



Federal Office
for Information Security



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



Third edition of the Franco-German common situational picture



Influences of COVID-19 on the IT-security situations in France and Germany

Information technology (IT) has become an integral part of our modern life. IT enables everyday activities and governments, critical infrastructures and the broader economy are highly dependent on it. Therefore, confidentiality, integrity and availability of IT has become a necessity and precondition for our modern and interconnected world to run smoothly.

When the World Health Organization (WHO) assessed on 11 March 2020¹ that COVID-19, the infectious disease caused by the Coronavirus SARS-CoV-2², could be characterized as a pandemic, this also caused major impacts on the national and international IT security situation. In a pandemic, more than ever people's lives are at stake and every available resource counts. Notably, disruption of healthcare facilities, which were under tremendous stress to address COVID-19 patients' needs, would have had a dramatic impact. Cyber-attacks on the wider IT supply chain underpinning healthcare actors, products and services could also have resulted in major effects on our ability to cope with the pandemic properly. Moreover, this targeting of the supply chain is an increasing threat in the ever-growing context of outsourcing of services and infrastructure.


Both the French National Cybersecurity Agency (ANSSI) and the German Federal Office for Information Security (BSI) have furthermore expected a rapid shift in the attackers' focus, especially in the cybercrime domain, towards the exploitation of the overall uncertain situation. This expectation was further aggravated by a continuing sophistication and professionalization in the cybercrime domain even before the COVID19 pandemic. As for cybercrime activity, ANSSI and BSI have been observing a growing trend of highly sophisticated professionals working in what has now become a very specialized and structured cybercriminal ecosystem in conjunction with a shift towards an opportunistic targeting of high-value targets, who are capable of paying large ransom demands, also called "Big Game Hunting". This overall trend enabled criminals to spend less time on adapting their tools in order to leverage the COVID19 pandemic and more time on targeting and attacking vulnerable IT systems and connections.

ANSSI and BSI recognize two major types of threat actors in the current cyber-threat landscape. These are state or state level actors, which mainly focus on cyberespionage, destabilisation or sabotage on the one side, and cybercriminals who operate with a financial motivation and are responsible for the greater majority and volume of attacks on the other side. The delivery vectors of malware mainly observed remain as of today e-mails, whether as spam, phishing or spear-phishing.

The significant increase of remote working – resulting from the need of physical distancing in both countries – led to a substantial growth of the attack surface in terms of interconnecting services and hardware provided and used. This trend consequently facilitated the possible exploitation of security flaws for cybercriminal campaigns. Beyond the exploitation of people's fears and uncertainties, the lack of cybersecurity awareness of the victims as well as the new uncharted setting for system administrators, particularly successful cybercriminal campaigns were observed in 2020, if not in sheer volume at least in terms of financial losses.

1 <https://www.who.int/news-room/detail/29-06-2020-covidtimeline>

2 <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses>



Finally, ANSSI and BSI note a trend that constitutes a recognizable aggravated cyber risk for the foreseeable future. The digitalisation of production processes underpinning the core activity of an entity, through the connection of operational technology (OT), will carry risks for the near future. Those OT systems have usually a long life cycle and are expensive. Hence, they are not changed or upgraded on a regular basis. Therefore, ANSSI and BSI have to assume that most of the currently working OT systems were installed at a time when IT security was not recognized as a vital factor for the operation of OT systems.

It is against this background that ANSSI and BSI took proactive actions towards their constituents to limit the risk and potential negative consequences both during and after the COVID19 pandemic. Even if the IT security threat landscape is ever evolving, those actions were and are still driven by the basic principles of cybersecurity: ensure confidentiality, integrity and availability of an IT infrastructure. Those principles are complemented by wider information assurance measures like robust risk analysis, awareness raising campaigns, adhoc communications and normative productions.

In this third edition of the Common Situational Picture (CSP) the focus lies on the different actions undertaken by ANSSI and BSI in the context of COVID-19. To do so, the following report goes through the impact that the COVID-19 pandemic may have had across healthcare, government and civil society, and the response measures, which were taken to cope with it. In order to reflect the different approaches, respective risks foreseen and to allow for a comparative approach, each agency presents its view separately. At the end, ANSSI and BSI will draw a common outlook on the IT security situation at hand.

Taking into account the official assessment of COVID-19 as a pandemic by the WHO, this CSP will primarily highlight the timeframe from March 2020 to September 2020. Where applicable, events outside this scope will also be included. While writing this report, the pandemic is still ongoing. Therefore, not every event can possibly be considered for this joint work of ANSSI and BSI. Furthermore, it should be noted that for ongoing events details might still be developing.

