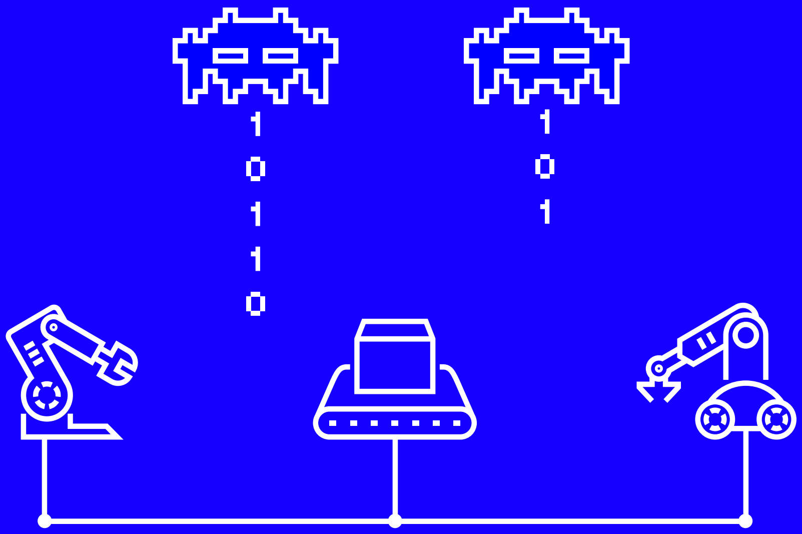

White Paper | April 2021

Recommendations for Better Cybersecurity in the Belgian Manufacturing Industry

Based on the report 'Cybersecurity in the Belgian Manufacturing Industry: Which businesses are ahead of the game?'

.AGORIA

howest

GHENT UNIVERSITY

sirris
driving industry by technology

Contents

Context

Agoria, Sirris, Howest and Ghent University carried out a study into industrial cybersecurity in the Belgian manufacturing industry. The main conclusions of the research are:

1. There is very little awareness and knowledge of cybersecurity risks in OT among our manufacturing businesses.
2. OT security policy is in many cases non-existent, rarely integrated with IT security policy and clearly subordinate.
3. Those responsible for OT often lack essential basic information to implement an effective security policy.
4. The OT environment is technologically very vulnerable.
5. Our manufacturing businesses are often unable to react adequately to and rapidly recover from an OT cybersecurity incident.

Recommendations

in the following section we dive deeper in to the 10 recommendations out of our study that should allow businesses to critically reflect on their cybersecurity approach for OT. It is important to state that there is no “silver bullet” for industrial cybersecurity: each business has its own infrastructure and risk profile.

Nevertheless, most of the recommendations are applicable to a large number of businesses. Do you have feedback? Don’t hesitate to share it with us.

Scan the QR code to read the report in Dutch or go to **www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie**

Scan the QR code to read the report in French or go to **www.agoria.be/fr/etude-Cyber-securite-dans-industrie-manufacturiere**

RECOMMENDATION 1

Implement from the top down a positive, learning security culture for safety, cybersecurity and business continuity, based on systems thinking

Learn from 'security' in other domains

For businesses, a positive organisational culture for business continuity and resilience (see book by Jan Dillen[1]) is necessary to properly deal with risk management, safety, security and, bottom line, survival. Cyber security is a small element within this much larger category, and there is a lot to be learned from the basic principles of 'safety' in the context of the relatively young domain of cybersecurity.

In aviation, for example, a safety culture (Just Safety Culture[2]) dominates, with one of the fundamental principles being that security needs to be treated as an entire system, not as individual parts or events. Everything is connected and nothing is entirely independent. A serious incident is therefore usually a series of failures of policy, people and training, procedures, communication and technology.

This is also the case in cybersecurity: incidents written about in the press are rarely the result of one single wrong mouse click. For a number of businesses that have had to deal with serious cybersecurity incidents, we notice that the causes are often the result of the lack of top-down security policy, pressure to give priority to productivity and profitability at the expense of security, negligence[3] and lack of care[4], such as not taking staff seriously when they report security problems.

Security culture starts at the top

A positive corporate culture regarding security can only exist if it is supported and actively promoted by top management. In companies where risk management is systematically done and physical safety on the work floor is part of the DNA, it's just a small step to implement cybersecurity into this safety culture.

A safety culture should promote and support learning. Based on this learning safety culture, initiatives should therefore be set up to allow teams to learn from each other, and thus acquire cross-functional knowledge within teams about IT, OT and cybersecurity.

Finally, cybersecurity is important but of course also requires money and resources: make sure to provide sufficient budget. Security is often invisible and therefore regarded as a cost to be optimised. By promoting safety and security as important corporate values and communicating transparently about it, you create a positive and reliable image for the outside world, such as investors, banks, new employees, clients, partners, etc.

A cybersecurity culture is a journey, not a destination

Introducing a cybersecurity culture aims to change values and standards, and this obviously takes time. To start with this, we recommend that you consider the following actions.

