Password guidelines for SME

Computer system and network security are crucially dependent on handling passwords correctly. The implementation of password guidelines or a password policy regulates creation, safekeeping and usage of passwords in an organisation.

The most important points to remember:

- Draw up a list of all password-protected system and application access options in your organisation.
- Establish a password policy for all system and application access options identified, stating your requirements for the creation, safekeeping and usage of all passwords.
- You should undertake periodic checks for strict adherence to your password policy.
- Sensitise all your employees to the dangers posed by improper password use.

Why is a password policy necessary?

The combination of a user name with a password is still the most widely used method of authentification and authorisation in any digital operating environment. For instance, this serves to confirm a user's identity and to implement access protection when accessing networks, logging into computer systems or using third-party services and applications. User names and passwords therefore play a central role in cyber security.

It is not surprising then that cyber-criminals do their utmost to obtain this much sought-after information by means of hacking, phishing or social engineering and to then take on the digital identity of their victim this way.

Users however are so familiar with the use of passwords that they quite frequently are not sufficiently aware of the risks involved. In an organisational environment in particular, a clear password policy providing users with clear instructions and protecting them from errors in this regard is therefore vital.

What is a password policy, and how do you create an effective one?

A password policy is defined as a set of rules drawn up to increase cyber security by encouraging employees to create secure passwords, to store them safely and to use them properly. A password policy is part of the official rules of an organization and should be part of any security awareness training programs.

It should be customized in accordance with the needs (of the complete system environment) and requirements (on a security level) of any organization so to ensure you achieve optimum effectiveness with reasonable effort. A first step should therefore consist of drawing up a list of all password-protected systems and application access options in an organisation and to assess the protection levels required. All access options thus identified will then have to be considered when drawing up suitable rules inside a password policy.

To be able to cope with the ever-changing threat situation, the password policy should be subject to periodical checks for continued relevance and effectiveness.

Which are the most important aspects of a password policy?

A password policy extensively regulates how passwords are handled inside an organization. It provides users with specific instructions and covers the following:

1. Use of passwords

As mentioned above, it is often already sufficient to know a password to completely take on someone's digital identity. You should generally therefore take all measures necessary to prevent any fraudulent use of this information.

Passwords are therefore strictly private and must be treated confidentially. Below some points to be particularly aware of:

1. Passwords must neither be passed on actively nor shared nor stored in a place open to the public.
2. Passwords must always be stored and transmitted in encrypted form.
3. When entering passwords, make sure that this process cannot be overlooked by third parties.

A password policy establishes guidelines on the use of passwords by way of a directive.

2. Password strength

The strength of a password is a measure of how difficult it will be for an attacker to discover a password unknown to them by simple guesswork or trial and error. The more unpredictable and complex and the longer a chosen password is, the stronger and hence more secure it is.

A good password policy emphasizes the creation of strong passwords by requiring users to make their passwords longer and less predictable (see our instructions on "Secure passwords" (http://www.ebas.ch/step4#passwords)).

In addition, the creation of strong passwords should be supported by providing technical tools, such as password managers (http://www.ebas.ch/step4#passwords) and stipulated in the password policy.

3. Password expiry

It is very simple to transfer passwords – something which over time can also result in them ending up in the wrong hands. Employees for instance sometimes pass on passwords to third parties without thinking or note them down in unprotected places. User passwords can also be disclosed unintentionally though as a result of data breaches. It is generally impossible to reclaim any leaked data.

In any such cases, changing passwords is the only effective measure to restore cyber security since this will render any leaked information useless.

The renewal and administration of passwords should be arranged for with the help of technical tools, such as making support from a password manager utility available.

4. Password history

Users tend to reduce the number of passwords they have to remember, for instance by reusing passwords they have used in the past. Cyber criminals exploit that kind of behaviour by regularly using lists with old passwords when carrying out their attacks. To make this impossible, users should be prevented from reactivating old passwords.

A password policy will ensure that systems keep track of a user's password history and check for reuse of old passwords when these are changed.

5. Password changes

Users should be able to change their passwords at any time and by themselves. However, you will need to ensure that such password changes are exclusively initiated by legitimate owners and not by attackers.

A password policy establishes the technical and organisational framework conditions providing for secure password changes. The introduction of two factor authentification for instance can render the process of changing passwords considerably more secure.

Passwords are still the most widely used security component of access protection in a digital environment. It is not surprising then that cyber-criminals do their utmost to obtain this much sought-after information by means of hacking, phishing or social engineering.

Password guidelines (or a "password policy") ensure clarity and certainty when handling passwords!