"The Time of Isolated Systems Is Over"

Interview with Thomas Brandstetter, Program Manager Product CERT, Siemens AG, Germany

Some years ago Computer Emergency Response Teams (CERT) were subject to IT security only. Now the first CERTs can also be found in the fields of process control and plant construction. Their task is to react quickly and with coordination to security incidents. Thomas Brandstetter is head of Product CERT at Siemens and experiences first hand the change of threat scenarios for industrial electronics.

a+s: *Mr Brandstetter, why is the SCADA industry sector now so electrified by security topics? Is Stuxnet the only reason, even though the attack was clearly defined and delimited?*

Thomas Brandstetter: Stuxnet was the straw that broke the camel's back. But even earlier clear trends could be observed. Classic IT technologies became more and more integral parts of industry facilities. The reason is that interoperability between SCADA and IT is a market requirement of today and for customers it is easier to use standardised environments. But this enables also the possibility to transfer known IT threats into industrial facilities. For many, Stuxnet was an eye opener but for insiders it was a logical consequence and came as no surprise.

a+s: *IT systems that are connected to the Internet will normally be targeted and hacked with automated attacks. Does this work with SCADA, too?*

Thomas Brandstetter: Not to the same extent. Automation systems are widely self-contained and use only a few and strongly controlled connections to the outside world. In the past these technologies were even more proprietary than they are today. But now we have many open doors because of the use of standard technologies like Windows or TCP/IP which makes the systems as vulnerable as the classic IT.

During the last few months we saw publications where experts gave examples showing how they could find fingerprints of automation systems on the Internet. This is not exclusive to a single manufacturer; it is caused by the customers who connect their systems directly to the Internet, against the manufacturers' best practice recommendations. In addition, the developments of the last few years practically do not allow implementing a system that is isolated from other networks. These times are really over.

a+s: *What, in your opinion, are the biggest challenges related to the security of SCADA systems?*

Thomas Brandstetter: In terms of security SCADA cannot be compared with office applications or data processing centres. Control components are tailor-made for specific use cases and require an entirely different concept than a PC which can run principally every kind

of software on a compatible processor. Automation components can have an operating lifespan between 10 and 30 years which makes it difficult to install 'something' subsequently without running the risk of endangering the working system. Today we have predominantly systems that were built 10 years ago or even earlier and they now face the situation of being integrated in open networks. This can easily cause problems and retrofitting is not as simple as under Windows.

a+s: *Why do we have these huge gaps in controlling? IT security has been an established topic with proven products and services for more than 10 years.*

Thomas Brandstetter: I wouldn't say that the manufacturers overlooked security. When I started at Siemens 7 years ago they had already invested massively in plant security. Security is now a top topic again because the awareness has increased. Some CERTs like we have at Siemens are pointing out the weak points and what attackers concentrate on. But open standards and routable protocols find their way into the industrial sector and with them come the problems of classic IT, too.

At the moment the manufacturers are making an effort to handle these problems and are trying to find answers to questions like: How might possible attacks occur? How can they cope with weak points? How can they get the high proportion of OEM technology under control? Another reason is the so far very showy hacking incidents in product environments. There is only a handful of reported incidents but Stuxnet has shown what we should be prepared for.

Malware in industrial environments has created an awareness of security topics which is surely related to the generation change as well. Today's customers are often very experienced and competent experts who have learned through long experience how to control and administrate processes. This is the classic art of engineering based on an age bracket from a time I would call pre-IT-time. The succeeding members of staff however see things from a different angle. They are more demanding for modern IT security measures including SCADA systems and appropriate answers to incidents.

a+s: *To what extent can classic IT security measures be used in the industrial sector? Are there any limits?*

Thomas Brandstetter: Limits are set by deterministic controlled processes. How could one ever handle this with multi-purpose systems or Windows? The usage of standardised hardware and software has advantages of course, but the operator has to consider carefully the resulting security implications. Siemens tries to make appropriate security recommendations especially for standardised software which causes the biggest threats and now we also have service units to support our customers.

In this case, the limit is set by the system or product design and the sales volume. If we as a manufacturer deliver components which can be used throughout a variety of different systems we can only concentrate on a certain part of security. An integrator who assembles the customer's entire system has accordingly the opportunity to offer a comprehensive security concept.

a+s: *Is there a cooperation with producers of security software like anti-virus or firewall solutions?*

Thomas Brandstetter: Yes. Siemens' "Industry Automation Division" has partnerships with Symantec, Trend Micro and McAfee for system solutions. Apart from classic virus scanners – which are at their limits, by the way - we also use other concepts, too. For example application whitelisting is a very reasonable concept for automation systems because these environments are much more static than office applications. The focus is also on the integration of SCADA specific protocols in IDP/IDS engines. ■

About the author

Thomas Brandstetter has been responsible for the topic of product security at Siemens, Germany for seven years. After the Stuxnet incident he became the head of the Siemens Product CERT. He focuses on incident-handling and vulnerability management for Siemens products. Before that, he did preventive intrusion and hacking tests within the "Hack-Proof Products" program.

This is an excerpt of the interview with Mr Brandstetter in the new magazine a+s. The original interview contains additional questions and answers about the following topics: security details about protocols, the responsibility of manufacturers, how to deal with a case of emergency, the legal situation of compliance for the industry and facts about Siemens' CERT.