Fundamental Pro-active Approaches against Insiders Security Policy Violations

Ansari Neha[1], Dr.DandHiren Jayantilal[2], Dr.Shaloo Dadheech[3],

[1]*(Research Scholar,Pacific University, Pacific Hills, Airport Road, Debari,Udaipur, Rajasthan 31300)*
[2]*(Coordinator, Department of IT, Mulund College of Commerce, University of Mumbai, Mulund West, Mumbai 400080)*
[3]*(Assistant Professor,Faculty Of Computer Application, Pacific University, Pacific Hills, Airport Road, Debari, Udaipur, Rajasthan 313003)*

Abstract: *Information Security Management is one of the most fundamental requirements of most of the organisations today.But just deploying Information Security Management by focussing on security attacks from outside is incomplete until and unless security policy violations from inside the organisations is also considered.Having a complete proactive approach from security threats in both directions (inside and outside) is the need because they can help the organisation to prevent as well as control security threats.Infact, having a security policy is of no use for the organisation unless there is some security practice to support it and security tools for monitoring its violations.Insiders threats are more dangerous for the security of organisations intellectual property as compared to external attacks this is because the insiders have direct access and privileges on the resources of the organisation.Insiders security policy violations can be accidental or deliberate,but organisations security system must be robust enough to defend from both accidental as well as deliberate security policy violations.*

Keywords: *Information Security Management, Security Policy, Intrusion Detection and Prevention System, Firewalls, Audit log software, Insiders Attack*

I. Introduction

Insiders security policy violations whether deliberate or accidental can be very dangerous for the organisation from both economic as well as organisation's good will perspective.It cannot be left of to be handled with reactive approaches the need of the hour is to have efficient proactive approaches for handling such policy violations.

IT organizations that allow users to access personal webmail accounts from inside the corporate network infrastructure are placing their corporations at risk on several fronts. However, despite these risks the use of personal webmail has become a widespread practice, and it would appear that many IT managers and executives are even unaware of the implications.

A survey by computer economics says that only 17% of all organizations have a policy against the use of webmail from within the corporate network and also have mechanisms in place to monitor and/or block its use. Another 7% have a policy against the use of personal webmail, but do not monitor or block its use. But over three-fourths of organizations have no policy against this practice at all.

There can be many precautionary measures which can be taken by the organisation to protect such security policy violations because of web mail access to the employees.

The below research focuses on such approaches.The paper is divided into four sections. Section 1starts with a hypothetical case study demonstrating a scenario of insiders security policy violation.Section II is about the analysis of the case study.Section 3 describes some of the security controls that can be used for proactively handling such security policy violations by insiders and section 4 is the conclusion part.

II. Case Study

In a renowned I.T. Firm that handles foreign organisations project.It so happens that a software engineer is allocated to handle a project.He gradually works with this project for many years.After some days he gets some work for the same project but to code in a programming language that the engineer is not familiar with.He finds some complications in dealing with this new programming language.He tries with some r & d for some days but finds difficult to frame certain logic in the programming language.Eventually he decides to take help from a friend in learning the language, understanding the code already stuffed in the code repository and to develop new code.This friend whose help he aughts to take does not work in corporate and so does not belong to any firm .In order to take help from this friend the engineer zips all the source code from the repository and mails the zip file using his corporate email id to friend's email id which of course belongs to a public emailing system like Gmail,Rediff mail.

For the software engineer he feels that he has just sent some source code of company to a trustworthy friend who will be helping him in his office work little did he know that in all his innocence he has also mailed security credentials of the client organisation to his friend.The blunder that he makes is he does not check all files properly before sending he assumes that all the files have some source code. But some of the files actually have private security credentials of the client organisation.Now with an equal proportion of deliberate and accidental attempt this becomes an act of violating the security policies of both the client as well as employer's organisation.These violation of security policy now takes the shape of data breaching.

III. Analysis of Case Study

This kind of scenario cannot be actually called as an **"Insider Attack"** because making an attack was not the actual intention rather the intention was to handle the company job process but with some assistance from an outsider which led to a security policy violation.Ironically the scenario cannot be ignored as well because the way of handling job process was against the security policy of the organisation.Thus, instead of framing this as an **"Insider Attack"** this can be very much called as **"Insider's security policy violation".**

If a proper analysis of the entire case study is done,it may be found that the blame though should be put over the shoulders of the software engineer but not entirely somewhere or the else there were some loop holes in the organisations security management system as well.This data breaching which was not actually meant to be a security attack could have been very much avoided.Just making security policies are not enough for ensuring information security instead security practices must be encoupled with every security policy proper monitoring of the security practices is also equally important.

