Stopping a Phishing Attack Before It Became a Supply Chain Crisis

When a company we had partnered with on previous projects reached out to us, the situation was urgent and highly sensitive. The business owner had fallen victim to a phishing attack and unknowingly shared both his password and a one-time password token. This gave attackers full access to his Office 365 account. From there, they began sending convincing SharePoint invitations to the company's partners, attempting to harvest even more credentials and expand their access.

Recognizing the seriousness of the breach, they contacted Howest almost immediately. Within the same week, we worked together to contain the incident. We identified which devices were compromised, reconstructed the steps the attackers had taken, and helped the company quickly warn their partners about the fraudulent emails. Acting fast prevented the situation from escalating into a wider supply chain compromise.

Our investigation uncovered valuable technical evidence, including the IP addresses and domain names used by the attackers. With this information, we supported the company in reporting the incident to the Centre for Cybersecurity Belgium so appropriate follow up actions could be taken.

Beyond containment, we focused on strengthening their resilience. Drawing on experience gained through the ICIL project, we helped implement reliable and affordable backup solutions and thoroughly verified that no backdoors or unauthorized account changes remained. Thanks to this combined expertise in incident response and backup strategy, the compromise was resolved quickly and effectively, leaving the company with a strengthened security posture.

Security Audit at a Belgian Brewery

We were asked to carry out a security audit at a small well known Belgian brewery. Because of the experience we gained during the ICIL project, especially around cyber risks in industrial environments, we approached this assignment with a strong focus on how their office IT and production systems were connected.

The goal was to perform a penetration test. We took on the role of an external attacker and tried to move through the environment the way a real threat actor would. That meant looking beyond simple vulnerabilities and focusing on how small weaknesses could be chained together into something more serious.

During the test, we identified several ways to obtain valid user credentials. With those credentials, we were able to access the internal network where both office systems and industrial devices were connected. From that position, it became clear how much impact an attacker could have. Production systems were reachable. Processes could potentially be modified. In the worst case, brewing operations could be disrupted or even stopped entirely. For a company whose core business depends on continuous production, that is not a minor risk.

We documented every finding, explaining not only what was vulnerable but also what the real-world consequences could be. After delivering the report, we organized follow up calls to go through the results in detail. We discussed concrete short-term measures, such as tightening access controls and monitoring, as well as longer term improvements like better network segmentation between office IT and industrial systems.

By combining practical penetration testing with the industrial cybersecurity knowledge developed during ICIL, we helped the brewery gain a clear understanding of where they stood and what steps were needed to better protect both their data and their production line.

Safeguarding Critical Infrastructure at De Watergroep

We carried out a security assessment at De Watergroep, the largest supplier of drinking water in Flanders. Given the importance of their operations, we visited multiple sites and reviewed different layers of the organization, from office environments to water reservoirs and production centers. The aim was to look at both their corporate IT and operational systems in a realistic, practical way.

As an ISO 27001 certified organization, they have already taken solid steps to secure their environment. Security processes were in place and clearly embedded in their operations. Still, during the assessment we identified several critical gaps that could have led to serious consequences if exploited. A large part of the vulnerabilities we found were tied to machines and services managed by a third party. These systems were not always fully visible within their internal monitoring and security processes, which made them blind spots.

One of the most significant findings was a previously unknown critical vulnerability in a widely used industrial device from a European vendor. The issue had not been publicly documented before and could have exposed sensitive systems if misused. We responsibly disclosed the vulnerability to the vendor, who acknowledged the problem and is working on a fix. Since this device is used at other industrial sites and is sometimes publicly exposed, the broader impact could extend beyond a single organization.

This assessment underlined something important. Security does not stop at your own perimeter. The partners you choose to manage parts of your infrastructure play a crucial role in your overall resilience. Having reliable partners, clear visibility, and strong communication channels is just as important as having the right technical controls in place.

Strengthening Security Step by Step at a Belgian Machine Builder

A small Belgian machine builder asked us to help them improve their overall security posture. They wanted a structured approach that covered everything, not just technology, but also processes and people. Together, we worked out a clear three phase plan.

In phase one, we carried out a security assessment that included a penetration test. We approached their environment the way a real attacker would, looking for gaps and testing how far we could get. The goal was to understand the realistic impact if someone with bad intentions targeted them. We identified weaknesses in both their IT and OT environments and documented how these issues could be abused. The result was a detailed report outlining the technical findings, their potential impact, and practical steps to fix them.

Phase two focused on the human side. We ran a phishing campaign across all departments to see how employees would respond to realistic phishing emails. This gave us insight into where awareness was already strong and where extra guidance was needed. It also made the risks tangible instead of theoretical.

In phase three, we organized several awareness sessions to address the issues discovered in the first two phases. We kept the sessions practical and relatable, offering simple tips that were easy to apply immediately. We also spent time on what to do when something feels off. How to recognize and report phishing emails. Who to contact if a machine starts behaving strangely.

The sessions were held on Monday and Friday, and it was rewarding to see how quickly the ideas spread. Employees who had not yet attended were already picking up tips from colleagues who had. For example, if someone left their laptop unlocked when stepping away, a colleague might post a message in the group chat saying they would bring cake the next day. Small actions like that made the message stick.

It showed that cybersecurity does not have to be heavy or complicated. With the right structure and a bit of creativity, it can become part of everyday culture.

Experiencing Cybersecurity Firsthand

To make industrial cybersecurity more tangible for SMEs, we organized several small-scale afternoon sessions with groups of around ten participants from different roles and companies. The idea was simple. Instead of only talking about risks, let them experience them.

We started each session with a focused awareness briefing covering the essentials of industrial security. We discussed common attack paths, typical weaknesses in IT and OT environments, and the kind of impact incidents can have on production and business continuity. To make it concrete, we also demonstrated real vulnerabilities that were identified during the ICIL project.

After that introduction, the participants stepped into the role of an attacker. We brought along a guided and realistic lab environment that simulated a company they had never seen before. Their starting point was the public website. From there, they worked their way in, gaining initial access and scanning the internal environment to see what they could find.

It did not take long before they discovered interesting systems. A thermal printer, several PLCs, an HMI, and even an engineering workstation. With guidance, they explored misconfigurations, weak passwords, and unpatched systems. They were able to run controlled exploits and see firsthand how quickly access to critical machines could be obtained.

As they progressed, concepts like open ports, hashing, segmentation, and patch management stopped being abstract terms. The importance of proper network separation and strong credentials became obvious through experience rather than slides.

We ended each session with a recap discussion. Participants shared what surprised them, what challenges they encountered, and which risks felt uncomfortably familiar in their own environments. Together with the other companies present, we exchanged practical ideas on how to address those issues.

By the end of the afternoon, the conversation had shifted. Cybersecurity was no longer theoretical; it was something they had touched, tested, and understood.