Mike Nelson – SED article

Self-Service Password Reset in the Enterprise

Passwords have become a mandatory addition to our lives over the last few decades, and are even more prevalent now with the advent of being able to do almost anything and everything online. From your personal banking to your online purchasing to your social media accounts, passwords are required for it all. And almost all of those online services do provide some sort of self-service password reset functionality, in in almost immediate fashion, for you to use if you forget what it is. So, why are some companies reluctant to implement these same solutions for their end-users?

There have been many studies done and articles written about the amount of time and resources that a Helpdesk person, or even system administrator, spends over a period of time providing a service of account password resets. Forrester Research estimates that on average the cost of a single password reset done by the Helpdesk is about $70. Gartner estimates that between 20% to 50% of all helpdesk calls are for password resets. It's pretty much a given that if you can relieve the burden of these calls from your I.T. staff, you can be much more productive on other areas that need their attention, and reduce those costs from your budget.

Many I.T. departments face the challenge of changing corporate cultures and moving forward to a better, more efficient, less costly, and faster way for users to get back online, without waiting on hold. One of the factors that have been limiting the acceptance of such a solution for the end users is actually the users themselves. In many corporate cultures, many non-technical users have a set routine that they follow and change for them is difficult, even for such a quick and easy fix. Some just do not like to pick up the phone and make that call to the Helpdesk or fill out that online ticket. Users who are more techno-savvy tend to have already been exposed to this mostly during their education, and their general daily life online, so it is an easier adjustment for them, and may even be a huge sigh of relief for some. Understanding what and who your user base is and how they work is critical to implementing a solid solution.

There are many different products on the market that provide some sort of password reset functionality for the corporate domain, and have many different scenarios and solutions. In simplest form, there are three primary components to almost every solution, the enrollment process, the authentication method used, and the mechanism to reset the password itself. There are many additional functions that software vendors add, such as account lockout reset and more, but they tend to add complexity to the solution rather than simplify it for the users as well as the I.T. staff.

The method that is used for authentication is the most important for you to look at, understand, and implement well. The most common is called Fallback

Authentication, or the method of presenting the user with any number of personal questions that they must answer correctly to be given a password reset. One issue that arises when implementing such a solution is that by providing your users with this type of service and functionality, you are introducing another avenue of possible vulnerability to your domain network. This has been very well studied in the online world of the internet, focusing on such sites as Facebook as an example in an article written by Ariel Rabkin at UC Berkley, but not so much studied inside the corporations. It would however be naive to assume that in this age of technology that the threats that are introduced outside the company could not be implicated and used inside the company as well.

There are solutions that provide an even higher level of security, for the company as well as the user, that utilize such authentication methods as tokens, assisted methods, and PKI. I found the assisted method interesting as it relies on someone who "knows" you, such as a manager or co-worker, to also enter their credentials to allow for the password reset to proceed. While this may be an inconvenient method to some, especially for people who are outside the corporate network, it is more secure and reliable than simple personal questions. Secure tokens and PKI are even more secure methods to date, but do require the backend infrastructure to support them and tend to be higher maintenance, both administratively and in budgets.

In the end, as the mantra we I.T. people live by says, it's all about the user. The real truth is though, if we can make the users lives easier, it doesn't necessarily make our jobs easier. Introducing a self-service password reset system in your company may take some time and some extra user education, but the payoffs will be a lower I.T. budget, happier and more productive I.T. staff, as well as users who will feel a new sense of empowerment from I.T. that frees them from having to make that dreaded call to the Helpdesk.

Useful Links –
Mandylion Research Labs Password Cost Estimator -
http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm
Love and Authentication Whitepaper –
http://www.ravenwhite.com/files/chi08JSWY.pdf

Some Products -
Forefront Identity Manager (Microsoft)
http://technet.microsoft.com/en-us/edge/Video/ff945082
Citrix Password Manager
http://www.citrix.com
Psynch (Now Hitachi ID)
http://www.psynch.com/technology/user-interfaces.html
Specops
http://www.specopssoft.com/products/specops-password-reset
Toos4ever
http://www.tools4ever.com/products/self-service-reset-password-management/