LATTIMORE BLACK MORGAN & CAIN, PC
CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

How to protect yourself from the rising tide of cyber attacks on financial institutions

Thomas Lewis, Partner, LBMC Security Services

Cyber crime is on the upswing, so it should probably be no surprise that a recent report by the prestigious Center for Strategic and International Studies found that 59 percent of executives surveyed in the financial services sector reported a penetration attack on their computer networks in the past two years.

Stewart Baker, a former senior official at the National Security Agency who led the study was quoted by the Wall Street Journal as saying that penetration "is a form of attack that's rife in critical infrastructure."

The consequences of a successful cyber attack can be devastating from both a financial and reputation standpoint, but fortunately, there are steps that banks and other businesses can take to minimize the threat. We will outline those a little later in this article. But first just a bit more about the latest trends in cyber attacks.

- While attacks on system infrastructure are still quite common, cyber criminals are turning their attention to workstations occupied by end users, where security measures may not be as rigorous as those applied to the infrastructure. For example, penetration of individual workstations can occur where security patches are not consistently applied to programs such Adobe PDF and the Microsoft Office suite.
- Cyber criminals are also making use of social media to gather intelligence about companies that allows them to trick employees into allowing them access into systems. Malware attacks are also being launched from social media sites such as Facebook or LinkedIn when they are utilized by employees.
- Malware is getting smarter and nastier. It has evolved from a straight piece of code that can be identified by its signature to one that can change its signature, making it very difficult to detect. Major commercial anti-virus programs are not always able to identify these pieces of malware.

The average cost of a security breach is $200 per record, which includes legal expenses, fees for identity theft coverage for those affected and the cost of technical work to repair the problem. Many breaches involve thousands and thousands of records.

71 percent of organizations have no external insurance coverage for losses caused by computer security problems, according to the annual Computer Crime and Security Survey conducted by the authoritative Computer Security Institute.

And many organizations believe that they don't have a security problem because they know of no breaches. The fact is that cyber criminals don't want to make their presence in a network known and unless an organization has effective monitoring, it may not find out about a problem until it hears from a customer, law enforcement or the media.

But the good news is that 80 percent of attacks are preventable, according to testimony last year to Congress by the National Security Agency.

While there is no silver bullet for the problem, creating the right processes and cultivating an effective security culture will go a long way towards protection. An important overall step is to implement a cyber security framework, such as NIST, ISO or HITRUST.

Here are four areas to focus on:

Configuration and patch management: Create a system to ensure that security patches are applied in a timely manner to all systems and applications, whether they are at the infrastructure level or the end-user level. A good source of guidance is http://www.cisecurity.org.

System security monitoring: Make sure you have an effective system in place to detect and prevent system intrusions. It is also critical to fully staff those systems or outsource the function.

Secure web applications: Web applications with holes are a major points of entry for cyber criminals, particularly those committing credit card fraud. Make sure developers follow security protocols when they create your web applications and that the applications are fully tested. Perform a hostile security test -- in other words, try to break into your own system through the web application. More information on web development protocols is available at http://www.owasp.org.

Security awareness: Insure that all of your employees, not just your IT staff, are aware of safe computing practices. Techniques include training, newsletters, posters and simulations.

LATTIMORE BLACK MORGAN & CAIN, PC
CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

LBMC's Managed Security Services can help you strengthen your defenses against cyber attacks.

Our intrusion detection/intrusion prevention solution includes a state-of-the art device that is like a burglar alarm system monitoring traffic coming into your system. Our staff monitors your system 24/7/365 and instantly alerts you to problems. It is equipped with a portal that allows you to see what is going on with the monitoring at any time. Our solution can be much less expensive than in-house monitoring.

The device can also function as a managed firewall, creating a layer of protection for corporate networks from untrusted, hostile environments such as the internet, as well as from networks operated by business partners and from possible infiltration at remote offices.

We can also provide managed vulnerability scans. We periodically scan your network and provide a detailed report of vulnerabilities with recommended configuration changes that will continually increase your level of protection.