Quick Reference Guide

Insider Threat

This quick reference guide shows key best practices for mitigating insider threats.

Physical Security

Hire a professional security team, ideally former military people, who will strictly follow your security instructions. They should prevent suspicious people from entering areas with critical IT objects (such as server rooms or rooms with switch racks). Have them inspect everyone at the entrance for IT devices and document any they find. Instruct everyone to disable their cell phone cameras while they are in the facility. When employees leave your facility, hard format all their flash drives and hard disk drives (HDDs).

Security Software and Appliances

Deploy and properly configure the following software: Active Directory, Endpoint protection system, Intrusion prevention system, Intrusion detection system, Web filter, Traffic monitoring software, Spam filter, Privileged access management system, Encryption software, Password management policy and system with at least two-factor authentication, Call manager, Data leakage protection system. Enable mailbox journaling on your exchange server, preferably with E-discovery software installed.

Wireless/Mobile Security

Deploy and properly configure wireless intrusion detection and prevention systems as well as a mobile data interception system.

Network Security

Configure your firewall properly: Blacklist all hosts and ports, and then white list only those you need. Configure a DMZ. Do not implement VPN or FTP; ensure that no critical systems interface directly with the internet.

Surveillance

Monitor all critical facilities in your company by video cameras. Enable session screen capturing on all critical servers.

IT Security Trainings

Train and test your employees against social engineering regularly. Perform your own phishing attacks on their mailboxes or make social engineering attacks by phone, and provide additional training for anyone who doesn't pass these tests.

Documentation, Policies and Procedures

Every security software solution and appliance must have its own management policy and configuration documentation. Work hard with your HR to create policies about almost every employee interaction with IT environment. You should establish an incident response policy, a third-party access policy, a user management policy, a user monitoring policy and so on. All these policies must be verified by your legal department and signed by your CEO. It is very important to document what actions will be taken and what penalties will be applied if these policies are violated and your investigation identifies the culprit.

Recycling

Before discarding or recycling a disk drive, completely erase all information from it and ensure the data is no longer recoverable. Moreover, old hard disks and other IT devices that contained critical information should be physically destroyed; assign a specific IT engineer to personally control this process.

Log Storage and Visibility

Keep all your device logs for up to 10 years to enable incidents investigation and ensure historical evidence is easily accessible. Implement log management and change auditing software that deliver enterprise-wide visibility. Monitor and document every critical change made to your IT environment.

Archiving, Backup and Disaster Recovery

Implement and configure file and mailbox archiving. Implement and configure a backup system and create a backup policy that includes a full backup at least every month. Also establish and test a disaster recovery plan.

Alerting

Configure alerting on all critical systems and events. Ensure the alerts warn you through multiple channels.

Corporate Headquarters:
300 Center Drive, Suite 1100, Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social