Timber Line Electric & Control Corporation -

Loading Microsoft Updates: The "May 2017 Roll Up"

When it comes to computerized SCADA systems, Districts should have a plan on when and how to accept/apply Microsoft updates. When Microsoft releases an update, (usually at 2:30 AM on a Tuesday or Wednesday), it will be the first time any of us have seen the information. That means that GE (iFix), Rockwell (Allen Bradley), Specter (Win911) are also seeing it for the first time. Occasionally, the MS updates are incompatible with the existing control software and can cause minor or major issues with SCADA computers. To try to solve this, most SCADA computers have the automatic updates turned off completely, or the computer will accept the update and not apply it until a human approves the download. This gives the software companies a few days or a few weeks to check compatibility and make any changes to their programs to assure happy commingling of programs.

Just about the time we are all comfortable with this procedure a nasty malware or ransomware is spread on the internet and Microsoft responds with a security patch. It is often bundled with other MS patches. At this point all IT professionals groan because they have the choice of risking a virus infection, or loading an unproven update that might cause problems. Generally, if Districts strictly follow the suggestion to NOT use the SCADA computer for any other purpose, the risk of a virus infection is very low. But if many people have access to the SCADA computer (especially those Districts that have night shifts), then the chance of someone using the SCADA computer for internet access increases.

As of the first week of June, we are recommending that Districts accept/apply the **May 2017 roll up**. This release offers security patches for some ransomware. Be aware that ransomware can be spread over a network so any computer on a District network can be the entry point for a nasty malware infection.

Generally, we offer the following suggestions:

1. Have a current backup of your system that is no more than one week old. If your District is generating lots of data, then a daily or twice daily backup is appropriate.

2. Send these suggestions to your IT provider.

3. Remove the internet browser icons such as Chrome and Edge from the SCADA desktop (monitor display). This makes it more difficult for a bored operator to access the internet.

4. Remove any email service such as Microsoft Outlook from SCADA computers.

5. Never load new software (such as a PDF reader or video player) on a SCADA computer.

6. Check with Timber Line before applying an MS patch.

7. Do a complete backup before loading an MS patch.

8. Avoid loading patches on a Friday afternoon. Preferably, call Timber Line before loading a patch to make sure we have someone available to help if your SCADA software quits working.

9. Then, smile broadly when everything works! You did your due-diligence!

Kim Evezich
Timber Line Electric & Control Corporation
303-697-0440