Insights from the BSI

Healthcare

Critical Infrastructure

IT security in critical infrastructures is regulated by the ordinance for critical infrastructures (BSIKritisV)³ in accordance with the Act on the Federal Office for Information Security (BSIG)⁴. Healthcare is hereby one sector of critical infrastructures according to the BSIKritisV. When such facilities reach certain thresholds defined in the BSIKritisV, they have to comply with specific requirements defined in BSIG.

As mentioned in the introduction, in a pandemic every available resource even medical laboratories or hospitals, which normally would be too small to fall under existing regulations, becomes vital. Incidents that normally could be compensated would then put additional stress on an already strained complex ecosystem of critical infrastructures in the healthcare sector. Therefore, together with trusted partners, BSI started in March 2020 to advise the healthcare sector in Germany in a broad fashion, warned against potential risks and issued recommendations on how to deal with them. In doing so, BSI was additionally able to deepen its understanding of the aforementioned complex ecosystem and its internal dependencies.

Released Studies

In June 2020, the results of two studies commissioned by BSI before the pandemic on the current state of IT security in medical laboratories and hospitals in Germany were published⁵. These studies considered organisations above as well as below the thresholds defined by the BSI-KritisV. The studies were intended to identify relevant processes of critical services provided in the healthcare sector as well as the status of IT security in medical laboratories and hospitals within Germany, which form branches in the healthcare sector in accordance with BSI-KritisV. Furthermore, recommendations for raising the level of protection against cyber incidents were provided and an outlook on the future of digitalisation in both branches was given.

In general, the studies concluded that German medical laboratories and hospitals are well protected against cyber-attacks and outages of their critical services. The studies showed furthermore that technical preventive measures are predominantly implemented in a sound fashion while there is still high demand for organisational protective measures especially in hospitals. For example, the systematic risk management has not yet been implemented on the required level in various hospitals considered by the studies.

Legislation

In order to improve investments in hospitals – including for their IT security – the German Federal Parliament passed in September 2020 the law “Krankenhauszukunftsgesetz” (KHZG). The KHZG came into effect in October 2020 and aims to provide 4.3 € billion in funds in total for hospitals. The fund “Krankenhauszukunftsfonds” (KHZF) is composed by 3 € billion from the federal government and another 1.3 € billion from the federal states. Among other things, the law supports investments in modern emergency

³ The ordinance is called BSI-Kritisverordnung (BSI-KritisV).

⁴ The act is called Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG).

⁵ https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/KRITIS_Studien_300620.html

capacities and an improved digital infrastructure. As an orientation, in Germany hospitals are financed by a dual financing system. The federal states cover the investment costs of the hospitals like construction and equipment. The health insurance funds and self-paying patients finance the actual costs of treatment and therefore the operating costs of the hospitals.

Every investment supported by the KHZG is required to set 15 % of the funds aside for measures to improve IT security. These 15 % are mandatory, because IT security is an integral part of digitalisation and it needs to be considered from the start through every phase of a digitalisation project. The state of digitalisation in hospitals in Germany will then be evaluated until 30 June 2021 and a second time until 30 June 2023.⁶

Ransomware attack on university hospital

IT security in German hospitals is in a relatively good state, as also shown by one of the aforementioned studies. However, one German university hospital became victim of a major incident in September 2020. The hospital treats around 50,000 inpatients and around 300,000 outpatients per year. It is therefore above the defined thresholds according to the BSIKritisV and hence considered as critical infrastructure.

On 10 September 2020, a cyber-attack with a ransomware was detected. Multiple central servers were affected by the ransomware known by the name DoppelPaymer. Following the outage of services provided by those central servers, the hospital was forced to close its accident and emergency department, cancel operations and other medical treatments. An investigation by the responsible law enforcement agency is still ongoing at the time of writing this report.⁷

More generally, the cybercrime actors commonly associated with the use of DoppelPaymer are known to steal data before an encryption of target hosts. This stolen data is then threatened to be leaked to the public, which increases the pressure on the victim to pay a ransom demand by the attackers. This strategy has become a norm in recent months and will be highlighted in more detail later in the chapter on Civil Society. In the given case, an exfiltration of data can so far neither be confirmed nor dismissed.

The ransom demand left behind by the perpetrators in this concrete case was addressed to a different institution, which led to the assumption that they falsely attacked the university hospital. Considering this possibility, German law enforcement contacted the attackers and informed them about their actual victim. According to the Ministry of Justice of the state of North Rhine-Westphalia⁸, the attackers handed over the necessary decryption keys, likely after realising their mistake. With backups and the decryption keys at hand, the university hospital started to rebuild their IT infrastructure. After 13 days, the hospital was able to provide emergency services again on 23 September 2020.

