Cybersecurity for Operational Technology in 5 Steps

All over the world organizations, including companies that are part of critical infrastructures, remain vulnerable to digital incidents. Cybercriminals are increasingly targeting the primary processes of companies, which can jeopardize production processes and continuity and even cause social instability. The damage caused by this, according to the British insurer Hiscox, runs into the hundreds of billions of dollars. Kiwa and Hudson Cybertec are jointly committed to increasing digital resilience.

Utilities and industry are increasingly facing cyberattacks on their Operational Technology (OT) systems. This is not surprising in itself, because while cybersecurity is often taken into account when designing IT environments, this is much less the case in OT environments. Machine parks and technical installations used operate apart from other systems and the internet, so cybersecurity was not always the top priority here.

Due to digitization and the growing need for data exchange, the OT and IT worlds are becoming increasingly interconnected. Linking these environments entails new risks that can affect the digital resilience of the entire organization.

How do you stay resilient and alert to the latest threats in this digital world?

Since May 2021, Kiwa and Hudson Cybertec, specialized in cybersecurity for Industrial Automation & Control Systems (IACS) have partnered up to increase OT cybersecurity. With Hudson Cybertec's expertise in the field of cybersecurity and Kiwa's authority on Testing, Inspecting and Certification (TIC), all knowledge is in-house to help organizations inventory, assess, certify and maintain digital resilience. Central in this are people, organization and technology.

People

Analysis of, among other things, the cybersecurity awareness and knowledge level of your employees.

Organization

Determine whether your organization has, for example, taken appropriate security measures.

Technology

Analysis of your organization's technical security measures.

Cybersecurity for Operational Technology in 5 Steps

The 5 steps

Kiwa and Hudson Cybertec offer cybersecurity solutions for the most diverse organizations and processes. From organizations just starting to shape their OT cybersecurity to companies that already prioritize OT cybersecurity. This joint approach is summarized below in 5 steps. Kiwa and Hudson Cybertec offer several services that help you to go through these steps in a way that suits your organization.

Step 1: Inventory

We map the digital resilience of your organization. Based on a baseline measurement on both organizational and technical level you know exactly where you stand.

Step 2: Plan of action

Together with you we determine which level of digital resilience is appropriate for your organization and set a step-by-step plan to achieve this. This gives you clarity and overview.

Step 3: Implementation

We make your organization digitally resilient. We help you to implement your cybersecurity policy or enable you do it entirely yourself, supported by our consultancy or workshops.

Step 4: Maintenance

We keep your organization digitally resilient. We manage cybersecurity for you or help you to do it yourself. This way you are always in control.

Step 5: Certification

To create extra value and regularly assess your digital resilience, Kiwa offers cybersecurity certification services such as IEC 62443, the international standard for cybersecurity for Industrial automation & Control Systems (IACS).

Following these steps will keep you in control and enables you to build defense mechanisms that keep you resilient against the latest digital threats.

Independence guaranteed

Kiwa and Hudson Cybertec each have proven track records in their own fields of expertise, are fully complementary and are committed to offer a joint integrated solutions when it comes to cybersecurity and (product) certification to secure primary processes in companies and organizations. The first four steps are in the hands of Hudson Cybertec. Kiwa, completely is responsible for step 5.

More information

Due to the unique combination of in-depth domain knowledge, extensive cybersecurity experience and expertise in both industrial and technical automation, Kiwa and Hudson Cybertec are your OT cybersecurity partner. Do you want to know more about our services in the field of cybersecurity and TIC?
Please contact Bart Scholten (bart.scholten@kiwa.com) or Ramona Houweling (info@hudsoncybertec.com).

For more information you can also visit our websites: www.kiwa.com/nl/en/cyber-security or www.hudsoncybertec.com.

HUDSON CYBERTEC