Threat, Threat Everywhere; Cyber-Criminals on the Prowl

Combating Cyber Security Threats

V Balasubramanian,
ManageEngine

Abstract

Of late, cyber-criminal activities across the globe have assumed such grave proportions that all enterprises - big and small, are exposed to security breaches and identity thefts of various kinds. Many sabotage were found to have been caused by the insiders of the enterprises - either disgruntled staff or greedy techies or sacked employees. As stolen identities seem to have served as the 'hacking channel' for many cyber-crimes, improper management of the administrative passwords is believed to be at the root of a good number of security threats. This paper discusses the causes of security incidents in detail and suggests ways to effectively tackle the challenge.

Contents

Increasing Cyber Security Attacks – The Challenge

If Samuel Taylor Coleridge were alive today, he would have probably rephrased his immortal lines 'Water, water everywhere, ne any drop to drink' as 'Threat, Threat Everywhere, Cyber criminals on the prowl'! Of late, cyber-criminal activities across the globe have assumed such grave proportions that all organizations - big and small, are exposed to security breaches and identity thefts.

Let us take a quick look at some of the major cyber-crimes happened recently:

- A trader allegedly stole the passwords of IT operators of a reputed European Financial Services Company and racked up a mountain of fraudulent trades that created financial loss to the tune of $ 7 billion to the company. This incident is considered one of the largest cyber-frauds in the history.

- In San Francisco, a disgruntled network administrator allegedly planted network devices that enabled illegal remote access to the Fiber Optic Wide Area Network and eventually changed the passwords of servers and devices. He refused to hand over the new passwords to the IT administrators. As a result, other staff of the organization could not access the network, not to mention the financial loss that stemmed from the episode

- A cyber-mafia hacked the network of an international hotel chain, used the credentials of an employee and reportedly hacked the personal data of millions of customers of the hotel chain. The stolen data includes addresses, telephone numbers, credit card details, and places of employment

- The employee of a hugely popular social networking site was using the same password for many of his online accounts. It came in handy for a hacker, who got hold of the password, gained access to the network of the social networking site and released their sensitive business documents publicly

- The personal information of about a half-a-million residents in Germany was freely viewed on the internet due to an exposed password

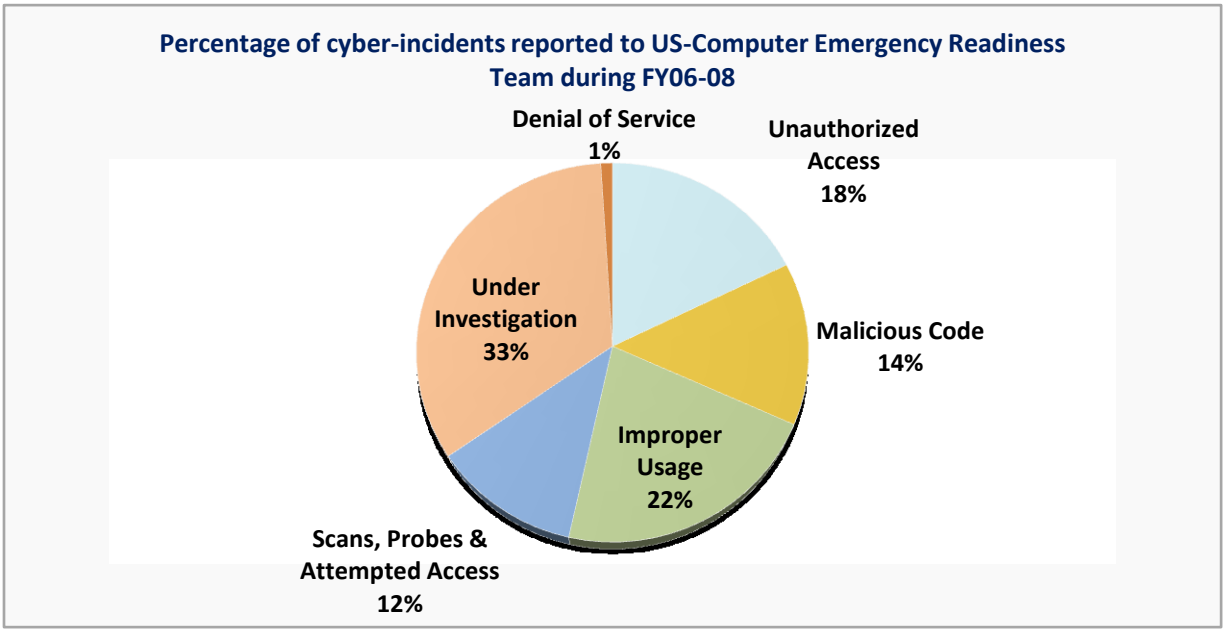
- A former Network Engineer of a health clinic in San Diego was sentenced to 63 months of imprisonment for intentionally damaging the protected computers by disabling the automatic backup database containing patient information

