International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

SECURITY POLICIES IN AN ORGANISATION

T.SAMBA SIVA RAO

Lecturer in Dept of Zoology, K.B.N College, Vijayawada

Abstract— Every organization, regardless of size, should have documented security policies. Surprisingly, many organizations do not. The key word in the first sentence is "documented". Every organization has a position or policy on security; it just may not be written down anywhere. If your organization falls into this category, beware! Sooner or later, you are likely to encounter a situation where it could make all of the difference in the world if you are able or unable to produce your documented security policies. It is not uncommon for individuals tasked with developing and maintaining these security policies to prefer visits to their dentist over taking on this effort. Where do you start? What should the policies cover? Will anybody really take the time to read them? How do you know if you have hit or missed the mark for developing good security policies? Invest the time up front to carefully develop sound policies and then identify ways to gauge their effectiveness and assess the level of compliance within your organization. Commit to spending the time and resources required to ensure that the policies are kept current and accurately reflect your company's security posture.

Keywords: Policy Enforcement, Password Appraiser, Auditing, e-mail

s

I. INTRODUCTION

Effective security policies form the foundation of your organization's entire approach to security. These policies should mirror your corporate culture and should be in harmony with your demonstrated business practices. Security policies are a living, breathing component of any successful organization. But as such, they require careful planning, development, and on-going attention in order to be of the greatest value to your organization.

Where to Begin:

If you have been given responsibility for the development or management of security policies for your organization, the task at hand could vary significantly. You could inherit a complete set of well-written, clearly understood policies that will only require that you keep them up to date. You may find that security policies already exist for your organization, but upon review discover that they are nearly ten years old. Or, you could be given a completely clean slate and asked to develop your security policies from scratch. All but the first scenario described above can seem overwhelming. At times, it can be hard to even know where to begin. There are so many areas to be addressed that it can become a "can't see the forest for the trees" situation. However, it doesn't have to be so difficult. First of all, accept that you will not have a policy for every situation that could arise. Aim for creating broad policies that are far-reaching to address all of the areas that you deem critical to the security of your organization.

Remember, the procedures you develop that actually allow security to happen must support your security policies. If you feel completely lost, or think that your company doesn't have a security position, the SANS Institute recommends that you review your firewall rules as a starting point. The things that you allow or do not allow through your firewall will begin to define what your security posture really is. Finally, if you are having writer's block or simply cannot get started, select a few common areas to begin with and then move on to more complex topics. Good starting points include policies on passwords (length, composition, change frequency), Internet usage, and e-mail.

II. SECURITY POLICY DEVELOPMENT

The following section lists additional things to keep in mind as you tackle the security policy beast.

Develop policies that you plan to enforce.

A policy that you are unable or unwilling to enforce is useless. If your policy states that Internet usage is strictly limited to conduct business-related tasks, but you do not block site access or have the capability to monitor an employee's Internet activity, you should do away with the policy.

Explain the purpose of the policy. Policies should be developed with specific objectives in mind. Be sure to explain the need for the policy and specify what the policy is trying to accomplish. Some policy development guidelines suggest a format that includes a background section in addition to the actual policy statement.

If you cannot explain why the policy exists, you cannot expect your employees to understand it or follow it. Get rid of it.

Develop security policies that do not require updates too frequently. If your policies require frequent updates, they are probably too restrictive or too specific. For example, if you

have a desktop operating system policy that states that "All desktops will be deployed with a Windows NT 4.0 operating system" you would have to update the policy as newer operating systems were released, like Windows 2000 and Windows XP, and the older ones become unavailable. In this example, a policy that states, "All desktops will be deployed with a secure, company-standard operating system" would allow more flexibility.

Differentiate between policies and standards or recommendations. Your policies should be comprehensive and thorough but should not be so specific or detailed that what you really end up with is a set of best practices or recommendations instead of policies. Start with a high-level policy statement and then drill down to more exact specifications using standards and recommended ways to comply with the policy. For example, you could have a policy that states, "All data transmissions sent over an open network must be encrypted". Your company standard may specify that 128-bit encryption is required as a minimum encryption level. Your recommended encryption solution might be triple DES or AES. The key thing to remember is that as minimum encryption key lengths change or the encryption algorithm you prefer changes, your base policy would not have to change.

Don't develop your policies in a vacuum. Since your security policies will apply to all employees across the company, it is a good idea to include employees from other departments in their development. Include at least one representative from each business unit in your policy development efforts. At a minimum, include a cross section of other employees in the policy review process. These individuals may think of something that you did not include and will provide feedback as to whether or not the policy is easy to understand.

Make your security policies available to everyone. You can have the best policies ever written, but if your employees never see them or do not know where to find them, they will never be effective. Also, if they only see them at new hire orientation, do not expect them to remember and follow them. Policy distribution can be accomplished through many ways. Some software tools allow you to post policies on your company Intranet. You could always place a read-only copy of your policies out on your network in a publicly accessible directory. A complete hard copy of the policies can be distributed at employee orientation and re-distributed on a periodic basis.

Make sure your policies stay current.

While it is true that policies should be developed in a way that they should not be constantly updated, they cannot last forever without some modifications. If you do not have an existing policy on wireless communication and certainly on Internet usage, your policies are in desperate need of a refresh. Plan to review your policies on an annual basis and actually schedule the review. A good time to conduct this review could be at the end or the beginning of your fiscal year.

Make sure your policies are understood.

Develop policies that are straightforward and not too complicated. If employees cannot understand what the policy requires, they cannot be expected to follow them. A policy that is to long or complex will most likely never be read (in its entirety) and certainly will not be followed. Some software tools (discussed later) allow you to include simple quizzes with your policies to test an employee's understanding of the policy.

