CYBERSECURITY IN OT ENVIRONMENTS: REALITY TRUMPS SECURITY

THE CHALLENGES OF CYBERSECURITY

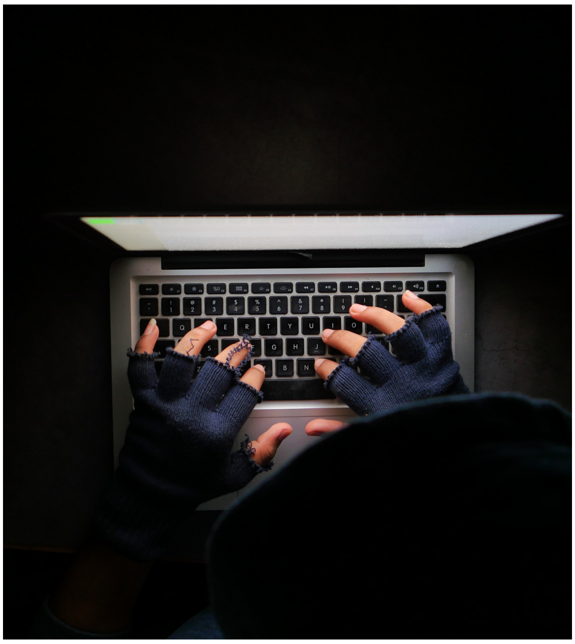
BY AG SOLUTION

Do you sometimes wake up in the middle of the night? Sweating in fear, knowing that IT and OT are at constant risk? That phishing and ransomware are a very real threat today and are the main cause of data loss, branding damage and downtime? Perhaps not. And yet ...

TABLE OF CONTENT

www.agsolutiongroup.com

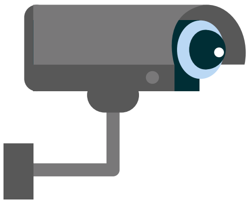
Introduction



Something is definitely going on and it has been here a while. In 2007, an infiltrator walked into the Iranian nuclear complex in Natanz with an infected USB stick to release Stuxnet into the system. *We would immediately detect this person in our OT environment?* They thought so too. And have no illusions: 'the dark side' innovates at a rapid pace. At the start of 2021, The New York Times reported that at least 250 American companies and government institutions had been directly affected by the SolarWinds hack. That is a lot more than what was first suspected. Who, what, where it all went wrong is one question, but the security hole was cause by updates to the SolarWinds Orion network management software. Updates, these things that occur on smartphones, networks and in professional IT and OT environments almost by default and on autopilot. Hundreds, thousands, tens of thousands of times per minute, per hour, per day.

Between the manual introduction of Stuxnet in 2007 and the mass breach via SolarWinds in 2021, there are not only a good thirteen years, but also a number of impressive evolutions. To refresh your memory: 2007 is the year in which the world got to know Mac OS X 10.5 'Leopard', Windows Vista, the PlayStation 3 and the very first iPhone. The first, indeed. Between then and now we also got to know WannaCry, Triton, Bluekeep & DejaBlue.

