International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-1, Issue-1, May 2015 Pages 16-21

The Insider Threats

Marwan Albahar

Abstract— **This paper is aimed at discussing on how the so called privileged users place the important data at a risk. Also, this paper will handle issues to do with how data in some organizations are violated by intrinsic users via malicious actions. In this respect, this paper will shed light on three dimensions in which sensitive information can be protected. To start with, how can one restrict the degree of access to the sensitive info even if the user is logged in with strong accounts for instance administrator's access? How can organizations set rules to safeguard sensitive data plus implement new technologies on the same? And lastly, what is the process and order needed for mitigation in case of leakage in data?**

Let's start by limiting the access of the users even when logged in with the administrator accounts which are the most powerful; in order to have a high level of data security, creating an account with least privileges will be a good move in respect to data security. More so, it is good to examine the actions of the privileged user's action and the risk that they might cause.

Also, it is good to implement the best technology that will ensure that the data of a certain organization is not pruned to any form of internal risk. This guarantees the organization of safety of information from the intrinsic side. To start with, the most effective way to reduce the risk of sensitive data is by applying data-centric security; i.e. the manner in which data-centric security is employed plus the presented authorization procedure. This should be followed by the establishment of the firewall as the second procedure in the process of authorization and authentication. The firewall building and the huge of implementation are aimed at time-wastage reduction.

Index Terms—**Threats, Access Control, Governing Policies.**

I. Introduction

Begin with the definition of privileged user; the privileged user is a unique role within an organization. They are granted the right to access systems on which sensitive applications and information are found on the condition that they know and abide by all corporate governing policies. However, many people are disturbed by the security of sensitive information, the hiking value of data plus the number of coupled privileged users in the organization who are likely to increase the difficult to maintain this data without compromising with its integrity.

In the year 2013 July, the breach in database in the case referred to as Wikileaks led to the signing of the executive order that was aimed at countering the insider threat by the US president Barrack Obama. In this case, Pfc. Bradley Manning an army private was convicted for leaking the biggest cache of classified info in American history. It is an open secret that concerns of the integrity of information within an organization from the insider's threat is among the fundamental threats in security as implored by several studies.

The year 2012 only recorded what is called insider-related fraud of 43%. With this, one can conclude that there is little security from the traditional approach on the integrity of the data. Monitoring tools, Internet, loosing data plus other conventional controls is failing to protect the sensitive info from the looming breaches in data that can largely be blamed on the insiders. The volumetric insider threat report (2013) that was carried out by ESG (Enterprise Strategy Group) demonstrated that about 54% of the experts in IT and security professionals are for the thought that the threat from insiders is more likely to go un-prevented or undetected in comparison with the case that was there by 2011.

It is worth noting that huge amounts of money are being spent in public sector to ensure the integrity of their data from the risk of external players, by doing so, they fail to remember that there is also a threat from within. It is till the data/info is compromised from within when the organization starts looking for the security solution over the same. To start with, the organization believes that insider don't pose a substantial threat as per se. Little did they understand that it is the one, which is the most dangerous?

II. The Principle of Least Privilege

Here, one might ask oneself of the importance of least privilege in management of essential info? It is worth noting that the administrator's user is the strongest account in the information system. This strength allows it to alter the configuration of the desktop, applications and installations. Therefore, it is worth noting that a slight error might lead to a risk for instance of compromising with the whole network or culminate to malicious attacks [1]. Users whose computers are attacked by worms, viruses and other malicious software enjoy the privilege from the security principle of "least privilege". Here, the lower the privilege the lesser the damage since the administrator user employs the non-administrator access to see the task accomplished. In this manner both the users and the hackers are restricted from installing or downloading anything from malicious USB Drives, web and the likes. It is worth noting that even if various users might use the administrator accounts, the data security is guaranteed when one runs a user account with least privileges [2].

Since the user account with low privileges is likely to cause lease alarm in comparison with the high privileged users, the non-administrator accounts are smarter than the administrator accounts in maintaining the privacy and integrity of sensitive data. This is more protective to data when it comes to host

Marwan Ali Albahar, Department of Computer Science, Frost Burg State University, Maryland, USA.

malware, internal and external security attacks, and intentional or accidental attacks on confidential data [2]. It's worth noting that when a certain worker logs in with an account of high privilege users, he can access, change and/or delete some data for instance names or social security numbers. It is worth noting that hackers are in a better position by accessing the data system from a high privilege user and hence alters it in a while.

