Global Information Assurance Certification Paper

Managing Desktop Security

Amran Bin Munir
Version 1.2e

Purpose

This document describes the defence mechanism for security of desktops (including notebooks or laptops) in a network computing environment from the approach of security requirements among users, process of implementing and enforcing security policies and technology within an organization.

Introduction

Why would any organization need to care about the security of their desktops ? Correct! Desktop is the primary access to the organization's resources and business applications. It is the gateway to the organization's highly valuable and confidential information assets. For this reason, we want to be really sure that the bedrock principles of information security – confidentiality, integrity and availability – is strictly maintained.

The findings from the 2001 Computer Crime & Security Survey conducted by the Computer Security Institute (CSI) and FBI confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting. The survey indicated that 85% detected computer security breaches within the last 12 months and 64% acknowledged financial losses due to computer breaches. The most serious financial losses occurred through theft of proprietary information and financial fraud. Based on this finding, it is obvious that we need to continuously beef up the level of computer security and one of the very critical area that need to be properly addressed is the desktop security.

This paper only addresses some of the techniques, at high level, that can be implemented to ensure effective desktop security. Future research papers may be developed to provide more detail analysis of each of the method described. Issues and challenges that may face the implementation of desktop security are also not discussed. This can be the potential subject matters for other research papers as well.

Implementing Desktop Security

Patrice Rapalus, CSI Director, remarks that the Computer Crime and Security Survey has served as a reality check for industry and government:

> *"The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive*

approach to information security, embracing both the human and technical dimensions."

In line with the above note, this paper will approach the techniques in implementing desktop security from three angles - People, Process and Technology factors.

A. People

The first angle is the "People" factor. Two important aspects under this category is:
o education and awareness
o enforcement

1. Education and Awareness

We are all aware that human is always forgetful. To make people remember, we just need to continuously remind people . Security is as strong as its weakest link, and people is the weakest link. Educating users is essential to computer security. We need to instill user awareness so that they become security-conscious and security becomes part of their culture.

Many network security intrusions occur due to lack of knowledge and best security practice among employees. There was a case study on how a security team auditing a particular user network managed to log-in into 80% of the systems simply by looking at the passwords written on sticky notes, etc. in the immediate vicinity of the users' desktops. This is what will happen when security awareness is lacking.

Some of the threats that need to be constantly communicated to desktop users are:
a. Using programs that send passwords in the clear
b. Bad password management
- weak password, sharing password, never change password, "post-it note" habits
c. Guest accounts or open accounts
d. Social engineering attacks
e. Virus and other malicious code attacks
f. Unsolicited email attachments
g. Downloading software from untrusted Internet sites
h. Installing softwares from untrusted sources
i. Modem connection to desktop within the LAN thus creating a backdoor.
j. Unattended desktop, without screen lock.
k. Packet sniffing
l. Bad desktop management
- no anti-virus, outdated virus signature, no backups, no desktop lock, open folder shares without password, opening insecure access

Some examples of education and awareness programs are:
a. Conducting regular seminars and roadshows to instill security awareness and on the importance of information security.
b. Publishing weekly posters in Bulletin Board.
c. Issuing friendly reminder when employees accidentally or unintentionally commit

security breach.

d. Publishing security reminders on screen saver messages.
e. Giving small token of appreciation for reporting security incidents. The token does not have to be expensive but it does go a long way. It gives a real meaning to the users and emphasizing that their efforts are being recognized and appreciated by the management.

All of these efforts are meant to reminding users so that they are fully aware of the threats and to obtain help and cooperation in taking protective measures to prevent or minimize security incidents. The objective is to ensure that all users are better informed and will take proactive actions with regard to security. If security incidents do happen, they are ready and will know how to respond to those incidents.

2. Enforcement

Now users are properly informed about security policies, standards and procedures pertaining to desktop security. They are aware of their responsibilities with regard to their desktop security. They had been told what are the do's and don'ts within the guidelines in proper handling of their desktops including notebooks. They know what are the consequences if they intentionally breach the security parameters. Following this step is to enforce what have been stipulated in the policy to those non-conformers.

Why do we need enforcement? Enforcement is the key in ensuring that the policy developed is effective and implementable, not merely a "dust collector". The effectiveness of a policy will be tested in enforcement, and that will determine whether the investment in money and resources is paid off.

However, enforcement of policies requires sufficient proof and evidence, in order to support the claims and accusations. Thus, it is of utmost important that the security mechanisms in place are able to generate audit trails and verification whether in the form of text, audio or video.

