NetWrix
Systems Management and Compliance

# White Paper: The Business Case for Account Lockout Management

*written by*
*NetWrix Corporation*

## WARRANTY

The information contained in this document is subject to change without notice. NetWrix Corporation makes no warranty of any kind with respect to this information. NETWRIX SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NetWrix Corporation shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

## TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

http://www.netwrix.com
phone: +1.888.NETWRIX (888.638.9749)

Updated—August 20, 2007

# CONTENTS

# INTRODUCTION

How many help desk calls you get from users asking to reset their passwords? How much you spend on administrative staff just to handle account lockout issues? Loss of productivity, lots of frustrated users, huge administrative burden are just some of inevitable implications of implementing a strong password policy which is business critical to succeed today. You're not alone – recent research shows, in most organizations, more than 30% of helpdesk activity caused by account lockout issues. So, should you just give up to user complaints or there is a better way to keep up strong security requirements and effectively resolve account lockouts at the same time? Of course you can simplify password policies and reduce costs associated with your helpdesk, allowing easy to remember, non-secure passwords which never expire. But obviously, such practices make enterprise more vulnerable and introduce some other undesired effects.

This white paper covers account lockout management process and introduces new cost-effective workflows of account lockout resolution, describing significant ROI enterprises can achieve through the use of automated management solutions.

# Benefits and Disadvantages of Account Lockouts

Account lockout is the process of automatically disabling (“locking”) a user account based on certain criteria such as too many failed logon attempts. The purpose behind account lockout is to prevent attackers from brute-force attempts to guess a user's password - too many bad guesses and you're locked out.

On the one hand, account lockout provides a good base for implementing secure password policies as it makes quite impossible for an attacker to perform password guessing (also known as brute-force) attacks against user account passwords. Typical value for Account Lockout Policy (suggested by Microsoft in their Account Lockout Best Practices white paper[1]) automatically locks user accounts after 10 invalid logon attempts, preventing further logons for 30 minutes. Then after 30 minutes elapse, the attacker gets another 10 attempts, but obviously it will take thousands of years to successfully crack the password. Combined with Password Policy, namely ‘Maximum Password Age’ setting, which forces users to change password periodically (e.g. every 30 days), this creates virtually bullet-proof password security.

On the other hand, imagine the situation when user returns from long vacation and tries to remember his or her password, doing a number of guesses, and exceeds given number of attempts. Or the user can just mistype password 10 times at once simply because he hasn’t had his coffee yet. This makes account locked out and follows with a call to helpdesk, consuming expensive business resources, both in terms of the time spent resolving this issue and the loss of employee productivity. Password expiration brings another challenge – once password is changed, it gets updated in Active Directory, but nowhere else. What does it mean? Ideally, users change their passwords in the beginning of business day, during first logon. But in practice passwords expire at any time and the old password still remains in use in many places by active user sessions, batch processes, mapped network drives and others. Most complicated scenarios occurs when critical system services and scheduled tasks continue to use stale credentials constantly making their account locked out without giving any visual indication – the applications start behaving unpredictably and services will eventually fail.

[1] White paper is available at the following URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=8c8e0d90-a13b-4977-a4fc-3e2b67e3748e&DisplayLang=en

# THE CHALLENGE OF ACCOUNT LOCKOUT MANAGEMENT

Needless to say, account lockout is a must have feature for all modern networks and failing to implement that you are putting your entire organization's security at big risk. But how to deal with all complications related to account lockout issues?

Let's first divide common reasons for account lockouts into major categories and then describe typical workflows. Categories are:

1) Human factor - user mistyped or forgot his or her password.
2) Machine factor - system services, background applications and similar objects that use stale credentials.
3) External factor - brute-force attacks attempting to break your network security.
4) Other reasons - e.g. failure of Active Directory replication.

## *Human Factor*

Mistyped or forgotten password is the most common scenario, which happens all the time and creates many helpdesk tickets, however is quite straightforward to resolve: helpdesk person obtains account name from user, asks some verification questions (e.g. mother's maiden name or place of birth) and first tries to unlock the account, in case the user can still remember the password. If the user can't remember, helpdesk person sets new temporary password, user logs on and prompted for new password by the system.