- Carefully look for examples of how security is approached in other sectors. For example: security in aviation, the nuclear sector, drilling platforms, railways and shipping. In most of these sectors, knowledge of 'security' is decades older than in the digital world, and it is remarkable that many of the security best practices can be applied to cybersecurity.
- Exchange knowledge and experiences with peers from your sector via learning networks, informal gatherings or purely via proximity. Did you know that Agoria and Sirris regularly facilitate this, via cybersecurity learning networks, for example?
- Actively look for reports about cybersecurity incidents and try to learn from them. Ask yourself: could this attack have happened to us? How would we have detected such an attack and how would we have reacted? One example of a well described cyberattack is the one that took place at the University of Maastricht. Fox-IT wrote an extensive report[5] about it. Another is the Equifax data breach in America, about which the US House of Representatives published a 96-page report that is now even used as teaching material in many schools.
- Constantly gathering knowledge is a challenge; fortunately, there are specialised communities, forums and information subscriptions (e.g. Threat Intelligence) that provide relevant insights for OT and ICS. Subscribe to such a service, share interesting insights with colleagues and engage them in theoretical 'what if' discussions to reflect on emerging threats, tactics and scenarios..
- Organise cyber awareness training for management and the board from a positive, fact-based approach. Avoid 'fear, uncertainty and doubt' (FUD): scare tactics often only add to resistance and disinterest among top management. Give them knowledge, make good analogies and refer them to peers who are doing better. Provide cyber awareness training for all employees. Always start with the why[6] and give extensive examples, including cause and effect. Make sure that cyber awareness training does not come across as too simplistic and nagging.
- One of the best ways to encourage values and standards is to teach employees things they can also use in their private life. Give them training and tips to increase cybersecurity literacy at home, for example by looking at how children can be safe online, or how family members can choose smart passwords. By involving the whole family in the topic, cybersecurity quickly becomes part of their values and standards, rather than just a dry

policy at work. Perhaps you can also make professional security tools available for home use, such as a subscription to antivirus and firewall software.

- Encourage people in IT teams to take part in training about OT, and vice versa.
- Encourage curiosity: an employee asking about cybersecurity is a great example of engagement, even if the questions may seem irrelevant or ignorant. If approached positively, every question is an opportunity to turn an employee into an ambassador for cybersecurity.
- If possible and relevant, you may consider including certain security objectives in all employees' annual objectives.

Make cybersecurity a business enabler

From a helicopter view, our collective expectations about cybersecurity (and partly privacy too) are an irreversible progression, always moving forwards and never backwards. As an analogy, compare it with road safety: before 1991, it wasn't compulsory to wear a seatbelt in the rear of a car, but today we are unlikely to get in a taxi that doesn't have seatbelts. Where initially perhaps just one car brand took on safety, it's now a leading sales enabler for almost all brands.

So make cybersecurity one of your business enablers. If top management supports it, that will also make it easier to implement and follow all the other recommendations in this white paper.

To summarise

- Convince the top management and the board of the enormous opportunity that security offers: security is a socially evolving requirement that is gradually becoming part of everyone's values: customers, investors, employees, bankers, suppliers, etc. It is a given that all companies are moving in this direction: the choice is yours to keep up or lag behind. Make security part of your DNA.
- Introducing a positive, learning safety culture is an evolution, not a revolution. Look for inspiring examples from other domains, such as aviation and the nuclear sector.
- Promote curiosity, knowledge and knowledge sharing, and provide cross-functional cyber awareness training that focuses on the 'why'.
- Communicate transparently about cybersecurity, and promote the use of your own cybersecurity corporate values as a 'business enabler'.
- Look at processes that are currently not cyber, and see if it would make sense to add a cybersecurity component. For example, add a cybersecurity component to existing problem/incident/defect procedures.

RECOMMENDATION 2

Increase central visibility of all assets that need protection using asset management and scanning

You can't secure what you don't know you have

It is essential to have a clear overview of the entire IT and OT infrastructure at all times, as well as the network topology and how all assets are connected to each other. 'Assets' doesn't mean only hardware components, but also digital assets such as software, data, configuration information, logfiles and digital keys. For effective systems thinking and impact analysis, you must also map interconnectivity and data flows[7].

Architecture and inventory

To map everything, use the Purdue Enterprise Reference Architecture (PERA)[8], which is still very relevant for OT, even if it presents challenges in relation to IoT and edge computing (an architectural model that shifts a large part of processing tasks to the client side[9]).

Such an inventory should contain information such as:

- description and categorisation of the asset
- OS and firmware versions and their last update
- a list of employees who have access to these devices
- what kind of data these assets store, process and forward (classification)
- possibly even a history of incidents involving the asset

An additional option for your inventory is to automatically scan for new devices on the network. Specialised software exists that can do this, including in OT environments, though there are still significant limitations depending on the protocols used. Such solutions are usually based on a combination of examining the traffic that uses the various networks (passive scanning) and deliberate interrogation of all connected devices (active scanning).

> A fairly new trend is for manufacturing companies to work with only one manufacturer of OT equipment, which then supplies devices that can be centrally managed by means of a secure cloud application.