- The identity theft from a reputed discounts stores chain in USA and Canada reportedly made hackers to gain access to customer information related to at least 45.7 million credit and debit cards

The list of cyber-crimes and security incidents will go on and on and will fill volumes, if one were to point out all. Still worse, a good number of security incidents are not revealed for fear loss of reputation. The above list however gives an indication of the magnitude of the problem. It also indicates that:

- Businesses of all types – financial firms, healthcare institutions, federal agencies, service organizations, hospitality sector, educational institutions, hi-tech enterprises – and all sizes are impacted
- Establishment of intrusion detection systems and other security infrastructure alone could not effectively combat security incidents
- In many incidents, disgruntled insiders had acted with malicious intent and caused the damage
- By and large, the perpetrators have stolen the digital identities of others to creep in to the network and wreak havoc
- The security incidents have resulted in huge financial loss and damage of reputation to the enterprises

In many incidents, disgruntled insiders had acted with malicious intent and caused the damage. By and large, the perpetrators have stolen the digital identities of others to creep in to the network and wreak havoc.



Source: United States Government Accountability Office Study, May, 5, 2009

Security Incidents - Causes

Past trends show that the exact cause of most of the security incidents goes unreported. Of course, there have been instances where the culprits had been brought to book and their modus-operandi revealed to the outer world. But, the fact remains that exact cause of most of the incidents remains a secret, unfortunately.

Traditionally, keylogger trojans (which monitors keystrokes, logs them to a file and sends them to remote attackers), cross-site scripting (which enables malicious attackers to inject client-side script into web pages viewed by other users and exploit the information to bypass access controls) and viruses have mostly acted as the security attack channels.

However, of late, as stolen identities seem to have served as the 'hacking channel' for most of the cyber-criminals, analysts generally believe that improper management of the Administrative Passwords, which are often aptly referred as 'Keys to the Kingdom', is at the root of many security threats.

Another harsh fact is that many a sabotage had been caused by the insiders of the enterprises. Either disgruntled staff or greedy techies or sacked employees were involved in many of the security incidents. That means, in this hi-tech era, breach of trust could occur anywhere, anytime leading to serious consequences. Quite often, lack of well-defined internal controls and access restrictions pave the way for security incidents.

Of late, as stolen identities seem to have served as the 'hacking channel' for most of the cyber-criminals, analysts generally believe that improper management of the Administrative Passwords, which are often aptly referred as 'Keys to the Kingdom', is at the root of many security threats.

Administrative Passwords – Scenario Today

Before analyzing the causes further, let us dwell on the current scenario. How administrative passwords are being handled in enterprises?

If truth be told, even many big enterprises do not have any effective password management system in place at all. Employees follow their own, haphazard way of maintaining the passwords; there is rarely any meaningful management.

