Published in AUTlook on 14.06.2022
https://autlook.at/meinung/nis2-kommt/

Expert highlights importance of the NIS2 guideline for industry

After protracted and controversial negotiations an agreement was recently reached for the new EU Cybersecurity Directive NIS2 (Network and Information Security), which imposes extensive requirements on the industry. We discussed the impact of the new directive on the Austrian industry and its implementation with the expert, Herbert Andert, from VTU Engineering.

Herbert Andert, Division Manager
Automation and Industrial Digitalization
VTU Engineering GmbH

How have you followed the negotiations for the NIS2 directive and how would you assess the result?

Herbert Andert: I have been following the discussion since December 2020 when the first draft was presented. Further negotiations were pushed into the background due to the pandemic. The NIS1 Directive has been around for a long time but some very large infrastructural service providers such as hospitals have yet to implement the directive. Which is why I am doubtful whether NIS2 will be implemented across the board within a reasonable period. In fact, no directive should really be necessary for companies to deal with the issue of Cybersecurity. Cyberattacks take place and the industry must protect itself and prevent production losses. Here many companies still have a lot of catching up to do.

Negotiations conducted in trialogue meetings between the Commission, the Council and the Parliament were very tough. The Commission named the pandemic as the reasons, but it might also be because the companies put up a tough fight. You advise your customers in the implementation of Cybersecurity directives, what do you hear from them?

Andert: We notice that in many companies the responsibility for the Cybersecurity is being shifted back and forth between departments and in the end, no one really assumes responsibility for it. The business priorities often lie elsewhere, so that the issue of Cybersecurity is not being pursued at the moment. For those companies that have been the victim of cyberattacks this issue has suddenly become of the highest priority and no measures seem to be too costly any more. In the end in turns out that a poor or non-existent security system costs significantly more than a good one. Unfortunately, a lot of companies see the added value only after they have been actually attacked and production losses result in damages running into tens of millions. I personally have a hard time understanding why a lot of people are still so reluctant when it comes to Cybersecurity. Getting companies to plan for some protection in order to protect the entire infrastructure requires uniform regulations.

NIS2 is supposed to enter into force this year. The member states then have 21 months to implement the directive. Do you expect the same indifference on the part of the companies as was the case with NIS1?

Andert: If it is not monitored and not sanctioned in case of non-compliance, the implementation of NIS2 is likely to be as shabby as that of NIS1. Companies that make profit and otherwise act successfully often see no reason for investing in prevention, because they do not consider Cybersecurity as important enough. A lot of them think their company does not represent an attractive target for a cyberattack, some perhaps simply hope that it will not happen to them. With increasing digitisation, it should be in the interest of the companies to protect their own know-how and the production facilities as best as possible. When I first started in the field of Automation in the 90s, there were numerous proprietary interfaces, because Cybersecurity still did not play a major role. But in the meantime, we also have to deal with challenges in production, which were previously known only in the IT.

Directives must be implemented at national level. Who should monitor and control the implementation in Austria?

Andert: There is a separate group within the competent federal ministry that deals with NIS. However, at an information event you can notice that this group has very few staff resources at its disposal. Getting companies to plan for some protection in order to protect the entire infrastructure, requires uniform regulations that are harmonised across EU. It is the task of politicians to create uniform rules with which the costs can be kept down. The cost factor is decisive for small and medium sized companies, because the costs basically add up to the same as for a large company. IT and OT work closely together, but they should both maintain their point of view and keep a critical eye on other divisions.

What should a company expect when planning to implement the NIS2 directive?

Andert: We proceed based on the procedural model VDI/VDE 2182 where all the steps are defined. Our project team evaluates the actual status of the production facilities and systems and creates a risk analysis according to IEC 62443. Then we draft a technical and budgetary roadmap together with the customer, with all required steps for the implementation of the directive. The customer decides which steps he wants to implement. The analysis and the conception usually require a few days to complete. The implementation can last significantly longer, even up to several months, if e.g. the system engineering process also changes in the course of modernisation.

How complex are the requirements of the directive? Is it at all possible for a small company to implement it by itself?

Andert: Cybersecurity is not just an IT issue, but also impacts the OT. In other words, to implement such measures aspects from the system planning and know-how from automation must also be taken into account. The IT department of a company does not possess this know-how and, therefore, should not additionally be made responsible for the security in the OT. IT and OT work closely together, but they should both maintain their own perspective and keep a critical eye on other divisions. If this know-how from engineering and automation is not available in-house, external partners must be involved. In practice, the way this usually works is that this special know-how is used during the planning and thereafter audited annually. This outside perspective is essential - which is why we too work with an external partner, which analyses and evaluates our work once again.

NIS2 at a glance

- Companies are required to prepare a risk management concept containing a minimum list of basic safety elements.
- There are clear provisions regarding the procedure for reporting incidents, the content of reports and deadlines.
- There are strict supervisory measures for the national authorities and implementation requirements.
- A fine is stipulated according to GDPR model for breach of security measures.
- Selected companies will be required to deal with Cybersecurity risks in supply chain and supply relationships.