Read this post online

Ransomware attacks: Best practices to protect yourself and deal with them

For several months now, ransomware cyberattacks have been on the rise. Recent attacks echoed by the media show that all types of organizations, whether private or public, can be affected, whatever their size.

In this context, this article offers a reminder of the best practices to implement in order to limit the risks and to know how to react effectively in case of an attack.

First of all, what is a ransomware?

The French National Cybersecurity Agency (*Agence nationale de sécurité des systèmes d'information*, also known by its acronym "ANSSI") provides the following definition:

> *"As a common cybercrime attack technique mode, ransomware involves sending the victims a malicious software that encrypts all of their data and asks for a ransom in exchange for the decryption password"**[1]**.*

In recent months, there have been many victims of ransomware attacks: Among the most emblematic are the French companies *Sopra Steria*, *Bouygues Construction* and, more recently, the American oil pipeline *Colonial Pipeline*.

The consequences for companies can be disastrous: In addition to the potential loss of data or the payment of a ransom, the victims must face up the disorganization or even the discontinuation of their operations and a subsequent drop in revenue. Not to mention the serious risk of reputational damage and the negative impact on their relationships with customers and business partners.

In this context, how can organizations protect themselves against ransomware attacks? And what if an attack nonetheless does occur?

In August 2020, the ANSSI, in partnership with the Directorate for Criminal Matters and Pardons (*Direction des Affaires Criminelles et des Grâces*, also known by its acronym "DACG"), published a guide that sets out a number of recommendations aimed at limiting the risks and reacting adequately in case of a ransomware attack[2].

In view of the recent increase in these attacks, you will find below a brief reminder of the ANSSI's recommendations.

Measures to reduce the risk of attack

Acting upstream of any attack can be a winning strategy that can prevent attacks or, at least, reduce losses. This involves implementing the following cybersecurity principles within the organization[3].

- ***Back up data***

It is important to perform regular backups of all the organization's data.

Knowing that ransomware can also reach backups, it is imperative to provide, at least for the most critical data, backups disconnected from the computer network, for example through external storage systems.

- ***Keep software and systems up to date***

To limit the vulnerabilities of information systems, it is essential to promptly and regularly install software and system upgrades that contain security patches.

- ***Use and maintain up-to-date antivirus software***

Antivirus software can help prevent file corruption and encryption. To keep them effective, it is important to update such software frequently.

- ***Partition the information system***

Ransomware is intended to spread throughout the organization's computer network. It is, therefore, useful to organize a partition between the different network zones. It is also possible to partition and isolate the highest levels of management to make them difficult to be reached by the ransomware.

- ***Limit user rights and application permissions***

Limiting which workstations have administrator rights is also an important measure to put in place. It may also be useful to have some administrative workstations without Internet access.

- ***Control Internet access***

Because ransomware often exploits Internet access, implementing a secure Internet gateway to block

illegitimate traffic is crucial.

- ***Implement the supervision of logs***

In order to monitor the organization's IT security, it is important to ensure that incidents are monitored by implementing an event log policy. This supervision can help detect a possible corruption and save time in understanding incidents.

- ***Raise staff awareness***

The ransomware attack is often the result of negligence on the part of a staff member of the victim organization, for example by opening a booby-trapped attachment. It is therefore important to train and educate users on good digital security practices.

- ***Evaluate the opportunity to subscribe to a cyber insurance***

Some insurance companies now offer cyber insurance policies that include coverage against cyberattacks, including legal assistance and financial coverage for the damage suffered.

- ***Implement a plan to respond to cyber attacks***

A ransomware attack can significantly disrupt the operation of an organization. It is therefore important to determine, upstream, a response plan aimed at ensuring IT continuity in case of an attack.

- ***Think about the cyber crisis communication strategy***

The consequences on the image and reputation of the organization victim of a ransomware attack should not be overlooked. To limit these negative impacts, it is important to prepare an adapted and effective crisis communication strategy beforehand.

How to react in the event of an attack

Preventive measures are not always sufficient to prevent attacks. In case of an attack, it is important to know how to react quickly and efficiently to limit the impact of the ransomware.

- ***Adopt the right reflexes***

In case of an attack, several actions must be taken immediately, including:

-Opening a logbook to trace the actions and events related to the incident;

-Isolating infected equipment by disconnecting it from the network;

-Disconnecting non-infected backup storage media;

-Turning the equipment with encrypted files on deep sleep mode (since a complete power shutdown could compromise a future data recovery) and leaving unbooted equipment turned off.

- ***Coordinate the management of the cybercrisis***

It is advisable to set up a crisis unit at the highest level of the organization to coordinate the response to the attack and make the strategic decisions required at the operational level, but also in terms of internal and external communication.

- ***Finding technical assistance***

In the event of an attack, technical assistance is essential. If the organization does not have internal resources for this purpose, it is imperative to use external service providers specialized in the response to this type of security incident.

- ***Communicate at the appropriate level***

To determine the communication actions to be taken, a technical, media and social assessment of the attack must be carried out. Support for employees can also be organized through appropriate internal communication.

- ***Do not pay the ransom***

It is not advisable to pay the ransom, since this does not guarantee that the cybercriminals will allow the decryption of the systems. Moreover, ransom payments finance cybercriminal organizations and encourage them to multiply this type of attacks.

- ***File a criminal complaint***

Filing a complaint with the police or *gendarmerie* (another type of police force mainly responsible for law enforcement in small towns and rural areas). Filing a complaint will allow an investigation to be conducted, which may provide elements to decrypt the altered data. In addition to allowing for the identification and subsequent conviction of the cybercriminals responsible for the attacks, filing a complaint is a necessary prerequisite to the compensation of the damage suffered by the organization.

- ***Restore systems from healthy sources***

Infected equipment should be reinstalled and data restored from backups preferably made before the system was compromised. It is imperative to verify that the restored data is not infected with the ransomware.

For a more detailed description of the ANSSI's and DACG's recommendations, we invite you to consult their guide "*Ransomware attacks, all concerned – How to anticipate them and how to react in case of incident*", available on the ANSSI website[4].

[1] https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/

[2] https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/ (in French only)

[3] These rules stem from the ANSSI' IT hygiene Guide available @ https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/ (in French only)

[4] https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/ (only in French)