STORMSHIELD

Yearbook

2020

2020: a busy year for news

Relive the year's highlights with the different awareness-building content produced by Stormshield.

If you had to sum up the year 2020, what would you say? This year will remain an extraordinary one from a health, economic and political perspective. And in the cyber sense?

All over the world, malicious cyber acts have played on contemporary circumstances, and even adapted to it – often taking advantage of the urgency of the situation and lower levels of alertness. And despite the growing media exposure these malicious cyber-acts are attracting, the work of raising awareness of cybersecurity issues clearly remains more relevant than ever. And this constant examination forms an integral part of the mission we have set for ourselves at Stormshield. In addition to providing protection for critical infrastructures, their sensitive data and operational environments, our mission is also to question, analyse, understand and share. Just as we did last year, we have decided to create special content that ties together all of our lines of thought drawn from 2020.

These reflections and questions are the result of a collective initiative which combines the opinions of our Product Marketing, R&D, sales and pre-sales teams. In these pages you will meet fresh faces who have joined us to enrich the quality of our teams and make this content more relevant. And because an initiative like this cannot be a solo effort, I am delighted to see even more external contributors featuring in these pages – whether partners, customers, researchers, academics... or just curious minds.

In this work of just over 150 pages, you'll find several different reading levels – to address varying levels of maturity and audience types. Papers to educate and raise awareness, pieces providing a more expert and cutting-edge angle, business perspectives and future projections: you're sure to find something of interest for you here. •

Part #1

Strong signals in 2020

Part #2

Weak signals in 2020

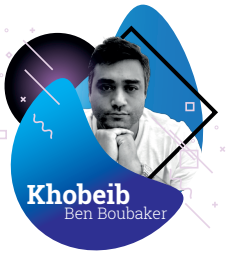
Part #3

The cyber question: food for thought

Part #4

Cyber solutions: facing up to the challenges of tomorrow

Authors
Stormshield



Khobeib Ben Boubaker
Head of Industrial Security Business Line

Matthieu Bonenfant
Chief Marketing Officer

Florian Bonnet
Director of Product Management

Adrien Brochot
Product Manager

Simon Dansette
Product Manager

Marco Genovese
PreSales Engineer

Pierre-Yves Hentzen
CEO Stormshield

Vincent Nicaise
Industrial Partnership and Ecosystem Manager

Julien Paffumi
Product Management Leader

Victor Poitevin
Digital Manager

Stéphane Prévost
Product Marketing Manager

Fabien Thomas
Chief Technical Officer

Sébastien Viou
Cyber-Evangelist Consultant

Contributors

Nebras Alqurashi
Business and Technical Development Manager for the Middle East and Africa Stormshield

"An attack on the electrical industry is an attack on the heart of how society operates. For example, if a cyberattack causes a blackout, this could have dramatic consequences and cause a wide range of human and material damage" p. 55

Charles Blanc-Rolin
CISO for a French regional hospital group

"In French regional hospital groups, only 1% of the overall budget is assigned to digital technology in general (including security), compared to 5-6% in Northern European countries" p. 68

Philippe Blot
Lead Expert Certification at the ENISA

"The idea is to create European pathways, a European form of governance, where all stakeholders agree on the rules of the game" p. 127

Markus Braendle
Head of Airbus CyberSecurity

"Europe must ask itself how dependent it wants to be on others for its cybersecurity, and find the right balance" p.127

Manon Deveaux
In charge of cybersecurity issues within TECH IN France's Public Affairs team

"The general public has realised that public services such as hospitals could also be affected, and that the consequences could be serious" p. 131

Franck Gicquel
Partnerships Manager Cybermalveillance.gouv.fr

"If we maintain a philosophy based on prohibition and punishment, we are perpetuating a view of the employee as a weak link in the security chain. And yet the whole point of awareness training is to make them the strong link!" p. 86

Raphaël Granger
Account Manager Stormshield

"From a cybersecurity perspective, by having access to this data, a hacker might more easily find out how to turn up the heat to the maximum setting, cut off the air intake, or prevent a fire alarm from going off... The tragic consequences are easy to imagine" p. 81

Alice Louis
Winner of the 2020 "Cyber Woman Trophy" in the category "Jury's favourite"

"This approach to ethics explains that the morality of an action must be assessed in terms of the consequences of that action. From this perspective, hackers become clear allies for organisations" p. 96

Jean-Christophe Mathieu
Head of Industrial Security Orange Cyberdefense

"When IT/OT governance is unified, there is a better integration of cybersecurity for industrial systems" p. 36

Fabien Miquet
Product and Solution Security Officer Siemens

"The world of IT has a strong focus on confidentiality and integrity: in the case of suspected attacks; there is an immediate tendency to disconnect the system. A factory, by contrast, needs to maintain uninterrupted production, and has to deal with both human and environmental risks" p. 42

Vincent Riondet
Head of Cybersecurity Projects and Services teams Schneider Electric France

"A person with an IT background won't use the same definition of SCADA as someone from OT" p. 38

#1 STRONG SIGNALS iN 2020

What will 2020's cyber trends be?

January 27, 2020

Every year, Stormshield experts put together an analysis of structural trends for the coming year. What major issues will the world of cybersecurity be facing in 2020? As with last year, we've been looking closely at a number of weak signals, the latest industry analyses, and the opinions of our experts. We project these into 2020, examining four assumptions (and four scenarios) which may shape cybersecurity in this new year. And not a crystal ball in sight...

By

Victor Poitevin

Trend 1:

the rise of multi-level phishing?

Weak signals from 2019:

In 2019, the share of main attack vectors composed of phishing attempts increased, according to a Microsoft report. And the level of sophistication seen in the methods used presents a challenge, with fake 404 pages, fake pages indexed with Google and even phishing campaigns disguised as assessment interviews!

The deepfake threat became tangible in 2019. In September, a British company fell victim to a CEO scam after an employee made a payment of £200,000 to a Hungarian provider. The employee had thought they had received a telephoned instruction from the CEO, but it was in fact a deepfake produced from a voice recording. Another example (this time involving images) was a video released in November, showing footage of Donald Trump announcing the worldwide end of the AIDS epidemic. But it was a false alarm: in fact, it was a campaign from a French association, based again on a deepfake. In addition to these items, Google announced that the rollout of Duplex, an automated phone calling system using artificial intelligence, was to be brought forward. So will 2020 be the year of deepfake-driven social engineering?

Possible scenarios for 2020:

The addition of deepfakes to the cybercriminal's arsenal poses a genuine technical challenge in terms of prevention and security. And most experts are fretting as they ponder the complexity of this threat. With deepfake production tools now starting to become universally available, it is highly likely that 2020 will see an increase in deepfake-driven phishing campaigns. So how does it work? Practically speaking, a deepfake could be used as part of a phishing or spear-phishing campaign. For example, imagine an audio deepfake presented as a call from an executive committee member, informing you that she's about to send over a PDF requiring urgent attention. And no sooner have you clicked on it than the ransomware is installed...

The threat of a 'deepfake-as-a-service', serving to increase the effectiveness of cyberattack campaigns, is therefore a serious one. So much so, that a report from the Forrester consultancy firm estimates the costs of deepfake attacks could be as high as 250 million dollars in 2020. However, creating a credible deepfake would appear to be a complex & expensive business. And it is precisely this cost factor which adds a caveat to the anticipated explosion. A team from the French newspaper *Le Monde* tried, and gave up: too complex and expensive. But will the same be true of cybercriminals with more substantial resources; for example, of the State-sponsored variety? Or small-scale independent experts? All this leads to the conclusion **that 2020 could be the year of multi-layered phishing attacks**, with simple campaigns – playing on the credulity of their targets using tried and tested techniques – and more complex campaigns, making use of the latest technologies to fool more seasoned warriors.

Events of 2020

In June, the American NISOS security firm published a report about an audio deepfake used by attackers to impersonate a company CEO. The voice message was created using computer software, but failed to deceive the targeted employee.

In October, mobile security solutions publisher Lookout conducted an educational phishing campaign targeting the top cyber players, meeting for the Assises de la Sécurité security conference in Monaco. Using the list of subscribers and phone numbers retrieved from LinkedIn, the publisher sent a message with a shortened URL, posing as a trusted sender. And the results speak for themselves: almost half the recipients clicked the text message link. Like the proverbial shoemaker whose own children go barefoot...

Trend 2:

will cyberattacks against food companies become commonplace?

Weak signals from 2019:

In April 2019, French giant Fleury Michon paid the price of a successful cyberattack which forced it to freeze its operations for five days. In December 2019, the Italian catering brand Fratelli Beretta was hit by the Maze ransomware, as was the Belgian beer company Busch afterwards. More than ever, the food industry seems to be in the eye of the cyclone, attracting the enthusiastic attention of cyberattackers of all flavours.

At the same time, public awareness of the issues involved in food production is increasing, and consumers are becoming more demanding. A telling statistic: 92% of Yuka users put products back on the shelf if they are badly rated by the app (according to co-founder Julie Chapon, citing an impact study in a September 2019 article on *Forbes*).

Possible scenarios for 2020:

A hypersensitive industry, a largely automated production chain and a quality assurance system which is a vital cornerstone of the industry: **all these aspects combine to ensure that the food industry will remain a high-risk area in years to come.**

Whether from a state-sponsored actor or a cyber-terrorist, it is highly likely that 2020 will see increasingly frequent cyberattacks against key players in the food industry. And some fairly grim scenarios can be imagined. For example, one in which a targeted attack could affect the programming of machinery, or force some industrial components to operate while empty, causing premature wear. Why? To sabotage the industrial installations in question. How? With a good old-fashioned USB key or a phishing campaign, designed to infect a workstation before spreading through the network. Some industry giants have foreseen this scenario and have implemented effective protection, and have as a result secured their assets. However, small- to medium-sized actors in this industry seem more vulnerable to this kind of cyberattack – which could lead to serious financial losses and a PR disaster in terms of brand image.

Events of 2020

In August, French company MOM (which owns brands such as Materne, Pom'Potes and Mont Blanc) fell victim to a cyberattack, probably via ransomware. The result was immediate, halting production at its four sites in France and the United States.

At the same time, the Brown-Forman company (one of the US's largest wines and spirits companies, owning brands such as Jack Daniel's), was also hit by an attack. The target: a terabyte of stolen data, which – according to the attackers – included confidential information on employees, company agreements, contracts, financial statements and internal correspondence.

Trend 3:

is tomorrow's malware already in place?

Weak signals from 2019:

"*Mass cybercrime is on the increase,*" emphasised Guillaume Poupard, Director General of the France's ANSSI cybersecurity agency, in an interview with *Libération*, another French newspaper, reflecting on developments in 2019. And indeed, 2019 did see the propagation of complex, large-scale cyberattacks. Consider, for example, the ransomware that hit the M6 TV station and Rouen's University Hospital in France.

In March 2019, the US attack on a power station in Venezuela provided an illustration of such large-scale cybercriminality, often conducted at State level.

In November 2019, a study revealed that some flaws and vulnerabilities have been in use for more than ten years by cyberattackers, and are still being exploited today. In some cases, the companies in question know where the vulnerabilities in their systems lie, but lack the resources needed to replace the affected applications. This scenario is a common one in the medical sector, which uses applications that are only capable of running on old operating systems. In the industrial sector, some IT components are retained even when obsolete, accentuating the risk of being targeted by an attack 'planted' several years ago. Which prompts the question: does a vulnerability's disruptive potential increase with its age? We may learn the answer to this in 2020...

Possible scenarios for 2020:

In that same way that certain viruses can lie dormant in the human body for many years, some attacks have been 'sleeping' for long periods of time following their installation on sensitive information systems. This makes it easy to conceive of a scenario **in which key sectors (health, food&beverage, energy industries) could be infected by malware that has lain dormant for years**.

And it is relatively easy to imagine a catastrophe scenario here. How would a major international firm cope if, in the middle of the night, all of its production plants around the world were to stop working simultaneously? A disastrous image on the TV news, and guaranteed financial losses. The cause? A discreet, successful phishing campaign several years ago, leading to the infection of various company networks with dormant malware. The malware then spreads locally to workstations which are still running an old version of Windows, and is activated remotely. Since it has already propagated to all workstations, even the emergency measure of unplugging the cables is useless. Cue black screens everywhere.

Events of 2020

In mid-September, a council employee in France's Gironde department noticed that their computer was being operated remotely. The council's IT manager then discovered that a number of computers had been infected by malware since... 2017. Cyber-espionage? An attack on democracy? An isolated act? The jury's still out.

In October, Kaspersky teams discovered spyware on Asian diplomats' computers. The software was capable of reinstalling itself on a computer even after the hard drive had been wiped or replaced. An endless malware story.

Trend 4:

are hacktivists about to make a big comeback?

Weak signals from 2019:

Although attacks by hacktivists are said to have fallen by 95% since 2015, recent world news reveals a rise in emotive causes to be fought: criticism of the Australian Prime Minister's response to the country's bushfires, revolts in Hong Kong against the Chinese government, French protests against plans by public bodies to use facial recognition systems, etc.

In December 2019, during demonstrations against pension reforms in France, the MEDEF employer federation's website suffered a DDoS attack which took it offline for a couple of hours. Shortly before that, in November 2019, the hacker Phineas Fisher launched his personal bug bounty against oil companies and capitalist institutions.

Possible scenarios for 2020:

Could 2020 mark **the return of large-scale hacktivist attacks, matching the growth in social movements**? It is probable that militants from a new genre (striker-hacktivists – 'Strhactivists?') could use their talents as a vehicle for a political message. If there is a trade union dispute, why bother getting involved face to face when you can strike the IT system instead? Rather than physically blocking entrances to bus depots, why not lock the gates remotely? And any automated metro lines still in operation can be brought down with a quick visit to the IT network. By applying the same mechanism to certain media publications or places symbolising power, it would also be possible to amplify protestors' voices, and the media impact of their actions.

On another level, other brand-new scenarios could emerge – for example, one linked to the vegan cause, in which a hacktivist succeeds in removing all meat from some ready-made meals. Alternatively, a group of hackers could take control of a major distribution platform to ship consumer goods to those in need, in a 'Robin Hood 2.0' spirit.

Events of 2020

In April, French hacker Baptiste Robert (alias Elliot Alderson) undertook an in-depth analysis of personal tracking applications. Having detected and exposed weaknesses in the Indian Aarogya Setu application, he set his sights on the French (StopCovid) and Pakistani (COVID-19 Gov PK) versions. On each occasion, he revealed serious technical issues relating to personal data protection.

In October, amid the debates over the US presidential elections, Donald Trump's website was hacked by someone declaring that the world has had enough of the fake news.

RANSOMWARE

What's new in the world of **ransomware in 2020?**

December 14, 2020

Since early 2020, ransomware attacks have increased in number and made front-page headlines. All professionals – large companies and small operations alike – seem vulnerable in the face of this evolving threat. And the number of cases of attacks – with varying degrees of success for the attackers – is becoming a concern. We take a dive into troubled waters to examine the No.1 cybercrime phenomenon of 2020.

"*Organised cybercrime is now using cyber tools to hold its victims to ransom,*" noted Guillaume Poupard, Director General of France's ANSSI cybersecurity agency, addressing French senators in November. And whether in France, Europe or worldwide, the effects of ransomware continue to reverberate. From the SAOG insurance company in the Sultanate of Oman to the Campari spirits group, and taking in Bouygues Construction and the Brazilian court of justice along the way, it seems that no-one is immune. Furthermore, the trend in ransomware is towards an increasingly professional approach, with a well-developed economic ecosystem between the creators and operators of malware, operating as a fully-fledged business featuring partnership levels and discounts, etc. 2020 has confirmed the rise of the ransomware threat, with increasingly well-prepared and organised attacks employing a more technical approach. This fundamental trend is prompting companies to rethink their defence measures and improve their ability to counter-attack.

By

Sébastien Viou

Encryption, propagation... how is ransomware evolving?

For as long as ransomware has existed, its end goal has remained unchanged: to exact a ransom payment. And the same is true on a technical level, where very little has changed. Indeed, the modus operandi of malware remains essentially the same: scan through a disk, search for files by extension type and encrypt whatever is likely to have the most impact on the target's business activity. The choice of data to be encrypted will depend on the cybercriminals' strategy: having access to the computer without access to the file is sometimes worse than having a computer that won't even start. For this reason, cybercriminals are careful to encrypt only certain extension types. On the other hand, it is clear that ransomware is changing in terms of how it propagates and infects systems.

The actual mechanics of extortion have also changed significantly since the early days. Ransom demands via PayPal are no longer the flavour of the month for attackers, as they are too easily traceable; most cybercriminals demand ransom payments in Bitcoin. It is a payment method that appears to be more stable for ransomware operators, and also makes it more complex to track the ransom through

mixing platforms (Smartmixer, BitcoinMix, etc.). In addition, in early 2020, the FBI stated that between 2013 and 2019, ransomware-related extortion operations amounted to a value of no less than 144.35 million dollars in Bitcoin.

In terms of propagation, "*ransomware operators are constantly monitoring news of the latest vulnerabilities in information systems to enable them to bypass protection mechanisms*" , explains Thomas Gendron, Malware Research Engineer at Vade Secure. Since mid-2019, several VPNs have been exposed to a number of key vulnerabilities which have attracted the attention of several groups of cybercriminals, who have seized the opportunity to launch waves of ransomware.

Although emails with infected files remain popular, **other forms of infection have been observed** in recent months. Leaks of passwords used on VPNs, VPN flaws, distribution by botnet, etc.; ransomware operators today seem to have a substantial arsenal of resources for propagating ransomware. Once an infection has succeeded, cybercriminals will attempt to extend the attack laterally and detonate the ransomware payload on as many computers and devices as possible. A recent example has been the Zerologon vulnerability, which has been heavily exploited by operators of the Ryuk ransomware. Operators can use this flaw to gain quick admin access to the Active Directory before extending the attack laterally across the IT infrastructure and obtaining access to privileged accounts. Infection, lateral movement, privilege escalation: all the cybercriminal then needs to do is to implement their "action on objective."

"Ransomware operators are constantly monitoring news of the latest vulnerabilities in information systems to enable them to bypass protection mechanisms"

Thomas Gendron
Malware Research Engineer
Vade Secure

Opportunistic vs. targeted attacks

Of course, the main ransomware trend to be borne in mind relates to the current extraordinary health crisis. Although phishing campaigns generally show little evidence of careful planning, experts have noted increased efforts by cybercriminals in the social engineering approach. Anxiety-provoking health and economic news has proved to be the perfect lever for playing on fears, such as false orders for masks, false redundancy notices, etc. "*Companies have invested heavily in protecting their perimeters with workstation protection solutions, IS security configurations, etc.*, explains Adrien Gendre, Chief Solution Architect at Vade Secure. *Ransomware operators are therefore looking for ways to circumvent this protection and gain internal access to companies. Phishing is a means by which mailboxes can be compromised, thus enabling ransomware and even spear phishing attacks to be launched from within the company*".

And there has been a proliferation in the methods used to force victims to pay ransoms, too. In October 2020, for example, a group of cybercriminals published a set of health data on the dark web that they had stolen from a Finnish company that controlled a chain of psychotherapy centres… in 2018! When the health company refused to pay the ransom, the cybercriminals first turned to patients' families before deciding to sell the precious data to the highest bidder… Another recent example was the attackers who used the Facebook social network to publish malicious fake advertising intended to force an Italian spirits group to pay a ransom.

However, these attacks seem to be mainly opportunistic in nature. And we should not allow them to

obscure the main trend in 2020: ransomware is becoming increasingly professional.

Increasingly professional ransomware

The trend towards *ransomware-as-a-service* (RaaS), following its first emergence in 2016, is gaining strength in 2020. "*You can now actually buy ransomware, and even tutorials teaching you how to use it*, says Edouard Simpère, Technical Leader Stormshield. *It's all sold as a service, in the same way that malware is sold in the form of ready-made tools that have long been available on the dark web*". Ransomware or extortion applications are sold on the dark or deep web, and are becoming products in their own right, with their own market rules (competition, etc.). For example, a number of cybercriminal operations have formed structures in which each majors in a particular task. But that's not all: "*As they have become more professional, attackers have each developed their own speciality: ransomware developer, phishing specialist, payload deployment operator, etc.*," Thomas Gendron explains. By forming a complex, more dynamic, more efficient ecosystem, these cybercriminals also protect themselves against disturbances to their important operations in the event that one link in the chain is arrested.

This increasingly professional approach by attackers goes hand in hand with the rise in targeted attacks against large companies and organisations. "*The current trend in ransomware attacks is towards an improvement in the infection methods employed. The use of tools to deliver the ransomware to the most appropriate place is more akin to the technical level one would associate with some APT or FIN groups, and shows a sharper operational intelligence than before,*" explains Grégory Baudeau, Technical Leader Cyber Threat Intelligence at Airbus CyberSecurity. Working alongside associate researcher Frédéric Boissel and analyst Quentin Michaud, Grégory Baudeau recently produced a model of an operation to deliver a Sodinokibi (also known as REvil or Sodin) payload that was discovered when responding to an incident. This RaaS – which has been available since April 2019 – has targeted a multitude of sectors such as energy, finance, construction, biomedical, aeronautics and even the telecommunications sector. One of the specific characteristics of this ransomware is also that it publishes exfiltrated data on dark web forums, and even holds auctions. This is what happened in the USA in June: the group behind Sodinokibi is said to have auctioned off 50Gb and 1.2Tb of data belonging to two US legal practices. In addition to data theft and extortion, therefore, new ways are emerging for cybercriminals to make financial profit from their attacks.

Lastly, in an age in which smart objects are part of our daily personal and business lives, questions must be raised over the attack surfaces of such devices. Whether the threats are proven cyberattacks against cash registers in supermarkets or printers, or even proof-of-concept attacks against smart coffee machines, the surface is expanding with the advent of devices offering low levels of security. "*This attack surface provides accessible gateways: attackers scout around, waiting for the right time, the right target, the right place to deploy their ransomware. It's just the thin end of the wedge,*" Edouard Simpère maintains.

The world of ransomware is becoming more professional and attacks are becoming ever more sophisticated and precise. And that makes them increasingly complex to detect for companies who, in turn, must be ruthlessly organised if they are to fight this cybercriminal trend.

What are the best anti-ransomware strategies?

Has it become acceptable to pay ransomware demands? The answer is no. However, the "*to pay or not to pay?*" question remains, especially for infrastructure such as hospitals. They are critical infrastructures which, when they fall victim to ransomware, become unable to carry out their vitally important

activities. Because from an operational point of view, attempting to circumvent ransomware is a complex process that takes time – a luxury such organisations cannot afford. In addition, from a moral point of view, it should be remembered that ransomware is blackmail. Paying the blackmailer will indicate a weakness that is hard (or even impossible) to defend in media terms, as well as ethically. Lastly, from a strategic point of view, there is no guarantee of a return to normal following a payment, whether in terms of actual data restoration or the continued existence of a back door left behind by the attacker. "*Paying ransomware means providing oxygen to the business behind it, and on principle, that is never acceptable. So what you need to do is to set up alternatives to avoid ever being in that position,*" Adrien Gendre warns. In the United States, for example, the US Treasury is seeking to prevent the payment of ransoms by companies by imposing civil penalties on third-party companies (such as cyber-insurance, cybersecurity companies, etc.) who assist victim organisations in paying their ransoms. The goal that organisations should strive for is never to be in a position that forces them to decide whether or not to pay a ransom.

At the same time, publishers and cyber players are also stepping up to counter the increase in attack surfaces and the propagation of ransomware by developing appropriate cyber solutions that provide support for such organisations. There seems therefore to be an increase in awareness, making it possible to implement the best protection against this type of malware.

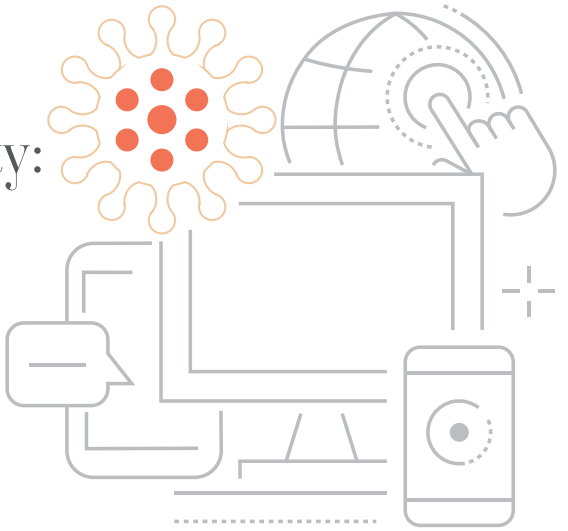
A number of mechanisms are possible to fight against attacks that deliver ransomware payloads, **including training employees in good digital hygiene**, implementing appropriate patch management policies, adopting a rigorous rights and authorisations management policy (compulsory password changes every 90 days for privileged accounts, use of two-factor authentication, etc.). "*One way you can protect yourself against ransomware right now is to implement protection and digital hygiene standards that are high enough to deter potential attackers,* Grégory Baudeau adds. *It is important to have employees who are sufficiently well trained in phishing techniques and monitoring security events on VPNs, ADs and equipment that has experienced critical vulnerabilities providing access to networks or central equipment of the company in the last six to nine months. It is also important to train security teams to detect suspicious behaviour. All companies and organisations need to have incident response teams, and the ability to shut down services and restore them again to provide a rapid response to an intrusion, avoid delivery of the payload wherever possible, and ensure that services can be restored as quickly as possible*".

In addition to these available means, there is a solution that provides an effective defence against such ransomware: the backup. Every organisation and company – even the smallest – needs to implement a backup policy, and all systems in all organisational structures must be equipped with solutions of this type. The backup is the cornerstone of an effective anti-ransomware policy, and this includes the implementation of offline backup systems that cannot be encrypted, and also a system of regular backup control procedures. In April 2019, agri-food business Fleury Michon fell victim to a ransomware attack, halting production for three days. However, the company was able to restart its operations fairly quickly thanks to its backup systems, which enabled it to recover the data it needed to recommence production and thus avoid paying the ransom demand.

The outlook for ransomware may still be bright for now, but companies are far from beaten, and should be able to keep strengthening their defensive postures and rejecting ransom demands as often as possible. If this is in fact the case, will cybercriminals perhaps be seeking, in the next few years, to switch to new and more lucrative activities? •

THE IMPACT OF **THE HEALTH CRISIS**

Covid-19 and cybersecurity: anticipating tomorrow's threats



July 1st, 2020

At the peak of the pandemic, companies were obliged to focus their efforts on ensuring business continuity even if this meant taking a few liberties with cybersecurity. So, how do you remain agile in a storm without jeopardising digital security? How do you avoid the risks of malicious cyber activity for organisations? And above all, how do you predict what comes next? Here we provide some clues to the puzzle.

By

Julien Paffumi

The pandemic's repercussions in cyberspace

The pandemic saw millions of staff working from home, with an explosion in requests for remote access and access via VPN. "*With the crisis, everyone found themselves working from home virtually overnight with infrastructure which was simply not up to the task in terms of performance,*" explains Stormshield's Customer Service Director Alain Dupont. For his part, Stormshield's Technical Support Manager Farid Ichalalène estimated that "*We experienced activity levels 30% higher over the last 15 days of March, particularly concerning requests from network and systems administrators who had to set up remote access connections virtually overnight*".

But faced with the urgency of the situation, IT managers have also had to accept compromises where security is concerned, even if this meant downgrading it. They have had to grant more access and set up remote desktops, without being able to apply all of the usual IT security procedures and with no preliminary risk analysis being performed. This reduced vigilance and digital uncertainty can only be beneficial to cyber criminals hoping to penetrate networks and steal sensitive data.

Among the organisations most concerned are those which had never or rarely used remote working and who therefore were not fully familiar with the organisational procedures needed to protect IT systems in such a situation. Governments, ministries, town halls, local authorities and other sensitive public operators saw their IT systems sorely tested during this pandemic. And their digital fragility laid bare for the whole world to see. There are numerous international examples, and here we will simply mention one from Germany, where the federal state of North Rhine Westphalia suffered a phishing attack with losses running into the tens of millions of euros, and one from the United States, where hackers actively targeted organisations involved in research to com-

bat Covid-19. In France, it appears to be small and medium-size businesses which have been most affected. Everywhere we look, the Covid-19 epidemic has revealed the weaknesses of the IT and operational networks of companies and local authorities, of their dedicated applications and of the devices used by their employees.

"*Currently, thanks to the procedures forming part of the Business Recovery plan / Business Continuity Plan, we are able to maintain the availability of the IT systems in the event of natural disasters or of a fire in a datacentre for example. And we actually had an anti-pandemic plan which had sat in the draw for several years, but nothing could have prepared us for this,*" explained the CISO of a major industrial group.

The urgent need for good diagnostics

Although we seem to slowly be getting back to a situation resembling normality, **this would appear to be the right time to carry out a thorough 'digital autopsy'**. During the pandemic, we advised everyone to carefully trace all special accesses which had been established in order to review them. It's now time to take stock. After the acceptance phase, it would appear logical to move on to the inspection and verification phase. CISOs should now perform a forensic examination in several stages, with the detection and removal of pockets of infection and the implementation of remedial measures. In the case of structural defects with the architecture, a redesign of the IT infrastructure will be required (in addition to the OT infrastructure, its counterpart in the operational world). We're talking about another scale of investment here. The ultimate goal is to durably regain control of the data and access systems. Because although computer hackers have taken advantage of the general haste arising from the coronavirus crisis, they do not appear to have created new forms of cyber threats. They have simply adapted their attacks to the prevailing conditions.

In Farid Ichalalène's view, there are a number of common-sense responses, such as for example "*only allowing necessary access according to the departments concerned*". For example, the R&D and accounts departments don't have the same requirements. Getting back to basics with perhaps more simplicity. Should we restrict what users can do, for their own good? The question is open for discussion… "*I feel that it's essential to simplify infrastructure, which has become too complex due to the sheer quantity of technologies and solutions proposed. We're also increasingly seeing that not all infrastructure has the necessary human expertise required for its satisfactory operation. The use of excess security layers is a problem in this respect: we need to get back to a simpler situation to be able to manage things more effectively. Even if this only means setting up a security control station to detect incidents as quickly as possible and to prevent cyber criminals from gaining long-term access,*" adds the industrial CISO.

Adopting good digital health measures

The widespread use of teleworking has made the IT manager's mission more complex: this new situation must take account of the companies' security policies and IT departments must continue their systems adaptation strategies in line with this. Firstly, the Covid-19 pandemic should not be seen as a "one-off" event: the IT structures must be ready if a new critical period comes around, backed by the right responses and dedicated tools when the time comes. It's now important to be able to quickly respond to remote access requests under satisfactorily reliable and secure conditions. This period of mass teleworking looks set to continue until the end of the year and become commonplace in future. It brings with it a requirement to support staff with the new requirements and practices associated with working off-site – with videoconferencing systems and the issue of their security being just one example among others.

CISOs must expect new challenges every day and prepare for the future. According to the CISO of the major industrial group, the most complex part

lies in the fact that: "*Sometimes with no other choice, CISOs find themselves in the position of having to approve infringements of the security or IT systems policies that they themselves have put in place over the years to guarantee minimum security. When employees are able to return to their place of work, it will be necessary to reduce their scope for action and restrict open access to the exterior through necessity. Going back to the way things were will probably be complicated as many people will now consider these special measures as being the rule. With so much lost ground to be caught up, each new access authorisation request must be based on preliminary studies. Question: with what budget? Although some suppliers have offered their services free of charge during the crisis, let's not forget that during all this urgency and haste, a number of VPN accesses have been purchased without having had the time to negotiate the prices with the different suppliers*".

All added complications, further adding to the ever-present stress under which CISOs have laboured for several years now.

Reviewing your IT budget to stay in good health

For several years now, managers have become increasingly aware of cyber risks, often highlighted during digital transformation projects. And even more so with the health crisis. But at the moment, the economic impact of the pandemic where the IT and cyber security fields are concerned is limited to simple hypotheses.

Astonishingly, 40% of IT decision-makers in Germany, the United States, France and Great Britain state that they would like to reduce their cybersecurity budget to limit the financial impact of the Covid-19 crisis. The CESIN's members, all of whom are drawn from major French companies and public authorities, have put forward similar figures with almost a third of respondents mentioning a reduction in the cyber budget. But another study is more optimistic: almost 48% of respondents stated that **the cybersecurity budget should not affected by the crisis**. And according to the same study, almost 20% envisage increasing their cybersecurity budget.

"It's one thing to work from home but it's another thing to guarantee the same security levels as when you're in the company"

Alain Dupont
Stormshield Customer Service Director

"*The risk of a new lockdown is real and with it the need to work from home. Decision-makers are now taking account of this in their IT projects and IT security projects,*" explains Farid Ichalalène. "*Although certain investments may be reviewed to save money, for their part the cyber budgets will be maintained for the simple reason that it's one thing to work from home but it's another thing to guarantee the same security levels as when you're in the company,*" adds Alain Dupont. Part of any revised budget must go to providing better training and awareness building for employees. Franck Nielacny, Stormshield's IT Director, explains that: "*Naturally, our staff are very familiar with digital resources, which helps things. This is why we must also place our trust in the teams. They are able to adapt and display good resilience*".

And very often, it's during such difficult times that people reveal the best of themselves: Franck Nielacny mentions the excellent solidarity present in his own team, with the goal of "*working together as a team and displaying a high degree of responsiveness and a sense of service in dealings with our internal clients*". Whatever people may say, company life goes on… •

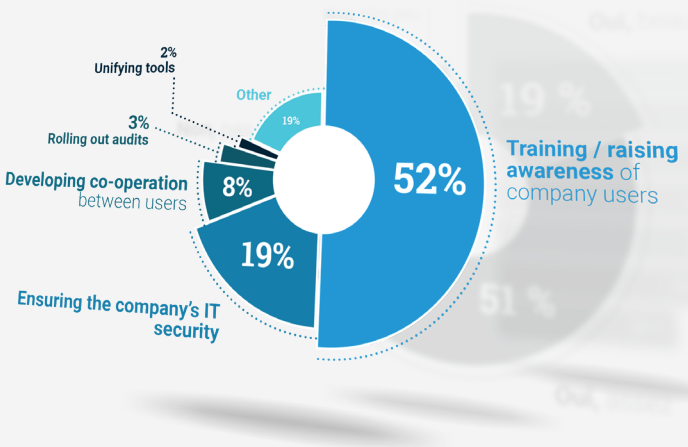
The digital transformation barometer:

putting maturity to the test?