II. SUCCESSFULLY IMPLEMENTATION OF THE PRINCIPLE OF LEAST PRIVILEGE

The main aim of this exercise to allow employees in a particular organization to access the info they need only with a view to do their job in a safe environment. In order to capitalize on how to successfully implement least privilege access, the following critical steps should be keenly followed:

1) Involvement of all stakeholders in defining privilege access levels

Here, one requires the approval of the company at hand plus make it understandable to them what you mean about levels of access and the question at hand. Therefore, it is advisable to involve all the stakeholders. If the whole system in the organization will call for representatives from department for instance marketing, human resource, finance and other dockets to be incorporated, then they will be in a position to elect who will require access to the sensitive info within the departments. This is more efficient and effective than what is referred to as IT "Blindly" doling out access [3].

2) Take a role based approach

If it is possible, assigning roles instead of allocating individuals are more controllable and easy to maintain privilege access from an operational angle. Users are not likely to gain additional entry to the confidential data with time since revoking of the roles is much easier. It is more applicable especially in instances where employees are transferred within any particular organization [3].

3) Defining the review process

It is advisable to carry a review process on the whole system at least once annually. This will ensure that the access permissions / roles are still within the required standards of business and least privilege [3].

III. MONITORING AND LIMITING THE NUMBER OF PRIVILEGED USERS

The increasing trend toward a mobile workforce has also increased the potential for malicious use of mobile devices. Their cameras, microphones, mass storage, and communications capabilities could be used to capture and exfiltrate sensitive information. Organizations must be aware of potential risks posed by mobile application functionality that insiders could use maliciously. A multi-layered defense can include prohibiting personally owned devices, limiting remote access to critical data, limiting the number of privileged users with remote access, and using application gateways for non-organizational equipment. Organizations should more closely log and audit all remote transactions and ensure that remote access is disabled during employee termination

This entails narrowing down the responsibility to answer the question, who did what? The best way to deal with this case is installing a camera within the system. It is worth noting that privileged users must be monitored to avoid risks and damages on sensitive info being caused.

One of the practice that is highly impacted upon by in the reduction of the risk caused by the privileged users for instance as an alert suspect activity, block or audit a user, employing extra-caution, pinpointing unaccepted activities for instance alert data system, plus coming up with a weekly report on the security of the system.

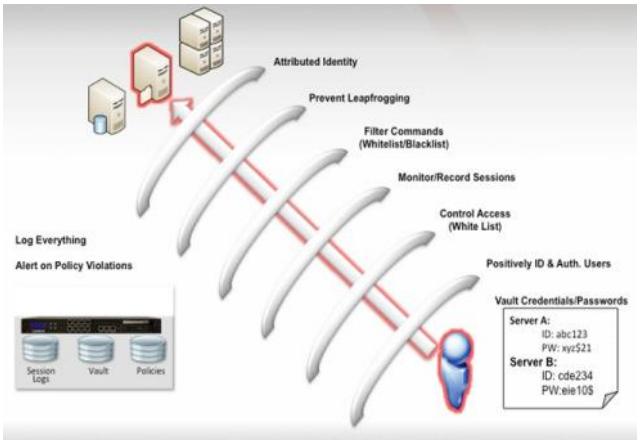

Figure 1: Privileged Access Control

Tracking Privileged User

Databases and files that can be accessed via privileged access including the audit user creation, local system access; newly granted privileges plus restrict usage of shared privileged accounts [4]. In order to track the activities of a privileged user, a staff in IT must ensure that:

a) He changes the administrator passwords in a periodic manner.
b) There is no generic, shared or group privileged passwords or accounts.
c) The rights to access of the data are confined to least privileges needed.
d) Privilege accounts that are inactive are disabled or removed in every three months.
e) For the cases of termination of a user, the privilege account is removed immediately.
f) All components of the system are protected by passwords security policy.

A. Alert or Block Suspect Activity

Here, one needs first to identify a behavior of a user that exceeds the normal pattern of access that is limited onto him/her, block or alert suspicious activities that might suggest breach by a privileged user. Users carrying out these activities should either have their privileges reviewed or else are revoked. More so, there is a necessity to audit the analytical tools and reports to support the forensic investigations [4].

B. Identify Unauthorized Privileges Changes

While changing data systems users or data objects from unauthorized user, a thorough investigation is required by the respective organization on the activity and how to control it. By controlling I mean coming up with a technology that will remedy the situation if it recurs in future.

More so, privileged users are not supposed to monitor since they might change the controls to hide their unauthorized activities [4].