Procedures are king

OT inventory management is still a manual job in many cases, however. In that case, implement strict procedures to guarantee that the inventory is always accurately adjusted to purchases, replacements, relocations and decommissioning. However, as is always the case with manual inventories, they are not complete most of the time, and thus most likely give a false sense of security. So, the final recommendation regarding inventory: check regularly (for example once a year) that the inventory is accurate, regardless of whether it was maintained manually or automatically.

A fairly new trend is for manufacturing companies to work with only one manufacturer of OT equipment, which then supplies devices that can be centrally managed by means of a secure cloud application.

To summarise

- Make an inventory of all IT and OT assets.
- Map the physical and logical interconnectivity between all assets.
- Define and implement a strict process to ensure this inventory is always up to date.

RECOMMENDATION 3

Draw up an integrated IT-OT cybersecurity policy based on both estimating and consciously dealing with risks

Start with a risk analysis

The question is often asked: when is there 'enough' cybersecurity? Of course, 100% cybersecurity doesn't exist, and no organisation has unlimited resources. Determining a cybersecurity policy is therefore always about seeking a balance between risk and investment, freedom and impediments, investment and its return. To help businesses apply their resources most efficiently and effectively, we recommend following a risk-based cybersecurity strategy. For businesses that operate critical infrastructure, or organisations with a high-risk profile such as defence, determining the risk profile requires a detailed and scientifically based approach. For the majority of businesses, it is sufficient to classify risks, probability and impact, for example, as low, medium or high, without going into too much detail.

Decide how you will handle risks

Identify and group all IT and OT assets on the basis of possible threats and vulnerabilities, determine the severity of the risks (impact and likelihood) and record the most optimal and cost-effective measures. Most risks will be mitigated, some will be accepted and others will be (partly) passed on to third parties such as insurance companies or suppliers. It is also possible that as a company, you will decide to reject a particular risk, for example by deciding not to work for particular categories of clients and therefore not be subject to strict regulations.

> Clearly communicate internally the outcomes of this risk assessment. Determine in your policy how you deal with possible risks and what the approach is for certain technical solutions.

Clearly communicate internally the outcomes of this risk assessment. Determine in your policy how you deal with possible risks and what the approach is for certain technical solutions. As a company, you can use the objectives of confidentiality, integrity and availability to calculate the possible impact in case one of these three is compromised for a particular asset.

How to carry out a risk analysis

There are various methods for carrying out a risk and impact analysis. The most common is a Business Impact Assessment (BIA[10]). Another more practical method is scenario thinking. To simplify this scenario thinking, there are number of methods and models, such as STRIDE-LM[11], which can map threats such as spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege and lateral movement.

Mapping threats (or Threat Modelling) is best done alongside an up-to-date list of potential attack techniques and tactics. You can find these on the MITRE[12] website, for IT security, mobile security, ICS and operational security.

This step should identify the most likely routes of attack and assess their potential impact. As well as direct damage such as loss of productivity or turnover, don't overlook other forms of damage such as physical damage, environmental damage, reputational damage, damage related to intellectual property, data leaks and possible fines, the costs of remedial measures and compensation to victims. Do not work this out in detail, but only in orders of magnitude. Invest the most where risk and impact are highest.

Systems thinking wins

In such an exercise, systems thinking is essential. Hackers or malware find their initial entry point in the place of least resistance, from where they can jump through the network from one component to another (lateral movement). It therefore makes no sense to heavily protect the production environment but then to connect the unsecured computer that controls the air conditioning to the network and a 4G dongle (a real example). Always try to determine where the weakest spot is through which malware or a hacker could enter.

Risk-based security policy and certification

Summarise all agreements in the risk and security policy with general rules and more specific procedures. Communicate them to employees and nominate a person to be responsible for these procedures, so that they are continually taught, evaluated and adjusted in a team context.

A security policy includes a description of:

- roles and responsibilities
- architecture
- risk management
- factory security
- network security
- security of individual systems
- security of information/data

More advanced companies will also define metrics that allow them to measure the effectiveness of their policy and will often track the progress of their cybersecurity maturity[13] in relation to accepted frameworks[14].

To professionally integrate the policy in the organisation, you may consider certification (see recommendation 10). But while waiting for certification (or not), it is always useful and interesting to compare the criteria and emphasis of various relevant certificates, e.g. ISO27001 and IEC62443[15].

To summarise

- Start with a thorough risk analysis, decide and communicate the decisions taken in this risk assessment.
- Use systems thinking to map the connections between devices, processes and data.
- Based on the risk analysis, draw up a coherent IT-OT security policy with rules, procedures, roles and named responsible persons.
- Determine metrics, success factors and a future vision.

RECOMMENDATION 4

Implement network segregation

Splitting up prevents outbreaks

Computers in an IT network are usually fitted with antivirus and firewall software (such as Endpoint Detection and Response, EDR), usually use a recent and still supported operating system, and are typically automatically provided with the latest firmware and software patches. This ensures they have a high level of self-protection.

For devices in an OT environment, on the other hand, the opposite is true. There is often no option to install automatic patches and updates, due to their long lifespan they often use old operating systems that are no longer supported, and there is rarely the option to interrupt production by providing the latest firmware and software patches. As a result, they are very vulnerable because bugs that have been discovered are publicly known and can be exploited, for example to obtain root access, to change the programming or to destroy the firmware.

