STORMSHIELD

OPINION ARTICLE

OT AND CYBERSECURITY: A JOURNEY TO THE HEART OF OPERATIONAL INFORMATION SYSTEMS

Stéphane Prevost
Product Marketing Manager, Stormshield

Operational information systems are ubiquitous, from manufacturing plants to museums, shopping centres and public transport. By misuse of language, they are often reduced to industrial information systems or OT. They discreetly accompany our every move on a daily basis to guarantee our comfort and safety in all circumstances. This is a paradigm shift from traditional IT information systems which favour data security rather than safety and security of operation. However, the cybersecurity of industrial systems should not be neglected as the risks associated with cyberattacks are very much present. Let's take a more detailed look.

THE OMNIPRESENCE OF OT

In a certain collective imagination, OT (for Operational Technology) should only concern sectors such as the manufacturing industry, energy, health or transport. But the number of fields of application covered by OT is far greater than this popular belief: **operational information systems are absolutely everywhere.**

"*For example, in an airport, there is a visible part with lighting, fire detection, video-surveillance or air-conditioning. And a less visible part with baggage sorting systems, access controls for restricted areas, runway lighting...*", says **Jean-Christophe Mathieu,** Head of Industrial Security at Orange Cyberdefense. And examples abound: escalators, check-in kiosks, underground trains, cash registers, ticket dispensers or security gantries...even if these tools do not evoke the industrial world because they do not produce anything, they are operational systems in their own right. And, by the same token, they are critical systems.

"Cybersecurity for OT systems is therefore of paramount importance as it contributes to their operational safety."

Vincent Nicaise, Industrial Partnership and Ecosystem Manager at Stormshield

"*These operational information systems control equipment that acts on the physical world. An attack on the fire safety system can render the safety systems of a public building inoperative, for example,* says **Vincent Nicaise**, Industrial Partnership and Ecosystem Manager at Stormshield. *Imagine a football stadium plunged into darkness by a cyberattack targeting the lighting system...it is not hard to imagine the crowd moving in a panic and the disastrous consequences that would ensue. Similarly, a malicious attack on the dynamic signalling system that modifies the lane assignment signals in a tunnel can cause serious accidents.* ***Cybersecurity for OT systems is therefore of paramount importance, as it contributes to their operational safety.***"

THE SPECIFIC CONSTRAINTS OF OT SAFETY

While it is common to confuse OT with IT because of their convergence, these two worlds are total opposites in their operational constraints. Thus, despite IT/OT convergence, the objectives are not the same: where IT processes data, OT steers it to operate a physical action with an impact in the real world. Moreover, while it is relatively easy to update a "classic" information system, its counterpart on the OT side, this "industrial IT" or "operational IT", is more complex. For example, you cannot cut off the activity of a sanitation and drinking water supply network without direct consequences on the distribution - which requires the finest organisation and planning of updates.

Moreover, information systems set up in industrial environments are generally set up for long periods (thirty years or more). They are **ageing and, therefore, fragile**: obsolete components, no or few integrated cybersecurity mechanisms, management patches that are complex to implement, etc.

Finally, **the environments are often restrictive, even hostile,** with their specific operating conditions (dust, very low or high temperatures, vibrations, electromagnetism, harmful products in the vicinity, etc.) and the sometimes difficult access possibilities (tunnels, pumping stations, electrical substations, isolated places, etc.).

Thus, the main concerns of OT security are to avoid personal injury, environmental and material damage, and to maintain industrial activity, even in deteriorated conditions. "*It is above all a question of dealing with episodes such as the attempted attack on the Israeli water network last April, during which chlorine or other chemicals could have been mixed with the water in the wrong proportions*", describes Vincent Nicaise. An attack in line with those against the French factories of Fleury Michon in April 2019 or Honda in June 2020, with the impossibility in both cases to continue operations on the production lines. In addition to this concern for operational safety in OT, system availability takes precedence over data integrity and privacy. A big difference with IT, which is going to prioritise privacy first and foremost. "*There are exceptions in certain sectors where privacy is still important. This is the case, for example, with pharmacology, which scrupulously protects its manufacturing recipes. Here, intellectual property is a real competitive advantage. But, for most factories, protecting manufacturing secrets is not a challenge in itself: in any case much less than having to keep hundreds of machines operational with operators who are not necessarily careful*", says Jean-Christophe Mathieu.

OT IN THE FACE OF CYBER RISKS

With IT/OT convergence and the ubiquity of digital technology, traditionally isolated operational information systems are becoming more efficient and agile. But this new flexibility goes hand in hand with new cyber risks. To protect against this and to guarantee cyber security for OT systems, let's look back at a few basic principles of digital hygiene.

- **Network segmentation**: IT/OT convergence and the digitisation of operational information systems is leading to a breach in these historically hermetic critical systems. Therefore, it is essential to set up network segmentation as provided for in the IEC 62443 standard dedicated to the cybersecurity of operational installations. It provides system isolation and limits the spread of a cyberattack.