Tricky part here is a secret question/answer pair – special database shall be maintained which associates user accounts and their secrets. If you don't implement verification procedure, you lose security, since potentially anyone can contact helpdesk, request password reset and easily logon to the network, gaining access to confidential business data. User verification is also a part of Sarbanes-Oxley (SOX) compliance with regards to secure organization environment.

## *Machine Factor*

As stated above, such issues arise when services and applications continue to use old password after it was changed because of password expiration policy requirements. New password must be applied to every place where account is referred, failing to do this results in account lockout, since programs accessing protected resources request authentication on domain controllers using old credentials and domain controllers enforce lockout policy. Other ways account can get locked out include:

- Stale logon credentials cached by Windows.
- Scheduled tasks setup under stale credentials.
- Network shares mapped under stale credentials.
- Disconnected terminal service sessions that use stale credentials.
- Users logging into multiple computers at once and changing password on one of them.

Resolution of account lockout in this scenario is much more complex and usually involves routine checking of every possible object which might be causing account lockout. Server administrators must update all references manually (e.g. set new password for service accounts and scheduled tasks, remap network drives, reset terminal sessions etc) and then unlock the account in question. Note this way may require multiple iterations to fix all possible references.

### External Factor

Brute-force attacks can pursue two possible targets: password cracking and logon prevention. In the first case, the attacker performs sequential password guessing, usually dictionary-based, which works for weak passwords, such as common cat and dog names, year of birth and some other typical words which people tend to use for passwords. In the latter case the attacker doesn't care for the user's password, but rather interested in preventing the user from logging on to the network or disrupting operation of some business-critical service, to create denial of service (DoS) condition.

These examples may seem somewhat contrived since they assume an attacker has physical access to the network, however new wireless technologies can provide perfect base for this.

Typical responses to such attacks include firewall-based blocking of IP addresses, MAC addresses and SSIDs of wireless devices.

### Other Reasons

Active Directory is a fail-safe distributed environment which involves usage of multiple authentication points (domain controllers). Along with many benefits this architecture introduces some weak points related to domain data replication and critical point here is account passwords. Whenever password is changed after expiration, it must replicated to all domain controllers within organization, otherwise authentication will work inconsistently – some DCs will use new passwords while others continue to use old ones.

First thing to consider is latency - replication is not instant, especially when it comes to multiple AD sites. Another thing is possible replication failures – network links break from time to time, domain controllers become temporarily unavailable and many other reasons can prevent replication to occur timely and properly.

## THE COST OF ACCOUNT LOCKOUT

Even the most efficient organization can spend too much on account lockout management. Typically almost one third of time is spent by IT departments for resolution of account lockouts and password issues. The time spent by IT personnel is only the top of the iceberg, as soon as lost user productivity and service downtime are taken into consideration.

It can be difficult to calculate exact cost of a single account lockout resolution, since it depends on organization and types of accounts affected. For user accounts, assuming that every incident takes 1 hour in average, both for IT person (time needed for investigation and unlocking) and user itself (lost productivity), the cost can be $50-$100 per incident. The most expensive part is service accounts – the cost of their lockout can vary from few hundreds to many thousands of dollars, depending on number of users affected by service downtime. But even in the best case, given the lowest numbers possible, it becomes evident that automated account lockout management solutions can quickly bring significant benefits and dramatically reduce associated costs.

# AUTOMATED SOLUTION APPROACH

Is there any way of minimizing expenses associated with account lockout management? The answer to this question is automation - specialized software solution capable of doing most routine work related to account lockouts - detection, identification of reason and resolution. Combined with improved helpdesk workflow, this can reduce implementation costs dramatically. Primary goal of such solutions is to simplify common tasks performed by helpdesk personnel and decrease average time required to resolve account lockouts.

