GEERT
BAUDEWIJNS

NEGOTIATING IN THE DARK

Lannoo

CONTENTS

01

THE ANTWERP CASE

‘The City of Antwerp is hacked.’

Although my business card says something else, when people ask what I do, I usually say: 'Negotiating with cybercriminals.' That's the most clear-cut aspect of my work in cybersecurity: communicating with hackers who use ransomware to cripple a company's network. Those hackers are always devising new ways to infiltrate networks, install malicious software, encrypt all the data, and copy it. Then they demand a ransom to reverse the encryption and not publish your data. Blackmail, pure and simple.

The targeted companies have their backs to the wall. Nothing works anymore and they have no choice but to send their staff home, suspend production and services, and have their IT personnel clock up overtime. In most cases, they soon conclude that paying the ransom is the quickest, most cost-effective – or even the only – solution. That's when they come to me for help. As a negotiator, my job isn't to track down cybercriminals, but to talk with them for days or even weeks. My goal is to drive down their price and figure out how they got in. Of course, giving in to the demands of unscrupulous hackers feels galling, but I do all I can to minimise the ransom demand so that most companies survive an attack unscathed.

The most notorious hacking in Flanders is probably the cyberattack on the City of Antwerp in late 2022. Whenever I strike up a conversation with someone and mention my work, I'm always asked: 'What happened in Antwerp?' The cyberattack on the city, and on 5 December, St Nicholas' Eve of all nights, has lost none of its fascination, and is etched in the collective memory. The story has all the ingredients to pique the imagination: an iconic date, a major city, and a mysterious denouement about which rumours persist.

For me, this is a loaded question because, frankly, 'the Antwerp case' still gets under my skin. At the time of the hacking,

as suppliers we were closely involved with Digipolis, the city's IT partner, responsible for an extensive range of services, from maintaining the city network to the digital development of city services. Their remit also includes cybersecurity, something Antwerp had taken particularly seriously since the Liège hacking.

Liège was hit by a ransomware attack carried out by the Ryuk group in June 2021. A Belgian metropolis was brought to a standstill for the first time. Media reports claim the city paid thirty million in ransom, which set off alarm bells in Antwerp. Cybersecurity was suddenly high up on the agenda and the city council made extra resources available to avoid a scenario like the one in Liège. With this in mind, they tasked Digipolis, their technology partner, with developing a comprehensive cybersecurity plan. The goal was clear: to reinforce the city's digital defences and make its systems cyberattack-proof. Digipolis put out several invitations to tender, a few of which our company won. Specifically, our job was to track down and identify potential weak spots in the network. We were not involved in the operational side of things; our role was to pinpoint places where attackers could gain access. Our analysis uncovered numerous vulnerabilities, which isn't uncommon, and something we see in many companies. Keep in mind that, like the networks of many other large cities, Antwerp's infrastructure dates back 20 or 30 years.

At the time of the hacking, as suppliers, we were closely involved with Digipolis, the city's IT partner.

Many of our clients face the same issue. They start with a small network that needs to grow rapidly without disrupting the operation of existing applications or services. Over the last 15 years, the digital transformation of city services caused the

Antwerp network to grow before our very eyes. The focus was on building, building, building, and the speed at which this had to happen overshadowed the question: are our foundations properly and correctly secured? Are they sufficiently robust to enable continuous expansion? Are they sufficiently future-proof when it comes to network security, for instance?

Modernising such an old system is far from easy, and IT people often see it as the most demanding task because you have to find a way to link old and new technologies. This not only requires considerable time and financial investments but also extensive technical expertise. One of the most effective methods to strengthen security is to apply 'Chinese walls', also known as 'subnetting'.

Subnetting is the process of dividing a larger network into smaller, manageable segments or subnets. Each of these subnets can function as an independent network, with its own unique security protocols and access management. By segmenting the city's network like this, each section is shielded from the others, limiting the scope of potential cyberattacks and protecting sensitive data.