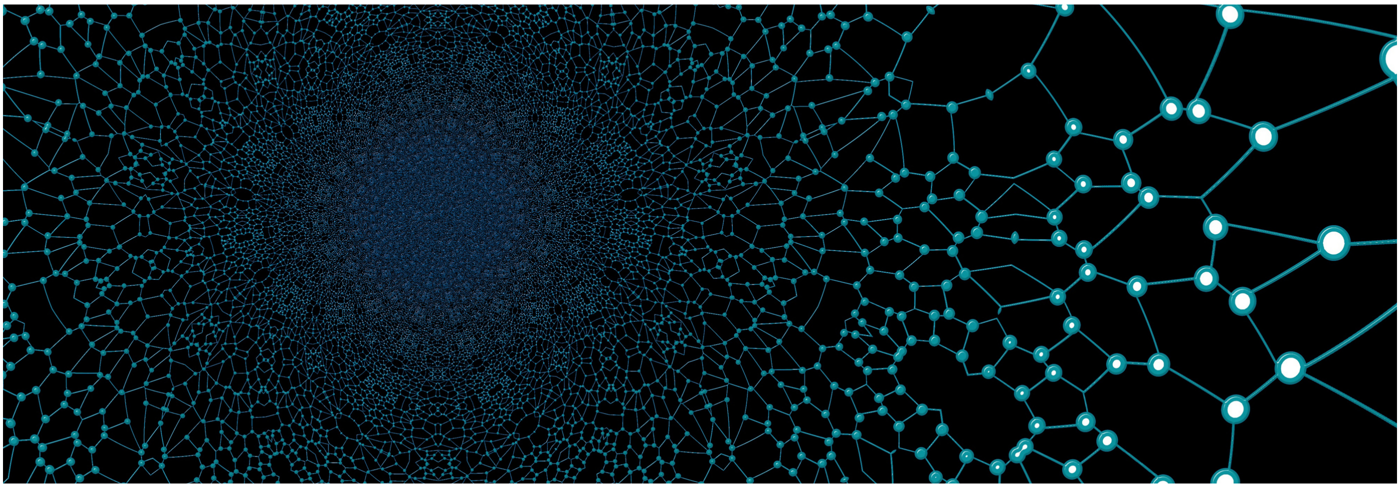
WannaCry infected over 200,000 windows computers in 150 countries on a single Friday afternoon in 2017 (figures: Europol). Renault, the UK's National Health Service and FedEx, among others, received a ransom demand in their mailboxes in exchange for resolving the encrypted information in their networks. In 2019, Microsoft itself disclosed two security holes (Bluekeep and DejaBlue) that allow an attacker to take over systems remotely and without the slightest user interaction. Simply connecting to the Remote Desktop Protocol (RDP) is sufficient. Every day employees and companies use this vulnerable connection to work remotely on their own systems.



‘In 2019, Microsoft disclosed two security holes (Bluekeep and DejaBlue) that would allow an attacker to take over systems remotely and without the slightest interaction from the user. The time of the lone hacker is over and well organised crime, thoughtful use of fast changing tactics and a deliberate strategy will take its place.’

Professionalism of cybercrime

With a little sense of minimisation, we could argue that such things are the work of hackers and cyber-enthusiasts operating in isolation and demonstrating the shortcomings of digitisation. And it may have started that way, but the professionalisation of bad intentions is undeniable. The 'OT/IoT Security Report (2020 1H)' by Nozomi Networks mentions a report by law firm BakerHostetler, which mentions a tenfold increase in the average ransom demand, to more than $300,000 per attack. Increasingly, ransomware attackers are choosing their targets specifically. The criteria? Sensitive information and, above all, sufficient budget to pay the ransom. Read: large companies, government institutions and the energy sector. And it must be said that this professionalisation is doing the cybercriminal no harm. The time of the solitary hacker is over and it is replaced by well-organised crime, the well-considered use of rapidly changing tactics and a well-considered strategy.



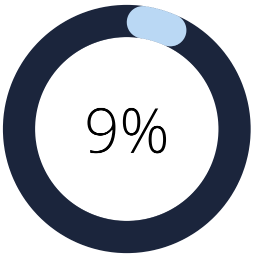
COVID-19 as an extra impulse

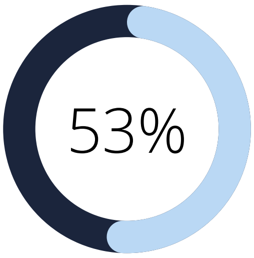
The current situation and the way we organise our society and our companies is an extra asset for cyber criminals. Although the outbreak of the coronavirus meant a brief standstill in society, after a few weeks we plunged headlong into home- and telework. Digitalisation on a global scale. Still in the 'OT/IoT Security Report (2020 1H)' by Nozomi Networks, it states that the FBI's Internet Crime Complaint Center (IC3) has recorded a fourfold increase in complaints since the start of the corona crisis. In absolute figures, we are talking about 4000 complaints. Per day!

There are a number of reasons to explain this serious increase. The fact that the outbreak of a worldwide pandemic - with the corresponding mortality rates, but also the many conspiracy theories and the fact that we, as humanity, do not have an immediate ready-made answer - causes a general concern and fear, makes people remarkably vulnerable. At home, behind the screen, without direct contact, without a sounding board and overwhelmed by the news and the multitude of information, it is not always easy to make a correct judgement. Phishing - of which we all think 'we won't fall for it' - is booming.