All incidents involving breach in security must be fully and thoroughly investigated. For minor incident, sending a reminder from Security Dept may be sufficient. A more serious offence must be referred to Human Resource Dept for appropriate disciplinary action. For criminal cases which is defined as incidents breaching the laws of the country, the legal department must be notified and subsequent legal actions may be taken against the responsible parties.

B. Process

The second angle is the "Process" of implementing desktop security. What we need to consider under this category is:

o Governance
o Policies, baselines and procedures
o User classification
o Review and audit
o Penetration testing

1. Governance

The level of governance required for each organization may be different, depending on number of staff, organization policy, technical competency, organization structure, etc. For a large multi-national organization, having several governance may be justified. For medium-size or small local organization, it may be simpler. The purpose of having governance is to ensure the security of any desktop implementation. Some examples of the governance are as follows:

a. IT Steering Committee
This is the highest level committee that formulate strategy and setting up direction in the implementation of any IT initiative. Since security cuts across IT and policy in implementation, it is of utmost important that the highest committee be chaired by the top management of the organization, for example, the CEO or COO. Failure to do so may create difficulties in enforcement, holistic and effective implementation of security policies.

b. IT Security Council
This council formulates Policy and Baselines and oversees the enforcement and security implementation. The council will also deliberate and propose new initiatives to the IT Steering Committee in enhancing desktop security application implementation. In addition, they will ensure that any change to the production system had been properly deliberated and verified so as there will be compliance to the policy for desktop users .

2. Policies, Baselines and Procedures

Any desktop implementation must be governed by IT security policies and baselines. In addition, day-to-day operational procedures must be strictly adhered. The objective is to ensure confidentiality, integrity and availability of information.

"Lack of accepted and well-promulgated security policies, procedures, and guidelines" is in the list of top 14 security vulnerabilities. (Hacking Exposed, p662).

a. Policies
"Policies are the primary building blocks for every successful information security effort. In order to be successful, every information security effort needs to have a set of policies which provides clear instructions and establishes management support. Policies are used as a reference point for a wide variety of information security activities including : designing controls into application systems, establishing user access controls, performing risk analyses, conducting computer crime investigations, and disciplining workers for security violations."
(Information Security Policies Made Easy, p1.)

On desktop security, it may states that all unattended IT equipments must have appropriate and approved security protection.

b. Baselines

Baselines are the minimum security standard applied to any system configuration. Baselines can be categorized into two groups. General baselines specify general standard which cover overall systems in a company while technical baselines is more specific towards a particular system platform or application. Example of baseline : password must be alphanumeric and has minimum length of 8 characters.

c. Procedures

Procedures are about specific operational steps. They describe in detail the flow of processes to be followed for any given task or activity. E.g., a new user applying ID for desktop access (within network computer environment) must fill-up and sign certain registration form, get it approved by the management, submit it to the Security Dept and wait for the ID creation.

3. User Classification

In a network computing environment, classification of users for desktop access is an effective way of access control. This technique classifies users into several types, e.g. type 1,2 and 3 to differentiate them against each other. Type 1 users may obtain standard desktop applications, approved optional softwares that suit their tasks and functions, and have access to A and C drives. On the other hand, type 2 users may only get standard desktop applications and have no access to A and C drives (all applications and data reside in central servers). Type 3 may be assigned as mobile users.

Delivering set of toolsets or application access is based on user type. One of the advantages of user classification is that desktops can be centrally managed and with this, future growth in terms of delivering client applications to users will be much easier and simple.

Another advantage is that users' access can be controlled by category. For example, only type 1 users are able to access the Internet. With restricted access, the number of abuse cases can be minimized. This is especially critical if we look at the 2001 Computer Crime & Security Survey which reported that 91% detected employee abuse of Internet access privileges. (e.g. downloading pornography , pirated software, or inappropriate use of e-mail systems.)

Other things that need to be controlled are *"user or test accounts with excessive privileges"* and *"unauthenticated services like X Windows allow users to capture remote keystrokes."* (Hacking Exposed, Top 14 Security Vulnerabilities, p662).

4. Review and Audit

Review and audit are performed to check and verify compliance against baseline. Security audit is an activity that focus solely on security aspects and to be done on a regular basis. At any time, if the need arises, ad-hoc audit shall be conducted. Ad-hoc audit may be required upon request by user department or when incidents occur.

In addition to formal audit by Security Dept, self-compliance review can also be practiced. Self-compliance review allows users to conduct their own reviews using standard template given to them. The benefit of this exercise is that users will be able to gauge their system

security and do corrections. Submitted reports from the compliance reviews will be useful for the improvement plan.