Adding Chinese walls into an existing network is a massive and extremely complex job. You have to implement new protocols, train employees to work with the new structure, and replace outdated systems. You can't just shut all the city services down; every adjustment must be made without affecting the city's day-to-day operations. So, besides technical skills, it requires a great deal of coordination. On top of that, and we shouldn't trivialise this, adjustments of this kind cost money. A lot of money.

An additional problem with old networks is that some software cannot easily be upgraded because the underlying technology is too old. After all, if you want to secure such an old system effectively, you need the supplier's support. However, suppliers often stop supporting technologies five years after developing

the software. Because of this, it's impossible to install security updates at a later date. From this point on, the clock stands still for those old applications, but the hackers' clock begins to tick. Hackers look for weaknesses they can exploit, knowing that the suppliers won't step in to fix them. In other words, it is only a matter of time before something happens. As a city, you're heading for disaster because your old applications must continue to work, with or without the suppliers' support.

So, at one point I requested a meeting with the CEO of Digipolis. I wanted to personally inform him of the seriousness of the problems and convince him to act. Our meeting went well. I explained to him, little by little, where the weaknesses were, and the CEO nodded more often than I had expected. He agreed that something had to be done, yet I felt that the people at Digipolis didn't grasp the urgency of the situation.

I'll make no bones about it. That frustrated me. Although I am acknowledged as an expert in many parts of the world, at home I'm often dismissed as just another consultant. And yet, every day I'm in the thick of the action, am more familiar with the information and tools that can be found on the dark web than almost anyone else, and my team and I can identify exactly where the holes in a security system are. We often detect an attack before it has even occurred because the first signs can always be found on the dark web. That sets us apart from other security firms. There are many things I can't do, but what I can do is this: sense when things are about to go wrong, and show where they can go wrong, simply by using information we find on the dark web.

At a certain point, I saw so many red flags that I took matters into my own hands. In early November, I sent a message to Bart de Wever, the Mayor of the City of Antwerp and party chairman of

the N-VA. That wasn't such a big step, although I had never met him in person. Our company works closely with N-VA nationwide, and I had stood for election on behalf of that party in my municipality. I simply sent him the following message: 'I would like to meet with you sometime.' His reply came fairly quickly: 'Good, schedule something through my secretary.' We picked a date, 28 November, and he and his cabinet secretary set aside an hour for me.

That day I walked through the imposing doors of Antwerp City Hall, which I had previously only seen from the outside. After registering and signing in at the reception desk, I walked up the stately steps, past beautiful paintings, to the mayor's offices. He and his chief of cabinet welcomed me warmly, though we wasted little time on pleasantries; I was there on a mission. What was originally intended to last an hour became an intense two-hour conversation. I shared my concerns about how hackers operate, pointed out weaknesses, and expressed my frustration with certain things that simply wouldn't change.

Scarcely a week later, while I was in Japan on a trade mission, I received a message from the head of our technical department: 'The City of Antwerp has been hacked.' It was 6 December; I'll never forget it.

I promptly flipped open my computer and dived into the dark web. And there it was: Play, one of the large hacker collectives, claimed responsibility for the Antwerp attack. On its 'wall of shame' – where they publish the names of companies they have successfully targeted – *the City of Antwerp* was at the very top, including a countdown clock to the deadline set by the hackers. All major ransomware collectives have a wall of shame. They remove the name of their victim from the wall once the ransom is paid. Here that was not yet the case: the clock below the name Antwerp was ruthlessly counting down the seconds.

I admit that I was quite surprised by the speed with which my words had become reality. Less than a week before, I had warned of a possible attack, and now it was happening. I instantly contacted Bart De Wever: 'The City of Antwerp has been hacked. Have you been alerted yet?' That may seem like a strange message to send, but senior executives are often not informed of a cyberattack until fairly late. It's quite common for IT departments to try to resolve the issue, or report back to their immediate supervisor before notifying the CEO or, in this case, the mayor. Bart promptly replied that he was in no doubt about what was happening. He asked me not to do anything for the time being and teasingly wrote, 'After predicting exactly this kind of cyberattack a week ago, you're our number one suspect.' I couldn't help chuckling, and answered, 'Every story needs a suspect and I'm happy to play that role.'