- Sensitive passwords are stored in volatile sources such as text files, spread sheets, print-outs etc.,

- Many copies of the administrative passwords are circulated among the administrators who require them for their job functions. The passwords thus become impersonal in the shared environment – no accountability for actions
- When other members of the organization such as developers, database administrators and support personnel require access to IT resources, passwords are generally transmitted over word of mouth
- The administrative passwords mostly remain unchanged for fear of inviting system lockout issues
- Still worse, most resources are assigned the same, non-unique password for ease of coordination among administrators
- There is rarely any internal control on password access or usage. Administrators freely get access to the passwords of all the resources in the organization
- There is generally no trace on 'who' accessed 'what' resources and 'when'. This creates lack of accountability for actions
- If an administrator leaves the organization, it is quite possible that he/she may be getting out with a copy of all the passwords

From the foregoing, it is clear that the haphazard style of password management makes the enterprise a paradise for hackers – internal or external.

The haphazard style of password management makes the enterprise a paradise for hackers – internal or external. Unfortunately, enterprises generally do not tend to attach importance to this crucial aspect of administrative password management until a security incident or identity breach rocks the enterprise. This negligence often proves costly.

Unfortunately, enterprises generally do not tend to attach importance to this crucial aspect of administrative password management until a security incident or identity breach rocks the enterprise. This negligence often proves costly.

Many security breaches like the ones discussed above might have stemmed from lack of adequate password management policies and internal controls. Analysts strongly believe that most of the security incidents are actually avoidable by placing access restrictions and well-defined password policies.

The Solution

Take preventive action, safeguard your data

With cyber-threats looming large, enterprises should think of taking preventive action by strengthening internal controls. Manual processes and home-grown tools may not be able to provide the desired level of security and controls.

It is pertinent to quote here a recent research report by Gartner:

"Manual procedures for managing shared account passwords can be intrusive, interrupting normal operations and unacceptably delaying the resolution of problems. These procedures can also be fragile, failing to consistently deliver the desired level of control and accountability and exposing organizations to insider threats."

*(**Source:** Gartner, Inc., "MarketScope for Shared-Account/Software-Account Password Management", Ant Allan, Perry Carpenter, 16 June 2009).*

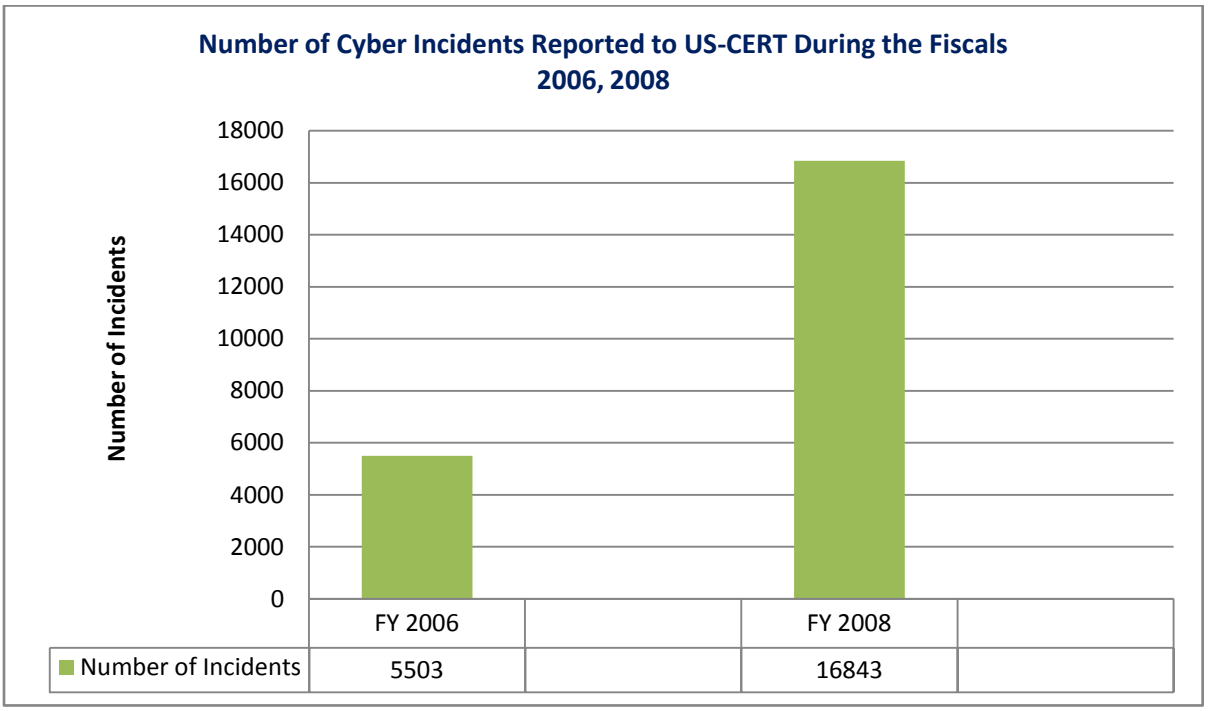
One of the effective ways to achieve internal controls is to deploy a Privileged Password Management Solution that could replace manual processes and help achieve highest level of security for the data.