IV. DATA CENTRIC SECURITY

This refers to a model of info security that aims at securing the data itself as opposed to applications, networks or other installation [5]. If one has the ability to preserve data and maintain its original form, examine and perceive the trait, aim and fundamentally the value embarked on that info, then you have the ability to preserve it through its lifecycles in a way that it will be shielded from malicious users whether from inside or outside the organization as Bower argues [6].

In this respect therefore, one can understand that with the data-centric security approach, organizations protect their very data itself as opposed to the network systems. Data encryption is therefore a good remedy where only the authorized users can access to data via decrypting it. To the users who are unauthorized, the data appears as something that is not legible and therefore can never decipher its codes [7].

A. Implementing Data Centric Security Model

Implementing an automatic data-centric security solution with strong encryption is the best way to reduce the risk on sensitive data. The administrative and encryption controls are maintained via the management policies. One has to consider the guidelines in which the sets of data will be handled before employing the approach of data-centric model. These are as per the basis of the organizational policies. Another important factor to put into consideration is the ability to insert key a contingency for access to the code data by the officials in charge of security to monitor or in case the employee ceases to member a member of the organization. In an environment governed by the federal government, the FIPS (Federal Information Processing Standards) offers a framework standards and guidance for securing sensitive info. FIPS 140-2 authorizes the use of renown AES 256 encryption, digital signing and digital certificates to ensure that all sensitive data is secured. All the employees in the federal systems are allocated a digital certificate that will be saved on their CAC or PIV card that characterizes the deployment of data-centric security methods supporting the digital certificates a fairly quick and easy procedure.

The checklist of functions and figures in an effective data-centric security solution entails:

- Securing file names, files, e-mail messages and attachments, their security format not withstanding via the use of strong encryption.
- Enable integration of computing platforms like Excel, word, outlook e.tc plus the desktop and hence reducing the complexity via activating seamless user workflow.
- Reduce the exposure of sensitive info via securing of files by employing digital certificates (PKI encryption) or/and complex passwords.
- Avoid the recovery of temporary files holding sensitive info that have been shredded/ deleted.
- Implement the application of data protection via the use of security policy that is maintained from a central position in an organization.
- Offer a contingency key support that will enable the IT security to access all encrypted files in case of emergency, audit purposes or for protection against malicious insiders.
- Offer an easy adoption into in-stream applications and streams of jobs via API or command line interface.
- Enable access of encrypted info via a mobile device [8].

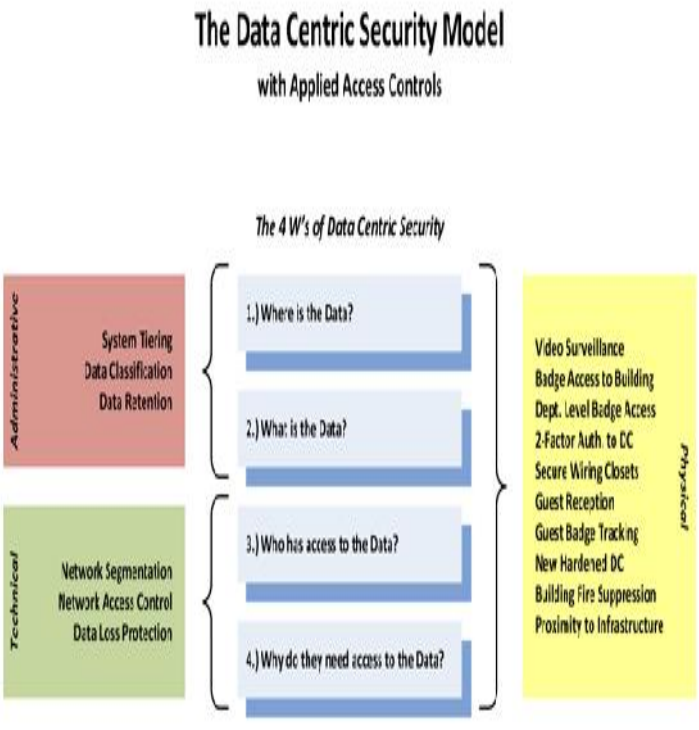

Figure 2: **The Data centric security model**

B. Authentication and authorization: role-based data-access control

Authorization, authentication, and disclosure control are at the central point in data-centric security where various components are required. The component for authorization needs the user to offer authentication and credentials that corresponds to the profile of the user. A monitor constituent allows access to the sensitive data and calls for authorization to carry out the needed operations. A role-based data-access component is the one that dictates whether a policy denies or allows a certain action on a given category of a particular data [9].

This engine of policy enforcement is fundamental aspect of data centric-security model. It gets the privileges of a user gaining access to a category of data, the business aspect of such process in business plus the operations that ought to be executed on the very data.