Increasing interconnectivity

'You don't have to be a multinational company, or a utility company in a medium-sized country, to be in the crosshairs of the cybercriminal. On the contrary. The fact that they are confronted with it mainly illustrates that there are virtually no safe havens anymore. Unless you create them yourself.'





Ransomware is also taking advantage of the opportunity. Besides this general human state of mind, there are also a lot more digital activities to observe during the radical and sudden switch to home and teleworking. Nozomi Networks notes that remote access to machines and private company networks in some companies increased from 9% to 53% in just a few days. The occasional home worker became the new standard overnight. Time will undoubtedly provide more up-to-date and very precise figures, but it is certain that COVID-19 has given remote working a serious boost.

Exact numbers are still to come, but Gartner, Inc. predicted about a year ago that the Internet of Things would increase by 21% by 2020. As much as the increase from 2018 to 2019 and now responsible for 5.8 billion connection points worldwide. The extent to which everything and everyone is connected to each other is increasing rapidly.

The question is whether our systems were ready for this. In practice, we were creating a huge number of new connections and links, all of which provide access to networks and systems. Online, virtual, digital, all well and good, but would you give a hundred passers-by a key to the factory gate? Andrea Carcano, co-founder and CPO of Nozomi Networks, states: "There's a risk of opening access to all of your plants. You're opening a new door that used to be closed. If it's an opening for you, it could be an opening for an attacker."

So there are new doors. More than half are simply open and for the others we have handed out lots of keys.

Linking IT and OT implies risks

THE THEORY

To be clear: the number of potential gateways was already on the rise. The link between IT and OT is not new. Let's dive into recent history. OT systems are ubiquitous and necessary: you use them to control a building's lift, a complete production process, but also the safety of a nuclear power plant. Until recently, the software used for this often had to be operated physically. Think of the lift, where you as a user press the right button to cause an action. OT as an autonomous system: no key, no access.

But, as we have written two paragraphs ago, we have recently added keys online, virtually, digitally. A lot. And access ports too, in the form of connections that we increasingly operate remotely. Today, more than ever, the OT environment is digitally connected to the outside world. In a way that allows someone to send the elevator to the top floor without having to press the button downstairs.

Is that a problem? It is always a problem, if only because the reliability of that elevator from our example becomes more uncertain. So much for that. The sectional garage door that opens when you turn in to the street with your car may, at best, close again right in front of you if someone gains access to the OT network. Annoying. There is little chance that your garage door, central heating system or self-dispensing coffee machine - although all OT and connected - will be targeted by cybercriminals who want to exploit the weaknesses of that specific OT environment.

It's a different story if your garage door fails while you are inside a running car. Opportunity and bad intentions, the combination is not ideal. And what if we are talking about the OT environment of a nuclear power plant? Vaccination lists? Or the production hall of your company? Recipes? Food safety? Dosage? What if it's about controlling and getting hold of sensitive info, in a place where, in the eyes of the cybercriminal, there is enough budget to pay a ransom?

Linking IT and OT implies risks

THE PRACTICE

The examples are numerous. We list a few below - the most striking - but there are more. Many more. Small and large. With annoying, expensive or downright dangerous consequences. And you don't have to be a multinational or a utility company in a medium-sized country to be in the crosshairs. On the contrary. The fact that they are confronted with them illustrates the fact that there are hardly any safe havens left. Unless you create them yourself.

A.P. Moller Maersk was forced to reinstall 4,000 servers and 45,000 computers in 2017 after a cyber attack by NotPetya, but above all had to stand idly by as port terminals came to a standstill worldwide. The Danish global player estimates the damage at around 300 million dollars and was adrift for a fortnight.

A petrochemical site in Saudi Arabia that had the dubious honour of being hit by TRITON in 2018 serves as an example of possible extra-financial consequences. The TRITON cyberattack led - fortunately for just about everyone - to a security freeze and not a complete disruption but may still be seen as a milestone when it comes to cyber security, or the lack thereof.

