datel

expanding the world of sage

Network Security Recommendations

1. Accounts

There are generally two kinds of accounts used in a Sage installation. There are the actual user accounts used for logging onto the servers or connecting via remote access and there are the accounts that are used to run software automatically, e.g. via services.

For accounts used to run services, Datel makes the following recommendations:

- Where possible make these domain level accounts to avoid permissions issues if access to other machines is required
- Set the account so that the password never expires
- Remove it from any group policy configuration that may attempt to force a password or policy change
- Remove any login or remote access rights for the user so they cannot actually be used to log onto a server.

For accounts used to access servers, including any used by Datel or other third parties to connect remotely, Datel makes the following recommendations:

- Do not use the domain administrator account for any routine access and do not allow third parties to access your system using this account, unless they provide a domain administration function
- Each third party should have a single login that only they use. This should have local administrator access to any machines that are required by the third party, so for example the account used by Datel should have local administrator access to the Sage server
- These third party accounts should ideally be set with a password expiry that allows the third party to change the password themselves when it expires; this avoids access being lost if the account is disabled when the password expires
- Passwords for the domain administrator and any account that is allowed remote access should be sufficiently complex to be secure (see point 2 below)
- Any passwords for these accounts should be changed on a reasonably regular basis. Changing too often can add an administrative overhead, particularly as any third parties would need to be notified of the change, but each password should be changed at least once a year.

2. Passwords

Choosing a suitable complex password is not straightforward; the password needs to be complex enough that it cannot be discovered easily by simply trying lots of passwords, but also needs to be something that is easy to memorise and relay. A password that is just random characters or is too complex is less secure than a memorable one as people need to write it down for themselves or email it to communicate it.

Here are some recommendations for choosing passwords:

- Avoid simple dictionary words or names. Particularly avoid ‘password’, ‘Password123’, ‘p455w0rd’ and the like
- Substituting numbers for letters increases the complexity but avoid obvious substitutions, e.g. 4 for ‘a’ or 5 for ‘s’
- Prepending a number is more secure than appending a number. If you do this avoid obvious numeric prefixes or suffixes e.g. 123. Inserting a number into the password is even better.
- Punctuation marks increase the complexity of the password, even better if they are not ! or ?
- The longer the password the more secure it is (as long as it’s memorable)
- Space is a valid character in passwords (except at the beginning or end)
- Avoid generating a new password by taking the old password and incrementing any numeric portion.