Computing Platform Security Tips

SEL understands the importance of security for SEL computing platforms. Please take a moment to review some tips to keep your computing platform secure. Your company computer security policy should take priority over any of these suggestions.

Recognize That an SEL Computing Platform Is Not a Protective Relay

Unlike protective relays, computing platforms need to have the operating system safely shut down before removing power. This shutdown will increase the reliability of your computing platform. Computing platforms with the enhanced write filter (EWF) need to have any changes saved before powering the system down or those changes will not be preserved.

Secure Your System and Set a Baseline

SEL uses a National Institute of Standards and Technology (NIST) guide (http://csrc.nist.gov/itsec/guidance_WinXP.html) in securing Microsoft® Windows® XP-based computing platforms. Most guides recommend disabling ports and services that are not in use. Consider a benchmark such as the Center for Internet Security (http://benchmarks.cisecurity.org) when creating your own security baseline. Use your baseline to assess computing platform changes and measure risk. Consider using the items below as part of your baseline.

Protect Against Malware

SEL computing platforms are malware free from the factory, but will not stay that way without proper precautions. Antivirus and whitelisting applications help prevent infections. Antivirus applications, while relatively easy to set up, require frequent updates. Whitelisting applications must be carefully configured, but require fewer updates and have little impact on performance.

Restrict Entry Points

USB and network shares increase your risk of malware infections and data leakage. To minimize risk, be careful about what you plug into your computing platform. If you must use USB or network shares, then define a safe process for USB and network share use.

Use the Firewall

On most computing platforms the firewall is enabled by default. This is the preferred setting and provides another layer of security for your computing platform. Ensure that the firewall is enabled, and minimize the number and scope of exceptions.

Limit Services and Rights

Malicious software exploits rights and services on the computing platform. Only enable services that are absolutely necessary. Improve computing platform protection by reserving administrative accounts for specific maintenance and installation tasks.

Change Default Passwords

Change the default computing platform passwords and follow strong password selection guidelines. To maintain multiple passwords, consider using an encrypted password vault application as permitted by your company's security policy.

Limit the Use of Third-Party Software

Only install the necessary software for your intended functions. Installing software changes your security baseline. Double-check security settings and make a new baseline after installing new software.

Employ Network Architecture to Your Advantage

Do not connect directly to the Internet. Leverage network architecture to protect your computing platforms. For example, limit network access with security gateways, firewall rules, and access control lists (ACLs).

Use Encryption When Possible

Enable encryption where feasible to prevent communications channel eavesdropping and hijacking and to protect critical data.

Test and Apply Software Updates

SEL monitors Microsoft's Security Bulletins* for security vulnerabilities that may impact the Microsoft Windows embedded operating systems and issues security updates when appropriate.

Test and apply updates on noncritical computing platforms before deploying to all company computing platforms.

*SEL does not distribute security updates for operating systems that customers can upgrade directly from the operating system vendor. For example, customers can update Windows 7, Windows Server 2008, or Windows XP Professional directly via Microsoft Update.

Consider Physical Security

Verify that only authorized personnel have physical access to the computing platform. Physical security is extremely important in maintaining a secure environment.

Utilize Logs and Alarms

Configure and regularly review computing platform event, network traffic, and alarm logs, which contain useful information for discovering potential threats. Use eventid.net to help understand Windows event log entries. If possible, forward a copy of computing platform logs to a central location for more in-depth review and automated notification.

Back Up Your System and Settings

Back up setting and data files periodically. A complete computing platform backup is preferred because it enables quick recovery from computing platform failures. Data recovery and downtimes can be very expensive. Backing up your computing platform, and more often your configuration settings, can shorten downtime. Ensure backups are stored in a safe and secure location.

PLS00065

Schweitzer Engineering Laboratories, Inc.

Date Code 20120228