Lessons learned

In summary, it can be stated that the overall threat level for a cyber-attack on the healthcare sector has not risen above levels observed before the COVID-19 pandemic. However, the consequences of a successful cyber-attack have to be differentiated from this assessment since they highly depend on various factors like the availability of redundant emergency capacities, the general preparedness for a cyber-attack or the current state of the COVID19 pandemic. BSI and its trusted partners will therefore continue their work of observing, warning against and counteracting any cyber-threat for the healthcare sector in Germany.

6 <https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz.html>

7 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

8 <https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3855.pdf>

Government

Rapid pace of change

The pandemic confronted government, society and economy alike with an unprecedented sense of urgency to adapt to this new situation. Very quickly, digital solutions became pivotal in every area of life. It should however be noted that in large parts, the need for digital solutions is not a recent development. Digitalisation is an ongoing process in our current information age. Nonetheless, the pandemic did not allow for any further postponement of using digital solutions like for example remote working. Looking back on the last few months, the pandemic can undoubtedly be considered as a catalyst for the digitalisation process in Germany.



Remote working in home office has grown significantly in the COVID-19 pandemic.

From an IT security standpoint, BSI sees this digitalisation process as an inevitable necessity in order to deal with the ever-changing requirements of our daily life. However, the rapid pace by which digital solutions were implemented in the last few months presents risks for IT security. In general, the weakest link in regards to IT security in a digitalised process has to be seen as sufficient to compromise the whole process and potentially the infrastructure attached to it. Because of the aforementioned unprecedented sense of urgency to adjust to the situation, priority was given to the aspect of operability of such processes. In the worst-case scenario, IT security is then seen as an obstacle. To prevent and counteract this worstcase scenario, BSI positioned itself on every available channel with guidance and recommendations on how to deal with the need for digital solutions, the need for IT security and how to consider both these aspects in parallel.

Support and situation monitoring activities

To name an example, in the pandemic physical distancing is one of the elemental measures to limit the spread of COVID-19. This fuels among other things the need to work and keep in touch remotely. To enable citizens to fulfil that need in an IT secure manner, BSI published a set of recommendations and warnings in early April 2020.⁹

⁹ https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Sicher_vernetzt_Corona_070420.html



Aside from recommendations adapted to different stakeholders like government officials, operators of critical infrastructures and citizens, BSI took reasonable precautions in order to keep track of the evolving situation and warn about potential risks accordingly. To achieve that goal, BSI intensified – especially in the early months of the pandemic – its situation monitoring and assessment. This intensification entailed a shift of resources towards monitoring and tracking on the one side and an extensive exchange with trusted partners, domestic and foreign alike, on the other side. Especially this exchange enabled BSI to comprehend and assess the vast number of developments happening simultaneously.

Tracing App

Another measure to limit the spread of COVID-19 were the so-called COVID19 tracing apps that many different countries in Europe and beyond started to develop in spring 2020. BSI supported this process for the German “Corona-Warn-App” (CWA) right from the start in a consultative manner to ensure the highest degree of IT security possible.¹⁰

Civil Society

Uncertainty due to a crisis situation

As mentioned in the introduction, BSI expected an exploitation of the overall uncertain situation caused by the COVID19 pandemic. In such circumstances, affected entities and organisations such as the general public or businesses experience a natural need for information and guidance on how to deal with the situation at hand. Experiences from the past show that adversaries exploit this natural need ruthlessly and immediately. The experiences gained so far in the COVID19 pandemic confirm this assessment once more. The significant difference between other crises and the COVID-19 pandemic is the sheer scale on which civil society, critical infrastructures and governments have been affected worldwide. In the wake of the pandemic, nearly every aspect of daily life was turned on its head. Questions like how to protect oneself against the virus, how to work and learn remotely or which official restrictions currently apply were raised. In regard to questions about digitalization, BSI published recommendations targeted for example at citizens¹¹. Nevertheless each of these questions raised, offered thereby also an opportunity for adversaries to exploit them.

Exploitations

For example, BSI observed fraudulent websites mimicking official websites or presenting themselves as a trustworthy service. The fraudulent intentions extended from offering products in high demand like personal protective equipment (PPE), collecting personally identifiable information (PII) to the distribution of malware. In one prominent case in Germany, websites tried to lure in applicants for the COVID19 relief funds. The presumptive target was to collect PII that the applicant has to give in order to receive a payment form one of the COVID19 relief funds. The PII could then be used for fraudulent claims against one of the relief funds or for other kinds of identity theft. – Especially in the case of identity theft, an underground market exists on which the collected PII could be sold for profit.

To raise the likelihood that such fraudulent websites are considered as authentic and trustful by potential victims, multiple strategies are used. Those strategies consist for instance in a professional web design, a trustworthy domain name and a search engine optimization to name a few. In order to limit the impact of those fraudulent websites, BSI and its partners as well as law enforcement agencies were even more on

10 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Corona_Warn_App_160620.html

11 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Sicher_vernetzt_Corona_070420.html

the lookout for suspicious domain name registrations and reports for example from the general public. When necessary and applicable, website takedowns were initiated.