- **Secure process communications**: controlled security requires a detailed knowledge of exchanges at process level. "*It is important to know the communication flows between the automatons as well as the exchanges with supervision*, says Vincent Nicaise. *Once you have this visibility, you need to be able to analyse the patterns and authorise only legitimate communications. In this way, any illegitimate order or exchange can be blocked. At this level of the information system, work on security is only possible if the security equipment is capable of analysing the industrial protocols used to control the process.*" Implementing protocol analysis goes a step further by guaranteeing the legitimacy of messages exchanged between automatons.
- **Securing remote maintenance and remote control:** within the framework of plant maintenance, the system integrator may be required to connect to the production network. Therefore, it is essential to authenticate the operator and to secure the communication flows between the industrial site and the maintainer, for example by encrypting them alongside installing a firewall or VPN. On the other hand, it is recommended to define their scope of intervention and to allow access only to what is strictly necessary. "*This is all the more important since there may be several dozen external participants who may intervene on various scopes of industrial systems*," Vincent Nicaise points out. The same applies to the remote control of distributed processes for which it is essential to ensure the security of communications and guarantee data integrity.
- **Securing monitoring workstations:** in this inflexible and ageing environment, malware can spread in no time at all. Supervisory workstations use operating systems that are often obsolete, which makes it difficult to secure them. "*In this case, we need to be able to harden the workstation and implement a whitelist (or allowlist) of the applications that are strictly necessary,* says Vincent Nicaise. *This way, we will be able to block any malicious application or process that tries to get started. We should not forget that most of the production stoppages in recent years have occurred because of ransomwares that have taken over the supervisory workstations in the factories. Hardening them is therefore essential.*"
- **Controlling the fleet of USB flash drives:** a point not to be underestimated, since many USB flash drives are still used in the operational world. Whether employees or outsiders who wish to collect data on the supervisory workstation or update automated devices. The same list principle can be applied in this case: any operation from an unauthorised profile is rejected.
- **Data security:** data protection is essential in the pharmaceutical and food industries where it is vital to have traceability of everything that has been produced or processed. But, generally speaking, in the event of a cyberattack, a manufacturer must be able to recover their data at any time and reinject it into the information system. In this case, a backup of the PLCs (programmable logic

"*All these layers of security are elements of an in-depth defence system,*" says Vincent Nicaise. This approach is encouraged by the French National Agency for the Security of Information Systems (ANSSI), whose memo published in 2004 remains fully relevant.

THE NEED FOR IT TO UNDERSTAND OT

The IT world often considers the world of OT to be too standardised with many requirements to be respected. However, if IT understands the OT ecosystem and its issues, it can prove to be a real added value for the latter. "*The elements to be protected are sometimes located in geographically remote, almost inaccessible places: therefore, they lack human resources, real experts. The only on-site maintenance agents are those who manage the firewalls, which is a problem in itself, since they do not have the network and cyber knowledge to replace faulty equipment. One of our customers had this problem: together with the integrators, Stormshield has developed a specific process that meets this challenge,* says **Khobeib Ben Boubaker,** Head of Industrial Security Business Line Stormshield. *Another of our customers, who had chosen our Endpoint solution, was wondering how to shut it down in case of maintenance, without an expert on site. The idea was to put a specific file on a USB key recognised only by our solution and unreadable by third party solutions; this would then go into an unrestrained phase during maintenance time. These kinds of little things, which IT people are used to doing, help the OT people a lot.*"

To conclude, in addition to protection against proven threats and abnormal behaviour, it's vital to introduce a number of restrictions on the workstations. But this must be achieved as part of an approach which also attaches great importance to raising awareness of the need for "digital hygiene" along with greater accountability for users. One of the lessons to be learned from the current health crisis is that whatever we may think, rules and personal discipline are needed to stave off a persistent threat. In a constantly-changing environment, we must also take account of the fact that the degree of "severity" of these rules can and must evolve. Adaptation is therefore the key here. To achieve this, it's vital to draw parallels with users' personal lives. "*If people firmly believe that this can have an impact on their personal life, they will be likely to repeat it in their professional life*", stresses our colleague the CISO in the aeronautical sector.

"When IT/OT governance is unified, there is a better integration of cybersecurity for industrial systems."

Jean-Christophe Mathieu, Head of Industrial Security at Orange Cyberdefense

In a webinar on hospital buildings, we asked the question of **who is responsible for the OT network**. For two-thirds of respondents, IT will manage this operational network, improving its understanding of the subject as it goes along. But this lack of collaboration between IT and OT teams is a hindrance to the overall cybersecurity of companies that wish to take full advantage of their convergence to increase their competitiveness. According to Jean-Christophe Mathieu, "*very often the subjects surrounding industrial security are entrusted to the IT teams. However, while OT is an environment with which IT is becoming increasingly familiar, it is not yet familiar enough to decide unilaterally on the solutions to be implemented. For cyber security to integrate harmoniously into industrial systems, there must be joint work between IT and OT teams.*"

Finally, is the main challenge of operational and industrial cybersecurity a human one? Dialogue between IT teams, with their experience in cybersecurity, and OT teams, with their specialist skills in their own operational network, would therefore be the real key to better security of the overall infrastructure. Some manufacturers seem to have understood that these industrial cybersecurity issues require an increase in their teams' skills. And encourage their CISOs to train in OT and the operational and organisational constraints of these systems. This increase in skills is reflected in the appointment of first OT positions reporting to CISOs. **What if IT/OT convergence also involved a convergence of teams?**

STORMSHIELD

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. Further information: www.stormshield.com