ManageEngine Password Manager Pro

WikiLeaks-type security incidents can be prevented with Privileged Identity and Information Management Solutions!

White Paper

V Balasubramanian, ZOHO Corp.
www.passwordmanagerpro.com

Abstract

WikiLeaks - the global buzzword today is a rude shock to many, big surprise to some, huge disappointment to a few and a great fun for others. The motive, effects and ramifications aside, WikiLeaks-type exposures perhaps represent the biggest information security threat to Government agencies. Lack of well-defined access control policies and enforcement mechanism potentially lie at the root of security issues like this. Malicious insiders seem to be causing this harm by either illegally accessing the documents or giving credentials to too many un-vetted people who then route them to WikiLeaks or, in fact, any other media outlet. In the backdrop of the WikiLeaks exposures, this paper analyzes the various dimensions of information security, the causes for tight security policies, the need for controlling privileged access and the strategies to mitigate the threats.

Contents

WikiLeaks-type security incidents – The challenge

Media worldwide are now agog about the WikiLeaks episode. A good part of the coverage revolves on 'what', 'why', 'who', 'where' 'when' and 'how' of the WikiLeaks story.

While a lot of research is going on to find the real motive of an Army Intelligence Analyst and WikiLeaks in exposing various secrets, there is one fact that is crystal clear in this murky sequence of events: Malicious insiders in Government agencies are causing this harm by either illegally accessing the documents or giving credentials to too many un-vetted people who then route them to WikiLeaks or, in fact, any other media outlet.

In the most recent controversy involving the publishing of a cache of 220 of the US diplomatic documents, Bradley Manning, a 22 year old Army Intelligence Analyst stationed at Iraq, is believed to have leaked the classified documents to WikiLeaks.

Ever since the arrest of Manning, a hot discussion is going on as to how he got access to those sensitive data. In a private chat with former hacker Adrian Lamo, Manning supposedly confessed that the leaking was possible due to the lack of information security measures. Lamo supplied the chat transcriptions to Wired.com and the FBI.

Manning reportedly had access to two classified networks owned by the Department of Defense and the State Department, and the Joint Worldwide Intelligence Communications System respectively. *"I would come in with music on a CD-RW labeled with something like 'Lady Gaga,' erase the music then write a compressed split file. No one suspected a thing and, odds are, they never will,"* writes Manning to Lamo.

This gives rise to a fundamental question on the whole episode – how did Manning manage to gain access to the sensitive networks? That is where the problem starts!

Manning's exact modus-operandi is not yet fully known. However, we can categorically assume that he should not have had the access to all those networks from which he had siphoned off the sensitive data. Without any genuine need or necessity, he had access to varied networks. This leads to the inference that lack of well-defined access control policies and enforcement mechanism potentially lie at the root of security issues like this.

As government agencies, military and other federal departments are increasingly leveraging the power of information technology to manage their activities and offer various services, information security has become the top concern. The WikiLeaks episode has once again proved that effectively securing sensitive data has emerged a big challenge for government agencies.

Nowadays, the concepts of 'work-from-home' and 'tele-commuting' are being increasingly adopted in Government agencies. This has resulted in proliferation in the usage of laptops and storage devices such as memory sticks. When data resides in these devices, it becomes cumbersome to ensure information security. It could very easily get into the hands of malicious users.

It is cruel to throw a passing comment that many insiders act with malicious intent - only a miniscule number do. But, through improper and insecure handling of sensitive data, well-intending users create room for security incidents.

The effect of cyber-threats to private establishments may be limited to financial and reputation loss. Perhaps, it could be greater in the case of corporate or industrial espionage, but security incidents in government agencies might jeopardize even National Security. The political ramifications of the WikiLeaks transcend international boundaries and political analysts believe that these types of exposures pose the biggest threat to National Security.

Nevertheless, just as private establishments, government agencies are also tasked with building up public trust through integrity and confidentiality of information while serving the citizens.

A recent study by Computer Emergency Response Team (CERT) states:

"The number of cases of insider IT sabotage in the IT sector is quite striking. The government sector is second in number of insider IT sabotage attacks"

-- Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1, Dawn Cappelli, Andrew Moore, Randall Trzeciak and Timothy J. Shimeall, CERT, Carnegie Mellon University.

As a result, there is a greater sense of caution and necessity among the government establishments at all levels to protect sensitive information and secure their IT infrastructure. As government agencies embrace new technologies, newer threats keep pace. Adoption of cloud computing and virtualization has made enterprise security all the more difficult and highly important.

