SHIFT④

Simple Clues to Early Detection of a Computer Breach

Defending your computer systems from internet-borne threat agents can be a daunting task. Threat agents take on many forms. Among some of the nastiest are Remote Administration Trojans (RATs) and key-loggers that record data for later extraction through the RAT. Threat agents can squeeze through the tiniest crack in your internet defenses, so the only surefire way to protect your systems is to disconnect them from the internet, power them down, and lock them up in a vault. This is obviously not a viable option because you need to use your computer systems.

So, when your internet defenses fail, early detection of a security breach is your last line of defense. For that reason, you must constantly be vigilant for anomalous activity that may indicate your systems have been breached. Early detection of a security breach is the key to minimizing damage to your company's good name.

The ability to recognize the clues that may indicate a security breach is an essential skill for anyone who handles sensitive data. The following are some simple clues that your system(s) may have been breached:

- Pop-up messages from your antivirus software indicating nefarious activity

- Security software (antivirus) has been disabled

- Network/computer activity tracked back to a user not working at that time the activity was logged

- Passwords have changed without explanation

- A user account has unnecessary escalated privileges

- Administrator rights are reinstated after they have been removed

- New users have inexplicably been created

- Applications that used to work no longer work

- New applications suddenly appear on the desktop or in program folders

- It takes longer than usual to boot or reboot

- Computer(s) are running slower than normal

- Computer is performing operations without human input

- Inability to access Task Manager, Registry Editor, MSConfig, Control Panel, Run Command, or other tasks that require an escalated privilege

We recommend you take a moment to share these warning signs with all members of your staff who are involved in the payments process and who have access to your payment systems. Not only will this help you comply with PCI requirement 12.6 (having a security awareness program), it will also help you more quickly identify and isolate potential issues. Further, have your incident response plan conspicuously posted in sensitive areas so that all employees will know exactly what to do and whom to contact should any signs of a breach appear.