technology becomes, the more sophisticated the security threats against that technology become.

Today's threats are basically two-fold, says Peter Mariahazy, director of technology and

human resources at Modern Business Machines, Appleton. One is unauthorized access from outside — people accessing a network without clearance. The other is protecting portable data.

“Laptops, jump drives, exter-

nal hard drives and things like that allow data to physically walk out of the building. That data can easily be recovered by someone who's unethical,” says Mariahazy.

Installing multiple layers of firewall protection is a way to combat the first problem. That can help prevent unauthorized access into one's facility, Mariahazy says.

“In our business, for example, we have a standard firewall, a secondary firewall, and a tertiary software-based firewall. That helps us control access. The problems can also be reduced by programmatic changes of passwords,” he says. “For example, we have two wireless networks here instead of just one. We have one that's outside of our network but has access to the Internet and is open to the public. And we have one internally that's behind our firewall and is password protected. And we change that password on a regular basis, also.”

Senteras CEO Steve Luebke agrees that having a layered defense in place is the best offense.

“It should do the following, and these are in no particular order: Protect the physical, protect the data, protect the transmission and protect the access. That includes a combination of policies and procedures, physical security, network appli-



ances and things like firewalls and anti-viruses,” he says. “But remember, people are the weak link in this. If you have everything configured properly and have the best security system in the world but an employee walks out the door with sensitive customer data and it’s unprotected, the millions of dollars of security have just been defeated.”

Protecting data can easily be accomplished by using encryption software. So even if someone gets their hands on a device, they can’t access the data. Encryption software can encrypt everything on the device or selected data, depending on what your needs are. And almost all laptops today have a hard drive encryption, Luebke says. As you start your computer up, it asks you for a password.

“And that password is coded into the hard drive, meaning that I can pull that hard drive out of one computer and stick it in another computer but it’ll ask you for the same password. A person couldn’t even reformat the hard drive using this option, because without the password, it won’t even let someone get to the operating system,” Luebke says.

As companies do business in an increasingly global, more networked economy, security threats become more prevalent, says Raj Veeramani, director of the University of Wisconsin E-Business Consortium.

“It has necessitated companies to create touch points between their infrastructures and those of other companies,” Veeramani says. “If those touch points are not configured with proper security in mind, it can

Laptops, jump drives, external hard drives and things like that allow data to physically walk out of the building. That data can easily be recovered by someone who’s unethical.

**PETER MARIAHAZY
MODERN BUSINESS MACHINES,
APPLETON**

create potential security breach problems. And sometimes you can have the correct technology-based solutions but if you don’t address people and process-related issues, there are still potential vulnerabilities.”

IT security professionals recommended detailed data policies for employees and communication to ensure they are aware of potential security problems. Have them change their passwords on a regular basis >> and make sure that they keep their devices secured whenever possible; computers should not be left on and unattended.

“Common sense practices make a world of difference,” says Mariahazy.

Finally, spam is a huge threat, as are spyware, adware, malware, viruses and worms, mainly because if they get into your computer or if you open something that has one of these attached,

the sender can gain access to confidential or personal data.

“The spam is just an atrocious, atrocious thing,” says Heath Petersen, field technician at Baycom in Green Bay. “A lot of it is just advertisements. But that’s where a lot of the viruses are starting to come in, in the adware, spyware, malware, whatever you want to call it, to basically track your activity in numerous ways. A lot of these e-mails, if you were to open them, will install a program that will do just that and it will send back to the sender information that you’re thinking is secure.”

Petersen recommends using a good antivirus suite.

“The highest rated software program right now is Norton Internet Securities Suite 2007. There are a couple others out there that come pretty close, but when you look at overall protection, that’s the one that’s rated No. 1, across the board, at this time,” he says (it should be the Internet suite program, 2007 version for maximum protection). “It protects you from all the aspects of problems, not just virus, not just spam, and it’s not just a firewall.”

Finally, having a quality network provider is important because that provider can also monitor for security breaches.

“Obviously, if someone is very focused and very dedicated in trying to get in, it’s possible that they’re going to find a way in. It’s like locking your car and setting the alarm; a professional car thief is probably still going to be able to get in. And it’s the same here. You just need to make entry from every avenue as difficult as possible.” **M_p**