White paper

Just like every year for the past three years, we have been interviewing companies and organisations – large, small and medium – to find out more about their digital projects and security. Just like every year? Not really, as you can imagine. 2020 is already – and will remain – a remarkable year on all fronts.

That's why, in this third edition of our Digital Transformation Barometer, we are conducting a more in-depth analysis of the short and medium-term effects of current events.



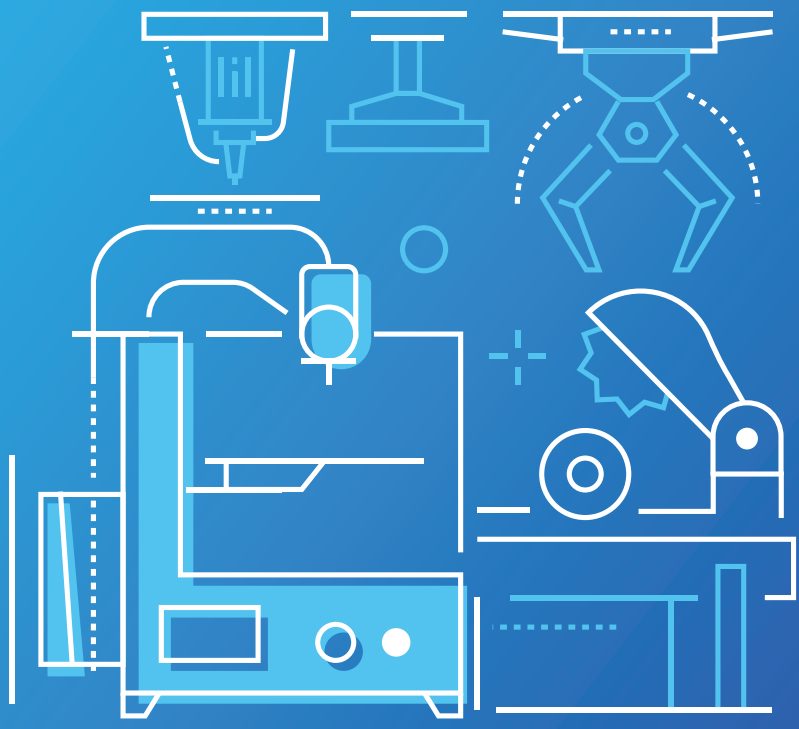
A word on 2020 barometer

The 2020 edition of our Barometer survey marks a clear break with previous editions. The widespread use of teleworking and the enforced switch to working electronically have acted as a catalyst, and in some cases a trigger, in terms of the transformation of certain organisations. For more mature organisations, 2020 will have provided a real-life test of their ability to maintain and develop their operations in a predominantly online environment. And as always, cybercriminals have taken advantage of these extraordinary circumstances, exploiting certain people's anxieties or applying pressure in areas where harm could be done; hospitals, which are already under great strain, have been particularly hard hit by this phenomenon.

Against this background, sharp changes in the trends observed in the first two editions of the survey were to be expected. But have things really turned out this way? The answer is not so simple. Based on feedback from more than 200 decision-makers, the 2020 survey presents a highly diverse and nuanced picture. The survey revealed many advances in terms of digital transformation and cybersecurity, and it would be extremely reductive to claim that these developments stemmed solely from the public health crisis that we have been living through for the past several months. New challenges for cybersecurity have also emerged, requiring companies to adjust some of their approaches or to invest in new, enhanced systems for protecting their intangible assets and maintaining business continuity.

We hope that you will enjoy reading this latest digital transformation Barometer survey as much as we have enjoyed creating it.

Matthieu Bonenfant
Chief Marketing Officer Stormshield



INDUSTRIAL CYBERSECURITY

What sort of cybersecurity is required for industrial systems in the industry 4.0 era?

December 21, 2020

The industry 4.0 is flourishing, bringing its fair share of threats... But also misconceptions. How can we guarantee overall security in an area which increasingly combines industrial systems, the Internet of Things, the Cloud and Big Data? Spoiler: it's not all about sensors.

By

You've probably heard the story of the web-connected coffee machine which resulted in ransomware being introduced in an industrial petrochemicals business. This story illustrates the challenge of protecting an increasingly connected industry 4.0 – namely that of securing an ever-increasing attack surface. It's a bit like trying to track down draughts in a building in which ever more doors and windows are constantly being opened. The gradual introduction of smart sensors and/or Cloud links has created new connections with the outside world. These are all potential breaches in an industrial sector which is already significantly targeted by cyberattacks and which is certainly not safe from internal errors.

A multi-layered technological environment

In practice, industrial systems are comprised of physical items of equipment within the factory (motors, pumps, valves and sensors), managed by control systems, whether remotely or otherwise, (PLCs and SCADA applications) and IT systems (for data analysis). "*What we today refer to as 4.0 is a concept based on the digitalisation of industry with the aim of achieving continuous improvement*, stresses Thierry Hernandez, Stormshield Account Manager and industry specialist. *This concept is based on several factors including changes in tools and resources (robotics, AGVs,*

augmented reality software, etc.) and technologies (telecommunications protocols, sensors and connected items to supply data). All of this is interconnected throughout the factory. The end purpose is to feed data to a cloud or edge computing system hosting solutions offering extensive calculation capacities based on state-of-the-art algorithms. Its main role is to offer operational excellence through energy efficiency, time reductions, reduced material consumption or predictive maintenance".

Production is now optimised, flexible and more fluid as a result. Thanks to predictive maintenance, it can even anticipate breakdowns, therefore maintaining throughput.

"*Put simply, production is organised into four layers*, explains Thierry Hernandez. *The first layer is comprised of the PLCs, which run all of the actuators and all of the valves. The second is the SCADA (the supervision and acquisition software based on the data supplied, to ensure that everything is going well and that the tanks are being filled properly for example). The third layer is management with the MES, which handles all of the production tracking and planning processes. Finally, the fourth layer is the ERP system, which among other things issues production orders*". These software packages make it possible to manage all of the company's processes, making them an essential factor which should not be overlooked as part of the overall cyber-protection strategy.

If we add the cloud and 5G into this, it's clear that a 4.0 factory is a multi-layered technological environment with a complex architecture, operating in accordance with its own rules and codes.

Designing industrial cybersecurity

Although it's in the process of taking shape, cybersecurity for industrial systems must contend with a certain degree of inherited 'baggage'. And this can be precisely the problem. "*In France, an industrial system has a life expectancy of around 15 years on average. This is the average age of the production machinery. For trains and metro systems, these life expectancies stretch out to 30 or 40 years. And if we examine even more critical systems such as the nuclear sector, the power stations have a life expectancy of 60 years. Naturally, these systems, which are sometimes very old, are vulnerable,*" adds Jean-Christophe Mathieu, Head of Cybersecurity Orange Cyberdefense.

"*Historically, this infrastructure has often been introduced haphazardly. In other words it's been designed and automated on an ongoing basis according to requirements, with people wiring things up however they wanted (or however they could!)*, explains Stéphane Prévost, Product Marketing Manager Stormshield. *As a result, all of these automated systems have been installed on a 'flat' network. To secure them today, it's necessary to compartmentalise them*". The segmentation of the IT system has therefore emerged as one means of isolating the most sensitive assets from the others and protecting them. The result is that cyber threats are contained and performance is optimised for the different items of equipment. At a time when increasing numbers of sensors, machines and production flows are being interconnected in factories, segmentation offers an essential bulwark for industry 4.0.

An 'OT first' approach

These '4.0' problems are no longer only managed by the factory's operational staff. What's now required is a skilful combination of disciplines to ensure successful IT/OT convergence. And these two worlds must come to understand one another. "*We are still finding that in far too many companies the IT and OT teams are still not communicating effectively with one another. Significant cultural differences persist and petty squabbles still occur. However, it's impossible to achieve an overall approach to security if people are not talking to one another and not working together,*" Jean-Christophe Mathieu points out.

For the IT activities, this means adapting their cyber approach to encompass the challenges of OT. "*The*

OT people have one key obsession, and that's to keep everything running. It's therefore important to find the right balance between the protection system and the need to ensure production and business continuity," explains Thierry Hernandez. This means that a firewall is okay on condition that it doesn't obstruct anything down in the factory.

Another words, IT protection should not be achieved to the detriment of production. "*Security must be guaranteed in a manner which ensures the availability of the system and keeps it running,*" stresses Stéphane Prévost. This key requirement has led to a new approach including the emergence of industrial cybersecurity, which is well on the way to becoming a discipline in its own right. With increasingly specialised cyber service providers, including Stormshield, who can propose transparent solutions for the existing system. "*This transparency must be available during the integration phase but also later, should hardware faults occur, to avoid penalising production*, adds Stéphane Prévost. *Our industrial firewall solutions are all equipped with several guarantees to underpin operational security, with bypass or safe mode features, the notion of equipment clusters or redundant power supplies*".

Cloud and Edge computing, new factors to be considered

Data feedback is a key component of industry 4.0. "*It's important to ensure the perfect integrity of the information arriving from the PLCs and sensors, and for this data to be quickly forwarded to the ERP and the Cloud*, explains Thierry Hernandez. *Protecting the lower layer of the operational network is an initial key objective, which makes it possible to secure this information at source, before it is used further up the line*".

This is before we even begin to consider the applications and the information transiting via the IoT. "*Edge computing, including everything related to the calculation of energy consumption, is fed back at a point located as close as possible to the operational network, which is directly connected to the Cloud infrastructure*, adds Stéphane Prévost. *This adds further interconnectivity, making the operational system more vulnerable to cyber threats*".

Industry 4.0 must therefore have a comprehensive overview of its security. With the identification and mapping of sensitive assets, segmentation (or even micro-segmentation for the IIoT) to isolate each part from the others and to avoid an attack spreading, in addition to securing PLCs and control stations, industrial cybersecurity now seems to be maturing. But in Jean-Christophe Mathieu's view, this presupposes that everything works in a highly organisational manner. "*We need to know who's doing what, when and how, accompanied by extensive traceability. To prevent anyone accessing the system. Or, when someone accesses it, to be able to know exactly who this is and what they're doing there.*"

And the security solutions deployed in the factories must be able to track this. "*At Stormshield, we go as far as inspecting the messages issued by the command and control system to the machines*, explains Stéphane Prévost. *When an engineering workstation submits a change of settings to a PLC, it must be possible to check that it's the right workstation with the right person logged in, and that the command being sent is authorised*". This message control function also makes it possible to check that the values being sent to the PLCs are fully compliant with the operational process. "*We can tell whether a value exceeds a certain level, in a manner likely to compromise or break an item of equipment or even pose a threat to the whole production system.*"

Industry: a prime target for hackers

As is often the case in the cybersecurity field, standards provide an important guide for the deployment of 'safety nets'. In the case of industrial systems, the IEC 62443 standard is the reference in this field. Each sector then proceeds according to its own specific characteristics, particularly in industries clas-

sified as OSE (operator of essential services), which require very high security levels. The Clusif, a French association for IT systems users, has produced an overview of the standards in the field of cybersecurity for industrial systems. And at around fifty, there are many of them!

Despite these standards, industrial systems nevertheless remain vulnerable. Particularly because physical equipment (PLCs, controllers, regulators, etc.) whether connected or not, are used for vastly different purposes and occupy a central role in many systems. As an example, we find the same types of PLCs being used to handle the management of a building (heating, ventilation, air conditioning) or on a production line for making cars, for example. Once a vulnerability is discovered on one of these widely used items of equipment, all of these systems must then be considered at risk. "*We find a great deal of analogy between the different industries*, notes Thierry Hernandez. *A cosmetics company can be compared to one in the pharmaceutical sector as the infrastructure and architecture used can be similar. But the level of security will be dependent on governance*". And therefore to **a certain extent on awareness of cyber threats**.

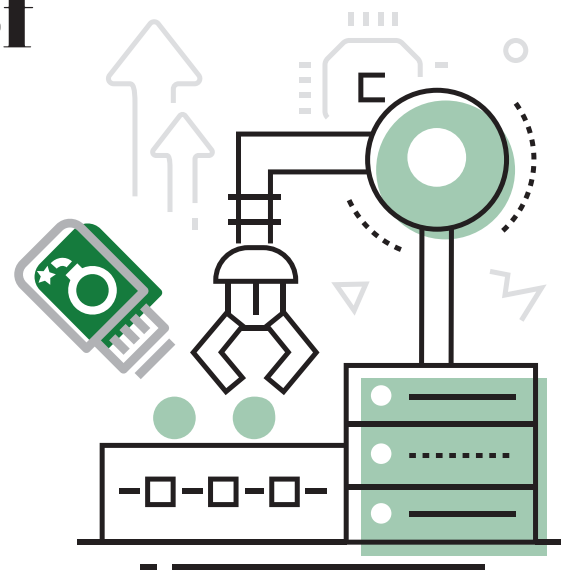
And these threats are very real. Over and above data theft and industrial espionage, the hackers' targets now include PLCs and security controllers, threatening the production system with a major ransomware event. This also risks bringing about disasters such as operating incidents or the stoppage of production, all seen as harmful risks. "*Whatever the consequences of a malicious act or internal error, the greatest threat comes from a stoppage of production. There's a huge economic cost,*" adds Thierry Hernandez. The shipping company AP Moller-Maersk put a value of 300 million dollars on the cyber-attacks it suffered in 2017.

Attacks can target supply chains, which are becoming increasingly complex, extensive and interconnected. For example, a sensor which has been 'reconfigured' by a cyber-criminal may allow a valve to open more than it's supposed to. In the case of a water tower, this could result in the whole area being flooded. Or cause a serious operating incident. In November 2020, Israeli researchers even suggested a scenario in which it would be possible to create a biological virus from a computer virus. Scary stuff.

As we have seen, IIoT solutions and industrial systems are insufficiently prepared for operation in a connected environment, more exposed to cyber-attacks. The information which these connected items collect and pass on should not directly interact with the core system. "*However, if it does, it must be sufficiently filtered in a unidirectional manner to ensure that it only heads towards the exterior, towards these famous connected items, and not to the heart of the system*, warns Jean-Christophe Mathieu. *It's important to ensure that the system core is insulated from the rest*". And to manage the architecture effectively from end to end. •

The paradox of USB drives in the industrial world

December 17, 2020



USB drives are a paradox for industry. They play leading role in how operational environments function, but can also cause incidents if they are managed or handled improperly. They are also one of the most coveted means of attack by cyber criminals. Here is a situational review of the ambivalent role of USB drives in the industrial world. Between operational effectiveness & necessity and intentional or accidental danger.

By

Even if they are relatively isolated, the industrial world and its operational networks with its factories, production sites, and automation must come to terms with the threat posed by USB drives. While we might be tempted to see it as a malicious threat only, it may also simply be a matter of chance. In fact, some industrial CISOs are more worried about the accidental introduction of malware that could jeopardise the production line via, for example, an employee's USB drive that they had previously used in their personal life. It is hard to judge a person harshly who simply copied a seemingly harmless file onto their USB drive. And yet, it can happen.

So should industry therefore move away from USB drives? Is that conceivable for all branches of the sector? Can USB drives be replaced by alternative solutions that are appropriate for the operational infrastructure? How can we ensure a site's IT security without slowing down or stopping production? There are so many questions and the issues inherent to industry are very real. Insights.

USB drives a necessity in OT

For all of those years when OT machines and workstations were not connected to the internet, USB drives were the preferred – sometimes the only – means of exchanging data. Furthermore, for a long time, people in industry have believed that the internet posed the biggest risk of cyberattacks rather than physical devices. USB drives therefore have historic

value in OT, which tends to evolve and transform at a slower rate than IT. "*OT has a lower-level focus and is applied in a context where the systems cannot be stopped or slowed down. In industry, therefore, the paradigm is the opposite of that used in other sectors: continuity and fluidity are prioritised over security. We prefer to take the risk of using USB drives rather than take the risk of blocking production*," explains Thierry Hernandez, Global Account Manager Stormshield.

The inherent operating methods of the industrial world include that the people in charge of maintenance at industrial sites (for automated systems, sensors, and more) are external contractors who are not always able to connect to the network. USB devices, including drives, are vital for these integrators who use them for all sorts of operations such as installing updates and recovering saved copies or backups. However, there is nothing to guarantee to an industrial site that this type of action by third party companies is conducted with the same rigorous security standards as those followed by the company itself, which can lead to risks.

But choosing to forgo USB drives and this operating method in OT can prove to be particularly complex depending on the specific industrial sector in question. In so-called 'heavy' industry (such as the agri-food, steel, water, and chemical industries, among others), machines and workstations are not very connected and USB drives are essential for intervening on each workstation directly. But the practical nature of these USB devices is counterbalanced by the fact that they are a formidable vector of contamination.

USB drives as vectors of malware

A USB drive makes it possible to exchange any data and brings unknown elements into a network. This includes sensitive elements within an industrial site. Additionally, a USB drive does not go through all of the perimeter defences of a structure, arriving instead directly at a user workstation. "*A USB drive can have anything on it and the negligence of users who do not have the instincts to check its contents before inserting it into a machine is commonplace and dangerous*," states Thierry Hernandez.

"In industry, we prefer to take the risk of using USB drives rather than take the risk of blocking production"

Thierry Hernandez
Global Account Manager
Stormshield

With the advent of Industry 4.0, factories are increasingly connected and therefore increasingly vulnerable to malware. For attackers, USB drives are a point of entry to gain access to a system and infect all or part of a network. There are many cyber risks, from production line blockage to the installation of malicious programs, remote espionage, or even data locking.

When it comes to malicious actions, critical industrial infrastructure are the targets of attacks and according to SANS, 56% of security incidents targeting them involve USB drives. Cyber criminals are increasingly inventive and creative and have used many forms of USB-based cyber attacks in the IT world. In 2005, the AutoRun feature, which Microsoft intended to automatically launch programs when a USB device was connected to a workstation, created the perfect opportunity for attackers. Simply plugging a device into the workstation could trigger the automatic execution of malicious applications or codes on the drive. In the early 2010s, the rubber ducky USB drive-based attack became a common means for cyber criminals to pirate IT systems. The PHUKD attacks (Programmable HID USB Keystroke Dongle) used the same ideas, imitating the activity of a keyboard or mouse.

In 2014, the BadUSB hack appeared, exposing a flaw that some researchers considered critical for industrial control systems. Then 2017 was the year of the P4wnP1, a programme designed to conduct attacks using Raspberry Pi Zero and Raspberry Pi W. Several years later, it was Bash Bunny that made a splash. Then, much more recently, the USB Killer attack has been able to crash a machine in seconds just by plugging in the malicious drive to the targeted workstation.

Applied in the world of industry, these infection methods have led to many cases of cyberattacks. In 2017, critical infrastructure in the Middle East was targeted by Copperfield malware distributed by a USB drive at a workstation shared by several dozens of employees at the structure in question. Copperfield is a remote access Trojan (RAT) that specifically targets critical industries. As soon as the infected USB drive is connected to the workstation, the malware spreads, using the Windows Script Host to take control of the machine. That same year, in their report entitled *The Guidelines on Cyber Security Onboard Ships*, several actors in the maritime sector raised alarms about the risks related to USB drives for their industry. The report analyses many cyberattacks including two that were possible due to the use of USB drives. The first attack involved negligence or a lack of knowledge on the part of the crew. A member of the security team on a merchant marine vessel accidentally connected an infected USB drive to the ship's IT system. The USB drive then spread the malware throughout the systems and the crew did not find out until several days later due to abnormal behaviours in those systems. Another example involves the core of a ship's energy management system. IT service providers in charge of the ship's systems detected dormant malware there. It was inactive because the device in question was not yet connected to the internet, but it would spread within the systems once connected to the network. Finally, much more recently, the automotive industry narrowly avoided what could have been a large-scale attack. In August, a Tesla employee was approached by a Russian cyber criminal who offered the modest sum of one million dollars to spread malware within the company's IT systems using an infected USB drive. If the employee had not informed the FBI and foiled the attack, Tesla could have joined the long list of victims of USB drive attacks.

The world of industry finds itself caught between a rock and a hard place, needing to ensure sustained and fluid operational activity while also taking into account the risks of using USB drives within the company.

Securing or eliminating USB drives

To protect themselves and limit risks, some structures are relying on software solutions to control USB drives. The goal is to be able to continue using these external devices while strengthening control over the data being exchanged. "*It is possible to use cyber security kiosk procedures to ensure secure use of USB drives within the company*, explains Adrien Brochot, Stormshield Product Manager. *It comes down to scanning the drive to ensure that there is no malware, but also to calculate the footprint of its content to know its current state and check it when it is connected to any workstation that needs protection. If the footprint has been changed, then the person needs to verify if those changes are authorised on an internal workstation that is also protected. If not, access is denied*". Controlling and inspecting USB drives means excluding certain ones. In privileged settings, only authorised USB drives will be allowed for use. To secure the USB drives, endpoint security solutions may also be used. In any event, ensuring the reliability of a USB drive is particularly important for critical industrial workstations, especially those that perform supervision operations.

Some companies opt more for security policies with very restricted lists of authorised USB devices. In 2019, the France's ANSSI cybersecurity agency tack-

led the difficult subject of USB drives head on, presenting its open source project Wookey, intended to strengthen the security of workstations and specifically combat BadUSB-type attacks. Finally, structures simply banned the use of USB drives to reduce the risk of attacks, following in the footsteps of IBM and the American army.

Industry 4.0: A potential alternative to USB drives

Additionally, a new trend is emerging in OT to potentially replace USB drives by using servers like in IT, true spaces for file sharing or application flows.

The USB drive is, in some structures, much less used than previously and files are increasingly shared via the network. Network connections and telemaintenance could therefore be an interesting alternative to these devices. "*Replacing USB drives with digital systems could save significant time and provide real user comfort. The people in charge of backups at industrial sites could, for example, save 3 to 4 days of work per month with a digital system*, explains Fabrice Tea, the Schneider Electric Technical Director of Digital Transformation, adding: *We must have an alternative to USB drives before considering replacing them and increasing the connectivity capacity of a network can be a good option*".

One point to note, however, is that the 4.0 approach is not generalised in Industry. Many facilities do not currently have it in place and interconnecting critical workstations can prove to be a sensitive cybersecurity issue for operational systems. By connecting workstations to one another and especially to the outside world, you create more potential areas of industrial infrastructure to attack. This is particularly true for small facilities that do not have the resources of large industrial actors. Publishers therefore have a key role to play in assisting organisations as they adapt to the culture of Industry 4.0 cyber. •

"We must have an alternative to USB drives before considering replacing them and increasing the connectivity capacity of a network can be a good option"

Fabrice Tea
Schneider Electric Technical Director of Digital Transformation

The importance of **OT and IOT cybersecurity**

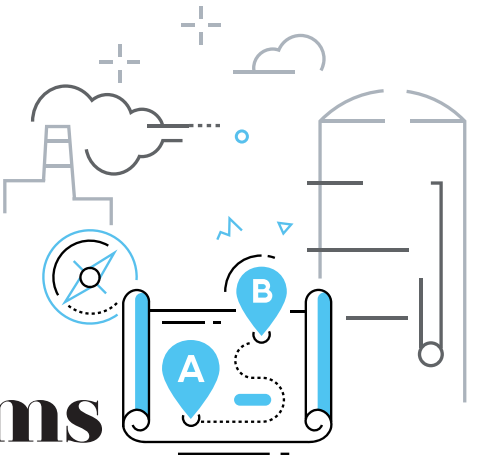
In 2020, we have seen the importance of managing OT/IOT cybersecurity too. Malicious acts, espionage and the disruption of vital activities are no longer in the theoretical realm; they are actual events that are being witnessed practically every day in France, Europe and worldwide.

There must be a strong, co-ordinated response to such cyber threats from governments, of course, but also from the companies that are stakeholders in this new ecosystem. However, we must not overlook the fact that this environment and its operational networks can be endangered as much by malicious acts as it can by internal errors. To help professionals become more mature in cybersecurity matters, Stormshield is therefore increasing the volume of content it produces for this new ecosystem and its players.

Eric Hohbauer
Sales Director and Deputy Managing Director of Stormshield

OT and cybersecurity

a journey to the heart of operational information systems



September 17, 2020

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.

"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 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*

By

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.

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

Vincent Nicaise
Industrial Partnership and Ecosystem Manager Stormshield

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 cybersecurity 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 sys-

tems 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 controller) is required, as well as a business resumption plan.

"*All these layers of security are elements of an in-depth defence system*," says Vincent Nicaise. This approach is encouraged by the France's ANSSI cybersecurity agency, 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*".

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 cybersecurity to integrate harmoniously into industrial systems, there must be joint work between IT and OT teams*".

"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

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?** •

Why should we stop talking about SCADA?

February 20, 2020

Nowadays, industrial systems are increasingly digitally controlled, raising their exposure to cyberattacks. In the face of this mounting risk, a knowledge of the basics of industrial cybersecurity – and the associated technical terms – is now an essential requirement for effectively dealing with threats.

SCADA, ICS, DCS, HMI, PLC... Behind the innocuous initials 'OT' (Operational Technology – as opposed to IT, Information Technology) – lies a maze of industrial jargon with a host of meanings whose interpretation varies from sector to sector, and company to company. "*Even the term 'OT' itself has a complex, diverse set of meanings*, says Vincent Riondet, Head of Cybersecurity Projects and Services teams Schneider Electric France, *having been orphaned from the traditional information system*". These industry-specific terms, often poorly translated or understood in different ways, can be a source of confusion, not least among information security teams. If we are to protect industrial equipment and implement appropriate defences, we need to have a precise understanding of how it operates and the terms that describe it... and all the more so when a response to a cyberattack is required.

By

What is SCADA?

The term SCADA (Supervisory Control And Data Acquisition) is a veritable crossroads of industrial jargon. However, **its definition is subject to a range of interpretations which can vary not only by geographical area, but also by business area**. SCADA can mean software installed on a PC to collect data, or refer to a general monitoring system. And this initial approximation is a problematic one.

"*This SCADA terminology is what creates most confusion for IT actors*, explains Vincent Riondet. *A CISO will tend to use SCADA as a blanket term for all forms of operational technology*". *"But for an automation engineer, SCADA refers to a system which is able to acquire and process a large volume of data. It is a monitoring application. For those not involved in the automation sector, the word can be twisted to mean any industrial control system,*" adds Fabien Miquet, Product & Solution Security Officer Siemens. Similarly, an integrator will invoke SCADA to described all installed parts of an industrial system, up to and including the controllers.

In reality, SCADA is generally taken in Europe to refer to a remote management and telemetry system with a real-time communication mechanism, used to monitor installations. But on the other side of the pond, it's a different story.

ICS, DCS, HMI, PLC: cutting through the industrial jargon

Particularly in the United States, the term SCADA is given a wider definition than its European cousin, referring to a general monitoring system consisting of ICS, DCS, HMIs and other PLCs.

The ICS (Industrial Control System) is an acronym that encompasses the industrial system as a whole. Its purpose is to control everything, including – according to the European conception – the SCADA, with which it is often confused. "*Through a corruption of language, the ICS is what 'non-automation specialists' refer to as a SCADA,*" explains Fabien Miquet. **As an overall system, it is often viewed as the 'Achilles heel' of industrial cybersecurity** as its attack surface – that is, its exposure to cyber risk as a function of its size – is by nature larger.

As well as ICS and SCADA, the term 'DCS' (Distributed Control System) is also used... and confused with the two other terms. In connected form, this other system enables multiple robots to be networked (and possibly replaced) to make it possible to manage more complex processes, with distributed local tasks.

Human-Machine Interfaces (HMIs), for their part, are interfaces enabling the user to connect to a system or robot. This is the communication channel between the SCADA (which collects the data) and the human (who needs to have access to the data). In France, this term is often confused with SCADA. "*Sadly, they've missed out the rest of the translation,* sighs Vincent Riondet. *French automation specialists tend to use the term SCADA only to mean the upper layers of the control-command process (for data logging and monitoring), while other European automation specialists understand it also to refer to the controllers themselves*".

> **"A person with an IT background won't use the same definition of SCADA as someone from OT"**
>
> **Vincent Riondet**
> Head of Cybersecurity Projects and Services teams Schneider Electric France

Lastly, another commonly-used term, the PLC (Programmable Logic Controller), is a device for controlling independent robots. Are you following all this?

"*Each of these domains... IT, OT, automation... have their own jargon. If you use the term SCADA to refer to the whole setup, your staff will get pretty confused. And failing to agree on technical terms creates potential vulnerabilities in the event of an attack,*" Fabien Miquet explains with hindsight.

The importance of mastering industry jargon

And **this confusion between genres could be partly responsible for the industrial cyber risks of the future**. Using the wrong terms – or confusing terms that look similar but have different functions and purposes – makes cybersecurity in industrial systems an even taller order.

Without getting into a "spot the difference" game, it is possible to give a quick summary of the main differences between SCADA and DCS – a real minefield of industrial jargon.

- A DCS is process-oriented, whereas a SCADA system is more focused on data collection;
- A DCS is controlled by processes through the interconnection of sensors, controllers, terminals

and actuators, while a SCADA is controlled by events (chemical, physical or linear);
- A DCS is more integrated and can perform more complex tasks, but a SCADA is more flexible.

Knowing this means being better able to anticipate their respective vulnerabilities and cyber threats... and being able to tackle them upstream, thus offering more effective protection for your industrial system.

Providing industrial cybersecurity in today's world

From a manufacturing point of view, the main cyber risk relates to production units. A cyberattack can disrupt and damage or even halt them, with often heavy financial losses as a result and, in some cases, human and environmental impacts. This vulnerability stems mainly from the fact that **the OT world is not developing at the same speed as its IT counterpart**.

"*OT is developing more slowly than IT. Cybersecurity needs to adapt to industry, and not the other way around. It's a fairly rigid system. Sometimes you have to reverse engineer what you already have to find the best possible solutions,*" says Franck Bourguet, Stormshield's Vice-President of Engineering.

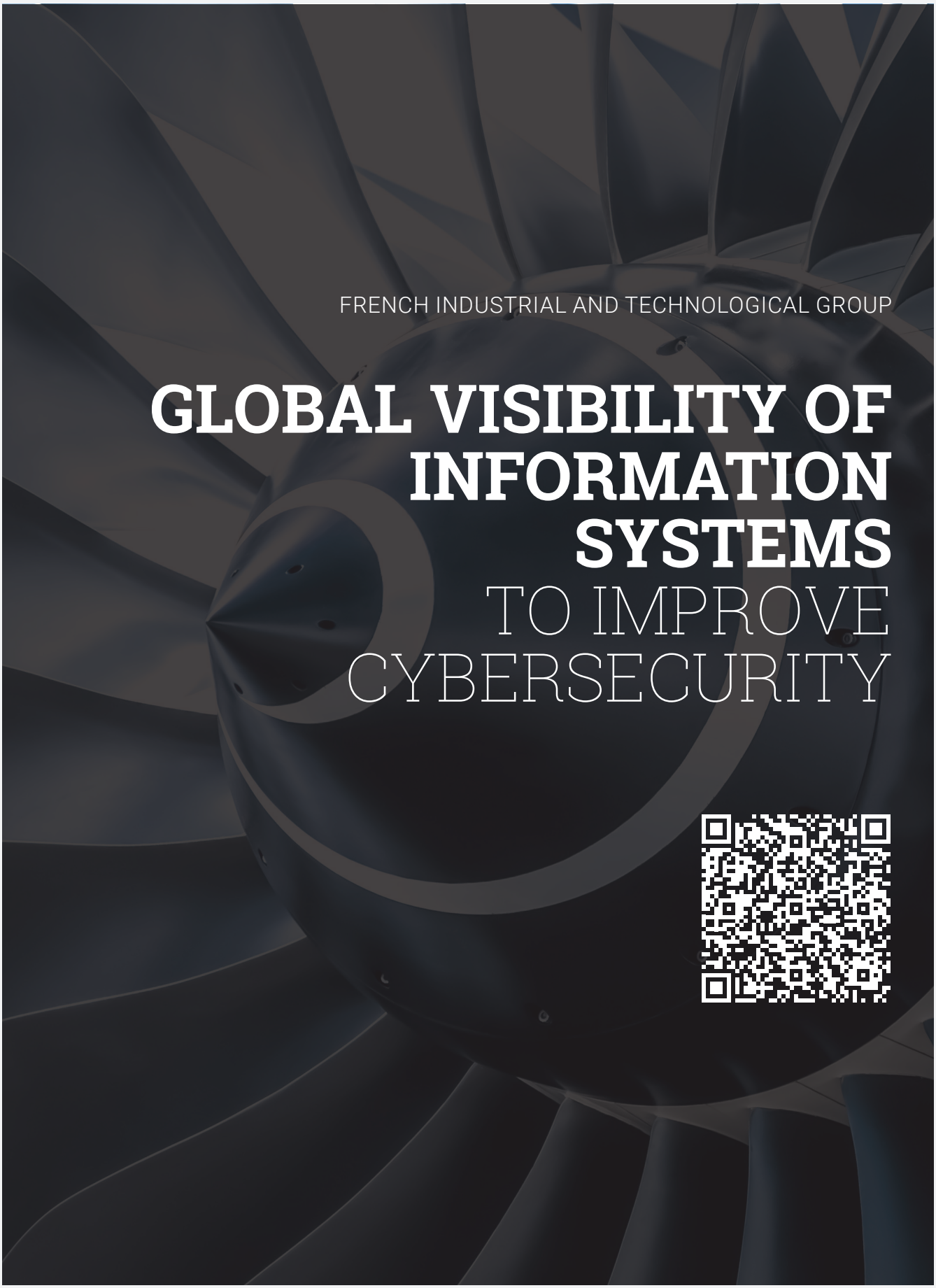
After all, production equipment is designed to last for several decades, and has to work constantly. This is not ideal when it comes to updates outside of maintenance phases, which are rigidly planned for minimal impact on production lines. In addition, the OT world has historically operated without the Internet, and therefore in isolation from threats coming directly from the Internet. But with the digital revolution and automation, factories are getting online and must now deal with cyber risks.

