Cyber-security: Whitelisting with e-terra software solutions

06/02/2016 - 3.36 pm

CYBER-SECURITY NETWORK MANAGEMENT
OIL & GAS

Cyber-attacks are becoming increasingly frequent and virulent. The power networks need to have an in-depth defense strategy to protect them against such attacks. Whitelisting is a key component of such a strategy.

Post a comment

Source: ThinkStock

Wednesday December 23, 2015. 3.30 p.m. People in the Ivano-Frankivsk region of Ukraine were preparing to go home from work. Suddenly, three power distribution centers went mute, tripping some 60 substations. That left around 230,000 residents in the cold and dark.

The outages were the result of an unprecedented cyber-attack—the first to take out a power grid—launched by some very skillful hackers. Despite the limited damage caused, the episode demonstrates that cyber-attacks to control systems have stepped up to another level—well planned, multiple-step and highly sophisticated.

The attacks have highlighted the need for very effective cyber-defense mechanisms to protect control systems. Whitelisting is a security solution that represents a key layer in a global defense strategy. Sharon Xia, GE Grid Solutions principal software architect, explains: "Whitelisting is the opposite of anti-virus software. The latter is a blacklisting solution, detecting and quarantining known—but not unknown—malicious code. On the other hand, whitelisting assumes that everything is bad unless

told that the application is authorized and safe to run. It prevents malware because it refuses to allow all unwanted software—known or unknown. As a result, it is much more effective than the anti-virus approach."

e-terra tested

To help utilities to protect their applications more tightly, GE Grid Solutions has tested the industry-leading whitelisting solution, Intel's McAfee Application Control, on its **e-terra** Energy Management System and **e-terra***pipeline*. "This was a proof-of-concept test," Xia points out, "with the objective of verifying that McAfee Application Control is compatible with the Grid Solutions products." The test results have demonstrated that it is technically feasible to use an application whitelisting solution in e-terra systems. Utilities can now deploy the McAfee solution in the knowledge that it will function correctly. "In fact, one **e-terra***pipeline* customer has already deployed it," says Xia, "and other customers have expressed interest, especially after the Ukraine attack."

Setting up for security

There are, of course, a number of precautions to take when configuring a whitelisting solution. "This demands a certain investment in time and resources, but that is well worth the effort considering the benefits," says Xia. The first step is to build an application whitelist on each host in the system. Some application whitelisting solutions are able to pull the list off the host automatically. However, the list should be reviewed to make sure that all required applications and binaries are listed, and none of the unused applications are in. It is a good opportunity to baseline the system while creating the whitelist.

Another key step is testing. A thorough functional test is required to ensure system availability. Different application whitelisting solutions support different testing modes. The McAfee Application Control[1] solution supports "Observe" mode. When running in this mode, it emulates "Enabled" mode, except that it records observations rather than preventing applications or code from running. Each observation is logged and corresponds to the action McAfee Application Control would take in "Enabled" mode. "We recommend that customers run the whitelisting solution in 'Observe' mode after the

baseline whitelist is established, conduct a full functional test for e-terra applications, review the log, and adjust the security policies in Application Control, if necessary," Xia explains.

Because application environments are dynamic, whitelisting deployment needs to be underpinned by a software patch and update process. This means that any application whitelisting solution has to be set up to allow planned software updates and patches, otherwise the system may simply stop working. The McAfee Application Control program includes mechanisms to do this. For example, after adding the Grid Solutions certificate as a trusted supplier, all software signed by that certificate can be run, including installation kits and upgrade kits. "However," adds Xia, "to be on the safe side, we recommend a thorough functional test after each software update or patch. In fact, continuous monitoring of application health is crucial in ensuring that all applications run as they should. In any case, GE Grid Solutions consultants are available to help customers install, run and monitor the whitelisting solution."

[1]: McAfee Application Control is a trademark of Intel

RATE THIS ARTICLE

COMMENTS

LEARN MORE

EXPERTS

Sharon XIA, CISSP-ISSAP

Grid Solutions – Principal Software Architect

SEND A MESSAGE TO OUR EXPERTS