



Subject: Intrusion Detection/Incident Response: Can't Have Just One

July 27, 2006

Dear Real Estate Executive,

After you put up the barbed wire fence, an intrusion detection system (IDS) is like adding closed circuit TV cameras so that security guards can monitor your facilities for an attack. Intrusion detection is the process of detecting improper use of computing resources by unauthorized outsiders or employees.

Today computing environment needs intrusion detection because it is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. This environment is constantly evolving and changing fueled by new technology and the Internet. To make matters worse, threats and vulnerabilities are constantly evolving as well. Intrusion detection products are tools that can assist in managing these threats and vulnerabilities.

Whether you implement and manage your own IDS or use a managed service, your investment will be wasted if you have not implemented an incident response capability. How will you respond to an attack if you do detect it? It was a simple decision before — just pull the plug on the Internet. But now that we rely so heavily on the Internet, this decision is no longer trivial.

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

Before attacking your systems however, an intruder needs to identify potential vulnerabilities that can be exploited. According to Carnegie Mellon University, 95% of all attacks come from vulnerabilities and misconfigurations. So it only makes practical sense to find these vulnerabilities first by implementing a vulnerability management program. This allows you to assess your information assets, analyze which ones to fix first and then fix them. Vulnerability

management process steps can be automated with technology and there are a variety of products, designed for businesses large and small, on the market today that can certainly meet your needs.

In the end, vulnerability management is a process that can be implemented to make your environment more secure. Having an effective means for detecting and responding to security incidents requires your organization to adapt to the rapidly changing demands of the Internet environment.

Mark Lesswing
Vice President
Center for REALTOR® Technology
mlesswing@crt.realtors.org

REALTOR Secure program resources
<http://www.realtor.org/crtsecure.nsf/pages/resources?OpenDocument>

Creating an incident response team:
<http://www.cert.org/csirts/Creating-A-CSIRT.html>

Article on vulnerability management:
<http://www.computerworld.com/printthis/2006/0,4814,107647,00.html>

Intrusion detection article:
<http://www.informit.com/articles/article.asp?p=25334&rl=1>