E-Mail campaigns

On a much greater scale than bogus websites, BSI observed e-mail campaigns aimed at phishing as well as the distribution of malware that abused COVID19 as a subject of interest to entice a recipient to interact with the e-mail content. Some of those e-mails pretend for instance to provide information on the current state of the pandemic or try to mimic contractual partners that need to change their business operations because of COVID-19 or impersonate health authorities like the WHO. As manifold as the impacts of COVID-19 are, so diverse are also the ways adversaries try to exploit them.

In general, when BSI detects such e-mail campaigns or fraudulent websites, it warns the relevant target audiences like for example affected critical infrastructure sectors against the specific threat at short notice. Since the beginning of the pandemic, BSI has observed that the modus operandi applied is not inherently new and does not amount to a significant shift in the overall threat landscape. Nevertheless, over the last few months, BSI tracked a trend in ransomware attacks that is not caused or necessarily connected to the pandemic itself. This trend makes use of encryption and data exfiltration as a dual approach.

A general ransomware trend

In 2019, only some cases were observed that made use of encryption and the threat to leak exfiltrated data to the public. This modus operandi was then picked up in early 2020 by more and more cybercrime groups and has now become the “new norm” in ransomware attacks. When attackers are able to encrypt central servers, network shares and client systems, they will most likely be able to steal data from those systems. In a multitude of ransomware attacks in the last months, that BSI is aware of, exfiltrated data was threatened to be released to the public. Multiple cybercrime groups even operate dedicated leak-sites only for this purpose. By doing so, the victim is confronted with a disruption of its operations, encrypted data and the risk of publication of the latter one. Since attackers carried out their threats of publication of exfiltrated data in the past, those threats have to be considered as serious.


This dual approach from cybercrime groups is with a high likelihood a modus operandi that will also be used in the future. Nevertheless, BSI discourages the payment of any ransom demand since that fuels cybercrime activities overall. That is why BSI revised its evaluation and outlook on advanced cyber-attacks in June 2020¹².

Reliability of the internet infrastructure

Aside from BSI’s prediction about a shift in the focus of adversaries towards exploitation of the uncertain situation, a widespread concern was the reliability of the internet infrastructure under a rising workload fuelled by the effects of the COVID19 pandemic. An unprecedented number of people were expected to use remote working, video conferencing, streaming and online gaming. To comprehend the effects of COVID-19 on the internet infrastructure in Germany, BSI took a closer look on publicly available data for Internet Service Providers (ISPs) and Internet Exchange Points (IXPs) in April 2020.

The analysis confirmed the expected change in making use of the internet for example in regards to video conferencing. Similarly, the internet usage by time of day as well as the overall internet traffic volume changed. The raise in internet traffic volume is apparent at multiple IXPs. Nevertheless, the experienced growth did not exceed the scheduled capacities and therefore did not pose a risk for a failure of the internet infrastructure due to an overload scenario.

12 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.pdf



In Germany, the effects from the perspective of users of the largest ISPs were marginal. The internet latencies remained almost unchanged. Only the download speeds were partially lower compared to data before the pandemic¹³. Overall, BSI concludes that the internet – especially in Germany – handled the changed demands very well.

13 BSI's findings were also confirmed by another independent analysis: <https://www.zafaco.de/de/unternehmen/aktuelles/artikel/news/detail/News/das-deutsche-festnetz-in-der-corona-krise-eine-analyse/>

Insights from the ANSSI

Healthcare

The healthcare sector and its facilities have multiple cyber risks inherent to their nature. Firstly, their activity is critical per se as with regard to the preservation of life and as such to the Nation itself. Secondly, the patient information they handle is highly sensitive: whether as per patient/doctor confidentiality or as per the General Data Protection Regulation of the European Union (GDPR). Thirdly, the inherent costs of acquiring and operating expensive medical systems within the context of constrained budgets pushes the facilities to extend the life of the systems beyond the software providers' maintenance support period. In the context of digitalisation, such connected systems do then become an inherent risk in terms of cybersecurity, and also, by extension, in terms of impact on the continuity of activity of hospitals or laboratories.

French framework

Healthcare facilities are under the oversight of the Ministry for Solidarity and Health¹⁴ (MSS). As such, some facilities were declared by the ministry as Critical Infrastructure Providers (CIP) by decree in 2008. This physical security framework was further enhanced by a cybersecurity facet in the Military Programming Law (LPM) of 2013. This enhanced framework evolves around a risk assessment and a set of ensuing security measures at both operational and organisational level. The risk assessment approach is considered more flexible than a pure regulation as it can be adapted without further legislation to the evolving cyber threat landscape and its *modi operandi*. The LPM of 2013 was later further enhanced by the European Union with the Network and Information Security directive (NIS directive) and designation in France of Operators of Essential Services (OES).

