

Protecting Your Business from Internet Threats

By BNET Editorial

published on BNET.com 10/25/2007

Internet security is a critical issue for any business. A breach in Internet security that damages your business computer system can result in reduced productivity and lost consumer confidence. Internet security depends as much on human expertise and experience as it does on security software, so be sure to involve all of your employees in developing and implementing Internet security plans.

What You Need to Know

Are cookies a security threat?

Cookies are installed in your computer by Web sites that you visit in order to collect information on how you browse the Web. Cookies are a relatively low security risk, but can cause users to become lazy about security practices because one purpose of cookies is to remember user names and passwords.

Can you get a computer virus by opening an email?

Yes. It was once impossible to have a computer infected by a virus transmitted by email unless you opened the email attachment. However, more recent viruses simply require the opening of the email itself. Be very careful about unexpected emails from unfamiliar sources. If in doubt, delete without opening.

What to Do

Develop an Internet Security Policy

Your overall Internet security policy should include provisions like these:

- Restrict the number of people who have access to the inner workings of the security system—the fewer people, the better. That's because many security breaches come from within an organization. Keep track of everyone who has access to the system and immediately revoke the access of anyone who leaves the organization.

- Streamline hardware and software. The more complex the system, the more vulnerable it is to attack. In your server software, for example, strip away as many of the optional features as possible.
- Set a password policy. Do not allow simple or obvious passwords. Make sure passwords are changed regularly.
- Set up procedures for regular data backup and for responding to security breaches and recovering from security disasters.
- Hire an external security profession to assess your policies and procedures.
- Be vigilant. The Internet security threat is constantly changing.

Understand How to Use Firewalls

A firewall is software that polices the space between your computer system and the outside world. The design and management of firewalls has become more complex since the advent of the Web because of the vast increase in activity between computers and the Internet. If the firewall is too stringent, it slows everything down and prevents people from performing certain legitimate activities. If it is too lax, it opens the computer up to attack.

Protect Your Business From:

- *Viruses*. Computer viruses are becoming more sophisticated and widespread. You must have antivirus software and make sure it's kept up-to-date.
- *Hackers*. Hackers are people who try to get access to computer systems they're not authorized to use, sometimes for malicious or criminal purposes and sometimes just for thrills. Again, make sure you have the best available security software and that you continually monitor your computer systems for any suspicious activity.
- *Denial-of-service attacks*. These are attacks intended to crash a Web site by deluging it with phony traffic. Sites operated by CNN, E*Trade, Amazon, and other well-known companies have been the victims of these attacks. While it's difficult to stay ahead of determined hackers, some firewalls are designed to combat denial-of-service attacks.

Prepare to React to a Security Breach

After a security breach, there are two basic objectives:

- *Find out what happened* so you can stop it from happening again. It's best to have an agreement with an external security professional, whom you can call quickly if a breach occurs. The professional can help you determine if your information has been tampered with and guide you in setting up protection and monitoring systems to prevent further problems.

- *Find out who did it* so you can prosecute or otherwise deal with them. Unfortunately, it is very difficult to prosecute an individual for a security breach without hard evidence, and it's very easy to contaminate or destroy such evidence.

Protect Your Web Server

Web servers interface with the World Wide Web and are very vulnerable to its hazards. If hackers can break into your server, they are closer to breaking into your entire computer system. Make sure you understand and deal effectively with threats to your server. If you offer e-commerce, it's essential to have a server with encryption and secure data storage capabilities, so credit card data and other information can be protected.

Consider Restricting Access

You can restrict access to all or at least part of your Web site in a number of ways. The most common is implementing a user name and password system. You can restrict access by IP (Internet) address, so that only people connecting from a certain address or domain can access information. Perhaps the most powerful approach is to use public key cryptography, which allows only the person with the assigned cryptography key to request and read the information.

Pay Attention to Outsourcing

Outsourcing creates an increased security risk. You must ensure that vendors will adhere to your security policy and conduct all work according to security procedures. Ask yourself these questions about any vendor you may use:

- What is the vendor's security policy?
- What are its data backup and disaster-recovery procedures?
- How is your data safeguarded from that of other customers?
- How is your data safeguarded from the vendor's own employees?
- How is the vendor insured with regard to security breaches?

What to Avoid

You Drop Your Guard

There is no such thing as a perfect security system. Without constant vigilance, computer systems become an open invitation for hackers and viruses. An essential part of such vigilance is having the very latest security patches and antivirus software installed.

Viruses are becoming increasingly common. If you haven't had one so far, either you are tremendously lucky or you have excellent antivirus procedures, which you should rigorously maintain.

You Think That You Are Anonymous on the Internet

In general, you are not. When you visit a Web site, you may reveal your IP address, the Web site you visited previously, the operating system on your computer, and other information.

Where to Learn More

Books:

Ellis, Juanita, and Tim Speed. *The Internet Security Guidebook: From Planning to Deployment*. Academic Press, 2006.

Schweitzer, Douglas. *Internet Security Made Easy*. AMACOM, 2001.

Web Sites:

CERT Internet Security Center: www.cert.org

IT Security: www.itsecurity.com