Although there was little to laugh about in this story. Lots of services were unable to function and had ground to a halt: no passports, no building permits, container parks were closed – all digitised services had to operate manually.

Also, the hackers had captured 557 gigabytes of data, which they threatened to publish. The exact data they were referring to was unclear. The fear was that citizens' personal data had been copied, something the mayor would deny several weeks after the attack.

Journalists quickly sensed danger and published one article after another about the large-scale attack on Antwerp's systems. At the centre of this was the mayor, who maintained his position: 'We don't negotiate, we don't pay. If necessary, we'll rebuild the entire network from scratch.'

He delivered a clear and consistent message. Yet something curious happened: Play removed Antwerp from their wall of shame. Without paying? Hardly likely; hackers aren't altruists,

and Play is a well-oiled machine that wouldn't let the City of Antwerp slip from its grasp. That same evening, Bart De Wever sent me a message. 'Antwerp's been taken off the wall of shame, and we didn't do anything. Have you ever known this to happen before?' My answer was short but to the point: 'No. This proves that negotiations are underway, or the ransom's been paid.' The mayor firmly reiterated that this was not the case, which might be possible, but it's rather unlikely. I am convinced that De Wever genuinely believes that the hackers were never contacted, although through my network I heard that Digipolis was looking for a negotiator, provided that they weren't connected to our company. Because I had directly approached Bart De Wever, the relationship with Digipolis had soured somewhat.

Honestly, I'm not sure about the exact manner in which that case was handled. Were there really perfectly usable backups, as people claimed later? And even if there were, didn't anyone even initiate negotiations? My hunch that the city paid up is as strong as ever, even though I can't prove it. Ultimately, it doesn't really matter. The main thing is that the city seized on the attack to put extra effort into cybersecurity. It decided to use the attack to tackle the issue head-on, and completely upgrade its aging network with Chinese walls. Today, the network's foundations are considerably stronger. Digipolis finally implemented the updates and improvements we'd asked for so often. Despite that, our collaboration suffered; trust had been lost. After the incident, our contract with them was scaled back seventy per cent. Now, they only approach us for what we are uniquely known for in Belgium.

It's funny that rumours circulated about a third party that allegedly paid the ransom for Antwerp, about drug traffickers trying to suppress the emergence of sensitive information, or criminal syndicates wanting to conceal their inner workings at all costs.

Sensational stories, but the chances are extremely slim. You can't just negotiate with hackers. Communications have to go through a secure environment created by the hackers. You can only access this through a link in the ransom note – the message the hackers send to your computer telling you what's happened and the steps you're required to take.

I estimate that around fifty city employees saw that note, but someone clicking on the link and paying a couple of million in bitcoins without anyone knowing? There's zero chance of that happening, right?

It's funny that rumours are circulating about a third party that allegedly paid the ransom for Antwerp.

It's also not as though you can email the hacker and say, 'Hey, I want to pay this for Antwerp, can we make a deal?' That isn't how it works. Because it was a high-profile case, plenty of journalists tried contacting the hacker platform Play. But hackers don't respond to that.

I'm not sure exactly what happened in Antwerp. I'm also not entirely certain which of the network's numerous weaknesses the hackers used to gain entry. All I know is that the network there has become a lot more secure thanks to a substantial investment, and the fact that this attack resulted in downtime led to the IT services upgrading everything. Journalists and politicians estimated the cost of the cyberattack at 100 million. How expensive the lesson for the city really was, we may never know.

02

HOW IT BEGAN

‘Geert, promise
you’ll never go into
electronics. If you do,
you’ll give our school
a bad name.’

It is curious how some moments later turn out to be tipping points, harbingers of what's to come. As a child, I could never have imagined that one day I'd own my own cybersecurity company, let alone spend days negotiating with cybercriminals. But there were certainly circumstances and people in my childhood that shaped me, that taught me things, that got me where I am today.