In the backdrop of the WikiLeaks exposures, it is pertinent to analyze the various dimensions of information security, the causes for tight security policies, the need for access control and the strategies to mitigate the threats.

Let us begin from the basics - Achieving the highest level of information security is the obvious goal for enterprise and government agencies. But, this goal is fraught with two main challenges:

External Attacks - Organizations come into contact with a variety of people in a variety of ways. Sensitive information and IT resources need to be exposed or shared with other departments, agencies and citizens. A large number of employees are required to access sensitive data and an ever increasing number of citizens turn to information technology to access business or government services.

Transparency in transactions being the hallmark of government functioning, many details are required to be exposed to the public. Government agencies, by their very nature, deal with an enormous amount of sensitive data/information. All these make the Government establishments vulnerable to data breaches and cyber-attacks from amateur and expert hackers.

Analysis by IT security experts reveals that unauthorized access to IT resources by malicious insiders is the fastest growing security threat for government agencies. And, the insider threat is growing at unprecedented rates....

Internal Threats - Threat to information security does not always stem from outside. It could well be generating right inside the organization. Disgruntled staff, naïve or greedy employees, tech-savvy contractors and sacked employees could act with malicious intent and misuse privileged access. The business and reputation of some of the world's mightiest organizations, including many government agencies have been shattered in the past by a handful of malicious insiders.

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 external security attack channels.

However, of late, internal threats seem to be far more alarming and prevalent as many of the reported security incidents have been caused by malicious insiders having authorized or unauthorized privileged access to the enterprise and government IT resources. Malicious

insiders can potentially misuse the privileged access to IT resources and wreak havoc by stealing, manipulating and destroying sensitive data.

In fact, analysis by IT security experts reveals that unauthorized access to IT resources by malicious insiders is the fastest growing security threat. And, the insider threat is growing at unprecedented rates.

While security devices, intrusion detection solutions and other applications help combat the external threats, effectively mitigating insider threats is a huge challenge and mandates a multi-pronged strategy. Before discussing the ways to combat insider threats in government agencies, it is worthwhile to delve into the causes.

How do internal threats develop?

In many of the reported cyber-sabotages, misuse of privileged access to critical IT infrastructure and stolen identities have served as the 'hacking channel' for the malicious insiders to wreak havoc on the confidentiality, integrity and availability of the organization's information systems.

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.

Privileged passwords are aptly called as 'keys to the kingdom' as they enable the users to get virtually unlimited access and full controls to the IT resources such as servers, databases, network devices and IT applications. Those who login through the privileged mode could access absolutely anything with ease.

Typically, government agencies have thousands of privileged passwords, majority of which are used in shared environment. That means, a group of administrators use the common privileged account to access the resource. In reality, the passwords are just left open to be managed by the group.

It is increasingly becoming clear that improper management of the privileged passwords could potentially remain at the root of a good number of security threats

The privileged accounts are accessible to all the members of a team. The 'shared' nature grants anonymity, which enables misuse without a trace and as a result, privileged passwords remain virtually in utter disorder.

It is increasingly becoming clear that improper management of the privileged/administrative passwords could potentially remain at the root of a good number of security threats. In fact, a recent analysis by experts reveals that more than **80 per cent of the internal attacks had stemmed from people having access to privileged identities.**

80 per cent of the internal attacks had stemmed from people having access to privileged identities

- Sensitive passwords are stored in volatile sources such as text files, spread sheets, print-outs, home-grown tools or even in physical vaults. Many copies of the administrative passwords are circulated among the administrators. If the text file or spreadsheet containing the shared administrative passwords reaches the hands of a malicious user, data security would be thrown to winds

- 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. It is not uncommon to see UNIX administration team having full access to the Windows passwords, developers having full access to database passwords and so on

- The passwords remain impersonal in the shared environment. Mistakes – accidental or intentional, could never be traced to individuals. There is generally no trace on 'who' accessed 'what' resources and 'when'. This creates lack of accountability for actions

- When other members of the government agency such as developers, database administrators, support personnel and contractors require access to privileged passwords purely on a temporary basis, they are supplied with the required passwords mostly orally or through emails. There is no process to revoke temporary access and reset the password after the temporary usage, which leaves a big security hole

- Given the complex nature of sharing, it would be cumbersome to find who has access to what resources. When someone leaves the organization, changing all the privileged passwords of the enterprise is the only solution to rule out any possible access or intrusion by that person in future.