Typical non-automated resolution workflow usually looks like this:

1. User receives 'account locked out' error and calls helpdesk.
2. Helpdesk verifies user, unlocks the account, and optionally resets password. Unlock and reset operations must be done on domain controller closest to the user, otherwise the account could be locked out once again.
3. If the problem persists, user calls helpdesk once again and asks for further investigation.
4. Helpdesk person performs routine lookup of possible sources of account references, which might be causing the account to become locked and asks user to fix them.
5. After checking all account references, helpdesk person unlocks the account.
6. If the problem persists anyway, steps 4 and 5 repeated until all causes are fixed. For example, if task scheduled to run weekly uses stale credentials, it will cause account to become locked out each week until updated with new password.

Improved automated workflow would look like this:

1. Helpdesk personnel are automatically notified when account is being locked out, even before user picks up the phone.
2. Software performs routine scan of account references and reports this information to responsible helpdesk person.
3. User calls helpdesk and, after verification, helpdesk person either provides a list of account references which need to be fixed and/or performs reset password/unlock operation (solution automatically does this on closest domain controller to avoid replication issues).

Apparently, improved workflow includes fewer steps, takes less time to complete and has one important advantage – account lockouts are handled pro-actively – helpdesk team start resolving them even before frustrated user gives a call. Total number of lockouts decreases significantly, since all possible lockout reasons get eliminated at once, without any further reoccurrences.

Additional benefit of specialized solution will be simplicity of user interface with minimal learning curve, to avoid hiring expensive high-skilled IT personnel or educate helpdesk personnel to use complex administrative tools like Active Directory Users and Computers and many other programs required to perform this task. They will use only one tool, easy to use and narrowed down to the problem area. Good solution should also allow web-based helpdesk access, which is a simple to deploy and very cost-effective approach.

# CALCULATING RETURN ON INVESTMENT

Let’s estimate ROI for automated account lockout management solution based on most optimistic numbers for 1000-user company as an example.

### ASSUMPTIONS

| | |
|---|---|
| Number of regular users | 1000 |
| Number of IS/IT employees | 4 |
| Average IS/IT employee salary / hour | $25 |
| Average number of account lockouts for each user per year | 4 |
| Time needed to resolve account lockout without automated solution (in minutes) | 20 |
| Time needed to resolve account lockout by means of automated solution (in minutes) | 5 |
| Cost of automated solution (per admin user) | $300 |

### COSTS

| | |
|---|---|
| Annual cost w/o automation | $33’000 |
| Annual cost with automation | $8'300 |
| Software investment | $1’200 |

### ROI ANALYSIS

| | |
|---|---|
| 1 Year ROI / Savings | $23’500 |
| 3 Year ROI / Savings | $70’500 |

# CONCLUSION

On the one hand, account lockout policy is a must have requirement for most organizations, on the other hand account lockout resolution is a very challenging task, which consumes many IT resources and introduces additional costs. The benefit for implementing an automated account lockout resolution is significant. Improved management workflow combined with specialized software solution reduces costs, brings security enhancements and ensures compliance.

NetWrix Corporation offers the Account Lockout Examiner to address major account lockout challenges, including ones described in this white paper. Please visit www.netwrix.com to learn how this product can meet requirements of your organization and request your free evaluation.

# ABOUT NETWRIX Corporation

Established in 2006, NetWrix Corporation provides innovative and cost-effective solutions that simplify and automate systems management and compliance. With in-depth knowledge and experience in managing IT environments of all sizes, the company delivers solutions to meet complicated business requirements while fulfilling the highest expectations of IT professionals. NetWrix Corporation is a privately held company headquartered in Paramus, New Jersey.

## Contacting NetWrix

Toll-free Phone: 888.638.9749
Web site: www.netwrix.com
Address: 140 E. Ridgewood Ave
Suite 415 South Tower
Paramus, NJ 07652

## Contacting NetWrix Support

Technical support is available to customers who have a trial version of a NetWrix product or who have purchased a commercial version and have a valid maintenance contract. Contact NetWrix Support at http://www.netwrix.com/support.

# NOTES