Adminizer – Techinical summary

Windows Security relies totally on the fact that end users should not have administrative rights to their computers. For example these facts give a good example of this problem:

- **There is no possible way to prevent a local administrator from reading and changing local files**
- **The company issued policies such as Group Policies can be ignored by anyone with administrative rights**
- **There is no way to prevent users from running unwanted software on their computers**

Other ways to manage user's passwords rely on online connections and aren't very secure:

- **SCCM, Altiris etc can easily manage the users password when the computer connects to the network but don't work when working offline**
- **Group Policy can be used to administer passwords but it relies on online connection, transmits the password over the network and can be easily cracked to plaintext format with for example PowerShell**

Based on this it is easy to understand the need to zero down the amount of computers that need their users to be administrators to for example run business critical apps or to change settings such as local IP-address' to maintain an external system.

Adminizer changes the way administrative rights are given to a user from a session lasting or permanent to a onetime only. Adminizer gives the company ability to provide administrative rights to a user for a single operation or a single logon session in a way that can be achieved 100% offline – no connection to Internet or Intranet is required. As it works totally offline it never compromises the password by transmitting it over the network.

The add-on bonus that Adminizer gives you is that you can forget about changing the local administrator passwords for the next four to eight years – easily a lifetime of a Windows installation! Microsoft does offer management via Group Policy Preferences but the method is child's play to decrypt and makes your environment unsecure.