"*The increased connectivity of industrial systems, and their interfaces with IT networks, increase security risks as they present new attack surfaces,*" Franck Bourguet explains. Today, cybersecurity companies and publishers need to be able to respond to global issues that include IT and OT and take a customer's overall architecture into account, as part of the concept of protecting these attack surfaces at all times.

Using the right tools and adopting best practices

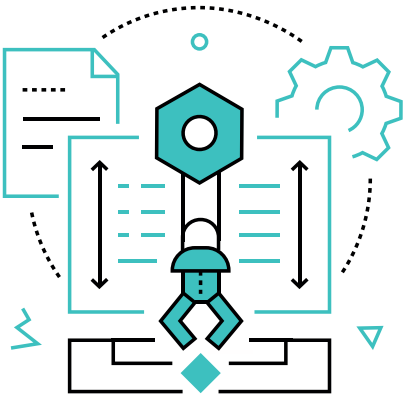
Creating a defence in depth featuring several barriers – cryptographic signatures, principle of least privilege, blocking of USB ports and other peripherals, network segmentation – is the beginning of a response. But let's not forget that human beings still remain the best defence to date. "*The rules of digital hygiene (password management, updates, backups, etc.) provide efficient protection and can eliminate 80% of cyber risk,*" concludes Fabien Miquet.

In the interests of improved protection, harmonising industrial jargon must be a priority, to ensure that staff can understand one another and make the right decisions. In today's corporate world, digital best practice is everyone's business. •



FRENCH INDUSTRIAL AND TECHNOLOGICAL GROUP

GLOBAL VISIBILITY OF INFORMATION SYSTEMS TO IMPROVE CYBERSECURITY



IEC 62443 the essential standard for industrial cybersecurity

July 29, 2020

For many years, cyber risks in the industrial world seemed to apply only to sensitive areas such as the energy or nuclear sectors. However, recent cyberattacks have shown the reverse to be true: regardless of the nature of the operational networks and their scope of application, they can find themselves exposed to criminal digital acts at any time… and all the more so as they increasingly overlap with the world of IT. The IEC 62443 standard forms an automatic part of this discussion regarding the issue of cybersecurity in industrial installations. We explain why.

By

A common foundation for industrial cybersecurity

In 2007, the first standards specific to industrial cybersecurity were created, at the initiative of the ISA's 99 committee. A few years later, the IEC 62443 international standard was born. It provides an in-depth cyberdefence benchmark for industrial systems of all kinds, whether employed by your local artisan chocolate producer, a water purification plant or a transport network. "*A cyberattack, even on a small bottling plant, can result in disruptions to production; and consequently, a financial impact which in turn could potentially have fatal consequences for the company,*" explains Khobeib Ben Boubaker, Head of Industrial Security Business Line Stormshield.

Up until that point, there had been two standards: one was for information security management systems (ISO 27000), and the other for industrial safety (operational reliability and functional safety with IEC 61508 and sector-related standards). The IEC 624443 standard now serves as a link between these two environments, which are indeed seeing increasing convergence. It forms a virtuous circle for managing cybersecurity risks in industrial installations as a whole. However, this area of overlap between OT and IT is still a complex one. "*The world of IT has a*

strong focus on confidentiality and integrity: in the case of suspected attacks; there is an immediate tendency to disconnect the system. A factory, by contrast, needs to maintain uninterrupted production, and has to deal with both human and environmental risks," points out Fabien Miquet, Product and Solution Security Officer Siemens.

However, the IEC 62443 standard is a set of recommendations; it is not binding upon either manufacturers or their critical infrastructure. This flexibility ensures that the standard can be adapted to the specific characteristics and contexts of critical installations. "***The IEC 62443 standard is a useful cybersecurity benchmark for industrial installations, because it provides a common foundation***. *It can be used partially, depending on requirements, or be supplemented by another business standard. For example, IEC 61850 refers to electrical installations, which will take different practical forms in the context of a sub-station, a Smart Building, or a hospital,*" Khobeib Ben Boubaker points out. This standard therefore seems to provide a necessary framework, especially as "*the industrial world is very heterogeneous in terms of the number of different trades it encompasses*, says Anthony Di Prima, Senior Manager at Wavestone. *Components and systems will differ between, say, the worlds of chemistry and energy. The IEC 62443 standard incorporates a proposed harmonisation of best cyber practice for this fragmented market, which is used to operating inside closed systems. This standard enables a move towards greater interoperability, and with international scope*".

IEC 62443: what it's all about

The IEC 62443 standard consists of several documents – for informed audiences – grouped into four sections.

- **"General 62443-1":** this first section groups together documents covering general concepts, terminology and methods. In particular, it defines a glossary;

"The world of IT has a strong focus on confidentiality and integrity: in the case of suspected attacks; there is an immediate tendency to disconnect the system. A factory, by contrast, needs to maintain uninterrupted production, and has to deal with both human and environmental risks"

Fabien Miquet
Product & Solution Security Officer Siemens

- **"Policies & procedures 62443-2":** this second section specifies structural measures, and is aimed at operators and maintainers of automation solutions. It also contains recommendations for corrections and updates to system components, in compliance with the specific characteristics of critical industrial infrastructure (IEC-62443-2-3);

- **"System 62443-3":** this third section focuses on operational security methods for ICSs (Industrial Control Systems) – or rather, IACSs (Industrial Automation and Control Systems, not to be confused with SCADA), as the standard provides its own definition of command and control infrastructures. It provides an up-to-date assessment of the various cybersecurity tools, describes the method and resources for structuring their architecture into zones and channels, and provides an inventory of cyberattack protection techniques. In this way, it provides a means of segmenting IACSs into zones, based on equipment criticali-

ty levels (62443-3-2), yet with an understanding that these zones can then communicate with one another – whether by USB key, network cable or VPN link. **It is certainly the most interesting part, in its in-depth examination of the components of a cyberdefence system**;

- **"Component 62443-4":** lastly, this fourth section is intended for manufacturers of command and control solutions: PLCs, monitoring systems, engineering stations and other switching equipment. This part describes the safety requirements for such equipment, and sets out best practice for product development.

"*IEC 62443 is the most comprehensive standard on the market:* ***it takes into account both pure IT security and operational reliability****. It is pragmatic. In industrial environments, unlike office environments, you can't implement a cybersecurity system without taking operational reliability into account. That's one of the main reasons why the IEC 62443 standard really comes into its own when talking about the security of industrial IT systems,*" Khobeib Ben Boubaker points out. So it's vitally important to define the zones and channels of each industry's infrastructure and the level of risk for each of these zones, and to apply the related security measures as defined in IEC 62443-3-3.

The seven fundamental requirements of the IEC 62443 standard should be added to this zone distribution:

- identify and authenticate all users (people, software processes and devices) before authorising access to a system;
- control use (enforce the privileges assigned to an authenticated user);
- ensure the integrity of data, software and equipment;
- ensure the confidentiality of information in data flows, and in data storage spaces;
- restrict unnecessary data flows;
- respond to attacks by informing the competent authority in a timely manner;
- and ensure that the system is resilient against a DDoS attack.

To address most of these security requirements, "*the firewall is one of the most appropriate security measures. However, it needs to be optimised and hardened physically. A traditional firewall can't be deployed in a refinery or water network, because the physical constraints are not the same as in a traditional computer room. It needs to be able to withstand extremes of temperature, dust and electromagnetism,*" explains Simon Dansette, Product Manager Stormshield.

A plea for in-depth cyber defence

The principle of defence is the clear message that embodies the standard; it amounts in practical terms to ensuring that each sub-assembly of the system is secure. It stands in contrast to a perimeter-based view of system security. "***A system's security must not be based on one single barrier***," Fabien Miquet says. *And that's why the IEC 62443 standard advocates this principle of defence in depth. Compliance with this standard is therefore an assurance of maturity in terms of cybersecurity*".

As an actor with a commitment to the protection of sensitive systems, Siemens was one of the first major groups to make use of the IEC 62443 standard to certify its development processes for automation and drive products, including industrial software. "*The IEC 62443 standard is one of the only standards to cover security at an industrial level for not only an individual product, but a group of products – a system, a solution – and even the development process for the product. In addition, it is internationally recognised across the en-*

tire industrial sector: which is perfect for Siemens, whose activities cover diverse areas such as energy, health, pure industry (food, drink, etc.) and construction. That made it an obvious choice, Fabien Miquet continues. *Siemens has around thirty IEC 62443-certified factories. We have a lot of confidence in this standard, as do our customers: and that ensures we're all on the same page*".

But **it must not be forgotten that the industrial sector is a complex one**: most factories lack maturity in terms of cybersecurity, particularly as a result of systems introduced for long periods of service (20 to 30 years, or even longer), which are becoming obsolete. For this reason, the challenge is not to set up cybersecurity systems for the processes operated by the factories of tomorrow; but rather, for those of the factories of today and yesterday. Changing machines and controllers would represent an expenditure of millions of euros – something likely not to be within many companies' reach at the present time. Today, the important thing is to implement an initial level of cybersecurity before it ultimately becomes an essential requirement in the factory's development strategy.

IEC 62443: a constantly-evolving standard

Although the IEC 62443 standard was drafted several years ago, it is still ongoing. The standard is the fruit of working groups from the ISA (International Society of Automation), or more specifically, the GCA (Global Cybersecurity Alliance) ISA under the aegis of the IEC (International Electrotechnical Commission). "*Like other standards, the IEC 62443 standard needs to be continually re-assessed, even during its development process. Regular updates are required, especially in an industrial environment. An environment – and more generally, a 4.0 industry – in which more and more objects communicate with the outside world, and in which sensitive subjects such as the IIoT, the cloud and even remote systems must be constantly re-examined*," says Anthony Di Prima. "*The more new functions and new modes of operation there are, the more the standard will evolve; and as it does, so will its adoption rate: many domestic and international calls for tenders now make reference to the IEC 62443 standard. There has been a real trend in this direction over the last five years*," Khobeib Ben Boubaker says.

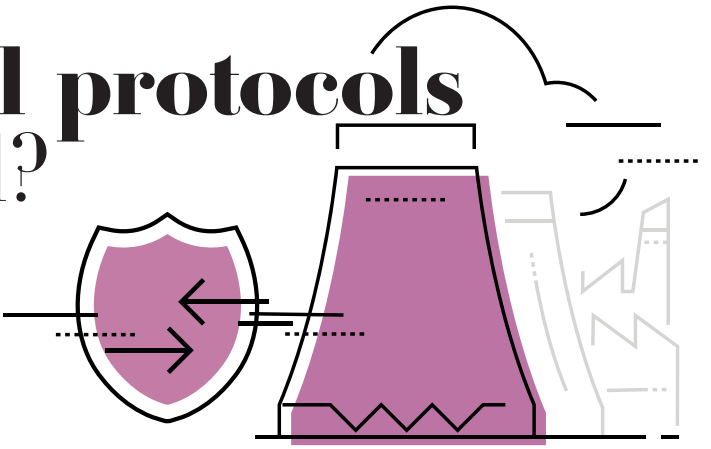
"The IEC 62443 standard is one of the only standards to cover security at an industrial level for not only an individual product, but a group of products"

Fabien Miquet
Product & Solution Security Officer
Siemens

Indeed, developing Secure by design products means thinking about cybersecurity from the start of the process. "*The traditional approach of designing the product first, and considering security issues later, is now out of date. Cybersecurity is no longer an option: it has become an operational performance requirement in its own right*," concludes Fabien Miquet. •

How can **the security of industrial protocols** be controlled?

November 4, 2020



Communicate, inform, order... in the industrial world, PLCs have their own language to communicate with each other and operate an entire operational infrastructure. This is what's known as industrial communication protocols. It is a lexical field which has laid semantic foundations for the notions of safety, efficiency, productivity and, since the Stuxnet cyberattack, cybersecurity. This event forced the industrial world to become aware of the vulnerabilities of industrial control systems. And to get on the cyber train.

By

Marco Genovese

Ten years ago, Stuxnet attacked

Back in 2010, this computer worm targeted the programmable logic controllers (PLCs) that controlled the centrifuges on a uranium enrichment site in Iran. It damaged the nuclear infrastructure by disrupting the working of the centrifuges. As a result, it also opened the industrial world's eyes to the vulnerabilities of control systems and the need to apply security solutions to industrial communication protocols.

The sector became aware that the PLC data exchange formats, developed decades ago, were no longer in sync with **the reality of an increasingly connected world**. Cybersecurity had not been a concern until then, and few industrial protocols offered native security features. And this is still the case.

The BlackEnergy and Industroyer attacks, specifically designed to disrupt electricity grids in Ukraine, are a leading example of such cyber methods. Water pollution, pipeline ruptures, explosions, or physical damage - there are many different disaster scenarios. "*Industrial PLCs are interconnected and communicate with each other – and with the supervision station – using industrial protocols specific to these environments*, says

Vincent Nicaise, Industrial Partnership and Ecosystem Manager Stormshield. *This form of language has a major impact in the real world since it enables physical systems to be controlled. For example, opening a tank draining valve, switching a traffic light to green, or controlling a building's boiler. As the level of criticality of such communications is very high, it is essential that a layer of cybersecurity be added to ensure they are legitimate*". But is it that simple?

Industrial cybersecurity up against the temporality of OT

Even after the Stuxnet attack, **most industrial protocols do not include a cybersecurity dimension**. Nor they do provide any authentication or encryption mechanisms. This situation is all the more dangerous because the OT equipment that uses these protocols has a much longer lifecycle than IT equipment. The cyber risk therefore grows over time... This is particularly true for best-known protocols such as Modbus, Profinet, BACnet (specific to building management systems), IEC 60870-5-104 and DNP3 (specific to power distribution grids). In recent years, proposals have been put forward in an attempt to improve the security of some of these industrial protocols.

"*Nevertheless, in most cases, none of these solutions guarantee an acceptable level of security*, says Vincent Nicaise. *Mainly because automation equipment suppliers had developed them without any knowledge or experience of the cyber risks. Today, the number of secure protocols can still only be counted on one hand.*"

A lack of awareness of the risks accompanied by deeply ingrained misconceptions. The most common misconception is that held by industrialists, who believe they are protected from cyberattacks if they use proprietary protocols and databases. While proprietary solutions may provide reassurance to some, they may also not have undergone any security analysis. It all depends on how much attention the designer paid to the security of their solution, on code auditing, security analysis, etc. In a sector that has historically not been particularly vulnerable to cyber threats, the risk now is more than legitimate. Furthermore, it is important to bear in mind that while a protocol might not be vulnerable, the entire chain underlying the protocol may well be. Take the OPC UA protocol for example, which introduces the use of signatures and encryption as protection: since it is itself based on the TCP transport protocol, it is vulnerable to TCP, IP, and Ethernet attacks. From the protection of isolated industrial networks to restrictions in response times that are incompatible with security mechanisms, there are many other myths related to industrial systems out there.

> **"Automation equipment suppliers had developed them without any knowledge or experience of the cyber risks"**
>
> **Vincent Nicaise**
> Industrial Partnership and Ecosystem Manager Stormshield

The importance of knowing your equipment

"*Most industrialists are aware of the protocols used by their equipment, but they do not have a detailed knowledge of all the communications that may be exchanged, such as: which PLCs are communicating with each other, and with which actuator and sensor are they also communicating, etc.? It is important to know the physical and logical mapping of your network. Finally, and most importantly, it is important to be able to monitor and update this information regularly, because infrastructures evolve over time,*" says Simon Dansette, Product Manager Stormshield. A network probe can respond to this need: listening on the network, it analyses protocols and communication flows, and can map the installation's flow

matrix. But its actions are limited as it has no mechanism that could block flows or isolate equipment that it identifies as 'infected'. "*This solution is only useful for increasing visibility when used alongside an industrial firewall, as it does not in any way secure flows by blocking malicious actions,*" says Simon Dansette.

In addition, it is essential to understand how industrial processes work. Unfortunately, most OT training courses for IT professionals are limited to understanding HMIs (Human-Machine Interfaces) and PLC configuration. However, it is essential to know which industrial protocols are used to transport a command or activate a service, and what type of anomalies can occur on the network. Cyber experts in charge of securing OT networks find themselves at a disadvantage in that they do not know the industrial environments, how they work, or their operational constraints. These shortcomings, linked to the convergence of IT and OT networks, are reminiscent of the divide between VOIP (voice over IP) and traditional telephony that occurred 20 years ago. At that time, there were two worlds: that of network experts and that of telephony experts. Each was unaware of the other's problems. Compared to the telephony convergence that occurred 20 years ago, we now have an advantage: virtualisation. In the age of digital twins, it is now possible to create virtual replicas of an industrial plant to test attacks and solutions.

Viable security solutions

Fortunately, some industrial protocols propose native security mechanisms. This is the case, for example, with DNPSec (a secure version of DNP3), OPC UA (signed/encrypted), IEC 62351, and CIP Security (an extension of the CIP protocol). However, changing equipment to support these protocols is too time-consuming and costly for manufacturers, so the short-term solution is to apply a layer of industrial cybersecurity to their non-secure protocols.

The sector currently has two main approaches to apply this layer of industrial cybersecurity. This first is the use of detection probes to detect an illegitimate flow or process drift. However, as mentioned above, they will not be able to block illegitimate traffic or intervene in the system. The second approach is the use of industrial firewalls. Generally based on signature detection technology, they use a database of known malware signatures to recognise, in real time, intrusion attempts and block them. Yet, this method of protocol analysis also has its limits: if a new, unknown attack occurs, it will not be associated with a signature and will thus have no trouble passing as a legitimate communication flow. "*In addition, signature analysis can slow down communication between PLCs and seriously affect processes*, says Vincent Nicaise. *This is problematic in an industrial system, where each piece of information sent is expected to arrive at a specific time for processing*". It should be noted that an industrial control system with about fifty PLCs will generate nearly 20,000 requests per second. And just as many responses. The system as a whole therefore generates a total of 40,000 packets per second - or 40 packets every millisecond. Hence the importance of choosing a suitable industrial firewall solution to avoid latency. An alternative is the use of an IPS (Intrusion Prevention System) plugin, which contextualises the analysed data to identify the industrial protocol and its specificities. This way, the industrial firewall becomes capable of identifying the codes or functions used and letting them pass through (according to the defined security policy). As such, legitimate flows that are strictly necessary to control a process

"It is important to be able to monitor and update this information regularly, because infrastructures evolve over time"

Simon Dansette
Product Manager Stormshield

are recognised – and are the only ones that can pass through, like with whitelists (or allow lists). And to go even further, this protocol analysis can be coupled with firewall rules. This is particularly interesting in the context of remote maintenance: the use of a certain protocol can be authorised to an authenticated person only and/or only during a specific intervention time slot.

In such situations, "*it is preferable to choose an intrusion prevention system that will contextualise communications according to the protocol detected and thus focus the conformity analysis,*" says Vincent Nicaise. Indeed, these systems limit false positives, facilitate the management of custom function codes – which often go hand in hand with industrial protocols – and provide comprehensive contextual protection for communications between PLCs and control stations.

And to go further still, an industrial firewall must be able to integrate custom patterns by customising and specifying certain functionalities. "*I can thus ensure that the temperature of my oven should never exceed 500 degrees, regardless of the data being exchanged. The custom pattern, via the firewall, analyses the rules and allows precise control of certain variables. So, if the order 'turn the oven to 1,000 degrees' comes through, it will be blocked and not processed,*" explains Khobeib Ben Boubaker, Head of Industrial Security Business Line Stormshield. These customised rules allow manufacturers to adapt to the industrial context and to control communication flows with even greater precision in situations where a threshold is exceeded, or rules have not been previously established. It is one step closer to cybersecurity for industrial systems. •

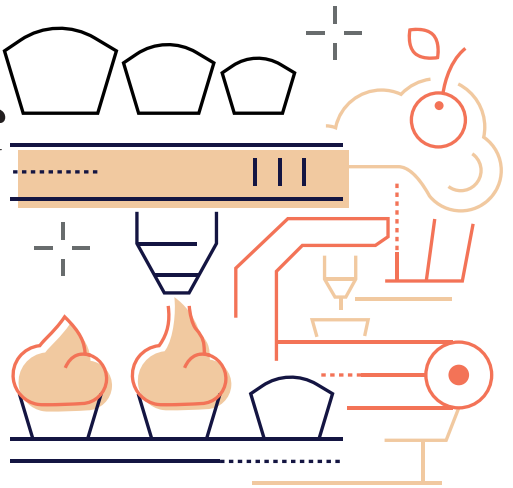
"It is preferable to choose an intrusion prevention system that will contextualise communications according to the protocol detected and thus focus the conformity analysis"

Vincent Nicaise

Industrial Partnership and Ecosystem Manager
Stormshield

The manufacturing industries faced with cyber threats

May 14, 2020



The discovery of new forms of ransomware, specially designed to attack operational networks, marks a new development in the field of industrial cyberattacks. By directly targeting production lines, this malware is changing the digital security perimeter of industrial groups by striking at their very heart. What if destabilising production lines was the cyberattackers' new objective?

By

Khobeib Ben Boubaker

The news arrived in a tweet. On 6 January 2020, the researcher Vitali Kremez, from the Malware Hunter Team group announced the discovery of Snake (or Ekans), a ransomware program able to take down industrial networks and paralyse production lines.

This news caused quite a stir in the cyber community. However, Snake is not the first ransomware program to target OT networks. Back in 2019, the LockerGoga ransomware program caused major disruption, particularly for the Norwegian aluminium producer Norsk Hydro – jeopardising their operational activities and causing serious financial losses. So why all the fuss about Snake then? This is chiefly because this ransomware program is believed to be able to attack even more services used only within industrial networks. With the number of cyberattacks and their complexity increasing, **should we now expect industrial production to become a prime target for cyberattackers?** After Industroyer, does the advent of Snake mark a new development in the field of cybersecurity for industrial systems?

Manufacturing and the industrial environment

Manufacturing is a sensitive sector with a number of specific characteristics, which are all potential vulnerabilities. The first challenge concerns the life expectancy of equipment, which is designed for an average of twenty years' use. On most industrial sites, *"you'll find a combination of infrastructure of differing ages, with recent and not so recent network architectures and operating systems, which don't all feature advanced security standards as upgrades are expensive,"* stresses Vincent Riondet, Head of Cybersecurity Projects and Services teams Schneider Electric France. This is the case for example with IT workstations dedicated to the command and control of machines: they often run very old versions of the Windows operating system, which were usually not connected to the Internet. *"Many legacy plant control systems may be running outdated operating systems that cannot easily be swapped*

out or a custom configuration that isn't compatible with IT's standard security packages," adds the researcher Nisarg Desai in a blog article.

Another challenge is the lack of uniformity between the suppliers of equipment, control software and components. Not all of them meet the same requirements, standards or conditions concerning creation, control and other factors. A single vulnerability or a single back door can then bring down the entire production line. As these production lines are often complex, involving stakeholders who do not communicate with one another, they can be particularly vulnerable to outside attacks. And to further complicate matters, some maintenance operations can be performed by off-site operators using USB-based media to update or configure the equipment. Here too, this type of work can provide a channel for cyberattacks, as in most cases the servers are not protected.

Finally, much like the rest of the industrial environment, the production chain, which was long considered as an isolated system, is increasingly less so. The very term IT-OT convergence implies the connection of OT networks, one of the main infection routes. As a result of this connectivity, the production chain is now faced with new cyber risks, already very familiar to the IT world...

"And so you'll find a combination of infrastructure of differing ages with recent and not so recent network architectures and operating systems, which do not all feature advanced security standards as upgrades are expensive"

Vincent Riondet

Head of Cybersecurity Projects and Services teams Schneider Electric France

Manufacturing-related risks

From the supply chain to networks, the extent to which manufacturing is exposed to the risk of cyber threats has grown considerably over recent years. And with it, the scope for potentially devastating effects. As an example, the Danish manufacturer Demant, which produces hearing aids, has already been the victim of a blockage of its assembly lines in September 2019. **The estimated cost of the ransomware?** More than 95 million dollars. Most of these losses stem from lost contracts and the firm's inability to honour its orders, explained the company.

It's easy to imagine that a targeted attack against vulnerable operating systems for example, would make it possible to compromise the command and control systems of several companies in the food industry or the pharmaceutical sector, leading to the production of defective products. This would pose **a major risk for these companies**, which are required to guarantee the complete traceability of their products as part of their quality control systems. There is also a major risk of industrial espionage via targeted attacks. Finally, we should not ignore the fact that certain cyberattacks against production lines could endanger the physical well-being of the operators themselves and also result in serious environmental incidents.

To fully understand the attraction of the manufacturing sector for cyberattackers, we must consider the business model of these industrial companies. Because apart from guaranteed media coverage in the event of sustained disruption, the cyberattackers are above all motivated by the desire for financial gain. Indeed, stopped production lines entail clear losses for businesses, a factor which may make these industrial companies more disposed to pay ransoms promptly. Though with no guarantee of recovering anything.

Industry 4.0: extending the scope of the attack

At a time when the industry of the future is emerging, the development of the Industrial Internet of Things (IIoT), the digitisation of factories and artificial intelligence technology are making OT networks ever more connected and communicative, particularly with regard to IT networks. But this ultra-connection exposes them even more to the threats. "*Especially as OT networks often have no network barrier or endpoint barrier,*" adds Vincent Riondet. The many different components of OT are therefore all possible entry points, in particular because the convergence between IT and OT is still largely a delicate one or even inoperative in certain cases.

"*With industry 4.0, the number of access points has increased in response to a requirement for interconnection, which has been undertaken with no real thought given to security-by-design,*" explains Vincent Riondet. The arrival of the IIoT and automatic order integration or the arrival of augmented and virtual reality have opened up new vulnerabilities. In May 2017, in collaboration with the Polytechnic University of Milan, another stakeholder in the cybersecurity sector demonstrated that it was possible to take total control of a robot and to install malware on it capable of 'reprogramming' it.

Guaranteeing the integrity of the OT sector

How are companies in the sector facing up to these new threats, which mark **a new development in the industrial cybersecurity world**? For the moment, efforts to guarantee the cybersecurity of the manufacturing perimeter are not uniform in nature. "*Improving the security of the OT sector firstly means securing the operating systems of network equipment more effectively,*" explains Vincent Riondet. But at the same time, one of the major challenges where manufacturing infrastructure security Is concerned is to fully control network communications.

Encrypting all communications between the machines is therefore an additional step toward greater security. "*In addition to appropriate network segmentation, it's possible to focus on securing data flows by guaranteeing the privacy and integrity of the data,* adds Vincent Seruch, ICS Security Team Leader at Airbus CyberSecurity. *This means mapping all communications on the IT networks and encrypting them using cryptographic methods. But this must also be achieved while taking account of the need to inspect the data flows*". Remote maintenance is another opportunity. The performance of remote updates makes it possible on the one hand to do away with potentially dangerous USB-based media and secondly to limit the risk of errors inherent to excessively frequent changes of operators. The result is greater efficiency where updates are concerned, on condition that access to this remote maintenance is also secured.

The Covid-19 health crisis today raises the question of industrial sovereignty and the relocation of certain factories in strategic sectors back to Europe. The implementation of such a plan could then serve as a life-size test, in as far as this 'industrial de-globalisation' would be accompanied by increased automation. The OT sector would be increasingly exposed. It's a fair bet that between now and then, industrial cybersecurity will have assumed a greater profile. •

Events of 2020

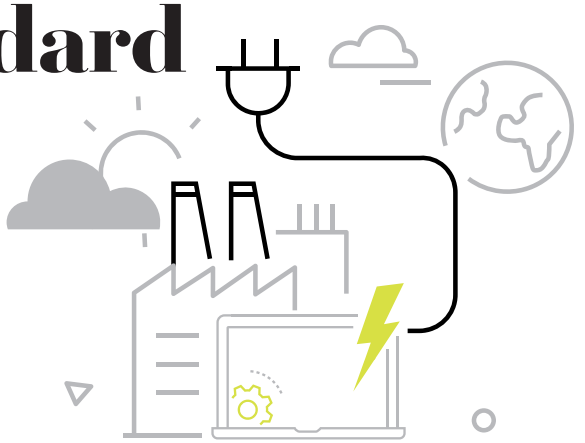
In June, Japanese giant Honda announced a malfunction in its computer networks and the suspension of some of its production lines. Sources close to the case have suggested that the US subsidiary's IT department may have been hit by ransomware.

In August, German carmaker Volkswagen and Tesla in the US were in turn targeted by malware. The second case featured a scenario straight out of Hollywood; the networks were supposedly infected by an employee of Russian origin, with attendant suspicions of state-sponsored interference.

ELECTRIC
FACILITIES

How the IEC 61850 standard structures the electrical industry

December 1st, 2020



The International Electrotechnical Commission writes the standards that govern how the electrical industry works. And among this proliferation of standards – which sometimes come with rather forbidding abbreviations – one has a very special role to play, as it specifies communications for electricity distribution infrastructure. We explain IEC 61850 and the cyber risks it faces.

By

Khobeib Ben Boubaker

Riding on public transport, watching TV, listening to the radio and even boiling the kettle may seem completely straightforward, but that's because the entire energy sector – and the electrical industry in particular – is hard at work to ensure continuous distribution and access to energy. This sector is highly standardised, and must satisfy the requirements of many international standards. These include the IEC 61850 standard, governing the operation of smart grids. **And smart grids are synonymous with networks connected to the outside world, and also with interoperability**. In both cases, such communications introduce an additional aspect for this industry, which is as a result also required to address the question of cybersecurity in electricity distribution infrastructures. However, cyber players – with software publishers at the forefront – are there to facilitate the transition towards the adoption of cybersecurity, considering not only the constraints imposed by the IEC 61850 standard but also security issues.

IEC 61850: the issues behind the acronym

What is the IEC 61850 standard? This international standard is dedicated to the world of energy in general, and the electrical industry in particular. Although hardware requirements for electrical environments are also part of this standard, we will be concerned mainly with the protocols it specifies. More specifically, these protocols related to 'IEDs' (Intelligent Electronic Devices) – intelligent network components located

in electrical substations. And what is the purpose of these protocols? To scope and ensure the operation of these smart grids, covering the specification of communications, the connections between energy production sources and electrical networks, etc. "*IEC 61850 provides a structure for communications and interaction between equipment, making it possible to specify a template for exchanged data and the level of abstraction: who does what in an electrical environment? Etc. This provides a route from design through to operation,*" explains Simon Dansette, Product Manager Stormshield.

The purpose of the IEC 61850 standard is therefore to simplify the management and control of electrical substations, and to ensure their integrity and availability. For example, the tasks performed by these substations are subject to very short latency times, and IEC 61850 satisfies this constraint by recommending that system operations are monitored in real time. In order to properly fulfil the specifications inherent in electrical substations, this standard therefore includes several protocols which play a regulatory role and guarantee the running of the electrical grid. Among these, three major communication protocols for IEDs should be borne in mind: the MMS (Manufacturing Message Specification) protocol, which sends configuration actions; the GOOSE (Generic Object Oriented Substation Event) protocol – a real-time protocol that provides meaningful interoperability between equipment of different brands and very low latency times for decision-making – and lastly, the SV (Sampled Values) protocol, which is also a real-time protocol, dealing with the transmission of values to the IEDs. This all provides an orderly framework to ensure the smooth running of electrical substations.

"Electrical substation infrastructures were not originally connected to external grids, which means they were not designed with cybersecurity issues in mind. However, with the arrival of smart grids, that paradigm has been changed"

Simon Dansette
Product Manager Stormshield

Although the IEC 61850 standard imposes a very standardised and formalised framework, all communications being conveyed via the various protocols appear vulnerable from a cyber point of view. The data carried via these communications are in plain (i.e. unencrypted) format, and there is no mechanism for verifying message authenticity (which is particularly true of the 'SPAC' system protection, automation and control system). "*Electrical substation infrastructures were not originally connected to external grids, which means they were not designed with cybersecurity issues in mind. However, with the arrival of smart grids, that paradigm has been changed,*" explains Simon Dansette. To address business and environmental requirements, electricity production and transmission optimisation work needs to take the form of greater interconnectedness. And that means facing cyber risks.

Although it was already possible for electrical grids to be targeted by cyberattacks, such as bounce attacks (in which, for example, a workstation could be infected in order to gain access to the heart of an electrical grid and compromise its communications), **smart grids clearly raise the question of cybersecurity in electrical substations**.

Smart grids: a target for cyberattacks

Consequently, the IEC 61850 standard has little or nothing to say about communications security and the question of cybersecurity (these concepts are covered by a different standard, IEC 62351). And yet electrical substations are key points in the entire energy distribution process, where the shutdown or sabotage of the electrical system could prove to be extremely critical. "*An attack on the electrical industry is an attack on the heart of how society operates. For example, if a cyberattack causes a blackout, this could have dramatic consequences and cause a wide range of human and material damage,*" warns Nebras Alqurashi, Business and Technical Development Manager for the Middle East and Africa Stormshield.

Because of the interconnection between all the points which comprise it, the entire electrical industry's infrastructure is fragile and sensitive. And whether the issue is the failure of an electrical line, an energy overload or a total blackout, the electrical industry needs to have the ability to react quickly to limit potential impacts. Italy still remembers its largest blackout back in 2003, caused not by a cyberattack but by a tree falling on an electrical line. Most of the country was then unable to function normally and, among other problems, trains running at that time were stopped in their tracks, affecting 30,000 passengers. "*You have to start from the assumption that if the electricity stops, pretty much everything stops working and there are immediate consequences: for example, traffic lights stop working, causing a cascade of accidents, or the water supply to remote regions runs dry…,*" Nebras Alqurashi explains. Obviously, then a failure in the energy sector is bound to cause a domino effect that impacts a number of dependent sectors – backup systems notwithstanding. In 2011, Germany produced a report listing the potential material consequences of a blackout: a reduction in telecommunications, paralysis of water treatment plants, shutdown of cold chains, etc.; and in 2015, British insurer Lloyd's produced a calculation of economic damage, taking the example of a blackout that simultaneously hit 15 US states: the potential bill to the United States was a modest sum ranging from 243 billion to 1,000 billion dollars.

