BDO LEGAL | 2023 PRIVACY WEEK SERIES

Lessons learnt from data breaches due to ransomware attacks on government services (check your cybersecurity).

PIETER GOOVAERTS | BDO LEGAL - BELGIUM

What are ransomware attacks and how are government services affected?

In 2022 several Belgian government services were the victim of ransomware attacks. Ransomware in itself is a virus that encrypts the infected data, rendering access impossible for the owner of the data, unless it is decrypted by the hackers. In some cases, the hackers also copy certain data. The ransom part comes in when the target is contacted by the hackers with a demand for ransom to either decrypt the encrypted data or to prevent the hackers from publishing the copied data.

Such ransomware attacks are frequent. In 2022, 148 ransomware attacks were reported worldwide on government services alone, with an average ransom demand of 9.4 million EUR and an average of 39,383 records impacted per attack. Government services are a preferred target for such hackings as in general they cannot afford to interrupt their services to the public and any encrypted or stolen data is usually difficult and costly to recreate. As governments are digitalising and providing more and more services online there is also a bigger area for the hackers to be active in, whereas these public services may have issues keeping up with evolutions in technology, increasing the number of potential vulnerabilities.

What happened in Belgium?

One of the cases in Belgium involved a police department which was a victim of a ransomware attack, which resulted in a data breach. In that event, a large number of files (around 6 Gigabytes according to the hackers) were posted on the dark web by the hackers. These files included internal administrative documents, internal guidelines, but also operational and even judicial information, such as personal data of citizens and employees of the police department. One of the issues that was shown by this leak is that the data management of the department was lacking, as information that belonged in a closed police network, was transferred to a less protected network for easier transfer to other services.

In another instance, the network of a large city was hacked and submitted to ransomware, resulting in a severely reduced availability of the systems, and city services such as libraries, museums, schools, and police departments having to revert to working on paper. Affected personal data included accounting data, employee records, insurance files and emails. No large-scale citizen data, such as copies of passports or driver's licences, was stolen. The hackers allegedly copied 557 Gb of data.

In this case, an audit from 2020 had shown that cybersecurity of the city was not on point and certain essential improvements, such as multi-factor authentication, had not yet implemented.

As far as this was communicated to the public, in neither of these instances was a ransom paid to the hackers.

Who are these hackers and how do they act?

This is not a single organisation, but there are several collectives with different backgrounds. It appears that they work together on a kind of freelance basis, where some members seek out targets, some infiltrate the ransomware into the network of the target and others take care of negotiations with the target. The common motivator seems to be money, but some groups have been linked to certain countries condoning such actions against third countries in order to destabilise them, attacking, for example, energy infrastructure.

The hackers just need a way to access the network in order to encrypt or copy the data of the target. One way of gaining access is using stolen login data of employees, often through phishing, or exploit known vulnerabilities in software that is used by the target. They then look around in the network to find useful data and encrypt or exfiltrate it. Finally they ask for a ransom in return for not exposing the information on the (dark) web or to decrypt the infected data.

How is this relevant for me?

These cases show that hackers will attack any organisation which holds data that can be stolen or encrypted and then ransomed, whether it be government, healthcare, business or education services. When this happens, personal data is involved in almost every instance and, if EU citizens are involved, such a ransomware attack will result in a data breach that will likely have to be notified to the competent Data Protection Authority and even the data subjects. Such notification may raise questions from the larger public and scrutiny from clients and partners, and the organisation should therefore be able to show that all reasonable measures had been taken. There is indeed no way to protect 100% against such attacks, but there are many measures that will at least mitigate the impact.

What can I do?

An organisation can adopt multiple measures to be better protected against the occurrence of these hacking attacks and, if they happen, to handle them in the most effective way possible.

Of course, technical measures are the first that come to mind to protect your systems against ransomware attacks. These groups usually use the path of least resistance, so if it is too difficult to access your systems, they will move on to another target.

Preventative measures, which help in ensuring that hackers cannot get access to your organisation's network, include:

- running up-to-date end-point security and anti-virus software for all your emails;
- deploying vulnerability management tools across your systems to understand where the organisation is vulnerable, and how to mitigate the vulnerability;
- blocking malicious websites;
- for backups, the 3-2-2 rule is recommended: make 3 backups, 2 of which are kept locally on 2 different supports and 2 of which are kept elsewhere (1 in another location and 1 in the cloud);
- adopting multifactor or two factor authentication on all remote accesses;
- taking care of network segmentation;
- regularly updating your software to rapidly remedy vulnerabilities.

Monitoring measures, to make sure that if hackers are trying to get access to your network, or get in, this gets picked up so the damage can be mitigated:

- monitoring tools across your systems and understand where key assets and critical business process lie;
- provide a plan for logging, monitoring and backups of the log servers.

Protection against ransomware attacks is not just a technical issue. To be effective, there are many organisational measures that should be taken.

Organisational measures include making an inventory of your data and your data flows and making sure that data is only accessible by those who need it, not only within the organisation, but also any third-party vendors.

This includes data mapping, data classification, user access, application management and vendor risk management programmes. Not only will this show any processes where data is shared in an overly broad manner, it allows at the same for the organisation to minimise personal data processed for certain activities.

Awareness is another organisational measure which greatly reduces risks of a ransomware attack. People are on the one hand a possible gateway for hackers to enter the network, through obtaining their logins, by phishing mails for example, but on the other hand, are crucial to detect possible access to the systems by malicious persons. By fostering a culture focussed on data protection within the organisation, through continuous training and mock phishing emails, chances of hacking are greatly reduced.

Plan ahead: establish and test plans for specific situations. Have your IT security architecture and policy reviewed by a specialist and create a cybersecurity strategy based on the results, establish a plan on how to handle a cyber-attack, which includes communications, analysis and recovery.

For further information:

PIETER GOOVAERTS
SENIOR LEGAL ADVISOR | BDO LEGAL - BELGIUM

+32 485 76 32 81
pieter.goovaerts@bdo.be