Top of the list: school. Not for the reason you might think; I still can't write five sentences without mistakes and when it comes to maths, I don't get numbers at all. This was partly because when I was at primary school, I spent a lot of time in hospital due to severe asthma attacks. When I was about thirteen, the attacks stopped, but I couldn't catch up. I struggled to concentrate. Those were the days before things like ADHD were talked about, and I struggled through secondary school. Sometimes I passed, sometimes I had to repeat a year; that phase of school lasted agonisingly long. I hated every day I had to spend at school not only because I could barely cope with the subject matter, but mostly because of the constant stress of being bullied. And bullied I was, throughout my miserable school years, about something as trivial as my weight. Don't get me wrong: there is really nothing positive to say about bullying, but it did teach me a skill that I can still put to good use: I learned to disappear. I can blend into the crowd quite easily, behave in such a way that people don't see me. Those who don't stand out can watch, observe people, assess what another person is thinking or will do. I trained myself to figure out people's motives, to know what their next move would be, to wriggle out of a tricky position and not be intimidated by some bully. I don't need to explain that this gift comes in handy when a cybercriminal hurls the vilest insults at me.

Fortunately, I grew up in a loving family, in the borough of Tervuren, in Moorsel, a small village where time stood still 45 years

ago. We lived close to both my grandparents, who lived barely five houses apart. So, you can't say my father had to venture far to find the love of his life. My sister and I spent a lot of time with them, though I mostly remember that they were hardworking people, just like my parents by the way. My father's father had the most wonderful job: he grew and tended geraniums in all the railway stations in Brussels. When he came home, he always tapped on the window to warn us that he was coming. Then, my sister and I would hide under a cupboard or under the sofa, and he'd come and find us, making all kinds of funny noises. Those moments were wonderful, but short. Once he'd found us, we weren't allowed to disturb him. It was drummed into us from an early age that working people were entitled to some downtime. Well, my grandfather didn't get much time to rest, as he often went to help out on his parents' farm after work.

My other grandfather also worked extremely hard. He worked at the post office in Tervuren until about four o'clock, after which he did odd jobs as a gardener for people in the neighbourhood. He had five children to feed, including my mother, who was not his biological daughter but whom he raised as his own.

We didn't discover my mother's story until recently, and it's too good not to tell. After World War II, the Belgian army controlled part of Germany. One of the barracks was in Siegen, where my grandfather was stationed as a soldier in 1950. Once his shift was over, he'd sneak out of the barracks and go dancing at one of the town's many bars. Landlords always welcomed him; he was the heart and soul of the party, and, in due course, a civilian suit awaited him at every bar, and he was paid to dance and encourage other customers to get onto the dancefloor. Why the civilian clothes? Because soldiers were forbidden from leaving the barracks and he didn't want to be seen in his army uniform.

My grandmother, 21 years old, lived in Siegen, not far from Cologne. Like other young women her age, she dreamed of a family, but there weren't many options after the war. Almost all the young men had been killed. So, like most of her friends, she went to the taverns near the barracks. That's how she got to know a soldier from Aalst. One thing led to another, and they would probably have married if he hadn't suddenly contracted a liver disease and been rushed to a Belgian hospital. Before she could tell him that he was going to be a father, he vanished from her life.

Their child was born, a girl, after which my grandmother went to the barracks again and this time met my grandfather. He fell so deeply in love with her that he took my grandmother back to Belgium with him once his army stint was over, and my mother stayed behind with her grandmother in Siegen. That decision was made after careful consideration. At the time, barely six years after World War II, turning up in Belgium with a German fiancée was bad enough, let alone a German woman with another man's child.

The secret didn't come out until five years and one child later, when my grandfather's parents asked why their daughter-in-law kept sending children's clothes to Germany. They were furious when they learned why. Not because their daughter-in-law already had a child, but because they had been kept in the dark for so long. The next day, my grandparents jumped in the car and drove all the way to Siegen to pick up my mother. That must have been a shock for her, but she didn't get much time to adjust. The very next Monday, she had to start school.

My mother turned out to be resilient and radiated a kind of pride that she never lost. As was the way in those days, she was soon assigned household duties and helped bring up her younger siblings.

She was the ideal match for my father, who saw hard work as the ultimate virtue. While my mother went out to work at the