"An attack on the electrical industry is an attack on the heart of how society operates. For example, if a cyberattack causes a blackout, this could have dramatic consequences and cause a wide range of human and material damage"

Nebras Alqurashi

Business and Technical Development Manager for the Middle East and Africa Stormshield

A successful cyberattack on an electrical industry will therefore have a phenomenal impact. However, an excellent knowledge of electrical grids' protocols, systems and infrastructure would be required to deliver such an attack. And attackers who engage in such practices are often groups sponsored by state actors. Indeed, the energy sector in general, and the electricity industry in particular, are targets for cyberattacks of geopolitical scope. Ukraine and its electricity network have already been hit several times. In 2016, BlackEnergy malware was used to knock out a portion of the country's electricity resources, affecting around 1.5 million people. The attackers targeted an electricity supplier in western Ukraine, bringing down a number of lines. According to researchers, the attackers' modus operandi was as follows: use of BlackEnergy malware functions to erase part of the power station's hard drive and prevent operating systems from

restarting prior to the remote hijacking of computers infected by the malware. It is suspected that Russia was behind the attack.

In 2017, another attack targeted the Ukrainian capital, aimed at energy supplier Ukrenergo and plunging part of the city of Kiev into darkness. Although Russia was once again suspected of having sponsored the attack, the attackers' MO was different, this time using the Industroyer malware, known for its ability to take control of electrical substations by adapting to the communication protocols they use. "*An attacker will be able to take advantage of these protocols' functions to conduct their attack*, explains Marco Genovese, Pre-Sales Engineer Stormshield. *In the case of the IEC 61850 standard, the GOOSE protocol's role is to provide high-speed communications, which means it does not have time to wait for confirmation that packets have been successfully received. An attacker could take advantage of this weakness to inject malicious packets into the network*".

In 2018, following the Ukraine, it was the turn of the United States, which – via the country's Department of Homeland Security – reported that it had been targeted by cyberattacks against energy infrastructure since 2016. The attacks were thought to have been conducted by the Energetic Bear group (also known as Dragonfly), with links to Russia. According to US authorities, Energetic Bear had first infected the networks of small production facilities, then conducted targeted spear phishing campaigns in a gradual move towards the largest industries in order to remotely hijack the networks of companies in the energy sector.

The electrical industry is therefore one of the most critical sectors in terms of cyberattacks, and, **although awareness is rising as the cyber risk increases, systems and infrastructure remain complex**. And change is coming in small steps. This means that software publishers have a key role to play in supporting these industries by offering solutions that meet the operational constraints of the IEC 61850 standard while ensuring that IT infrastructures remain secure.

What's the right balance between cybersecurity and the requirements of the IEC 61850 standard?

The task of taking the requirements of both information security and the IEC 61850 standard into consideration poses a sizeable challenge to publishers. Because if publishers do not provide a response to the business requirements of this industry, it is difficult (or impossible) to see them responding to the cyber requirements: within the context of IEC 61850, the three protocols mapped by the standard – GOOSE, MMS and SMV – are among the few that can be used, even though other protocols such as IEC 104 can also sometimes provide a solution to this security requirement. The standard thus imposes stringent hardware requirements, while the protocols have business implications to which cybersecurity solutions must adapt. The task facing publishers is therefore to place a cybersecurity layer over existing infrastructure. "*It must be possible to integrate solutions transparently within electrical networks and check the compliance of messages for all three protocols,*" Simon Dansette points out. Another important aspect: given that the electrical industry operates with very short latency times, there is a need to avoid presenting solutions that would impact the speed at which electrical substations operate, if at all possible. Lastly, a small additional difficulty: publishers need to consider security problems at electricity substations outside the world of the OT. For example, because the GOOSE protocol runs on Ethernet networks, all successful attacks against this network will work equally well with the GOOSE protocol.

But what solutions will satisfy IEC 61850 requirements while also providing the cybersecurity layer that the electrical industry needs? Several options are possible, following an essential first stage of network segmentation for the various electricity network in-

frastructures in order to minimise the risks of intrusion into the systems. IPS (Intrusion Prevention System) functions in some industrial firewalls are based on signature detection as a countermeasure against attacks or anomalies. However, this system is insufficient on its own to ensure the security of electricity networks because, as Marco Genovese explains, "*Signature-based IPS can only detect what is already known and listed. But it's difficult to make advance predictions about cyberattacks and the forms they may take*". Some publishers have also developed solutions with integrated plugins that can strengthen compliance checks on communications for electrical substations, and ensure that these communications meet the requirements of IEC 61850. "*By implementing industrial firewalls, this approach enables deep packet monitoring and inspection that takes the communication context into consideration (Stateful DPI), with a simple goal: to allow only what is deemed to be legitimate,*" says Nebras Alqurashi. The electrical energy sector needs to have access to systems capable of analysing and reconstructing traffic to recontextualise it and establish whether it is legitimate, or whether (for example) there has been an attempt to inject packets with a malicious payload into the communications.

In the electricity industry, a consideration of cyber risks needs to be viewed in the same way as the IEC 61850 standard is in the world of electrical substations: as an essential component! ●

"If publishers do not provide a response to the business requirements of this industry, it is difficult or impossible to see them responding to the cyber issues"

Khobeib Ben Boubaker
Head of Industrial Security Business Line Stormshield

Events of 2020

In March, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced that it had been the victim of a cyberattack. Fortunately, it seems that no critical control systems were affected.

In May, US President Donald Trump declared a national emergency after foreign cybercriminals threatened the country's power grid. He even went so far as to prohibit the purchase of foreign equipment.

At the same time, a cyberattack struck the heart of the British electricity grid. Fortunately, "only" the Elexon company's IT structure was affected.

White paper

FROM 2015 TO TOMORROW: CYBER-INTRUSIONS IN ELECTRICAL GRIDS

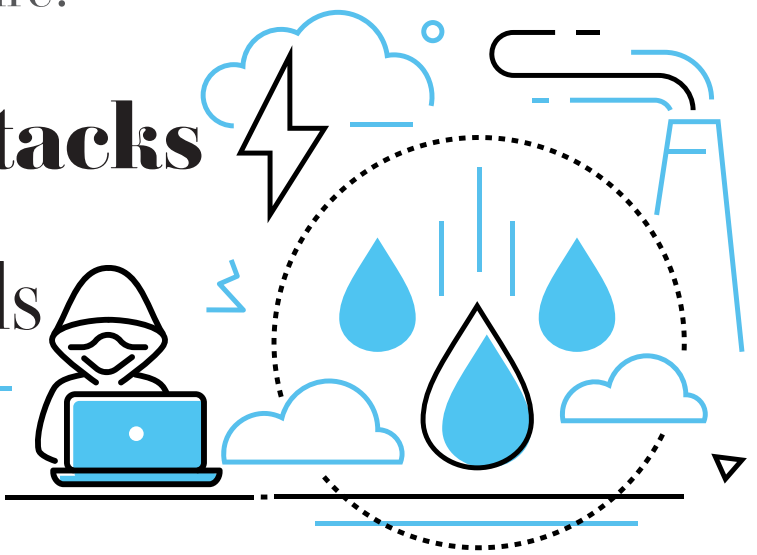
Nothing in our modern world operates without electricity – from our industries through to service-sector companies, and including cities and homes.

Cyberattacks that are sufficiently well conducted that they paralyse a power plant or even cause a blackout can also have a major impact on populations and states. Being able to inflict damage on power grids means having a powerful means of political and financial destabilisation. Cybercriminals have understood this and, in recent decades, have made a special effort to focus on energy systems.

We present a white paper that examines this evolving and contagious threat.

WATER
MANAGEMENT

Water infrastructure: when states and cyberattacks rear their ugly heads



November 16, 2020

Attempted cyberattacks targeting dams, irrigation systems or wastewater treatment plants have received little coverage in the media. However, these attacks exist and present an unusual strategic challenge. What's the worldwide situation with cybersecurity for water systems?

By

Khobeib Ben Boubaker

Generally speaking, cyber protection for human beings is a major challenge, ranging from the supply aspect to that of health and water management. Over and above the critical issues inherent to this sector and the vital importance of this resource, the water industry must also deal with the scale of the cyberattacks directed against it. Just like the industry itself, the cyberattacks targeting the water sector are complex and sophisticated. They are often orchestrated by state-sponsored bodies whose objective is to destabilise a country's economy. Water companies must therefore simultaneously reconcile important production challenges and critical security requirements. The goal is to effectively protect all critical infrastructure and equipment by adopting a defensive position aimed at limiting the damage which could be caused by large-scale cyberattacks as far as possible.

What's the current situation with cybersecurity for water systems?

The main digital developments in the water infrastructure field are related to the replacement of RTC connections (the communication method formerly used) which have become obsolete, and migration to the ethernet network or 4G and 5G networks which offer improved connectivity. All water industry sites are gradually implementing this migration and are therefore being connected to the outside world, which was not the case previously. In the good old days of RTC, most systems (such as PLCs)

were insulated from the Internet. But with the end of this communication method, these systems are now being connected and are consequently facing new cyber threats.

This paradigm shift presents the water industry with a twofold challenge: converting ageing industrial systems and equipment (Windows XP and others) to better performing – and better connected – technologies and taking onboard the notion of cybersecurity as an integral part of their industrial activities. "*The water industries are now having to give thought to securing their systems as they are part of the IoT or even the IIot (Industrial Internet of Things) landscape, with all of its inherent security issues,*" explains Raphaël Granger, Account Manager Stormshield.

However, the water industry must also face threats inherent to its very nature. Due to the existence of numerous physical sites (water treatment basins, distribution centres and water towers for example), the water industry uses distributed architectures through which messages and orders travel. The challenges of guaranteeing the integrity and privacy of such information flows have now become critical in order to guarantee the quality of a vital resource at the end of the chain, at a time when remote management is becoming commonplace. But these challenges also require genuine cyber-awareness by all participants - like the remote maintenance operators.

A multi-speed regulatory approach

In France, for several years now sensitive infrastructure assets related to the water industry have been categorised as operators of vital importance, as part of the military planning law. As a result, they are monitored closely by the France's ANSSI cybersecurity agency. By necessity, this close attention from the state is forcing the water sector to become more aware of the cyber challenges inherent to its activities.

Internationally, most major stakeholders in the water sector in the developed countries are also beginning to incorporate cybersecurity as a prerequisite. "*The cybersecurity levels of water systems do not yet match the threat levels with which the water industry is faced*, explains Nebras Alqurashi, Business and Technical Development Manager for the Middle East and Africa Stormshield. *But more and more authorities are sounding the alarm and would like to get things moving for the better*". On the other hand, in the developing countries, cybersecurity is way down the list of priorities for water companies. "*For these countries, the challenges are of a completely different kind: water scarcity, water treatment, efficiency of distribution networks, wastewater disposal, etc. Where water management and water access are concerned, not all countries are on an equal footing*", stressed Tarik Zeroual, Global Account Manager Stormshield. When you have inequality and scarcity, you soon get rivalry and conflicts developing around water and the control of its related industry. These economic and political circumstances help create an environment conducive to cyber attacks, which then become a means used by states to pressurise and destabilise one another.

The high stakes involved in the cyberattacks

You could almost say that the water industry spawns problems when we consider the particularly vulnerable facilities and equipment (run on older operating systems), transition to the IIoT or the geopolitical and strategic challenges related to water resources. It's therefore impossible for critical infrastructure to avoid the unwelcome attention of cyber attackers.

As a result, water-related infrastructure is today in the cyber firing line and the preferred weapon used by attackers appears to be ransomware. According to the American company Gray Matter, more than 22 cyberattacks of this kind were recorded in 2019 in the United States alone. And if we go back still further to 2017, cybersecurity researchers at Georgia State Uni-

versity developed a new form of malware capable of poisoning water by changing the chlorine levels used in drinking water production facilities. To simulate this attack, the researchers took control of the facility's PLCs (Programmable Logic Controllers). In their report retracing the simulation, the researchers described the operating methods attackers could use to take control of these vulnerable PLCs. These firstly involved a reconnaissance phase to detect Internet-connected PLCs (including by using the Shodan specialised search engine), and to use them as access points. Once inside the system, the attackers could then proceed to propagate throughout the facility's system, collecting key data about the facility such as information for accessing and controlling the PLCs. Finally, the last stage involved increasing the quantity of chlorine added to the water and displaying false readings.

"A successful cyberattack against the water industry is an attack which can generate an immediate risk"

Tarik Zeroual
Global Account Manager Stormshield

Because this is also one of the objectives of the cyberattacks directed against water infrastructure: advanced strategic attacks, the impact of which may endanger the lives of part of the country's population. And bring about the destabilisation of an entire country. The challenge of protecting public health linked to water is a critical one, which the water companies must take into account as part of their efforts to combat cyberattacks. "*If you can affect a water distribution site you can affect the population, with the risk of significant physical harm. A successful cyberattack against the water industry is an attack which can generate an immediate risk,*" warns Tarik Zeroual.

Looking beyond the work carried out by this university, changing the chemical treatment of water could pose a real risk. Last April, Iran attempted to do just this using cyber attackers to affect the quality of the water supplying part of the Israeli population. The attackers firstly took control of American servers to cover their tracks before then moving on to attack the target water distribution systems. The attack ultimately failed, but had it succeeded, the harm to public health would have been considerable, with part of the population probably being poisoned.

Last July, Israel reported two new attacks against its critical water infrastructure. This time, it wasn't the urban water systems being targeted but those used for the agricultural sector. It was therefore a lower level attack, although Iran is suspected of being the originator of these attacks with the aim of destabilising the state of Israel and weakening it politically. For both attempts, the attackers once again used American servers to the affect the pump control programs.

Cyberattacks against water infrastructure seem to be generally well-run and executed: they are anticipated, prepared and extremely well-documented. The attackers are familiar with the systems they are targeting. Nothing is left to chance and none of this is the result of opportunism. This leads us to suppose that cyberattacks targeting the water industry seem to be ordered by or for states and that the groups of cyber attackers carrying them out are certainly no amateurs. "*The cyber attackers acting against the water industry are organised groups – generally Russian, Chinese or Iranian APT groups – financed or headed by state bodies*", explains Tarik Zeroual.

Water therefore offers the possibility to carry out large-scale cyberattacks with a real strategic dimension involved. The water companies consequently need to equip themselves to limit as far as possible the hijacking of their infrastructure for cyber warfare purposes, against a geopolitical background.

The water industry's answer: improved protection through segmentation

Major problems require major solutions. To counter the cyberattacks targeting it, the water industry needs to filter everything arriving in its facilities from the outside world. To do so, the sector has introduced a segmentation policy on its different sites. This is a vital approach when it comes to protecting water infrastructure, all the more so as it can take varying forms. "*The water companies are segmenting each of their sites and controlling the communication flows transiting through them,*" explains Raphaël Granger. Over and above the segmentation of their operational sites, the water industry is also separating the IT environment (PCs, servers, users) from the OT environment (the operational environment) within them. This segmentation is designed to isolate the operational part in the event of an attack. Finally, within the OT part, it's possible to find another form of segmentation, with a separation between the supervision part and the implementation part (PLCs).

The key stakeholders in the cyber sector, including the software publishers, are supporting the water companies in this move to segmentation and through a certain number of security solutions aimed at improving their capacity to prevent cyberattacks. "*To guarantee cybersecurity for water systems, the software publishers are helping the companies operating in this sector to check the reliability and compliance of their network protocols. Using industrial firewalls, the idea is to ensure that these protocols are not modified or compromised by a cyber attacker,*" adds Raphaël Granger. For this industry, it's therefore very important to have solutions able to verify the legitimacy of the orders performed by the PLCs and to introduce systems making it possible to manage and secure remote access (for remote maintenance or alert management, etc.).

The water industry is organising to fight back against cyberattacks, but this is only just the beginning. In the near future, the industry will need to face a new challenge, that of extending its security policies throughout the whole chain, beyond the water treatment facilities, and adopting a more advanced IIoT approach which involves securing communications and systems from end to end, from the plant through to the consumer. ●

Events of 2020

In January, a water supplier in North Carolina (USA) was hit by a cyberattack. There appears to have been no impact on integrity and distribution, but online payments for half a million people were complicated.

In April, during the Israel-Iran conflict, Israel accused Iran of hijacking SCADA systems in water distribution installations.

In July, the same players were back in the news again. Fresh attacks were reportedly carried out against sensitive water infrastructure, this time used by the agricultural sector.

URBAN AREA WATER BOARD

OPTIMISING CYBERSECURITY **TAKING INTO ACCOUNT OPERATIONAL CONSTRAINTS**

HEALTHCARE

Covid-19 and cybersecurity: hospitals on the front line like never before

June 8, 2020

The Covid-19 health crisis has seen hospitals on the front line like never before in terms of their exposure to cyber risks. A combination of phishing campaigns, Trojans and ransomware has created a constantly shifting cyber risk. But what's behind the digital weakness of the hospital sector?

By

Victor Poitevin

Between February and March 2020 – the months that marked the start of the pandemic in Europe – **malicious attacks against hospitals have risen by 475%** – a figure five times higher than in normal times (according to another cybersecurity player). So much so, in fact, that Interpol has become involved, publicly stating its concern at the proliferation of cyberattacks in health establishments. This warning message was echoed in late May by an opinion column signed by the likes of ex-heads of state and government, former leaders of international organisations, companies and lawyers – Ban Ki-moon, Desmond Tutu, Mikhaïl Gorbachev, with Brad Smith as its principal signatory. The article called for concerted action by governments in the face of the cyber threat.

The Covid-19 crisis has been a depressing confirmation that systems in hospital environments are hypersensitive to cyberattacks. But is this situation purely a product of current circumstances... or is it a public demonstration of digital weaknesses and issues that have been affecting the health sector for a number of years?

Hospitals on the front line

When asked about his daily work as CISO for a regional hospital group in France, Charles Blanc-Rolin confirms that in addition to the considerable work the sector has faced in dealing with the crisis and the creation of new dedicated technology units, **hospitals are indeed being targeted by malicious attacks themed around the Covid-19 issue**. These malicious attacks range from traditional phishing attempts, targeting hospital staff with requests to install false webmail updates, through to more sophisticated CEO fraud. "*Some cyberattackers have claimed to have stocks of FFP2 masks in their attempts to conduct bank transfer fraud against a number of health establishments,*" he explains. In France, university hospitals in Paris have fallen victim to a denial-of-service attack (DDoS) aimed at disrupting

access to hospital staff email accounts. According to a press release from France's ANSSI cybersecurity agency, the incident was "*handled quickly and efficiently by hospital teams, without any critical impact*".

Operations may not have been disrupted in this case; but for other hospitals, the impact of such cyberattacks has been greater: there have been numerous occurrences of this kind in recent months, with cyberattacks in the United Kingdom, the Czech Republic and in Romania.

A lack of cyber maturity

But what sense can we make of the motivations behind cyberattacks? The evidence shows that **hospitals have always been a target of choice for cyber attackers**. "*There are two main types of financially-motivated attacks against hospitals: health data extraction, and ransomware. Health data is information of ultra-sensitive, strategic value in the running of hospital services – which makes it a target of choice for cyberattackers, being of greater value than ordinary personal data. And when dealing with ransomware, hospitals are unfortunately more likely than other organisations to pay out because of their obligation to ensure continuity of care,*" points out Raphaël Granger, Account Manager Stormshield. "*And let's not forget, either, that just like any other company or organisation dealing with this sudden health crisis, hospitals were unprepared for this double blow,*" Charles Blanc-Rolin continues.

In comparison to other strategic sectors such as industry or the banking system, it also appears that health systems generally suffer from a lack of maturity in terms of digital sensitivity and cybersecurity. For example, the widespread adoption of teleworking among some health staff has not made matters easier for already overworked hospital CISOs. Similarly, the remote appointments solutions implemented to deal with the influx of patients have increased the attack surfaces presented by hospitals.

"In French regional hospital groups, only 1% of the overall budget is assigned to digital technology in general (including security), compared to 5-6% in Northern European countries"

Charles Blanc-Rolin
CISO for GHT15

The truth is that the suddenness of the crisis has compounded an already difficult situation. And initial flashes of optimism at the start of the crisis – with some hackers having stated that they would not attack hospitals – have quickly evaporated, highlighting the underlying structural problems.

Chronic underinvestment in IT

As an example, "*the French health system's IT systems have been compromised by chronic underinvestment,*" according to a stark warning issued by French senators Olivier Cadic and Rachel Mazuir in an opinion piece published in early May. "*In French regional hospital groups, only 1% of the overall budget is assigned to digital technology in general (including security), compared to 5-6% in Northern European countries,*" warns Charles Blanc-Rolin. And this issue is made all the more critical by the policy of grouping hospitals together (which has led to the creation of France's GHT regional hospital clusters). "*The need to link and interconnect hospitals, and to make use of various types of smart equipment, has resulted in an increase in the attack surface, and thus in the vulnerability of hospital IT infrastructure. At the same time, inadequate IT budgets and security in the healthcare sector is a limiting factor for such organisations, which are not sufficiently well equipped to face such threats,*" explains Raphaël Granger.

This underinvestment is particularly visible in the

area of healthcare equipment, which is frequently automated. With its coverage of domains such as medical imaging (MRI, scanners), probes and blood and genetic analysis, the ecosystem of automated devices is a particularly varied one. And although some hospitals have the resources to afford the latest equipment, most have to make do with old machinery. "*We're talking about 6-digit invoices for these devices. They're extremely costly, which means that hospital investments are in the 15-20-year timeframe. In most cases, the control stations that operate such equipment are running obsolete operating systems such as Windows XP or Windows 2000,*" explains Raphaël Granger. So when there's a problem, or a machine breaks down, CISOs find themselves stuck: the devices are very often subject to medical certification which prevents the application of security patches. "*The only solution is to isolate these devices within specific networks, avoiding connections with the outside world as far as possible and controlling any necessary data transactions,*" says Charles Blanc-Rolin. But such precautions obviously come at a cost. In the face of dwindling public funding and ever-increasing demands for return on investment, cybersecurity for medical devices seems to have become an issue of secondary importance.

CTM / BMS: a question of operational cybersecurity

As hospitals are transformed into connected, automated systems, we need to bear in mind **the role of cybersecurity in operational technology (OT) networks if we are to understand its vulnerabilities**. Within a hospital building, this covers energy and fluids, such as air conditioning, air pressure levels and fire safety – factors which lie at the heart of smart buildings and their connected infrastructure. And all the more so considering that sensitive hospital environments such as operating theatres, MRI machines and resuscitation rooms require constant air pressures and temperatures. These systems are encompassed within the terms 'centralised technical management' (CTM) and 'building management systems' (BMS). "*Because of the configuration of hospital buildings and certain spaces, air handling is vitally important, and the health risks obvious. Sadly, it's all too easy to imagine the importance of air renewal in operating theatres, and even in rooms, to avoid the spread of bacteria or viruses. Temperature and humidity management are equally crucial; for example, in neonatal and burns departments. And we also need to remember that there can be financial risks, too; for example, when controlling an MRI's cooling system to avoid damaging it,*" points out Vincent Nicaise, Industrial Partnership and Ecosystem Manager Stormshield.

And in a more general sense, "*some medical activities performed by a hospital – such as resuscitation, A&E and intensive care – are sufficiently critical to warrant the use of specific installations that provide a continuous power supply*, Vincent Nicaise continues. *This is an aspect covered by French legislation in public and private health establishments, which demonstrates a clear need to maintain a secure supply of energy at such facilities*". Such a vulnerability was highlighted by the attack on Rouen's University Hospital in France, recalls Rémi Heym, the hospital's director of communication, writing in France's *Le Monde* newspaper: "*Shutting down the entire system is no trivial matter for a hospital, where everything is computerised: prescriptions, analyses, reports, etc.*".

Hospitals are vital infrastructure, yet vulnerable, and subject to very specific threats. They have shown their resilience during the recent crisis... but for how much longer? How many more weeks before another hospital finds itself in the eye of the storm? In addition to the enormous challenges that accompany the 'return to normality', we predict that **the cybersecurity issue will be a central feature of discussions regarding hospital administration**. Will the topic of an increase in ring-fenced budgets be on the agenda? •

#2

WEAK SIGNALS
IN 2020

RAIL
INDUSTRY

The rail industry in the connected era

promising potential versus cyber risks

March 23, 2020

This is the story of one industrial revolution meeting another: for even the rail industry is subject to digital transformation. Electronic tickets, onboard WiFi... the benefits in terms of traveller experience are obvious, but change is also taking place at industrial level, amid national infrastructure. Bringing with it new drivers of operational excellence, but also a fair share of associated risks – chief among which are cyber threats. So, a brief overview...

By

When we talk about digital transformation in the railway sector, we tend to think of e-tickets and onboard connectivity. However, innovation is slowly permeating all layers of a rail network that is becoming more connected every day. The Internet of Things, cloud/edge computing, automation, robotisation and artificial intelligence... just a few disruptive technologies that are propelling the rail industry into a new era.

The promises of Rail Industry 2.0

Franck Bourguet, Stormshield Vice-President of Engineering, sees the opportunities afforded by digital technologies in the rail sector as falling into three main categories. And of these, **operational excellence** is in top position: "*One of the promises of Rail Industry 2.0 is that it provides solutions to boost existing network capacity by making optimal use of available infrastructure*". The issue here is to optimise the service provided by improving the frequency and punctuality of trains, while continuing to deliver – or even improve on – the required operational safety. Another major aspect is that of **passenger safety**: new tools, such as video protection or IIoT sensors, integrated with control and monitoring systems, provide new levels of visibility on board trains and at stations. Lastly, the **passenger experience** is enhanced, particularly through the use of onboard or station-based services, with information and entertainment screens, or electronic ticketing.

To take advantage of these opportunities, operators need to deploy new connectivity capabilities at stations and in trains: IP protocols, WiFi, GPRS and 4G LTE standards, etc. They provide trains with abilities such as interaction with the control centre using the train-to-ground communication system. And these technologies are not merely the preserve

of new equipment: they are now bringing openness (i.e. communication and intelligence) to systems that were traditionally closed.

But opening up your networks also means making them vulnerable and exposing them to malicious attacks... For critical infrastructure such as rail, the serious nature of the issue is evident to all: "*When an attack is made against the transport sector, there can quickly be utterly dramatic consequences, including on human lives,*" pointed out Guillaume Poupard, Director General of France's ANSSI cybersecurity agency, at the International Cybersecurity Forum in Lille (France) in 2017.

Why rail is vulnerable to cyberattacks

Rail transportation IT systems require high levels of availability, accessibility and security, which means that they need to be strong and resilient to cope with cyberattacks. What factors make rail infrastructure vulnerable?

Franck Bourguet identifies several types of risks. Because driver assistance and control systems now feature connectedness and communication, their vulnerabilities present new attack surfaces. If these weaknesses are exploited, it could have serious consequences – potentially including seizure of control of the train.

Another potential risk area is ticketing and the associated financial risks. The issues faced by these highly-exposed rail information systems are ultimately similar to those faced by websites, such as payment security or ticket validity.

And lastly, passenger safety and comfort may be targeted by malicious attacks. Franck Bourguet puts forward a scenario which highlights the critical nature of certain functions, using the case of driverless trains: "*If a train's ability to communicate with its control centre or with its passengers is interrupted, for example in the middle of a tunnel, this can result in scenes of extreme panic,*" he explains. Less dramatic, but nonetheless disastrous in terms of image, is the hijacking of information and entertainment systems, either on board or in the station.

Lastly, **the application of Industry 4.0 technologies to the rail sector creates new risks**. Consider the case of predictive, connected maintenance technologies which are making giant strides forward, driven by progress in artificial intelligence: "*When technical monitoring systems are rendered unavailable, or their data is falsified, there is a potential risk of damage to equipment, undelivered services, and possibly even accidents,*" Franck Bourguet points out.

"When an attack is made against the transport sector, there can quickly be utterly dramatic consequences, including on human lives"

Guillaume Poupard
Director General of France's ANSSI cybersecurity agency

What risks are we talking about?

Cyber attackers have clearly identified this broad spectrum of threats. According to The Cyberthreat Handbook, a report published in 2019 par Thales and the cyber-intelligence company Verint, transport is the fourth largest sector targeted by hackers – after the defence, financial and energy sectors.

On a smaller scale, consider the example of this 14-year-old script kiddie who succeeded in taking control of the tram network in Lodz (Poland) in 2008 with a simple modified television remote control. The hack resulted in the derailment of four trains and 12 injuries. Or a larger-scale event in 2015 at the CeBIT exhibition in Hannover (Germany), at which a simulation reconstructed a typical infrastructure

(video surveillance data flow, control interfaces, time scheduling, etc.) to estimate the type and intensity of malicious acts. Over a 6-week period, researchers recorded a total of 2,745,267 attacks, 10% of which succeeded in taking partial control of the system.

So, what are hackers' methods of choice? The distributed denial of service (DDoS) attack remains a classic: "*Sometimes it's easier to block communication than to break into a system,*" comments Franck Bourguet. Another frequent attack vector is ransomware, which spreads as a result of human weakness (phishing and booby-trapped attachments); although easy to implement, the damage it causes can be significant. German rail company Deutsche Bahn fell victim to the notorious Wannacry in May 2017. In this case, ransomware infected 450 computers, affecting passenger information systems, ticket machines and video surveillance networks. Another example came in 2016, when the transport system in San Francisco (USA) was hit by ransomware, locking up its ticket machines for 48 hours. This forced the SF Muni company to deactivate its barriers and open up the transportation system, resulting in heavy financial losses.

Rail cybersecurity: multi-level tiered responses

It's easy to understand the importance of legacy systems in the rail industry. This older infrastructure (IT, equipment, etc.), dating back to a time when digital technology was either in its infancy or non-existent, may still be in use today. And in an era of intelligent networks, the belief that such equipment – designed for non-connected environments – is somehow protected is now an obsolete concept.

Franck Bourget believes that some proprietary protocols have not been designed to provide security for the data they carry. And corrections are impossible to make without a retrofit and significant investment. However, **cybersecurity solutions do exist**, adding a layer of firewall protection, with an encryption or filtering ability along with protocol analyses to confirm that transfers are legitimate.

Another area for attention: not only networks but also workstations and various other devices need to be protected if they are to be preserved from local attacks or malicious code and malware. In an industrial environment, this refers to control stations, sensors, actuators and other autonomous devices. So, if the network is corrupted, solutions exist to block the attack, which would also target this industrial equipment.

Data protection is also an area where work is required: as the French transport operator, RATP, opens its artificial intelligence laboratory in Châtelet-Les-Halles (Paris, France), we should consider the confidentiality issues relating to videos recorded on trains or at stations, as well as the use of the Internet and the Cloud to circulate the data that drives the algorithms. These are issues for which encryption solutions are able to offer tailored responses.

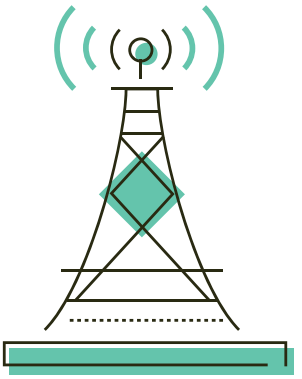
Mission-critical systems, sizing of infrastructure, convergence of IT and OT networks, the rise in artificial intelligence… for these reasons, rail operators urgently need to incorporate the concept of cyber-resilience into their philosophies. And they also need to keep in mind three basic principles: adopt a risk management policy, identify your sensitive assets and segment your network. **After all, the question is no longer how to guard against an attack... but what to do when one happens.** •

CRITICAL COMMUNICATION NETWORKS

April 7, 2020

TETRA / PMR

radio communication in the era of cyber threats



Developed in Europe in the 1990s, Terrestrial Trunked Radio (TETRA) is a system for managing digital mobile communications for emergency services. The system serves as a standard for building critical Professional Mobile Radio (PMR) networks. But as technology evolves and new applications arise—such as the mass migration to IP protocols—these networks must contend with escalating cyber threats.

By

PMR: critical communication networks

The PMR networks that we're referring to here have a very simple definition: they are the networks that must keep going when everything else is going wrong. Their primary users are emergency services, such as firefighters, ambulances, hospitals, the police and airports. These services must be able to communicate, either internally or with each other, as part of a joint operation led by a prefecture or government task force.

These types of networks are also found in sensitive industrial infrastructures, such as refineries. "*The common denominator is the major issue of public security,*" explains Dominique Allietta, Stormshield Project Manager. "*It may have something to do with an emergency, such as a bus crash, or with the ability to communicate in places where public infrastructure doesn't even exist, such as an offshore platform,*" he adds.

As such, PMR networks are used in any situation that carries a risk for human safety—from the transportation sector (metros, trains, etc.) to entertainment venues (amusement parks, stadiums, etc.). **Service continuity** is therefore critical for these networks. For example, the PMR system used by the Belgian police force, which is run by an entity known as Astrid, found itself completely overwhelmed during the Brussels terror attacks in March 2016. At the time, the size of the infrastructure wasn't designed to absorb the spike in activity caused by this exceptional situation. In order to conduct rescue operations, they were forced to communicate via the Whatsapp application.

Another feature that sets these networks apart is that **confidentiality of communications** is more critical

for them than for other networks. The information exchanged via these networks is sometimes subject to the kind of clearance levels seen in the defence industry, meaning that more stringent operational requirements are needed. "*The challenges therefore have as much to do with stability of communication as they do with maintaining the integrity of the information transmitted*," notes Dominique Allietta.

Novel applications that increase cyber risks

Little by little, **PMR networks are migrating to more modern and efficient architectures that rely on the IP protocol**. This trend exposes next-generation PMR networks to 'classic' cyber risks (data manipulation, breaches, leaks, etc.). It is therefore essential to strengthen authentication and encryption.

At the same time, several other factors have further eroded their defences over the last few years:

- **Application data:** In addition to voice and low bit-rate data, such as SMSs or geolocation data, PMR users need to exchange photos and videos or use applications. This allows for more effective organisation when managing a crisis.

- **The development of hybrid solutions:** In order to meet these emerging needs, current solutions have incorporated PMR networks into high-speed communication solutions on commercial networks (i.e. 4G, and soon 5G).