The rules-based engine gives the feedback: this tells whether the access is filtered, denied or allowed. The engine can also make decisions on whether some transformations on the team's data can be carried out before they are made accessible. Depending on the hierarchy of data importance, permission might be prevented on either non-compliant or generate with the events' correspondence [9].
It is worth acknowledging that data-centric security approach ensures cost-efficient protection of the integrity of info.

Furthermore, the flexibility that characterizes updating of security policies within operational systems ensures that the organization at hand has full control to adapt to the requirements of the business [9].

V. Building Firewall

There are various reasons that elaborates the importance of an organization owning a firewall, these are:

- Lab or test networks from unauthorized activities that might be conducted within a network.
- Low security in particular regions of the network.
- High security in particular regions within network.

It is worth noting that firewalls mediate between two regions of one particular organization or between two different organizations co-joined by the fact of sharing one network rather than between Internet and a single organization [10].

A. Suspicious activities in the network

Test networks and laboratories are the first networks that are given the first preference of being separated from the rest of organization by many people when it comes to data security. BIF employees usually work on routers; the type of firewall can be very simple owing to the fact that the department of IT is not required to offer several services. In several instances, it is preferable to obtain a packet filtering router, which enhances any incoming activity to the network being tested, but only authorized activities from it [10].
To ensure that time is not wasted in the process of router's testing, one can carry the following steps:

- Employ different protocols of routing from the one being tested and disable the whole of the protocol being tested.
- Instruct the router to reject routing updates from the interface being tested and also filter the packets out of the routing protocol.
- Specify the actual host from which the updates directed to the router will be from it [10].

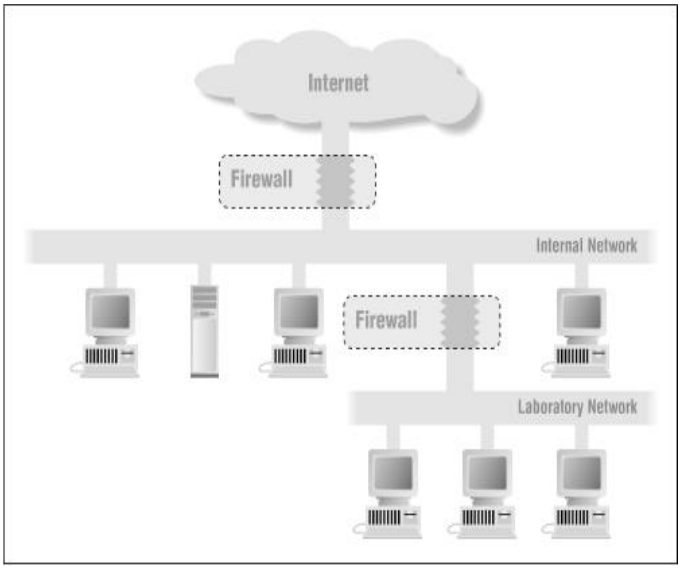

Figure 3: **Diagrammatic representation of a firewall**

B. Insecure Networks

Various organizations might have more secure networks in comparison with others. In order to restrain confidential info from leaking to other networks, dual-homed host or packet filtering router, which will limit the networks, connections to servers seems to be secure. One of the remedy will be limiting trusted users from engaging in unauthorized activities while carrying some operations on the networks for instance leaving the account unlogged out or accessing confidential emails. This ought to be carried out in combination of force and training that will succeed in deterring insecure uses [10].

C. Extra-Secure Networks

Most organizations are unsafe at a particular point. It is worth noting that most of them are conscious in terms of security to some extent for instance, company is developing a new product; in most places, finance and accountant machines call for extra protection. To meet the high security standards via encrypting traffic that passes by the internal networks or by creating up separate networks for safe traffic. Separated networks are basically easier to protect. As the user signs in into a secure data in a certain server so as to serve, it is advisable to set up a straightforward single-machine firewall for instance router that filters packets. The firewall will treat it

as a normal network because the machines in the lab don't need to be offering many services. Perimeter net is required (for secret venture) while a bastion host is not [10].

VI. Policies

The following steps are the ones that are carried out so as to tell areas that are prone to high risk of insider threat and hence other counter [11].

A.Identify the team

In this area, a team refers to a group of people who will create policies, make decisions and make out issues in case they arise. This group includes members of executive management (COO) with representatives from HR, budget authority, IT and legal department. In addition, the agenda of setting the first meeting is important when it comes to handling the elements of the plan. The team should be in a position of working throughout the organization at hand so that in case a problem occurs, it can be easily remedied [12].

