Healthy Network Testing to Identify APTs

Advanced persistent threats (APTs) were utilized to breach financial information, costing millions of US dollars during the recent Facebook, Capital One, Google Plus and Uber breaches. APTs are so named because of their ability to hide in the backups and system memories and, therefore, survive the typical policies and procedures used to discover and destroy viruses, phishing attempts and other invasive malware. However, the analytical skills developed by internal auditors and the expert knowledge of network administrators can be combined to test for APTs effectively.

APTs are cybersecurity threats designed to hide inside, but not disrupt, the host network and relay information back to their creators. Unlike phishing, APTs are highly sophisticated and subtle, capable of acquiring not only discrete data, but also penetrating proprietary and copyrighted software; the successful creation of APTs requires extensive knowledge of cybersecurity protocols, procedures and routines. The APT label is only given to long-term infiltrations that usually remain undiscovered until their mission is complete, that is, all the captured information is transmitted to the APT owner or enterprise operations are completely disrupted.¹

Network administrators acknowledge the ability of an APT to hide and protect itself from being discovered. Auditors have responded to the threat by requiring detailed policies and procedures and constant system monitoring. Creative network testing must be added to find these well-crafted APTs. Careful restoration to the production state after an unusual resource shortage can cause an APT to reactivate despite the direct supervision of the network administrator and internal audit team.

To build a proactive defense against APTs, the internal auditor must aid network administrators in conveying the following critical message to business managers: Internally testing a working network and causing temporary reduction of performance and possible temporary disruption of employee resources may be necessary to avoid larger disruptions.

Benefits to Reduced Productivity

Although management generally objects to activities that reduce the organization’s productivity, sometimes the benefits are worth the costs. For example, scheduled fire drills cause productivity to drop to nothing, but the cost is negligible when compared to the possible loss of life during an actual fire.

Network administrators routinely back up entire networks and, when necessary, restore single files at the request of data owners. These normal procedures help protect the data held within the computer network. However, when was the last time a single drive was completely reformatted to see if only the known files were installed or if unauthorized access had been granted to the entire drive? When was the last time the network administrator required every employee to turn off their computer for several minutes during the workday? Since network administrators are often

---

¹ Healthy Network Testing to Identify APTs

Timothy Neuman, CISA, CIA
Has more than 20 years of information systems auditing and consulting experience. As a senior local county governmental auditor and South University (Savannah, Georgia, USA) adjunct professor, he utilizes the latest information system tools to evaluate, analyze and instruct the citizens of the Savannah area.
rewarded for keeping the computer systems available and working, they have no incentive to change the availability of the networks or to request approval for work stoppages during business hours. Their success in these areas means management cannot compare the benefits of temporary stoppages against the costs of a major loss of data.

APTs are built to withstand the normal low-volume tests and planned disaster or other restoration processes. Even properly planned and executed standardized audit testing can be completed without incident.

Internal auditors have been challenged to "have a solid understanding and awareness of more than just general and application controls." As auditors, "We keep earning our seat at the table, by building collaborative relationships." Working in collaboration with the network administrator, the internal auditor can provide management with more effective proactive measures. When conducting unusual tests, there are some suggestions to keep in mind.

Mandatory Live Testing

Testing of any healthy network should be conducted by qualified personnel. Internal auditors with a Certified Information Systems Auditor® (CISA®) designation are highly recommended to understand the implications of the results. There are several steps that provide a safe testing environment.

Step 1
The careful shutdown of a healthy network begins by understanding the resources utilized by the known applications that execute on each network segment. Using the Cybersecurity: Based on the NIST

Cybersecurity Framework audit program, the internal auditor can evaluate the established security controls. Network administrators can use the results to update network policies and procedures. Then, management can understand the importance of controls established within the network.

Step 2
Useful network logging systems should be utilized. Network administrators use various logging techniques to monitor the network's performance, and internal auditors use specific automated data analytical tools that emphasize data protection. The resulting teamwork can provide an efficient and effective foundation for detecting unauthorized system information changes.

Step 3
The live test can now be conducted. Because the network administrators and auditors determine the timing and the testing methodology (not the situation or management requirements), the servers, network equipment and segmented network resources can be specifically tested for hidden APTs. While the recommendation is not that department managers and employees should not be informed, the key to the live test is that management does not control any part of the process development.

The tests outlined in figure 1, while not a comprehensive list, are designed to encourage discussions between network administrators and the internal auditor.

The collaboration between the internal auditor and the computer network administrator will further protect network resources.

Step 4
Adopt a policy to continue to repeat these scenario types. Since APTs have not changed their overall strategy of seeking information and disrupting daily operations, the internal auditor does not need to significantly change testing methodologies. While more resources will be spent by the specific network administration, the general control risk and internal auditing skills developed by each testing process will increase the efficiency and effectiveness of the internal auditors.
Conclusion

APTs live inside externally connected networks. Internal auditors and network administrators can work as a team to perform healthy network disruptions during normal business hours. Forcing an APT to reinfect or regain required network resources—under the control and awareness of a cybersecurity auditor—can be an effective strategy to controlling the effects of an APT.

Endnotes


