# SECURITY WARNING INFOLETTER 17/10

## MALICIOUS STUXNET WORM ATTACKS SIEMENS SCADA SYSTEMS

There is a new malware spreading around which affects Siemens software like WinCC or PCS 7. This so called trojan is named Stuxnet and distributes via USB sticks. Just viewing the content of an affected USB stick will activate this trojan.

How Stuxnet exactly harms infected systems is not completely verified yet. Siemens founded a separate group of specialists which are working on detection and removal tools for this malware and gain more information about the behaviour of this trojan. The only thing which is known already is, that Stuxnet is able to open an internet connection and send data to an unknown third party server. This may be confidential information, process data and more.

**Do I need to worry about my Brückner line?**

Basing on the actual knowledge about this malware, only computers with WinCC or PCS 7 software are affected. This software is normally not installed on Brückner workstations or FieldPG`s. Additionally, the IT-infrastructure on Brückner plants is self-contained, protected with a firewall and therefore safe against attacks from the outside (internet). Even if your system would be infected, the malware is, due to the restrictive security concept, not able to establish any connection to third-party computers or servers and send sensible data. Anyhow, there are a few things which should be considered:

- Don’t use any third party USB-stick with your Brückner system (workstation, terminals, etc.)
- Don’t browse the internet on computers which are connected to the plant network (i.e. FieldPG)

***NOTE: Remote connections to your plant by Brückner specialists are secure and can be used without any concerns (i.e. remote service or gotomeeting session)!***

**How can I check whether my system is infected or not?**

Siemens released detection and cleaning tools which are able to scan your system and remove possible infections. This tools and newest information about the Stuxnet trojan can be found and downloaded on the official Siemens website http://support.automation.siemens.com by searching for the Article ID **43876783**.

**What should I do if my system is infected?**

If you find your system infected by this malicious software, immediately contact Brückner Servtec to assist you removing and cleaning your system.

In case you need further information about this issue, please contact the Electrical Service department E-SERVICE@BRUECKNER.COM or check the Siemens website http://support.automation.siemens.com for **43876783** (Article ID).

One Step Ahead – with Brückner Servtec

Best regards,

Your Brückner Servtec Service Team