**Reducing "Human Factor" Mistakes**

Date: Jul 23, 2003
Author: Dancho Danchev

Nowadays companies and organizations face the problem where massive attempts at illegal intrusions hit their network on a daily basis. In spite of the latest technological improvements in security, it's still the network users who are often unknowingly inviting security breaches through carelesnes and a lack of awareness. This paper will try to summarize various mistakes done by system administrators, company executives and of course the end users, and will also provide you with useful strategies that will definitely help you reduce or completely eliminate the mistakes.

Nowadays companies and organizations face the problem where massive attempts at illegal intrusions hit their network on a daily basis. Whether successful or not, they still pose a significant threat to the proper functionality and continuity of the institution's processes. The majority of these institutions tend to think that any future security related implementations would cost too much effort and resources and place a burden on the budget. On the other hand, the constant media reports of large and well-known corporations broken into really discourage them.

In spite of the latest technological improvements, it's still us, those interacting and configuring these devices/programs; it's our staff members, the ones unknowingly contributing to the dissemination of malicious code, to the exposure of sensitive or classified business information.

This paper will try to summarize various mistakes done by System Administrators, Company Executives and of course the end users, and will also provide you with useful strategies that will definitely help you reduce or completely eliminate the mistakes.

**The Top 5 System Administrator Mistakes**

System Administrators are those mainly responsible for the continued operation of your computers and for the proper functionality of your network, however in most of the organizations these people are also responsible for the Security of the devices, the detection of potential intrusions and securing the organization's network. Taking a lot of responsibilities increases the number of potential mistakes by the individual due to the stress and the constant work on several issues simultaneously. Here I'll review the most common mistakes done by System Administrators which could somehow endanger your organization and the sensitive data you're holding.

**1. The lack of a well established Personal Security Policy**

Believe it or not, most of the average System Administrators don't have a personal Security Policy covering important issues like Physical Security of the terminal, the chaotic way a system's software is being updated and the way that new patches are applied. Even the big and well-known companies suffer from the fact that some of their systems are not patched as soon as a new bug is discovered, another proof of the importance of this issue.

Sometimes the Administrator isn't even aware of the latest vulnerabilities discovered, which could lead to a potential security breach within the organization. Security is a never-ending process that requires constant monitoring of new threats and technologies. Although most of the Administrators are not Security Experts they should continue to learn about new and much more powerful methods to protect and secure their networks, while on the other hand increase their competitiveness. Nowadays those

having some sort of Security certification or extended knowledge in the Information Security field are usually a step ahead of those whose skills are up to networking only. Below I've tried to summarize various recommendations and tips for improving the Security of your terminal, organization and broaden your knowledge on the subject.

- Physically secure your terminal and working place, realize the dangers of malicious "snoopers" walking around your workplace, having access to your terminal.
- Logout each time your leave the terminal, or set up a time out, so even if you forget to logout, the system will be protected once it detects you're not in front of the keyboard.
- Consider subscribing to various Security related newsletters, mailing lists with the idea to keep an eye on the latest vulnerabilities discovered.
- Visiting the appropriate exploits related web sites is an important process acting as an early warning system for potential intrusions due to outdated or unpatched software.
- Reading the latest Security related white papers is an essential step of the Administrator's self education process, which ensures he/she is up to date with the latest topics discussed over the community.
- Limit the use of notes and papers for any sensitive information such as passwords, IP's and anything that might help a potential intruder gain access to your systems. However if you use these, shred and destroy them each time before you leave your work place. Malicious "snoopers" around the workplace might take advantage of this well known weakness, so limit or completely eliminate the use of these notes.

**2. Connecting misconfigured systems to the Internet**

- With the ever-expanding company's needs, new systems and servers are connected to the Internet on a regular basis, thereby increasing the current level of productivity or significantly limiting the overall expenses of the institution. However, most of these systems are connected to the Internet without the proper Security Auditing, thus being exposed to malicious attackers by the time a proper Security Audit is done.

The majority of Administrators mainly rely on the fact that the system is new, no one knows about it, no one knows its reserved IP, and so it will be impossible to break into something you don't know that exists. However, this mode of thinking represents a threat to any organization. There are people or automated scripts scanning the Internet, or specific company's network, especially for such "test systems" with the idea to break into them, hide within, and use the system for committing further illegal activities. And how about if someone knew the right day, time and the IP reserved for the system, through advanced social engineering techniques, how about if someone is non-stop stealthily scanning your network for such systems? Realize the dangers and take the appropriate measures by following some recommendations listed below.