Mostly when organisations go for risk assessment the threats ,vulnerabilities and attack that they consider are in context to external attacks.[1]External security attack are given prime importance and insiders attacks and policy violations are in comparison not given that much care that they deserve .This is the reason that why most of the security controls placed in the organisation are for security against outside attacks .Had there been security controls that not only perform log of the employees action but also a real time analysis of it such attack could have been avoided.Defending against external attacks and just logging internal actions are not sufficient enough .Security controls for defending and monitoring the security policies meant to be followed by inside employees should also be included for a complete information security management.[2]

IV. Security Implementations

Few security implementations are described in this section which could have been deployed to protect against such violations of security policy.

1) Combination of Audit Tools and Intrusion Detection and Prevention System (IDPS)

As it is known that audit trail software can maintain log of all activities or events that takes place on the system. Logging of the events can be application, operating system or user based. Log details for every key press event can also be done through key-stroke monitoring or key-loggers.[4]

But just keeping the log details is of no use if it is not analysed at the right time.Normally the analysis of the log data is done if some security incident happens or on a near-real time basis .Near real time analysis can be collecting data for some hours or some days and then doing the analysis of it.

If the log software is integrated with intrusion detection and prevention systemthen the log software can capture details about the events and the intrusion detection system can analyse these log data to check if the events are benign or intrusions and if they are intrusions then their preventive counterpart can take action against intrusion and stop it from causing any damage.[5]

Now let us analyse how this solution could have avoided the security policy violation as described in the above case study.

For the above case study the application-based audit trail software could have been used on top of the email server application so that any email that is transferred by or reached to the email server are logged.As mentioned above just the logging is not the optimum precaution unless analysed in a timely manner.The entire scene may had taken a twist if the audit log software was integrated with the intrusion detection system.

When the software engineer sent the email to his friend using his corporate's mail id the email, he composed would have definitely reached the organisations email server for transfer and hence this event would have been logged by the audit log software.From the log software the log trail could have been taken up by the intrusion detection system for analysis and assuming that the IDPS system is properly configured as per the organisation's security policy it could have detected this email transfer as an intrusion and the intrusion prevention system could have blocked the email from leaving the organisations network boundaries

Thus this security policy violation could have been at the very real time and the data breaching could have been avoided.

2) Application based firewall or Dedicated Application Proxy Firewalls

Firewalls are one of the most widely used security control. There are different types of firewall each serving a different purpose and effective at different layer of TCP/IP protocol suite.Firewalls used for the protection at application layer level are Application based firewall or Dedicated Application Proxy Firewalls [5]

Blocking the outgoing emails by checking their contents as well checking the recipients email address or recipients email server can be done by both Application based firewall as well as Dedicated Application Proxy Firewalls .These firewall can help organisations to configure rules based on their security policies .Provided the rules are configured properly the firewall can block the emails containing sensitive information from leaving the organisations network no matter how much the employee tries. The proxy firewalls can also decipher encrypted mails.

In case of the above case study if an additional firewall layer of Application based firewall or Dedicated Application Proxy Firewalls could have been placed behind the packet filtering firewall then this firewall would have blocked the email sent by software engineer by analysing its contents and the recipients email id.

Also, most of the employees are given laptops or desktop-based systems by their employers to do their office work. If these laptops or desktop-based systems are pre-configured with personal firewalls with proper rules set then such security violation performed via employers own computer system can be avoided. Even the modern operating systems now a days have in built firewallson which application-based rules can be set. Thus the bottom line is that if such systems armed with efficiently configured security controls are provided to the employees by the employers for doing work such security violations can be avoided .

V. Conclusion

Organisations always try to maintain a very cordial combination of functionality usability and security. Sometimes for the smooth functioning of some business processes they have to keep security at stake. But that absolutely does not mean that they should compromise on security. Giving access of web mail services may be the business need but many security policies, practices and controls can be implemented to make sure that employees does not make a blunder out of such privileges given by the organisation for office work.

References

[1]. The Security Risk Management Guide by Microsoft Solutions for Security andCompliance and Microsoft Security Center of Excellence.

[2]. Guide For conducting risk assessments-NIST special publications 800-30

[3]. An Introduction to Computer Security: The NIST Handbook by Barbara Guttman and Edward A. Roback

[4]. Guide to Intrusion Detection and Prevention System (IDPS)-NIST publications

[5]. Guidelines on firewalls and firewall policies-NIST publications

[6]. https://www.computereconomics.com/article.cfm?id=1060

[7]. Warkentin, Merrill, and Robert Willison. "Behavioral and policy issues in information systems security: the insider threat." European Journal of Information Systems 18.2 (2009): 101-105.

[8]. Bulgurcu, Burcu, HasanCavusoglu, and IzakBenbasat. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." MIS quarterly 34.3 (2010): 523-548.

[9]. Salem, Malek Ben, ShlomoHershkop, and Salvatore J. Stolfo. "A survey of insider attack detection research." Insider Attack and Cyber Security. Springer, Boston, MA, 2008. 69-90.

[10]. Crossler, Robert E., et al. "Future directions for behavioral information security research." computers & security 32 (2013): 90-101.