- **Interoperability:** "*We need to ensure that all of these actors can securely communicate with each other, including OESs and municipal police forces, for example. As the Olympics approach, this aspect is not only crucial, but must also contend with the extraordinary scale of the event and the thousands of professionals who will be involved in security*," explains Eric Davalo, Head of Strategic Development at Airbus Secure Land Communications, in an article in a French magazine. At the 2008 Olympics, "*80,000 first responders were using the PMR network at the time*".

How can we protect PMR networks in this context?

As it turns out, then, protecting PMR networks is no simple matter. In order to reach a PMR network from a simple IT network, you need more advanced resources than what traditional pirates use. As a result, there is a higher risk of sophisticated attacks. It is possible, for example, to intercept and alter data travelling via the PMR network, and thereby provide false information.

As such, organisations or businesses that use PMR networks may be classified as Operators of Essential Services (OESs) in the EU, requiring them to use certified or qualified security products.

While PMR services on 4G networks are still being standardised, 5G is practically there, ready to become the standard for commercial applications. To stay in the game, then, every actor (operators and customers alike) will need to be on the same page when it comes to the future of these infrastructures—as well as the technological advancements that could increase the capacity of these networks. For example, at higher speeds, there is likely to be a greater amount of critical information flowing through these systems, making it even more critical than it is today. **'Anticipate' and 'secure' will be the watchwords for ensuring these new technologies do not introduce any new weaknesses.** •

SMART BUILDINGS

Smart Buildings in the age of cybersecurity

September 29, 2020

Current and future smart buildings offer the promise of user comfort and energy efficiency, all managed by increasingly interconnected systems. Smart networks and other applications central to this technology have proliferated rapidly in recent years, and continually exchange a variety of different data—sometimes to the complete detriment of security. As such, safeguarding a smart building against cyberattacks (whether they involve IT or OT networks) represents a sizeable challenge—but not an insurmountable one.

By

Julien Paffumi

For a while, the first smart buildings (connected tertiary buildings designed for professional or residential use) were limited to collecting information from a single building system (also known as a 'work package'), such as lighting, heating or air conditioning—a process referred to as Centralized Technical Management (CTM). By connecting systems and networks together, Building Management Systems (BMSs) provided a layer of automation and monitoring to CTM. Building management became smart and integrated for all systems, including lighting, HVAC (heating, ventilation and air condition), fire protection systems (smoke detectors), elevators, parking sensors and surveillance cameras, to name just a few examples. All of this data is used to monitor the facilities, produce operating statistics, and initiate preventive and predictive maintenance operations.

Smart buildings under the crosshairs

However, this additional layer of automation and monitoring comes with non-negligible cyber risks. Since data is vital for smart buildings, its integrity must be maintained. And since the volume of data is exponential, and may come from a variety of different suppliers, maintaining security is a complicated

task. The protocols and operating systems may vary, and not all suppliers have the same level of maturity when it comes to tackling IT and OT cybersecurity risks.

In 2014, the American company Target suffered a cyberattack that provided an early textbook case: in order to steal payment card info from millions of customers, the hackers broke in directly through the network of one of the company's subcontractors, which was in charge of the air conditioning systems. And according to a study by Kaspersky, nearly four in ten computers used to control smart building automation systems were hit with cyberattacks in the first half of 2019.

Understanding the different types of attacks

The interconnections between these systems and the building network, as well as the abundance of stakeholders involved, make these buildings more vulnerable to cyber risks. Put simply, **if a smart system is remotely accessible for the building manager or one of its subcontractors, it is potentially accessible for a cyber-criminal as well.** Using BMSs, multiple types of cyberattacks can be launched against smart buildings. Attackers may hack into the networks and servers, modify data, or shut down the building with ransomware, undermining the building's operation and even leading to physical or material damage if they gain control of the elevators, fire alarms, door locks or ventilation systems. These scenarios offer a hair-raising perspective for shopping centres and hospitals.

And the development of smart devices and the IoT, which are particularly vulnerable to security issues, are making buildings more susceptible to attacks that are closer to home, via open wireless networks (such as Wi-Fi or Bluetooth). A few years ago, two researchers successfully hacked into smart light bulbs to demonstrate the vulnerability of the IoT and the security flaws of wireless networks. They managed to remotely take control and upload malware throughout a smart building using a malicious update.

"If digital security is not an integral part of upstream data production, then you're just making the hackers' job easier!"

Denis Boudy
Sales Manager, Digital Solutions at ScredIn

Note as well that cyberattacks may also occur from inside the building by inserting a simple USB stick into a piece of equipment.

Whether they involve IT or OT systems, attacks may lead to material or bodily harm, with dramatic consequences. Accordingly, these cybersecurity problems are even more of an issue for highly sensitive sectors such as healthcare, since utility systems (air conditioning, air-level systems, fire security) are central to any hospital building. The prospect of a cyberattack disrupting the air treatment system in an operating theatre constitutes a critical health risk.

The importance of anticipating risks

"*We are now aware of the cyber risks affecting CTM-BMSs, whether they involve OT, IT or the IoT, but the lack of forward planning speaks volumes: we are working from a backward-looking mindset. We are preparing for the future by examining risks linked to attacks that have already taken place. Cyber risk should be addressed right from the design and construction phase of a smart building,*" notes Denis Boudy, Sales Manager, Digital Solutions at ScredIn.

In smart building projects, the "operation and maintenance" phase is preceded by "design and construc-

tion". During this initial phase, all architectural, engineering and construction data will be aggregated into a digital mock-up, a process known as Building Information Modelling (BIM). This data is then organised, cleaned up and optimised to develop a digital twin. Once additional data has been added (from the IoT, for example), this twin will be used throughout the operation and maintenance phase, providing real-time graphical representations of the smart building's management system. The initial design phase is important, then, since sensitive 3D-modelling data will be processed throughout the building's lifetime.

The risks will therefore need to be anticipated. "*If digital security is not an integral part of upstream data production, then you're just making the hackers' job easier*, says Denis Boudy. *During building renovation, it is common for some companies to use foreign contractors to put together 3D models, for budgetary reasons. There is no guarantee when it comes to the integrity of the data; it's all open to everyone. You don't need to jump straight to a cyberattack; even a physical attack on the building is conceivable. Anyone who has had access the digital model may have access to sensitive information and know exactly what to do to shut off the lighting, or know exactly where the surveillance cameras are. Recently, a number of French government agencies digitised their buildings and properties using 3D scanning, and didn't ask for any information on how the digital models were produced. We know that many companies outsource this type of process, and they've sent all of the required data abroad, unencrypted. This is a genuine risk to the safety, confidentiality and integrity of the data*". "*From a cybersecurity perspective, by having access to this data, a hacker might more easily find out how to turn up the heat to the maximum setting, cut off the air intake, or prevent a fire alarm from going off... The tragic consequences are easy to imagine*," says Raphaël Granger, Account Manager Stormshield.

The design and construction phase may last anywhere from two to four years. During this period, more than 400 people will be producing data, and more than 1,000 will have access to it, says Denis Boudy. The likelihood of a security breach is therefore considerable. "*Having a BIM manager or a data manager determine the criticality of the data is crucial during this stage: it's their job to determine the permission levels needed (to access a camera, for example), and to manage communication flows and encryption. If you're not careful to ensure access security for all of the data aggregated throughout the BIM process, then it may be used to actively monitor the system to prepare for an attack.*"

Beware of the cloud and 5G

Smart buildings are increasingly spread out. Connectivity is essential for transmitting information—as long as it's secure and reliable. If a fire breaks out in a smart building, the right information must be sent to the right person as quickly as possible.

This requires information relays, which often take the form of decentralised mini-computing centres. This process is central to edge computing, and soon enough 5G. While edge computing helps cope with the considerable amount of data that needs to be stored, analysed and processed, a decentralized data system carries just as many cyber risks. "*We need to find a happy medium between simplifying our lives and taking risks*, notes Mathieu Demont, Product & Solution Security Expert Siemens Smart Infrastructure. *Providers of cloud storage solutions offer unlimited data processing capacity to businesses, but what happens behind the scenes is murky. The connections aren't visible, and we don't always know who really stores the data, or on what hardware. Is our data shut away in containers, themselves integrated into private servers? Or is it pooled together with other customers' data? All of this remains unclear, and while we're sitting here thinking that our data is properly protect, all of it might at some point get mixed with other data that contains viruses*". With 5G, the flow of information will increase, which makes it essential to address processing capacities.

"5G will offer greater bandwidth capacity, but of course that's just as true for cyber-attackers as it is for companies. That means our systems need to be more robust, and that's why we account for cybersecurity as early as the design phase," adds Mathieu Demont.

A safe and (cyber)secure smart building

In order to safeguard data processing and ensure the reliability of smart building data, it is recommended to set up a governance framework that requires strict authentication for users. It also strongly advised to strengthen information system security by segmenting the networks and installing a firewall. Lastly, it is essential to safeguard production using robust end-to-end data encryption.

All of these measures need to be supported with consistent, day-to-day organisation. *"We often say that technology accounts for 30% of security, and the remaining 70% is essentially organisational,* says Mathieu Demont. *In our heads we have this image of a fire extinguisher that's blocked by a door in order to 'air out' the hallways—a major error if the doors ever need to be closed... That may seem anecdotal, but poor organisation can impair the reliability of technical measures and undermine the overall security of the system. That's why we do a fair amount of training and awareness-raising at Siemens Smart Infrastructure, particularly when it comes to cybersecurity".*

These measures also apply to smart industry, and to smart cities more widely, which entail similar issues to smart buildings, only on a broader scale. There are more players involved, which raises issues in terms of governance, confidentiality and data security—particularly since new sensor technologies (LoRa, SigFox, 5G) are accelerating the development of future cities. This transition to smart cities cannot occur without some measure of cybersecurity. •

"5G will offer greater bandwidth capacity, but of course that's just as true for cyber-attackers as it is for companies"

Mathieu Demont

Product & Solution Security Expert Siemens Smart Infrastructure

#3

THE CYBER QUESTION: **FOOD FOR THOUGHT**

A CYBER **CULTURE**

Awareness training: how can we promote an effective cybersecurity culture?

February 10, 2020

"Please update your password." 49% of employees, upon receiving this message, are happy just to tweak their old password, according to an HYPR study in 2019. And thus "p@$$W0rd2019" becomes "p@$$W0rd2020", delivering no security improvement whatever for the information system. So are we to conclude that prevention efforts are struggling to bear fruit?

By

Corporate cybersecurity is everyone's business; but in reality, it's someone else's problem. Beyond the technical tools involved, the staff awareness and education aspect is vitally important. And when it comes to getting staff on board, **charters, rules of good conduct and other digital hygiene guides are doomed to fail** if they are not conceived as part of a bigger, more engaging process. So what exactly is the miracle recipe for good cyberculture?

Awareness training is not yet a universal 'given'

In the 2019 Stormshield / L'Usine Digitale study, initiatives to promote awareness of best practices top the list of cited measures for addressing cybersecurity challenges, but their implementation remains patchy: **28% of respondents do not invest in staff awareness training**, or at least, not regularly.

Franck Gicquel, Partnerships Manager Cybermalveillance.gouv.fr in France, confirms this unevenness: "*The reality for a large group and for a micro-business is inevitably very different, with the latter relying on a service provider for its IT management: the micro-business is not always in a position to deliver awareness messages*".

On the other hand, a positive result from the study is that security aspects seem to be increasingly integrated into training sessions on new digital transformation tools (48%, a 9-point rise compared to the 2018's barometer).

The role of top management: setting examples or issuing sanctions?

The role of the company's governing bodies is key because, as well as setting an example, they alone can **require that awareness training be prioritised** and allocate the necessary resources for this purpose.

However, top management is not always sufficiently mature to address these issues. This is why Gérard Leymarie, CISO of the Elior group, sees an urgent need for a change of approach by CIOs: "*We need to get out of our "old school" ways of thinking and comfort zones, and become proactive in our efforts to convince the executive committee*". Franck Gicquel believes that converting the management team into ambassadors for cybersecurity issues means "*delivering the same*

message via a variety of sources, increasing the chances it will be understood and adopted".

There is also an expectation that top management will adopt a policy on possible sanctions relating to poor digital hygiene. With the GDPR, we are starting to see early hints of third-party legal sanctions. But with the exception of spectacular cases of poor managerial practice, experts agree there is a need to **avoid overly directive approaches, as these are likely to provoke anxiety and have little effect** in the long term. "*If we maintain a philosophy based on prohibition and punishment, we are perpetuating a view of the employee as a weak link in the security chain. And yet the whole point of awareness training is to make them the strong link!*," Franck Gicquel says.

Theory without practice equals a wasted training budget

The desired result will certainly not be achieved by annual PowerPoint presentations or *cyberwashing*. The challenge is to positively incorporate best cybersecurity practices into everyday life. Here are some tips for how this could be achieved.

Breaking out of the box

"*Repeat without being boring*," is the goal according to Franck Gicquel. To do this, he advises that awareness messages should be delivered not only by the IT department, but also by other company functions (business units, HR and other departments). For example, the Stormshield / L'Usine Digitale 2019 barometer shows that an average of three different main stakeholders are involved in implementing a digital project within the company. So it would seem sensible to share out the work of raising awareness. "*This shows that it's everyone's business, and it makes it possible to vary the tone, approaches and examples used to establish a genuine cyber culture.*"

Creating contacts

And to get as close to employees as possible, why not identify points of contact within operational teams? Whether on a departmental or team basis, these "security" contacts would occupy the roles of facilitators (and also of experts), ensuring that cyber messages and directives are known and understood by all employees.

Adapting to the target audience

To stimulate interest in this issue within a large company, an SME or indeed a school, it is vital to make use of specific business examples and make connections between the issues and personal experience.

Lightening the tone

The technique known as "*croissantage*" is a good example of this philosophy, in which an observant, non-malicious colleague uses an unattended workstation to send a group email notifying everyone that its owner will be providing breakfast the next day. It's a quick, simple way of **introducing the basic concepts of digital hygiene** in a company.

Measuring the effectiveness of awareness training

Lastly, it's important to check the awareness message actually received by employees. In the case of Elior and its *Hacking Diner* operation, the indicators in question are viewing statistics for the dedicated site, the security information feedback rate (a fourfold increase in under a year), and the success rate of attacks against the company.

Could this (at last) prove to be a template for raising awareness effectively? A strategy initiated by an IS department using effective communication, supported at a wider level by all company departments, with illustrations from business practice or real-life issues... What's more, these awareness initiatives seem to add up to a genuine training process, in which all staff members have **a role to play in improving corporate cybersecurity**. •

Cybersecurity: should staff be restricted for their own good?

April 20, 2020

Teleworking is one of the most visible signs of the digital transformations providing new opportunities within companies and responses to the health crisis we are currently experiencing. However, depending on how they are used and the way staff behave, such new applications can undermine corporate security. Should the access and functions of certain workstations be restricted to guarantee overall security? Any attempted return to the days when access and installation rights were required for a workstation may meet with some resistance. And leave IT services between a rock and a hard place.

By

Julien Paffumi

With digital transformation, the virtualisation of services and worker mobility, the company's external borders are changing and the barriers between work and private life are now increasingly porous. Whether it's someone accessing the internal network from an unsecure Wi-Fi connection or copy-pasting a critical company document via a personal flash drive, devices are today being combined and interconnected. We should begin by pointing out that one thing is clear: this situation takes no account of hierarchy. The naive intern, the sales representative in a hurry or the CEO who believes himself infallible are all significant sources of cyber-risks. Especially as many of them have administrator rights for their workstations. We must therefore ask ourselves the following question: **should we return to yesterday's methods and restrict everyone for their own security?**

This question is all the more relevant in the context of the current health crisis as urgency and cybersecurity have never been good bedfellows. To enable companies to continue their activities, digital services and especially teleworking have now been shifted to employees' homes. But they haven't made

the trip alone... the company's vulnerabilities are also being exported to the homes of its employees. "*With Covid-19, those companies surviving the effects of the economic crisis could find themselves devastated by cyberattacks,*" warns the CISO of a major company in the aeronautical sector, earnestly. These words succinctly express the fears of the whole profession at a time when the worst health crisis for a century is sweeping the world.

Let's be bold here, and point out the parallels between this unusual health crisis and the restriction of employees' IT rights. The government's decision to impose a lockdown of the population is a restrictive measure but one based on the need to guarantee collective safety and security. Could this also be a solution where cybersecurity is concerned?

Autonomy and efficiency, a restrictive environment

One possible solution is making employees liable and accountable for their actions, which in certain cases may lead to disciplinary measures. But is this a desirable solution? Another option would be to return to the days when access and installation rights had to be requested for each workstation. Is this viable in the context of today's companies, in which numerous staff have direct administrator rights for their workstation? "*To understand how we got to this point in certain companies, two key challenges must be taken into account. Firstly, the wish for autonomy from some employees, who possess advanced IT skills and would like to be able to install specific applications, write scripts or prepare models without needing to contact the IT department to obtain some authorisation or other*, explains Franck Nielacny, Chief Information Officer Stormshield. *We must also take account of a second factor, related to the availability and responsiveness of the IT teams. In some cases, an IT Manager can be extremely busy and must manage incoming requests based on priority. A simple solution to this is sometimes to grant admin rights*".

"With Covid-19, those companies surviving the effects of the economic crisis could find themselves devastated by cyberattacks"

Despite this, it is recommended that a few simple rules be respected with regard to filtering and access control. "*My recommendation is a twofold one: those job categories which are not overwhelmingly technical in nature do not require administrator' rights. For more technical users, the idea would be to have two accounts: a standard one for use on a day-to-day basis and an admin account, the latter possessing the most restrictive functions possible and strictly governed when in use by means of an IT charter,*" adds Franck Nielacny.

Numbers surely speak louder than words. According to the Beyond Trust's annual Microsoft Vulnerability Report for 2020, 77% of critical Microsoft vulnerabilities could be eliminated by implementing the principles of least privilege and removal of admin rights. And the Undernews site dug even deeper into the report's conclusions, claiming that **100% of critical Internet Explorer and Microsoft Edge vulnerabilities could have been eliminated by deleting admin rights...**

Restrict, block, hold accountable: a three-stage cyber solution

In a normal context, it's difficult to envisage adopting a coercive approach involving extensive restrictions on staff. Indeed, who knows how staff would react to measures they consider overly restrictive or as violating their fundamental rights? "*Only a critical situation in which the company was in real danger*

could justify the use of tough restrictive measures for all staff, continues Franck Nielacny. *These measures could only be temporary*". The current context, characterised by the dual constraints of autonomy and efficiency, appears to meet these criteria for the moment: the lockdown is being accepted because the situation is exceptional and temporary.

Another example of such restrictions is the decision as to whether or not to authorise access to personal e-mail accounts in professional contexts. Once again, the midway solution would involve authorising access but prohibiting the opening of attachments, making people fully aware of the risks of infection through this channel. Because we should never forget that the risk of users trying to get round any restrictions and the resulting risks of shadow IT are never far away! "*It's important to be realistic*, stresses Franck Nielacny. *We today find ourselves in a working environment in which there's a fine line between work and private life. Shadow IT is a reality for all companies and even more so with Covid-19 and the lockdown. The challenge lies in ensuring a leakproof environment in relation to the company's IT system by limiting the exchange of data to and from third-party systems*". **It's therefore vital to improve awareness and responsibility from the outset.** We can't stress enough the need to instil an effective cybersecurity culture.

"The challenge lies in ensuring a leakproof environment in relation to the company's IT system by limiting the exchange of data to and from third-party systems"

Franck Nielacny
Chief Information Officer
Stormshield

Zero-trust, a future paradigm?

As we have seen, crisis situations, the changing external borders of the company and increasing staff mobility all make it necessary to rethink IT systems security. Against this backdrop, more and more people are now talking about the zero-trust approach. What does it entail? Adopting a genuine zero-trust approach to users, terminals or workstations and managing exchanges between the machine and the rest of its environment in as far as possible. "*Thanks to this model, the company can control who has access to what, how and when*," wrote Pierre-Yves Popihn, technical manager at NTT Security France in the French newspaper *Les Echos*.

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. •

Why do we **still** need a password?

April 27, 2020

Passwords can be a daily headache and can represent a major source of vulnerability for companies due to the human factor. So we often hear people saying that the time has come to do away with them. But how reliable are the proposed alternatives? Can we really do away with passwords?

By

Password theft is one of the main forms of illegal intrusion. The annual survey carried out by the American telecommunications operator Verizon recently highlighted the fact that 29% of malicious intrusions are down to stolen passwords and that in 80% of cases the cause was a weak password. Each year, countless rankings for the 'worst password' are published, guaranteed to put a smile on any IT manager's face… or to lead them to despair.

From the classic "123456" to the most mnemonically "incorrect" –not to mention the bold "p/q2-q4!a"–, passwords can be a thorny issue as the need for security often clashes with the realities of day-to-day use. The twofold requirement to remember a number-letter-capital combination of varying degrees of complexity and to replace this combination at regular intervals can often be a headache for users. And there's a great temptation to note down your passwords on a post-it note or even to use the same password for all applications (this is the case for 78% of employees according to an Harris Interactive study for CaptainCyber). This need for 'practicality' combines with the general lack of maturity of individuals and staff.

In this context, many people are now calling for "*an end to passwords*" and the advent of the passwordless age, while others see biometrics as a promising solution. Others consider two-factor authentication as an effective supplement to passwords. So what's the situation with these different alternatives? **Will we still need a password** in the weeks/months/years to come? As security and constraints go hand-

in-hand, do we need fewer passwords but better quality ones?

Biometrics: practical but not infallible

Biometric identification (scanning our fingerprints, facial contours or the patterns of our eyes) have quickly emerged as alternatives to traditional passwords. Opening your telephone using your fingerprint is faster and less tedious than entering a code comprised of several numbers. And it's certainly true that individual physical characteristics, those which by their very nature are unique and specific to each user, offer a useful means of generating signatures. After retina authentication, a concept so dear to Hollywood, the rest of the human body has now been brought into play. Amazon recently lodged a patent to analyse the traces of veins, lines and wrinkles on the skin for authentication purposes. For its part, the Japanese giant Hitachi has opted for a process which makes it possible to analyse blood vessels, as the network the veins in our bodies constitute unique structures.

These companies view these alternative biometric identification methods as being more reliable than fingerprints or than facial recognition, which also has its limits. A team of researchers at New York University recently developed a technique making it possible to generate 'universal' fingerprints, and therefore to fool the captors used on 70% of telephones. And when they're not being falsified, fingerprints can also be stolen (this was the case in 2015 during an attack against the American Federal reserve – FED) and end up being sold in marketplaces specialised in the resale of biometric data. In 2019, the fingerprints of more than 60,000 users were made available on GenesisStore, a marketplace on the darknet. As for facial recognition, the journalist Thomas Brewster from *Forbes* demonstrated it was possible to trick telephones using a 3D print of your face…What also obviously comes to mind is deepfake technology, which makes it possible to produce highly realistic videos and therefore to potentially fool sensors. So as you can see, there are plenty of experiments underway in the field of biometrics but the risk of identity theft remains.

Ultimately, a combination of two biometric factors, for example a fingerprint and the venous circuit or a fingerprint and facial analysis, could limit these risks. But this solution comes up against cost considerations. Sensors are expensive and it's difficult to imagine a widespread rollout of devices fitted with dual biometric sensors without these costing a fortune. In short, biometric processes are not sufficiently reliable when used alone.

FIDO2: the advantages and limitations of passwordless technology

In February 2020, a press release from Microsoft reopened the debate on the scrapping of passwords with the announcement that passwordless technology was to be included in their AzureAD environment. FIDO2 makes it possible to verify the user's identity based on a strong authentication key contained on a physical medium. The FIDO token can therefore be used as an additional authentication factor. The advantage of the FIDO2 technology is its low cost, making it accessible to both private individuals and companies.

Two-factor authentication: possibilities and limitations

According to Microsoft, two-factor authentication can also prevent 99% of attempted intrusions. Nevertheless, the FIDO key is first and foremost a physical medium, which doesn't eliminate all constraints. *Passwordless* but *not yet painless*. What do you do for example if it gets lost, stolen or forgotten? The telephone is often used as a short-term backup to receive a token sent by text message or e-mail. However, recent studies have revealed that attackers can get

around this second authentication factor, like for example the Cerberus malware.

This solution is therefore not infallible, especially if you don't have the FIDO key on you at all times, although it does enable you to increase your security level, particularly for critical networks or infrastructure.

A password vs. a pass phrase

As we have seen, recent developments provide some comfort for users but certainly do not offer the prospect of passwords disappearing any time soon, particularly in dual authentication scenarios. But what exactly makes for a good password? Standards concerning the right complexity level generally require a combination of upper-case letters, numbers and special characters, with the combination being changed regularly.

A recent paper from the NIST (National Institute of Standards and Technology, in the United States) has challenged some of these certainties however, followed by another paper, this time from the BSI, the Federal Office for Information Security in Germany. According to the researchers interviewed by the NIST, the great complexity of certain passwords is simply not viable for daily use, when users are required to type in a combination several times a day. They therefore recommend using a phrase, which is easier to remember and just as difficult to crack for any possible attackers, as there are so many possible combinations of words. This begs the following question: what should the limit be in terms of the number of words? The paper does not mention this. Concerning the BSI, the agency has reconsidered its recommendations concerning the need to regularly change passwords. One of the German researchers even stressed that: "*You can securely use the same password for years*". The German agency's position is simple: regular password changes would cause more harm than good as this would result in individuals using weaker passwords created based on a certain 'template', making them easier to crack by a cyber-attacker.

Fewer but better

If it proves impossible to use either biometrics or a FIDO2 key, it's always possible to follow a simple rule: choose fewer passwords but better quality ones. Based on the BSI's recommendations for example, it would be possible to select five complex passwords and to assign them to groups of websites ranked in advance according to their importance. A technique which has the benefit of being accessible to all.

As you have seen, we still need passwords, even in the case of strong authentication. There are plenty of possible combinations to help achieve optimal security however. One recommendation would be to always use:

- Something you know (like a password),
- Something you own (like a FIDO2 key),
- Something you are (a biometric element).

The challenge for the IT departments is to ensure that everyone finds the right compromise where security is concerned, the method best able to avoid intrusions while also making daily life manageable. Because as we have seen with the shadow IT phenomenon, the more constraints you add, the more the users will be tempted to try and get around them. •

How do you **combine ethics and cybersecurity?**

June 17, 2020

Extraordinary responses to extraordinary times: in early March, hacker groups such as Maze, DoppelPaymer, Ryuk, Pwnd-Locker and Ako announced a ceasefire during the Covid-19 health crisis. Despite this, on March 16, 2020, the US Department of Health and Human Services suffered a distributed denial-of-service (DDoS) attack. And on March 22, in France, while overcrowded hospital departments were being deluged with patients, the Assistance Publique-Hôpitaux de Paris in its turn fell victim to a violent cyberattack. These events raise the valid question of whether ethics are a consideration in hackers' actions

By

Answers to questions on hacker ethics are necessarily coloured by your own point of view, and by your own definition of what is – and isn't – ethical. Recently, two hacktivists offered their own partial definition of ethics. Citing individual data protection concerns as a motivation, French hacktivist Baptiste Robert (alias Elliot Alderson) undertook an in-depth analysis of personal contact tracking applications. Having detected and exposed flaws in India's Aarogya Setu application, he concentrated on the French version, StopCovid, and the Pakistani version, COVID-19 Gov PK. Last year, in a different genre, Phineas Fisher launched his own bug bounty as a reward to anyone launching politically motivated hacks leading to the disclosure of documents of public interest... while in related news, a Canadian organisation assisting young homeless people was hit by ransomware in early January 2020. In a complex, multi-faceted landscape, is there any room for ethics?

Ethics: an eminently subjective notion

First, a quick philosophical introduction. Jean-Jacques Nillès, founder of the French Socrates con-

sultancy specialising in ethics, believes the question is not so simple: "*Although the distinction between legitimate and legal is widely accepted, not everyone accepts it at face value. The relationship between law and ethics is a complex one, and there is a tendency to simplify it. Our laws are founded on ethics and ambitions. Some atypical cases reveal a dissonance between legal and ethical considerations; but once again, this is not entirely accurate... instead, these are ultra-rare cases in which a principle of law sees itself telescoped into a rule. The law does not provide clear-cut answers. What it does is to spell out a certain number of possibilities. And it is within this multiplicity of options that ethics finds its place*". In short, the law defines a number of possibilities, and the role of ethics is to make a choice between these. For Alice Louis, the director of a project to establish the "Cyber-Ethics Fund for Digital Sovereignty", "*ethics is the thought of principles and values. In this respect, morals and/or morality tell us which actions are right, good or bad. In other words, and as stated by the likes of sociologist Max Weber: ethics is an act of empowerment which cannot be reduced to the mere expression of an opinion*". This opinion is shared by Philippe Sanchez, a consultant and trainer at the Socrates consultancy: "*Ethics is a subjective notion that can vary from one individual to another. It will always make its nest where a gaping hole is left by the law. Without rules, any of us could justify our actions by citing a liberal interpretation of ethics...*"

"Ethics is a subjective concept that can vary from one individual to another. It will always make its nest where a gaping hole is left by the law"

Philippe Sanchez
Consultant and Trainer at the Socrates consultancy

Many among us would acknowledge an ethical dimension to the work of hackers operating in Tunisia during the Arab Spring movement… but it would be more problematic to accept the legitimacy of a group in the pay of the Kremlin, undermining the principle of non-interference in international law by infiltrating US Democrats during a presidential election. So is one man's cybercriminal another man's hacktivist? Maybe. Especially if we take the opposing view to that of the philosopher Immanuel Kant by viewing **ethics as a relative concept shaped by concepts specific to a given culture...**

The codes of the hacker community

Hacker ethics are steeped in the cyberpunk subculture, a core value of which is protest. Characters in these novels are anti-heroes, often pawns manipulated within an imbroglio of secret societies, government departments and crime syndicates, all of them run to varying degrees by senior executives of multinationals which have become more powerful than states themselves, and whose leaders are often devoid of any morality. These anti-heroes are then presented as small pieces of grit in the machinery. A later development has been the addition of a search for knowledge and understanding of computer systems – and a desire to preserve the Internet as a place of absolute freedom from rules imposed by governments and corporations. For that reason, it is legitimate to infiltrate systems owned by various government, financial and military institutions in order to dissect their architecture. In 1984, the journalist Steven Levy, the author of *Hackers: Heroes of the Computer Revolution*, summed up the hacker ethic as follows: don't destroy the computer networks you infiltrate, don't make a profit, and share information.

So does this hacker community have its own codes? Black Hat, White Hat, Grey Hat and even Blue Hat: there is a wide and diverse range of hacker profiles, each of which has its own codes. These codes differ according to hacker loyalties/allegiances, which may inspire varying degrees of confidence from a

third-party standpoint: "*A 'grey hat' like Baptiste Robert will publicly divulge the existence of a flaw that endangers users, while a 'white hat' will give information to the company they are working for. The white hat will never 'cross the line' legally, even though others may follow different paths,*" explains French hacktivism specialist Fabrice Epelboin.

At what point does a hacker decide which path to follow? And can their decisions be influenced over the course of their personal journey? In other words, **is ethics a question of maturity?** This series of questions leads us to consider the case of script kiddies, amateurish hackers driven by results rather than knowledge, and inspired by complex motivations. "*The fundamental difference with script kiddies is their ignorance of the mechanisms involved. They will use ready-made solutions instead of developing their own code, which can sometimes cause them to underestimate the damage they're doing,*" explains Davide Pala, Stormshield Pre-Sales Engineer in Italy. However, this doesn't stop them from sometimes uniting under the banner of shared values in the name of ethical principles which – once again – are theirs and theirs alone. "*For example, that's exactly what you find within Anonymous*, Fabrice Epelboin explains. *Among their number are many script kiddies doing nothing more than pushing buttons. However, when viewed as a whole, the fact remains that they can represent a significant strike force. This crowd effect can also be employed for the ends of political machinations and digital crime, giving rise to bug bounties or ransomware, depending on the value systems of the specific individuals*".

At the same time, it is clear that IT vulnerabilities have now spawned an economy in its own right. So, **does ethics have a price?** Because they can be associated with significant financial rewards in real or 'dark' markets, issues around vulnerability have for many years been attracting mafia organisations, large groups of shadowy hackers and also major state-sponsored groups. Each of these has its own objectives, and more importantly, its own abilities in terms of resources; initially financial, and later, human. The colossal financial muscle that can be flexed in this way – along with the promises of astronomical 'easy' profits – can seduce some hackers and lead them to compromise some or all of their personal ethics. Especially considering that on the other side of the mirror, the bug bounties on offer and the salaries offered by institutions and companies hardly compare.

But to what extent can you trust a hacker? And what is a hacker's word really worth? There is no clear-cut answer to these two questions: it always depends on exactly who you're dealing with. Although some vestiges of the early hacker movement still remain, the landscape has become more diverse and the codes that govern the community no longer act as a clear rallying point. So, in an attempt to make this complex landscape easier to understand, the term "ethical hacker" has emerged. But it hasn't been all that successful...

The ethical hacker: an empty phrase?

The need to combine these two terms suggests that they were somehow diametrically opposed at the start. Does that mean that white hats are the good guys, and black hats are the bad guys? "*That's completely wrong*, claims Fabrice Epelboin. *Black hat, white hat, ethical hacker, cybersecurity engineer; these are just marketing labels that tell you very little, except that the media loves to simplify things*". He believes that the only thing separating a grey hat from a white hat is the legal framework in which the latter operates, in the interests of maintaining cybersecurity. "*In reality, the ethical hacker could be working for arms dealers, or for a company like Monsanto, and they would still be considered as 'ethical'. But that has nothing to do with ethics, merely law. Obviously, a hacker can behave in a way that is both ethical and illegal; for example, when dealing with oppressive regimes...*"

“Black hat, white hat, ethical hacker, cybersecurity engineer; these are just marketing labels that tell you very little, except that the media loves to simplify things”

Fabrice Epelboin

French specialist in hacktivism

Fabrice Epelboin believes that binary distinctions between ethical and non-ethical hacking can never reflect reality. In his opinion, **appearances can be deceptive**. “*Hacker culture doesn’t really lend itself to a 9-to-5 lifestyle... One possible permutation is that you could be a white hat during the day to earn a living, but grey hat at night as you fight for your principles. To be honest, I don’t know any hackers who’ve never crossed the red line, because it’s such a small step from legal to illegal, and it’s so easy to be anonymous. In addition, protecting users often means forcing companies to adopt secure practices, which can involve methods frowned upon by law.*”

Cyber-ethics: in search of a framework

Some see them as universal, while for others they're relative... but if we are to agree on the question of ethics, we need legal boundaries. Indeed, many platforms such as Yogosha, YesWeHack and HackerOne devote themselves exclusively to hunting down digital flaws through bug bounty programmes, while other companies such as Synacktiv specialise in penetration tests.