Critical operators are highly encouraged in their risk assessment to use ANSSI's Ebios Risk Management methodology. This methodology inherently requires the entity to take into account questions relative to supply chain management. Indeed, following this framework, operators not only assess their own vulnerability to cyber-attacks, but also the cybersecurity maturity of their suppliers and customers, thus assessing the impact a cyber-attack could have with regard to their own continuity of operation. Finally, the methodology being conducted by the operator itself ensures an intimate knowledge of critical assets necessary to its functioning.


A textbook case: the ransomware attack against the University Hospital of Rouen in 2019

On 15 November 2019, the University Hospital¹⁵ (CHU) of Rouen in Normandy was compromised in a ransomware attack.

While the attack succeeded, the fact that the hospital had a dedicated Chief Information Security Officer (CISO) and that it had a few months earlier updated its computer incident response procedure helped mitigate the incident in terms of activity. The updated procedure ensured reflex actions such as cutting access to Internet and the internal network, identifying and segregating uncompromised part of the IT

¹⁴ Ministère de la Santé et des Solidarités

¹⁵ Centre Hospitalier Universitaire (CHU)



like the backup data storage. The quick escalation into the highest IT incident response level mirrored the severity of the attack as demonstrated by the fact that emergency treatments had to be rerouted to other healthcare facilities. The remediation was further helped by the constitution of a cyber crisis cell for coordination and the keeping of an incident logbook. While the former, with four dedicated staff, helped absorb the increasing workload and efficiently coordinate, the latter was also precious in terms of information sharing during the incident and later to identify lessons learned during the post mortem of the attack.

Although the hospital already had a robust cyber incident mitigation procedure, its staff, on top of being helped by previously contracted IT suppliers, were in close coordination with and benefited from the support of both the MSS' CISO and active support from ANSSI. According to the CHU's CISO testimony, being transparent in its communication of the situation to the patients, the public and the health authorities also proved beneficial.

Lessons learned

The cybersecurity awareness campaigns provided by ANSSI and by the MSS in the case of healthcare facilities helped the Rouen CHU to be better prepared for this contingency. Yet the feedback from this attack helped underline improvement areas that are consistent with problems encountered by other healthcare facilities in France.

Consequently, following the attack, the MSS with the help of ANSSI took proactive measures to identify a set of common and shared issues relating to cybersecurity in healthcare facilities and to devise a global program to improve cybersecurity of hospitals.

Healthcare sector during the COVID-19 confinement

Traditional healthcare operators: hospitals

As stated in the preliminary presentation of France's framework, normative actions were already taken so as to secure its healthcare critical operators as well as initiate a far-reaching program of shoring up the cybersecurity of other healthcare facilities following the attack against the Rouen CHU. It is within this context that the pandemic and subsequent general confinement started.

On 22 March 2020, the university hospital trust operating in Paris and its surroundings (Assistance publique – Hôpitaux de Paris, or AP-HP) was the target of a distributed denial-of-service attack (DDoS attack). This attack incepted a further element about the already sensitive nature of a cyber-attack against a hospital, namely public perception. In terms of severity, a DDoS attack, even if successful, does not impact the capacity of a hospital to conduct its daily or emergency clinical procedures as it targets per se only the extranet (while OT is operated through a separated intranet). Yet, given the heightened state of the public's awareness of healthcare issues, the cyber-attack had a greater media coverage in comparison with the attack against the Rouen CHU.

In a broader perspective, the healthcare facilities in France, unlike other sectors, were not as impacted by home working or ad hoc inception of home working connections during the pandemic. On site staff was obviously deemed critical, although support and administrative personnel of those facilities were to some extent required to perform home working as well. This both resulted in a more or less stable attack surface and a less acute trend of speedy digitalisation of operational technologies¹⁶ (e.g. MRIs, scanners, and any other computer systems in use in clinical procedures). However, the lack of dedicated cybersecurity staff for small to medium facilities compounded by the stress caused by the pandemic on the healthcare system led to a potential numbing with regard to cybersecurity best practices. Indeed, main

¹⁶ Set of information software or hardware directly linked to the core activity of its owner, e.g. user interface that allows a dam operator to control the water output, a connected MRI machine in a healthcare facility or a computed diagnostic tool for cars in a car workshop.

priorities were focused on increased output and resilience of IT systems, rather than on cybersecurity.

