Interested in learning more about security?

SANS Institute InfoSec Reading Room

Inadequate Password Policies Can Lead to Problems

This paper explores how, overall, the security administrator's duty is to reasonably ensure the security of the network, and how he/she can do this by setting policies commensurate with the risks of losing data, financial damage, theft of information, public embarrassment and/or reduction in share/stake-holder value. The administrator should set policies to cover how passwords are stored, how they are changed, the frequency at which they should be changed, and the fiduciary duties of the users, management and network a...

Inadequate Password Policies Can Lead To Problems

Leonard Hermens

Version 1.2f

Password policies are necessary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of computer systems. The fundamental protection of computers and networks (the password) is still in use. However, not all companies yet realize the risks they are taking by having poor password policies. The risks include user confusion, system denial-of-service issues and user education problems if the policy is not communicated clearly to the users.

Password policies of companies may vary in their complexity depending on the perceived need to secure the company's assets. I have worked for companies who had no password policies, but thought that passwords were a good idea and used them. The defacto policy was that the employee and administrators used passwords, but there were no rules on how to secure them, generate them, store them, change them or manage them.

I have also worked for another company had an entire division that didn't use any passwords at all. Each user had a login ID on their Novell network, but no passwords. As a result, when we set out to network their division to ours via a WAN, they specifically requested that we not route Novell IPX packets to or from their site to "ensure the security of their data." They simply didn't perceive the risks to their business and operations.

Another company took passwords seriously only for their financial data. For many of their various manufacturing and employee self-service applications, employees were required to use their United States government-issued social security number (SSN) as their authentication password. The SSN for an employee is not difficult to obtain, and only recently was the SSN removed from this company's check stubs for security reasons. Still, the SSN is being used in too many system at that location.

It is clear that even at the lowest level, some companies don't take security too seriously. However, the password policy is a good place to start to shore up the security of a network. The password policy cannot be an island, rather it must be an integrated part of an umbrella policy to ensure the security of corporate information.

Many password policies specify attributes and procedures for handling user passwords. Among these attributes are: minimum length, allowed character set, disallowed strings (all numbers, dictionary words, variations of the username or ID), and the duration of use (expiration) of the password. The password policy should also include human factors (social engineering factors) to ensure the integrity of the user's password. For example, the password should be known only to the employee who needs access to the resource, and new passwords must be changed by the user immediately. This reduces the chance for illicit account access and allows for traceability and accountability of employee actions on the network.

Should a security issue arise, forensic data might point to a certain user account. The password policies and procedures in force at the time of the event may aid in determining culpability of an employee. If the employee revealed a password, contrary to the policy, then the employee may be liable for the security breach, regardless if the employee was directly involved.

Password polices need to be sensible and reviewed for legal issues, human factors and their cryptographic strength of protection. I know a company who has a small network. They are connected to the Internet. The administrator of this network decided to shore up the security and had a certain password policy in mind. In general, this was a good idea. However, the administrator didn't tell anyone what the policy was. There was a failure to formalize the policy, have management sign off on it and communicate the policy to the end users (train and educate them). All of these steps are necessary for a successful company strategy on security processes.

There were several problems with the administrator's home-brewed policy (but there were some good things, too). First, the policy didn't take into account the failings of humans. The mystery password policy locked the user account after three attempts to log in. While that might not be so bad for the administrative secretary who types error-free at 72 words per minute, it didn't bode well the average computer user at their site. On networks that I have managed, apparent account probe attempts are most often users simply typing their password incorrectly, usually with CAPS LOCK on.

On the "mystery" password policy network, I had forgotten my correct password and was eventually locked out -- permanently. I asked the well-meaning administrator why I was locked out and

what the policy was. “Three tries and the system will lock you out,” he replied. “For how long?” I quizzed. “Until I unlock it,” he said confidently.

What mistakes were made? First, the policy should have been published to all users, explaining what was expected of them and indicating the lockout policy.