> They are very vulnerable because bugs that have been discovered are publicly known and can be exploited, for example to obtain root access, to change the programming or to destroy the firmware.

> The minimum acceptable degree of network segmentation ensures the splitting up of IT and OT networks through firewalls, as well as the segmentation of devices that are connected to the internet.

Minimally split IT and OT

The most suitable way to work with such vulnerable devices is to place them in logically separated networks. This technique is called network segmentation. Technology that can allow or block traffic between segments in a smart way is referred to as segregation. For example: if two devices are in separate networks with a firewall between them, this is segregation. The minimum acceptable degree of network segmentation ensures the splitting up of IT and OT networks through firewalls, as well as the segmentation of devices that are connected to the internet, either because they can be reached via remote access or because they themselves connect directly to the internet.

Zero Trust architecture

In the past, segmentation could only be realised with hardware, but today segmentation can also be done with software, i.e. via virtual network segments. The latest evolution in this trend is Zero Trust Security Architecture, in which each device effectively forms an individual network segment in itself. In principle, this ensures that if a device is compromised, it is not possible for malware or a hacker to move from one compromised device to another. Moreover, Zero Trust offers additional benefits such as authentication, authorisation and central orchestration of security policies.

To summarise

- Split IT and OT networks into small segments and place firewalls between these segments, so that malware is no longer able to move from one device to another.
- Ensure that only strictly necessary communication between segments is allowed, and block all other traffic.
- Note: Network segmentation is the subdivision of the network into parts. Segregating a network is ensuring there are rules regarding communication between the parts.

RECOMMENDATION 5

Continually and adequately evaluate and manage vulnerabilities through risk and vulnerability management

Threat and vulnerability management

Risk and vulnerability management is the process of identifying, evaluating, handling, monitoring and reporting insecurity and bugs in device software and firmware. In an IT environment, this is a recognised and robust process, and is usually talked about in the same breath as patch management and vulnerability scanning. Active scanning for vulnerabilities is usually impossible in an OT environment, as scanning can result in production interruptions. There are various solutions that can detect vulnerabilities through analysing all network traffic (passive scanning).

Combine with asset management

Recommendation 2 advises increased visibility through actions including the implementation of asset management solutions. Based on the asset inventory, you can track to what extent devices have particular vulnerabilities and how urgently they need to be resolved. Keeping an eye on this manually for all devices based on newsletters from manufacturers is a hopeless task. Good vulnerability management software downloads the latest information about vulnerabilities for all devices in your inventory. Such a solution offers an overview of all the vulnerabilities of all OT devices in use at a glance, as well as the recommended action and urgency. Vulnerabilities can then be reduced as a matter of priority by installing patches, performing software updates or replacing devices.

Minimise vulnerabilities through hardening

Vulnerabilities can also be reduced by deactivating unnecessary applications, services or protocols on devices. Operating systems come with many optional services and capabilities as standard, all of which can have certain vulnerabilities and which are often enabled by default, even if they are not used, and can usually be disabled or removed. Think of the Microsoft IIS web server, the SMBv1 protocol, support for USB keys or an FTP server component. Removing unnecessary services from a risk management perspective is known as hardening. The Centre for Internet Security has guidelines[16] and a hardened image available[17] for almost all operating systems.

Replace old devices, or at least protect them properly

Part of risk and vulnerability management is also that outdated devices or software that are no longer supported, and for which no security updates are available, should be replaced. In an emergency, when replacement is not an option, the device with outdated software should be placed in a separate, well-secured network segment (see recommendation 4).

Initial installation and decommissioning

During the life cycle of a device, there are two particularly important times when cybersecurity must be part of the procedure: 1) the initial installation of a purchased device, which must be placed in the correct network segment, updated, adjusted according to the firewall rules between the segregated network segments, configured, unnecessary services disabled, standard passwords replaced, etc. and 2) taking a device out of service, which must involve the removal of all configuration information and private information such as API keys, passwords and certificates.

To summarise

- Provide training, processes and technology to ensure continuous and adequate visibility of all known vulnerabilities of all assets in the company.
- Put in place rigid processes to ensure vulnerabilities are resolved quickly by installing patches, security updates, new software releases and firmware updates, and where this is no longer possible, isolate or replace the devices.
- Reduce the potential attack surface by removing all unnecessary services, protocols and programs from computers to reduce the total vulnerability (hardening).

RECOMMENDATION 6

Provide means to detect anomalies at various levels and to respond effectively (possibly in real time)

In-depth defence

Good security consists of many layers, and it would be wrong to rely on just one layer. A common analogy is the way in which additional safety measures made driving safer. For some time it was thought that to make a car safer the only option was to make it stronger and more robust: a car made of three tons of steel would be safer than one made of two tons of steel. This turned out to be incorrect; in fact, cars became significantly safer because additional measures were taken with regard to technology, training and regulations.