Such ethical hacking is then practised in very tightly-controlled environments. In this scenario, hackers adhere to the compliance requirements imposed by companies and governments, and sign up to certain codes specific to the environment: any detected flaws must be reported; the privacy of the organisation, its employees and users, and of third parties, must be maintained; and any breach that is created or exploited must be sealed. These principles, set out by the Forum of Incident Response and Security Teams, were re-stated in a recent article by the Kaspersky French team. Hackers who comply with these requirements can even obtain the title of “Certified Ethical Hacker”, awarded by the EC-Council body in the US.

Alice Louis concludes: “*There are hackers who seek to operate within a legal framework, and thus align themselves with an ethical approach in the sense of normative ethics in general, and consequentialism in particular. This approach to ethics explains that the morality of an action must be assessed in terms of the consequences of that action. From this perspective, hackers become clear allies for organisations. Obviously, a certain number of precautions need to be taken, with checks made in advance, e.g. with trusted third parties, and ultimately, a rigorous set of contractual terms set to govern the work they do*”. An essential foundation for a relationship built on trust... •

CYBER
PROTECTIONS

Efficiency and security: the benefits of information system segmentation

October 19, 2020

As part of the digital transformation process, the increasing openness towards the outside world and the interconnection of different information systems make companies more vulnerable to cyberattacks. However, there are effective ways of protecting oneself, such as the segmentation of the information system. A technique that makes it possible to contain threats by preventing them from spreading to other areas. This also optimises the performance of the equipment. But how can the network be segmented? And in the age of Industry 4.0, when we consider operational requirements, business continuity and obsolete systems, is it really that simple in the industrial world?

By

Network efficiency and security

Network segmentation is initially very important for purely functional reasons: to guarantee the availability and efficiency of equipment. When too many items of equipment are connected to the same network, with innumerable communication flows and private connections, a sort of 'background noise' is generated. In an industrial environment, for example, the PLC will not be able to ignore it: even if it does not process all requests, it analyses them systematically. This runs counter to the requirement for operational efficiency in this area of activity. "*This background noise diverts the PLC from its primary function, a situation that can quickly lead it to reach saturation and therefore to malfunction. A factory cannot continually expand its network architecture without segmenting it,*" explains Vincent Riondet, Head of Cybersecurity Projects and Services teams Schneider Electric France.

But **it is regarding cybersecurity that segmentation brings its greatest benefits**. Segmenting areas according to each person's specific usage requirements allows us to provide employees with only the

resources and access they need. The data related to organisational, operational and automatic systems is thus contained in zones which may themselves contain sub-zones. Segmented in this way, they are less likely to leak or be compromised. "*In order to achieve this division into homogeneous networks, it is necessary to carry out a precise inventory of your equipment and its types, and to know how the items of equipment are physically connected to each other. All this information will allow us to access a communication matrix and launch a risk analysis: this is essential to know what to prioritise and how to segment everything,*" adds Vincent Riondet.

IT/OT: multiple levels of segmentation

In the beginning, there was IT. Within companies' information systems, initial levels of segmentation are needed to separate certain groups of services or computers, according to their exposure to cyber threats - mainly related to Internet connections. In the largest companies, there will therefore be a tendency to plan internal segmentation to isolate the departments exposed to the Internet, staff computers, internal services, but also field-based staff and visitors.

At the same time, under the influence of the digital transformation of companies and the advent of Industry 4.0, industrial networks have evolved over time under the dogma of IT/OT convergence. "*Initially the industrial network was not connected to the IT system*, explains Tarik Zeroual, Stormshield Global Account Manager. *Today though, for governance and business reasons there is a real willingness on the part of companies to automatically collect information from the field. Operational and maintenance data is no longer enough. Industrial companies now want to know how often their equipment is used, as well as having information related to the breakdowns and downtime of this equipment*". **Establishing a barrier between the worlds of IT and OT is therefore a fundamental security measure**, in order to guarantee the cyber-protection of industrial networks.

This convergence represents a major challenge for most manufacturers, says Vincent Riondet. "*The vast majority of our industrial networks are very poorly structured. They were installed and set up by automation specialists, so this is not their core business: they did not take into account the problems of IP addressing, broadcasting and flow management, for example. Their only objective was to make the items of equipment communicate with each other*". A challenge that is all the greater since the threat does not necessarily come from very far away. Factory employees and outside personnel still often use USB sticks, whether to collect data from the supervision workstation or to update PLCs. However, it is still common for them to become infected. A simple connection could corrupt an entire information system. "*This segmentation makes it possible to protect against all internal and external threats, whether they come from the Internet or from external parties,*" says Vincent Nicaise, Industrial Partnership and Ecosystem Manager Stormshield.

Segmentation: more than just a recommendation?

Network segmentation is therefore the most effective measure to contain cyber threats and prevent malware from spreading within an IT or operational infrastructure.

It is also one of the key recommendations of the IEC 62443 standard. This industrial cybersecurity standard has developed the concept of division into "zones" and "conduits" according to the criticality levels of the dedicated equipment. A defence-in-depth logic which, thanks to the integration of firewalls, strictly and immutably determines the authorised and unauthorised communication flows between predetermined segments or blocks. Divided into blocks, the network as a whole becomes more difficult to attack by a cyber-criminal.

Recommended by the texts of the IEC 62443 standard, **segmentation provides an essential bulwark**

to limit intrusions and deal with cyberattacks. Like wearing a seatbelt in the car, this technique is a must – regardless of the type of network involved.

Physical or virtual separation

There are two segmentation methods: physical segmentation and virtual segmentation. Physical segmentation consists of creating parallel networks so that they are completely separate. A switch will be installed on each category of machine – PLC, PC, printer, etc. Virtual segmentation, on the other hand, offers the same hardware switch for the different items of equipment: connected to different ports on the switch, the latter are separated virtually by virtual networks (VLANs) simulating separate switches, thus making it possible to segment a physical network using software. They cannot communicate with each other unless they are linked to a firewall that allows them to do so.

"*Both methods have proved their worth in terms of segmentation, one is no more vulnerable than the other in cyber matters, if they are done well. The only difference, in my opinion, is in terms of cost. Physical segmentation makes it necessary to purchase numerous new devices. Very few companies can afford this luxury. Virtual segmentation is the most economically viable,*" says Tarik Zeroual.

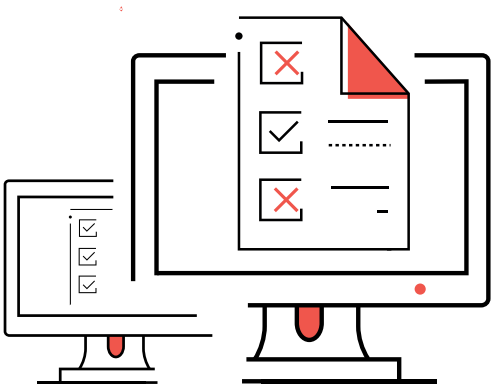
NAT, a useful mechanism

In some cases, the implementation of network segmentation, whether virtual or physical, requires a change in the organisation of the addresses used by the items of equipment to communicate with each other. The factories initially deployed equipment according to operational needs, without taking into account the allocation of IP addresses. As the network was 'flat', all the items of equipment were able to communicate with each other without any problem. "*But with zone segmentation, items of equipment can only communicate with those in the same zone, the same sub-network. However, it's impossible to ask a factory that has spent fifteen years or so developing its industrial systems to reconfigure this equipment item by item and test it all over again to see if it all works. It would be a financial drain on them,*" says Vincent Riondet.

To solve the problem in the short term, it's possible to use the NAT (Network Address Translation) function. This system allows addresses to be 'transformed', to match IP addresses to other IP addresses. "*This function involves translating an address in one sub-network to an address in another sub-network to ensure interconnection. It allows you to leave the applications untouched and not have to configure them again. NAT can be a temporary solution that allows information to pass through while waiting for industrial systems to be modernised or replaced*, continues Vincent Riondet. *We have clients with whom this migration scenario is spread over two years. However, we have already laid the foundations for these future reconfigurations, set our targets and defined our segmentation strategy. But in the background, it takes time on every maintenance stoppage. The industrial sector is complex, and we have to move forward step by step. Without NAT, most industries would not be able to secure their systems*". Address translation also makes it possible to integrate an industrial subsystem into the overall operational infrastructure without losing the manufacturer's or service provider's certification.

And so, as we have seen, **the segmentation of the information system is a complex operation that takes time**. To achieve defence-in-depth, it's therefore vital to get down to work on it without further delay! •

Workstations: exploring the world of suspicious behaviour



November 23, 2020

Trying to define what exactly constitutes suspicious behaviour can be something of an enigma, as this is a vast and complex subject. However, whether it comes from users, applications or lines of code, investigating suspicious behaviour on workstations is an integral part of efforts to guarantee digital security in companies. Here's why.

By

Adrien Brochot

With the advent of Bring Your Own Device (BYOD), shadow IT and now the widespread use of teleworking, IT security within companies is now being sorely tested. Cyber threats in the workplace are many and varied, and staff workstations are key aspects to be taken into account as part of your IT security procedures. In doing so, they must be painstakingly examined. Having access to files, registers, networks or application launches, the thousands or even millions of actions performed each day on our workstations are anything but standard as they each correspond to a particular context, activity or use. Observing, contextualising and analysing such actions enables an organisation to define what constitutes suspicious behaviour and what should be considered as legitimate actions performed on a workstation. And to react accordingly.

How do we define suspicious behaviour?

What is suspicious behaviour? Suspicious behaviour on a workstation can be defined as an action which runs without the user's knowledge, for the purpose of performing a malicious act. Suspicious human behaviour would include for example an unusual log-in time such as the middle of the night, or the fact that a user suddenly connects to his workstation from abroad. For its part, suspicious technical behaviour can be defined as an anomaly within the

workstation. On this point, we can list several major categories. Firstly, there's the presence of unlisted software, or software installed without the IT department's knowledge which can 'only' be considered as tell-tale signs of shadow IT. Next, there's the type of suspicious behaviour which is clearly malicious and which differs significantly from the normal use of an application or workstation, such as for example a ransomware program which finds its way onto a workstation and which then quickly sets about deleting backups and encrypting files. Another type of suspicious behaviour sometimes seen is the hijacking of the normal operation of a software program or application to fool the user. This kind of hijacking or misuse is more subtle than the clearly malicious behaviour. This is particularly the case with phishing. Finally, suspicious behaviour may also be defined as a series of fairly common actions which operate discreetly before they can be detected. This is especially the case with APTs (*Advanced Persistent Threats*).

"Defining suspicious behaviour can tell us what we need to be detecting"

Thierry Franzetti
Technical Leader Stormshield

The task of defining suspicious behaviour is not limited to simply being aware of these three major categories. In fact, it can be quite complex. A form of behaviour defined as suspicious by one department or occupation will not necessarily be considered suspicious by another department or occupation. "*Today, it's the IT Managers who have the task of defining suspicious behaviour. But the IT department can't possibly know everything and some activities have uses and practices which differ widely from the norm and may be considered as verging on suspicious behaviour,*" explains Sébastien Viou, Cyber-Evangelist Consultant Stormshield. Over and above the IT department's role, it's therefore a good idea for each activity to define its own usages and to be an active stakeholder in ensuring its own security. "*Cybersecurity should concern everyone*" adds Sébastien Viou. **Defining suspicious behaviour based on different activities and usage types is a valid but difficult objective**, as you need to simultaneously control and monitor such usage while at the same time ensuring that it remains fluid.

Understanding suspicious behaviour, defining it and then detecting it is therefore no easy matter and requires a great deal of research and analysis. But if the task is such a demanding one, why define what constitutes suspicious behaviour? "*Defining suspicious behaviour can tell us what we need to be detecting. For all stakeholders in the cyber field, this exercise also makes it possible to share knowledge using a common language, particularly via the MITRE ATT&CK framework,*" explains Thierry Franzetti, Technical Leader Stormshield. Among other things, this sharing of knowledge allows us to keep pace with the different techniques being used for malicious purposes. But a prerequisite for this analysis work is to have a thorough understanding of the attack techniques used and in particular the major vectors of infection for workstations.

The main vectors of infection for workstations

Whenever suspicious behaviour is detected on a workstation, an attack is generally underway or being prepared. Some vectors of infection target workstations, among which four merit particular attention.

Phishing

The main vector of infection used is phishing, with 75 to 80% of malware programs using it. Phishing is popular with many attackers as it is simple to perform, effective and makes it possible to reach as many people as possible.

As an example, in December 2019, researchers at Kaspersky discovered that cyber criminals had used the launch of one of the most eagerly awaited films of the year, Star Wars, to carry out a phishing campaign: around thirty fake Star Wars-themed websites were detected. Using these websites, the attackers were able to deceive many surfers by proposing a free version of the film, available for download from these malicious websites. Proceeding in this way, the attackers were able to harvest the personal data of the surfers they had lured in. These phishing attacks have also increased in scale over recent months during the pandemic, something which has been exploited by the attackers. Numerous phishing campaigns were launched focusing on health and prevention during the Covid-19 epidemic. The move towards teleworking from home, affecting a large percentage of the population, has only exacerbated this trend. According to the initial figures, attempts at phishing are believed to have increased by 400% during the first week of lockdown.

USB peripherals

USB peripherals are another vector used to infect workstations. Including mice, flash drives and keyboards, etc., these peripherals are considered as more targeted vectors of infection. This operating method involves leaving a USB flash drive with a malicious payload lying around on the ground near a target company. The natural curiosity of some staff will ensure that the key is quickly picked up and plugged into a workstation.

In a study into attacks using USB flash drives, the SSTIC highlighted the large attack surface provided by these peripherals and particularly flash drives (data breaches, elevated privileges, etc.) and the operating methods which may be used by the attackers. For example, a workstation may become infected when the user opens one of the files stored on the flash drive or simply when the drive is plugged into a workstation.

Remote Desktop Protocols

Another possible vector of infection is the ability to compromise RDPs (*Remote Desktop Protocol*). These protocols make it possible to access workstations or machines remotely. This type of vector of infection is used by ransomware programs for example. This is the case with the SamSam ransomware discovered in 2015, which specifically targets Windows servers. In 2018, the FBI investigated the way SamSam operates and revealed that the RDP is used as a vector of infection to attack Windows servers.

Where RDP protocols are concerned, once again the pandemic has helped amplify the phenomenon and particularly brute force type attacks. With the lockdown and the widespread use of teleworking, staff often find it necessary to access their work environment remotely from their home computers without necessarily being up to speed with the security rules for teleworking. The number of instances of RDP protocols being compromised has therefore increased sharply.

These vectors of infection all present risks of malicious cyber activity for organisations, to which should be added the issue of guaranteeing cybersecurity when teleworking. More than ever before, companies need support from key players in the cyber field to limit any risks of security breaches which may exist and to control and better understand so-called suspicious behaviour, in order to be better able to combat cyber criminality within the company.

Endpoint solutions to the rescue

The security solutions making it possible to detect and monitor suspicious behaviour have evolved over time. Previously, the go-to solution used to protect yourself from cyber-attacks was an antivirus program. This approach was soon found to be insufficient, as antivirus programs don't detect behaviour but only known malicious code. "*Some attack techniques seek to hide from antivirus programs, so you need*

to come up with solutions to supplement this type of detection and which can also envisage non-standard usage," explains Thierry Franzetti. More advanced security solutions then came along, firstly with the use of Endpoint Protection Platforms (EPP), which make it possible to detect clearly malicious suspicious behaviour, and which offer workstation protection functions. Subsequently, Endpoint Detection & Response (EDR) solutions also appeared. These EDR solutions meet this demand for the detection of suspicious behaviour as they operate based on the proactive detection of as yet unknown threats, by 'listening' to everything which happens on a workstation and picking up faint signals, such as the sudden launch of numerous operations on the same workstation for example. EPP and EDR solutions each provide useful levels of protection, which supplement one another according to the company's usage methods. Artificial intelligence (AI) is a solution which often goes hand-in-hand with EDR. "*In particular, AI provides greater calculation capacities, enabling it to identify instances of unexpected behaviour and to assign a score to them, in order to then be able to categorise them and react to them,*" explains Sébastien Viou. AI seems to be increasingly used within the different blocks comprising cybersecurity solutions and researchers appear to agree on its value. As an example, British intelligence recently carried out a study into the value of AI to combat cyber threats, and the identification of suspicious behaviour emerged as one of the areas in which the use of AI may be of considerable value.

In addition to Endpoint solutions, other solutions can be considered, like sandboxing, which makes it possible to open files or to run unknown or suspect content in an enclosed test environment, without taking the risk of compromising the workstation.

However, although a number of security solutions exist to meet the challenges of corporate cybersecurity and more particularly those related to suspicious behaviour, these solutions must be implemented taking full account of the contexts in which they apply. The software publishers' task is to correctly define the suspicious behaviour being targeted, beforehand. "*A security solution is just a tool. What's important is the way it's configured and maintained,*" adds Sébastien Viou. The software publishers therefore must be able to pre-configure their solutions by including all measures and rules (configurable rules adapted to each business context) to enable them to provide the right detection level. But also provide an easy-to-configure environment for administrators. To be effective, the solutions must therefore incorporate combinations of protective measures (peripheral management, elevated privileges, etc.) and the associated behaviour patterns. Additionally, Endpoint solutions are not infallible and false positives exist. "*Although we can define the basic factors for protection, the variety of suspicious and non-suspicious behaviour on a workstation is so great that there will always be exceptions,*" explains Thierry Franzetti. To limit false positives, the ideal is to be able to create a *whitelist* (or *allowlist*), to avoid blocking legitimate uses. To be fully effective, it's a good idea to be able to tailor this approach to each activity and to adapt the protection to different behaviour types.

Displaying a window in a web browser, opening a Word or PDF file or downloading files are all day-to-day tasks within the company which will undoubtedly be the subject of in-depth consideration where IT security matters are concerned for some time to come. And suspicious behaviour, a major subject in the corporate cybersecurity field, will continue to be a headache. •

And what if a cyber-attack originated from your antivirus solution?

December 28, 2020

Often seen as a key line of defence against cyber-threats, antivirus solutions are nevertheless vulnerable. The news reports have shown that these protective solutions have become particularly attractive targets for cyber-criminals. We explain.

By

Victor Poitevin

You never know where a cyber-attack's coming from. But the hack targeting Mitsubishi Electric in 2019 may come as something of a surprise: cyber-criminals successfully exploited a flaw in its... antivirus system. More precisely, they hijacked the antivirus solution to gain elevated privileges enabling them to extend their grip over the infected machines. And it's a serious matter: **a compromised antivirus solution won't prevent a cyber-attack. Worse still, in some cases its presence on the workstation can actually facilitate an attack**. This new modus operandi speaks volumes about the way cyber-attacks are changing and the responses that need to be put in place.

Why attack an antivirus solution?

It may sound counterintuitive: by targeting an antivirus solution, aren't cyber-criminals taking the risk of triggering alerts of all kinds? "*For a long while, intruders sought to hide from security solutions when performing their illicit activities*, recalls Adrien Brochot, Product Manager Stormshield. *But this became more difficult for them as antivirus solutions became ever more sophisticated. And so current techniques involve deactivating the antivirus system before carrying out a prohibited operation. Or even using the antivirus solution to increase their privileges on the machine*".

Because increased privileges are the Holy Grail sought by cyber-criminals. "*In a classic attack scenario, you begin by taking control of an exposed service with a low level of privileges*, explains Sébastien Viou, Cyber-Evangelist Consultant Stormshield. *But using another vulnerability, you can take control of a higher-level process making possible to run code or commands. And this lets you extend the scope of your activities*". This process is "*fairly simple to put*

in place, according to Sébastien. *The difficult part lies in finding the vulnerabilities*". The research phase can take time but always bears fruit, including in the case of protective solutions. By successfully compromising the antivirus system, the cyber-criminals can even access the administrator's rights for a workstation and subsequently the domain administrator rights. How the antivirus system has become a prime target for cyber-criminals…

Enlarge your attack surface

An antivirus solution is a piece of software. And as software, it has lines of code and possible bugs which can become vulnerabilities. "*When you're coding, statistically you'll have one bug per 1,000 lines of code. And a software solution contains hundreds of thousands of lines of code. So when you add a software solution to an item of equipment you're naturally increasing the attack surface,*" stresses Sébastien Viou. It's what's known as a measure-related risk: **in addition to the residual risk there's also the risk of the measures you introduce**. Including in the case of protective measures.

A recent study by CyberArk revealed major flaws in most security software. CyberArk's researchers identified around a dozen vulnerabilities including in market-leading antivirus solutions. A goldmine for cyber-criminals.

A three-phase attack

To hijack an antivirus system, an example of a widely used vulnerability involves symbolic file links. The aim of this approach is to direct the antivirus solution's attention towards a file other than that containing the malware – often one of the files comprising the antivirus solution itself – to then deactivate it. As the purpose of an antivirus solution is to scan all files arriving on the workstation, it will naturally scan the malicious file and attempt to delete it. But because of the symbolic link, it instead deletes the 'legitimate' file. "*This technique makes it possible to hijack the operation of the service. It's the simplest method to use and can involve just a few lines of commands,*" notes Sébastien Viou. This is the first stage in a cyber-attack, the stage enabling the cyber-criminal to gain a foothold in the system.

"One of the current techniques involves deactivating the antivirus before carrying out a prohibited operation. Or even using the antivirus solution to increase their privileges on the machine"

Adrien Brochot
Product Manager Stormshield

The second stage involves increasing your level of privileges. For example, an application which does not properly control its resources can load a Dynamic Link Library (DLL) controlled by the attacker instead of its own, thereby allowing the attacker to run code in the application with high privileges. This vulnerability is then sufficient to trigger the now-familiar chain reaction. "*The security solution has extensive powers on the workstation. It has the highest rights, enabling it to block all kinds of critical applications. If you make it through to administrator level, you can grant yourself all rights over a machine,* explains Adrien Brochot. *And as antivirus solutions are generally installed on all workstations in the company, finding an exploitable vulnerability on a workstation means that you can exploit this on all of the other machines*".

"*Once you have administrator rights on a machine, it's relatively easy to control other machines in the company or even the whole system. This is why the AD is subsequently targeted,*" adds Sébastien Viou. This is the third part of the attack, the launch of the malicious action. "*The*

intruders seek to be discreet during the initial stages to infect as many machines as possible before really unleashing the malicious part including data theft, the blockage of workstations and the destruction of production activities, etc., adds Adrien Brochot. *Generally, it's at this stage that the company realises it's under attack. People start getting locked out of the system and can no longer access what they need... And it's at this stage that the admins can really start panicking, because it's already too late*". With sometimes serious consequences including a stoppage of production

How do you build a robust cybersecurity system?

And here, antivirus solutions are not the only ones concerned as cybersecurity solutions in the wider sense are not immune to this threat either. A quick look at the list of CVEs concerning software publishers is guaranteed to send a shiver down your spine… These vulnerabilities are numerous and well-documented – and that's before we even consider the backdoors, deliberately built into some systems and solutions.

But how do we tackle these threats when the very tools which are supposed to be protecting us have embraced the dark side of the Force? A complex question to which the initial answer is relatively simple: **we need to make them more robust**. And therefore more secure. And it's the responsibility of security solution publishers – like Stormshield – to introduce the best practices and all the tools needed to achieve this as part of their development cycles, by applying the concept of security-by-design.

From the very design phase for these tools, it's vital to anticipate all applicable security requirements and to perform a risk analysis. Thus, the choice of a micro-service type software architecture for example will offer greater resilience than a monolithic solution. This micro-segmentation involves segmenting rights and isolating the workflow for each service, as Adrien Brochot explains: "*we break down all of a solution's functions into several different services. Each one has the minimum required rights needed to perform its operations and can only communicate with certain other specified services*". This is the application of the lowest privilege principle, as recommended by the France's ANSSI cybersecurity agency. The goal: to reduce the attack surface to the bare minimum and limit the spread of the malware. Next, during the development phase, code control tools should be used and specialised outside companies called in – encouraged by a bug bounty for example. Finally, before launching the solutions in the marketplace, the solutions and their source code should be audited by independent third parties to ensure that there are no backdoors or structural vulnerabilities. It's a simple question of trust.

"Once you've got administrator rights on a machine, it's relatively easy to take control of the machines in the network or even the whole system"

Sébastien Viou
Cyber-Evangelist Consultant
Stormshield

Despite all of these precautions, no security solution can always guarantee to be bug-free. However, it's possible to demand a guarantee of robustness from the solution and to ensure that it has the capacity to protect itself or even repair itself in order to minimise the impacts of any possible corruption. For this reason, the best solution to be adopted is to **favour the use of trusted technology**, to guarantee an overall optimal security level for your system. •

CYBER
MATURITY

Can the ROI in cybersecurity investments be measured?

April 13, 2020

Measuring the ROI in cybersecurity investments is a recurring issue for IS departments and CISOs. In the face of a threat some consider as a mere hypothesis, how can you account for expenses that are not hypothetical? And, most importantly, can the way people think actually be changed? Thus shifting from a paradigm focussing on cost avoidance to a model that promotes investments.

By

As the CISO of a big company said: "*we have been trying to identify possible risks and damage and the probable occurrence of cyberattacks for the last fifteen years, in order not to miss out on the necessary security investments*". However, sometimes, these are difficult to account for and, thus, some companies only make drastic changes in their strategies once the first attack has occurred.

Issues regarding the efficiency and profitability of security expenses are indeed recurring issues. And the question is asked as follows: how do you link an actual expense with an unforeseeable threat? And can the executive managers be persuaded that non-productive investments are necessary? The growing media coverage of security incidents does, however, place this issue on the agenda.

Cost avoidance: an excessively restrictive paradigm

Undeniably, the maturity levels of Executive Committees have improved in terms of the understanding of cyber risks over the last few years. More often than not, the growing awareness has given rise to significant increases in the budgets allocated to IS departments.

Nonetheless, many CISOs reveal that their senior management regularly hold them to account, subject to revising their budgets downwards. "*We have actually seen the budgets of some companies stagnate over the last few months,*" said Benjamin Leroux, Chief Marketing and Innovation Officer at Advens.

It is often complicated for a CISO to demonstrate the benefit of security expenses, since the prevailing paradigm remains that of cost avoidance. It is thus preferable to explain that protection expenses made it possible to avoid losing X million euros, rather than saying that they earned Y million by implementing them.

However, assessing the costs of a cyberattack may prove very complex. Whether in terms of the ransom to pay and/or the disruptions in operations, the impacts may serve as landmarks, provided the appropriate scale is used. According to the Hiscox insurance company 2019 report, the average cost of cyber-incidents for a small company is estimated at 14,000 euros. This amount should be compared to the amounts stated by companies such as Demant, one of the major manufacturers of hearing aids in the world, which expects a 95-million dollar loss further to the ransomware that affected their production and distribution facilities in Poland, Mexico, France and Denmark. Or Eurofins Scientific, which lost 75 million euros because of another ransomware. These examples offer a wealth of information while, still according to the Hiscox report, the cost generated by all cyber-incidents is an average of 110,000 euros.

Along with this financial impact, possible regulatory penalties should be taken into account. At a European level, the GDPR indeed imposed fines as a percentage of the turnover (4% of the worldwide turnover) on all the companies that have been negligent in the protection of the data they process. In July 2019, British Airways faced a significant fine after a data breach.

But some other costs are difficult to assess, when it comes to disrupted operations. "*There are incidents for which assessments fluctuate considerably. For instance: what is the cost of a one-hour unavailability of an e-commerce site during the sales period, following a DDoS attack?*, asks Benjamin Leroux. *Moreover, indirect costs should not be overlooked, neither should the impact of a cyberattack on a brand image*".

In addition to these already complex calculations, two aspects also need to be taken into account. The first aspect is that **cybersecurity solutions often provide solutions that are not purely cyber**. For example, a firewall offers QoS management, URL filtering and management of multiple links, and therefore provides enhanced connectivity for the most important uses. Along a similar vein, VPN features provide the opportunity to implement remote working or remote maintenance. Generally speaking, adding a layer of cybersecurity can help to modernise some practices that used to require the presence of human beings. The second aspect involves calls for tenders – namely of major purchasers –, in which the measures regarding IT security outlined by tenderers are given pride of place, or even are now the decision criterion. **Cybersecurity may then become a differentiator between a company and their competitors.**

Assessing risks: a multifaceted exercise

At a time when more and more people underline the essential part played by cyber resilience, we should bear in mind that, most of the time, **the question is not *whether* your company will be attacked but rather *when* the cyberattack will take place**. If assessing the costs of a cyberattack that has not (yet) taken place is a theoretical exercise, the latter, however, increasingly turns into an operational reality. The cybersecurity news is full of numerous examples.

Finally, explaining why it is complex to calculate the return on investment of IT security involves taking into account the fact that our sector is still young and, above all, is little known. We only have little hindsight and don't have enough reliable data to implement robust models.

Moreover, making the buzz (often fuelled by the media) highlights the major cases for which costs reach several hundreds of million euros, although they only are the tip of the iceberg. Conversely, many SMEs that have been particularly exposed are reluctant to provide the amounts of the attacks they were the victims of. The opacity in our sector therefore makes calculating estimations even more difficult.

The ABC of the risk approach

In spite of the obstacles mentioned here above, solutions do exist. The France's ANSSI cybersecurity agency has for instance developed the Risk Manager EBIOS method to help organisations identify and understand the risks that are specific to them. "*The purpose is to uproot the irrational elements in the conventional risk analysis, which is mostly based upon estimations*, Benjamin Leroux underlines. *In this method, each type of attack is listed, characterised according to its impact and associated with a cost. It is then possible to implement a risk management plan (antivirus programs, firewalls, awareness campaigns, organisation, etc.) that can actually be evaluated*". The analysis in terms of ROI can thus be conducted by removing the amount to invest from the anticipated losses.

Once the calculation has been done, it is essential to measure the effectiveness of the risk management plan, with a logic of control. Another difficulty arises at this stage: if I implemented a solution to detect an incident, but nothing happens, is it because no incident occurred or because my solution was not effective? Although the reports or frequent management charts on the attempted attacks provide part of the answer, there are still doubts. "*In these cases, companies conduct audits and may ask pentesters to run penetration tests to check the effectiveness*," Benjamin Leroux explains. But there again, it is difficult to actually demonstrate the profitability of cyber investments, since these penetration tests do not enable companies to earn money in the strict sense of the term.

Finally, in the conventional risk approach, it is also important to rationalise the protection measures. A new challenge to rise to in cybersecurity, since we try to optimise the cyber-mix without setting aside the plurality principle and the principle of dual barrier technology. And this is far from easy.

To bring about a qualitative leap in cybersecurity

However, there is an alternative move, i.e. a model in which promoting investments in cybersecurity may help earn money. "*Lately, the Société Générale bank implemented OPPENS, a security coaching service meant for very small businesses/SMEs,*" Benjamin Leroux points out. What for? To sell the know-how developed in house to companies with a view to promoting these investments.

Halfway between analysing risks and rationalising protection measures, **measuring the ROI in cybersecurity is complex**, but more essential than ever. What we see taking place is the need to shift the paradigm, to move from a strictly quantitative analysis to an analysis that includes the qualitative factor. The perspective changes when we move from a strictly monetary ROI, based on a costing approach, to a ROI based on the value of security investments. **It is high time managers see cybersecurity as an opportunity**, and not as a threat. •

CISO: a profession on a knife edge

June 23, 2020

They've paid a personal price during the pandemic. On the front line of the Covid-19 crisis, unhappiness among CISOs – torn between urgent internal demands and long-term security requirements – seems to have risen to new heights. To such an extent, in fact, that the topic of burnout is now no longer a taboo in the sector.

By

Victor Poitevin

In November 2019, the *CISO Stress Report*, based on a survey of over 800 Chief Information Security Officers and company leaders in the United States and the United Kingdom, painted a bleak picture of one of today's most in-demand jobs. And it revealed some alarming figures: 88% of the CISOs surveyed considered themselves to be "*moderately or extremely stressed*", 48% said that their stress levels had an impact on their mental health, and 23% admitted that they had turned to medication or alcohol. With long working hours, limited budgets, recruitment difficulties, and a lack of representation on boards of directors, the situation is hardly promising, while at the same time employees and business teams require IT tools to offer ever-greater speed and fluidity. And there's also the constant stress as a result of the acceleration of new cyber threats, coupled with the fear of being held liable in the event of mishaps... **So what's the situation in terms of CISOs' mental health?** What approaches can be taken to improve things?

The culture at the root of the problem

Above all, CISOs suffer from being misunderstood. Yohann, who is looking for a job after leaving his

former role to avoid burnout, explains: "*What's frustrating is that when we do our work well, no-one sees it*". Which makes it difficult to showcase your value as a cybersecurity expert... And yet **the role of CISO is a role for people who are passionate** about new technologies, and for many of them it's much more than a job. "*The field of IT security is so huge that you can never do enough – we do it out of professional ethics and out of love for our work, but it can become exhausting,*" he adds. The CISO Stress Report clearly highlights the weight of the responsibility that these IT security experts shoulder: 44% of respondents said that the main reason for their unhappiness was single-handedly being responsible for their company's cybersecurity in a world that fails to recognise the severity of the challenges they face. And for 35% of those surveyed, the level of stress is so great that it affects their physical health. Following its publication, the study received mass coverage, and Russell Haworth, CEO of Nominet and the study's sponsor, reported receiving many messages from CISOs and cybersecurity experts confessing that they recognised themselves in the study's results.

