In WG 4 the decision was taking to lift the current TR (Technical Report) 18044 Incident Handling to international standard. The revision of network security series of standards is well under way and progresses as different parts of ISO/IEC 27033 (network security is a multi-part standard that contains 7 different parts). ICT readiness (ISO/IEC 27031) did reach 2nd working draft status (WD). ISO/IEC 27032 Cybersecurity was restarted but the current work is still on 1st WD status. The scope is still somewhat unclear.

The work in WG 5 is picking up very well and includes the development of ISO/IEC 29100, a privacy framework. There is also some work regarding biometrics and rfid going on in WG 5.

First Dutch Process Control Security Event

Mrs. Annemarie Zielstra
Programme manager
NICC
annemarie.zielstra@ictu.nl

On May 21st , 2008, the Dutch National Infrastructure against Cyber Crime (NICC) organised their first Process Control Security Event. Mrs. Annemarie Zielstra, the NICC programme manager, opened the event. She welcomed the over 100 representatives of key industry sectors. “Earlier studies in the Netherlands and abroad show that many organisations do not manage the information security aspects of their process control systems (PCS). As risk is increasing, there is an urgent need for public-private collaboration by government, process control system users, and manufacturers against potential cyber crime in the PCS domain. Since these systems monitor and control processes that are critical to society, there may be a major safety and economical impact when they fail.” Such processes comprise for instance the supply of power, gas, and drinking water; managing surface water; traffic control, refineries and other chemical industrial processing, automated food processing systems, automated milkers, and security systems. She continued: “The NICC started discussing and working on the process control security theme with various critical infrastructure sectors. After analysis of information security weaknesses in the PCS of the Dutch drinking water sector, a publication with 39 good practices for PCS security in the drinking water sector was developed. Currently, studies are in progress on the information security posture of PCS in the Rotterdam harbour and the energy sector.”

Mr. Foppe Vogd, Program Director Dutch CIO Platform, chaired the event. He emphasised: “This event is not a free ride. At the end of the day, the participants have a moral obligation to make the next step: enhanced security of their own PCS. This is not easy as it requires a joint effort by people at the technical level as well as management layers. One important question today is how to get to the point that CEOs and/or CIOs will pay attention to the PCS security risk. Or: how do we move the known risk to information security experts towards the board room?”

To increase awareness, the German white hacker Christian Gresser performed a live hack. He explained why most PCS hacks that have been published in the media seem to have happened quite some years ago: “People do not want to get the word out that the processes of critical utilities are vulnerable. However, the reality is that PCS are often 10 to 15 year old setups connected to office automation environments and also to the Internet. Intrusion is easy and free Internet tools may be of help.” And it is not only about hacking tools! He told the audience about some cases where physical access to PCS and information and communication technologies (ICT) of organisations become easy: “The anti-smoking laws help me and cyber criminals as well”.

The next speaker, Mr. Kees Jans, the CIO of the Schiphol Group, outlined the innovative use of ICT at the Schiphol airport and JFK’s Terminal 4. His environment is one of increased ICT-dependency and multi-vendor solutions with chained functions supplied by multiple organisations. Governance requires well-founded decisions, risk management and security auditing.

The overall view is left to the CIO. “PCS are a new risk factor to take into account. It is not a separated world anymore; increasingly PCS and the administrative and business process ICT are integrated.” His worries are that new systems and applications are put in place without proper security considerations by one of the many parties at the airport. The information security awareness is low! He was challenged by the chairman: “who will be on prime time news telling about the hack or virus taking down your baggage handling system, you or the CEO?” His answer showed that the hot potato may be given to a system manager (provided that the press accepts that).

Because of other obligations, the discussion between Mr. Frank Heemskerk, State Secretary Economic Affairs and Mr. André Haket, CIO of Stork, was shown on videotape. The outline of their discussion was about the increased tempo in which critical systems in our society become intertwined with normal ICT, the increased risk and the societal need for reliable infrastructures and safety. André Haket: “The risk is that we move too slow. The role of government is to boost action by the private industry as the cyber criminals will not wait. Of course, the private industry has to solve the security issues themselves and reduce the risk. That is not a task of the government. The government, however, can help to foster knowledge exchange on risk factors and good practices in reducing vulnerabilities.” Frank Heemskerk: “I agree that tempo is required. Both government and PCS owners need to address the challenges”.

The next speaker, Mr. Peter Hondebrink of the Ministry of Economic Affairs, stated that his department encourages the use of ICT on the one hand, but has to consider the vulnerabilities on the other hand. “The majority of the critical and economic sectors use PCS. Incidents in PCS in other nations show that serious PCS security incidents have occurred. But incidents have occurred in The Netherlands as well in multiple sectors as for instance a TNO-KEMA report highlighted.” PCS security requires a cross-sector approach. Multiple sectors working with the NICC are already addressing the PCS security issues. That requires confidentiality and anonymity amongst the participating parties. “The confidentiality issue, however, makes it a challenge to show that the government actions and the public-private partnership are effective”. He finished by stating that “The Ministry of Economic Affairs wholeheartedly will support the public-private efforts to increase PCS security in all sectors”.

