

INTERNET SECURITY WHITE PAPER

Author: Tom Currie, ICS Consultant

How many times was your Internet security tested this week? If you don't know, or worse, don't think it matters, read on. Current reality is that any routers or computers which have Internet addresses are being tested almost continuously.

Once upon a time, breaking into computer systems was the domain of a somewhat closed community. The favorite targets were big-name computer systems loaded with sensitive information. When the whole world met online, the Internet showed the whole world how to break into computer systems. With easy access to the tools of the trade, anyone with a modem can try their hand at becoming a hacker. This has created a synergy in the development of break-in tools to the extent that entire break-in product suites are available to anyone who cares to download them.

The process of breaking into someone's computers has been trivialized to configuring a robot program and turning it loose on the Internet. The robot tries every address on the Internet and reports back to it's owner which machines are unsecured and which lock pick to use on each system. The newest crop of hacker toolkits goes one step further and breaks into your system (leaving a back door) then reports back which machines are available and ready for use by the hacker. The ICS intrusion detection systems are indicating that there may be hundreds of such programs running loose over the Internet at all times.

We're not usually talking about seasoned technicians trying to steal national secrets. A more realistic analogy is vandals casually going through your neighborhood trying every door and window. The goal is not necessarily to access your mission critical data. It's more likely someone trying to use your computer as a launching pad for further attacks. Popular among current break-ins is taking control of many hundreds of remote systems to assemble an army of slave computers. The slave computers in turn get configured to look for other vulnerable systems, which will in turn be deployed to look for yet more vulnerable systems, and so on.

If you knew that strangers were casing your house every day, how would you react? The "bad guys" are scanning your machines all day, every day. You can't stop them from *trying* to pick the locks, but you have a responsibility to ensure your systems are locked down and (analogously) use good quality locks.

Like shoplifters in a department store, the "bad guys" will keep coming back, and they are there pretty much all the time. We suggest that IT managers follow the good store managers' model. They monitor everything, document every infraction no matter how slight and notify police whenever a crime has been committed.

The sad facts of network security are that every time the "good guys" plug a hole, the "bad guys" find a new one. This has created an ever changing landscape for the security battles. The rules of the game are changing daily and nothing should be taken for granted. "Good enough" yesterday is sometimes laughable today. So what is a responsible IT manager supposed to do?

The popular hacker toolkits are readily available and very effective. They allow any dolt to break in quite easily, but they can also be stopped quite easily. Your role as manager is to ensure you have sufficient security staffing to provide full monitoring capability. Some basic practices can thwart the assault of a robot hacker. First, implement a firewall. Second, keep your computers up to date. Third, have a legally enforceable security policy.

How to use a Firewall

1. Compile a complete list of all legitimate *inbound* connections such as:

- Incoming email only to your mail hub,
- Incoming Web browsers only to your Web server,
- Domain Name Services only to your DNS server, and
- Client e-business access only to the machines which serve up e-business.

This list must be maintained as your operation evolves and must be audited periodically.

2. Compile a list of legitimate *outbound* connections such as:

- Outgoing mail (only from your mail hub), and
- Outgoing Web access by your employees (only from your Web proxy).

Because the inbound and outbound lists must be continuously maintained, ICS advises our clients to appoint someone by name as the individual responsible for maintaining the lists. When you implement a good quality firewall to enforce these lists, you have now cut the threat to your systems by 50%.

Scrutinize your firewall logs. We've seen a recent change in the scanning patterns of some hacker toolkits. The various probes are now performed in random order, the probes are done slowly over many hours or in one case over several days. These changes mirror the improved defenses. Having a human check the logs needs to be mandatory.

For a clear, no-nonsense approach to implementing your first firewall we recommend [Building Internet Firewalls](#) by Chapman & Zwicky.

Keep your Systems Up to Date

Far and away the bulk of robotic exploits are based on defects in programs you are already running. Obviously, this implies that some programs are more secure than others, based on the quality of the software. Most vendors issue patches in a near real-time environment. The sheer volume of defects found and patches released would overwhelm you if you had to watch them all. A better practice is to have weekly team reviews of the major Internet vulnerabilities documents such as bugtraq, FBI (NIPC), CERT and/or SANS. The team decides which patches to apply and does so. Obviously, this will require a security staff.

Have a Legally Enforceable Security Policy

This is not as trivial as it may sound. When a user connects to your system does it say, "Welcome..." or in effect "help yourself to our data." Or does it say something like the sign on land, "This land is private property, trespassers will be prosecuted"? Although the first statement seems more user friendly, it also give outsiders open permission. You want to preserve your right to prosecute.

Your first line of defense against attack is a well implemented security policy. Your Internet security policy needs to be technically concise and flexible. This policy needs to be periodically audited and re-evaluated. All perpetrators must be dealt with. You must ascertain what is, and is not, against the law. Remember laws vary wildly from state to state; make sure you know your rights. As an IT manager, it is your responsibility to ensure that all proper steps are taken to maintain site security.

Good resources exist to help you develop your security policy. Many excellent books are also available. For a start we recommend Information Security Policy Made Easy by Charles Wood (Baseline Software). This book is a comprehensive guide to security policy written by an esteemed security consultant.