ANSSI notes that other significant successful cyber-attacks against French healthcare facilities have failed to materialise and that the sector has not been an enhanced target during the confinement. This despite a usual leveraging by cyber criminals of the ongoing pandemic and the ongoing trend of professionalization of this type of actor. However, it is certain that the pandemic further ensured ANSSI to better grasp the risks posed to healthcare operators.

The broader healthcare ecosystem: the providers and the supply chain risk and attacks


The French doctrine now takes into account risks related to supply chain and providers as cyber criminals have become more accustomed to this type of attack. These supply chain attacks posed a significant risk in the context of the pandemic by adding an even stronger risk on non-regulated operators, whose customers are the critical operators.

For example, the pharmaceutical industry plays a critical role in the COVID-19 crisis. The companies working on vaccine research or drug therapy for COVID-19 are in the media spotlight. Meanwhile, other healthcare industries suffer from strong tensions at a business level (e.g. products for intensive care units or medical reanimation, COVID-19 tests, chronic diseases, etc.). These industries are working on lean manufacturing systems and cannot afford any disruption in their production processes.

Regarding financial and political issues related to COVID-19 vaccine development, these industries are particularly targeted by cyber-attacks. Open source news related numerous cyber-attacks on that industrial sector. In France, some operators were indeed targeted as during the ransomware attack in August 2020 against Expanscience's servers, or the Nefilim ransomware attack in October 2020 against Panpharma.



Medical laboratories play a significant role in healthcare.



On another level, pharmacies are involved in the COVID-19 crisis, but they also play a crucial role to treat chronic diseases (heart or respiratory failure) that could be an exacerbation factor to COVID-19 contamination. Although medical biology laboratories have also a significant place in the COVID-19 screening tests phases, one should not forget their nominal tasks of delivering biologic analysis often critical for some specific issues as reanimation, obstetric or cancer. Pharmacies and laboratories are more and more digitalised in terms of processes and productions (drugs deliveries or biological analysis) making them credible targets of cyberattacks.

Finally, this crisis was the opportunity to develop many COVID-19 dedicated information systems with a national footprint. Amongst them, we can mention:

- Système d'Information de Dépistage (SI-DEP): an information system collecting all COVID-19 tests results from public and private laboratories, pharmacies, and health facilities across the French territories (including overseas).
- Health Data Hub Covid: a big data analysis platform dedicated to COVID-19 related research projects. This platform consolidates seven health databases (Oscour, SNDS, STOIC, ICANS, COVIDTELE, SIDEP and SIVIC).

The cybersecurity of those dedicated information systems, which had to be deployed in short timeframes, had to be ensured as they played a critical role in mitigating the pandemic.

Government

On top of its normal activities relative to its perimeter, ANSSI mainly intervened in a technical advisory support role to the benefit of ministries. Indeed, most of them created ad-hoc IT infrastructures with the aim of managing the COVID-19 crisis. The main beneficiaries of this support were the MSS, the Ministry of Finance and the Ministry of the Interior, the latter being the lead ministry with regard to national crisis management.

Paradigm shift

In normal circumstances, ANSSI intervenes as an advisor to government entities setting up new IT infrastructure following a structured assistance program, from risk analysis to technical assistance on IT architectures and audit. During the pandemic, however, ANSSI was required to rethink its approach to match various constraints.

Given the time constraints and high output awaited for dedicated COVID IT systems, as well as the sudden rise of projects, instead of having a structurally chronological approach where the project management is successively handled by the relevant expert units, task forces were constituted for each project. Those dedicated integrated teams incorporated from the inception all the relevant desks necessary so as to shorten the support process resulting in 30 projects being directly supported during the confinement.

ANSSI has been directly asked to intervene by the French executive level on specific priority projects from their inception on, demonstrating the willingness to make those cyber secure by design. Furthermore, to enhance agility, members of ANSSI's dedicated task forces were directly embedded in the broader sub-working groups (conception, risk analysis, architecture and audit) dedicated to each project. Those groups worked in parallel instead of chronologically to ensure deadlines are met (with the obvious exception of audit that can only be done once the project is at least semi-finalized). ANSSI used the

opportunity to further its concept of risk analysis driven method, in which each member of ANSSI task forces brought up information to feed a final and global cyber risk analysis of the whole project they were working on. This on the fly global risk analysis then permitted ANSSI to certify the projects on delivery and for each project owner to be aware of the remaining risks of the final product and his responsibility over them.

Here below, examples of such projects for which ANSSI provided enhanced technical support will be expanded.

MSS: SI-DEP

SI-DEP is a secured database ordered by the French executive level in order to collect COVID-19 screening test results and ensure that all infected persons are taken care of. SI-DEP is a partnership between the MSS (in charge of processing), AP-HP (project manager), the French National Agency for Public Health¹⁷ (SPF), medical laboratories, and their IT software providers. ANSSI was involved from the inception of the database.