Require acknowledgement of your policies.

Always, always, always include an Acknowledge statement with your policies and require that employees sign it. The acknowledgement statement should specify that the employee has received a copy of the policies, that they have read the policies, and that they agree to abide by the policies. Be sure that this signed acknowledgement form is retained in their employee file and that it can be retrieved if needed. Also, make sure that everyone in the organization has signed an acknowledgement form. No employee, regardless of their position, should be excluded from following the policies.

Include your policies as part of your security awareness training. Plan to include at least one policy to be reviewed as part of your periodic security awareness training. This can be accomplished in many different ways. Reminders could be included as part of any classroom-style training. E-mail messages could be sent out on a regular basis. Banner messages that appear during login could contain a policy of the month reminder. The key is to raise awareness of your policies on a routine basis and use a combination of methods to keep a fresh approach that employees will notice.

Determine up front what is required to make a policy "official". Policies that apply to the entire company typically require approval from multiple levels within the organization. Make sure you know exactly what is required to make a policy active and who has to approve it. The amount of time it takes to get policies approved and deployed can be significant in some organizations. If you work in are mote site or are a smaller part of a large company, find out early on if global policies already exist or if they have to "come down from Corporate".

Make sure your legal department is involved.

Since your security policies are extremely important to protecting your organization and since failure to follow the policies could cause severe damage to the corporation and loss of employment to the employee, make sure that you obtain

your legal department's review and approval of all policies. Failure to obtain this approval could result in creating legal issues for the company.

Stick to security topics for security policies.

Security policies only make upon part of an organization's total policies. If your assignment is to develop security policies, avoid trying to include policies that really should come from other areas. Examples include human resource policies, procurement policies, or accounting policies.

Security Policy Assessment and Enforcement

After investing a considerable amount of time and effort in developing good security policies, you need to be able to determine if your employees understand them and are following them. This section includes tools and techniques that can be used to give you an indication of your policies' effectiveness or help you identify possible avenues for breaches in security. Some of these suggestions can also be used to help identify areas where additional security and policy awareness training is needed. In addition, some of the tools described below can be used to help enforce the policies that you develop.

Password Appraiser

Quake bush Consulting, Inc. offers a product called Password Appraiser for Windows NT-based systems. This product is designed to provide capabilities above and beyond those already offered by existing NT password filters (passfilt.dll). In addition to enforcing password rules for length and composition, one of the enhanced features includes the ability to set password rules based on the type or level of user.

E-mail Review

E-mail usage policies in today's environment are as essential as any that you have to develop. Appropriate uses of how the company-provided e-mail system is to be used must be defined. Periodic reviews of e-mail accounts can be very useful in determining if your policies are being followed. These reviews can also help identify possible espionage and other breaches in security and confidentiality. At a minimum, for those who do not want to be viewed as "Big Brother", conducting reviews of e-mail accounts after an incident has been detected can provide very meaningful evidence when needed. However, if you plan to ever conduct a review of employee e-mail, either manually or through monitoring software, there are some basic requirements that must be included in your e-mail policies.

Internal Auditing

One of the best ways to determine if your policies are being followed does not require any type of software package. All you need to do is conduct an internal audit. A moonlight audit, so named because it is usually performed at night after your normal business hours, allows you to make one pass throughout your entire organization and assess numerous items related to compliance with security policies.

Get approval to conduct the audit. Make sure that you have approval from the proper authorities within your organization before you start roaming around your office in the dark. Also, make sure that your management has a clear understanding of exactly what the audit will try to accomplish. Finally, get the approval in writing and make sure that each member of the audit team has a copy with them during the actual audit. You may need to show this document to other employees working late, property management personnel, or security guards if you encounter any of these people while carrying out the audit.

Don't exclude anyone from being audited. Every office and workspace should be included in the audit. Do not exclude your own department, your IT department, or your executive's offices. You might be surprised by how many high-ranking officers are guilty of security violations.

Keep the audit secret. Involve as few other people as possible. Only disclose your plans to the people directly involved in supporting the audit. If you have to recruit help, ask for volunteers for a special after hour's project and only give them the full details of what is to be done at the briefing before you begin.

Protect the audit team members. Make sure that each audit team consists of at least two people. No individual should be allowed to enter your other employees 'work areas alone. This measure provides more integrity to the audit and safeguards participants from being accused of removing personal property that may suddenly be reported as missing. Also, try to keep the names of the specific team members involved in your exercise confidential. Believe it or not, some people will not be pleased that you "invaded their privacy" by conducting your audit.

III. CONCLUSION

Having a complete set of documented security policies should not be viewed as optional for any business. Keeping the policies that are documented updated is just as important. Only document the policies that you intend to enforce. Make sure that every employee has access to the policies, reads the policies, and acknowledges that they will abide by the policies. Include policy education as a part of ongoing security awareness training. Finally, identify and use mechanisms that help you determine if your policies are complete, are understood, and are being followed. Like so many other things within the security discipline, developing good security policies requires careful thought and planning as well as on-going care and feeding.

IV. REFERENCES

[1] http://www.pentasafe.com
[2] http://www.pentasafe.com/products/vspm.
[3] http://www.polivec.com/
[4] http://www.polivec.com/products.htm
[5] http://www.polivec.com/polivecbuilder.html
[6] http://www.polivec.com/pvbfeatures.html
[7] http://www.polivec.com/polivecscanner.html
[8] http://www.polivec.com/pvsfeatures.html