News

Coronavirus in the cyber world: do you know how to protect your company?

Written by: Horiens - 13/04/2020

From the physical to the virtual world in a snap. Yes, Covid-19 made cyber risks light up fire red on companies' agendas. If cyber attacks were already considered one of the great risks of today, the problem has now become considerably more critical.

In Brazil, the number of digital devices in use already exceeds the number of Brazilians. Add to that, the increase in the volume of strategic information that circulates online during quarantine to prevent the coronavirus and, consequently, while working from home. All of this creates a scenario of greater vulnerability, full of cyber crimes, of the most varied types and proportions.

"The need for companies to adopt a strong digital information security strategy has never been greater than now," explains Eduardo Damião, the specialist in Cyber ??Risk Insurance at Horiens.

The size of the problem

We already know that well before the new coronavirus, cyber risks had a captive place on the list of the greatests risks of this century. To give you an idea, the FBI's 2019 Internet Crime Report consolidated data of more than 400,000 complaints from around the world, which added up to more than US$3.5 billion in losses for victims.

Brazil is an important target for cyber attacks. A study by Symantec shows that the country is among the main targets and ranks 4th in cyber crime rankings, only behind the United States, China, and India.

In the midst of the current crisis, a report from the World Economic Forum released last March, includes cyber attacks among the risks that can have negative impacts in various sectors for a period of 10 years. According to the report, 75% of the approximately 750 experts and leaders consulted expect an increase in attacks that search for data or money in the current scenario.

Another study by Apura Intelligence, a Brazilian consultancy company specializing in digital security, released data totalling more than 63,000 potentially fraudulent events mentioning the word "coronavirus" in Brazil.

It is evident that there is no lack of data to alert the potential for cyber risks.

But which are the most common cyber risks?

This includes from data theft to invasions and sabotaging of infrastructure, energy, and supply systems or even financial ones, for example, with the potential to cause major impacts on society and the economy in general. The consequences can be localized or of gigantic proportions. All of them, in some way, cause losses.

According to the data included on the FBI’s Internet Crime Report – a report cited above – about half of the losses computed in 2019 were due to Business E-mail Compromise (BEC) fraud, by which scammers bribe company employees through email messages to make payments to accounts controlled by hackers. There are more advanced modalities of this type of scam, with intrusions into a company’s network to seek payment and supplier information.

In 2020, the fight against the Coronavirus has ended up creating the ideal environment for hackers to attack. Fraudulent files that use the name Coronavirus are widespread online – but make no mistake and be careful – often, the purpose of these files is to damage or encrypt data.

Among the most common cybercrimes, both for end-users and companies alike, the so-called **DDoS** ones stand out, i.e. denial of service attacks carried out by overloading the servers of a company, taking services offline. This type of crime has a direct impact on operations, causing financial losses. But the problems do not stop there; often this type of crime is a distraction designed to deviate the focus of IT security resources and open up other opportunities for more elaborate scams.

The list of possible crimes also includes **data hijacking (ransomware), system intrusion, installation of vulnerabilities, leakage of data or personal content, and compromise of security systems**, among others.

E-mails disguised with unknown sender or bots, the so-called internet robots, are examples of strategies used by hackers to commit cybercrimes.

How to be protected?

Experts warn that the question is not “if” a company will suffer a cyber-attack, but rather “when”. In the information age we live in, it is necessary to address the issue, understand the risk and its consequences, through and through.

This includes actions such as constantly updating technology systems, periodically revisiting the company’s digital security policy, conducting educational campaigns for employees, and contracting specific insurance policies, for example.

“The demand for cyber risk policies is greater. Companies need to assess their exposure first and then transfer part of those risks to an insurance policy that best meets their needs. Even when not transferring all risks through insurance, there can be mitigation of possible damages/claims. The topic requires attention and action by companies”, concludes Eduardo Damião.