Alarming news: the City of Antwerp fell victim to a ransomware attack

14 December 2022, 11:37

Tatiana Galibus

The city of Antwerp fell victim to a ransomware cyber-attack last week. Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access.

Most services of Antwerp are now frozen, including the e-services of the city, museums, and libraries. Cyber Play claimed the attack on its website on the DarkWeb. The group seems to be a newly emerged one, as it is not mentioned in the Kaspersky report, a list of the 8 most dangerous ransom crews in the world. Goes to show that even smaller ransomware groups can have a disastrous impact, how fast powers can shift, and threats can emerge in the cyber world.

Can the cyber-security of Belgian companies be guaranteed today?

The short answer is ‘no’. We know that ransomware groups are well-organized. Sometimes better than the companies they attack. And they love to use old-age technologies: phishing, spear phishing, USB sticks etc. And as last week's attack shows, these methods still work.

Why do they work? Because with an organized group like this, you do not deal with just a program or a script, but with a well-organized group of people, each with their specific skills, that are all focused on achieving the same goal. The famous Conti group leaks, affectionally dubbed “The Panama Papers of Ransomware” showed us the manuals and inner workings of a group like that.

> Did you know that on average a Belgian company deals with over 3.000 cyber-attacks a year? And in 2022 alone there was an increase of 28%. So it’s time to take action.

Cybersecurity culture is a must

That is why a clear and precise cyber-security culture in companies is important. As a manager you should be able to answer the following are basic questions without hesitation, to be protected in this fast-changing world:

- Are all my employees aware of what phishing is? Do they know how it works, what could be signals of a phishing attempt?
- Am I reassured that no one in my company will do that mortal click or insert that USB into a computer out of curiosity?
- Do we have clear access control and politics?
- Do we store your sensitive data separately on encrypted data storage?

A lot of no’s? A lot of hesitation? A higher sense of urgency is urgently needed regarding your cyber-security.

How can Sirris help?

We run 2 trajectories in the next months, dedicated to cybersecurity for digital services as well as manufacturing. Both trajectories are designed as learning journeys, with in-depth theory modules and tailor-made practice sessions. We partner up with other cyber-security partners to deliver the best lessons learned and give you networking experience. On top you'll get several **micro-coaching sessions for your specific concerns.**

Authors

Tatiana Galibus