

No chance for Stuxnet & Co!

How industrial systems can effectively protect themselves against cyber attacks

■ Since the attention aroused across the globe by the Stuxnet worm that infected tens of thousands of engineering and visualization PCs and the controllers of industrial plants, the risks associated with malware and insufficient IT security within automation networks can no longer be overlooked. Solutions for industrial network security provide protection by preventing unauthorized external manipulations and network access.

The Stuxnet computer worm has caused a worldwide sensation since its discovery in June 2010. This cyber attack is the first publicly-known, targeted rootkit attack on industrial plants. Tens of thousands of PCs became infected and then passed on the malicious program code without it being discovered. The intention of the computer worm was to manipulate Windows-based

automation software in order to infiltrate malicious codes into the controllers of special industrial plants.

The actual danger today is much wider-ranging than Stuxnet alone. The methods used by this worm have been sufficiently analyzed and the corresponding detection signatures are known to the manufacturers of anti-virus software. However, IT security specialists regard copycat mutations as a serious risk.

While Stuxnet was programmed to target only a specific type of programmable logic controller (PLC) of one manufacturer with a very precisely defined configuration, mutations may also be able to infect components from other manufacturers. The risks inherent to this for operators and the plants affected could be considerable.

One lesson learnt from the Stuxnet attack is that conventional virus scanners do not provide any routine protection against attacks of such quality. Analyses of the malicious code have shown retrospectively that the worm was already in circulation for at least 12 months before it was even discovered. It was not detected by anti-virus programs during this time because it

did not have any signatures to be recognized by.

To develop suitable protection measures against attacks by the Stuxnet worm and potential mutations, it is necessary to understand its mode of operation. The worm develops its adverse effects in four stages and on various levels:

1. Infection of Windows PCs: The worm uses a mixture of aggressive mechanisms to spread

into and infect Windows PCs both via network connections as well as via USB memory sticks.

2. Misuse and manipulation of automation software: If Stuxnet is on the WinCC visualization system or the Siemens STEP 7 engineering software installed on the infected PC, it manipulates WinCC databases and STEP-7 projects it finds there to ensure its further spread and continued existence on the PC. The controllers detected in the projects are identified out as potential targets for stage 3.

3. Infiltration of malicious code into controllers: Via a manipulated system library, Stuxnet can infiltrate any malicious code into the configured controllers, then hide these manipulations from the developer, and protect itself from being overwritten.

4. Communication with servers on the Internet: From the infected PC, the worm attempts to

Stuxnet mutations are the actual danger



Following the Stuxnet attack, even the operators of industrial plants have to pay serious attention to IT security

establish communication with several servers on the Internet. If contact is made, then spyware can deliver stolen information and new instructions, and updates for the worm itself can be received and run by its “digital bomb”.

But the operators of industrial plants are not defenseless against cyber attacks. Innominate, a company within the Phoenix Contact Group, has developed with mGuard a technology with a range of preventive and diagnostic functions with which un-

authorized network attacks and manipulations within computer systems can be reliably detected in real time. This increases security against attacks similar to Stuxnet and reduces the associated risks.

► Continued from page 1:

Protect industrial systems against cyber attacks

Immediately detect malware: mGuard Integrity Monitoring

Using the mGuard CIFS Integrity Monitoring Procedure (CIFS = Common Internet File System), file systems can be configured to be monitored for unexpected changes from the executable code. In a test carried out by the Institute of Industrial Information technology (inIT) at the University of Ostwestfalen-Lippe, they were able to verify that the mGuard CIFS Integrity Monitoring Procedure would already have been able to detect infections of Stuxnet as unexpected ma-

nipulations on the very first day, long before any anti-virus programs, and to have warned the user accordingly

Contain the spread, prevent contact with servers: Firewall mGuard

Due to its distribution over networks and according weaknesses in operating systems, malware often uses network connections that are not even necessary for the productive operation of a plant. Securing industrial PCs and controllers or groups of such devices with Firewall mGuard allows non-required or undesired connections to be reliably blocked and

the spread of malware to be stopped.

Authenticated and authorized configuration: User Firewall mGuard

Many of the controllers used today contain little or no protective functions for authentication and authorization of your configuration. Contrary to a common assumption, no special configuration software or software authorized by the manufacturer is required to program and manipulate many controllers.

The User Firewall mGuard is an effective means of preventing manipulations to controllers caused by unauthorized configuration access. Access to the configuration port must thereby first be approved by an authenticating user authorization at the firewall.

The mGuard-based network components are available within the Phoenix Contact's product range as part of the FL Mguard product group in a multitude of types and configurations.

This means that effective technologies and products are available right now to reliably combat the attacks of Stuxnet & Co.

