NRB

DARING TO COMMIT

PROTECTING YOUR DATA TO PROTECT YOUR COMPANY

CYBERSECURITY IS A MAJOR ISSUE FOR BOTH THE PRIVATE AND THE PUBLIC SECTORS, ESPECIALLY AS ATTACKS HAVE NEVER BEEN SO NUMEROUS.

"A secure computer is a computer with the power turned off. And even then…"

This quote from Bill Gates dates from the beginning of the millennium. Twenty years ago, cybersecurity was already a hot topic. Today, the problem continues to spread at an extraordinary rate, particularly in the wake of the events that have shaken the world over the last years. "*The lockdown associated with the coronavirus and the war in Ukraine have contributed hugely to an increase in online attacks* ", confirms Vincent Ceriani, Head of NRB Group's Cyber Risk Services.

There is no shortage of examples of data theft. Every week, a new case comes to light, and the consequences can be disastrous. Big cities and hospitals as well as companies are targeted by hackers, who are always looking for a victim on whom they can launch an attack. "*Smaller companies are afraid of losing money or having their production stopped for weeks at a time. Bigger companies are afraid of their reputation being damaged* ", explains Lorenzo Bernardi, Head of Security Services of NRB.

The threats are well known, as is the nature of the attacks. "***Hacking and ransomware are the two trendy options***, *so to speak. For example, two of our clients have already been hacked during the first three months of this year* ", says Lorenzo Bernardi. "*Malicious characters can take possession of data because updates have not been carried out regularly. Yet it's a simple thing to do, but too many companies still don't have that reflex. Everyone talks about cybersecurity but, in reality, we notice that there's a real lack of knowledge in this area.*"

The NRB Group's expertise is recognised in both the private and the public sectors. This is evidenced by the fact that the turnover related to cybersecurity has increased sixfold in the last four years, and the value of contracts in the first three months of 2023 has already exceeded that of 2022. "*This is not surprising because there are more and more connected systems, everything is computerized and criminal organisations understand very well the financial interest they can gain from it* ", explains Vincent Ceriani.

THE PROBLEM: LACK OF KNOWLEDGE

Cybersecurity is a subject that is regularly discussed in the media and in companies. However, **putting in place a good defence strategy is not as simple** as it appears, as everything seems new. "*Let's take the example of teleworking, which developed during the Covid pandemic. Remote working solutions were launched to enable employees to work from home under better conditions. Unfortunately, some of them did not opt for strong authentication, bypassing the need for a second authentication via mobile phone. In this situation, hackers only need a name and a password to hack successfully. Once they've got into a company's system, all the data is available to them* ", continues Vincent Ceriani.

Obtaining the data can be done with a single click. "*Imagine that a member of the secretariat, who's not very security conscious, opens an email promising them they'll win a super telephone if they give their name, telephone number and password. Like this hackers can access all the data and undertake whatever actions they want. A client told me recently that a hacker had stopped his company's billing emails being sent, had edited them to include the hacker's own account number and had then sent them out to the clients. You can imagine the consequences.*"

Companies are responsible for any personal data they have at their disposal, whether it concerns their own personnel or their clients. The General Data Protection Regulation (GDPR) was passed in April 2016, but the general public is still not familiar enough with its contents. *"Sometimes I get the impression that there are those who are only just discovering this law. If a hacker steals data, it's the company that will be held responsible.*

A client recently explained to me that they had given a sheet of paper to their delivery drivers with customer details and the schedule. Strictly speaking that doesn't pose a problem - unless the delivery drivers leave the sheet with the last customer because they don't need it anymore. Then the customer ends up with all the other customers' data (address, phone number, etc.)", explains Vincent Ceriani.

— **Vincent Ceriani**
Head of Cyber Risk Services The NRB Group

Fortunately, these problems are not insoluble. "***Hackers are very well trained*** *but there are standards and measures to slow them down*", says Lorenzo Bernardi. "*The CCB (Center for Cybersecurity Belgium) is making companies more and more aware of this issue. The Walloon Region is also multiplying the initiatives at different levels (training, education, society), as is the Cyber Coalition.*"

PENETRATION TESTS OFFERED DURING THE WAR IN UKRAINE

Data security is a major issue in society. Unfortunately, not everyone can afford to carry out an audit with a penetration test. At the start of the war in Ukraine, a time when hackers chose to increase their attacks, the NRB Group offered its services to non-profit organisations and schools. "*It was important to put our skills at the service of the population and the country. So we decided to free up time and staff to lend a hand to those who needed it most*", says Lorenzo Bernardi.

NRB GROUP RECOGNISED AS A SECURITY EXPERT

The NRB Group invests in Cybersecurity and offers a complete service to its clients. **Our experts can intervene on the legal and compliance level as well as on the technological level**. "*In our opinion, this combination represents the success of a security plan. Combining them closely is the way to win this battle*", asserts Lorenzo Bernardi.

To meet the needs of its customers, the Group is constantly recruiting security specialists. And they are given proper training. *"An IT specialist cannot secure an entire company, it's a separate job. There is a shortage of specialists in Belgium, to the extent that several thousand positions are vacant. NRB plays a fundamental role in this respect by recruiting young employees and then training them to deal with all the security issues. We could almost say that we are a talent university*" , concludes Lorenzo Bernardi.

Our company has a **full package** available, so as to be able to provide the best service for its clients.

1. The group is active in preventing attacks from inside and outside the company. The results are already significant, including, in particular, better protection against ransomware and awareness campaigns launched throughout the company.

2. Our experts are also specialised in detection, and carry out security audits of our clients, especially using "ethical hacking". Based on their findings, they draw up a roadmap for security improvements.

3. We help companies that have been victims of a cyberattack to recover their data and we offer them support concerning the regulations (GDPR).

4. Our Group is ISO 27001 certified, and our experts assist our clients in their own ISO 27001 certification.

— **Lorenzo Bernardi**
Head of Security Services of NRB

NRB EMPLOYEES TRAINED IN SECURITY

Not surprisingly, the NRB Group is a target for hackers. *"A big part of our internet traffic comes from Russia and China. Today, 25% of this traffic is still automatically blocked because we have identified it as a potential threat. We regularly face a significant increase in traffic, which is the sign of an attempted intrusion. Fortunately, our systems are protected effectively*", explains Lorenzo Bernardi.

To counter these threats, every employee is required to follow various modules dealing with security. The Quality & Risk team, headed by Emmanuelle Lhermitte, is responsible for this training and for raising awareness among our personnel, especially via phishing tests that are carried out each quarter. If a randomly selected person falls into the trap, they will be followed up individually. *"Every employee must follow these training courses, according to the needs of their job. Each module ends with an assessment. We do our utmost to raise awareness of the risk of hacking throughout the group"*, says Emmanuelle Lhermitte.

CONTACT

INFO@NRB.BE

www.nrb.be

www.linkedin.com/company/nrb

@daringtocommIT

info@nrb.be | +32 (0)4 249 72 11

NRB S.A. / nv Parc Industriel des Hauts-Sarts - 2e Avenue 65 - 4040 Herstal | Boulevard Bischoffsheim, 15 - 1000 Bruxelles / Brussel

THE NRB GROUP

bsi. ISO 9001:2015 Quality Management FS 706532 ISO/IEC 27001 Information Security Management IS 706533

Designed at NRB | 23/11/2023