Industrial control systems need a new approach to IT security

Comapny guides

Advice on best practice is available from many sources, including ISA 99, Industrial Automation and Control Systems Security, which is the first standard to cover industrial controls system security.

Vendors such as Siemens, Rockwell Automation, Cisco and Mitsubishi Electric have also produced guides to security and networking. Siemens' white paper Security concept PCS 7 and WinCC - Basic document provides a set of recommendations for creating secure networks for plants, with the aim of facilitating co-operation between IT administrators and control engineers.

Cisco provides an overview of threats to manufacturing networks and a solution based on the ISA 99 standard in a white paper Cisco Ethernet to the Factory Solution: Securing Today's Global Networks in Industrial Environments. This is expanded upon in the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide published jointly by Cisco and Rockwell Automation.

More recently, Mitsubishi has published a white paper Security - Tackling Emerging Threats to Manufacturing and Process Control, in which it argues that there are security benefits in using control systems based on PLCs rather than PCs.

Portable memory

One of the infection routes used by Stuxnet was USB memory sticks, and these devices have also been known to spread other malware.

An interesting solution to this problem, aimed at OEMs requiring secure transfer of data, is the Ruggedrive memory tokens and receptacles from Datakey Electronics (Fig. 2). These are physically daifferent from consumer USB memory sticks to provide a base level of protection.

From a customer perspective, an alternative approach might be to issue company USB memory and control its usage, while ensuring that each device is scanned for malware prior to use on control systems.

With Windows Group Policies, it is possible to prohibit USB memory use, or permit the use of just a particular brand and type.

Applications are also available to disable the Windows auto-run feature on DVDs and USB memory. More sophisticated applications such as Endpoint Protector from Cososys enable centralised control and include reporting functionality, the ability to enable/disable specific USB devices and to force encryption of data to prevent its loss.

Norman Data Defense Systems offers a number of means by which organisations can protect against potential threats. Norman Network Protection (NNP) is a network gateway appliance that is simply added to the network and to perform real-time malware scanning, malware isolation, outbreak prevention and damage control.

With Norman Device Control, organisations can enforce USB security for removable devices, and also provide encryption and port protection.

Pages 1 | 2 | 3 | 4 | 5 | Next »

Tags:

design , **computer systems and software**

Related Stories

- 30/03/2009 - Securing industrial control systems against threat of cyber infection