5. Penetration Testing

Penetration testing is another important activity in managing desktop security. The objective is to test desktop adherence to baselines by simulating hacking techniques. This activity must be carried out with due care – it must be properly approved by the management, conducted by authorized and trained personnel, and strictly governed by code of conduct and good ethics.

C. Technology

The third and last angle is the "Technology." Under this category, there are quite a number of technologies that can be implemented to support desktop security, amongst them are:
o Centralized management
o Password protection
o Single sign-on
o Desktop lock
o Virus detection
o File encryption
o Personal firewall

1. Centralized Management

A better approach to effectively and securely manage desktop implementation is thru centralized management. In network computing environment, the master application and database servers are centralized. However, the client application still need to be manually installed at each user's workstation that is authorized to use the application. Using centralized management, client applications are not pre-installed on the individual desktop. The deployment of authorized client applications to desktop will be made automatically and centrally upon user login to the network. This will include all the standard desktop applications, (e.g. e-mail, office tools, ERP client) accessible by all users, and any specialized application unique to the user. The method ensures that users only get what they are authorized to access on the desktop.

An added benefit is that users will be able to login from anywhere in the organization network and still obtain access to all authorized application they need to access because the client applications are not permanently stored on the individual desktop but rather are centrally distributed based on users' profiles. It also means better access control security since access points to all applications are controlled by user profiles instead of desktop specific. Thus, regardless of from where the user is accessing the organization's network, he or she is still unable to use the unauthorized applications.

2. Password Protection

Based on the 2001 Computer Crime & Security Survey, 23% of respondents suffered unauthorized access or misuse within the last 12 months. To improve the access control

and for better security, each of the application accessible from the desktop must be protected by an effective password system. This include access to the organization's network, email application, ERP system, office administration system, etc. The purpose is to ensure that access to each application is granted to the authorized users only.

To further enhance the security, the following features may be incorporated in the security baselines and become a mandatory security settings for each of the application.
a. Password must have a minimum length of 8 characters.
b. Password must be alpha-numeric.
c. Password must not be based on dictionary words.
d. Password must be changed every 30 days.
e. Account will be locked out after 3 consecutive unsuccessful login attempts.
f. Multiple concurrent login is not allowed.
These controls are necessary as *"weak, easily guessed, and reused passwords at the workstation level can doom your servers to compromise."* (Hacking Exposed, Top 14 Security Vulnerabilities, p662). Thus, depending on risk assessment of information on the corporate system, it is highly advisable to implement strong authentication system, which utilize at least dual factor authentication, for example, a token and a PIN.

3. Single Sign-On (SSO)

When there are multilevel security in multi systems, multiple passwords for a single user can also pose as a weak link in security management. As such, password protection can be effectively and securely managed using SSO. With SSO, passwords for multiple applications are captured once and permanently stored. Authentication for subsequent access to separate applications are auto-verified. Users just have to log-in into the organization's network and access to all authorized applications are automatically granted.

SSO definitely provides convenience to the end users. They don't have to remember many passwords for all the applications which they require access. However, to support the security aspect of this SSO, a strong authentication policy need to be applied and enforced. To overcome the potential threats of reusable password, the use of one-time password may want to be considered. Additionally, usage of multi-factor authentication method is highly recommended. This may include all or any combination of what you have (e.g. smart card), what you know (e.g. PIN) and what you are (e.g. thumb print scanning).

4. Desktop Lock

Desktop lock is an effective method to protect unattended desktop from being used by unauthorized users. During office hours, there will be many times logged in users are away from their desktops. They may be going to the washroom, pantry, discussion, meeting or just hanging around at other people's workplace. It is not practical that every time a user need to go away from the workstation, he or she must log out and then log in again later after coming back.

A more practical solution is to be able to easily lock and unlock the desktop as required. This is fine to the concerning users. Of course, there are also users who do not bother to do this simple thing. They may be going outside the office building for few hours and just

leave the desktop on with all the applications open. With this wide open access, an intruder can do a lot of things: performing transactions on the servers, copying information from the local disk, planting a trojan horse on the local machine, distributing viruses, sending emails on behalf of the user, etc.

To avoid this problem, the desktop lock should have the capability to lock automatically after certain minutes of inactivity (idle time-out). Once locked, the desktop can only be unlocked by a logged in user's password.

5. Virus Detection

Virus attacks are a common phenomenon especially to desktop users. 94% of the respondents in the 2001 Computer Crime & Security Survey detected computer viruses. As such, it is imperative that anti-virus is installed.
A minimum virus protection measure should be able to detect the presence of a virus on files stored, introduced to and processed by the desktop. It should also have the capability to do manual on-demand virus scanning on all the storage devices that the desktop supports.