B. Conduct a Risk Assessment

If money is the most important asset in the company, then to protect the business calls for the stakeholders to understand the dynamics of the asset at hand and implement the plans to make the asset secure. Knowhow of the physical location, ways to access, guarding and protection, recording, actual amount is all what need to be there.

If data is the most important asset in the company, then determination of the mode of data storage whether physical or manual should first be made. The location of the file, the way to access it and who accesses it is all what matters.

After one understands his/her asset, then coming with the best way to protect the organization becomes the agenda. What if the info leaks to foreigners or competitors? Monitor who accesses the info and then limit its exposure by controlling who accesses it and who should not access it. In case there is lapsed in security, the organization should be in a position to terminate the access [12].

C. Tighten Up Policies

The team to work on the insider threat will promote the operation of the agenda, implement change, get the feedback and also document the policies introduced. Procedures and policies to protect the assets are the ones that are first examined in risk assessment. Acceptable Use Policy for the organization is adapted to tighten the procedure [12].

VII. Conclusion

It is argued by most IT experts that data leakage from insiders poses a bigger threat than that any other source of the threat. Insight Express carried a study that involved over 2000 employees, IT experts from 10 countries. The choice of countries was in relation to their business and social cultures and it was aimed at understanding better the factors that affect leakage of data [13].

It is true that there is an external threat to sensitive data but the internal threat also leaks massive sensitive data. The threat from insiders is characterized by malicious activities of employees trying to access, steal or sabotage with the intention of leaking confidential data. It is in this respect that organization should restrict the malicious action and avoid its further occurrence by employees.

References

[1] Paul Kenyon. (2012, November) GSN. [Online]. "http://www.gsnmagazine.com/node/27821"
[2] Jenni Merrifield. Security TechCenter. [Online]. http://technet.microsoft.com/en-us/library/cc700846.aspx
[3] Dominic Vogel. (2013, May) Techrepublic. [Online]. http://www.techrepublic.com/blog/it-security/how-to-successfully-implement-the-principle-of-least-privilege/
[4] IMPERVA. [Online]. HYPERLINK "http://www.imperva.com/solutions/ric_privileged_user_monitoring.html" http://www.imperva.com/solutions/ric_privileged_user_monitoring.html
[5] Margaret Rouse. (2012, April) SearchCloudSecurity. [Online]. http://searchcloudsecurity.techtarget.com/definition/information-centric-security
[6] Mark Bower. (2013, February) Bank Information Security. [Online].http://www.bankinfosecurity.com/interviews/move-to-data-centric-security-i-1791
[7] Jim Wyne. (2014, January) International association of privacy professionals.https://www.privacyassociation.org/publications/data_centric_security_reducing_risk_at_the_endpoints_of_the_organization
[8] Luther Martin. (2012, May) Voltage Security. http://www.voltage.com/blog/crypto/data-centric-security/
[9] Mike Bilger, Luke O'Connor, Matthias Schunter, Morton Swimmer, and Nev Zunic. (2006, December) IBM. [Online]. http://www-935.ibm.com/services/no/cio/risk/gov_wp_data_centric.pdf
[10] Simon Cooper & D. Brent Chapman Elizabeth D. Zwicky, Building Internet Firewalls, Second Editions ed.: O'Reilly Media, 2000,vol.6.[Online]http://docstore.mik.ua/orelly/networking/firewall/ch04_04.htm
[11] Brad Ruppert. (2009, April) SANS. [Online]. http://www.sans.org/reading-room/whitepapers/incident/protecting-insider-attacks-33168
[12] D.MillsKatherine.CTSC.http://www.gtscoalition.com/insider-threat-programs-5-easy-steps-to-protect-your-company/
[13] CISCO.http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html
[14] U.S Department of Justice. (2012, Janury) The FBI Federal Bureau of Investigation. [Online http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat
[15] 15 Cisco Systems, Inc. (2008) Cisco. http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf
[16] Vormetric, Inc. (2013) tech digital library. http://www.informationweek.com/whitepaper/Security/Vulnerabilities-and-Threats/the-insider-threat-how-privileged-users-put-crit-wp1389199997?articleID=191740673
[17] Sumanth Madimsetty. (2010, February) Ca technolgies. http://www.ca.com/ch/fr/lpg/Security/Security-Breaches/~/media/Files/TechnologyBriefs/ca_access_control_technical_brief_231751.pdf
[18] Jeffrey Hunker and Christian W. Probst. Insiders and Insider Threats. http://isyou.info/jowua/papers/jowua-v2n1-1.pdf
[19] Dave Shackleford. (2010, May) SANS Analyst program.