- The administrative passwords mostly remain unchanged for fear of inviting system lockout issues. Manually changing the passwords of thousands of resources would demand 'man-years' to complete the task

- Still worse, most resources are assigned the same, non-unique password for ease of coordination among administrators

- If an administrator leaves the organization, it is quite possible that he/she may be getting out with a copy of all the passwords

- In worst cases, if an administrator leaves without revealing a privileged password that was changed by him, the device/application might remain locked out for a prolonged period

- Apart from privileged passwords, there are the 'Application-to-Application' Passwords that are hard-coded in scripts. These hard-coded passwords pose a significant security threat as malicious users getting access to the script could easily decipher the password and unleash disaster

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.

Thus, administrative passwords are insecurely shared and lie scattered in the organization leaving little scope for any internal controls. The haphazard style of password management makes the organization a paradise for hackers – internal or external. Many security incidents and data breaches might actually stem from lack of adequate password management policies and strict internal controls.

Internal security need not be compromised!

Not all security incidents and data breaches could be prevented or avoided; But, the ones that happen due to lack of effective internal controls are indeed preventable.

Combating the sophisticated insider threats in government agencies mandates preventive steps and a multi-pronged strategy - controlling access to resources, enforcing security

policies, adhering to best practices, monitoring events for real-time situational awareness, recording user sessions, detecting vulnerabilities, tracking changes, ensuring compliance to regulations, analyzing actions, automated user provisioning and de-provisioning and a host of other activities.

It is pertinent to quote here one of the best practice approaches suggested by CERT. Advocating the implementation of strict password and account management practices, CERT states:

"No matter how vigilant an organization is in trying to prevent insider attacks, if their computer accounts can be compromised, insiders have an opportunity to circumvent both manual and automated controls. Password and account management policies and practices should apply to employees, contractors, and business partners. They should ensure that all activity from any account is attributable to the person who performed it."

One of the effective ways to mitigate insider threats is to automate the entire life cycle of Privileged Access Management enforcing best practices. **Privileged Identity and Information Management (PIIM) solutions** act as the alternative for the traditional, inefficient and insecure password management processes. They provide an automated, policy-driven solution for shared administrative password management and help achieve high level of security for the data.

PIIM solutions, also called as Privileged Password Management Solutions help organizations safeguard their data and thereby avoid security incidents in multiple ways:

One of the effective ways to mitigate insider threats is to automate the entire life cycle of Privileged Access Management enforcing best practices.

- 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
- Sensitive documents, videos and other digital data could be securely vaulted just like passwords
- Role-based, granular access restrictions can be enforced – administrators and other users get access only to the passwords/documents that are allotted to them, not all. Since the access to the password itself is controlled, malicious insiders will not get a chance to access

- Passwords/documents can be selectively shared with others on need basis - sharing passwords by word of mouth or through emails completely avoided

- Passwords can be automatically changed at periodic intervals assigning a strong, unique password to each resource – insiders cannot make intelligent 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 government agency meet regulatory compliance requirements such as SOX, HIPAA etc.

*In addition to deploying a PIIM Solution, it is worthwhile to leverage other data security solutions such as **Data Loss Prevention (DLP) software** that could go beyond access restriction into monitoring what users do with the access. **Session recording and playback** can also be leveraged*

- Real-time alerts on password actions help administrators continuously track and control the administrative passwords. In addition, SNMP Traps and/or Syslog messages can be raised to the management systems on the occurrence of various password actions and audit events. The traps/syslog messages can be sent to any **Security Information and Event Management (SIEM)** tool, which can thoroughly analyze these events, correlate them with other network events and provide informative, holistic insights on the overall network activity

- If an administrator leaves the organization, passwords owned / accessed by him 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

In addition to deploying a Privileged Identity and Information Management Solution, it is worthwhile to leverage other data security solutions such as **Data Loss Prevention (DLP)**

software that could go beyond access restriction into monitoring what users do with the access. Session recording and playback can also be leveraged to keep track of user activities. This will be particularly helpful in scenarios where tele-commuting and information storage on memory sticks and CDs are permitted.

If you are looking for a solution to bolster the security of your IT infrastructure and in turn, protect the critical data, ManageEngine Password Manager Pro would be the ideal choice. 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.

In Summary

Researchers repeatedly point out that insider threats and 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. Analysts opine that during the past six months, security incidents in key networks in Government agencies have nearly doubled.

Achieving data security is indeed a continuous journey, in which preventive measures that offer comprehensive protection take precedence. WikiLeaks is an eye opener - taking preventive action is the need of the hour. Use Password Manager Pro and Stay Secure!

ManageEngine

Website: www.passwordmanagerpro.com | **Tech Support:** passwordmanagerpro-support@manageengine.com
Phone: +1 925 924 9500 | **Contact:** eric.wegner@zohocorp.com