"The field of IT security is so huge that you can never do enough – we do it out of professional ethics and out of love for our work, but it can become exhausting"

The study was based on professionals in the United States and the United Kingdom, but the situation doesn't seem much better in France either. However, the scope of the problem differs as a result of different cultural characteristics: it seems that France places little value on those with technical profiles. Alice Louis, an IP/IT lawyer and expert in information asset governance, recalls the exemplary case of Louis Pouzin. "*A brilliant researcher and engineer and a Polytechnique graduate, he is recognised globally as being one of the founding fathers of the internet. The Cyclades project, which he led in the 1970s, resulted in significant advances in the field of network architecture. The Americans, who were in the midst of the Cold War at the time, soon saw the strategic benefits, while the French government decided to focus on Minitel. I'm stunned to see just how unable we are to learn from the lessons of the past! France has many talents, and French genius also shows itself in the form of information and communication technology.*" But this attitude isn't present across the pond. "*If you take the top 10 listed companies, three quarters of them are run by engineers or coders. This is absolutely not the case in France, where the engineering culture we take so much pride in is nothing more than a fantasy. There are no Polytechnique graduates in top state roles, only ENA graduates,*" says Fabrice Epelboin, an entrepreneur and teacher at Sciences Po.

In his eyes, IT is still viewed with a certain level of contempt, and he responds to this with provocation: "*Within companies, people don't know the name of their IS Director, and so they have nothing to do with them. For big French companies, the IS Director is a housewife – a well-paid one, yes, but someone in a position of a simple underling who you call when you have a problem.*" So what about CISOs, who are themselves subordinate to the IS Director? In the 2018 edition of the "*IT Threats and Security Practices in France*" study by Clusif, 77% of CISOs at the biggest companies reported that they were part of the IS Department. Meanwhile, in companies of fewer than 1000 employees, 55% reported directly to management.

In the United States and the majority of English-speaking countries, **the CISO is increasingly part of the management committee**. But in France, they are overlooked within their companies. "*It's to do with the fact that fundamentally, a CISO is a hacker. They don't come from the prestigious universities we val-*

ue, and they aren't familiar with their codes of behaviour, otherwise they would have become an engineer," Fabrice Epelboin adds. And as a result, CISOs are perceived as holding simple support roles.

CISOs in crisis before the crisis

Especially because, isolated and alone, CISOs aren't lucky enough to enjoy a support system within their company – in fact, the very opposite is true. "*It's a product of the organisational structure*, says Yohann. *We're seen as a necessary evil. Our missions clash not only with those of other departments, but also with the missions of the IS Director, our line manager, whose goals of ensuring infrastructure availability and ability to cope with loads are the opposite of our own*". When the two clash heads, the CISO – whose budget is nothing but crumbs and who often has a small team – must sometimes accommodate a bending of security practices in the name of the business's needs.

"CISOs are seen as a necessary evil"

Jérémy, another CISO, shares this view. "*We're caught between the IS Director, the management committee, and the users, who don't understand why we impose security standards. By going along with what IS departments want, we're often forced to approve dangerous situations and accept the risk of it coming crashing down on us.*" With a wry laugh, he repeats a well-worn phrase among CISOs: "*The IS Director is management's fall guy, and the CISO is the IS Director's fall guy*". If a problem arises, the CISO will soon be blamed – or even sacrificed.

And to top off this precarious position, along came the Covid-19 crisis to add to the friction. "*The sole aim in many executive committees at the moment is to survive, and that comes at the expense of the security standards we recommend,*" says Jérémy. Rolling out remote working for the entire company by generalising BYOD has opened up a number of weak points in IT security while also increasing the workload of already overworked CISOs. "*Everything had to change overnight. And no company was prepared*, says Jérémy. *For employees, there was no issue, because their work didn't change, whereas on our side it required a complete reconfiguration*". In the wake of these practices, new threats, such as shadow IT, are arising as a result of the use of applications and services alongside those offered by the IT department. "*By pulling out all the stops, CISOs were nonetheless able to quickly and successfully implement a number of initiatives. But this success was a double-edged sword: it hid the complexity and difficulties of our task,*" Jérémy adds.

And the cost of succeeding in this difficult balancing act can be the implosion of your personal life. "*I come home late from the office, I grab something to eat, and I get back to work until 1 am. I no longer have weekends,*" says Yohann. In English-speaking countries, the CISO Stress Report reveals the same unease: 95% of respondents reported working more than their contract requires, and 39% said they had missed a family member's wedding or even holidays because of their work.

How can you look after your CISO?

From within and without, CISOs are besieged from all sides. But they aren't doomed to their fate, and a number of solutions can be considered.

Yohann and Jérémy are unanimous: CISOs should no longer be subordinate to the IS Director. "*This relationship prevents the CISO from properly fulfilling their role as a cybersecurity expert and a counter-power that can only be achieved with independence,*" explains Jérémy. To do this, a more American cultural approach is required – one which is more open to delegating responsibility. "*The CISO also needs to be closer to the top management team and incorporated into the Executive Committee. Once they're on an even footing with the IS Director, they will be able to defend their positions in full transparency,*" adds Yohann. This would allow decisions to be made with full knowledge of the facts.

And at the employee level, one solution could be to organise educational workshops. "*In employees' minds, moving people to remote working is simple because they don't understand that this means protecting a different network with new concentrator flows. If only they knew,*" sighs Yohann. Establishing workshops to raise awareness of digital well-being would also help employees understand why certain best practices (no longer simply having an eight-character password, only using the recommended tools, etc.) are necessary. Because **at a time when the boundaries between personal and professional lives are becoming blurred** and when digital attacks are becoming increasingly common and increasingly sophisticated, employees haven't yet truly understood the scope of the risks they face. According to the CISO Stress Report, just 15% of respondents believe that the topic of cybersecurity is consistently discussed at meetings attended by company managers. And this means that the CISO, in their capacity as an IT security expert, must also become a teacher.

"We're caught between the IS Director, the management committee, and the users, who don't understand why we impose security standards"

Another approach supported by Alice Louis, who champions interdisciplinarity, is "*managing knowledge networks – in particular, networks of ethical hackers*", who are culturally closer to CISOs than IS Directors. Ethical hackers "*could be clear allies for organisations*", helping to **shift the balance of power in favour of cybersecurity**. These trusted hackers, who are sometimes more likely to be listened to, could play an important role in today's companies, becoming extensions of in-house security teams. Frans Rosén, a hacker from the HackerOne community, wrote in a press release published at the end of May: "*Some of my favourite highlights are [the] reactions to some of the bugs I've found. When the [IS Director] of a company calls me up in the middle of the night to understand the severity and panics when he realizes the impact*".

While Yohann and Jérémy have seen improvements to the situation, they nonetheless fear the role that Covid-19 could play. The epidemic could roll back what little progress they have witnessed in people's understanding of the role of CISO. So will the crisis accelerate progress or drive it back to the bad old days? It's still too soon to tell. •

CYBER SOLUTIONS: **FACING UP TO THE CHALLENGES OF TOMORROW**

CONTROLLED **SKILLS**

Cybersecurity: the fusion of yesterday's skills with tomorrow's technologies

October 12, 2020

"The best jam is made in old jars." This is a popular adage that could easily be applied to the cyber world, which juggles with future technologies and new uses while at the same time relying on existing skills and updating old, tried and tested methods for contemporary consumption. We serve up some food for thought.

By

Julien Paffumi

What are the limits of innovation in the cyber world? That's a question that everyone's now asking, but no-one can answer. And most importantly, when considering the question, we need to bear in mind the importance of the shared pool of existing knowledge. Because, although innovation is indeed a key pillar in this field, the ability to **capitalise on a solid skills base and recycle old techniques is also a core principle of the cyber world**.

A cunning blend of the old and the new that serves the interests of key cybersecurity players as well as it does those of attackers, and engages the ecosystem in an almost permanent arms race between the two camps. Hence the need for those on the defensive side to form a common front by sharing knowledge and best security practices.

Skills that are obsolete in some sectors, but ideally suited to others

When we think of cybersecurity, we think first and foremost of the IT world, a term covering everything related to computing and the Internet. We are less inclined to think of the OT one, which applies particularly to the industrial sector, a sector that is now quickly opening up and transforming and, in its turn, facing its share of cybersecurity issues.

IT is a constantly evolving world: new applications, new devices, new uses, and even new user groups, with the arrival of older users in this sector. Cybersecurity players have learned to live with this frantic rate of change, and to devise protective systems without having a clear vision of everything that could potentially happen. "*We need to accept the risk and create security solutions based on this philosophy,*" says Matthieu Bonenfant, Chief Marketing Officer Stormshield. Conversely, the world of OT is much more controlled and predefined. Every command sent to every component of the industrial system matters, and must be known and referenced. This is the polar opposite of improvisation, because the stakes are so high: "*By taking the risk that you might be sending the wrong command to an electrical substation, for example, you're taking the risk of bringing down the whole network,*" Matthieu Bonenfant adds.

But just what do IT and OT have in common? That's right, cybersecurity – and more specifically, the cyber world's ability to recycle various tried and tested defensive techniques. Protective methods that for decades have proved their worth in the IT world are also a perfect match for issues in the OT sector, which has been having to deal head-on with cyber issues since the advent of Industry 4.0. "*The arrival of cybersecurity in industry is still a fairly recent phenomenon, and what worked a few years ago for IT can still work today for OT,*" explains Adrien Brochot, Product Manager Stormshield. Working from this observation, cybersecurity actors in general – and therefore publishers in particular – must be able to capitalise by sharing their knowledge to replicate existing methods of defence on these new infrastructures.

"In reality, 90% of new attacks are based on old ones, and attackers are simply adapting them to get through security barriers and break into a system"

Adrien Brochot
Product Manager Stormshield

Take, for example, the case of IPS (Intrusion Prevention System), which provides a detailed analysis of network communications in order to check that a flaw in a protocol has not been exploited or a malicious command inserted. While IPS is still of genuine use in the IT world, the system is proving even more invaluable in industry, where the consequences of altered connection content can be catastrophic. The need to authorise only information that is deemed to be legitimate and matches a set pattern of behaviour is often critically important in this context.

New from old: the same goes for cyberattacks

The same principle applies to cyberattacks, which also take advantage both of yesterday's skills and today's technological advances.

Although new vulnerabilities and environments are exploited by attackers, the actual principles behind the exploitation of these vulnerabilities and environments change slowly. And to ensure that cyberattacks are profitable, groups of cybercriminals often turn to tried and tested recipes of the past. "*In reality, 90% of new attacks are based on old ones, and attackers are simply adapting them to get past security barriers and break into a system,*" says Adrien Brochot. After all, recycling is a hot topic in cybersecurity too, some 'new' malware actually being nothing more than variations of its predecessors.

In fact, the databases that identify such malware and its multiple variants are becoming too dense and heavy to be supported by operating systems. Consequently, such databases only include the most recent malware signatures, providing attackers with

an opportunity to exploit old and almost forgotten malware... such as the Emotet malware, for example, which was originally observed in attacks in 2014 and which is now back in circulation as of autumn 2020.

Cyberattacks are also frequently carried out at different periods of time; firstly, because they have proven their effectiveness in the past; and secondly, because even though patches are published when a vulnerability is discovered, not everyone applies these patches. Or at least, not simultaneously: this time lag provides a perfect entry point for attackers, who can also take advantage of this new, freshly revealed flaw.

"The key issue for attackers is, and will always be, to exploit areas that are poorly protected"

Matthieu Bonenfant
Chief Marketing Officer
Stormshield

Indeed, for a number of years now, there has been a considerable media focus on the discovery of vulnerabilities and cyberattacks; this varies according to the latest fads, serving the interests both of those seeking to protect themselves from them and of those seeking to exploit them. Some types of attack have received particularly strong media coverage, such as ransomware, webcam sextortion, and also the notorious CEO scams. This type of attack has really come to the fore in recent weeks with the Covid-19 health crisis: there has been an upsurge in instances of identity theft with the aim of extracting money. However, there are also types of attack which, by contrast, literally fly under the media radar, and are nurtured by a part of the ecosystem that analyses them – with some state agencies using this method so that they can discreetly exploit them later at a safe distance from any buzz effect.

"*Cyberattacks and the fashion industry evolve in somewhat similar ways: there are new things, old things and new things created from old codes,*" Matthieu Bonenfant wryly notes, adding that "*some old technologies will quickly reach their limits, and will therefore be adapted and brought up to date to make them efficient again, and so on, ad infinitum*". In 2017, the Wannacry ransomware attack made a lot of headlines, partially crippling a large number of major companies and organisations. And yet Wannacry – just like NotPetya a few months later – was propagated in a very similar way to the Conficker worm some ten years earlier.

Building on old methods, tailoring cyberattacks, making use of technological advances ... if you had to summarise the evolution of cyberattacks into one single concept, here's the most important thing to remember, according to Matthieu Bonenfant: "*The key issue for attackers is, and will always be, to exploit areas that are poorly protected*".

So what role do cybersecurity solutions play in all of this?

After all, the key role of cybersecurity solutions is to protect. But if they are to fulfil this protective role, we first need to establish how cyberattacks work and understand cyber incidents. Examining and analysing the operating methods of attackers and being on constant watch for the latest flaws discovered, developing systems capable of gathering 'traces' for cyberattacks... these are all key elements in adopting an adequate defensive posture.

Security analysts play a decisive role in the ability to assess a cyberattack. Their role is both to identify the attack vector (network, USB key, etc.) and to understand the action(s) performed by the attack and the way it spreads through networks, whether IT or OT-based. Such information is necessary for good control over the cyber-ecosystem – listing the different types of attack, having access to catalogues of vul-

nerabilities and patches – but also making it possible to take in the wider picture and tailor cybersecurity solutions accordingly. The 'tech' point of view is therefore essential in diagnosing a cyberattack and understanding its impact.

The way in which the cyber world is changing is a challenge for cybersecurity players, including publishers in particular, who must focus on new techniques and how they develop while at the same time keeping an eye on existing ones. They have a sort of "duty to remember", and it is their responsibility not to overlook old protection techniques which gradually fall into disuse over time, because this is precisely what attackers are counting on. Just like Emotet, other items of malware regularly make spectacular comebacks, such as those based on Office suite macros. Malware is never more dangerous than when it is believed to be extinct.

In the same spirit of creating continuity between the old and the new, publishers of cybersecurity solutions "*have a crucial informative role to play in the ecosystem: conferences, exhibitions, writing white papers, presenting use cases, etc.,*" explains Adrien Brochot, who sees such tools and opportunities for exchange as facilitating the sharing and leverage of knowledge within the cyber community.

The importance of sharing knowledge and best practices

To get the best out of changes in the cyber world and the digital era, cybersecurity players would do well to consider themselves as an ecosystem and make cybersecurity a common cause and collective responsibility. Even though many players in this ecosystem are competitors, this in no way prevents the sharing of information and knowledge, and the creation of partnerships. In addition, many technical databases are accessible to the community and updated by it, such as VirusTotal or MITRE ATT&CK.

This sharing of knowledge can also be achieved via public interest groups, such as the cybermalveillance.gouv.fr portal in France, which enables companies and individuals to report malicious actions perpetrated via the Web. Or also through information technology attack alert and response centres (the famous computer emergency response teams [CERTs] and computer security incident response teams [CSIRTs]), providing near real-time information on major cyber threats. These CERTs can be either public or private, national (CERT-FR in the case of France) or international (CERT-EU for the European equivalent). "*The ecosystem of cyber players is very rich in information and tools, but also very diverse in the way it presents and identifies knowledge: this poses something of a challenge when you need to sort through it and quickly and easily access the information that you need,*" explains Matthieu Bonenfant.

Here again, the technical layer (aka the security analysts) plays a decisive role in the ecosystem's ability to share its best security practices and skills. These experts have their own ecosystem within the cyber community, out of reach of any possible commercial disputes or other competitive strategies. And this represents a real boon and genuine added value for cyber players, because in this case, the process of pooling knowledge in this case is being driven by technical considerations, with a thirst for learning that irrigates the whole ecosystem. In this way, technical analysts analyse, dissect and share their findings, with a goal of constant improvement.

Sharing knowledge and best cybersecurity practices is therefore an essential aspect of the ecosystem in that it encourages cyber players to challenge themselves, improve, adapt and dream up the increasingly effective solutions of the future, in the interests of risk prevention and analysis. •

Intrusion Prevention Systems (IPS) will have a key detection and protection role to play in dealing with new and increasingly sophisticated threats.

White paper

DPI SYSTEMS AND NETWORK SECURITY

In this respect, the use of Deep Packet Inspection (DPI) analysis techniques for exchanged messages will be necessary in preparation for the protection of sensitive networks. To succeed in this challenge, the security solutions that are deployed must meet exacting requirements in terms of availability, integrity and confidentiality, arising from the various business challenges faced by operational networks.

We present a white paper to shed light on the various mechanisms that an IPS system needs to implement if it is to fulfil its role, and the information it needs to adapt to your security requirements.

A QUESTION OF **TRUST**

Europe: a bastion of cybersecurity

August 4, 2020

There was a time when, during the Cold War, the major powers were racing to conquer space. Now the race is to conquer cyberspace. The issues between the powers remain basically the same, but the rules have changed: now the game is about dominating your opponent by controlling the new playing fields occupied by cyberspace and its associated security issues. The opposing teams include the United States, China, Russia and Israel. Although it is competing, Europe seems to be playing from afar; in place of offensive and defensive strategies, it prefers the values of transparency and trust—which may one day take it to the top. It already has the tools to get there.

By

Matthieu Bonenfant

The geopolitics at the heart of digital technology

It is impossible to talk about digital technology and telecommunications these days without thinking about politics and geopolitics. For a few years now, we've seen the major powers, such as the United States, China, Russia and Israel, develop offensive and defensive strategies in the name of cybersecurity. Now more than ever, the most powerful tech actors seem to be at the mercy of states: while the cosiness between the NSA and the US government is well-established, its Russian counterpart can often only be accused of interference when sophisticated cyberattacks occur. "*On the Chinese side, it is public knowledge that an entire building near Shanghai houses officers of the Chinese army who are trained to deal with cyberattacks. On the Israeli side, the digital ecosystem is largely driven by former soldiers from Unit 8200, an intelligence unit of the Israeli armed forces. This shows that both offensive and defensive 'cyber forces' have risen to the highest levels of national strategic interest,*" says Pierre-Yves Hentzen, CEO of Stormshield. **Where does Europe fit into these cyber power games?**

The Covid-19 crisis has laid bare Europe's dependence on these major powers when it comes to issues of digital sovereignty. However, "*sovereignty doesn't mean closing oneself off or withdrawing from the world; it actually represents freedom: the freedom to make your own*

choices and take your own actions, without living under someone else's yoke. That's why I like to say that sovereignty shouldn't be viewed from a domestic perspective. I often hear people say 'we need to protect and support our French companies'. That's a counter-productive and highly reductive way of looking at it. What we need more is a global movement for a strong Europe with international esteem, insists Pierre-Yves Hentzen. *It's good to have European digital infrastructures, but their integrity and independence cannot be assured if we use non-European cybersecurity technologies to protect them. With these geopolitical issues and the mistrust they evoke, it is clear that origin criteria outweigh purely technological criteria when it comes to choosing a security product. Europe needs to shift course and assert its agency. It has the means to do so; it has proven it in other areas, when it moved to combat the health crisis and prop up the economy. Now it must also take action when it comes to cybersecurity*".

The need for financial and governmental support

The Covid-19 crisis has also revealed how much Europe lags behind when it comes to issues of digital sovereignty. "*We weren't ready. With video-conferencing solutions, for example, it's been American companies like Zoom that have reaped the benefits, with an explosion in user rates that have reached peaks of more than 200 million users a day. European solutions do exist, but they've proven to be functionally limited, sometimes for security reasons. And on top of that, they're struggling to stay afloat due to a lack of funds*," notes Pierre-Yves Hentzen. *A potential side effect of these security costs is a reduced level of investment in functionality. "It's not just the quality of the products that drives people to buy American, it's also the fact that they're better promoted and marketed. And it's all because they have the financial support needed to do so*".

This seems to be changing, however: in France, for example, it was announced that around twenty investors would be injecting six billion euros to fund French Tech startups. This isn't public money, but

"It's not just the quality of the products that drives people to buy American, it's also the fact that they're better promoted and marketed. And it's all because they have the financial support needed to do so"

Pierre-Yves Hentzen
CEO of Stormshield

money given by the largest French investment funds. The problem is, in Europe, it seems easier to invest in technologies with immediate returns. However, applications that require substantial R&D investments will not be profitable within a single year. Today, the world's top players that can afford such investments in cybersecurity are either American or Israeli. "*US companies in the sector are generally listed on the Nasdaq and heavily bankrolled by private equity funds, which allows them to invest hundreds of millions of dollars each year in R&D and marketing in order to capture market growth and dominate the field. Their strategy isn't to seek immediate returns, but to gain market share, which drives up their valuation. And unfortunately, our own decision-makers in France, whether they're public or private buyers, are feeding this well-oiled machine by mostly buying American technologies*," says Pierre-Yves Hentzen. For an example from the French health care industry, he points to Health Data Hub, which initially turned to Microsoft for its data hosting. This decision rightfully provoked an outcry: the French company OVHcloud invests heavily in this area, and could have been a more appropriate strategic choice to host such sensitive data. This matter will be one

to watch—along with the controversy surrounding Photonis. This company, which supplies sensitive high technologies to the armed forces, was nearly acquired by an American firm. The French Ministry of the Economy and Finance vetoed the sale. The company is still looking for French and European investors, but if they fail to find an acceptable solution on this side of the Atlantic, the deal may land back in American hands.

The importance of regaining control

Financial support and infrastructure control go hand in hand. China's internet is controlled by domestic firewalls in order to avoid dependency on the West, and on the United States in particular. Last year, Russia followed suit by isolating its internet from global servers. The move was deemed a success by the Russian government, which sought to pass a law establishing its own sovereign Internet. "*Infrastructure control has become a power game, and this also means controlling how the infrastructure is protected. The US, China and Russia understand this. A few months ago, Israel tested whether it could block all access to the Internet, to see if the country was capable of operating independently. This capability was clearly demonstrated,*" says Pierre-Yves Hentzen. The move represents a form of isolation and seclusion that raises issues of trust.

Still, today we can see how prevalent the problem is becoming: it is increasingly clear that some powers would not hesitate to use these methods to destabilise our very foundations. **But with its values of openness and transparency, Europe has a few cards of its own to play.** While the GDPR seeks to protect individuals and their individual liberties, the Cloud Act in the US allows the government to snoop through anyone's data, even outside of US soil. Compared to this intrusive system and the one in China, which is increasingly shutting itself off from the outside world, Europe comes across as open and trustworthy – even more so after the Privacy Shield was struck down by the European Court of Justice.

Establishing a common European regulatory landscape

While the GDPR is emerging as a model for other nations, the rest of the European regulatory landscape seems more disparate. Against this international backdrop, three European powers seem to stand out just ahead of their peers, mainly through their security agencies. All three of these organisations—the ANSSI in France, the BSI in Germany, and the NCSC in the United Kingdom (if we still take a broad view of Europe)—are globally recognised and accredited for their rigorous standards when it comes to IT system security and defence. However, Europe is a fragmented market, with different languages and cultures, as well as a sense of national allegiance that is still going strong in the various member states. That is why cybersecurity contracts are predominantly granted in the country of residence.

Breaking out of this comfort zone would require greater effort and investment. For example, companies would need to carry out translations, gain access to previously unknown media outlets, and adapt the product or service to different countries. A level of effort and investment that only the major players can currently afford. This fragmentation is an object of trepidation for the European Commission, particularly as it implements the NIS Directive. Indeed, with the creation of Operators of Essential Services (OESs), the directive "*has served as catalyst in many Member States paving the way for real change in the institutional and regulatory landscape with regard to cyber-security*" as noted in one of its recent reports. Nevertheless, "*there are diverging interpretations by Member States as to what constitutes an essential service. This makes it difficult to compare the lists of essential services*". To repair this fragmentation, regulations will need to be harmonised. In this effort, the ENISA will play an important role in building a single, secure digital market, the tech equivalent of the single market for goods and people.

Accordingly, under the Cybersecurity Act, **European certification schemes will be designed to establish a common framework on the market**. The first candidate certification scheme for cybersecurity products, which is based on pre-existing frameworks, has just been presented. This scheme was drafted by the ENISA, which relied on the expertise of member states and stakeholders—including Stormshield. "*The goal is to reduce this fragmentation, steer companies away from adopting a certification scheme based on the country where they want to market their firewalls, for instance, and limit the proliferation of national standards*, confirms Philippe Blot, Lead Expert Certification at the ENISA. *The idea is to create European pathways, a European form of governance, where all stakeholders agree on the rules of the game. Certification is a key element of trust. It subjects the product to a sort of trial by fire overseen by a third party. This party must be accredited and independent from the party that's submitting the bid, and must be supervised by the national authorities established under the scheme. This increased trust will help foster greater transparency in the bids. It will also help open the market to 500 million people*".

"The idea is to create European pathways, a European form of governance, where all stakeholders agree on the rules of the game"

Philippe Blot
Lead Expert Certification at the ENISA

The next step will involve cloud technology, as the ENISA has been tasked by the European Commission with preparing a European cybersecurity certification scheme for cloud services. The project is similar to Gaia-X, the European cloud platform that aims to create a reliable, secure data infrastructure for Europe, particularly for the health care industry. "*The encryption technologies used must be trustworthy, and the keys must be held by the company itself or by a trusted partner. I should be able to retrieve my data wherever it is stored: this notion of reversibility is essential, and Europe needs to work in this direction*," says Pierre-Yves Hentzen.

A Europe that is all too modest

But might Europe be just a bit too modest? "*The US, Asia and Israel have developed a strong culture of entrepreneurship: launching a startup over there is considered a real career opportunity. Their governments help and encourage them toward it, and the regulations there are more flexible than in Europe. The big tech players are more likely to emerge over there*," says Markus Braendle, Head of Airbus CyberSecurity.

Still, Europe has nothing to be ashamed of. It is home to a number of highly competent cybersecurity firms. It also has world-class universities for cybersecurity research, with highly talented cyber engineers. "*I think we're too modest and we under-estimate our traditional capacities. We're also at the centre of a new industrial revolution—Industry 4.0—with industrial leaders in aerospace, automotive manufacturing, pharmacology and chemistry, which are the envy of many. We have unrivalled know-how and unique expertise, which means even more cyber risks. As such, Europe must ask itself how dependent it wants to be on others for its cybersecurity, and find the right balance*," Markus Braendle concludes. •

CHOOSING A TRUSTED CYBERSECURITY SOLUTION

The question of technological and economic sovereignty at European level, particularly with regard to cybersecurity, is one of the major concerns to be raised in 2020, raising issues concerning transparency, trust and backdoors built into products.

In an attempt to answer these questions, Stormshield is following its own path, in contrast to its US and Israeli competitors. Faced with these sovereignty issues for our essential and vital companies and institutions, it is important for us to differentiate ourselves by supplying them with trusted, powerful European solutions.

A key theme in this respect is our pursuit of transparency. The proof: Stormshield is the only European publisher to appear on Gartner's map of the Firewall/UTM sector. By striving to ensure that our solutions are robust and our source code is audited, our intention is to help to bring peace of mind to your cyber-future.

Eric Hohbauer
Sales Director
and Deputy Managing Director of Stormshield

E-book

CYBERSECURITY COMPLIANCE

In a world of increasing cyber threats, every organization – large and small, public and private – is required to comply with cybersecurity regulations relevant to their market.

These regulations are designed to encourage organizations to enhance their IT security so as to protect users, data and networks. But in a complex and constantly changing regulatory environment, how do you know which regulations apply to your organisation?

Find out in this e-book, updated annually.

Do cybersecurity companies *have* a public service mission?

July 21, 2020

A general state of digital disruption during the Covid-19 health crisis has rendered companies, hospitals and public institutions particularly vulnerable to computer attacks. More than ever, the role of cybersecurity companies has been crucial in protecting these vital services which are so essential to the running of a country. But does that mean the sector has a public service mission?

The widespread switch to teleworking, often in situations of urgency and lack of preparation, not to mention general digital disorganisation, has created a perfect environment for cybercriminals. And this has been true worldwide. In the USA, the FBI has seen the number of reports of cyberattacks increase fourfold. Meanwhile, in France, the cybermalveillance.gouv.fr website noted a 400% rise in its traffic during the first two weeks of lockdown.

By

Pierre-Yves Hentzen

Cybersecurity: a public interest requirement

"*The three months we've just been through have demonstrated that digital technology is the lifeblood of today's society and economy*, observes Stormshield Chief Marketing Officer Matthieu Bonenfant. *They have also shown that a switch to all-digital technologies (use of computer equipment at the employee's home, videoconferences, increased use of the cloud, etc.) is not something to undertake without preparation, and securing these processes is essential. This crisis has highlighted* ***cybersecurity as an essential part of safeguarding assets and business continuity in companies and organisations****. This essential role is yet more marked in sensitive sectors of activity, such as drinking water distribution, energy production and transport sector regulation. In such environments, the consequences of cyberattacks can be catastrophic, damaging the integrity of assets and individuals*".

Of course, governments were aware of the importance of cybersecurity before Covid-19. Its vital role was officially recognised by the European Union in the Network and Information Security (NIS) directive of 2018, which was directly inspired by France's *Loi de programmation militaire* (military planning law). This directive recognises that it is critically important to ensure the cyber protection of Operators of Essential Services (OESs), as disruptions or failures in their services could have consequences for human life and the environment.

However, the crisis has served to raise the public profile of this issue. "*The general public has realised that public services such as hospitals could also be affected, and that the consequences could be serious,*" notes Manon Deveaux, who holds responsibility for cybersecurity issues within TECH IN France's Public Affairs team. As well as hospitals, local government organisations were also attacked during the pandemic. In particular, the city of Marseilles (France) was paralysed for a number of weeks by ransomware. The incident had a number of parallels with successive attacks on 22 American municipalities in 2019. And it is in line with a headline trend in recent years: the disruption of democratic life and frequent cyberattacks during electoral campaigns.

During the crisis, the cyber sector is standing resolutely against malicious attacks

Because they supply solutions to protect such vital services as a hospital or a voting system, **does that mean that cybersecurity companies have a de facto role of public interest, or even public service?** During the pandemic, the cyber community has taken its protective role very seriously; such as, for example, the publisher The Green Bow, which has made its products available free of charge to companies seeking to protect their teleworkers. And many other actors in the sector have offered their help to hospitals and companies for no financial reward. "*In these extraordinary current times, organisations needed secure IT and OT infrastructure more than ever. For that reason, we gave away licences for our virtual appliances to all companies. More than sixty took advantage of them. At the same time, we set up remote training courses, to replace our face-to-face training, and offered special terms for upgrading firewalls,*" Matthieu Bonenfant explains.

"Digital technology is everywhere. Its protection has become a critical and key issue"

Matthieu Bonenfant
Chief Marketing Officer
Stormshield

In the United Kingdom, cybersecurity researchers formed the Cyber Volunteers 19 group. Its goal was to bring together institutions that had fallen victim to cyberattacks and actors from the cyber sector seeking to provide voluntary assistance. "*The message we're sending out to cybercriminals is that we're standing alongside our public services. Attacking a hospital is shameful at any time, but during the chaos of a pandemic, it's revolting,*" Lisa Forte, the creator of Cyber Volunteers 19 explained to *Wired* magazine.

This wave of solidarity is a one-off response to a situation of crisis. However, it does seem to show that the cybersecurity sector does in fact exercise a public interest role.

The makings of a public cyber services and a right to cyber protection?

Although this role is not officially enshrined in any legal status, it is one that is embedded in the very culture of cybersecurity companies. "*Cybersecurity actors are aware of their mission*, notes Manon Deveaux. *And that's something you don't find in many other sectors. That sort of awareness is certainly connected to the cybersecurity culture; where, for example, you can find groups of ethical hackers, and to the fact that the issues faced by this sector are issues of national defence and policy, in the sense of aid to the city*".

How does this sense of mission manifest itself outside of a time of crisis? "*The way we have taken account of the public interest question has been through the accelerated development of our offers to companies in the industrial operations sector, including those supplying key services to citizens*, Matthieu Bonenfant explains. *We offer them peace of mind from a cyber point of view, enabling them to deliver their public service mission*". But even so, cybersecurity companies do not enjoy the status of a public

service. They are not required to provide a service that is accessible to all, equal for all and continuously available. "*A public service mission has a very specific definition that is hard to apply to companies in the sector – because it's a service supplied by the State or an organisation acting under State control*, points out Jean-Jacques Latour, cybersecurity expert Cybermalveillance.gouv.fr. *However, the case can be made that cyber companies have a public interest mission in that their role involves countering attacks against a country's citizens or sovereignty*".

A number of French companies exercise just such a mission; for example by joining the ACYMA public interest grouping (GIP), which has been running the cybermalveillance.gouv.fr since 2017. It raises citizen and corporate awareness of cyber risks, assists victims and puts them in touch with providers if necessary. "*Until only recently, there was a gap between key organisations protected by France's ANSSI cybersecurity agency and all other cyber victims (very small businesses, SMEs and individuals), who didn't always know who to speak to,*" Jean-Jacques Latour explains. "*At Stormshield, we joined the ACYMA GIP, along with fifty or so other members, because we believe we're involved in a mission, a collective drive to raise awareness; and this transcends commercial issues,*" Matthieu Bonenfant says. And this role is even more essential given that cyber issues are often viewed as purely technical in nature. The general public – and even companies – are sometimes resistant. "*Cybersecurity is still seen as a constraint,*" Jean-Jacques Latour confirms.

"The case can be made that cyber companies have a public interest mission in that their role involves countering attacks against a country's citizens or sovereignty"

Jean-Jacques Latour
Cybersecurity Expert
Cybermalveillance.gouv.fr

A human rights issue?