- Conduct a complete Security Audit of the system, before you physically connect it to your network.
- Make sure the system has the latest versions of the software, installed and securely configured.
- If there are network tests that need to be done, consider blocking the access to the test system from the Internet.
- Verify that the system you're about to connect doesn't contain any sensitive data yet.
- You might be interested in how often the new system is probed for various vulnerabilities. Install an Intrusion Detection System, and I'm sure you'll be surprised at the number of scans within the first day.

**3. Relying on tools**

Vulnerability scanners are often used to gather information about the current level of Security within the network scanned. Host Vulnerability Scanners are very useful in checking the Security within the host, like file permissions, passwords policies and many other issues related to potential local break-in. On the other hand, Network Vulnerability Scanners provide the Administrator with the hacker's point of view on the network, highly beneficial tools as far as Penetration Testing is concerned. Generally, these scanners would eliminate half of the potential security problems within the system, however they're not a complete solution in order to achieve maximum level of Security. Admins tend to run as many Vulnerability scanners, as possible thinking that the more they run, the higher is the chance to eliminate all the problems. Wrong mode of thinking, and there're even cases where inappropriate scanners are ran to check the Security of an OS they're not specifically created for. Indeed, Vulnerability scanners can save you a lot of time, resources and troubles, but they're not a complete solution and you should not rely only on these. Instead, learn more about the Security of the OS you're running, so that you'll be able to manually (or via some sort of scripts created for your very specific needs) eliminate potential Security problems that cannot be discovered by any Vulnerability scanner.

**4. Failing to monitor the logs**

Monitoring the system's logs is an essential step in detecting ongoing or forthcoming intrusions. It will help you understand the common vulnerabilities, attackers are scanning for, so that you'll be able to verify all of your systems are protected against specific attack. In case of an intrusion, it's your system logs that might help you trace back the attacker, if they're not modified of course. Realize the benefits of regularly checking and securely storing your log files, while on the other hand a contribution to the scene will help everyone. Dshield.org is a reasonable example.

**5. Running extra and unnecessary services/scripts**

Using the company's resources and network as a personal playground for testing various scripts and services, is another common mistake done by the average Administrator. Having these scripts and extra services running, results in a variety of potential new entry points for a malicious attacker, and let's not mention if this is done from the main server. If you really need to test scripts, run extra services for personal issues, consider doing it from an isolated computer, not connected to the network, while still having Internet access, thus limiting the chances of someone discovering these services and scripts.

**The Top 5 Company Executive Mistakes**

Company Executives are those managing and dealing with the company's resources, budget, those who are responsible for leading and expanding the institution. Nowadays, the Internet offers amazing advantages for any company worldwide. The term E-business is getting more popular and E-business Strategy is an issue included in every Business Plan. However, the global connectivity represents a threat to the sensitive information if the company is lacking a Security strategy. I'll try to summarize common mistakes done by the Company Executives that could possibly contribute to a Security breach.

**1. Employing untrained and inexperienced experts**

Without a doubt, every highly qualified and experienced Expert is a valuable asset to any company's resources. However their qualification and professional abilities require the Executive or the one responsible for employing them, to have extended knowledge on the issue, thereby hiring the

appropriate person for the right job. Having a basic understanding of various, if not the most popular certifications, ensures that you'll be able to make the best decision. I would advise you to take a look at gocertify.com/security in order to deepen your knowledge on the most popular Security/Network certifications available.

**2. Failing to realize to consequences of a potential security breach**

By realizing the devastating consequences of the problem, and eliminating the "This won't happen to us" mode of thinking, you'll be able to properly react instead of endangering your company's business activities due to lack of understanding the issue.

- Damaging other businesses online, by contributing to a DDoS attack
- Storing illegal information and unknowingly distributing it due to an undetected intrusion
- Exposing sensitive customer's information to a malicious attacker, thus endangering their privacy
- Damaging the company's image, loss of customers, loss of partner trust

And it's just the tip of the iceberg, realize the consequences and take the appropriate actions.

**3. Not spending enough money on the Information Security issue**

Convincing a Company's Executive on the benefits or the potential losses of proper/improper management of the Information Security budget can be a difficult task. Managers tend to limit the budget to the minimum because of their failure to realize the potential damages to the company, or sometimes it's the budget that limits them. Internet as a global network offers unlimited and fascinating opportunities for every Business out there, once the Information Security issue is well taken care of. Consider conducting a Risk Analyses, so that you'll be able to distinguish critical or less critical systems, thus fitting in the budget, while on the other hand have your sensitive systems properly protected.