In the related category of 'utilities', we also mention the double attack on the Ukrainian energy grid. In 2015 and again in 2017, hackers left hundreds of thousands of households without power. The first incident made everyone look towards Russia, the second time the hackers are said to have been hiding for months in the IT systems of energy supplier Ukrenegro. Both attacks are considered the first of their kind, and it should be obvious that the potential social impact of something like this cannot be underestimated.

In 2019, LockerGoga-ransomware blocked the OT environment of steel giant Norsk Hydro. A manual system takeover was necessary, resulting in a temporary 50% reduction in production. In addition, the administrative part of the system was hit hard and, for example, the invoicing system was disrupted. Norsk Hydro needed weeks to put its affairs in order. Estimated damage from lost production and delays: 70 million dollars.

We could add to the list, but it should be clear by now: an OT environment is a controlling element in almost every sector today. From goods transport over energy to production and ultimately the IT-linked administrative handling of all these things. The impact of a targeted attack is great.

In a production environment, the spectre of stagnation is invariably looming. At best, because when processes are no longer controlled, safety is also at risk. Think of uncontrolled pressure, pumps and valves that refuse to work and sensors that fail. We have also evolved towards an economic just-in-time model, in which control and planning are crucial elements throughout the production chain. If one link in the chain gets stuck, this leads to problems in the entire process. Reliability has always been the key, and what is it that fails the most? Exactly. Reliability.

Need for awareness and insight

If we add Fortinet's 'report-2020-ot-cybersecurity', we see some interesting figures and findings. For instance, 9 out of 10 organisations in their research had to deal with a cyber-attack on OT-systems in 2020. For 65% of them, this was one of three breaches or attacks. Cyber attacks in the OT environment are clearly on the rise. Meanwhile, OT systematically gets too little attention when we talk about security. Remotely controlled machines seem to be something you only get to see in movies, while they have become daily reality.

Fortinet's report is an eye-opener in that respect, in the sense that it illustrates that the number of organisations and companies not having to deal with a break-in in the OT environment is dropping. Cyber-attacks are becoming more frequent, and while Fortinet is obviously not an unbiased research institute, the conclusion remains striking: the cyber security challenges are diverse and initially actually low-level: awareness, resources, personnel and training. Far from being innovative or earth-shattering, they are much needed!

Victims of cyberattacks often lack - at least at first - a basic awareness of the increased risks. On the shop floor, behind the computer, but also in the meeting room and at management level. At home, remotely or physically present in the OT environment. Adequate, effective security begins, of course, with the knowledge that there is a risk. With that awareness.

The lack of it is therefore a problem. Companies need a correct insight into their current situation in terms of cyber security. In general, but certainly in the OT environment, where we have created extra keys and digital doors at record speed.

Need for international regulation and a clear framework

The digital world is difficult to capture in an analogue code. This seems obvious, but the degree to which digital and analogue are intertwined makes it very complex to separate the two. From the analogue reality, it is therefore very difficult to tackle digital crime.

Whoever breaks into an office or production environment - smashing the window or forcing the door - knows that he or she is treading on dangerous ground. The necessary physical presence and the risk of being caught red-handed, at night, creates a threshold that is not there at all in digital circumstances. Terms such as 'burglary' and 'sabotage' are familiar to everyone and we can imagine them. Cybercrime" is much vaguer, or at least it is perceived as such. Yet all the examples described in this paper are just as much about sabotage and burglary.

An additional difficulty is that national borders, nationalities and analogous rules are not taken into account, and the regulations are actually lagging behind. Although there are efforts that can change this. The NIST Cybersecurity Framework of the American National Institute of Standards and Technology initially focused on operators of critical (and therefore high-risk) infrastructure in 2014 but has since been applied in many companies. In Europe, the NIS Directive has been part of the cyber security guidelines since 2016.

The ongoing debate as to whether governments should get involved, or whether companies should take responsibility themselves, is still partly ongoing and illustrates that we as a society are not ready to create a complete and conclusive legal framework for the time being.

Why is a cyber attack in the OT environment dramatic?

First of all, because "we"- a generalization that you may find exaggerated,- cannot sufficiently assess the impact of such an attack. Anyone who has ever paid a ransom after an attack on OT systems is fully aware of the potential consequences. In 2021, cybercriminals choose their targets carefully.