But is a public interest group sufficient to continue this mission of raising awareness and providing protection? Should we be considering public cybersecurity companies? Matthieu Bonenfant is dubious. "*A centralised structure doesn't seem like a good idea to me. We need a heterogeneous and diverse ecosystem to maintain agility in developing technologies, he suggests. In addition, a structure of that kind wouldn't provide a Europe-wide oversight of cybersecurity. I believe more in the "national agency" model, like ANSSI in France, which provides support and assistance, and ensures that a viable ecosystem exists, overseeing initiatives such as Cybermalveillance.gouv.fr... rather than a more cumbersome state-run structure.*"

And what about the individual's right to cyber protection? There are certainly calls from NGOs such as Human Rights Watch for cybersecurity to be classified as a human rights issue. After all, some cyberattacks constitute violations of basic rights such as protection of privacy, access to information and even freedom of expression – as the GDPR now shows. Human rights are at stake when Saudi Arabia is suspected of hacking into the mobile phones of journalists and activists, or of their associates.

A "right to cyberprotection" would certainly be difficult to design and enforce, because it would be "*very wide-ranging*", according to Manon Devaux. However, recognition of this fact could in any case drive a growth in awareness of the importance of cybersecurity within companies, and for individuals. •

LONG-TERM **MANAGEMENT**

Managing cybersecurity solutions a job for the long haul

Year on year, cyberattacks are becoming increasingly sophisticated. A long-term response to the ever-evolving threats posed to cybersecurity cannot be provided merely by rolling out a security solution. Before identifying the company's sensitive assets and after performing a risk assessment, there is a vital need to manage cybersecurity solutions as part of the ongoing protection of workstations, servers and networks.

By

Increasingly rapid evolutions in these new threats call for an appreciation of the wider issues involved in cybersecurity. For this reason, the management of cybersecurity solutions is critically important, as it reduces attack surfaces and ensures a high level of protection. After all, there's no such thing as an easy ride when it comes to cybersecurity.

The (correct) implementation of a security solution

An initial phase consists of analysing existing resources and drawing up an accurate inventory of protection methods already in place. Before planning how to implement a solution, it's important to run pilot phases to examine how it performs in the real world. An initial phase is to anticipate anomalies and prevent possible disruptions.

This is followed by the actual deployment (or roll out) phase for the solution. In a perfect world, the solution should be fairly simple to implement. However, some situations are more complex than others: network architecture validation, new security policy, redesign of public key infrastructure (PKI)… and may require **specialist assistance from the publisher**. Here at Stormshield, such requests are handled by our Professional Services team – providing human resources directly on site to fine-tune the configuration of solutions in complex situations.

And make sure you don't forget to tick the **training** box, to ensure you make the most of the solution's potential.

Managing a security solution

Although the first part is often entrusted to standard IS Director/CISO profiles (specifying the security policy and network architecture), this stage applies more to system administrator or IT manager profiles. These are the people who will actually be getting their hands on the product itself. From initial implementation through to managing backups – via regular modifications and problem solving – the scope for intervention is a wide one!

This takes us into the maintenance phase – which

can assume a variety of forms and names. In summary, this covers: **in-service support** (ISS), the aim of which is to ensure that the daily life of the company runs smoothly and any breakdowns are repaired, and **security maintenance** (SM), the aim of which is to maintain the optimal level of security.

Whether in the form of **bug fixes** (as part of the ISS) or **security patches** (as part of the SM), **updates** are crucial, and they must therefore be applied as soon as fixes are available. However, they are not without their drawbacks: in cases where they require the reboot of a system, the result can be temporary production downtime. This is not always acceptable, and sometimes even impossible, particularly in an OT environment.

"*Some updates are automatic, such as antivirus signatures or IPS (Intrusion Prevention System) signatures, and are very regular, with checks made several times a day*, explains Stormshield Support Manager Farid Ichalalène. *Others are manual, requiring the solution itself to be updated: in this case, the frequency is variable, and requires staff to keep abreast of new developments, e.g.: via the RSS feeds provided by the editors, email updates, or regular visits to customer areas. With a non-updated product, the risk is that companies will expose themselves to cyberattacks, believing themselves (wrongly) to be protected. Hence the importance of remaining vigilant and being thorough with updates*". Updates are therefore an essential part of ensuring that systems continue to work correctly over time. "*And the maintenance contract is vitally important, as it governs access to updates and technical support. A security product without security updates rapidly becomes obsolete,*" Farid Ichalalène points out.

Lastly, administrators can find themselves dealing with situations involving anomalies or faults that they cannot resolve on their own. That's when **technical support** – a dedicated point of contact in difficult situations – comes into its own.

It is therefore vitally important for security solutions always to be covered by a maintenance contract, providing access to publisher support (from updates through to technical support, and including **hardware warranties**).

Cybersecurity solutions management tools

When presented in a list like this, all these cybersecurity solution management actions can appear daunting – in terms of their human costs. The key to addressing this concern is to make sure you are fully familiar with the security solutions management tools. The goal: to ensure the best security for your network on both an ongoing and a daily basis.

In cases where a single solution is in place, **the management console** should be easy to learn, and – most importantly – offer easy-to-read everyday dashboards.

However, assuming a pool of different security solutions, it is possible to automate repetitive tasks and, in this way, save time which can then be devoted to the most important tasks, thanks to an efficient **centralised administration system**. To reduce in-service support costs for the network security infrastructure, it is vitally important to optimise the tasks of monitoring, configuring and maintaining security equipment. Here, UX and ease of use become critically important factors.

Solutions management is thus based both on optimal solutions and on the key stages of deployment, maintenance and real-time systems monitoring. A combined solution of this sort will enable a company to protect itself effectively against cyberattacks and take a long-term view of its defence strategy. ●

Why do **updates** pose **a problem** in the cybersecurity world?

October 26, 2020

Ah updates… Those pesky updates, all too often labelled as restrictive. However, these updates exist for our own good. And although it's often difficult to make reasonable IT security choices if these are detrimental to production, updating is something which can't be put off until tomorrow. On the contrary, it should be a central aspect of any company's security policy.

By

Adrien Brochot

Why carry out updates? **Are updates absolutely vital?** Can't they wait for a while? These questions and many others are all too frequently asked in many companies, for whom digital hygiene, IT protection and best practices in the security field aren't always synonymous with updates. And they're not always a priority. For companies, business continuity and production capacities remain their number one priority, with the issue of IT vulnerabilities often taking a backseat.

However, although a company's production must never be brought to a standstill, cyberattacks are not going to stop any time soon either. As long as there are vulnerabilities, there will be attacks. And the updates are needed to patch these vulnerabilities and fend off these attacks! Although their efficiency and importance are well demonstrated, the road to acculturation is a rocky and winding one. Within companies, a combination of urgent priorities and ambivalence ensure that operational requirements are always placed ahead of the fight against the cyber risks inherent to their activities.

Neglected updates and vulnerable systems

The bugs and vulnerabilities in question, which are documented and published by stakeholders in the cybersecurity sector, can range from minor bugs to critical vulnerabilities. And if this information is available to companies, that means the attackers also have access to it… Systems which have not been updated are therefore particularly vulnerable to cyberattacks. "*The attackers use footprinting systems, namely scans of the networks and environments enabling them to identify the machines, to easily and quickly find workstations open to attack, in this case those which have not been updated,*" explains Guillaume Boisseau, from Stormshield's Professional Services Department. There's no doubt that **non-updated systems offer possibilities for attackers to carry out malicious acts**. "*The attackers will particularly develop an in-depth attack on an IT system in the case of old*

systems containing vulnerabilities, which are well-known and exploited by malicious networks," adds Maxime Nempont, Technical Leader for Security Stormshield.

When dealing with non-updated workstations, the Wannacry ransomware perfectly illustrates how vulnerable such workstations can be. In May 2017, this ransomware program was able to spread thanks to a vulnerability in Windows environments, within systems which had not patched the security flaw. However, two months before the attack, Microsoft had published a security patch for this vulnerability and issued a warning concerning its high importance. The final tally: 150 countries were paralysed by the Wannacry cyberattack and the financial losses have today been calculated into the billions of dollars.

Wannacry offers a snapshot of the reality we are still experiencing today: many companies have not yet clearly identified the vital importance of carrying out updates and of doing so as soon as possible to reduce the window of opportunity for attackers.

In May 2019, Microsoft once again published details of a security flaw concerning one of its system components. Baptised "BlueKeep", this flaw could have had the same impact as Wannacry if it had been exploited on a large-scale basis. Although for the time being cybersecurity researchers cannot confirm that BlueKeep has undergone large-scale exploitation by attackers, the risk certainly existed. Because a month after the revelation of the flaw and publication of the patch by Microsoft, almost a million systems were still exposed and vulnerable. All possible entry points to the malware ecosystem…

"*Some companies don't perform updates as they don't have the procedures in place to provide a framework to ensure these are done properly (such as a lack of test environments for example) and so the updates accumulate, and with them the attendant risks. It's a bit like your appointment at the dentist: if you have a check-up regularly, you'll only have a few minor things that need doing each time. On the other hand, if you don't go to the dentist for a long while, things accumulate and get worse. The same pretty much applies with updates!*" explains Guillaume Boisseau.

The spectre of Wannacry appears to loom large on a regular basis: this year, another major flaw linked to the Windows operating system was detected, named SMBGhost. A vulnerability in the same protocol as that used by Wannacry, the exploitation of which could have been catastrophic.

Attacks targeting non-updated systems are on the rise and won't be stopping any time soon. Both simple to perform and well documented, they offer many benefits, of which the attackers are all too aware. **More than ever before, performing updates should therefore be considered a priority by all companies**, whatever the business sector, and should become an ingrained part of any organisation's culture.

Reconciling cybersecurity and imperative operational requirements: between the Holy Grail and the eternal paradox

Updates to software, applications or devices are and will always be the subject of competing pressures, with the twofold objective of guaranteeing security and taking account of the operational constraints inherent to all activities.

Because although updates exist to squash bugs and patch critical vulnerabilities, they can also generate constraints for companies. In industry and operational networks (OT), updates are particularly unpopular as they can generate undesirable effects, such as a prolonged stoppage of production. And even once completed, restarting the system is a critical moment requiring careful attention in the industrial world. Through a rebound effect, unforeseen impacts can result in falling production, which has an adverse ef-

fect on turnover. "*Assessing the need for an update by carrying out a risk analysis and planning this while measuring the impact on production are therefore imperative aspects which should be taken into account in industry,* stresses Florian Bonnet, Product Management Director Stormshield. *For this reason, maintenance cycles must be carefully prepared and scheduled in the industrial world*".

But the constraints are not only found with OT. More generally, updates can result in the company taking a step backwards, with a website becoming unavailable, or in lost time for users who find themselves obliged to restart the equipment and to cease all office software tasks for a certain time. These same updates can also entail constraints due to the components they involve and directly affect software or applications currently under development, to the great displeasure of the developers! – or applications already deployed on the workstation.

So, whether you're the head of a textile production plant, a web developer or a common mortal sat in his office, updates are not particularly welcome, and their deployment can be a source of worry and reticence. The issue of updates is therefore as complex as it is paradoxical.

The question of the updates' impact

So, **should you or shouldn't you update?** To update or not to update? That is the question! And an important one too... According to the operational constraints and working environments (production environments, applications used, etc.), updates can prove be very complex or even impossible. "*Some work is required ahead of an update to be able to determine whether it's likely to affect the workstation or the working environment. For sensitive environments and critical systems for example, it's necessary to envisage a pre-production environment in the event that the updates result in the system malfunctioning – or in changes to the way it works,*" explains Guillaume Boisseau.

You should adopt the principle that in the wonderful world of updates, control procedures and anticipation are the watchwords, including in the case of automatic updates (PCs, tablets, etc.) for which it's also important to be able to check reliability and limit risks. "*In IT, automatic updates can be activated for workstations or office software in as far as they can always be postponed and performed at a more convenient time,*" explains Florian Bonnet. He adds that "*for IT servers or in OT on the other hand, automated updates cannot be envisaged as these are critical systems for which the consequences of updates must be managed in detail*".

Indeed, in some cases it's impossible to perform updates as such, as these require the deployment of high availability architecture – or even digital twins or other forms of virtualisation – to test them. In the OT field, this test environment is therefore vital to be able to assess the risks posed by an update and to avoid disrupting the operational system.

Other scenarios may make it impossible to perform updates, such as "*when an update results in an application becoming incompatible with an old operating system or in the case of systems at the end of their operational lives, for which the update and migration to the new system become excessively costly,*" explains Maxime Nempont. With this in mind, it's not hard to imagine why companies are reluctant to perform updates rather than the reverse – despite the IT security needs. In this case, the publishers play a key role as both advisers and facilitators, to help companies perform their updates and to find a workaround solution when this is impossible. Their goal: **To develop the simplest update systems possible** and to ensure that companies can benefit from these.

But first and foremost, it's the companies themselves who need to understand the importance of updates and their applicability. **Because failing to perform updates means leaving yourself exposed to cyber-attacks**, for which vulnerable systems offer a high-

ly-prized open door to your system.

Developing an "update culture"

Although, overall, companies are increasingly aware of the issue of updates, they may still experience difficulties in evaluating and understanding the risks of failing to implement them. Additionally, not all companies appreciate that they can be the target of a cyberattack. This is the case with OT, in which cyberculture is not yet widely developed. However, as Florian Bonnet reminds us, "*It's not a question of if you're going to be attacked but rather when*," before adding: "*making updates part of the company culture also entails accepting the cyber ecosystem more generally as part of the company culture and then keeping up to date with the latest news…*". Companies therefore need to become more aware of what's at stake, and the publishers are there to help.

'Proof by example' is a method which works quite well in the opinion of Maxime Nempont, who explains that "*you need to take concrete cases, and talk to people about the real-life exploitation of critical vulnerabilities, making them understand that this is not just theory*". As well as raising awareness, the publishers should also provide support through the update process and be very precise when issuing a new patch to inform the client, who must be able to clearly understand whether this is a bug fix or a vulnerability patch. "*The publisher must 'justify' the updates they propose and present the associated risks to reassure the company, because one way or another the customers will always be tempted to prioritise production over everything else*," states Guillaume Boisseau.

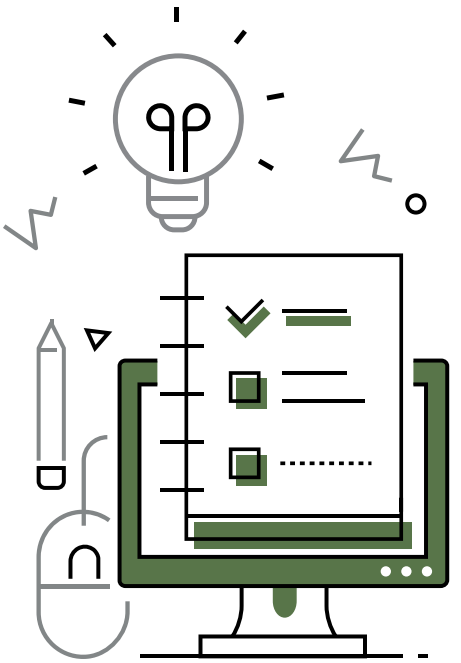
Clear explanations from the publishers are therefore essential for companies to take this onboard as part of their company culture, but more is required too. IT managers also play a key role as part of this process. Indeed, the updates and the related procedures (update frequency, the decision as to whether to activate automatic updates or not, etc.) are the responsibility of the IT departments and must be managed and centralised by them and not by the users. The IT teams are best placed to correctly respond to the issue of updates and to supply the right supervisory resources needed to deploy them.

But some countries have preferred more coercive measures as opposed to the simple provision of information, with an example being the United States, which adopted firm measures when faced with the recent threat of Zerologon – a security flaw affecting Windows servers within corporate networks. If exploited, this vulnerability could enable an attacker to take control of vulnerable machines, and in particular domain controllers. In such a context, the US Cybersecurity and Infrastructure Security Agency has acted firmly: all of the country's governmental agencies must have applied the patch for this vulnerability before midnight on 21 September. To avoid such a situation coming about and to give the provision of clear information a chance of succeeding, the best solution continues to be to focus on making this part of the company culture, helping firms to understand the issue and reassuring them of their ability to remain productive while also adopting the right security measures. ●

A PROCESS FOCUSED **ON THE END USER**

Cyberattack simulations: effective training to counter cyber risks?

May 25, 2020



Inspired by pen-tests or bug bounties, a number of IT departments organise cyberattack simulation exercises to improve awareness among their teams, against the backdrop of fast growing cyber threats. Whether it's to check security measures on the one hand or the digital habits of your staff on the other, is there a benefit in simulating cyberattacks to raise employee awareness?

By

Julien Paffumi

Do you see Jeremy from the marketing team over there? The new guy, who's just joined the team up on the first floor. He looks harmless, doesn't he? Well in actual fact, Jeremy is a highly experienced hacker, recruited by the company manager to carry out an in situ penetration test. He's got free reign to do what he likes, as his co-workers are about to discover. A plot worthy of any thriller, which you can discover in episode 36 of the Darknet Diaries podcast dedicated to cybersecurity, *Jeremy from marketing*. It illustrates a Red Team type internal attack scenario in a company, seeking to lay bare all possible security flaws in order to rate the security level for its infrastructure and networks.

More and more companies are today proposing pen-test services and simulations for employees. Including role-playing, "live my life" exercises and simulated cyberattacks, immersive solutions are becoming mainstream when it comes to developing cyber culture within businesses. For some IT departments, the question is the following: whether it's to check security measures on the one hand or the digital habits of your staff on the other, is there a benefit in simulating cyberattacks to raise employee awareness?

50 shades of intrusion tests

Using pen-testing or bug bounty solutions, attacking a product or network infrastructure to test its stability or security is a common practice in the cyber world. Frequently, companies which have attained a certain

level of maturity in the field of cybersecurity use external service providers to stress test their protective measures. "*In the case of "black box" pen-testing, the designated person will have access to the same data as in real life situations and will seek to attack the network from outside*, explains Adrien Brochot, Product Manager Stormshield. *The other possibility is to give him access to the code and the rules for the data flows, enabling him to try and overcome the protective measures by rereading the code. This is then referred to as 'white box' pen-testing*".

For larger companies or organisations with a more mature cyber profile, it's also possible to organise Red Team vs. Blue Team type simulation exercises. Here, the Red Team's task is to test the security level of a company, an IT network or an item of equipment via hacking techniques while the Blue Team seeks to defend itself. In June 2019 for example, the French armed forces ministry took part in such a simulation exercise, the purpose of which was to anticipate enemy action. This type of cyberattack simulation is intended to identify a company's weaknesses. To make the exercise all the more effective, it's also possible to plan on the inclusion of a Purple Team, given the task of interacting regularly with the defence and attack teams. And for the purists, to create a more complete perimeter we should also mention the Yellow Team, Green Team and Orange Team – all part of the BAD pyramid.

For the intrusion tests, the attack surface is defined beforehand between the company arranging to have its infrastructure tested and the service provider chosen to perform the pen-test. "*As an example, we'll try to attack a web server online or to send a phishing email*, adds Paul Fariello, Security Expert at Synacktiv. *We can also create tailored scenarios in which we send a person onto the site to try and enter the company's premises and to plug in an external peripheral such as a USB flash drive*". To achieve this, an initial social engineering phase is often required. And unfortunately is often effective.

Setting traps to improve awareness

A recent IBM study mentioned in the Usecure blog stresses that **human error is the source of 95% of in-company security breaches**. In other words, successfully managing the human factor can eradicate most breaches, in a context in which perimeter security alone is insufficient and in which each individual can become an attack vector. In France, in 2017, 30,000 staff from the ministry of the economy in finance fell into a trap… set by their own IT systems security department. The department's objective was to make these staff aware of the risks of phishing. They certainly succeeded!

As a direct consequence, more and more IT departments appear to be using pen-testing to raise awareness among staff of cyber risks. Why? To place them in a cyberattack situation to better educate them and help them learn to manage the potential consequences. In June 2019, during the G7 meeting, 24 financial authorities from the seven member countries were invited to take part in a major exercise to gain a better understanding of the extent of cross-border cyber risks to the financial sector.

"*Let's not forget that these operations take a long time to organise and are costly*," explains Adrien Brochot. But if the organisation of such cyber crisis exercises are outside the means of just any small business, IT systems security managers may nevertheless decide to use a modest version of the Red/Blue/Purple Team role-playing games. For a more accurate simulation, it's preferable that the departments handling the defence side should not be aware of the exercise. "*It's possible to come up with different situations according to the department concerned. Someone from HR can be tested without their knowledge to check that they have provided the necessary protection for a file containing personal data. Other departments will then try and access this file using different methods, whether technical or social*," explains Adrien Brochot. The key challenge for the IT systems security manager is then to highlight the parallels

between the simulated cyberattack situation and the main principles of IT security, such as the protection of passwords or basic protective rules to be applied when dealing with suspect emails. During the simulation carried out at the French finance ministry, the staff trapped by the phishing email were shown a webpage containing recommendations on the use of emails and the precautions to be taken, as explained by Yuksel Aydin, the IT systems security manager who managed the exercise, in the French newspaper *Le Figaro*.

The simulation boom

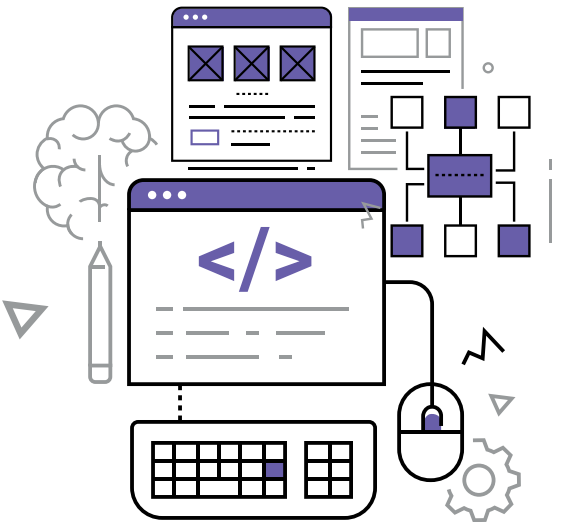
"*A good simulation is certainly worth a thousand PowerPoint training presentations,*" adds Paul Fariello. The challenge is to successfully **combine the pen-test or role-playing exercise with an effective message to raise cyber awareness**. "*It's therefore very important to take the time to review the exercise in a more general context, and to retrace the cyberattack point by point to learn all possible lessons,*" he continues. "*And even to run through the simulation again several months later to check if staff behaviour has changed and if the precautionary measures to be taken when facing such attacks have been fully understood,*" concludes Adrien Brochot.

> **"A good simulation is certainly worth a thousand PowerPoint training presentations"**
>
> **Paul Fariello**
> Security Expert at Synacktiv

As an example, the company IBM certainly sees the value of focusing on awareness-building in companies. In the summer of 2019, the supplier criss-crossed Europe and gave company managers a 'free' fright by showing them cyberattack scenarios, partially to encourage them to sign up to its paid training courses. And to remind them that there are ever more simulation service providers now that cyberattacks have become part of the day-to-day reality for all companies.

In previous articles we discussed several ways to successfully instil an effective and resilient cybersecurity culture in companies: from teaching cybersecurity in schools, to making staff liable for their acts. And so, with most IT departments still looking for the best way to raise awareness in 2020, we can bet that simulation exercises of various kinds could soon become part of their arsenal. •

The key role played by UX in cybersecurity



December 23, 2020

Maybe we should be viewing cybersecurity not as a restriction, but as a regular habit. However, if we expect the user sitting between the keyboard and the chair to become a strong link in the digital health chain, we need to provide them with tools that make them enthusiastic about this role. And UX can make this an area in which companies can make a difference.

1993 is the date when the concept of user experience was born. Its godfather was Don Norman, who "*wanted to cover all aspects of the person's experience with the system*". The whole approach behind this concept is to give users a desire to appropriate a tool, assimilate all aspects of it and derive benefit from it. This "User eXperience" (UX) can now be applied to any area, and is of particular interest in companies' digital strategies. When used to promote effective cybersecurity, UX can prove to be a real asset, reinforcing a company's defensive approach and its employees' digital confidence.

By

Julien Paffumi

Successful cybersecurity also involves UX

UX is not solely an issue for the end user. It is equally important for administrators to adopt and take ownership of a product. We should therefore identify two main groups of UX beneficiaries in the cyber world: the technical user (administrator) and the end user. "*There are interfaces for administrators and interfaces for business. In both cases, the goal of the UX is to ensure they can be used by everyone – remaining simple for an average user and more complex for an expert,*" explains Sébastien Viou, Cyber-Evangelist Consultant Stormshield. An administrator will need a security solution with a good UX to make it easier to administer agents within the IT equipment pool, implement security policies and monitor events. Another key cybersecurity point: a good UX will help the administrator to reduce potential configuration errors for security tools – which immediately become vulnerabilities for the company. And in terms of the end user, the UX must make it easy for them to appropriate a product, understand it and want to use it;

and there are even times when the experience should simply become "transparent". We should therefore be promoting a cybersecurity approach that uses the UX, taking into account the reality of the user requirements on which it is based.

The UX is also assuming an increasingly important role in the design of cybersecurity solutions. And, as Guillaume Poupard, Director General of the ANSSI cybersecurity agency, stated in 2018: "*You have to make digital security sexy; in other words, understandable.*" "*You need to understand what you are trying to secure, the threats you're dealing with, and the resources you have, and you need to involve people who are not part of the cybersecurity inner circle.*"

> **"You have to make digital security sexy"**
>
> **Guillaume Poupard**
> Director-General of the ANSSI

Cyber-user-friendly: bringing sexy to cybersecurity solutions

Cyber culture and UX are really the same thing. An effective cyber culture is a culture that provides for the adoption of security solutions by employees according to their sensitivity. Publishers must take this requirement into account in the design of their products and develop them by adopting a business approach, rather than a technical one. Technology is a resource, but the UX must be built around an understanding of users' day-to-day lives. So how can we make these products more '*user-cyber-friendly*'? The cyber community and publishers are working towards this goal, and a number of initiatives are already in place.

UX design sessions have started to appear, enabling publishers to work with partners and customers to challenge their solutions. The goal underpinning this approach is to be able to refocus or refine a product during its design, or improve an existing product, to ensure it is efficient and intuitive to use. These sessions are intended to develop a user interface that is more in tune with its users' business activities and needs. "*Before we develop graphical interfaces for our Stormshield Data Security solution, we develop mockups that we test on a panel of users*, explains Jocelyn Krystlik, Business Unit Data Security Manager Stormshield. *The idea is to bring together people who are cybersecurity product customers, and other people who aren't, to challenge the publishers*".

UX testing is also in widespread use. The aim of this procedure is to present users with a solution in real time and analyse their reactions to the product. This makes it possible to determine whether the solution is intuitive or not, and adjust it as needed. Some publishers also provide collaborative platforms on which their customers are encouraged to test products and share their feedback and comments. Virginie Ragons, UX/UI Designer Stormshield, believes that "*security solutions are generally found at the heart of complex ecosystems, and the goal is to provide users with harmonised interactive working practices and an intuitive interface in order to facilitate the achievement of the original objective*".

Another key issue of publishers in the age of UX: getting the pre-configuration of their solutions right. To what end? To avoid the old mistake of overloading interfaces with options that will not be used, and to identify in advance what will be used the most, and make it more prominent in the solution. This stage is critical, because the way publishers design an interface guides user choices.

Kaspersky claims that more than 90% of security incidents are attributable to human error. Suffice it to say that for successful cybersecurity, the last word on security products' UX should go to the user. And that user, it seems, should also have the last word on trends, with changing usage habits and therefore a design that should evolve accordingly, as Sébastien

Viou points out: "*20 years ago, it was all done via the command line. After that, security solutions took the form of fat clients, and now the trend is towards thin clients, with aesthetic interfaces. UX is following the general evolution of the web itself*".

Cybersecurity and UX: the key trends

By moving towards thin clients, and even devices with no agent at all, it is possible to adapt to new uses such as digital nomadism and the widespread use of teleworking. "*At Stormshield, we have applied this agentless concept with our data encryption solution, which can now be used directly from the browser. We now refer to Agentless Encryption in our Stormshield Data Security product*, Jocelyn Krystlik explains. *Because data encryption is an important issue that can affect a wide range of people within a company, it is vitally important to have the right solutions to support these groups and teach them how to use them*".

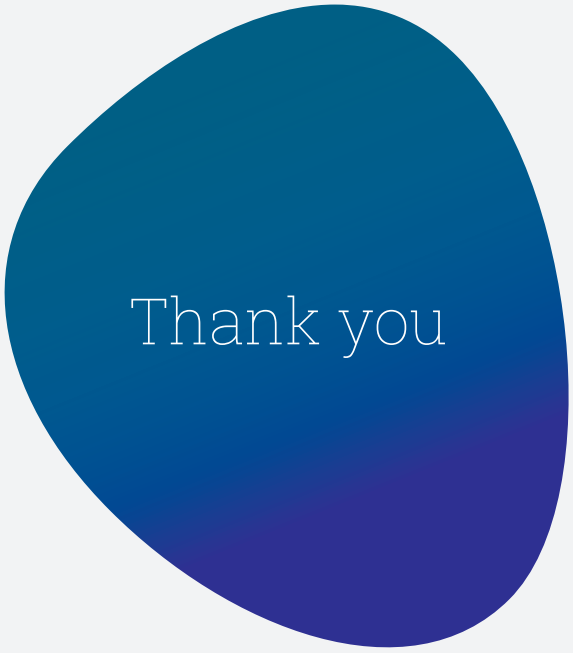
Employee empowerment is another key trend in UX. End users will be increasingly called upon to play a role in delivering security within their organisations. There is a tendency for the concept of cybersecurity to be extended to cover all business areas, and not just technical departments. All users must be able to play a role in this area. And here again, UX becomes a key component of digital hygiene: the right tools are required to support this trend. For example, UX needs to provide administrators with efficient, traceable methods of collecting and reporting information. Meanwhile, end users need to be able to supply information, most importantly to administrators. And indeed, they may need to be given a bigger role in making the security-related decisions that have in the past been the preserve of technical departments.

"The goal is to provide users with harmonised interactive working practices and an intuitive interface in order to facilitate the achievement of the original objective"

Virginie Ragons
UX/UI Designer Stormshield

UX therefore has many qualities, and there is a strong benefit to incorporating it into corporate cybersecurity and digital transformation strategies. Furthermore, an increasing number of cybersecurity companies are publicising UX and the key role it plays in their products. For example, the Hypori company has breathed new life into its security solution for mobile devices with the help of UX. Or the Callsign company, which has developed an authentication solution entirely designed by and for users.

Interfaces with a simplified, intuitive design, fewer operations for users to perform, more appropriate architectures... UX? Definitely a cyber trend to follow. •


Thank you

Here, then, is a retrospective of 2020 – a highly unusual year. But looking ahead, what are our plans for 2021? We will continue our efforts to create content… text, video and audio. If you want to get involved, or just submit ideas for topics, it couldn't be simpler: just contact our Marketing team!

And regarding the visibility of this content, you will also have a vital role to play. By sharing the content around you that interests you, you'll be helping us to reach a wider audience… and at the same time, playing your part in increasing awareness of digital hygiene and cyber risks.

Table **of contents**

Subjects

Contributors

Adrien Gendre, *VadeSecure*

Alain Dupont, *Stormshield*

Alice Louis, *Cabinet Dicé*

Anthony Di Prima, *Wavestone*

Benjamin Leroux, *Advens*

Charles Blanc-Rolin, *APSSIS*

Davide Pala, *Stormshield*

Denis Boudy, *ScredIn*

Dominique Allietta, *Stormshield*

Édouard Simpère, *Stormshield*

Fabien Miquet, *Siemens*

Fabrice Epelboin, *Entrepreneur*

Fabrice Tea, *Schneider Electric*

Farid Ichalalène, *Stormshield*

Franck Bourguet, *Stormshield*

Franck Gicquel, *Cybermalveillance.gouv.fr*

Franck Nielacny, *Stormshield*

Frédéric Boissel, *Airbus CyberSecurity*

Gérard Leymarie, *Elior*

Grégory Baudeau, *Airbus CyberSecurity*

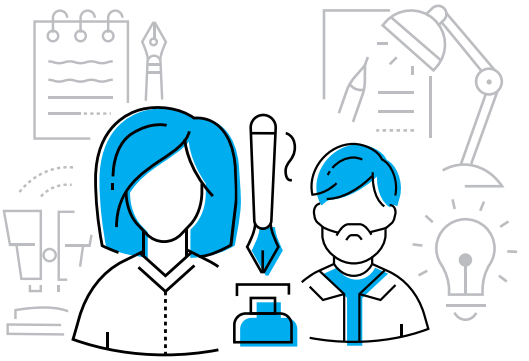
Guillaume Boisseau, *Stormshield*

Jean-Jacques Nillès, *Socrates*

Jean-Christophe Mathieu, *Orange Cyberdefense*

Jean-Jacques Latour, *Cybermalveillance.gouv.fr*

Jocelyn Krystlik, *Stormshield*



Manon Deveaux, *TECH IN*

Markus Braendle, *Airbus CyberSecurity*

Mathieu Demont, *Siemens Smart Infrastructure*

Nebras Alqurashi, *Stormshield*

Paul Fariello, *Synacktiv*

Philippe Blot, *ENISA*

Philippe Sanchez, *Socrates*

Raphaël Granger, *Stormshield*

Tarik Zeroual, *Stormshield*

Thierry Franzetti, *Stormshield*

Thierry Hernandez, *Stormshield*

Thomas Gendron, *VadeSecure*

Vincent Riondet, *Schneider Electric*

Virginie Ragons, *Stormshield*

Stormshield **warmly thanks all the contributors** for their participation.

STORMSHIELD

Around the world, companies, government institutions and defence organisations need to ensure the digital security of their critical infrastructures, sensitive data and operational environments. Stormshield technologies are certified and qualified at the highest European level to meet the challenges of IT and OT and protect their business activities. Our mission: to give our clients peace of mind concerning cyber risks so that they can concentrate on their core business, which is so crucial to the smooth running of our institutions, our economy and the services provided to people. Choosing Stormshield means opting for trusted European cybersecurity.

www.stormshield.com