The data stored on the platform can be classified under the following categories: personally identifiable information; context information for medical triage purposes (subject's contact details, professional occupation, type of accommodation, and date of first symptoms); contact details of general practitioner; and date of sample extraction for the detection test and its result.

Its goal was on one side to collect all COVID-19 test results from private and public biological laboratories on one database with consolidated and streamlined data and make those available to the

- SPF for the purpose of national strategic steering, epidemiology and crisis management,
- territorial health agencies¹⁸ (ARS) for the purpose of cluster tracking and management,
- National Health Insurance Fund¹⁹ (CNAM) for the purpose of invoicing and individual citizen advisories of possible contamination.

From a cybersecurity point of view, the technical challenges were to secure:

- the data feeds (containing highly sensitive personally identifiable and medical information) between about 4,400 laboratories²⁰ (public and private) on the French territory (including Overseas France);
- the connectors depending on the 15 different types of software in use in the laboratories,
- the database and its access by the above-mentioned administrative authorities.

The project was delivered within the scheduled seven weeks and incorporated five ANSSI full time personnel and seven on an ad hoc basis. As of now, ANSSI is still involved within the objective to technically assist the secured incorporation on the database through connectors of further 75,000 liberal healthcare professionals²¹ in France (pharmacists, doctors, and nurses) who have recently been declared able to conduct COVID-19 antigenic detection tests.

17 Santé Publique France, SPF

18 Agence Régionale de Santé, ARS

19 Caisse Nationale d'Assurance Maladie, CNAM

20 369 public laboratories; 4,039 private laboratories.

21 On a voluntary basis 15,000 pharmacies (out of 22,000 in total), 30,000 doctors (out of 100,000 in total) and 30,000 nurses (out of 130,000 in total).

Ministry of the Economy and Finance: platform for the State guaranteed loans

When the first confinement made clear that, there would be tremendous impacts on the French economy, the French government decided to set up a public guaranteed loans scheme for private companies. Due to the pandemic, the private sector entities would have to request access to those loans through dematerialized means and as such, a dedicated online platform (PGE) was set up. This mechanism is steered by the French Public Investment Bank²² (Bpifrance), which is itself under the supervision of the Ministry of the Economy and Finance.

Unlike SI-DEP, ANSSI was tasked after the platform set-up in March 2020, when it became clear that the platform could become a key target of cyberattacks and frauds. The agency's task was notably to ensure its high level of resilience as, for instance, if a DDoS did successfully render the platform unavailable, this would present a major reputational risk for the State and have a huge financial impact for the companies requesting help through the scheme. ANSSI used the opportunity to inject broader security concepts than just resilience in the project.

Its intervention had two objectives:

- An audit to identify the most urgent cybersecurity gaps, steer and make sure those were successfully patched.
- An assistance to the platform's IT providers in shoring up the cybersecurity of the IT architecture.

ANSSI invested ten full-time staff members for over a week and two part-time staff members from technical assistance for over three months to ensure the proper inception of initial recommendations.

Civil Society

French framework

As per its creation decree, ANSSI counts amongst its constituents the central public administration (down to, and included, prefecture²³ at local level) and the CIIPs/OES' under the LPM of 2013 and NIS schemes. As such, civil society does not befall under its main activities. Yet, ANSSI has undertaken over time numerous actions with regard to awareness raising and structuring the broader cyber security catering to the civil society. As such, it has published a MOOC²⁴ for citizens, operates a cybersecurity training centre for IT professionals (CFSSI²⁵) and contributed to the creation of Cybermalveillance.gouv.fr.²⁶ This latter structure has been incepted with the aim of filtering the broader offer of cyber security service providers that do not cater to central public administration and CIIPs, and index qualitative ones in a platform aimed at local public administrations, citizens, non-profit organisations, and SME's. Cybermalveillance.gouv.fr provides advice to victims of cyber-attacks in terms of remediation and can put them in touch with local cyber security service providers if needed. As such, this gives the structure a bird's eye view of the situation with regard to common cyber security threats to civil society during the confinement and broader COVID-19 pandemic, as the platform records citizens' and SME's requests to be put in touch with relevant providers.

22 Banque Publique d'Investissement France (Bpifrance)

23 Representative of the executive power at the "department" (rough equivalent of a Regierungsbezirk in Germany) administrative territorial division level.