The first conclusion is that an attack on the OT environment disrupts an entire organisation. Uncertainty and unpredictability are the greatest enemy of any modern, planned, well-functioning business environment. The acute threat and the realisation that an entire process can be manipulated from the outside are, at best, unpleasant.

Unfortunately, the average cyber criminal does not go for 'the best of the best', quite the opposite. Brand damage, production damage, the disclosure of information, of data, of recipes, they are all possible consequences. In addition to production stoppage, damage, ransom demands and all indirect economic consequences.

Conclusion: what can we do today?

If government and regulation find it difficult to come up with a ready-made answer while cybercriminals are laughing their heads off and taking advantage of the new opportunities without limits or restrictions, then it has to come from the business world itself.
After all, the situation in our industrial environment has changed. Interconnectivity has increased and virtually no sector, no production, hardly even a production environment or a single production line still exists as a disconnected, mechanical island in the sea of global connections. OT, like IT, has become part of a network. A network with countless access ports and even more keys to fit them.

We can wait and point at law books, government agencies or the other, but actually every company, every business, every OT environment should first and foremost look at itself and question its own cybersecurity, evaluate it and adjust it where necessary.

THE CYBERSECURITY AUDIT AS A FIRST STEP

For AG Solution cybersecurity of the IT and OT environment is an integral part of the total package. Any digital transformation should, in an ideal world, fundamentally pay sufficient attention to it. At AG Solution we believe that a regular cybersecurity audit is and will remain the best way to get an up-to-date picture of the security state of your computer systems, IT and OT infrastructure. Every vulnerability poses a risk. Workstations, communication networks, servers ... they are all potential entry points and vulnerabilities. Opportunities for ambitious cybercriminals, who no longer limit themselves to data alone, but focus even more enthusiastically on machines, installations and production environments. With all the consequences this entails.

The cyber security audit is a first step. An inventory of the risks, the pros and cons, the digital watchdogs and alarm systems, but also the holes in the fence. Next steps include closing those holes and taking care of vulnerabilities. Acutely and in the future. Next steps also include analysing the damage and consequences of incidents, evaluating any repair and recovery costs, monitoring and ensuring production quality, as well as the safety of employees who are often at serious risk from a cyber attack in an OT environment.

Having a recovery plan is part of an integrated cyber security approach, in which a constant self-critical attitude is also crucial. Cyber security in IT and OT, as we see and approach it at AG Solution, requires a comprehensive approach. A total approach in which every employee pays attention to a basic security concept and in which that employee is an active part of a safe working and production environment.

AG Solution is your expert partner in industrial cyber security. And that is the only thing you can be 100% sure of.

SOURCES :

Fortinet. (2020, June). 2020 State of Operational Technology and Cybersecurity Report.
https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf
Nozomi Networks. (2020). OT/IoT Security Report. https://info.nozominetworks.com/ot-iot-security-report-1h-lp-0

AG Solution
Process Automation & Industrial ICT

BELGIUM – Antwerp
AG Solution NV

Katwilgweg 4, box 2
B-2050 Antwerp
T +32 3 569 20 35
contact@agsolution.be

SPAIN - Barcelona
AG Solution Spain SA

C/Pujades 350, Planta 4, Puerta 1
08019 Barcelona
T +34 93 624 02 75
contact@agsolution.es

SPAIN – Madrid
AG Solution Spain SA

Carretera de Fuencarral, 22
28108 Alcobendas, Madrid
T +34 93 624 02 75
contact@agsolution.es

FRANCE – Lyon
AG Solution S.A.S.U.

Part Dieu Danica
21 Avenue Georges Pompidou
69003 Lyon T +33 4 72 91 39 93
contact@agsolution.fr

FRANCE - Lille
AG Solution S.A.S.U.

Lille Europe 253 Boulevard de Leeds
59777 Lille
T +33 3 28 53 59 58
contact@agsolution.fr

GERMANY – Cologne
AG Solution GmbH

Kranhaus 1, Im Zollhafen 18
50678 Köln
T +32 3 569 20 35
contact@agsolution.de

UKRAINE - Zaporizhzhia
AG Solution Ukraine L.L.C.

Ukraine, 69057, Zaporizhzhia
Soboryni Av. 160
T +380 68 861 65 34
contact@agsolution.com.ua