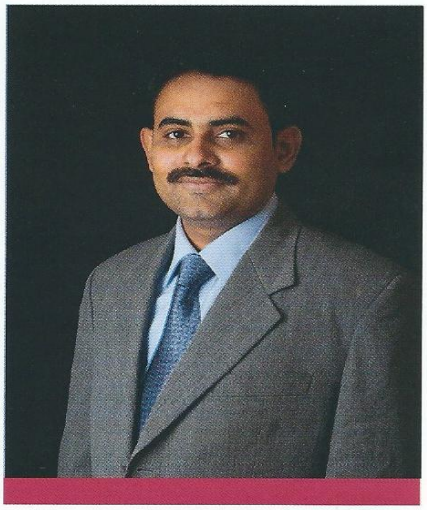
MY VIEWS

GRABBING THE CYBER THUGS BY HORNS

Organizations of all types and sizes face the tough challenge of ensuring information security and data integrity. V Balasubramanian, Marketing Manager, IT Security, ManageEngine shares his expert opinions on how to combat the increasing threats and watch out for the cyber thugs.



V BALASUBRAMANIAN,
MARKETING MANAGER, IT SECURITY, MANAGEENGINE

ENTERPRISE READINESS FOR BATTLING THE EVOLVING THREATS

An analysis of some of the recent high-profile security breaches reveals that the threat landscape is rapidly evolving with Advanced Persistent Threats (APT) leading the way. Though there are numerous loopholes, inadequate access controls and internal security measures, improper password management and lack of monitoring and log reviews are found to be causing the majority of cyber attacks.

The hackers' predominant activities include spreading malware infections, siphoning of login credentials and denial of service attacks that disrupt service to legitimate users. The traditional security attack channels include viruses, keylogger trojans and cross-site scripting. Perimeter security software and traffic analysis solutions help in combating traditional attack vectors.

However, hackers have changed their modus operandi in recent times. Cyber-criminals are now siphoning off login credentials of employees and administrative passwords of IT resources, using techniques that include spam and phishing emails, keystroke loggers, and Remote Access Trojans (RAT).

Majority of the attacks on IT infrastructure (on-premises and cloud infrastructure) are centered on brute force attacks on administrative credentials. Hackers always set their eyes firmly on the Keys to the Kingdom – the administrative credentials for control panel/management console and employee credentials.

Once the login credentials of an employee or an administrative password of a sensitive IT resource is compromised, the institution will become a paradise for the hacker. The criminal is then able to initiate unauthorized wire transfers, view the transactions of customers, download customer information, erase details or carry out sabotage.

The situation becomes much graver if a stolen password has also been used to access a variety of applications and websites. Nowadays, it is quite common for employees to use the same login credentials for multiple sites – social media, banking, brokerage and other business accounts. If the password gets exposed in any of the sites, in all probability, hackers would be able to easily gain access to all your other accounts too.

Insider Threats – Another Top Concern

As things stand today, the biggest threat to the information security of your enterprise might be germinating inside, right at your organization! The business and reputation of some of the world's mightiest organizations have been shattered in the past by a handful of malicious insiders, including disgruntled staff, greedy techies and sacked employees.

Administrative passwords, system default accounts and hard-coded credentials in scripts and applications have all found themselves in the cyber criminal's sights. Lack of internal controls, access restrictions, centralized management, accountability, strong policies and to cap it all, haphazard style of privileged password storage and management makes the organization a paradise for malicious insiders.

How ManageEngine helps combat?

Combating sophisticated cyber-attacks demands a multi-pronged strategy incorporating a complex set of activities. As outlined earlier, important combat measures include deploying security devices, enforcing security policies, controlling access to resources, monitoring events, analyzing logs, detecting vulnerabilities, managing patches, tracking changes, meeting compliance regulations, monitoring traffic and more.

Especially, privileged access should be not just centrally controlled, but also closely and continuously monitored.

Emerging trends like mobility, virtualization and cloud adoption have certainly complicated IT security. But, organizations can easily overcome the issues by ensuring the basic controls. ManageEngine's IT security solutions precisely help organizations in this aspect.