Cyberattack

Proj Trans Veille numérique

Emilien - Augustin - Nicolas

Introduction

Have you ever been hospitalised ? If so, your data may have been resold.
Consequences ? Hackers know your weaknesses.
My name is Augustin and my teammates are Emilien and Nicolas.
Today we are going to introduce you to our topic of cyberattacks and their consequences.
How did it start ? Who is targeted ? Why are they targeted ?
The presentation will be divided into 6 parts.
First of all, we will introduce you to the concept of a cyber attack and its consequences.
Next, we will see what tools are available.
Then the results of these searches.
And then we will see how hospitals are preparing.
Followed by our future forecast.
And finally what we would change if we had to do it again.

I - Cyberattacks and their consequences

A - What is a cyberattack ?

A cyberattack can be defined as a malicious attempt to disrupt, damage, or gain unauthorised access to a computer system, network, or device. A cyberattack uses various forms of technology such as viruses, malware, ransomware, phishing, or denial-of-service attacks.

B - Problems caused by cyberattacks ?

A cyberattack can devalue a companies reputation, leaving the company vulnerable and affecting customer trust. System paralysis, theft of sensitive data, exposure to blackmail, commercial damage, work stoppage... There are many consequences of this type of attack on a company.

C - Who is the target ? How did it start ? Why are they targeted ?

Hospitals in France began experiencing significant cyberattacks in November 2019, when attackers began targeting the IT systems of French hospitals, including hospitals in Paris. These attacks continued to occur throughout 2020 and have been attributed to malicious hacker groups, including Ryuk, Maze, and Egregor.

The attacks were particularly damaging during the COVID-19 pandemic, as hospitals faced increased demand for healthcare while their IT systems were compromised and inaccessible. Attackers used malware such as ransomware to encrypt hospital data and demand ransoms to decrypt it.

The reason for the attacks is unclear, although cybersecurity experts suspect the attackers are seeking a financial ransom or to steal sensitive data. French authorities have condemned the attacks and have been working with hospitals and cybersecurity experts to strengthen the security of hospital IT systems and prevent future attacks.

II - Our tools

FLIPBOARD

For the research into the cyber attack, I installed Flipboard. At the beginning the application asks you for 3 themes of your choice to already target the news that interests you. Then it takes you to a page where there is news on the chosen topics and if you are interested you can click on the news and it takes you to the site where it found the information.

For me, I installed Inoreader. Inoreader is a content player and flux rss online for web navigator and application for mobile devices. I started by creating an account and I chose my topic technology and the flux cyber security. Then I filtered with the word hospital.

And me, I Installed the application Feedly on my mobile phone. This application was very intuitive and easy to use. Directly on the application, I started to follow a pack of feeds, on cybersecurity. This permitted me to follow instantly 15 feeds on cyberattacks. Unfortunately, it was not possible to follow news feeds directly on the cyber attack on the hospitals, so I just filtered interesting topics.

III - Our findings

In 2021, hospitals in Dax, Saint-Gaudens and Oloron-Sainte-Marie were victims of cyberattacks, disrupting or closing their IT services.

Le Progrès reports that on Wednesday 25 January 2022, several establishments of the Ramsay Santé group were the target of a cyber attack, including the Jean-Mermoz private hospital in Lyon and the private hospital of the East Lyon region, in Saint-Priest.

In a statement, the group said that "the security procedure had been immediately triggered" and that "no data theft or cases of propagation of the incident to our patients" had been noted.

On Saturday 3 December 2022 at 9pm, the André-Mignot hospital at the Versailles hospital center was the victim of a cyberattack.

According to the hospital's management, some of the computers were blocked, screens went black and a message was displayed: "All your important files have been stolen and encrypted. Follow our instructions",. A group of hackers claimed responsibility for the attack.

As the consequence of this attack. The institution transferred 6 patients, 3 of these patients were from the adult intensive care unit and 3 from the neonatal continuing care unit. The machines dedicated to care were operating, what was not operating was the networking. So more staff were needed to oversee the patients.

The latest cyberattack is at a hospital in Brest. The attack took place on Thursday 9 March at 20:33. The Hospital of Brest University was subjected to an intrusion in its information system. Servers were impacted. As soon as this cyber attack was reported, the CHU put in place the necessary precautionary measures to ensure the continuation of its activities. To limit the propagation of the attack, the Internet information system was isolated. No health data leakage was identified and no internal data was compromised. The hospital has filed a complaint with the police.

10 days later, internet connections were still down from the attack. It was impossible to make appointments online or to make payments by credit card. A return to normal is not expected for several weeks.

Health data is the most lucrative data for cybercriminals. For example, the cost of a medical dossier can be as high as 350$ on the dark web, which is a fiftyfold increase.

To combat this growing phenomenon, the State allocated 25 million euros to the cybersecurity of health establishments in the wake of the Covid-19 epidemic.

To deal with these attacks, which are on the increase, the government has announced new measures to strengthen the cyber security of health establishments, including a "vast programme of preparation for cyber incidents" and a "digital white plan".

With the first measure, "the objective is that 100% of the most priority health establishments will implement new cyber defence exercises by May 2023", explains the Minister of the Interior “Gérald Darmanin” and the minister of Health “François Braun” and the Minister Delegate for Digital Affairs “Jean-Noël Barrot” in a joint press release.

The second measure, the “white plan” should enable "establishments to be equipped with the reflexes and practices to adopt if a cyber incident occurs", such as the activation of a crisis unit or the assessment of damage caused by hackers.