For example, it was initially not mandatory to have windscreen wipers and indicators, to wear seatbelts or to crash-test vehicles that were put into circulation. Safety measures then led to a significant decrease in road fatalities: front and rear seatbelts, ABS, safety cells, traction control, seatbelt tensioners, airbags, active collision prevention, compulsory driving licence, compulsory roadworthiness testing and certification, etc. Additional security measures (technology, training, processes) result in exponentially increased security. Cybersecurity is no different.

Businesses need to implement multiple layers by which anomalies can be detected, in order to respond to them adequately. In its simplest form, an example of such security with multiple layers is the combination of antivirus software on a computer, a central service that scans all incoming and outgoing emails for viruses, training that teaches users how they should react to an alert and why they are not allowed to do certain things, and a policy that prohibits them, for example, from installing software and using USB sticks. Each additional measure contributes to greater safety. For IT networks, such multi-layered security (Defense in Depth, DiD[18]) is normal, and is increasingly used.

Many layers make OT safer

Our recommendation is that OT companies should also strive for a similar multilayer integrated DiD approach. The degree of integration of all the processes depends on the risk profile of the company and/or asset. For example: if an industrial appliance fails in a critical environment, you might begin a 'defect' procedure, but you might also begin a parallel procedure to investigate whether the appliance has stopped because of a cybersecurity incident and whether other suspicious anomalies have been detected, and immediately switch the incident response team to a higher level of preparedness. This integrated response example does not apply to environments with a low risk rating.

> Our recommendation is that OT companies should also strive for a similar multilayer integrated DiD approach. The degree of integration of all the processes depends on the risk profile of the company and/or asset.

Security layers

We recommend that such multi-layered DiD security consists of at least:

- Network Detection and Response (NDR) solutions software and/or hardware that scans network traffic for anomalies. The OT network traffic has certain predictable patterns, based on which anomalies can be detected and reported. Depending on the industrial environment, these solutions can also provide response actions, though an operational checklist will usually be applied after detection to detect and remedy a problem. Without exception, all outgoing traffic from the OT network to the internet must go via an NDR solution, which allows or denies communication on the basis of white lists and in-depth analysis. Network taps or span ports on switches should provide as much insight as possible into internal OT traffic: between and within the different Purdue levels. It is also vital to get a good overview of all protocols used, which can be achieved through such NDR products.
- Endpoint Detection and Response (EDR) software where possible, such as antivirus and firewall software on all computers connected to OT devices. Often these computers are still based on outdated operating systems such as Windows NT, Windows XP, DOS, unix, OS/2 and old versions of Android. It can be a challenge to find an EDR solution for such old systems.
- A secure, integrated remote access solution, for example based on virtual private networking (VPN) or Zero Trust, which can analyse traffic, detect anomalies and provide response. People also use 'jump hosts', a kind of gateway that restricts access to an underlying network (e.g. supervisory or control zones).

- Secure DNS: devices that want to connect to the internet will usually reach services (IP addresses) using Domain Name Services (DNS). Anomalies can be discovered by keeping records of and investigating DNS requests. Using a secure DNS provider such as Quad9 also adds an additional security layer. Good visibility of DNS traffic is a very important part of incident detection.
- Solutions to detect suspicious changes to files and configuration data: File Integrity Monitoring (FIM) makes changes to files visible; these insights can then be used to flag suspicious changes. There is also software that detects and monitors configuration changes. Some solutions are also able to detect suspicious changes to the programming of PLCs.
- A cross-functional IT-OT Security Information and Event Management (SIEM) solution that aggregates, analyses and stores all security events such as alarms, logs and authentications, and enables the company to quickly detect threats from one centralised dashboard. It is possible to allow IT and OT SIEM to exist independently, but there should always be a method to aggregate information and coordinate actions between teams.
- It is essential to understand that simply investing in a tool is not enough. It is imperative that IT and OT teams work together on security, and that IT and OT expertise is combined through active involvement and knowledge transfer. Defined processes for IT and OT should provide a feedback loop (IT <-> OT).
- Finally, detection and response must be firmly anchored in policy by designating by name those responsible, their tasks and processes.

To summarise

- Implement multiple layers or levels of security in which knowledge, technology and processes are always provided to adequately deal with detected incidents.
- Invest where possible in Network Detection and Response, Endpoint Detection and Response, secure remote access with Detection and Response capabilities, secure DNS, File Integrity Monitoring, cross-functional IT-OT Security Information and Event Management (SIEM).
- Invest in training, IT-OT knowledge transfer and cross-functional IT-OT involvement.
- Clearly describe the governance structure and place people’s names alongside role descriptions.

RECOMMENDATION 7

Invest in incident response management and plans for business continuity

Processes and automation

Companies with high cybersecurity maturity have largely automated their incident detection and response processes, which means many incidents can be resolved entirely automatically or with very limited human intervention. A ransomware attack on an individual computer at a company with very high cybersecurity maturity will in most cases be automatically blocked, the computer will be isolated from the network, collection of evidence is automatically started and the incident automatically reported to the Security Operations Centre (SOC) or Managed Security Services Partner (MSSP).

The lower the cybersecurity maturity, the more incident detection and response depends on human intervention and ad-hoc activities. The opportunity for companies lies not necessarily in automating incident response but in drawing up practical and pragmatic procedures that describe how to respond in a number of scenarios.