One participant was not convinced. He put forward that utilities are privatised without proper governance controls guaranteeing resilience and reliability, in this case a lack of control on information security in critical PCS. “Should the privatisation of utilities policy not be reversed?”. Peter Hondebrink replied that “Security is the owners’ own responsibility. If failures regularly occur and it becomes a national issue, the right government department may pick up the escalation process.“

Eric Byres, a well-known PCS security expert, was next: “Who turned out the lights?”. Industrial PCS are vulnerable because many people still believe in myths. “Myth 1 – PCS aren’t vulnerable for hacks and malware. Wrong!”. PCS have limited resources but use the same operating systems and CPU as office systems with the same vulnerabilities. “Myth 2 – PCS are not connected to the Internet”. A large oil company found that 80% of its PCS are connected to its insecure corporate network, and that aside of the managed connection another 17 unmanaged connections exist between the PCS and the outside world. He showed a list of public examples of PCS security incidents, and some statistics about the way hackers have penetrated into PCS. He discussed the vulnerability of PCS for normal network security tools in the office environment. Security management systems in the office environment cannot be applied to the 24 by 7 environment. “Nevertheless, one can borrow 90% of the ICT security good practices and standards for the office environment, e.g. ISO/IEC 17799. The other 10% requires the same spirit but needs to be specialised due to differences in assumptions about the office and PCS operating environments. This involves issues like patching, asset management (and scanning), access control, standardisation of systems and applications, office hours versus 24 by 7 operations, and incident response. Perimeter security is not enough; one shall break-up plants into separate zones. Critical is the human factor and the security awareness of all involved in PCS.”

During the questions, it was remarked that “there is a major difference between people responsible for ICT and those operating PCS. PCS users talk about their ‘baby’, they are passionate to let it perform the process in the best way ever. ICT people do not care much about IT-hardware such as a laptop. It was suggested to refrain of speaking about security to PCS personnel. Instead, one should introduce security as ‘this is making your process more safe and reliable’. Several participants objected to this suggestion as a CIO or CEO needs to take control about reliability and shall require that (office) ICT and PCS work together as a single team.

After lunch, the audience was split up into five different work sessions dealing with the topics ‘(No) security solutions for PCS‘, ‘Patching and hardening’, ‘The way to Secure PCS’, ‘Organisation and Management’, and a special VIP-track in which the vulnerability of PCS was visualised by a live example. The incentives and disincentives for ICT security in general and PCS security in particular were discussed.

The day was concluded by a panel consisting of the work session chairmen. The main issues:

- A first dialogue between SCADA vendors, users and security application vendors started. A joint discussion and information exchange platform about PCS infrastructure security is regarded fruitful. A no-go area is a discussion about business risk and impact aspects.
- Security is still seen as cost factor; not as a risk mitigating factor or insurance; how to come to a business value?
- PCS patching and hardening is a security need; it is not done yet in the right way. Good practices need to be explored and exchanged. Legacy is an issue as very old operating systems are around.
- PCS security requirements should be part of procurement, but this is not always the case.
- The drinking water advancements in PCS security and their risk analysis approach are being looked at by other critical sectors that co-operate in the NICC. PCS security policies are needed, but that requires management awareness. How to quantify the risk for the management levels?
- When safety requirements are met, the security requirements for daily operations are often met as well. The remaining security risk is less rational and may hit unexpectedly. How to make this remaining risk quantifiable?
- Information security is good business practice as one can make risk assessment for PCS security comparable with safety risk assessment (e.g. explosions). PCS and ‘office ICT’ will converge over time. Education, training and partnering of all involved is required, the earlier the better.
- There are too many PCS security standards; a common international cross-sector view is required.
- Good risk management requires a bottom-up involvement of all people involved in the organisation. That may require another risk management culture in the organisation.
- A number of participants are in favour of an obligation to publicly report incidents if consequences are exempted (alike the FAA-model in the airline industry). An anonymous database managed by a trusted party is another alternative to increase the sense of urgency and awareness.
- PCS vendors stated that PCS security is often dropped first by the PCS buyers when the price exceeds the budget.

The assembly came up with tree recommendations to the NICC to jointly improve the security of PCS:

- Continue and intensify the dialogue about PCS security.
- Discuss the results of the Process Control Event in the NICC sector-specific working groups.
- Develop a database and anonymous reporting scheme for reporting PCS security incidents.

The event was closed by Mrs. Annemarie Zielstra. She asked all participants to consider their commitment about participation in the next steps. She announced that the next NICC Process Control Security Event will happen on November 20, 2008.