Guidance for Running Antivirus Software on SEL Computers in the Electric Sector

Huba Leidenfrost, CISSP

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Malicious Software Prevention Requirement (CIP-007-R4) requires electric sector asset owners to employ malicious software prevention tools on assets within the electronic security perimeter. Companies considering running antivirus products on SEL computers within the electronic security perimeter should proceed with caution. This application note guides the reader to the National Institute of Standards and Technology (NIST) Special Publication 1058, which contains information on the impact of antivirus software on control system equipment. This application note is intended to aid asset owners in antivirus decisions to minimize impact on critical processes.

PROBLEM

Antivirus solutions can be divided into two categories: blacklist and whitelist. Traditional blacklist (signature-based) antivirus products perform system scans, which use central processing unit (CPU) time and inhibit the performance of high-availability applications.

NIST and Sandia National Laboratories designed a series of laboratory performance tests using blacklist antivirus products and came to the following conclusions, supported by industry feedback.

> The major findings from the [NIST] laboratory tests are as follows:
>
> - Manual scanning, also known as “on-demand” scanning, has a major effect on control processes, in that they take CPU time needed by the control process (sometimes close to 100% of the CPU time). Minimizing the [blacklist] antivirus software throttle setting lessens, but does not remove this effect.
> - Active scanning, also known as “on-process” scanning, has little or no effect on control processes.
> - Signature updates can also take up to 100% of CPU time, but for a much shorter length of time than a typical manual [blacklist antivirus] scanning process. [1]

A computer CPU that runs near 100 percent capacity can compromise the functions of the device for which it is intended. These issues should be considered when making decisions on the installation and configuration of blacklist antivirus software on computers integral to control system operation.

SEL Solution

When deploying blacklist antivirus products, use NIST Special Publication 1058 for guidance on configurations that limit impact to high-availability applications.

Alternatively, asset owners should consider employing a whitelist antivirus solution. A whitelist antivirus solution runs a baseline on the system. New applications are prohibited from executing after the baseline. Whitelist solutions reduce impact on performance and work well for systems that are static, isolated, and accessed infrequently. Unlike blacklist antivirus solutions, approved applications are allowed to execute, and no other applications may run. This provides protection against zero-day vulnerabilities and avoids the problem of constantly updating virus signatures.

Reference

[1] J. Falco, S. Hurd, and D. Teumim, "Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts," NIST Special Publication 1058, September 2006, p. 1. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=823596.

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com