One of the effective ways to achieve internal controls is to deploy a Privileged Password Management Solution that could replace manual processes and help achieve highest level of security for the data.

Privileged Password Managers help enterprises safeguard their data and thereby avoid security incidents in multiple ways than one:

- Administrative passwords can be stored in a centralized repository in encrypted form – this helps avoid storing of the passwords in volatile resources. Even if someone manages to get hold of the password database, data cannot be deciphered
- Role-based, granular access restrictions can be enforced – administrators and other users get access only to the passwords that are allotted to them, not all passwords
- Passwords can be selectively shared with others on need basis - sharing passwords by word of mouth completely avoided
- Passwords can be automatically changed at periodic intervals assigning a strong, unique password to each resource – hackers cannot make wild guesses
- For enhanced internal controls, administrators / users may even be prevented from viewing the passwords in plain text. Instead, they could be directed to just click a URL to directly access the resource

- Users requiring temporary access to the passwords can be directed to follow password request-release workflow granting time-limited access. After revoking the permission, passwords can be automatically reset – this prevents users getting access to the passwords that are no longer required for them
- All password access activities are completely audited – this helps monitor the usage of privileged identities and fix accountability issues when something goes wrong. It also helps the enterprise meet regulatory compliance requirements
- Real-time alerts on password actions help administrators continuously track and control the administrative passwords
- If an administrator leaves the organization, passwords owned / accessed by them can be transferred to some other administrator and the passwords could be automatically reset – this helps avoid possible misuse of the passwords by disgruntled users



Source: United States Government Accountability Office Study, May, 5, 2009

Researchers repeatedly point out that identity theft incidents are on the rise and it will only keep growing due to many reasons, including economic situation, social factors and technological advancements that make the tech-savvy criminals more creative every passing day.

Not all security incidents could be prevented or avoided; nor could privileged password management software act as the panacea for all cyber security incidents. But, the security incidents that happen due to lack of effective internal controls are indeed preventable. Enterprises should take preventive action to combat cyber-criminals. Otherwise, enterprises might end up locking the stable after the horse has bolted!

Introducing ManageEngine Password Manager Pro

Password Manager Pro (PMP) is a web-based, secure vault for storing and managing shared sensitive information such as passwords, documents and digital identities of enterprises. It helps control the access to shared administrative passwords of any 'enterprise resource' such as servers, databases, network devices, applications etc. PMP enables IT managers to enforce standard password management practices. For more details, visit *http://www.passwordmanagerpro.com*

ManageEngine

A Division of ZOHO Corp. (formerly AdventNet Inc.)

Phone: +1 - 925 - 924 - 9500 **Website:** http://www.passwordmanagerpro.com

For Queries: passwordmanagerpro -support@manageengine.com