Are you in Control?

That was the key question discussed at the second Dutch Second Dutch Process Control Security Event at the Technical University of Delft, December 4, 2008.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl

The second Dutch Process Control Security Event attracted many process control people. The event was organised by the National Infrastructure against Cybercrime (NICC). Over hundred people responsible for the security of process control systems (PCS) and related networks in many of the Dutch critical infrastructures (CI) and key industries took part in the two plenary sessions and four parallel workshops. The event was co-located with the Production Process Automation (PPA) event for PCS/SCADA vendors and system integrators which was organised by the Dutch Federation for Technology Branches (FHI). They discussed a set of PCS issues including information security. At the end of the day, both events joined for a closing debate session on security and responsibilities.

Annemarie Zielstra, programme manager of the NICC opened the event. Besides the FIH, the WIB (Dutch PCS user association), and the Technical University of Delft participated in organising the event. In May 2008, the first process control security event identified a set of actions which set the agenda for this event: increase risk awareness by top management, sharing incident information, and establishing a common user - manufacturer view on PCS security requirements as part of the procurement process.

She continued: "The PCS security issues in the Netherlands are not addressed in isolation. The Dutch PCS community is both involved in the European SCADA Security Information Exchange (Euro-SCSIE) and the newcomer MPCSIE (Meridian Process Control Security Information Exchange). The latter has recently been established by the international governmental ICT-policy discussion group Meridian."

"The question 'Are you in control?' needs to be answered by all Dutch CI and key industries. Some weeks before this security event, a meeting of the Chief Information Officers (CIO) Platform and the Director-General for Energy and Telecom of the Dutch Ministry for Economic Affairs took place discussing today's theme. That meeting showed that not all CIO know who in their organisation is responsible for the information security of control systems. When something goes wrong, the CIO will be probably looked at.

One CIO became aware of control systems in his organisation when he was planning a move of his computer room. Obviously, not all organisations are in control of the information security aspects of control systems!"

"As a result, the CIO Platform plans to take a coordinated action in The Netherlands to increase risk awareness amongst the Dutch CI and key industries. It should become crisp and clear who is responsible for process control security within each organisation."

Currently it is unclear who is responsible for the information security of process control systems [Dutch CIO Platform]

The next agenda item was a plenary debate between Aad Dekker (Information security officer at NUON, a Dutch power distribution company) and Ted Angevaare, the SHELL global DACA (process control) security manager. Their views on process control security differed in details like their answers to the question "Is security the safeguarding against undesirable control of the process or is it the safeguarding against the disruption of the production?" Next was debated whether office ICT-security should include physical security and

whether the same approach holds for the process control environment as well. Screening of personnel, legal hacking as part of security audits, and formal reporting of incidents followed as topics. Regarding the latter, it was concluded that most organisations that use PCS do not have a rigid incident reporting scheme. Probably many incidents are not reported because the responsibility for the ICT-security side of PCS is not clearly organised in organisations. It is felt that motivating people about their work and security awareness is more important that taking sanctions against those who create a security breach. One of the debaters had to admit that he does not know how ICT-assets are decommissioned and whether computer media such as hard disks are properly wiped or destroyed.

Is top management able to take the right decisions about ICT security? "Probably not", was the answer as incident reports are not complete, and responsibilities for process control security are not totally clear. The risk is that top management will overreact in case of an incident which hits the press. How to avoid that? "Steering and preparing them by executing proper risk assessments and risk management. Above all, avoid scaring talks to them by vendors who want to push sales." One also should avoid being to dependent of process control hardware and software vendors. Understand one's own needs and fix your vulnerabilities based upon your risk assessment. And put far less trust in third party PCS maintenance people than in your own people.

What is the role for government? The answers ranged from setting de facto security standards, assistance when fighting a cyber attack to a better information position by information exchange with and easy access to law enforcement, and intelligence services. Leading should be "what is in for both of us?"

Use your female intuition!

Four workshops

The workshops were held in parallel and repeated after a break allowing participants to participate in two workshops of their choice. The four themes were set during the first PCS security event: good practices in the energy sector (by Randi Roisli, Norwegian StatoilHydro), social engineering (Jan de Boer, TIAS Business School), gaming and simulation (Mark de Bruijne, TUDelft), and the development of the Dutch PCS security incident database (Martin Visser, Waternet and Eric Luiijf, TNO and NICC).

Randi Roisli showed the highly complex, dependent PCS environment where a large set of operators and suppliers together control the oil production on a number of Norwegian off-shore and on-shore facilities. The joint Oil Industry Association (OLF) guideline 104 has been developed to address the process control security weaknesses, both organisationally and technically. A self-assessment tool assists the organisations in measuring their PCS security posture.

Jan de Boer is an ethical hacker who performs social engineering upon request. He showed the approach and the results of several cases. He pleads for using the "human (female) intuition" much more to avoid becoming tricked by a social engineering attack. Mark de Bruijne showed where different technologies meet each other in gaming-simulation. This new combined research field allows different actors, e.g., process control and ICT-departments, to learn from interactions between both departments in a simulated (risk free) environment. An example of a game to train dike patrol people was shown. Martin Visser presented the NICC context for sharing information about process control/SCADA incidents. Eric Luiijf continued by explaining the vision and long-term aims of a security incident database. Consultations with representatives of various NICC petals leads to a pragmatic approach: start as soon as possible, use a standard reporting form in English, anonymisation of incident reports by a trusted central body, and distribute the information to organisations which have agreed to keep the shared information secure. Details, especially the legal ones and the trusted party, still have to be worked out. Very worthwhile comments were received from the participants. Keep it simple, stupid and be pragmatic are considered the key to success.

Final debate

The final debate, organised by both NICC, WIB and FIH, brought together the PCS users, manufacturers, vendors, system integrators, and government. A main part of the debate circled around the responsibility for security. Users require more secure PCS, manufacturers and vendors have security knowledge, manufacturers point to PCS integrators as they do the configuration and integration of parts of multiple manufacturers, system integrators point to both the end users and the PCS manufacturers. "Security is dropped first when it comes to price while forgetting that cost reduction by using COTS software and hardware already has been cashed in". "Investments in security reduce downtime and increases production time." "Do not overlook the insider threat!" "Risk assessment shall be the driver, not regulations or laws. An independent regulator, however, may set the boundaries of a proper security posture for a critical sector." "Learn from the safety and security checklist for constructors (VCA) approach. Security can make organisations more efficient and effective!"

Obviously, this was not the last debate on this challenge, although some progress was made in understanding the background of the different positions. For that reason, the responsibility issue was selected as the main topic for the next NICC Process Control Security Event on April 23, 2009.