> The opportunity for companies lies not necessarily in automating incident response but in drawing up practical and pragmatic procedures that describe how to respond in a number of scenarios.

Processes as a focal point for cyber awareness training

Companies should invest in their operational Incident Response Management processes, which describe practically how to respond to predictable cybersecurity incidents, starting from the most common scenarios, and where possible aided by automation and/or external partners. Without exception, all staff members who may be confronted with a cybersecurity incident should know what to do if they notice abnormalities. This is a very important subject in cybersecurity awareness training, and should form part of safety training. Always react positively when someone reports an issue they perceive as an abnormality or a cybersecurity risk, even if their assessment is wrong.

> Always react positively when someone reports an issue they perceive as an abnormality or a cybersecurity risk, even if their assessment is wrong.

React to impactful incidents

Unfortunately, businesses occasionally have to deal with advanced complex attacks (Advanced Persistent Threats[19] or APTs), such as attacks in a hitherto unknown category, using new tactics or methods, also known as 'known unknowns' and 'unknown unknowns'[20]. When something like this occurs, the Incident Response Plan is put into operation: the emergency button, so to speak.

An Incident Response Plan is a clear and concise written document that is easily accessible on various platforms (including non-digital), and includes the following subjects:

- The identification of the Cyber Incident Response Team (CIRT) that will be called together, their names, contact details, roles and responsibilities. For example, IT staff, OT specialists, production managers, HR, marcom, legal, etc.
- Decision criteria for escalation and various phases of incident handling and management.
- Action plans with immediate measures to prevent a greater impact, securing digital traces for the subsequent forensic investigation and briefing all personnel.
- An alternative method to ensure rapid communication between all staff in the event that digital assets are unavailable.
- Contact details for all external parties that should be involved, such as cybersecurity partners, government services, suppliers, (crisis) communication agency and legal experts.
- Overview of legal and contractual notification obligations in this context.
- A number of communication templates that can be sent to employees, clients and suppliers.

Proactive planning and practice are key

Here too there is a great opportunity: if companies have to rely on improvisation in such an emergency and only begin looking for external help at the moment of attack, they lose crucial time and risk making mistakes that cannot be undone. It is advisable to conclude an Incident Response Retainer contract with a specialised cybersecurity company before any attack occurs, which assures your company of rapid expertise and assistance in an emergency. This may be supplemented with an insurance contract. All companies should draw up such a plan and simulate the described scenario at least every two years, just as a fire evacuation should be practised from time to time. Training on OT cybersecurity incidents could also become part of existing OT security tests.

Ensure production continuity

Further steps are Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP). A BCP determines how the company can, as far as possible, ensure minimal continuity during major failures. This could mean an entire plant without electricity, internet, IT systems, raw materials or crucial employees. Business Continuity Manager John Duncan[21] of shipping company Maersk (which was the victim of a cyberattack in June 2017) describes, among other things, the strategic advantage gained from the fact that old fax machines could be retrieved to quickly restore critical communication between offices.

Businesses must ensure they retain access to certain business-critical information, even if all IT and OT systems[22] are unavailable for a month: contracts, essential payment and staff details, etc. Details that are important for production should also be secured: designs, plans, configuration files, manufacturing processes, ingredients, component lists, contact details for suppliers and subcontractors, etc. Keep this information somewhere safe and up-to-date, such as a bank vault, and in a secure manner, such as on an encrypted information carrier.

To summarise

- Set up practical and pragmatic procedures that describe how to respond to known types of cyber incidents in the most common scenarios.
- Create an Incident Response Plan that describes how your company deals with an incident of major magnitude and impact, and make contact today with suppliers you will need.
- Draw up a Business Continuity Plan based on scenarios in which the IT and OT networks are down for several weeks.

RECOMMENDATION 8

Implement a well-thought-out access policy

Authentication and authorisation

Computer-controlled systems are easier than ever to secure, but if they use easy-to-guess or default passwords, many of those security measures are useless. On the production floor, many passwords and pin codes are often not personal but are shared between various people.

For IT networks, there are a number of best practices that should be followed.

- Users should not have administrator rights.
- Passwords should be long enough, though the requirement to change them monthly has proven counterproductive and is no longer part of the NIST Digital Identity Guidelines[23]. The best passwords are short phrases that also include digits and punctuation marks.
- Centralise authentication where possible, for example via AD or LDAP.
- Ensure authorisation (is this person allowed access to this resource?).
- Accounts of users who leave the company should be immediately closed.
- Remote access is subject to increased scrutiny, especially when it concerns accounts from external companies.
- Accounts should be temporarily closed if multiple incorrect passwords are entered, to prevent passwords being guessed.
- Where possible, use multi-factor authentication.

- Authentications and incorrect attempts should be centrally logged.
- All access rights should be checked regularly to confirm that they remain accurate.
- Many devices also have their own administrative web interface for management and configuration: these must also be secured, and this is not always easy.

In most cases, these best practices can be integrated[24] into the industrial environment, though the age of the operating systems plays a part in setting up such access policy.

> In most cases, these best practices can be integrated into the industrial environment, though the age of the operating systems plays a part in setting up such access policy.