24 Massive Open Online Course

25 Training Centre for the Security of Information Systems (Centre de Formation à la Sécurité des Systèmes d'Information)

26 Action against malicious cyber (Groupement d'Intérêt Public Action contre la Cybermalveillance)

Cybermalveillance.gouv.fr actions and feedback with regards to the confinement

Cybermalveillance.gouv.fr represents a relevant barometer of malicious cyber activity: in March, the number of visits to the web site had a tenfold increase, and over the first weeks of confinement, the requests related to phishing threats have risen by 400%. Furthermore, Cybermalveillance.gouv.fr notes that cyber fraud campaigns in France were more on the context of COVID-19 (parcel deliveries, SME refunding, fake Internet pages of free movement certificates, fake commercial sites for selling masks and / or hydroalcoholic gel, etc.) than on the sickness itself.

In the context of the COVID-19 outbreak and the rise of home working, the French government has been using Cybermalveillance.gouv.fr to relay cyber security-related recommendations. On 16 March, the eve of the first confinement, this instrument has been leveraged to publish a “call to reinforce cyber security vigilance measures” for individuals as well as for professionals. The government especially insisted on raising awareness of the risks of phishing/ransomware. More vigilance is needed on the reliability/seriousness of so-called medical websites, which proposed FFP2 masks, hydroalcoholic solutions or any kind of medicines/miracle vaccines for sale or telemedicine consultations. Within this context, it also stressed the importance not to relay fake news and advised caution about fraudulent online calls for donations. For professionals, Cybermalveillance.gouv.fr provided a set of advice concerning the increased risk of fraudulent bank transfers and raised awareness on the importance of information systems security to preserve companies’ assets – given that a lowered level of vigilance might have been exploited by potential attackers.

Signal Spam

Signal Spam is a public-private partnership that allows users to report anything that they consider to be spam in their e-mail client or webmail in order to assign it to the public authority or the professional that will take the required action to combat the reported spam. Public authorities such as the Ministry of the Interior, the data protection authority (CNIL), Police services occupy a seat on the board of the association.

In the early months of the year, Signal Spam did not notice a dramatic shift of balance between spams originating from marketing entities or from cyber fraud (around respectively 90% vs 10% of all spam declarations on the platform). The association did, though, observe a 600% increase in phishing declarations on its platform in the 72 hours preceding the start of total confinement (17 March) in France. During the first three months of 2020, most spam (marketing and cybercriminal alike) originated from France, the United States and Turkey. While cyber criminality-related spam did not surge in the absolute, the sheer volume of spam led to some significant and impactful downtime (up to half a day) within email services catering to people having to resort to home working.



Common assessment and outlook

Even before the pandemic, it could be stated without doubt that IT has become an integral and vital part of everyday life. Nonetheless, the last months gave a glimpse of what that actually means. The pandemic raised impacts of a potential major incident since scheduled redundant capacities came under stress, for example in the healthcare sector. Rapid adjustments and implementations of digital solutions such as remote working and video conferencing were required to allow the further functioning of the public, the economy and the government alike. Together with the overall uncertain situation and further compounded by a shortfall of IT staff on site this led to an increase in the attack surface for any potential adversary to exploit. Those exploitations could be exhibited in a vast array of phishing- and spam-campaigns.

ANSSI and BSI expect adversaries to continue their evolution towards more efficient and effective strategies. Considering the influx of capital through ransom payments over the last few months and the proliferation of successful strategies and modus operandi, new advancements are only a matter of time.

It is against this background that both ANSSI and BSI consider IT security as a pivotal necessity in this interconnected and digital environment. Looking forward, the risks outlined in this paper will continue to be a concern for the Cyber Security Authorities in France and Germany. It is therefore of utmost importance for ANSSI and BSI to continue their efforts to campaign for IT security as an integral part of our ever growing interconnected life towards their constituents. On top of that, both agencies should consider in the mid to long term to further promote the following aspects:

- foster development of various secured communication systems, means that proved scarce across the board during the pandemic;
- raise awareness with regards to supply chains issues, that should be an integral part of cyber risk assessments, whether from outsourced IT service providers or as part as the main activities of the entity;
- advocate life cycle management, security by design and by default on the part of IT providers.

Those last points should be considered as paramount to ensure a substantial increase in cybersecurity even before the products and services are delivered to the final users whether in a public or private context.



Imprint

Published by: Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn, Germany

Source: Federal Office for Information Security (BSI)
Section WG24 – Cyber Security for Citizens; Public Relations
Godesberger Allee 185 – 189
53175 Bonn, Germany
Phone: +49 (0) 228 99 9582-0
e-mail: bsi@bsi.bund.de

Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg
75700 Paris 07 SP
Phone: +33 (0)1 71 76 85 85
E-Mail: communication@ssi.gouv.fr

Last updated: December 2020

Item number: BSI-LaB20/001

Image credits: Fotolia_63989824_© milanmarkovic78 Subscription_Yearly_M_PLUS;
Fotolia_93974811_© pressmaster Subscription_Yearly_M_PLUS

The third edition of the franco-german common situational picture is provided free of charge and is not intended for sale.

