Ad password policy planning essay sample

Unit 7. Assignment 1. AD Password Policy Planning

To: Business Manager

A reasonable approach for an AD password policy, this will be determined by how, & what your ideas are and what your trying to accomplish. I know that you'd mention that a competitor has recently been hack into and security is the number one thing that should be addressed. This does not have to mean that you have to lose productivity over trying to secure your networks information. Simple measure like user names and passwords can be used to protect less sensitive information however how strong you make those usernames and passwords can have a great effect on how well your information is protected.

An effective password requires a necessary degree of complexity. Three factors can help users to develop this complexity: length, width & depth. Length means that the longer a password, the more difficult it is to crack. Simply put, longer is better. Windows, for example, is not always case sensitive; meaning it doesn't know the difference between ' A' and ' a'. Some operating systems allow control characters, alt characters, and spaces to be used in passwords. Here are good examples to use for secure practice:

1. uppercase letters such as A, B, C;
2. lowercase letters such as a, b, c;
3. numerals such as 1, 2, 3;
4. special characters such as $, ?, &;

When planning password policy’s stress extra protection, in some cases, a good password is enough protection to keep out intruders. In others, it’s just a start. Encryption and one-time passwords add extra protection to systems. Encryption means garbling the password to protect from sniffers or other onlookers, through a particular scheme that can be deciphered from the other end of the connection. Users should exercise extreme caution when writing down or storing passwords. Stories of hackers obtaining passwords through shoulder-surfing and dumpster diving are not urban myths, they are real. Here a good practice for a company to use, In order to ensure their ongoing effectiveness, passwords should be changed on a regular basis. Changing passwords securely is fairly simple. Windows passwords are changed through the Control Panel and in UNIX, the ‘ passwd’ command generally does the trick. Remember that in the “ Active Directory Users and Computers” you can make the user adhere to certain password policies like Password length, complexity, and expiration if you want them to change their password every month. I hope these tips help you make your network more secure without having to go out and spending a bunch of money, if you have any questions or concerns please contact me.