**4. Relying mainly on commercial tools and products**

"We use a world-known firewall, and a server based virus protection, so we are secured against hackers attacks" is one of the most common answers on "How is your company protected against hackers?" Security is a process, not a product. Although theoretical concepts became real-life solutions with the help of technology, this is not a complete solution for your Security. Company Executives need to have a basic understanding of what a firewall can, and cannot do, how useful and in some cases, useless a virus scanner is, thus they'll be able to invest in the right direction. Commercial tools and products are part of the process - securing your company's sensitive data, but they're tools that will not absolutely protect your organization.

**5. Thinking that security is a one time investment**

Security is an ever-evolving and ever-adapting concept, which requires monitoring, investments in both technology and most importantly, in people's education. New technologies appear every day, significantly saving you time and money, thus providing both the enterprise and the customers with a much reliable, yet cheaper services. However, new technologies and services pose different threats from those that you're currently protected from, which means that each time a new technology/service is implemented it will definitely enhance your productivity, but on the other hand the process requires a different Risk Management and the implementation of various new security measures.

**The Top 5 End User Mistakes**

End users are those handling the sensitive company's data on a daily basis. It's their decisions and activities that protect or somehow expose this highly critical data to a potential intruder/competitor. Here I'll review some of the most dangerous mistakes that end users tend to make.

**1. Violating the company's Security Policy**

The Company Security Policy is a document outlining the responsibilities of each of the staff members, having access to sensitive systems and information. The document is considered to be an inseparable part of any organization's Security Model, thus providing the staff members with an easy to understand way on how to protect the company's systems while using them. However, end users tend to violate the policy, thus exposing critical systems and sensitive information to a malicious attacker. The consequences of these activities could be devastating to your whole organization, that's why it is strongly recommended to provide everyone with explanation on why it is so important to follow the Security Policy, as we as discuss the potential damages of violating the Policy.

**2. Forwarding sensitive data to their home computers**

One of the most dangerous ways of having your sensitive data exposed to attackers, an activity which turns all of your Security measures into a completely useless process, is that of the staff member's habit to forward sensitive data to his/her home computer. The reasons are obvious, the consequences devastating. In fact, the users tend to forward a non-finished project or a business plan to their home computer, so that they'll be able to finish their work later at home, while on the other hand they don't realize that changing the company's secured environment, with their less secured home computer one, seriously exposes this information to an attackers/competitors. If it is absolutely necessary to forward data to their home computer, a regular Security Audits has to be conducted, ensuring their notebooks or home computers are protected from malicious attacks, while on the other hand the whole process increases the Risk level.

**3. Writing down any accounting data**

Creating and maintaining strong passwords, that's not your company's employees favorite process, as it's a time and nerves consuming one. Users hate creating passwords which they can't remember, while on the other hand the company's Security Policy states that this is the way a password should be created/maintained. Memorizing such a password is another issue that bothers them. In order to solve their problem, users tend to keep "secret" notes, under the keyboard, in their wallet, or anywhere else around their working place. These notes contain their sensitive accounting data, and using this way of storing, increases the chance of a Security breach due to irresponsibility. You should make your users aware of the potential problems that might occur, consider providing them with various password-memorizing techniques in order to reduce the current number of staff, keeping accounting data on notes. Play various scenarios on how a malicious attacker could find their note, and what would follow after that.

**4. Downloading from untrusted web sites**

Given the opportunity to download from the Internet, the staff members often abuse their privileges and even endanger the Security of their company. Downloading from unknown and untrusted web sites helps the spread of malicious programs all over the Internet. Once infected with any sort of malicious program (virus/trojan/worm) the infection will cause serious effects on the organization's functionality,

and let's not mention the potential spread of these programs on other networks. Staff members should keep the downloads to the minimum, in case they need a specific application, it is strongly recommended to contact the IT Department instead of downloading the program from an untrusted web site. Another problem that companies face these days is the installation of pirated (warez) software (downloaded from the Internet) on their systems. Educate the staff members via any sort of Malicious Code Best Practices, summarize the entire problem and help them understand the dangers.

**5. Failing to pay serious attention to the Physical Security issue**

Having a basic understanding of various Physical Security issues will definitely result in much more secured workplace, and thus adequately protect sensitive data. Generally, the staff member's behavior while using the company's workstations is likely to be highly irresponsible and "security illiterate". Users often leave their workstations unattended, their screensavers rarely have proper passwords, the list of problems is an endless one. Educate them on various strategies while using the company's systems; ensure they're able to properly handle sensitive information having the Physical Security issue in mind.

**Summary**

This paper explored in-depth the most common mistakes that could lead to a potential Security breach. Take these very seriously and if necessary renovate your current Security Model. Educating your users, administrators and even the company's executives will increase everyone's level of Security Awareness, thus ensuring the secured and continuous functionality of the organization. The author of this paper can be contacted at dancho.danchev@windowsecurity.com.