CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

August 5, 2009

AUDITOR'S ALERT

The Auditor's Office, in the form of an Auditor's Alert, periodically offers guidance and recommendations regarding fiscal matters, accountability, and best practices.

Recommendations to Strengthen Technology Security

Best Practices for Local Governments

In June 2009, $415,989 was taken from a Bullitt County payroll account through fraudulent electronic payment transactions using malicious software installed by an unauthorized intruder on a Bullitt County computer. The Auditor of Public Accounts examined controls in place at Bullitt County to make recommendations to strengthen security over the Bullitt County information system.

The Auditor of Public Accounts, as a result of this examination, makes the following recommendations to assist governments in designing and implementing information technology controls. We have provided a brief overview of various best practices that should be considered when evaluating the security policies applied to a government's specific information technology environment. A more comprehensive discussion of these best practices are available on the Auditor's website, www.auditor.ky.gov/Public/BJSecurityapp/bestpractices.html

We recommend a "defense in depth", where a multi-layered approach to information security provides the most efficient and effective defense against unauthorized system access. Simply put, there is not one single step that can be taken to provide sufficient information security. Instead, several steps must be put in place to create effective security.

1. Security Policy. To ensure that management and employees are collectively working to maintain the security of an organization's system and information, a policy should be developed outlining the decisions made by management related to information security.
2. Passwords. For those applications where a password is used for authentication, the password should be complex and appropriately secured.
3. Backing Up Data. In preparation for contingencies, it is imperative for businesses to perform actions that will allow them to recover and continue their normal business practices with as little disruption as possible. Part of this recovery planning is performing back up procedures for critical applications and associated data.
4. Anti-virus Protection. Anti-virus protection software provides protection from a significant number of malicious software (malware). Anti-virus protection software should be installed on local machines and timely application of vendor-issued updates be implemented.

5. Spyware Protection. Spyware protection tools are a type of detection software, similar to anti-virus, but it reviews systems specifically for spyware. Further, it will remove any detected spyware from the system. Spyware protection tools should be installed on local machines, with vendor-issued updates being made in a timely fashion.
6. Defensive Actions. Users should not open unsolicited emails; click on questionable links or open unknown attachments; provide user names, passwords, or other access codes to anyone; or install any personal software or hardware on an employer's network. Further, users should turn off or disconnect computers from the network when not in use.
7. Be Aware Of Computer Processing. Users should be aware of the normal processing of their system and any variations to that understanding should be reported to your information technology support staff.
8. Keep Software Up-To-Date. All software should be kept up-to-date and all applicable patches should be applied. By keeping software up-to-date and all vendor issued patches applied, the majority of known vulnerabilities should be addressed.
9. Default Passwords. Default passwords, and similar credentials, are those that are assigned by the manufacturer during installation. Default passwords are widely known and offer no security. Technical support should ensure that default passwords are changed prior to placing a system into production.
10. Default Accounts. Many systems and products come with default accounts established and available for use. Default accounts are widely known, so unless these accounts are needed for a business related purpose, they should be removed. Default accounts retained for use, should be properly secured by changing the associated passwords and default names, if possible.
11. Default Services. During the process of setting up a new system, installing new software, or upgrading existing software, unexpected network services could potentially become enabled and available for use. Prior to moving a system into production, all available services should be reviewed to verify necessity. Those services not necessary for the proper operation of that system should be disabled. Any services deemed to be necessary should be secured according to the production documentation.
12. Local Firewalls. A local firewall is software running at the local host rather than at a switch or other network device to limit traffic to and from the local host. This software can be configured to control the types of traffic the local host is allowed to send and receive. Where feasible, a local firewall should be installed on all local machines.
13. Network Firewalls. Networks should be designed to locate the staff hosts and devices within a protected inner area. Access in and out of the inner area should be monitored by a firewall or Intrusion Detection System (IDS).
14. System Hardening. System hardening is the practice of uniformly configuring each system in such a way as to enforce and provide the level of security required by the business' security policy. Every host and device should be hardened against attack and unauthorized use.
15. Conditions of User Notification. Every application and service should include a banner on the first page detailing the conditions for acceptable use.
16. Login Banners. As a general rule, the minimum amount of information necessary to allow a connection to authorized persons should be provided within the banner.
17. Vulnerability Reviews. Every network device, service, application, and host should be periodically reviewed to ensure that there are no identifiable vulnerabilities discoverable by an internal or external intruder.
18. Remote Support. Avoid the use of dial-up modems for communication outside a business' network.
19. Wireless Networking. All available security features provided by wireless networking products should be enabled and regularly reviewed.

Additionally, for those governments either currently participating in or considering using an on-line banking service, considerations should include:

1. Be Well Informed about On-Line Services and Features. Management should gather information related to the on-line application, including security features, security assurances provided by the financial institution, usage agreement related to liability of user and financial institution for incidents of fraud or abuse, and availability of information concerning the account features through the financial institution's website.
2. Logical Security Administration. For proper segregation of duties, we recommend the security administration of individual accounts and users either be delegated to the financial institution or, alternately, establish the administration functionality under an individual who does not have any responsibility for creating or authorizing payments within the account.
3. Account Access Changes. Changes to account or user access should be properly authorized by management. All requested changes to user access, including requests for e-mail address and password changes should be formally documented in either a request form or e-mail. These requests should be maintained to support changes to access.
4. Access Level Review. Access to on-line banking features should be granted on a need to perform basis, removing all accesses that are not necessary for their job duties or the type of processing being performed.
5. Transaction Review. Periodically, management should obtain a listing from the financial institution showing all transactions related to the on-line account. Appropriate management should review the transaction listing to ensure no unusual activity is occurring. All questionable transactions should be investigated and all parties involved be informed of the resolution.
6. Incident or Questionable Transaction Review Process. Management should develop and consistently apply a formal process to address questionable transactions. This process should specify appropriate contract individuals at the financial institution to notify about the situation. Further, documentation should be developed and maintained providing an identification of the situation, contacts made with financial institution and staff related to the situation, actions taken to resolve the situation, and the outcome of the review.
7. Multiple Approvals For On-Line Transactions. To help ensure transactions are properly approved, establish the same requirements for the issuance of a physical check to the initiation and approval of on-line transactions.
8. Dual Notifications. To help ensure that transactions being processed against the account are appropriate and approved, ask that notifications of transactions be sent to the user responsible for initiating the action and a secondary contact. This secondary contact should be aware of the transactions being performed on-line, but not have a specific role in the initiation of transactions.
9. Procedure Manual for On-Line Banking. Once controls are established related to the security over the on-line account and the processing of transactions through the on-line environment, a procedures manual should be developed to itemize the controls to be followed, user expectations, and consequences for failure to adhere to procedures. This manual should be distributed to all applicable staff and training should be provided to ensure staff are familiar with their responsibilities.