Second, the lockout policy was a bad idea in this case. Here’s why. The company had a Secure Sockets Layer (SSL) web email access server tied to the NT domain login. This server was publicly available to the outside world via the Internet. All the email accounts at the company were identical to the login ID of the user on the network. So for an outsider to acquire the user’s login identifier, they only needed to see an email message to or from that user. Once they had the user ID, the outsider could attempt a bad password a few times and lock that user’s account from access until the administrator was called upon to unlock it.

We know that the three principles of information assurance are: confidentiality, integrity and availability. The password policy can aid in securing confidentiality and integrity, but the administrator failed to attain availability.. The password policy would enable an outsider to perform a denial of service attack on the company’s email server, which locked users out of their workstations internally. Once this was pointed out to him, he changed the policy to lock the user account for ten minutes after five unsuccessful attempts. The system would reset the account lockout for more tries thereafter. At that time, passwords would expire and were required to be changed every 90 days by the user.

A couple days later, a pronouncement came out via email with all the details on how passwords should be selected, how long they could be used, and what happens to the system if you guess too many times when logging in. This was good, because now the users were informed.

The administrator had read some material on the Internet, thought that the articles were good for the policy, and implemented them. The password now had to be changed every 30 days, and there was a number of other restrictions on the character to be used in the password. The account lockout was set to 30 minutes after 5 attempts. After some quick work with a calculator, I showed that even if a user chose an all lowercase English dictionary word (if the system allowed it), a cracker

performing a brute-force attack on the console of the workstation would only have a 1 in 30 chance of getting into the system during a 30-day period, assuming that they could work undetected.

There were several important items that were not in the password policy the administrator established. One is prohibiting the use of the "Save Password" checkbox found on so many products (dialup, Virtual Private Networking (VPN), browsers and email clients). The other is to require that users maintain an external access password that is different from the internal system passwords.

An incident comes to mind where a salesperson at our company had a laptop stolen from his home. Fortunately, he reported the theft rather promptly to police and the information systems group, but a number of password security breaches were on that laptop. There was no BIOS (hardware startup) password – the first line of defense on a personal computer, the operating system did not require an authenticated login (it wasn't capable), and the dialup access, email client and contact database access all had "Save Password" set. The thief would only need to start the laptop, dial in and start roaming the network, gathering information. This person worked at a high-technology company, so this was particularly surprising and disturbing. Apparently, it was not atypical.

Periodically, an external financial audit team will come in and recommend to our company certain information system policies when we are deficient. For the past several years, I have heard the "change your password every 90 days" requirement. That's fine, but that policy is only one of a list of requirements, duties and procedures that must be followed to ensure the integrity of the company's financial assets.

There is more to a password policy than simply changing the password every 90 days. Some companies have general password policies at the corporate level and then have each business unit define the policy further to align with their system capabilities. Others define the details policy for all units explicitly.

At the company where I am currently employed, I wrote a general password policy that informs the users and set the direction for each system administration team to set their local policies for the information that they need to protect. It tells users that they are responsible for safeguarding their passwords for access

to the computer system. That their individual passwords should not be printed, stored on-line (in plaintext), or given out to others. That users are responsible for all transactions made using their passwords, which makes them responsible for the systems they log into. It states that no user may access the computer system with another user's password or account. Another important point to make in the password policy is that passwords do not imply privacy inside the company or campus. The use of passwords to gain access to the computer system or to encode particular files or messages does not imply that users have an expectation of privacy in the material they create or receive on the computer system.

There may exist certain "global" or administrative passwords that permit an administrator access to all of the material stored on the computer system. Users are told that passwords must be selected such that they are not easy to guess, using a password with character combinations that meet the following minimum criteria: it must not contain a dictionary word, it must contain numbers and/or special characters if the system allows it, and it should be at least 6 characters in length. A blank password is strictly in violation of the policy.