On February 9, 2023 on Weka. Gérald Darmanin, François Braun and Jean-Noël Barrot have reaffirmed that the new 2023-2027 roadmap for digital health will give a central place to the cybersecurity of institutions. To this end, a task force involving all the competent authorities has been set up, and aims to draw up a new draft for a massive multiannual cyber plan by March 2023.

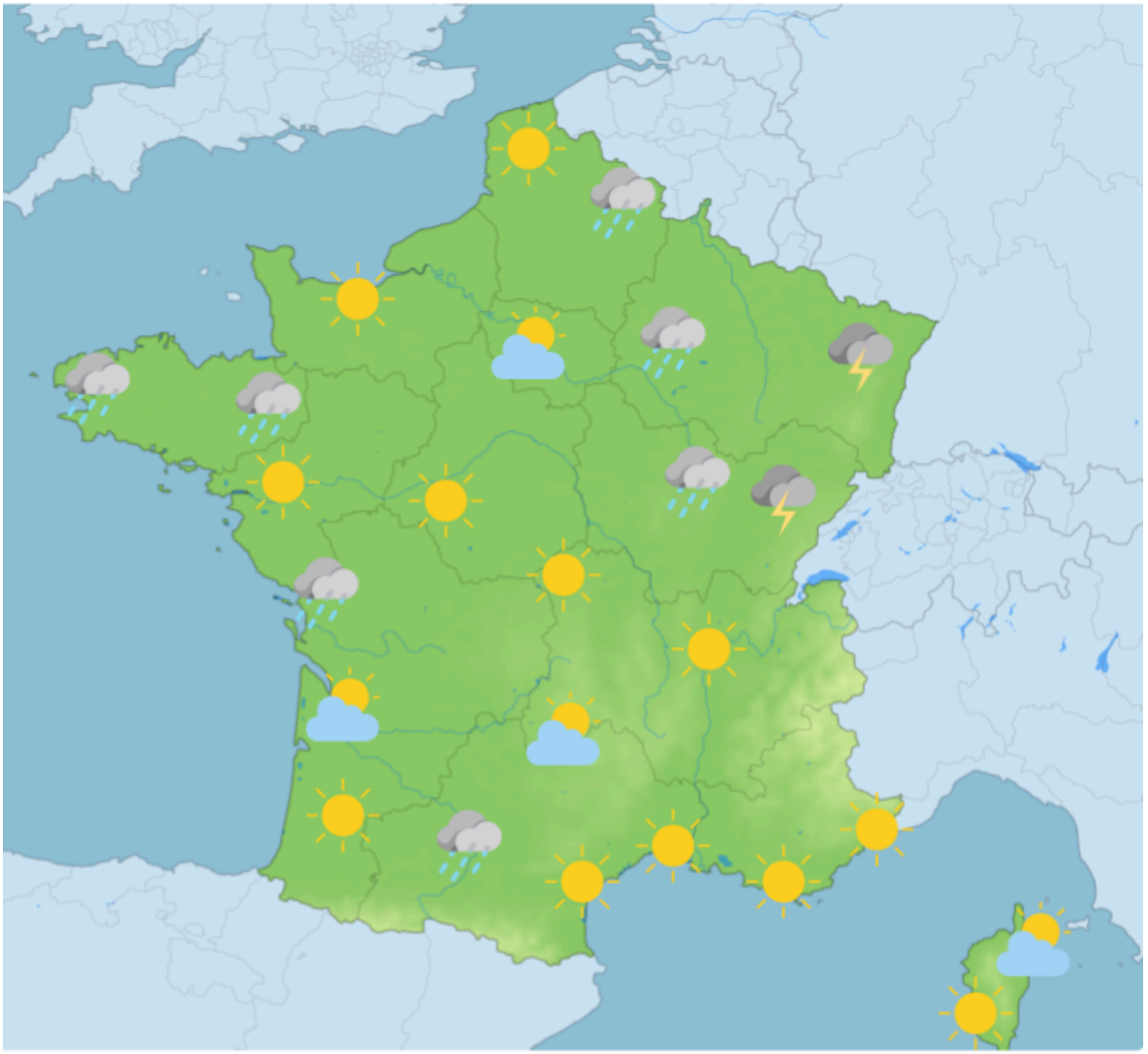
IV - Crisis Simulation

At the Hospital Reception in Nanterre, it was 9am when the exercise began. The first alert is launched by the hospital's health professionals, brought together and directed by a consulting company specialising in crisis management. In the morning, they launched the cyber-crisis scenario by phone to their managers.

They said : “When we arrive at a real crisis, we are doubly prepared”

V - Coming soon

Let's look at the forecasts for this year 2023.



The Lockbit storm coming from Russia will attack the great east which has been spared until now. The hospitals of Strasbourg, Besançon and Dijon are in danger.

Lille has not been touched for the moment. Is it for this year?

Brittany is not safe from an attack. As we have seen previously, Brest hospital was the first victim in the region at the beginning of March. This will soon be the case for its capital Rennes and the other cities, Lorient, St Brieuc, Quimper…

The south west has already suffered attacks, but the city of Bordeaux has not been targeted for the moment. They are therefore not sure that they will not be attacked.

The south east should be fine since it has already suffered several attacks last year. But be careful not to let your guard down.

VI - If we were to start again

The Inoreader application does not allow you to monitor a keyword, for that you need a pro account.