Building upon the conference theme, as well as much discussion throughout the conference, DHS announced plans to initiate a collaborative activity focusing on cybersecurity awareness raising. DHS plans to stand up a working group with interested Meridian delegates to carry forward this initiative in the very near future. The working group will focus on unifying and creating common, cross-cultural awareness raising efforts that will enable Meridian members to coordinate and leverage initiatives. In general, the group will aim to raise cybersecurity awareness among all constituents and emphasize that cybersecurity is a shared responsibility.

Marking the fifth anniversary of the Meridian Process, delegates were able to reflect on progress the community has made to date. Conference delegates left Washington prepared to carry on the work of the Meridian Process into 2010 and on to the next conference, scheduled for this fall in Taiwan.

The fourth Dutch Process Control Security Event

Annemarie Zielstra
Programme Manager
NICC
annemarie.zielstra@ictu.nl

Eric Luiijf
Consultant
NICC

On December 1st, 2009, the fourth Dutch Process Control Security Event took place in Baarn, The Netherlands. The security event with the title 'Manage IT!' was organised by the Dutch National Infrastructure against Cybercrime (NICC). Mid of November, a group of over thirty people participated in the Department of Homeland Security Red Team – Blue Team training on process control security in Idaho Falls, USA. The training was attended by a mix of people from various Dutch critical infrastructures, multi-nationals, process control vendors and application suppliers, government agencies, knowledge organisations, and universities.

The first part of the security event focussed on the feedback and lessons identified by the red-blue team training participants. A presentation presented by Jos Weyers, TenneT (collectively made by some participants) showed a very positive feedback and enthusiasm about the training itself. The training started with some days of parallel lectures and hand-on training to raise the knowledge level of the participants about process control protocols, and network defence. They learned, for instance, that process control protocols and their implementations are weak, and that detailed information about the protocols is globally available. The members of the red team received some training about publicly available attack tools and vulnerabilities.

The blue team was surprised about how easy it is to penetrate systems when for instance only a single critical patch has not been applied. On the game day, the blue team noticed and blocked a penetration by the red team. They declared victory. It did not take long, however, to realise that the penetration was on-going for quite some time. From that they learned that intrusion detection in process control networks is required, otherwise one does not know until late that a penetration takes place. Another annoying lesson is that a single firewall with a liberal ('optimistic') traffic blocking configuration allows attackers to penetrate with ease.

At the same time, one has to understand the normal own traffic patterns in one's network first. Otherwise it will be hard to determine whether one sees legitimate traffic or traffic by the bad guys!

The blue team also learned in a hard way that process control security requires a multi-level approach. Understanding by the top-level management of the security issue is required. There is a need for a corporate security policy for process control systems. There is a need for proper operational procedures like backup and recovery, and how to react when an intrusion is detected. Patch management is required as well as proper management of passwords. Another lesson was that process control applications most often do not use least user privileges when granting access thus giving bad guys a free ride. Another major lesson is that network configurations need to be standardised as much as possible. That will simplify the overall system and allows quick response to threats and incidents.

Above all, the human factor was identified as important. Humans will leak company classified information via email, social networks and contacts. USB-sticks and other computer media with sensitive information may become lost. Printed sensitive information may end in the dumpster. As such, each employee of an organisation has a role in protecting information and the key processes of the organisation.

A slide show of pictures taken during the Idaho Falls training was shown to the audience. The slide show reflected the hard work, the dedication, and enthusiasm of the participants. Some pictures showed that the red team even surprising the organisation of the training event by showing some initiatives not seen before in earlier training exercises like stolen blue team documentation and sending a blackmail message.

The next part of the event focussed on how to convey a process control security issue and mitigation plan to one's upper management layers. Philippe Raets, a manager, first presented the quite different topics which top management has to deal with and which topics interest them. Often that is not the content but the context! Conversely, technical experts are focussed on a limited set of issues dealing with (technical) content. Their advice is straightforward and well analysed about the single (technical) issue. It is their environment and their reality! However, top management uses diverse conflicts as a structuring principle. Their primary orientation is on the governance issue and the supervisory board. To assist the (process control) experts Philippe Raets gave some directions on how to convince top management. For instance, split your issues in important and non-important and in urgent and non-urgent. Do not mix the short term and long term issues. Do not expect a decision on all your (content) issues directly in a single meeting.

Then, the over 80 participants were split in groups which had to face a process control security challenge. One or more solutions had to be engineered and be brought to top-management for a go/no-go decision on investment and operational service level. Two groups were selected to present their proposals to their nasty manager (which was played by an actor). It was not easy to convince the manager. However, a simple slip of the tongue "I can do that in one week (if…)" was taken as agreed action item bypassing the 'if-clauses'. The two groups which had to present their proposal had a hard time. The other participants who had an observing role were glad that they were not challenged. All participants learned a lot on how to manage issues to be brought to the attention of their manager.

The day was closed with a social event. All participants received a process control security awareness booklet (in Dutch) which has been mailed to their management as well. An English version of that booklet and accompanying movie will be published by the NICC early 2010.