It is clear that there is room for improvement in this and any password policy. Some things one might consider for this policy are more criteria on password dictionary word checking, password aging and expiration. But there is a balance on the security and user-friendliness of a system. Many users will balk at a password that isn't a dictionary word, but clearly that isn't a good choice.

An interesting debate is how to handle contract workers and other transient employee accounts. Some systems won't allow an account to automatically terminate on a specific date, which would be needed for employees on temporary assignment or contract work. One way to overcome this limitation is to require a manual process to re-affirm an account at the password expiration window. The person must provide some form of identification to have the account reactivated.

Here are some common characteristics to consider for password creation:
Minimum password length
Maximum password length (if applicable)
Number of unique characters
Number of alpha characters
Number of numeric characters

Number of punctuation characters
Maximum number of consecutive characters
Maximum instances of any character
Use of shifted (capital) letters (if applicable)
Number of old passwords retained for comparison
Algorithm for comparison with old password
Forbidden characters (those that the system will not allow)

It is important for administrators and security officers to always be aware of the human factors in having overly complex rules regarding passwords, as the users will become frustrated if their password is required to be changed frequently with arcane requirements. There is always a cost/benefit tradeoff, and the cost (in this case, effort placed on the employee) should certainly not exceed the value of the assets one wants to protect. An evaluation of the risks should be part of the plan.

Administrative passwords can be particularly tricky to maintain, and are a special case of the user password. Policies must exist to have the administrative passwords changed whenever there is a security breach or if an employee with that knowledge changes job duties or leaves the company. For system-wide administrative passwords, it is important to keep the number of individuals who know these passwords small. However, be sure to have the passwords listed on paper in a sealed envelope and/or in a lock-box for non-administrative access. It is recommended that a procedure exists for non-administrators to have access to the envelope and box.

Helpdesk procedures for password changes are very important to the secure operation of a network. Many corporate and university help desk operations rely on honesty to have a user's account unlocked or for them to request a password change. The social engineering issues with password changes and account lockouts should be planted foremost in the help desk employee's mind. Some common methods of authenticating users is to have them register a pass phrase or answer to a question that is independent of the user's login and password, yet is easily remembered or can be known only to the employee or user. Helpdesk personnel should not reissue passwords or unlock accounts without photo identification or a verifiable attribute.

Overall, the security administrator's duty is to reasonably ensure the security of the network. He or she can do this by: setting policies commensurate with the risks of losing data, financial damage, theft of information, public embarrassment and/or reduction in share/stake-holder value. The administrator

should set policies to cover how passwords are stored, how they are changed, the frequency at which they should be changed, and the fiduciary duties of the users, management and network administrators. Once clearly communicated, the password policies work toward a good start to security in the workplace.

References

Dekker, Marcel. The Froehlich/Kent Encyclopedia of Telecommunications Vol. 15., New York, 1997, pp. 231-255. http://www.cert.org/encyc_article/tocencyc.html

McGraw, Gary and Viega, John. Protecting passwords: Part 1, August 2000, URL: http://www-106.ibm.com/developerworks/security/library/pass1/index.html?dwzone=security

McGraw, Gary and Viega, John. Protecting passwords: Part 2, September 2000,URL: http://www-106.ibm.com/developerworks/security/library/pass2/index.html?dwzone=security

Microsoft Security Bulletin (MS99-056), December 16, 1999 http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/fq99-056.asp http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS99-056.asp

Computer Incident Response Guidebook, August 1996, Department Of The Navy, URL: http://www.nswc.navy.mil/ISSEC/Docs/P5239-19.html

Penn State Password Policy, March 2001, URL: http://www.psu.edu/computing/policies/password.html

University of Waterloo, UWaterloo Password Policy, May 2000, v1.8, URL: http://ego.uwaterloo.ca/~uwdir/policy/Passwd.html

How To Eliminate The Ten Most Critical Internet Security Threats: The Experts' Consensus, Version 1.33 June 25, 2001, URL: http://www.sans.org/topten.htm

Last Updated: July 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
Security Awareness Summit & Training 2017	OnlineTNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced