

Inside NAFCU Services

Top five security initiatives for 2009

By Mark B. Bell

Information security is an ongoing process that requires constant evaluation and re-evaluation of risks and threats to sensitive or protected credit union information. Use the top five initiatives below as a framework to help keep your member information safe and to maintain your credit union's preparedness for your next information security and technology examination.

1. Update Your Information Security Risk Assessment Program

Conducting a risk assessment should be the first step in determining where risk lies and what steps and resources are required to mitigate threats. A formal risk assessment program is not only required by the NCUA, but is the foundation of any strong information security program. In order to remain relevant, a risk assessment must not be a one-time engagement. It must be revisited annually, as well as anytime a credit union experiences a significant change in operations, such as the introduction of a new core processor or the addition of an additional Web presence.

Now is a great time to review your risk assessment to ensure the mitigation strategies for previously identified risks are still current, and to identify if any new risks require review. This analysis will also provide additional justification for your IT security budget.

2. Formalize Your Vulnerability Management Program

Most credit unions already utilize a network vulnerability scanning application, managed by either an internal resource or third-party security vendor. However, many of these applications create a huge paper-based report that is unmanageable and virtually useless for tracking remediation status. Fortunately, paperless vulnerability management programs using software as a service technology exist and not only allow management of the program online, but reduce the overall cost since users only pay for using the software, not for owning it.

Another way to formalize a vulnerability management program is to base it on an accepted standard, like the National Institute of Standards and Technology Special Publication 800-40, "Creating a Patch and Vulnerability Management Program." This standard provides a framework for repeatable processes, prioritizing assets and associated remediation efforts, and identifying security metrics.

3. Conduct User Awareness Training

Having a robust user awareness training program is by far the most effective security initiative a credit union can implement. The most expensive, cutting-edge security technology on your network is useless if employees freely provide usernames and



passwords to social engineers over the phone or via e-mail. At a minimum, employees should receive formal security awareness training at the time they are hired, and they should be provided with refresher training semi-annually.

Additionally, awareness training should be regularly validated to ensure staff retains the information and uses it appropriately. This might include after-hours sweeps for written-down passwords and other sensitive information, social engineering exercises and regular Q&A sessions during all-employee meetings.


4. Implement Web Application Security

Most layered security programs include a firewall and intrusion detection/prevention system to help protect an external Web device. However, what if the IDS/IPS does not properly identify hostile traffic due to the lack of an attack signature or encryption (i.e. Web traffic over HTTPs)? A Web application firewall should be included in a layered network security program to ensure that inbound Web-based traffic meets certain criteria established for communication with a specific Web application.

For more information and a list of different manufacturers of Web application firewalls, please visit the Open Web Application Security Project at www.owasp.org/index.php/Web_Application_Firewall.

5. Perform Vendor Due Diligence

Letter to Credit Unions 07-CU-13 states: "At a minimum, the due diligence review should take into account the critical nature of the service, the level of expertise exhibited by the vendor, staffing changes, economic and regulatory changes, and risk mitigation strategies associated with the vendor oversight."

Even though you may have a strong internal security program, what about the vendors to whom you entrust sensitive member information? Security lapses by a vendor can have a disastrous effect, particularly if the credit union did not perform an adequate due diligence assessment. In 2009, ensure that your credit union's review of its information security and technology meets the minimum due diligence requirements. 

Mark Bell, CISSP, CISA, is the executive vice president of operations at Digital Defense Inc., a preferred partner of NAFCU Services. Digital Defense delivers a comprehensive portfolio of risk management services; more information is available at www.ddifrontline.com.