Physical access and vulnerability to theft

In addition to IT access, it is advisable to protect physical access to certain IT and OT components against theft and prevent the plugging in of personal equipment or bridging segmentation using cables. This can be done with lockable cabinets, possibly equipped with an alarm and/or camera.

To summarise

- Limit access rights to accounts that are strictly necessary; don't provide administrator rights.
- Access methods such as passwords, pin codes, tokens and badges must be strictly personal, and must be blocked as soon as access is no longer required (no longer at the company, long-term illness, etc.).
- Where possible use multi-factor authentication[25].

RECOMMENDATION 9

Include cybersecurity in your purchasing policy

Supply-chain cybersecurity

By formally including cybersecurity in your purchasing policy, you set clear and explicit requirements for suppliers of (partially) digital products and services. Cybercriminals are increasingly using vulnerabilities or configuration errors at suppliers to infiltrate larger companies. This is fairly well-known territory in the field of IT security, where the API economy enables companies to provide digital services to each other. Supply chain security[26] is a domain in its own right, particularly at large, heavily regulated businesses, where suppliers must prove their digital services are secure by means of questionnaires and security audits.

Question suppliers about their cybersecurity

Our research shows that in OT security, many opportunities for improvement remain with respect to cybersecurity of supplied digital products and services. We advise businesses

> Supply chain security is a domain in its own right, particularly at large, heavily regulated businesses, where suppliers must prove their digital services are secure by means of questionnaires and security audits.

to routinely question suppliers about the security of their products, how quickly they can guarantee software updates after a security leak or vulnerability, how long these updates are guaranteed for, how they approach cybersecurity themselves in the development process, and if they have particular security certification such as ISO 27001.

Cybersecurity can also play a greater role in the choice of products to be purchased, for example by requiring them to be tested against industry standards such as OWASP ISVS for connected devices, OWASP ASVS for web apps or CIS benchmarks for cloud configurations. Be sure to also ask about product certification; there is currently much progress in the EU[27] in this field.

> Because many companies ask their suppliers these questions, a chain reaction will eventually start throughout the entire supply chain with a positive impact on cybersecurity.

Because many companies ask their suppliers these questions, a chain reaction will eventually start throughout the entire supply chain with a positive impact on cybersecurity.

As a business, you can also be proactive by informing prospective suppliers that security is an important corporate value and explaining how the company approaches this at the top level. Proactive transparency on the subject is generally experienced as trust-enhancing.

To summarise

- Ensure that cybersecurity and privacy demands are part of your purchasing policy.
- Draw up a list of standard cybersecurity questions for suppliers of IT or OT services or equipment and make the answers part of your decision criteria for working with these suppliers.
- Routinely survey your current and new suppliers and make cybersecurity a regular topic of conversation.
- Communicate proactively about your own safety policy with customers and suppliers.

RECOMMENDATION 10

Test, document, improve and audit your IT-OT security policy, and consider certification

Cybersecurity is like a quality system

An effective IT-OT cybersecurity policy strives for high resilience through successful and sustainable security of all digital assets in the IT and OT environments. Such a policy ensures, among other things, that there is a predictable response to threats and incidents. But does it work? Regular testing of the policy is essential to detect shortcomings and adjust the policy.

Businesses indicate that it is not usually difficult to implement a new technological cybersecurity solution, to write the processes and guide employees. The real difficulty lies on the one hand in promptly and effectively following the processes, and on the other, the routine evaluation of test results and making adjustments based on the lessons learned. Anyone familiar with the Plan Do Check Act cycle will recognise this; these difficulties are no different for the field of cybersecurity. When a company draws up a cybersecurity policy, testing is necessary to determine whether it has the intended effect and achieves its goal.

Blame-free learning attitude

Testing can be done in many ways, but always keep in mind that a test should never result in an employee being blamed. It is essential that tests are conducted and discussed calmly, with curiosity and without blame, in order to cultivate an open culture where employees are never afraid to notify that they may have made an error, ask questions or report a failing process. Every mistake or shortcoming found should be viewed as an opportunity to learn and to adjust the policy.

Tests can be carried out from helicopter level to technical level on the work floor:

- Testing of Business Continuity and Disaster Recovery plans.
- How long does it take before files can be restored from a back-up? Can the processes be started if certain other processes are unavailable?
- Is connection to the network always necessary? Do all services still work if traffic is via the back-up line? After all the redundancy, is there still a single point of failure?
- Simulate a large-impact cybersecurity incident in which the Incident Response Plan is implemented.
- Test employees' knowledge about the applicable procedures in the event of an IT or OT cybersecurity incident.
- Test people's behaviour by, for example, asking for passwords, badges or security information, or leaving a 'lost' USB stick somewhere and seeing if it is plugged into a company computer.
- Test the vulnerability of devices and software, from both inside and outside.

OT testing challenges

An important aspect in testing industrial security is the guarantee that the test itself doesn't disrupt the production process. What happens to the test results? There will likely be a recommendation that system or firmware updates should be installed, but it is best for the company to determine in advance the criteria for updating firmware. An industrial security test includes a clear understanding of the scope of the test, the list of attack routes through which a potential attacker can enter, based on a risk assessment, the actual tests, and the conclusions with vulnerabilities and proposed actions (mitigating measures, configuration changes, software and firmware patches).