In addition, there must be a mechanism to ensure that the latest virus signature update is deployed effectively and efficiently with minimum human or manual involvement. An automated process is preferable, which is available in anti-virus supporting Client Server environment. For large organizations, it is a prime necessity.

6. File Encryption

File encryption is an important tool in preserving confidentiality of information. Most of the time, confidential information not only stored on central servers, but also resides on the local hardisks. With proper encryption, we can ensure that all confidential and classified information are accessible only to authorized users. This will be applicable throughout the cycle – while the information is being processed, in transmission and in storage.

7. Personal Firewall

Most organizations install firewalls at the network gateways to protect against external threats. This however does not protect internal threats. Unfortunately, intruders do not only reside outside the organization, they also reside from within. As a matter of fact, most of security threats are actually coming from internal users.

Globally, this type of threat is increasing as the organization's network security perimeter is disappearing. As the information technology becomes dominant, businesses require more and more connectivity to partners, customers, vendors, contractors, consultants, etc, to be in the leading edge and to gain competitive advantage. As a result, the organization's network is populated with people, both trusted and untrusted.

"It is estimated that 80% of attacks are from within the organization. The most serious security breaches resulting in financial losses occurred through unauthorized access by insiders. Insiders represent the greatest threat to computer security because they

understand the organization's business and how the computer systems work. Therefore, an insider attack would be more successful at attacking the systems and extracting critical information." (The Insider Threat).

Personal firewall which is installed at the desktop ensures some measures of protection from potential attackers. It will also detect and notify any unauthorized attempt to access the desktop or the information residing on it. Reports generated by the personal firewall can be the starting point for investigating potential threats, be it from external or internal parties.

Conclusion

Desktop is the entry point to the organization's information resources. If the security of the desktop is weak, potential intruders can easily by-pass the first obstacle. It is paramount to ensure that desktop has the right configuration that allow authorized users entry, deny unauthorized users entry and detect and block any attempt to by-pass its security parameters. In order to effectively manage desktop security, a blend of three components - People, Process and Technology - is necessary. We may implement state-of-the-art security technology and apply world-class processes, but if the users themselves are not taking security seriously or they are not aware of the threats and risks involved, then the investment and procedures become meaningless. All the three components are equally important and contributing to the maximum security protection of the desktop. If one of the component is missing, the desktop is more likely to be compromised and the most valuable information asset of the organization will be at risk.

Desktop security is a process. It is not a simple system where it has specific input, process and output. It is a process consists of Protection, Detection and Response. It is a continuous journey. The irony is that, despite the important contribution of investment in desktop security to reducing the risk of information security breach, it is difficult to quantify and justify and eventually to obtain buy-in from management for future investment, as compared to other IT initiatives such as application development and system implementation which has direct impact to business revenue. The only time when the organization realize that they need a good desktop security is when viruses are attacking and destroying all the files or confidential organization's data is lost to competitors and the list goes on. We have the option of acting early and not wait until a tragedy happens; by then it will be too late. Prevention is always better than cure.

References

Boston, Terry. "The Insider Threat." October 24, 2000. http://www.sans.org/infosecFAQ/securitybasics/insider_threat2.htm

Common Vulnerabilities and Exposures. http://cve.mitre.org

Computer Security Institute. http://www.gocsi.com

Counterpane Internet Security. http://www.counterpane.com

Foundstone. http://www.foundstone.com

Hacking Exposed. http://www.hackingexposed.com

InfoWorld Media Group. http://www.infoworld.com/security

Microsoft TechNet. http://www.microsoft.com/technet/security

SANS Institute. Information Security Reading Room. http://www.sans.org/infosec/FAQ

Security Focus. http://www.securityfocus.com

Security Issues. http://www.builder.com/Servers/SecurityIssues

Scambray, Joel, Stuart McClure, George Kurtz. "Hacking Exposed: Network Security Secrets & Solutions. 2nd Edition." 2001. Osborne/McGraw-Hill, Berkeley, California.
Snyman, Nelius. "The worst information security mistakes businesses make." February 27, 2001. http://66.8.39.94/Sections/techforum/2001/0102270901.asp?CiRestriction=nanoteq

Unix Security Overview. http://staff.washington.edu/dittrich/talks/security

Wood, Charles Cresson. "Information Security Policies Made Easy. Version 7." October 1999. Baseline Software, Inc., Sausalito, California.

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor