Ethical Hackers

Many people think the words "ethics" and "hacker" do not go together. Of course, if you are hacking into a computer illegally, they still don't. But ethical hacking has become a well-respected profession, and ethical hackers are employed by some of the biggest international companies in a bid to beef up internal and external IT security and assert a position of impenetrable strength against would-be hackers.

It didn't take long for corporations to realize that if they were going to have perpetrators break into their computer systems, it was better to have such hackers working for them rather than against them.

Why are ethical hackers needed?

Organizations must secure their IT networks. As hackers become more sophisticated, so do the threats. The dangers faced by organizations today include corporate spies hoping to dominate the market, teens looking for a challenge, and people releasing malicious code into the wild. Without the proper protection in place, any of these hackers can cause untold damage to an organization. So the rationale is that rather than relinquish control to such perpetrators, today's organizations should employ ethical hackers to plug up the security holes in their systems.

What do ethical hackers do?

An ethical hacker is predominately a penetration tester who is employed or contracted by an organization to attempt to penetrate the organization's security network. Ethical hackers use exactly the same tools as illegal hackers; the difference is that they have authorization from the organization to infiltrate the network and will be given detailed boundaries to work within. The ethical hacker will look for weaknesses in the system, report back to the organization, and plug the holes to enhance the security of the system.

How did ethical hacking start?

In the 1970s, as governments began to rely on computers to store confidential information, it became critical to ensure that their systems were secure. The United States government was the first to use a group of experts called "red teams" to hack into its own computer systems in order to establish and eliminate any weaknesses. Today, organizations such as IBM employ their own teams of ethical hackers. Computer security services have become a multi-billion-dollar industry as a result of this trend.

Today's ethical hackers can advise companies on ways to protect their data internally as well as externally. Organizations often fail to take even the most basic security precautions. One ethical hacking company explained that every organization it has worked with has had security threats of one kind or another.

While employing ethical hackers is a positive step toward securing an organization's computer systems, the illegal hacker always has one advantage: time. Hackers often have unlimited time in which to access a system, time they invest well for unethical gains. Still, it takes one to know one, so as long as an organization continues to use ethical hackers, they have the best system in place to combat a threat that increases with every change or upgrade in technology.