How to connect your legacy machines in a cyber-secure way

11 October 2021, 02:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

Sirris has recently launched its cybersecurity service for manufacturing. As we start to reach out to companies via our free intake or individual coaching, we receive more and more questions about connectivity. For manufacturers it seems a complex matter, but with several structured tips it can be easily resolved.

There is no one fits all solution to make legacy equipment cybersecure and, as we all know, the chain is only as strong as it weakest link. For these reasons it is important to build multiple *layers* to harden legacy systems and hence *reduce* the *risk* to cybersecurity issues.

Possible strategies and interventions

- The first important strategy to consider is to **prevent your equipment from becoming *legacy equipment***, or at least try to delay the process. This can be achieved by documenting all changes and updates carried out at the machine. If the machine contains a pc-based operating system, make sure to apply all (security) patches. This also applies to dcs or plc equipment. You could make this part of the maintenance contract between you and your supplier/integrator. If in time a certain part is no longer patchable by software, consider upgrading to new hardware. This involves a constant monitoring and continuous investments. But considering the cost of possible consequences related to modern cyberattacks, this might be a good investment.

- A second strategy is to **keep an overview of all your connected assets**, including dcs or plcs inside machines. The idea here is that you cannot protect what you don't know. So an inventory is key. Keeping it up to date will be challenging but important! Known vulnerabilities change over time, so scanning your equipment for them on a regular basis is a must. Make this overview visual, so you can see which hardening action will have effect on which part of your production or on which machines. This makes planning and architecting your infrastructure easier.

- The absolute minimum action necessary to take is to **segregate your office IT equipment with your production OT equipment**. This can be done by placing a separate industrial firewall between them. Further segregation between different departments, lines or machines is even better. No need to say that the firewalls themselves need to be managed and kept current by applying patches when provided by the manufacturer. Depending on the size of

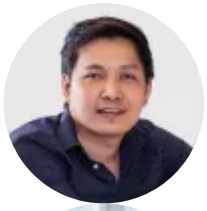
your facility, it is also considered a good practise to use devices from different vendors.

- A non-intrusive way to **monitor a system is to monitor the network traffic** going to or coming from a machine. It is a practise called virtual patching. You install an appliance between the machine and the rest of the network. When it detects that a known vulnerability is being exploited it blocks further network traffic and notifies the administrator of the event.

- Sometimes **old software** is still used to generate files for a certain type of machine (e.g. CNC). It is no exception that this kind of software only runs on Win98 or WinXP. In these cases it is advised to run the old OS and software in a virtual machine on a modern pc. This solves not all possible issues, but reduces the attack surface immensely.

The tips we give you in this blogpost are only a small overview of the possible ways to harden your legacy OT infrastructure. In our masterclass 'Cybersecurity for manufacturing companies' we shall have a deeper view with hands-on examples and practical step-by-step roadmap to securing your connected machines. Register now and join us on 8 November 2021!

Authors



Annanda Rath



Christophe Michiels



Tatiana Galibus