In order not to disrupt the production process, you can also choose to implement the tests in a controlled lab setting, possibly supplemented with theoretical testing and an architecture review.

To summarise

- Effective cybersecurity is not a revolution but an evolution that follows a roadmap of step-by-step improvements.
- Test the effectiveness of your individual controls, as well as the effectiveness of your safety policy as a whole, and document where it went well and where it went less well.
- Determine objective criteria against which you can measure the progress of your policy and set annual improvement objectives.
- Improve your policy based on perceived weaknesses or inefficiencies.

References

1. https://www.innipublishers.com/product/nieuw/naar-een-positieve-organisatie-cultuur-voor-bedrijfscontinuiteit-en-resilience/
2. https://skybrary.aero/bookshelf/books/2882.pdf
3. https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf
4. https://www.computerweekly.com/news/252498423/Cyber-security-complacency-puts-UK-at-risk-says-NCSC-head
5. https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt
6. https://simonsinek.com/product/start-with-why/
7. https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport
8. https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security
9. https://www.infradata.be/resources/wat-is-edge-cloud/
10. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bi-analysis
11. https://csf.tools/reference/stride-lm/
12. https://attack.mitre.org/matrices/
13. https://www.enisa.europa.eu/publications/maturity-levels
14. https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model
15. https://blog.nviso.eu/2021/01/04/securing-iacs-based-on-isa-iec-62443-part-1-the-big-picture/
16. https://www.cisecurity.org/resources/?type=benchmark
17. https://www.cisecurity.org/cis-hardened-images/
18. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/
19. https://en.wikipedia.org/wiki/Advanced_persistent_threat
20. https://cyber.forum.yale.edu/blog/2019/3/26/known-unknowns-and-unknown-unknowns
21. https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maerk%27s_NotPetya_cyber_attack
22. https://us-cert.cisa.gov/ics/Abstract-ICS-Cyber-Incident-Response-Plan-RP
23. https://pages.nist.gov/800-63-3/sp800-63-3.html
24. https://resources.infosecinstitute.com/topic/credential-management-and-enforcement-for-ics-scada-environments/
25. https://en.wikipedia.org/wiki/Multi-factor_authentication
26. https://www.ncsc.gov.uk/collection/supply-chain-security
27. https://www.cybersecuritycoalition.be/eu-cybersecurity-act/

Authors

Patrick Coomans

Agoria en Sirris

+32 477 40 53 09

patrick.coomans@agoria.be

Kurt Callewaert

Howest

+32 473 34 04 65

kurt.callewaert@howest.be

Wim Codenie

Sirris

+32 498 91 94 53

wim.codenie@sirris.be

Yves Schellekens

Agoria

+32 476 98 90 32

yves.schellekens@agoria.be

Contributors

Wolker Lemahieu

wolker.lemahieu@agoria.be

Alain Wayenberg alain.wayenberg@agoria.be

Tijl Atoui

tijl.atoui@howest.be

Johannes Cottyn

johannes.cottyn@ugent.be

Tijl Deneut

tijl.deneut@howest.be

Hendrik Derre

hendrik.derre@howest.be

Johan Galle

johan.galle@howest.be

Tinus Umans

tinus.umans@ugent.be

About Agoria

Technology federation Agoria paves the way for all technologically inspired businesses in Belgium that, through the development or application of innovations, strive for progress in the world. Together they represent approximately 310,000 employees. The organisation unites almost 2,000 technology businesses, of which 70% are SMEs. Agoria has about 200 employees.
Agoria's services and opinions are focused on digitalisation, the manufacturing industry of tomorrow, talent policy and training, market development, regulation, infrastructure, climate, environment and energy. Agoria aims to connect all those inspired by technology and innovation, increase the success of businesses and shape them sustainably.

Find out more at www.agoria.be

About Howest and UGent

The Hogeschool West-Vlaanderen (Howest) has 8 500 students and more than 800 employees. It offers students a diversified portfolio of 24 undergraduate and 13 postgraduate programmes. Howest is the largest university of applied sciences in Flanders in the fields of computer technology, cybersecurity, new media and digital arts & entertainment (Gaming and 3D).
UGent is one of the largest universities in Belgium. Its 11 faculties offer more than 200 programmes and carry out research in diverse scientific disciplines. The campus in Kortrijk offers three unique programmes: machine and production automation, circular bio-process technology and industrial design.

Find out more at www.howest.be and www.ugent.be.

About Sirris

Sirris is the collective centre of the Belgian technology industry, established in 1949 by Agoria. Every year, 150 Sirris experts help around 1,300 businesses to make the right technological choices and successfully realise their innovation projects. The combination of experts, exclusive high-tech infrastructure spread across the whole country and an extensive network of national and international partners gives Sirris a unique position in the field of technological innovation in Belgium. Around 2,400 Belgian businesses are members of Sirris and so have access to extensive services and knowledge.

Find out more at www.sirris.be

.AGORIA

howest

GHENT UNIVERSITY

sirris
driving industry by technology